RCA

Reference CCS Architecture

An initiative of the ERTMS users group and the EULYNX consortium

APS Concept: Route setting and route protection

Document ID: RCA.Doc.62
EUG and EULYNX partners

Table of contents

1 Preamble

1.1 Release Information

Basic document information:

RCA-Document Number: RCA.Doc.62

Document Name: APS Concept: Route setting and route protection

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	Maria Bertram, Peter Evans, Bettina Morman, Philipp Nicolaus, Christian Sadowski, Philipp Schneider, Frank Skowron	First published version for RCA BL1 R0

3 Introduction

3.1 Type of document

This concept paper is written as part of the RCA's vision for a digitalised and automated railway operation. It is one of the many detailed concept documents under the overarching APS Concept umbrella (refer to /RCA.Doc.51/) - a key part of the overall desired system architecture.

This paper contains the basic information for further definition by the System Pillar and it is aimed at infrastructure managers, railway undertakings, suppliers, authorities and other railway stakeholders, especially in Europe's Rail Joint Undertaking. The document shall be treated as a concept and as an input to enable future discussions and conceptualisation, aiming to achieve a detailed system design and specification work.

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

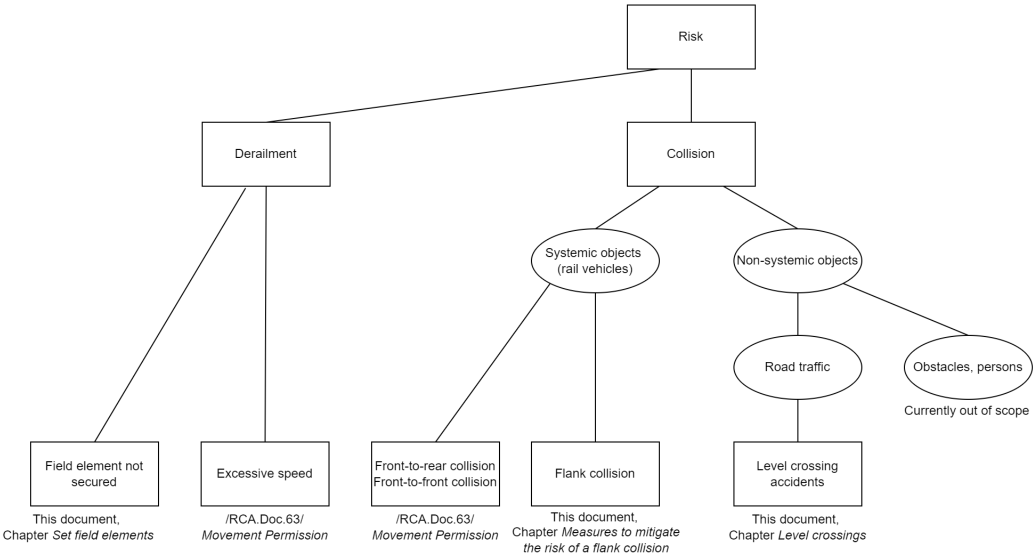
3.2 Scope

Enabling a train running from A to B requires two steps in RCA from the trackside perspective

1. Set all elements of the route from A to B to the required state /RCA.Doc.62/
2. Authorise a Movement Permission from A to B /RCA.Doc.63/

This concept focuses on the first step and only with the perspective of the safety logic. The objective of RCA of separating the safety logic from the operational planning also applies here.
The planning system (PE) is responsible to **identify** the needed elements and their required state for the specific route and to **request** those element states in time.
The safety logic (APS) is responsible to do defined **checks** for the requested elements and to **grant the request** to the appropriate element in the field or to **reject the request** if needed conditions are not fulfilled.

The defined checks in APS serve to avoid any collision and derailment: collision of rail and road users with respect to level crossings and derailment with respect to switchable field elements like points and derailers.


Risk
Derailment
Collision
Systemic objects (rail vehicles)
Non-systemic objects
Road traffic
Obstacles, persons
Currently out of scope
Field element not secured
Excessive speed
Front-to-rear collision
Front-to-front collision
Flank collision
Level crossing accidents
This document, Chapter *Set field elements*
/RCA.Doc.63/ *Movement Permission*
/RCA.Doc.63/ *Movement Permission*
This document, Chapter *Measures to mitigate the risk of a flank collision*
This document, Chapter *Level crossings*

The descriptions of the solutions to these risks are contained in the APS detailed concepts as indicated in the figure. Though flank collision risks have to be checked during the execution of the Movement Permission safety checks, they are described in this document to manage the complexity of documents.

3.3 References

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

3.4 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*.

3.5 Dependencies

Parts of the document are based on an MBSE model in Capella (are generated with information from the model):

Artifact	Version
Model name	rca-concepts
Model branch/revision	master/refs/heads/master
MBSE tool version	5.2.0

4 Set switchable Field Elements

Delimitation	This part is currently restricted to the switchable Field Elements simple points (no slip points) and derailers. Also, further investigation is needed into topics like • Further conditions preventing to set a switchable Field Element like usage restrictions; • Support of manually locked points (clipped and scotched); • Local operation of points (including local operation areas, and the handover of central/local responsibility); • Sprung points; • Maintenance scenarios.

