RCA

Reference CCS Architecture

An initiative of the ERTMS users group and the EULYNX consortium

APS Concept Movement Permission

Document ID: RCA.Doc.63

Table of contents

1 Preamble

1.1 Release Information

Basic document information:

RCA-Document Number: RCA.Doc.63

Document Name: APS Concept Movement Permission

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	Bettina Morman, Frank Schiffmann, Philipp Schneider	First published version for RCA BL1 R0

3 Introduction

3.1 Type of document

This document is one of the detailed concepts about the trackside Advanced Protection System (APS). After the introduction of the concept of APS in /RCA.Doc.51/, it offers more details on how the $requirements from it can be fulfilled by further describing the ideas and solution concepts in the problem space area.

Notes

- This document is a concept and not a specification.
- This document describes solutions in the problem space and rather not in the solution space - it shall not restrict the solution space and vendors' diversity of ideas, nor competition.

3.2 References

Please refer to the references listed in /RCA.Doc.52/ APS Detailled concepts overview and /RCA.Doc.6/ *RCA documentation plan*.

3.3 Terms and abbreviations

Please refer to the abbreviations listed in /RCA.Doc.52/ APS Detailled concepts overview and /RCA.Doc.14/ *RCA terms and abstract concepts*.

3.4 Purpose, scope and delimitations

3.4.1 Purpose

The purpose of this concept is the description of conceptional ideas about the handling of Movement Permissions by APS, based on the basic requirements given in /RCA.Doc.51/, for later detailing in the specification phase.

This concept presents the main ideas, starting from the viewpoint of the current solution split between route securing and signalling including train control in the interlocking and further systems like the Radio Block Centre for ETCS L2. This part is given as so-called *Problem description*. This section is followed by a summary and detailed views on the solution foreseen in the concept phase of APS, comprising of fundamental ideas and applied scenarios.

The documentation is seen as an extract from the current work for starting both a scope check in the sector and a detailing. Further information on scope and delimitations are mentioned below.

3.4.2 Scope

The scope for the Movement Permission is defined by:

- Ensuring the safeguard of movement after switchable Field Elements are in correct state;
- Providing the basis for enabling the issue of a Movement Authority (MA) to a train such that the on-board control functions can supervise the train

The Movement Permission sets the outer limits for the operational movement of the train, given as MA from trackside to on-board, and also includes risk areas secured around the MA to assure safe train operation. The MA is to be implemented by a driver, assisted by an Automatic Train Operation (ATO) system, if present. The concept of the Movement Permission covers an approach by getting rid of the historical split between route and train control. Further information on the present philosphies can be found in the section *Problem description*.

As of now, this concept's scope covers "normal operation".

In general, the kind of intended operation is reflected by the principles for securing the movement, the specific restrictions like speed and the supervision of the movement by the train control system and/or the driver.

Normal operation is characterised as the operational mode with the highest technical safety level. This implies the full supervision of the movement and no additional restrictions. In contrast, any kind of degraded situation can occur. Derived from that split, different modes of operation are present. These can be accommodated by defining operational categories (directed train movement following a secured route path, directed shunting movement following a secured route path, free shunting movement in a certain area) or by a flag of the train control (e.g. Full Supervision or On Sight, in terms of ETCS as train control basis). For the Movement Permission as the concept of securing movements, several modes of operation must be considered.

Normal operation is characterised by:

- Directed movement from A to B in accordance with the train direction
- Securing of the running path including risk mitigation measures
- Enabling of train control operation in level of Full Supervision mode or several modes for operation by an ATO system, e.g. Mode Automatic Driving in terms of ATO over ETCS
- Full on-board signalling as a required condition for partial or full automated operation
- No need of consideration of additional restriction, e.g. by written order
- All essential train capabilities (e.g. braking capacity, ATP equipment) are available

Therefore, degraded modes are out of scope in this concept. Further examples of operational modes can be found in the next chapter Delimitations.

The mode of operation must be known to APS for granting a Movement Permission. Thus, an abstract representation, e.g. of Train Control Mode (showing the kind of supervision and responsibility of the driver), is needed. This is similar to different route types or additional conditions for signalling in current interlockings. In addition to the mode, several conditions and restrictions apply for the Movement Permission (see Specific scenarios). The current scope will be set for enabling a radio-based MA with maximum responsibility lying on the technical solution and less at the driver. This can be recognised by the current ETCS modes Full Supervision (FS) or Automatic Driving (AD) in terms of usage by ATO.

3.4.3 Delimitations

3.4.3.1 Normal operation

According to the /TSI OPE/ there are three major categories for operational modes:

- Normal operation
- Degraded operation
- Handling of emergency situations

Delimitation	This document is currently restricted to normal operation.

Further modes of operation are grouped by e.g.:

- Movement with partial shift of responsibility to the driver, e.g. check of route path clearing in a defined section of the movement by the driver (e.g. in case of On Sight mode of ETCS or function Track Ahead Free Request used)
- Movement against the direction of train orientation
- Movement with restricted supervision
- Movement with very restricted supervision in fall-back situations, like in case of non-regular situations (incident/accident)
- Movement with reduced braking capabilities, e.g. incomplete braking link in operations like shunting movements today
- Free movements in a certain area without directed route path securing, e.g. a working machine can operate freely in a defined area
- Remote control of the movement
- Handling of incidents and accidents

Such operational modes are not analysed in this concept.

3.4.3.2 Operational scenarios

At the current stage of this concept, not all operational scenarios can be listed and detailed for impacting the Movement Permission approach.

Delimitation	This document covers only some operational scenarios. At a later stage a check between the technical solution Movement Permission and the to-be-covered operational use cases and scenarios must be made. This will enlarge the conceptional ideas of the Movement Permission.

3.4.3.3 Migration and handover

In addition to the intended usage of handover situations between different installations for migration purpose, the handover from and towards APS linked to legacy installation must be assisted. This means a coupling with route or line block information on the interface.

Delimitation	This document does not focus on migration and handover towards different signalling systems in detail.

4 Problem description

4.1 High level functionality

Efficient railway lines are characterised by a centralised entities, which secure and grant every train movement. The request for a movement is checked based on particular safety rules. The permission is submitted to the train, and the movement is then supervised by the centralised entity.

4.2 Current solution

The functionalities of the Movement Permission concept can be split into three major parts:

1. Route path securing, by route and/or line block information → route setting and locking
2. Indicate permission to move → issuing the movement restrictions, e.g. by signal aspect or on-board signalling
3. Train control functions for supervision → supervision of the movement according to the supervision functions of the Automatic Train Protection (ATP) system

The parts (1) to (3) are split into several domains in legacy applications and handled by different systems that are developed independently.

The overall application can be named as *block centric or track centric approach*, due to a historical lack of information on the trackside domain about the specific movement and the capabilities of the train. The securing is derived by track occupancy information according to defined rules. This means that the securing of a movement is in most cases independent of any other movements, but considers risk-based that further movements could be present, posing possible hazards towards the planned movement.

In addition, the current functionality is referring to different safety levels and responsibilities split between driver and the trackside signalling system. From a historical point of view, several modes of operation are present in various countries:

- Train movements using train routes on a high level of supervision (normal operation)
- Shunting movements using shunting routes
- Free movements in a certain area without directed route path securing, e.g. a working machine can operate freely in a defined area

As state of the art, different combinations of products are present. Two main bundles are:

- Interlocking with light signals and national ATP or a non-radio based ETCS solution with ETCS L1
- Interlocking with interfaced Radio Block Centre (RBC) (with or without light signals)

The interlocking is responsible for functionality (1) listed at the beginning of this chapter. The light signals of the interlocking or the interfaced RBC are taking over functionality (2) for the signalling. In case of an interlocking and an RBC being present, this is a mixture of a nationally developed product and an Interoperability Constituent (RBC) defined in the /TSI CCS/. The RBC is based on specific needs on the Infrastructure Manager and enables a technically

compatible exchange of information towards the on-board train control equipment for enabling functionality (3). A minimal standardised binding between route and signalling in terms of ETCS is used as train control system, given by basic operational definitions of the /TSI OPE/ and the operational annex. This includes e.g. the definition of the European Written Order, used in fall-back operation but also in standard use cases like the initial start of a movement.

The railway operation is handled through fixed routes on which trains can run free of conflict and in a safe manner due to the routes being implemented following site-specific locking tables. This means that every route has a fixed starting point which is usually signalled by a light signal, marker board or location marker. The kind of signals have an interdependency to the present train control system and its functions. At borders of interlockings, instead of routes line block information are used in many cases.

Trains - i.e. train drivers - are informed about the trackside equipment (light signals, marker boards, location markers, speed restrictions etc.), so they know how to adapt the motion state of the train (braking, acceleration). On-board signalling is possible, but not present on all lines. The permission and the authority of a movement are clearly split into several technical domains.

4.3 Problems with current solution

Today's interlockings are historically evolved systems that have been adapted to encompass new functionalities according to evolving requirements for risk mitigation (as a result from accidents or legislative changes) and new technological developments (e.g. higher grades of automation or the introduction of ETCS).

They also include non-standardised, national and site-specific operational rules and configuration implementations, which further inflates the necessary project engineering, testing and maintenance effort, e.g. in case of possible adaptations of previously existing rules and configurations. Furthermore, this leads to a high interdependency to lifecycles of neighbouring systems (e.g. an IM cannot replace an end-of-life interlocking without adapting the interconnected RBC), and thus to high lifecycle costs. These architectural and economic challenges are addressed in high-level documents like /RCA.Doc.50/ (Business strategy, targets, and problem definition).

Several problems refering to the securing of the route path can be derived explicitly for the enabling of the functionalities (1) to (3) introduced in the previous chapter:

- Movements can only start and end at specific locations, mostly indicated by a signal (board or light signal).
- Running path securing based on fixed rules without respect to the real need of securing based on risk evaluation.
- Running path securing takes place in fixed discrete sections, i.e. track/space oriented. This leads to an unnecessarily high capacity consumption.
- Optimisation of the usage of infrastructure by handling of different distances between trains by using full blocks and sub-sections is complex and limited to specific train control functions.
- The development of securing the running path and the signalling (interlocking) and train control part is not really aligned, due to historically diverging approaches.

- It creates great effort to put an interlocking into operation, because it is not designed to be fully interchangeable, scalable or arbitrarily expandable.
- Installation and handling of temporary restrictions lacks technical assistance and implicates a hugh effort.
- A modification of the topology leads to a major adjustment effort in the safety logic.
- Operational and safety functionalities are mixed in a safe product, which leads to a high degree of complexity.
- Several parallel existing operational rules increase the complexity of operation coping with the technical deficits.

5 Solution summary

The requirements derived in /RCA.Doc.51/ based on the business targets in /RCA.Doc.50/ and the subsystem objectives for APS listed in /RCA.Doc.53/ provide the basis for the solution concept defined in the next chapters. The requirements tracing is done separately in a tracing table.

Subsequently, a brief summary of the proposed solution to meet the APS requirements is given. Thus, the key paradigm shifts compared to today's principles to secure and grant a train movement, which were outlined in the previous sections, shall be explained.

- Route protection:
  - Shift from protecting a track area to protecting Movable Objects (MOBs, see /RCA.Doc.67/) using the track (or the space around the track)
  - Shift from securing whole routes, just in case an event occurs, to efficient, risk-based securing of track elements according to specific situations (e.g. existence of conflicting trains)
  - Therefore, the route protection measures may differ to today's fixed requirements and vary in a wider range (types of MP, specific measures fitting for each movement) compared to legacy applications depending on the Operating State
- Start and end of a train's running path
  - Shift from predefined starting and end points at discrete locations defined by interlocking routes for train movements, towards controlling (signalling) the train movement from any A to any B
  - The geometric extent of the secured path can be freely defined by the requesting system respecting the current operational environment
- Granting of a train movement
  - Shift from splitting route protection and granting a movement to one integrated concept (MP) covering both
  - With respect to ETCS that means a shift from having one route in the interlocking, one in the RBC and translating the signalling to the train as an MA, too. No distinguishing between components like an RBC (covered by /TSI CCS/) and nationally developed components like an interlocking
  - Functions (1) and (2) introduced in the previous chapter (*Current solution*) are performed by the concept of a Movement Permission which is the basis for function (3)

- Ensuring conditions for safe train movement are met
    - Shift from a continuous securing of all route-related elements to a risk-based securing of objects, depending on the Operating State
    - No securing of unused parts of a MP Extent, e.g. no need to provide flank protection, if there is no vehicle movement that can potentially endanger the protected running path (see Flank Protection section in /RCA.Doc.62/)
    - Generic Safety Checks that can be easily configured according to the requirements of the specific application
    - Usage of all present information in generic Safety Checks, enabling a specific movement reaching the safety targets

The Movement Permission is a discrete domain object covering the securing of a train movement based on a request. The domain object is described in /RCA.Doc.61/.

6 Solution details

6.1 Prerequisites

The following prerequisites are valid for the lifecycle and the function for enabling a Movement Permission in APS:

- Topology data including speed profile information must be present for the particular area of the movement.
- The setting of switchable Field Elements to the required state is already done before requesting a Movement Permission.
- Information on abstract representation of the train is present by the specific Movable Object (MOB), see /RCA.Doc.67/.
  Note: As this concept only covers normal operation, information on all *Movable Objects in an area is a prerequisite to make the risk based assessments without switching to degraded modes.*
  Note: In the following chapters "trains" will be referred to as "Physical Train Units (PTU)" if real-world trains on real-world tracks are meant. The abstract domain objects representing the PTUs, existing only inside APS, will be referred to as "resolved Movable Objects (rMOB)" or "unresolved Movable Objects (uMOB)".
- The Movement Permission Request derived from the Operational Plan with all information is present.

6.2 Relation to other concepts

For tracing the relation to other concepts established is given in a table. The ID refers to the documents named in /RCA.Doc.52/.

ID	Document	Description of relation
/RCA.Doc.47/	Concept: Plan Execution	This concept covers the conversion from the Operational Plan towards single requests to APS. The request for a Movement Permission is described as a trigger, for starting the lifecylce of a Movement Permission.
/RCA.Doc.51/	Concept: APS	This concept is the initial concept. It covers in chapters 4.3.3.1 and 4.3.3.3 the definition and the working principle. In terms of the Movement Permission concept, it defines the basic needs.
/RCA.Doc.54/	MAP concept	This concept describes how MAP provides reliable, validated topology and topography data, also referred to as Map Data, for all operational RCA subsystems, including safety-related components.
/RCA.Doc.57/	Digital Map - Evaluation Reference Model Topo/data	This document further evaluates the BNT (“Base Net element service Topology”).
/RCA.Doc.61/	Concept: Operating State	This concept describes the domain objects of APS. More information for Movement Permission e.g. the background and definition can be found there.
/RCA.Doc.62/	Concept: Route setting and route protection	The concept describes, among other things, the switching of Field Elements as an essential prerequisite for the Movement Permission. In addition aspects like the function of route clear proving is mentioned.

ID	Document	Description of relation
/RCA.Doc.67/	Concept: Movable Object and Object Aggregation	The concept describes the abstract representation of PTUs including the object aggregation. The presence of an rMOB covers a prerequisite for the Movement Permission.
/RCA.Doc.70/	Concept: SCI-CMD	This concept summarises the exact format of messages and data types on the interface exchange. The Movement Permission is one of the exchange items.

6.3 Premises

This chapter gives an overview of premises on which the concept of the Movement Permission is based on.

Deployment of generic Safety Checks

- No operational and processual checks are being performed.
- Purely geometric checks based on the topology and the Operating State, following the risk-based approach considering all operational information of the Operating State.
- Checking the requested running path and safety margins for occupied track sections that potentially overlay with the requested MP (formerly route clear checking).
- Prevent collisions with other objects of the railway system (clearance profile violation).
- The MP includes a summary of all present restrictions (e.g. due to topology or PTU configurations).
- If all Safety Checks are positive, MP request is granted by APS.

Representation of MP in the Operating State

- Like all APS Domain Objects, MPs follow the principle of geometric representation, as outlined in /RCA.Doc.61/. This means that their geometric extent can be precisely mapped to the base network topology (see /RCA.Doc.69/).
- Mechanical locking of Field Elements starting from the Device Control Layer is considered in /RCA.Doc.62/.
- MP must cover the full extent of the rMOB, for enabling movements and securing switchable Field Elements.
  Note: This may not apply in degraded situations.
- The MP request determines where the MP ends; this is known to APS.
- A train without an active mission (i.e. before Start of Mission (SoM) or after End of Mission (EoM)) does not need a MP, thus MP is a symbol for an intended movement.

Logical locking of switchable Field Elements

Logical locking of elements in APS is done according to the following principles:

- All DPS (groups) representing switchable Field Elements must be properly set and locked before an MP can be granted and supervised in its state during the presence of the MP.

- The Operating State (which also includes the setting states of switchable Field Elements) from the moment the MP request is processed, has to remain unchanged. DPSs are not permitted to change once an MP is created up to when the MP is removed, in the area of the requested MP. Thus, the MP object is created internally early for ensuring the logical lock of switchable Field Elements in processing phase of MP Request.
- All DPSs representing switchable Field Elements must be kept locked as long as an rMOB has authority to move on them, i.e. they are claimed by an MP.

The technical principles being used in different states are a prerequisite for enabling the functions for an MP:

- APS-internally a DPS group can be either locked - restricting the changing of element positions - or unlocked. However, a locked state in terms of MP can have two different operational implications:
  - Locked status, while an MP Request is processed: The DPS group is set and physically locked into the current position. When an MP request is processed, an MP object is created which locks the DPS group. The APS Operating State remains unchanged, as the MP request is not yet resolved.
  - Locked status, while a granted MP is present: The DPS group is set and physically locked into the current position. The APS Operating State is adjusted, an MA is issued.
  - The locking is released, if - for whatever reason - the MP object is not linked to the DPS group anymore.
- This technical principle of locking can be compared to the principles used in key interlockings.

To be investigated	There is also a need for an individual logical locking of elements, apart from the MP process. The process for this individual locking is yet to be defined.
	The definitions of the terms Safety Checks and Safety Rules are yet to be finalised. In this document Safety Check refers to the action being executed (function), Safety Rule refers to a specific safety principle being checked.

Communicating a granted MP

- MP is considered to be dynamic data in the Operating State.
- The principle used for train separation (i.e. fixed or moving blocks) is not visible to the PTU, meaning that each movement can start and end at any point, if further restrictions do not delimitate this. Therefore, the MA principle from ETCS following the combined ETCS Level "R" as sum of ETCS Level 2 and 3 is fully used, not restricting the position to the currently marked location like signals in the field.

Identification of safety condition violation after granting an MP

- Continuous supervision of the granted MP during its lifetime by APS.
- Results in an intervention (e.g. MA shortening at the front - shorten the permission to run, enabling a safe stop of the PTU), if a safety condition violation is detected.

- Keeping the MP securing the route path as long as needed.

6.4 Parts of an MP

In case of normal operation a Movement Permission (MP) belongs to a directed movement from A to B. Physical switchable Field Elements can be present, represented by DPSs (see /RCA.Doc.61/). This is the base for the so-called basic scenarios (see below).

The MP has a geometric extent and has mandatory and optional parts. These kind of information can be divided in general into two parts:

- **Running path** - the section in which the movement shall occur, in general including the rMOB itself.
- **Safety margin** - one or more buffer sections for reducing any risk of collision. In some situations there can be MPs without any safety margins.

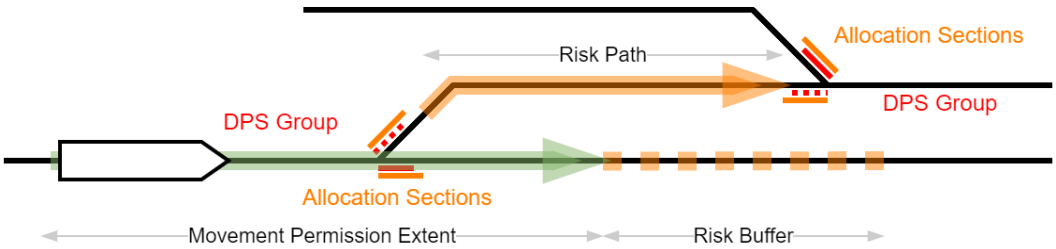
In case the necessity is marked "mandatory", this part is present for every Movement Permission. Optional means, that this content could be present, depending on a) the topological situation and/or b) the specifc rules of the Infrastructure Manager to be applied in a certain area. An Infrastructure Manager could opt out of the use of optional elements. However, this does not have an impact on the functional specification.