The term *route* is used also here in a general way and not to be mistaken with fixed interlocking routes. It is just a path through the railway topology from a Track Edge Point A to a Track Edge Point B and includes also the Risk Paths (flank protection area) and Risk Buffer (overlap).

4.1 Problem description

4.1.1 High level functionality

On operational layer, there is a need to set a single or a number of switchable Field Elements to prepare the safe provision of a route for a Physical Train Unit. The element setting can be done in different situations (for normal operation or for maintenance reason) and manually or automated.

Switchable Field Elements need to be set to the appropriate position/state. Relevant switchable Field Elements are all controllable infrastructure elements which involve a discontinuity of the track, either because of an interruption within the rail or because of an obstacle within the structure gauge. These elements are most commonly points and derailers, but movable bridges, movable buffer stops, movable gates, turntables, etc. must also be taken into account.

It is the task of the current interlocking and future safety logic to

- Grant or reject changing the position of a switchable Field Element (if it is occupied by a Physical Train Unit or if it is part of an actual or reserved route for a movement, or if other usage restrictions prevent this);
- If granted, set the element to the requested position.

4.1.2 Current solution

The setting of switchable Field Elements is triggered either for an individual element (e.g. for maintenance reason or in degraded situations) or, in most cases, as part of a route. Setting a route can be triggered either manually or via automatic route setting. From a technical point of view, the setting process is initiated with a command from the operating level, which is checked, processed and transmitted in the safety control layer of the interlocking; the safety control level usually has to meet SIL 4 standards. From there, the Point Machine is triggered, which then moves the point blades.

The operating state of a switchable Field Element is reported using not yet fully standardised interfaces from the Point Machine through new standardised interfaces of Object Controllers via the safety control layer of the interlocking to an operating system.

Some switchable Field Elements may be set via two alternative ways (either from a centralised interlocking or from a local, decentralised control panel). Such switchable Field Elements are in scope of APS, whereas exclusively locally operated switchable Field Elements are not.

As long as a switchable Field Element is in its normal state, it can be moved. There are several circumstances which may prevent switching it: an occupancy, the utilisation by another route (including its and), a manual blocking (e.g. for maintenance), a sequential locking to another element, or a failure. A failure state may have several causes, e.g. a point may not be available or supervised, its blades may not reach their final position (for one or both blades) or it might be trailed. If a failure is revealed, in most cases the switchable Field Element can no longer be used regularly as a route element; if it is already part of a set route when the failure is revealed, the respective signal immediately indicates a stop aspect, because the conditions for the route are no longer given.

Delimitation	There are optimisation functions realised in the interlocking like sequential setting to avoid peak power demands. With a strict separation of safety logic and optimisation, this function is not realised by APS but by PE and therefore not in scope of this concept.

4.1.3 Problems with current solution

- Depending on the number of elements, the setting of a route takes a significant time span. Today's safety logic demands setting of Field Elements which is not needed in every situation. A new flank protection concept (compare the respective chapter) will simplify this, and PE will only request flank protection where and when really needed.
- Different types of Field Elements require different handling: The interlocking must be aware of the concrete nature, properties, and behaviour of each Field Element - this increases complexity and reduces stability of the safety logic (when adaptations of Field Elements have to be made). This problem is not just restricted to setting the Field Element, but also to considering its state, e.g. when a MP is requested. The solution to this by DPS abstraction is described in /RCA.Doc.61/.
- The today missing abstraction of switchable Field Elements not only complicates the safety logic but also means more engineering and validation effort
- Setting of switchable Field Elements is prevented if they are occupied: If the corresponding Track Vacancy Proving Section (TVPS), due to cost reasons, is longer and not just covering the 'field' is undefineds, the release of the TVPS takes longer than strictly necessary. The occupancy might not even be on the switchable Field Element but on another part of the TVPS. APS will earlier release the occupancy by on-board localisation which will allow earlier element setting in turn. However, this concept does not contribute to the solution of this problem and will be handled by improved localisation /RCA.Doc.68/ and timely release of the Movement Permission /RCA.Doc.63/.

4.2 Solution summary

With APS, an abstraction of every concrete Field Elements type is made to the common characteristcs so that the different types are transparent to the safety logic which ensures a great stability within the core functionality of APS and a robust lifecycle. Further details to that vital solution of abstraction can be found in /RCA.Doc.61/.

According to the general structure of A.P.M - especially the separation of business and safety logic - the role of APS in the process of switching Field Elements is limited to three basic tasks:

1. It authorises or rejects requests from PE. This decision is made based on general (e.g. correct syntax) and usage related safety checks. The latter refers to the exclusion of conflicts with other movements, e.g. the check for occupancy or usage in a different Movement Permission.
2. If all safety conditions are met, a state change is commanded, requesting an *Object Controller* to change the state of a real-world switchable Field Element. However, within APS switchable Field Elements are solely represented by abstract elements called *Drive Protection Section*s.
3. State changes of switchable Field Elements are observed and asynchronously reported to APS where the state is represented in the *operating state* and in turn reported to PE, in order to provide a topical view on the state of the railway.

Within APS the process of setting switchable Field Elements is decoupled from the process of authorising a request for a movement.

4.3 Solution details

4.3.1 Prerequisits

APS must know all switchable Field Elements in the Area of Control which cause a discontinuity of the track. This information is provided by MAP data. As APS is using the *Drive Protection Section* abstraction, some subsystems in APS abstract from the actual nature of a switchable Field Element (subsystems *Safety Logic* and *Object Aggregation*), and some subsystems need it to communicate with (the *Object Controller* of) the specific switchable Field Element. This means, that topology data provide the needed information on switchable Field Elements, including the mapping from Drive Protection Section information to/from specific switchable Field Element information.
Topology data are detailed in /RCA.Doc.46/, including the topology update process. The abstraction concept of *Drive Protection Sections* is explained in /RCA.Doc.61/*,* together with the dynamic states of switchable Field Elements.

The communication with the Object Controller of the specific switchable Field Element is realised via interfaces specified by EULYNX. These EULYNX specifications are considered as an input for this concept. For more details about those interfaces, please refer to /EULYNX_SCI-P/ and /EULYNX_Req/.

APS must also know whether a switchable Field Element in its Area of Control is either occupied or presumably occupied by a Movable Object, or is part of the reserved track for a Movable Object (*Movement Permission*). How to detect Movable Objects at the location of the element to be set is explained in /RCA.Doc.61/. The concept of a Movement Permission is explained in /RCA.Doc.63/.

The candidate architecture for RCA (including subsystems and their interfaces) can be obtained from /RCA.Doc.40/.

4.3.2 General view: separate requests for setting switchable Field Elements and for Movement Permission

Generally, there are two phases covered by the main PE requests

- *DpsGroupRequest* - Set a (number of) switchable Field Element(s) needed for a route to a requested position

  This phase corresponds to setting and protecting a route and is subject of this concept

-
  - APS performs a number of safety checks if the request can be permitted (see further detail scenarios);
  - If permitted, the needed state changes are commanded to the *Object Controllers ;*
    - Otherwise, the request is rejected; the reason returned, and the scenario terminates;
  - The *Object Controllers* command the switchable Field Elements to switch to the requested position;
  - The *Object Controllers* report state changes (both temporary states like leaving of end positions for points and in case of success reached end positions);
  - APS subsystems continuously observe the *Object Controllers* for state changes and report these to PE.
- *MpRequest* - Request a (new or extended) *Movement Permission* using this route

  This phase is not subject of this concept and will be described in /RCA.Doc.63/. A precondition is that all switchable Field Elements are in the position needed for the *Movement Permission* which is the task of the first phase and APS checks if the precondition is fulfilled. If not, the *MpRequest* will fail.

In the following exemplary diagram, one among many possible specific orders of requests and results is shown.

PE requests the state change of point A and as APS grants and checks that request, PE now already requests the state change of point B.

The state change request for point B is authorised and granted as well and the state changes for point A and point B are commanded to the Point Machine.

In the given exemplary diagram, point B completes the request in advance of point A. Thus, the state change of point B is observed earlier than the state change of point A.

In consequence, PE can request a Movement Permission, which requires point A and point B in their now given state. The related process is to be found at /RCA.Doc.63/.