Part	Content	Explanation	Necessity	Remark
Running path	MP Extent	The Movement Permission Extent (MP Extent) is a Linear Contiguous Track Area (see /RCA.Doc.57/) on the topology in a defined direction. It describes the topological extent of the running path of the Movement Permission.	mandatory	It covers in normal operation the full extent of the rMOB. Further rules could be established for different modes of operation.
	Speed Profile	The Speed Profile of a Movement Permission is the requested speed profile for the intended movement.	mandatory	
	Further restrictions	Further restrictions of a Movement Permission could be the kind of the mode of operation, e.g. if the driver must take over responsibility in a certain area of the MP Extent.	optional	
	DPS state	DPS within the MP Extent must have a defined state for enabling the movement.	optional	Several DPSs can be present for one MP. An example are several points in the running path, each abstracted by a DPS Group.
Safety margin	DPS state	DPS present for safety mitigation, e.g. mitigitation of flank collision, must have a defined state for enabling the movement.	optional	Several DPSs can be present for one MP. An example are several points in the safety margin, each abstracted by a DPS Group.

Part	Content	Explanation	Necessity	Remark
	Risk Path	The Risk Path is a Contiguous Track Area on the topology. It is one potential path by which a non-permitted vehicle movement could result in a flank collision with a vehicle moving along an MP Extent.	optional	Several Risk Paths can be present for one MP. Each starts at an Allocation Section of a certain DPS. Further details on handling of flank protection are given in /RCA.Doc.62/.
	Risk Buffer	The Risk Buffer is a Linear Contiguous Track Area on the topology in a defined direction. It describes the extent of a navigable gap-free Track Area, in which a vehicle is protected in case of accidentally exceeding its authority. It must not overlap with another MP extent.	optional	

To be investigated	The handling of operational changes of Risk Buffers covering DPS groups, which represent switchable Field Elements, must be detailed at later stage. Thus, an operational solution shall be assured, which covers the demands from current present functions like "swinging overlaps".

The topological view based on /RCA.Doc.51/ can be taken from the following figure:



Note: The exact data object definition of a Movement Permission can be found in section Movement Permission Data objects*. The concepts of Drive Protection Sections (DPS) and Allocation Sections (AS) are introduced in /RCA.Doc.51/.*

6.5 Lifecycle of a Movement Permission

Considering the Movement Permission, several lifecycle phases are present. The phases and different functionalities are named in the table below.

Note: The lifecycle is seen from APS perspective. Hence, creation means the build-up of an MP in APS. Nevertheless an object which is complementary to the MP in APS already exists before on the level of TMS; it is part of the request given from PE to APS.

Lifecycle phase	Functionality	Description of usage
Creation	Request	The creation of a new MP must be requested for each Operational Movement. *Note: Since an Operational Movement can represent a long train run, it would not result in the request of one but more than one MP.* As a result of a request, the Movement Permission Domain Object is generated internally in APS, so that the Safety Checks can be carried out.
	Checking	After the request of an MP, Safety Checks have to be executed to determine if the request can be granted.
	Granting	Feedback to requesting system.
Modification	Extension	The topological extension of the MP extent can be requested before, during or after the execution of the train movement for which the MP was created. It involves the extension and/or relocation of safety margins.
	Upgrade	Changes of the upgradable attributes of an existing MP can be requested. An upgrade could be e.g. a higher permitted speed.
	Downgrade	Changes of the downgradable attributes of an existing MP can be requested. This implies, that a downgrade does not lead to unwanted braking reactions of the PTU. A downgrade could be e.g. a lower permitted speed.
	Shortening at front end	Before, during and after the execution of a train movement, the front end of the corresponding MP can be shortened if the avoidance or reduction of impact of a hazardous situation demands it. Another scenario is the shortening of unused parts in the safety margin, in case of operational completion of the movement.
	Shortening at rear end	The rear end of the corresponding MP is continuously shortened behind and advancing train movement.
Removal	Rejecting	If the Safety Checks were not carried out successfully, the request will be rejected and the data object MP will be removed.
	Removal	The removal of an existing MP can be requested before or after the execution of the train movement for which the MP was created. In certain situations, APS triggers the removal automatically.

6.6 Safety Checks

The basic task of APS is the establishment of a high level of technical safety. Therefore, before an MP may be granted, a series of Safety Checks are to be executed. As stated on a higher level in /RCA.Doc.51/, the primary task of these checks is not the fulfilment of operational or procedural requirements, though these cannot always be separated from safety requirements. Possible unwanted conditions like operational deadlocks shall be ruled out on a higher level, as the purpose of APS in general and of the following Safety Checks in particular is solely to avoid situations that directly lead to hazards. This is achieved by two categories of Safety Checks, namely

- General Safety Checks, e.g. providing unambiguous relations between an MP and an rMOB and

- Specific Safety Checks, which are always related to the respective topology. Good examples are the exclusion from conflicting movements or the providing of safety margins.

Coming to the point where MP Safety Checks are executed implies that other Safety Checks, if applicable, are already passed. These are referred to in /RCA.Doc.62/, e.g. dealing with DPS group states as representation of the correct state of the needed switchable Field Elements.

The execution of MP Safety Checks and following actions are based on a certain rule set:

- Each Safety Check requires the knowledge of the Operating State - see /RCA.Doc.61/. If this knowledge is not safely provided, the MP request must be rejected.
- Each Safety Check must result in either True or False.
- An MP request is rejected if at least
    - one Safety Check or
    - one required combinations of Safety Checks failed.

The specific Safety Checks are listed in the appropriate scenario chapters.

6.7 Basic scenarios

6.7.1 MP granting

This basic scenario deals with an initial request for an MP, succeeding APS internal Safety Checks and the eventual granting of the MP.

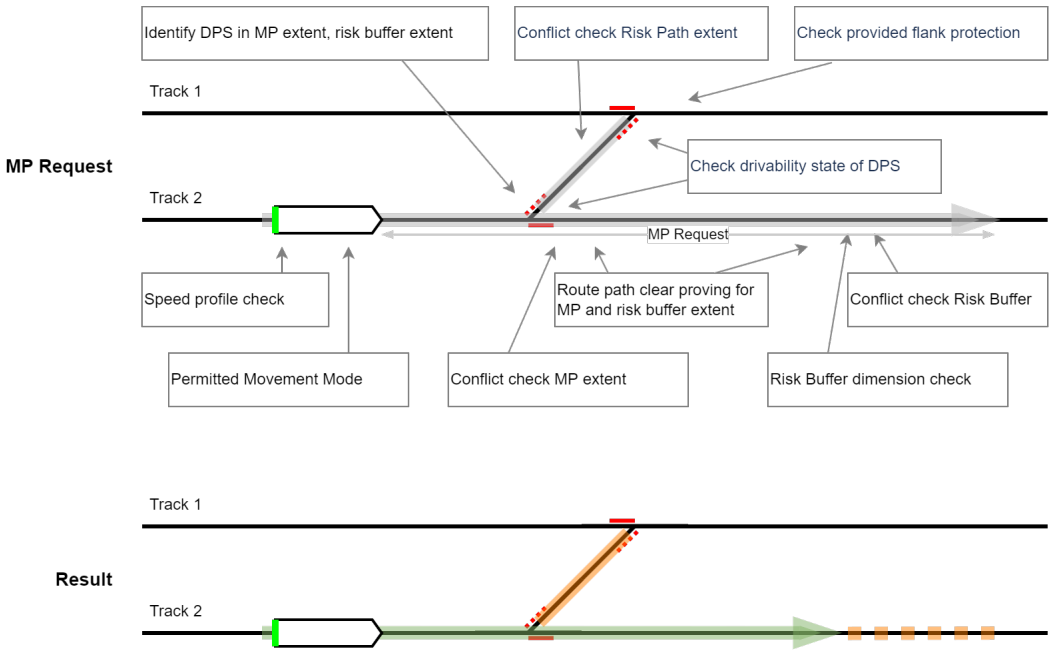
An MP request is sent by PE via SCI-CMD (see /RCA.Doc.70/). It aims only at the creation of a new MP - the upgrade or extension of an existing MP are not in scope of this scenario (see below).

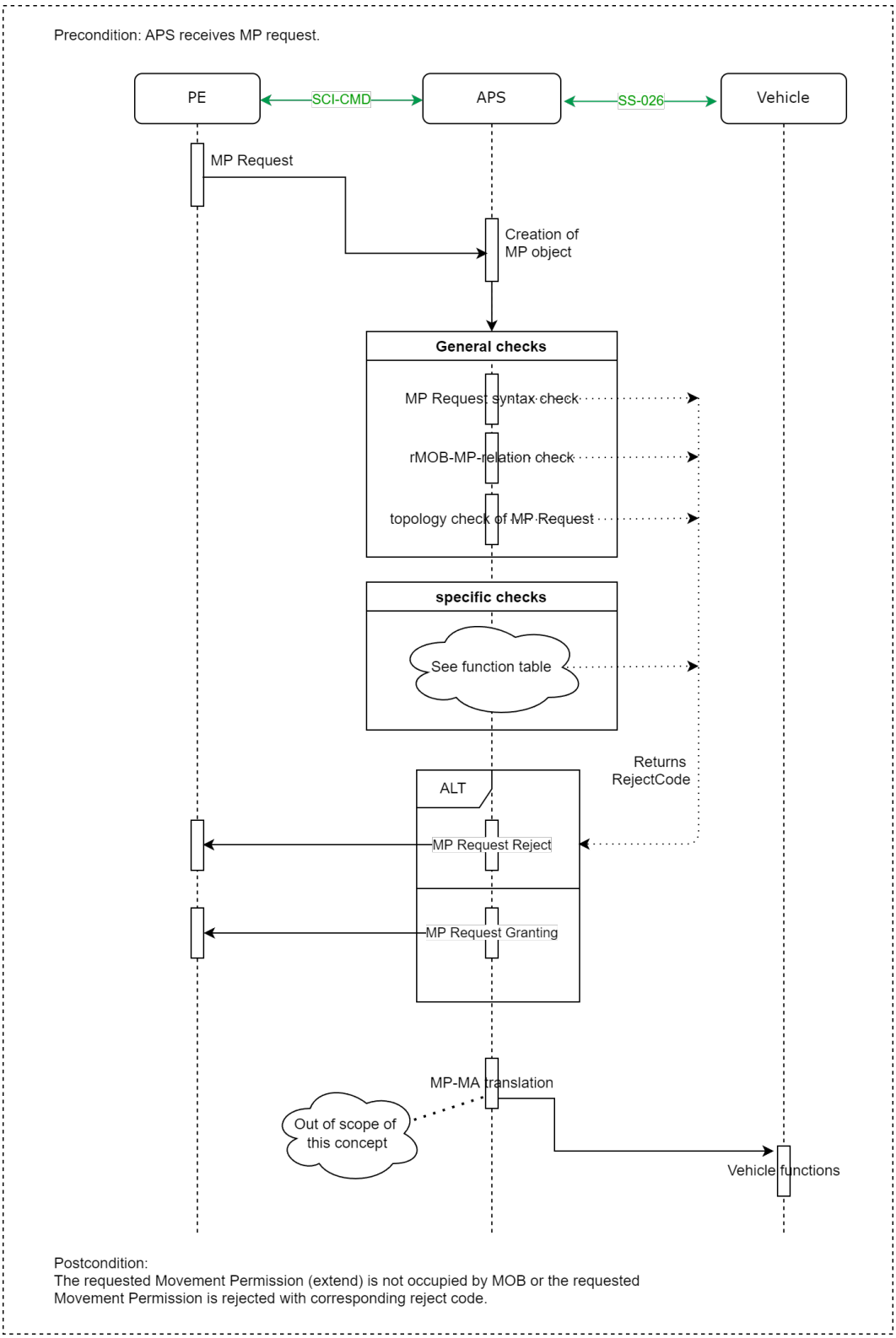
Being ready to receive an MP request implies the fulfilment of several preconditions with respect to the addressed rMOB. These preconditions are summarised in the following table:

Need on rMOB	Content	Explanation
rMobID	Unique identifier of the rMOB	The identification must be unique per train unit, this is done by a unique MobID of the rMOB. Therefore, an ID-Management is needed including a linking between rModID and the rMobDomainID. See /RCA.Doc.67/.
State	Referenced MOB is an rMOB	This scenario starts with an rMOB.
Localisation	rMOB is localised	The state of the localisation information (position) must be known for issuing the correct permitted movement-mode-dependent MP, e.g. valid and trustworthy.
MobExtent	rMOB has a safe extent rMOB direction	The extent of the rMOB must be known, mapped to the topology with its direction (rMOB direction must map to MP direction).

Note: Deviations from these conditions - e.g. the presence of a uMOB instead an rMOB - lead to the need for different scenarios. For details on the MOB concept, see /RCA.Doc.67/.

The following figures (first a topological view, then a sequence diagram) depict the scenario of an rMOB on a simple topology with two points and the respective DPSs. PE sends an MP request to APS. The requested MP can basically cover a linear contiguous track area between any two discrete locations on the topology. However, operational or construction restrictions may apply, e.g. non-stopping areas like tunnels or neutral sections. APS then performs a series of general and specific (topology-related) Safety Checks, which are summarised in the table at the end of this chapter. Eventually the MP is granted, as no Safety Check fails. A more complex topology would increase the Safety Checking effort in terms of more different checks and/or more applications for each check. However, this would not interfere with the illustrated principle.





For checking that the limitations from occupied track sections are being respected, APS basically compares two geometric extents for overlapping. This so called geometric overlap check is based on defined generic safety rules and will be used in a Safety Check to detect a possible overlap between the extents which are needed for the requested route with other

present occupancies. Any track occupancy of the following sections by an rMOB will result in the MP request being rejected:

- The MP Extent is occupied by any other MOB (rMOB or uMOB) than the one the MP is requested for;
- Any Allocation Section within the MP is occupied by a MOB;
- The Risk Buffer extent is occupied by a MOB;
- Any Risk Path extent is occupied by a MOB.

After the MP is granted by APS, two actions result as direct consequences:

1. The Operating State in APS is updated according to the granted MP. Afterwards, respective information (MP extent, Risk Path(s) and Risk Buffer) is sent upstream towards PE, so that the PE Operating State can be updated, too (compare /RCA.Doc. 61/).
2. Inside APS the MP is translated into an MA and then transmitted according to /ETCS SRS/ to the PTU. The chapter *Relation between MP and MA/signalling* provides some information on this process.

As mentioned above, if one required Safety Check or one required combinations of Safety Checks is violated, the MP request will be rejected and neither of the two aforementioned consequences will take place.

The following table lists the Safety Checks and additional functions which are executed after an MP request is received by APS from PE. All mentioned functions are triggered by an MP request, which also provides one portion of the input data necessary to execute the checks. Another important portion is topological input provided by Map Data (see /RCA.Doc.54/).

Some of the specific checks may be configurable to be compliant with national rules. One example are the different national requirements on flank protection measures. The identifier MovementMode is used for marking different kinds of movement. In this concept, this must be assumed as a fixed value, as only normal operation as operational movement mode is covered (see *Introduction*).

Function	Description	Remark
General Safety Checks		
MP Request syntax check	The syntactically correctness of the MP Request is checked.	*If not, MPRequestRejectCode: SYNTAX applies*
rMOB-MP-relation check	The relationship between rMOB and MP Request is unambiguous. This means no present further MP Request or MP is present, if the MP Request is marked as "initial".	*If not, MPRequestRejectCode: INCONSISTENT_WITH_MOB applies*

Function	Description	Remark
Topology check of MP Request	The geometrical extent of the MP Extent and the geometrical extent of the Risk Buffer of the requested MP are consistent/fit to the topology and to each other. Each of those extents are checked to be a LCTA.	*If not, MPRequestRejectCode: INVALID_TOPOLOGY applies*
Auxiliary functions		
Identify all DPSs and ASs in MP extent and Risk Buffer extent	This function returns all DPSs and ASs, which overlap with the requested MP Extent or Risk Buffer Extent. *Hint: This includes DPSs and ASs, which are not fully overlapping with the MP Extent or Risk Buffer Extent.* *Note: Whether and, if so, which DPS must be locked in the Risk Buffer is a matter of configuration.*	
Specific Safety Checks		
Route path clear proving for MP and Risk Buffer extent	The MP Extent and the Risk Buffer Extent of the requested MP are not occupied, except by the rMOB itself. Neither is any Allocation Section occupied, except by the rMOB itself.	*If not, MPRequestRejectCode: PATH_OCCUPIED or RISK_BUFFER_PATH_OCCUPIED or AS_OCCUPIED applies*
Conflict check MP extent	The MP Extent of the requested MP does not overlap with any other Movement Permission issued. The Allocation Sections in the MP Extent (including dependent Allocation Sections) do not overlap with any other issued Movement Permission.	*If not, MPRequestRejectCode: EXTENT_CONFLICT or EXTENT_AS_CONFLICT applies*

Function	Description	Remark
Conflict check Risk Buffer	The Risk Buffer does not overlap with any other Movement Permission issued, except the Risk Buffer overlaps with another Risk Buffer and this overlapping is allowed by parameter. No Allocation Sections in Risk Buffer Extent overlaps with any other issued Movement Permission, except the Risk Buffer overlaps with another Risk Buffer and this overlapping is allowed by the configuration parameter.	*If not, MPRequestRejectCode: RISK_BUFFER_CONFLICT or RISK_BUFFER_AS_CONFLICT applies*
Risk Buffer dimension check	The length of the Risk Buffer in MP Request is equal to or greater than the minimum Risk Buffer needed.	*If not, MPRequestRejectCode: RISK_BUFFER_TOO_SHORT applies*
Permitted Movement Mode	The Movement Mode(s) in the Safety Responsibility Profile of the Movement Permission must be equal or less to the Permitted Movement Modes according to topology.	*If not, MPRequestRejectCode: SAFETY_RESPONSIBILITY_PROFILE_ INVALID applies*
Speed profile check	The requested speed of the MP is equal or less than the maximum speed given by topology and the speed derived from the requested Movement Mode.	*If not, MPRequestRejectCode: SPEED_PROFILE_VIOLATION applies*
Check drivability state of DPS	This function returns, if each provided DPS in MP Extent is in the required state. *Note: The required state is set to "FULL" first.*	
Conflict check Risk Path extent	The Risk Path extent of the requested Movement Permission does not overlap with any other Movement Permission issued. *Note: In general Risk Paths of several movements can overlap, this shall not lead to a failed check. This is the standard case, if the securing element of one movement is the element to be passed by the other movement, e.g. in case of two points forming a possibility of track changes in a double-track.*	*If not, MPRequestRejectCode: RISK_PATH_CONFLICT*
Check correct splitting of riskPaths	This function returns true, if at each Track Node in the requested Risk Paths a Risk Path continues into each navigable direction.	*If not, MPRequestRejectCode: RISK_PATH_MISSING applies*

Function	Description	Remark
Check provided flank protection	This function returns true, if the requested end of the Risk Path provides the required flank protection, i.e. a sufficient safety buffer on the flank.	*If not, MPRequestRejectCode: UNPROTECTED_RISKPATH applies*
Route path clear proving for Risk Path extent	The Risk Path extent in MP Request is not occupied.	*If failed, reason RISK_PATH_OCCUPIED is returned*
Check Risk Path allocation	Based on the identified Allocation Sections, APS checks if for the end of each Allocation Section a Risk Path has been requested.	*If not, MPRequestRejectCode: RISK_PATH_MISSING*
Output functions		
MP Request granting	A Movement Permission Request fulfilling all general and specific Safety Checks will be granted.	This MP is the basis of issueing an MA.
MP Request reject	Reject Movement Permission Request if at least one Safety Check or one required combinations of Safety Checks failed	*If applicable, an MpRequestRejectEvent is sent with at least one MPRequestRejectCode*

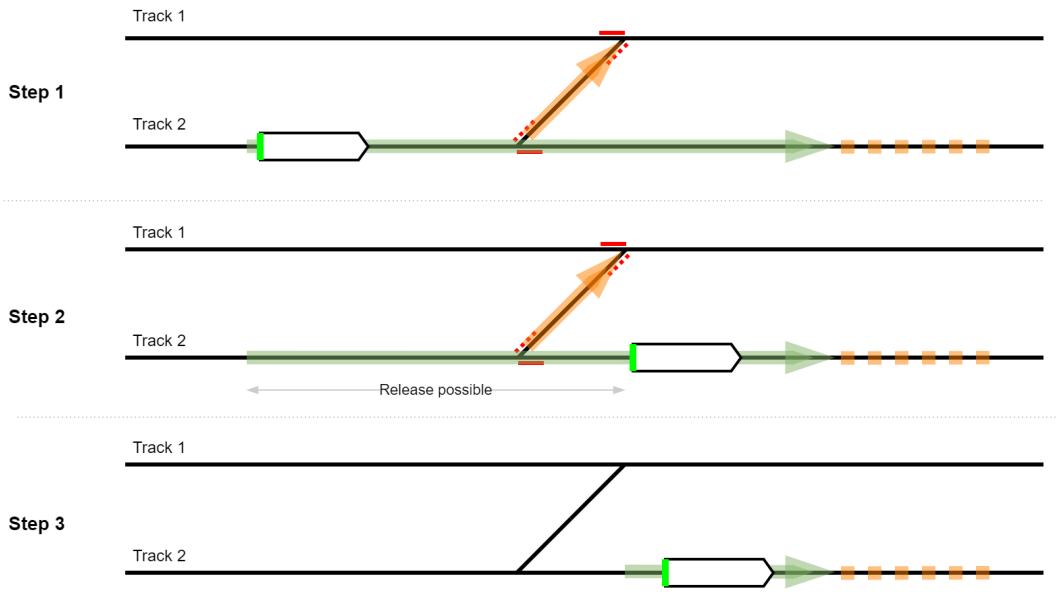
Note: The Reject Codes will be detailed in the SCI-CMD concept, see /RCA.Doc.70/.