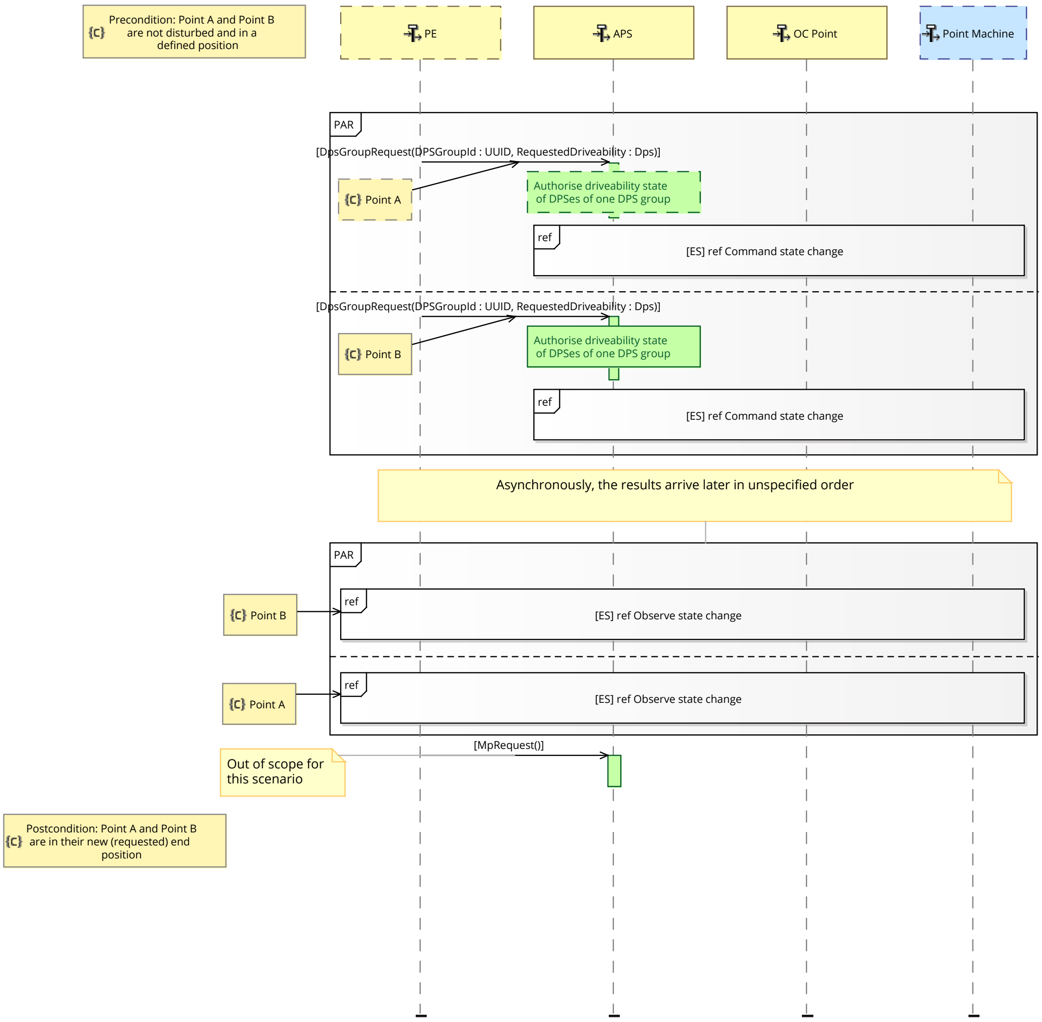

{C} Precondition: Point A and Point B are not disturbed and in a defined position
PE
APS
OC Point
Point Machine
PAR
[DpsGroupRequest(DPSGroupId : UUID, RequestedDriveability : Dps)]
{C} Point A
Authorise driveability state of DPSes of one DPS group
ref
[ES] ref Command state change
[DpsGroupRequest(DPSGroupId : UUID, RequestedDriveability : Dps)]
{C} Point B
Authorise driveability state of DPSes of one DPS group
ref
[ES] ref Command state change
Asynchronously, the results arrive later in unspecified order
PAR
{C} Point B
ref
[ES] ref Observe state change
{C} Point A
ref
[ES] ref Observe state change
[MpRequest()]
Out of scope for this scenario
{C} Postcondition: Point A and Point B are in their new (requested) end position

Figure 1: [ES] Overview

This provides flexibility to re-use the *DpsGroupRequest* in different scenarios:

- Main scenario: Prepare later *MpRequest* and set required positions of switchable Field Elements for *Running Path*, *Risk Path*, and *Risk Buffer;*
- Set a switchable Field Element independently from a *Movement Permission*, e.g. for maintenance or test reason;
- Other - this list is not exhaustive, and the true scenario APS is involved in is not transparent to APS, nor needs to be. Note that APS consequently will not be aware whether the requested position is needed for *Running Path*, *Risk Path*, or *Risk Buffer*.

4.3.3 Functions

To set a switchable Field Element, a number of general functions is needed. On the one hand, there are functions enabling communication between the different subsystems (e.g. transmit/receive/translate information). On the other hand, there are safety checks with the high-level aim to prevent any hazardous situations caused by a switching Field Element. A hazardous situtation could be a derailment of a Movable Object or a collision, because suddenly no is provided any more.

Out of the mentioned high-level aim, following conditions must be fulfilled when switching a Field Element:

- All movable parts of the switchable Field Element must be clear from any Movable Object;
- No Movement Permission (including Risk Buffer and Risk Path) is set over the switchable Field Element.

Transferring those general functions and conditions to APS, the following specific functions (see table below) apply and will be referred to in the following scenarios. If a function fails (non-succesful check or function cannot be executed), then the reason for rejection is given in the DpsGroupRequestRejectedEvent (see table with messages in the next section). Sequence diagrams with a DpsGroupRequestRejectedEvent can be found in the following chapters.

Function	**Description**
Function Description DpsGroup Request syntax check	The syntactically correctness of the DPSGroupRequest is checked.
Function Description DpsGroup Request existence check	The existence of the requested DPSGroup including all its single DPSs is checked.
DPSGroup clear proving	The extent of no DPS belonging to the same DPSGroup as the requested DPS is occupied (does not overlap any MOB extent).
Conflict check of DPSGroup in MP extent	The extent of no DPS belonging to the same DPSGroup as the requested DPS is overlapping any MpExtent.
Conflict check of DPSGroup in Risk Buffer	The extent of no DPS belonging to the same DPSGroup as the requested DPS is overlapping any Risk Buffer extent. Remark: Depending on national regulations, points used in a Risk Buffer in trailing direction may be switched. This will probably result in a configurability of safety logic (safety check).
Conflict check of DPSGroup and protecting elements in Risk Path	None of the DPSes of the DPSGroup is the protecting element of any RiskPath of any MovementPermission.
DPSGroupRequest granting	A DPSGroupRequest fulfilling all general DPS checks and all usage related DPS checks will be granted.
DPSGroupRequest reject	Reject DPSGroupRequest, if one or more safety checks failed.
translate DPSGroupRequest to PointDemand	Translate the DPSGroupDrivabilityDemand into a specific command for a point. Identify the type of the related Field Element to the demanded DpsGroup Checks if the DPS States of all DPS of the Function Description DpsGroup are not in conflict to each other regarding the switchable Field Element type

Function	Description
Command Point Machine	Performs commanding P3 according to EULYNX.
report Point Machine state	Performs monitoring P3 according to EULYNX
translate PointEvent to DPSGroupUpdate	The Point report via SCI-P is translated into a DPSGroupUpdateEvent. In case of a reported end position, derived from the topology, the Drivability for the DPSes representing point is set to FULL or NONE. The DPSGroupState is set to READY. In case of reported no end position, the drivability of all DPSes representing the point is set to NONE. The DPSGroupState is set to PROCESSING.

4.3.4 Setting switchable Field Elements - main success scenario

The following diagram is given for points but is assumed to be similar for other switchable Field Element types .

When a request is received, in a first place, two general DPS checks are performed, which is to check the compliance of the syntax and if the Function Description DpsGroup is known. Furthermore, usage-related safety checks are performed.

Those include (list not exhaustive)

- Is the DpsGroup clear?
- Is there an overlap of any DPS of the DpsGroup and any Movement Permission Extent?
- Is there an overlap any DPS of the DpsGroup and any Risk Buffer of a Movement Permission?
- Is there a DPS of the DpsGroup, which provides flank protection to any Movement Permission?

If all of those safety checks passed successfully, the DPSGroupRequest is granted and is translated to a point-specific command, sent to the ocPoint.

The ocPoint moves the blades according to /EULYNX_ReqP/ and also monitors and reports the position accordingly.

When ocPoint reports "no end position", APS translates this into a Function Description DpsGroup of state "PROCESSING" and two DPSes, each of state "NONE", which is reported to PE with a DPSGroupUpdateEvent.

When ocPoint finally reports "left end position" or "right end position", APS translates this into a Function Description DpsGroup State "READY" and one DPS State "FULL" and one DPS State "NONE", according to configuration, wich is reported to PE with a DPSGroupUpdateEvent again.