6.7.2 Shortening at rear end

Within this scenario, an rMOB is moving along a Movement Permission and the shortening at rear end shall be shown.

Preconditioned that an MP Request was already granted, a PTU is moving. This implies the stepwise change of position and extent of its representing rMOB. Thus, sections will be cleared by the the rMOB in the rear and can be used for further operational movements. This needs a release of the Movement Permission after passage of used sections.

The following figure illustrates the topological view with three simplified steps of the scenario:



The rMOB moves, leading to an update of the track occupancy. A release of a used/passed part is possible. The release of parts of the Movement Permission in this example covers also the handling of DPSs. The locking of the DPS representing the point which is already passed is released. This is valid for the passed DPS and the DPS representing the point giving flank protection and the Risk Path in between. The further parts of the MP Extent and the Risk Buffer is shown as unchanged. As a result of this scenario the track occupancy represented by the Movement Permission is shortened, DPS hold in fixed state needed for passage or mitigation measures are released, too.

The release of parts of the Movement Permission enables the following:

- Release of the locking of associated Drive Protection Sections (DPS) in MP Extent and Risk Path
- Release of track occupancy provided by the Movement Permission
- Usage of the released infrastructure for further movements or construction works

Apart from functions for the continuous update of the track occupancy for the rMOB as trigger for this scenario, functions for shortening the Movement Permission are needed. These are the following main functions:

Function	Description	Remark
Specific Safety Check		
Shorten MP at rear end	After the safe rear end of the corresponding rMOB is updated, the MP will be automatically shortened.	The sections to be cleared depend in the extent on the kind of information of localisation of the PTU, thus this can be referenced toward TVPS borders known by APS or on the abstracted representation of the PTU, the rMOB, or a mixture.
Output function		
Update shorten MP at rear end	APS forwards the updated MP with the changed MP Extent to PE.	This is the function to inform PE via SCI-CMD with information event MPUpdateEvent

Note: The description of the scenario is valid for the positive situation, that the release can be performed accordingly. Any handling of a manual release after passage, e.g. for the handling of any faults, will be elaborated in a later version of this concept.

6.7.3 Removal

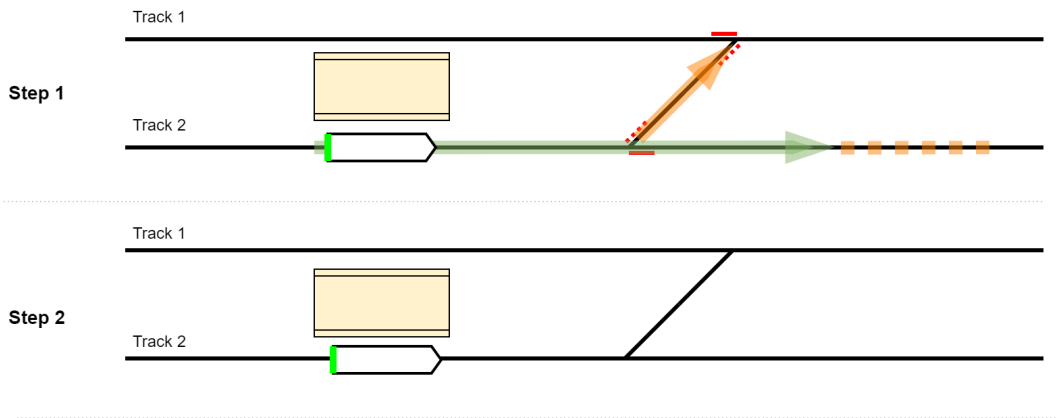
In addition to the possibilities of partially removing an MP, i.e. shortening at rear end and shortening at front end, a complete removal of the Movement Permission can be necessary.

Preconditions like in the scenario before with a presence of a granted Movement Permission apply.

Three triggers for this scenario may be under consideration:

- The removal is requested by PE.
- The operational movement is finished by the Train Driver or an ATO system, indicated by a so-called End of Mission.
- The movement is leaving the APS Area of Control (AoC).

The topological view shows the inital step 1 with a certain Movement Permission present. In step 2 the Movement Permission including the Risk Buffer, the Risk Path and the locking of the DPSs is released. Only the track occupancy of the rMOB representing the PTU is present afterwards.



Two results are generally possible:

- All parts of the Movement Permission are removed and only the rMOB is present (as shown in the figure above), or
- Removal was not performed, due to a Safety Check violation.

The following table summarises main functions needed in the sum of scenarios with a planned or automated removal of the Movement Permission. Not all functions must apply in each specific case.

Function	Description	Remark
General Safety Check		

Function	Description	Remark
Movement Permission Removal Request syntax check	The syntactically correctness of the Movement Permission Removal Request is checked.	
Specific Safety Checks		
Handle Movement Permission Removal Request	If the PTU reports a speed = 0 (stationary) and the cooperative shortening of the MA can be performed, the MP can be removed.	
Remove Movement Permission	When an End Of Mission is present and the conditions for removal of the MP are fulfilled, the MP is automatically removed.	this function is triggered automatically without any request by PE
Output function		
Update Movement Permission Removal	APS communicates to PE the removal of the Movement Permission or a rejection.	the result is given by a certain MPRemovalEvent or a rejection notification

6.8 Specific scenarios

6.8.1 Additional functionalities

In addition to a basic scenario for a simple check of an initial request for a Movement Permission and functions for handling a simple Movement Permission, several functionalities are needed. These functionalities originate in additional lifecycle phases or functions referring to further present data.

An overview of these functionalities is given in the table below. At this stage, there will be no full list of all needed functions given in detail.

Lifecycle phase	Functionality	Description of further Safety Checks	Specific scenario within this concept
Creation	Handling of additional checks, e.g. route suitability	An additional functionality that checks prior to issuing the MA whether the rMOB fits to the topological restrictions or not. Here the Safety Checks compare the limitation of the MP extent and the optional Risk Buffer with the provided information on the PTU known in the rMOB.	not in scope of this concept
	Flank Protection provided different to DPS state	In addition to providing flank protection by a DPS in required state, different conditions can apply. A safety mitigation could be possible by sufficient distance between the rMOB to be protected and further rMOBs, and knowledge of the exact location of the PTU. The Safety Checks will cover this scenario, if this is requested.	not in scope of this concept, see /RCA.Doc.62/

Lifecycle phase	Functionality	Description of further Safety Checks	Specific scenario within this concept
	Activation of Level Crossing	If a Level Crossing is present, the creation of a Movement Permission must consider this. Safety Checks will cover the specific behaviour of the type of the Level Crossing.	not in scope of this concept, see /RCA.Doc.62/
	Handling of Usage Restriction Areas	Safety Checks consider present Usage Restriction Areas within the MP extent and the optional Risk Buffer. These could include speed restrictions, for example.	see *MP restricted by URA*
	Handling of Warning Areas	Established Warning Areas are considered in addition in the Safety Checks. This implies the need of an in-time warning of Track Workers on the line in a certain area called Warning Section. This functionality can be extended by delay of start of movements for enabling the pre-warning time or a halt of the movement up to the confirmation of clearance of a certain area by the staff.	see *MP in relation with WA*
	Handling of Handover situation	In case the movement will start or end crossing a border of the Area of Control, the Safety Checks considers the needed state and information from the adjacent system.	see *MP at border/transition*
Modification	Extension	In case of requesting an extension, similar checks like for initial creation including the fitting to the existing Movement Permission will be performed. *Note: Extension means no change on the already granted Movement Permission, besides the exchange of a present Risk Buffer by a part of the MP Extent.*	see *MP extention*
	Upgrade	In case attributes shall be upgraded, the Safety Checks must be performed similar to the creation. If f.e. the upgrade covers an increased speed in a certain area, the request must be checked against the suitability considering the maximum allowed speed in the area. An increased speed referring to a higher grade of mitigation measure for flank protection, is also considered as an upgrade.	see *Upgrading an MP*

Lifecycle phase	Functionality	Description of further Safety Checks	Specific scenario within this concept
	Downgrade	A downgrade occurs if one of the MP attributes becomes more restrictive. The Safety Checks cover two main items: 1. The check against the topological limitations similar to a creation 2. The downgrade does not lead to unwanted braking reactions of the PTU *Note: In some cases a braking reaction is requested, thus the second mentioned item can be skipped in some variants of the scenario. The details must be defined at a later stage.*	not in scope of this concept
	Shortening at front end	For a shortening at front end, the Safety Checks covers the need of the fulfilment of the conditions of absence of possibility occupying the shortened area by the train movement.	see *Shortening at front end*

A mapping to further possible scenarios described in the next chapters is included in the table.

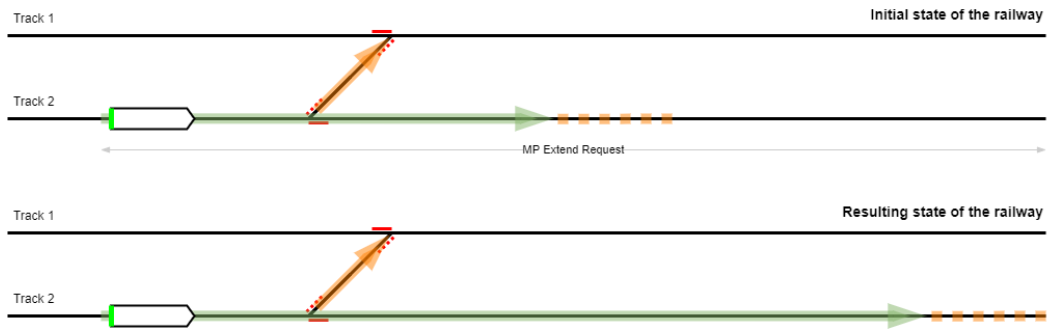
6.8.2 MP extension

An already granted Movement Permission can be extended, thus avoiding an unnecessary stop at the end of the MP if the PTU (from an operational and safety viewpoint) can continue running.