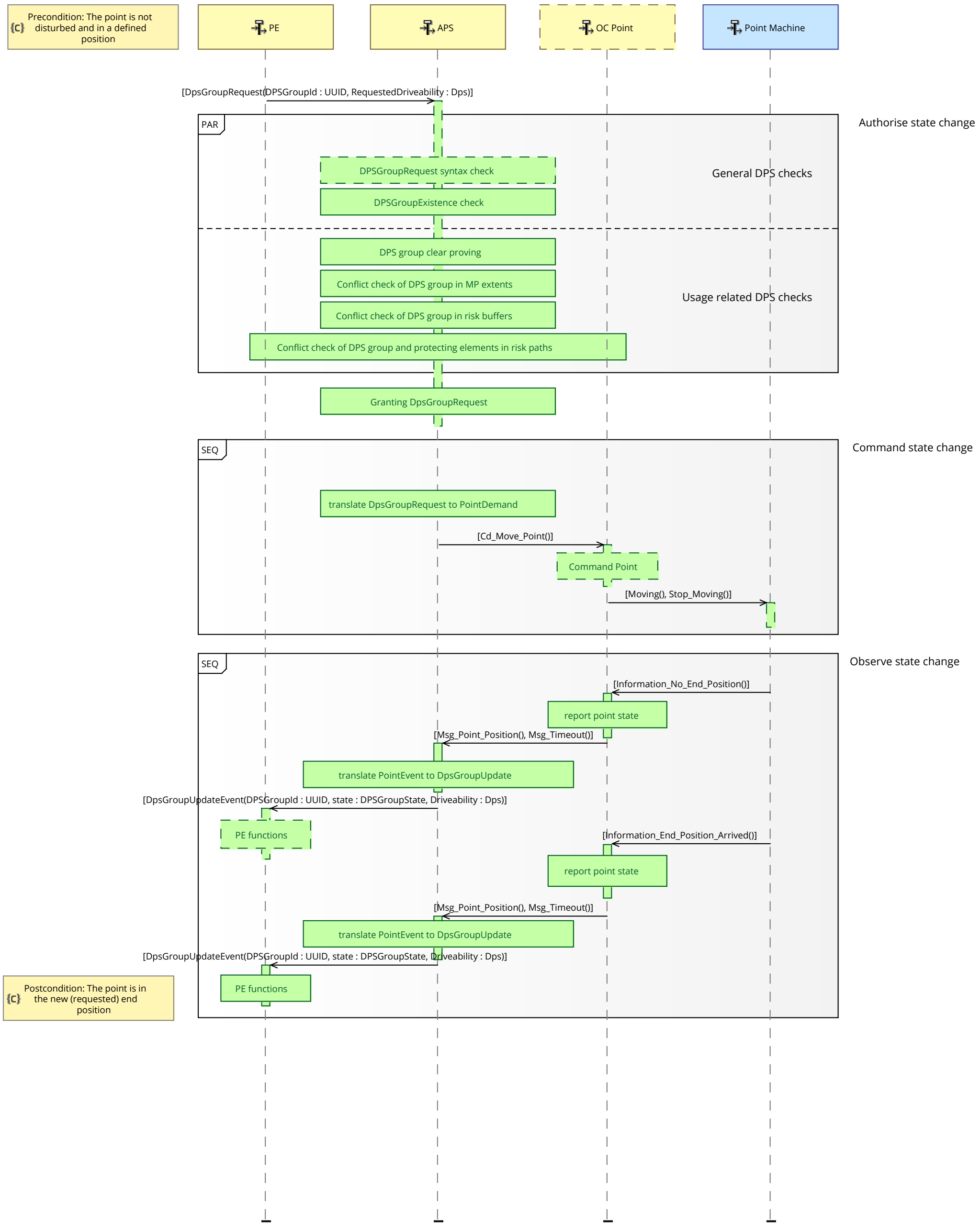

Precondition: The point is not disturbed and in a defined position
PE
APS
OC Point
Point Machine
[DpsGroupRequest(DPSGroupId : UUID, RequestedDriveability : Dps)]
PAR
Authorise state change
DPSGroupRequest syntax check
DPSGroupExistence check
General DPS checks
DPS group clear proving
Conflict check of DPS group in MP extents
Conflict check of DPS group in risk buffers
Usage related DPS checks
Conflict check of DPS group and protecting elements in risk paths
Granting DpsGroupRequest
SEQ
Command state change
translate DpsGroupRequest to PointDemand
[Cd_Move_Point()]
Command Point
[Moving(), Stop_Moving()]
SEQ
Observe state change
[Information_No_End_Position()]
report point state
[Msg_Point_Position(), Msg_Timeout()]
translate PointEvent to DpsGroupUpdate
[DpsGroupUpdateEvent(DPSGroupId : UUID, state : DPSGroupState, Driveability : Dps)]
PE functions
[Information_End_Position_Arrived()]
report point state
[Msg_Point_Position(), Msg_Timeout()]
translate PointEvent to DpsGroupUpdate
[DpsGroupUpdateEvent(DPSGroupId : UUID, state : DPSGroupState, Driveability : Dps)]
Postcondition: The point is in the new (requested) end position
PE functions

Figure 2: [ES] Set field element - base scenario

The messages shown in the figure above are sent via different interfaces. the following table describes the messages sent via the SCI-CMD interface:

Messages		
Interface	**Exchange Item**	**Exchange Item Element : *Type***
SCI-CMD	**DpsGroupRequest** Request the setting of a single switchable field element by its abstraction to a DPS Group. It is needed to supply the states of all Drive Protection Sections within the group with their requested state.	**dpsGroupId : *UUID*** Identification of the DPS Group to change. The concrete new state is requested by the DPS parameter (a DPS within the DPS group) **requestedDriveability : *Dps*** Requested new driveability of this DPS. Note that as many DPSs have to be specified as needed by their interdependency. Example: {NONE, FULL} cannot be set to {FULL, FULL} but {FULL, NONE} which requires two DPSs to be set.

Messages		
Interface	**Exchange Item**	**Exchange Item Element : *Type***
SCI-CMD	**DpsGroupUpdateEvent** Reports the state changes of the Drive Protection Sections in a a DPS Group and the state of the DPS Group itself. It is an asynchronous message which is either related to a previous DPS Group Request or any other event that changed the drivability of a DPS Group (e.g. trailed point).	**dpsSGroupId : *UUID*** Identification of the DPS Group **state : *DpsGroupState*** (New) state of the DPS group • READY This state indicates, that the switchable field element has an end position and is functioning. • PROCESSING Example: point lost its end position because the point is turning due to a DPS Group State request. • DISTURBED Example: A point does not reach its requested end position after timeout **driveability : *Dps*** (New) driveability of this DPS

SCI-CMD	**DpsGroupRequestRejectedEvent** Sent if the authorisation to change the DPS drivability cannot be granted.	**reason :** ***DpsGroupRequestRejectCode*** More specific reason for the rejection • UNKNOWN_DPS The Drive Protection Section is unknown to APS, e.g. checked-out. • UNKNOWN_DPSGROUP The DPS Group is unknown to APS. • DPS_OCCUPIED The Drive Protection Section is occupied and not switchable. • DPS_SECURING_RISKPATH At least one of the Drive Protection Sections in the Drive Protection Section Group is with the protecting element of a Risk Path and not switchable. • DPS_GROUP_DISTURBED The Drive Protection Section Group is disturbed. • DPS_SYNTAX The DPS Group Request is not conform to the syntax definition. • DPS_IN_MP_EXTENT The extent of at least one DPS provided by the Topology, which has the same DPS Group as the requested in the DPS Group Request overlaps any MP extent.