For the extension of an MP, the scenario unfolds mostly along the lines of the scenario *MP granting*. The "MP request" can be substituted by "MP Extend Request" to describe the scenario for extending an MP. For granting the MP Extend Request of an existing MP the following (pre-)conditions must be met:

- An MP with the received identifier (MP Id) must exist.
- The direction of the received MP Extend Request must match the direction of the existing MP.

The scenario for extending an MP is illustrated below.



Given that all Safety Checks for the received MP Extend Request are met, APS will generate the resulting Movement Permission by performing the extension as follows:

- The Risk Buffer of the resulting MP is the Risk Buffer of the requested MP.
- The attributes of Risk Paths, speed profiles, movement modes and track conditions of the resulting MP is the concatenation of the corresponding lists of the requested MP and of the received MP Extend request.

The following table summarises the functions needed in addition to the functions in the chapter *MP granting*:

Function	Description	Remark
Specific Safety Check (in addition to scenario *MP granting*)		
Extension check MP	Check if the MP Extent of the current Movement Permission with the same Id as the requested Movement Permission is fully contained in the MP Extent of the requested MP and does not differ in any attribute (Speed Profile, Permitted Movement Mode(s), etc). *Note: The requested MP extension must therefore cover the present MP at runtime. It is non-critical, if the requested MP covers more areas, e.g. because some are already released.*	*If not, MPRequestRejectCode: CHANGE_IN_EXTENSION applies*
Recalculate MP for extension	The requested Movement Permission in an MP Extend Request does not differ in any attribute from the current Movement Permission with the same Id within the MP Extent of the current MP.	If the MP Extend Request fulfils all general and specific Safety Checks, then • The existing MP Extent will be replaced by the newly requested MP Extent. • an MP Update Event is sent *If not, MPRequestRejectCode: RECALCULATE_IN_EXTENTION applies*
Output function		
MpUpdateEvent	An MP Extend Request fulfiling all general and route-related checks will be extended and will be granted.	

6.8.3 Upgrading an MP

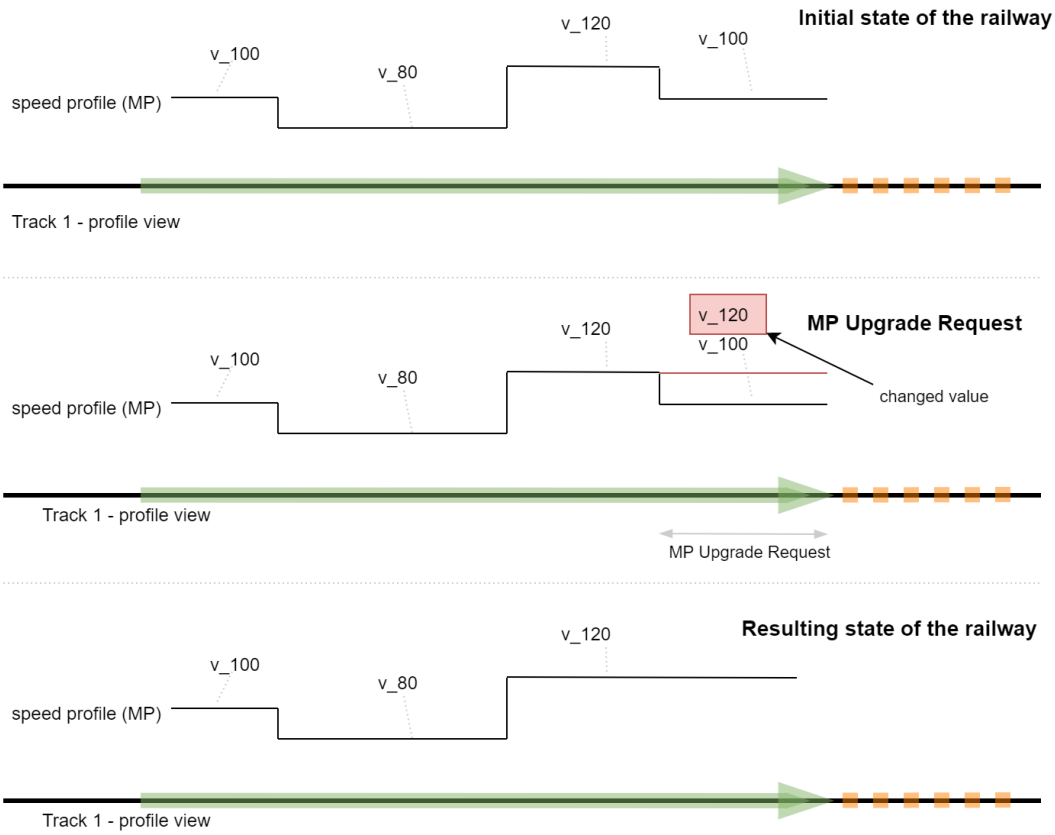
In case of changing track or operational conditions, an already granted MP can be upgraded to avoid unnecessary restrictions for the corresponding PTU.

In the following scenario an upgrade of the speed profile of an existing MP is requested. The MP Upgrade must meet the following (pre-)conditions::

- An MP with the received identifier (MP Id) must exist.

- No downgrade of velocity: At each position on the MP extent of the current MP to upgrade, the maximum velocity according to the speed profile must be less than or equal to the maximum velocity according to speed profile of the received MP Upgrade.

The scenario for upgrading an MP is illustrated below.



Given that all Safety Checks for the received MP Upgrade Request are met, APS will generate the resulting MP by performing the upgrade as follows:

- The MP Id, the extent and the track condition attributes of the resulting MP are given by the corresponding values of the MP to upgrade.
- The Risk Buffer, the Risk Paths, the speed profile and safety responsibility profile are given by the corresponding values of the received MP Upgrade.

If one or more of the Safety Checks are violated, MPRequestRejectCode: UPGRADE_CONFLICT applies

Note: The main functions for this scenario are not defined yet.

6.8.4 Shortening at front end

In addition to the scenario *Shortening at rear end*, an operational need of change ahead of the current movement can occur. Two kinds of changes are possible. A shortening at front end, taken into account in this chapter, or a full removal.

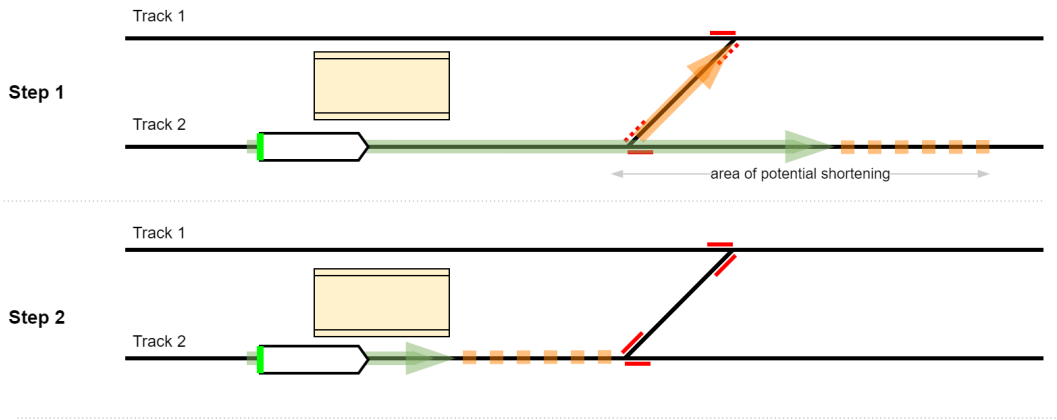
The same preconditions like in *Shortening at rear end* apply. A PTU is at standstill or moving along an already granted Movement Permission.

Moving in this manner of the scenario means that the PTU is actually moving or at a certain time stopping, e.g. at a station. An operational request for shortening the Movement Permission can be issued and granted if some main conditions are fulfilled:

- The area of potential shortening (MP Extent and Risk Bu ffer) is not already occupied by the rMOB.
- The new MP Extent is sufficient for the PTU to be able to stop (using the service brake, no emergency braking) without violating the Risk Buffer, if it already moves.
- The change must be possible with a modification of the issued MA, by means of the so-called Cooperative Shortening procedure based on the ETCS standard.

To be investigated	In emergency situations the shortening at front end may be done without fulfilling these conditions. However, as this concept only covers normal operation, this scenario is to be investigated later on.

The following figure illustrates the topological view with two simplified steps (start and end condition) of the scenario:



Based on the need of PE a request for shortening at front end is received. This can be given by:

- a new MP including e.g. Risk Buffer as the target Movement Permission (as shown in the example), or
- a simple Removal Request of the Risk Buffer, with unchanged MP Extent

The new end of the MP Extent is placed in the example at the end of the platform with a Risk Buffer towards the next DPS. As a handshake procedure the shortening is managed between trackside and on-board. If the on-board Train Control System can assure the stopping at the shortened position, the Movement Permission will be updated. This implies also a change of the Movement Authority (trackside and on-board).

Step 2 shows the result, that the MP Extent is shortened at front end, the Risk Buffer is relocated and the formerly used DPSs are released by indication of the release of the Risk Path and of the locking of the DPSs in a defined position.

Two results are generally possible:

- The MP shortening at front end is performed (as shown in the figure above) or

- The shortening at front end was not performed, due to any violation of a Safety Check,

The specific functions are not fully detailed yet. In conclusion no listing of main functions is given within this section.

The release of parts of the Movement Permission as shortening at front end enables the following:

- Release of secured parts, which are not necessary anymore from an operational point of view
- Changes of operational movements, e.g. by using a different running path. In the above illustrated scenario, an alternative running path over track 1 becomes possible.

6.8.5 MP restricted by URA

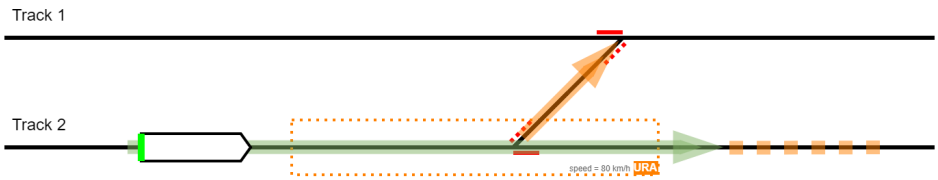
Additional operational restrictions can be implemented by Usage Restriction Areas (URAs). Activated URAs are generally possible in a requested Movement Permission.

The following scenario covers the presence of one or more activated URAs and a request of a Movement Permission covering parts or the full extent of the URA.

It must be considered for this scenario, that a lot of different URA types with specific functional impacts exist. Further information can be taken from the description of a URA in /RCA.Doc.61/. Generally speaking, an activated URA demands further restrictions, additional to present static restrictions, or demands a specific kind of an operation.