<table>
<tr><th colspan="3">Messages</th></tr>
<tr><th>Interface</th><th>Exchange Item</th><th>Exchange Item Element : *Type*</th></tr>
<tr><td></td><td></td><td>• DPS_IN_RISK_BUFFER
The Drive Protection Section Group is in conflict with a Risk Buffer.
• DPS_NETWORK_FAILURE
Network issues from Point of view of APS-FOT.
• DPS_STATE_CONFLICT
The requested DPS states are in conflict to each other from point of view of APS-FOT (e.g. single point FULL/FULL).
dpsGroupId : *UUID*
Identification of the DPS Group
dpsId : *UUID*
Identification of the DPS</td></tr>
</table>

To be investigated	DpsGroupRequestRejectedEvent: • Is there a need to send a reference to the request (not the DPS/ DpsGroup, it refers to), which was rejected (which could be done by an additional *invoke id* , being sent with each DPSGroupRequest)? • Should the first failed check abort the other checks or all failed checks be reported back?

4.3.5 Reporting the state of switchable Field Elements

PE needs a topical view on the *operating state* of the railway. The information on the state and position of switchable Field Elements is provided asynchronously by APS (*DPSGroupUpdateEvent* message) as the only source of information.

APS (subsystem *Fixed Object Transactor*) retrieves this information from *Object Controllers* which provide (example for a point) *Msg_Point_Position* messages. These are sent in two situations

- after a successfully granted *DPSGroupRequest* by PE (see scenarios above)
- after the detection of a degraded situation (see scenarios in subsequent sections)

4.3.6 Setting switchable Field Elements - alternative scenarios

4.3.6.1 Switchable Field Element already in requested state

If the switchable Field Element is already in the requested state, APS will still do all checks (e.g. check, if network connection to OC Point is established) and - if successfull - command the state 'change' to the Object Controller. However, the Object Controller will ignore the change as the element is already in the requested position. **Consequently, no status report will be sent, when the requested point position equals the current point position.**

Rationale: Simplification of APS. However, this situation should not happen as PE has a topical operating state including the knowledge about the already changed state.

To be investigated	The need of PE for a status update is under discussion.