As a first example for this scenario a URA from a type "Temporary Speed Restriction" is taken into account.

To be investigated	The scenario shall only show the impact of an activated URA and not the sequence and functional scope of activation and deactivation on a present Movement Permissions. The scenario, that a URA is placed over an existing MP will be considered in a later version of this document.



In conclusion further Safety Checks for enabling MP granting are needed, in case of one or several present URAs. The general safety function as a high level description is formulated by:

The MP Extent including the Risk Buffer is not in conflict with activated URAs.

The MP granting covers the Safety Checks for basic scenarios. Here, the *speed profile check* must consider this specific limitation in case of an activated URA with a Temporary Speed Restriction. In case this restriction is considered correctly in the requested speed profile (by PE) and the Safety Checks are performed successfully, the MP could be granted. If not, the request will be rejected. In case several URAs are present within the extent of the required Movement

Permission, for each URA the Safety Checks must be passed successfully for enabling a granting.

In the given example above a speed restriction of 80 km/h is given by the specific URA. In case the requested Movement Permission covers the maximum allowed speed by this URA, the MP will be granted. If not, a certain MPRequestRejectCode "*URA_SPEED_VIOLATION*" will be transferred.

For the mentioned different kinds or URAs and a presence of many URAs in parallel, further functions and Safety Checks are needed. These are not yet documented.

6.8.6 MP in relation with WA

For enabling Track Worker Safety the integration of Warning Systems for track workers is useful. This requires the interconnection between these systems and the potential granting of a Movement Permission, due to the fact that a warning must be issued in a timely manner. In addition movements should only be possible, if the warning was issued successfully.

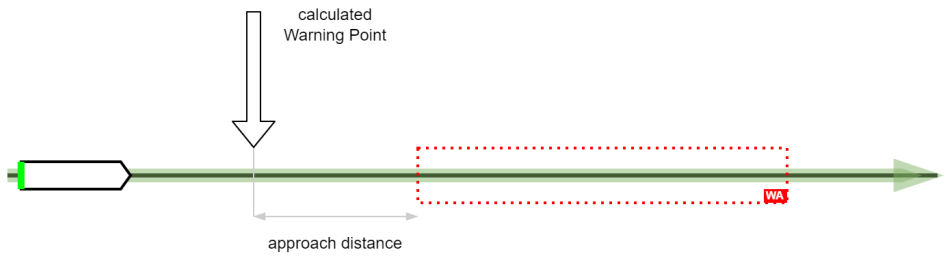
The scenario demands a presence of one or more activated Warning Areas (WAs) and a request of a Movement Permission covering parts or the full extent of the WA.

In general the functional scope can follow several principles:

- Simple start of warning (optical and/or audio) on several devices like headphones, lights/ sound-horn, portable HMIs - including notice of receipt back to APS
- Start of warning (optical and/or audio) including suppression of movements up to a confirmed acknowledgement by track workers

These principles can enable different use cases, depending on the operational and organisational situation present for the specific activities on or near the track.

The main principle is shown as an example in the following figure.



In the depicted example, an rMOB is approaching a track section with an activated Warning Area (see /RCA.Doc.61/). A warning must be issued at latest at a calculated warning point. This point is defined by several inputs for calculation of the approach distance.

In case such a movement shall be enabled, APS must consider all present activated Warning Areas within the extent of the Movement Permission. For each a specific Warning Point must be derived. In case the front of the rMOB reaches this Warning Point, an immediate warning must be issued to the warning device. The knowledge of this Warning Point must also consider, that the information of the front of the PTU is received only periodically. This leads to the fact,

that the Warning Point must be allocated primarily according to safety requirements, operational benefits are of minor importance.

Functions for this scenarios must cover:

- Evaluation of need of warning
- Calculation of the Warning Point, where the warning must be issued safely
- Optional functions covering the acknowledgement by the Track Workers

If all conditions are fulfilled, the movement can be enabled by using a granted Movement Permission and the Track Workers are warned for enabling the leaving of the construction area safely and in-time.

The distance must be of a sufficient magnitude, considering:

- The time for issuing the warning,
- Receiving a confirmation of the issuing to APS,
- The working time e.g. for clearing the tracks,
- The time for approaching the border of the warning area by the rMOB at maximum speed (line speed or specific speed),
- Additional margins for data transmission,
- Impact based on information cycles for updating the front position of the rMOB,
- The specific minimal braking distance for ensuring a safe stopping in case the warning cannot be issued,
- Additional safety buffers.

Notes:

A detailed functional definition must be performed at a later stage and the given minimal needs above must be transferred to a further document covering the handling of Warning Areas explicitly (e.g. determination of the Warning point, time management).

To avoid unnecessary clearance of warning area by track workers, and thus increasing capacity, PE has the possibility to request an MP ending well before the beginning of the Warning Area. This optimised management of an MP will be covered in detail in further PE documentation.

6.8.7 MP at border/transition

A specific scenario is the handover of a movement from one Area of Control (AoC) to another. This leads to the need of having a Movement Permission starting at a certain border or reaching this border depending on the situation:

- Handing over the movement to an AoC - this APS is called Handover APS (HOV APS).
- Accepting the movement from an AoC - this APS is called Accepting APS (ACC APS).

Note: An APS internal handover between different instances is not in scope of this scenario.

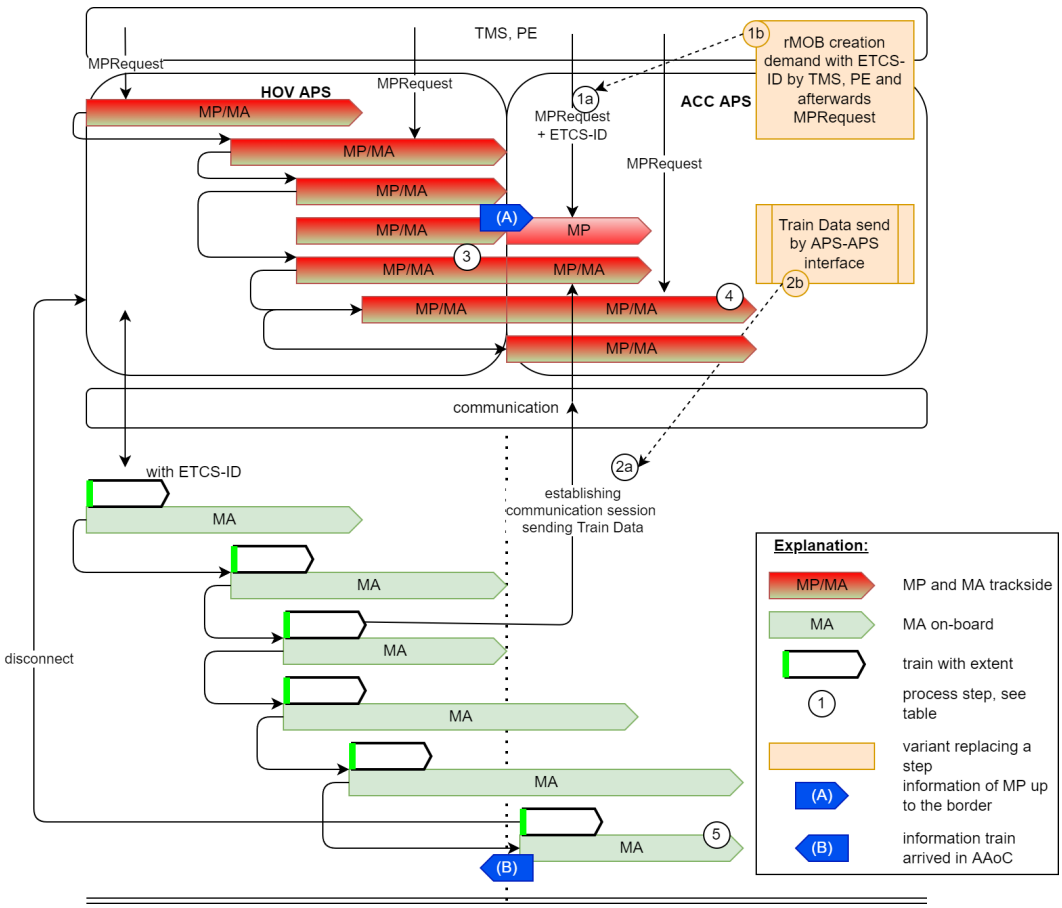
This situation can occur for several combinations of interfaced systems. Here, the focus lies on the interface between two APSs and their respective AoCs; legacy systems are not in the scope of this chapter. A detailed view on transitions will be made in document RCA.Doc.64.

The term Area of Control (AoC) is used, indicating the viewpoint on this area. The adjacent area is named as Adjacent Area of Control (AAoC).

Preconditions are:

- Border situation at AoC is given.
- Operational need of passage of a train movement over this border.

The main process is drawn as following:



The figure shows in the upper part the principle of stepwise granting of the MP considering the operational needs. Derived from the MP as MA on trackside is made leading to a specific Movement Authority on-board on the lower part.

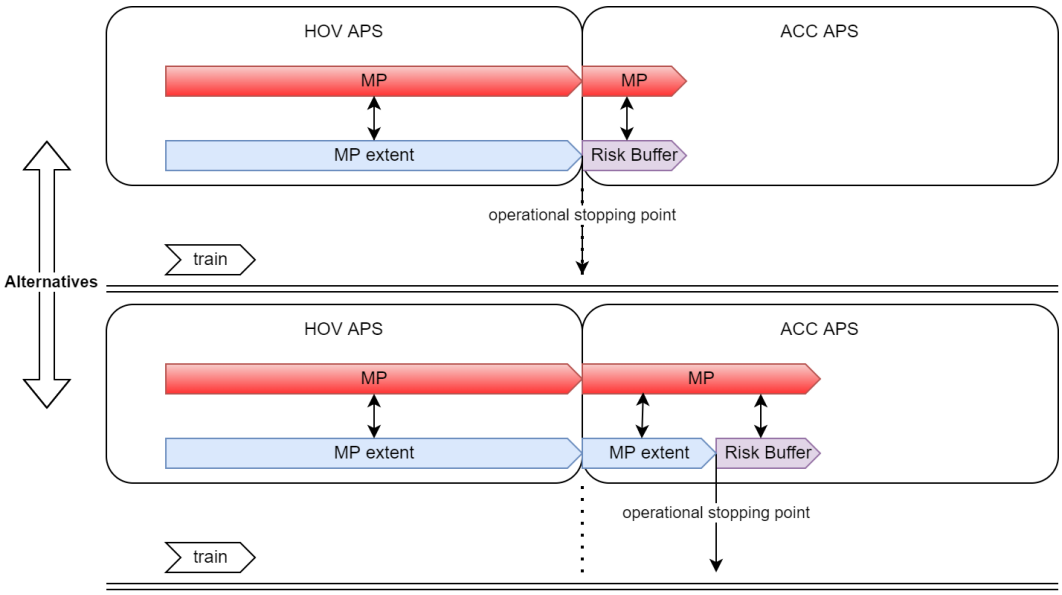
The stepwise procedure shall show the need of having a MP up to the border and a second one starting at the border. Steps (1) and (2) show the required precondition for registration of the train in the adjacent AoC. From MP perspective, step (3) shows the enabling of the handover. Based on the presence of a MP and a trackside MA transferred to the Handover APS, a summary of a MA for the train crossing the border can be issued. This leads to the MA on-board for enabling crossing border. For this step (3) the preconditions are an MP in

Handover APS up to the border, with a certain information on that towards the Accepting APS and the presence of an MP in the Accepting APS.

Step (4) shows a potential extension of the MP. After border crossing, an information will be transferred towards the Handover APS, that the rMOB is successfully arrived on Adjacent AoC and responsibility is shifted towards the Accepting APS. This trigger leads to the possibility of releasing the already used last parts of the Movement Permission in AoC as removal. This step is shown as (5) in the figure.

For the operational handling, alternatives on specific use cases referring to the operational stopping point could occur. Two alternatives are named and illustrated below:

- If the (last) operational stopping point is close, but in front of the border, it is sufficient to have only the Risk Buffer extent in the Accepting APS.
- In every case where the operational stopping point is located after the border, the MP in the Accepting APS must consist of an MP extent and a Risk Buffer.



Functions handling the topic of a Movement Permission for enabling this specific scenario are e.g.:

- General functions for granting an MP Request, including enabling Movement Permissions up to the border.
- Translation from Movement Permission into an MA, including merging of MAs of two AoCs (see also next chapter).
- Transmitting of *train arrived event*, for enabling the removal of a Movement Permission and the rMOB in the Handover APS.

6.9 Relation between MP and MA/signalling

As already introduced, the clear split of securing the running path and signalling is no more used in APS compared to legacy applications. But a kind of transformation of the information given by the Movement Permission towards another Layer is needed. The aim is to enable on-

board signalling with radio-based ETCS using an on-board MA, calculated by the on-board unit, based on a trackside ETCS MA.

Note: For special use cases, a signalling by switchable light and static lineside signal aspects on APS borders shall be assisted as well.

For a better understanding of the belonging and as a prestep for issuing a detailed concept on handling Movement Authorities in APS, the relation between the following objects shall be briefly explained:

- Movement Permission - granted trackside by APS
- Movement Authority trackside - translated Movement Permission into a Movement Authority for issuing towards the PTU
- Movement Authority on-board - calculated on-board based on the received Movement Authority from trackside

In order to clearly show how an MP is transformed into an on-board MA, there is a split between MA trackside (today's RBC) and MA on-board. Today's RBC functionalities will be included in APS, which means that the MP has to be translated into an MA trackside in APS.

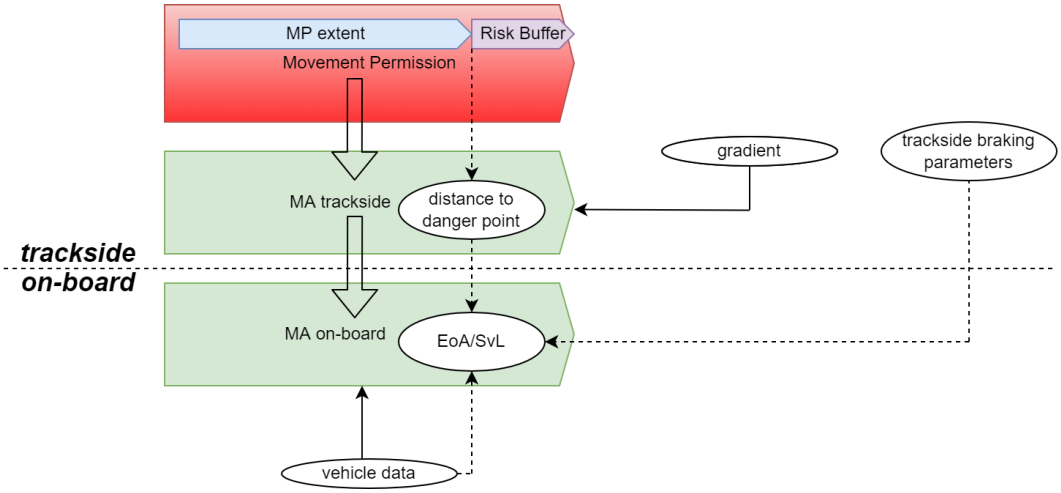
Note: The handling of Movement Authorities (ETCS) in APS will be detailed at a later stage in a separate concept.

The general principle is that the MA trackside will be built in APS based on the MP and additional information like topology data. Hence, the MA trackside consists of already enriched information compared to the MP.

The following table shows a linking of the relevant information:

Movement Permission	MA trackside	MA on-board
MP extent Risk Buffer	MA (ETCS packet 15) with/without distance to danger point	Transferred to information considering End of Authority (EoA) and Supervised Location (SvL) or Limit of Authority (LoA) in ETCS, under consideration of further sources; in best case EoA == border of MP extent and Risk Buffer of the MP
Speed Profile URA with speed as source	SSP (ETCS packet 27) Additionally optional speed restrictions (ETCS packet 51, 52, 65 and 66)	Most restrictive speed profile (MRSP)
-	Gradient (ETCS packet 21)	Gradient
Restricted Permitted Movement Mode symbolised by Safety Responsibility Profile	Optional information mode profile (ETCS packet 80)	Considered in MRSP
-	Optional information, e.g. linking, track conditions (ETCS packets 3, 5, 39, 40, 41, 68, 69, 70, 71 and 88)	Considered according to system functions

This means, the general relation can be outlined by a visualisation of main interactions:



Summing up, the Movement Permission sets the framework for securing the movement. The Movement Authority is defined trackside with additional data compared to the granted MP. Trackside braking parameters must be considered fixed by documentation and/or transmitted to the on-board. This leads to the specific Movement Authority on-board, under consideration of further information like vehicle data. This stepwise increase of restrictions for the movement leads to the strict need, that any (sub-)system considers the limitations. Example: The MP Request of PE must consider the mechanism for enabling a reachable final stopping point of the movement, symbolised by the End of Authority in ETCS.

The present MA on-board will provide the outer safe range of the movement, used by the driver. Thereby assisting systems are to be considered, like a Connected Driver Advisory System (C-DAS), or highly or fully automated operation enabled by Automatic Train Operation (ATO) systems.

Note: The general approach is that every movement will have its own Operational Plan. The movement is secured by exactly one Movement Permission in the AoC. There are no Movement Permission sequences similar to sequences of routes in classical interlockings. Each MP is transformed into an MA. Thus in general there is a 1:1 relation between MP and MA. This is valid for the running path and the Risk Buffer. Additional mitigation measures like the Risk Path are not part of the MA. Only in some degraded situations this 1:1 relation between MP and MA might not be present.

6.10 Movement Permission data objects

Concerning data objects for handling the Movement Permission, there are two categories that can be derived:

- Focus on input/output (request for MP and translation into MA)
- APS internal handling

The focus in this concept shall be given by the input and output for the MP Request only. Referring to the architecture, the interface SCI-CMD is the major exchange platform between the operational level and the safety domain of APS. The different information on

- Downstream (from PE to APS),
- Upstream (from APS to PE),
- Parameters and
- Data types

can be found in /RCA.Doc.70/.

For enabling a tracing within this concept, a reference between the scenarios and functions identified above and the data exchange on SCI-CMD concerning the Movement Permission are shown in the following table. The table is a summary of the basic and specific scenarios introduced before.

Note: Grey cells indicate that no message is associated with that functionality down- or upstream. "Not in scope" in column "Exchange object in SCI-CMD" is given, if the concept is not detailed enough or not mentioned here, so that associated messages cannot be derived.

Lifecycle phase	Functionality (basic and specific scenario)	Exchange object in SCI-CMD	Message on SCI-CMD		Remarks
			Downstream	Upstream	
Creation	Request	Yes	MPRequest		
	Granting	Yes		MPCreateEvent	
	handling of additional checks, e.g. route suitability	Not in scope			

Lifecycle phase	Functionality (basic and specific scenario)	Exchange object in SCI-CMD	Message on SCI-CMD		Remarks
			Downstream	Upstream	
	Flank Protection provided different to DPS state	Not in scope			
	Activation of Level Crossing	Not in scope			
	Handling of Usage Restriction Areas	Yes	MPRequest	MPCreateEvent	The request/set-up of a URA is not in scope of this view. The mentioning of URAs in this concept is limited to Temporary Speed Restriction as part of the speed profile. Further kinds of URAs will have different interdependencies to a Movement Permission.
	Handling of Warning Areas	Yes	MPRequest	MPCreateEvent	The request/set-up of a WA is not in scope of this view
	Handling of Handover situation	Yes	MPRequest	MPCreateEvent	
Modification	Extension	Yes	MPExtendRequest	MPUpdatedEvent	
	Upgrade	Not in scope			MPRequestRejectCode considered in functionality Rejecting respectivly MPRequestRejectEvent
	Downgrade	Not in scope			
	Shortening at front end	Not in scope			
	Shortening at rear end	Not in scope			Scenario is currently restricted on automatic shortening, a manual request must be introduced later
Removal	Rejecting	Yes		MPRequestRejectEvent	
	Removal	Yes		MPRemovalEvent	Request of Removal not in scope yet

7 Conclusion

With RCA the concept of a Movement Permission will be introduced. As it incorporates both the securing of the movement and the issueing of the permission to move, it differs fundamentally from today's approach.

Movement Permissions will usually be requested by the interfaced Subsystem Plan Execution. APS will perform generic safety checks and then grant or reject the request. These checks are restricted to excluding hazards, they do not deal with optimising operation.

As a Movement Permission is always linked to a resolved Movable Object, both concepts are closely related.

Several operational and planning benefits are achieved with the Movement Permission concept, for instance that movements can begin and end at any location, and that the securing of a route can be based on real evaluated risks (train centric instead of block/track centric), which increases the available capacity.

Open points, which remain to be investigated for later versions of this concept, especially refer to the corresponding processes in degraded situations.