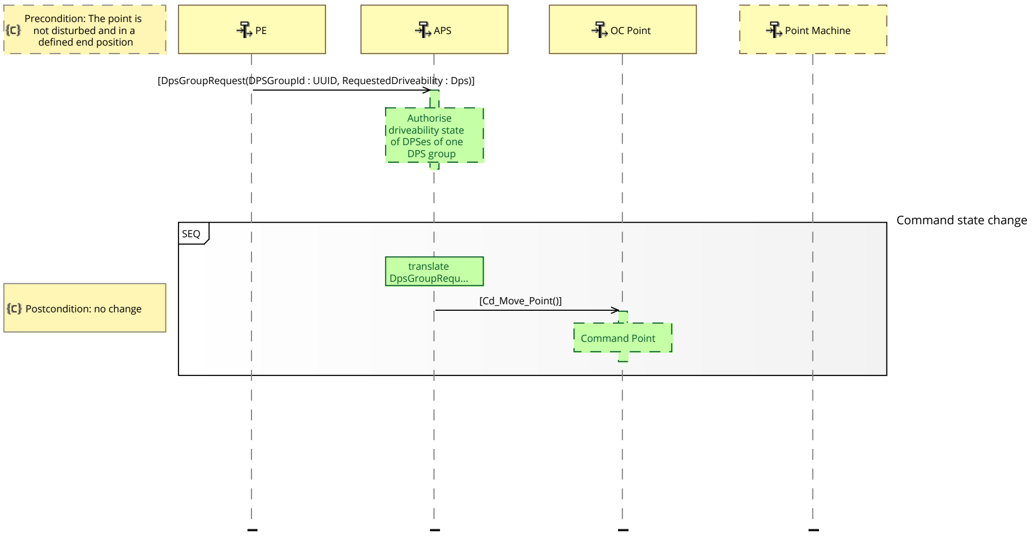
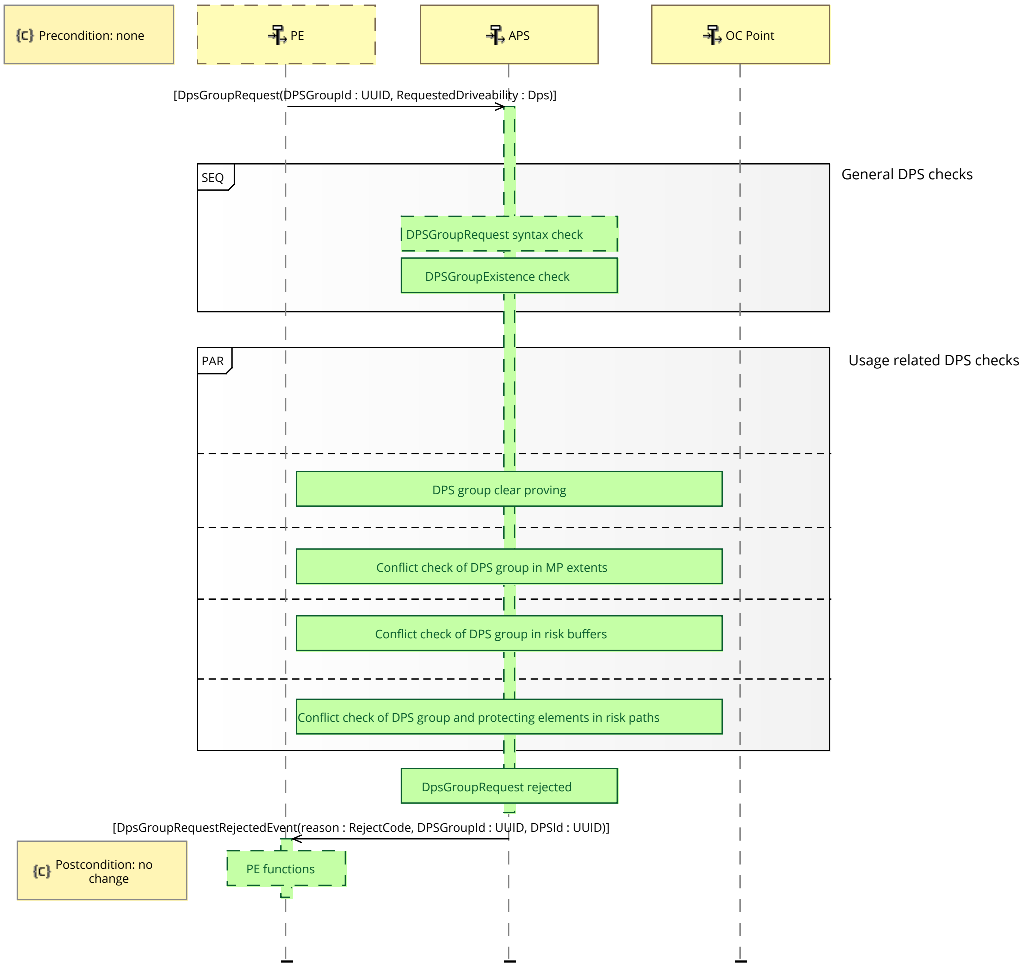

Precondition: The point is not disturbed and in a defined end position
PE
APS
OC Point
Point Machine
[DpsGroupRequest(DPSGroupId : UUID, RequestedDriveability : Dps)]
Authorise driveability state of DPSes of one DPS group
SEQ
Command state change
translate DpsGroupRequ...
[Cd_Move_Point()]
Command Point
Postcondition: no change

Figure 3: [ES] Set field element - already in requested state

4.3.6.2 Request rejected

When a is received, APS performs general DPS checks and usage related safety checks. If any of those checks fails, the DPSGroupRequest won´t be executed. A DPSGroupRequestRejectedEvent will be provided to PE.



{C} Precondition: none
PE
APS
OC Point
[DpsGroupRequest(DPSGroupId : UUID, RequestedDriveability : Dps)]
SEQ
General DPS checks
DPSGroupRequest syntax check
DPSGroupExistence check
PAR
Usage related DPS checks
DPS group clear proving
Conflict check of DPS group in MP extents
Conflict check of DPS group in risk buffers
Conflict check of DPS group and protecting elements in risk paths
DpsGroupRequest rejected
[DpsGroupRequestRejectedEvent(reason : RejectCode, DPSGroupId : UUID, DPSId : UUID)]
{C} Postcondition: no change
PE functions

Figure 4: [ES] Set field element - request rejected

4.3.6.3 Timeout

In some cases, the Point Machine does not succeed moving the blades to the required end position.

If so, after being commanded to move the blades by ocPoint, the Point Machine probably still reports the loss of the end position to ocPoint, what is then reported to APS. APS will translate that into a Function Description DpsGroup with the state "PROCESSING" and two DPSes, each having the state "NONE" and report that with a DPSGroupUpdateEvent to PE.

But then, ocPoint will detect and report a Timeout and thus will be translated into a Function Description DpsGroup with state "DISTURBED", both DPSes will keep the state "NONE" and APS will report that with a DPSGroupUpdateEvent to PE.

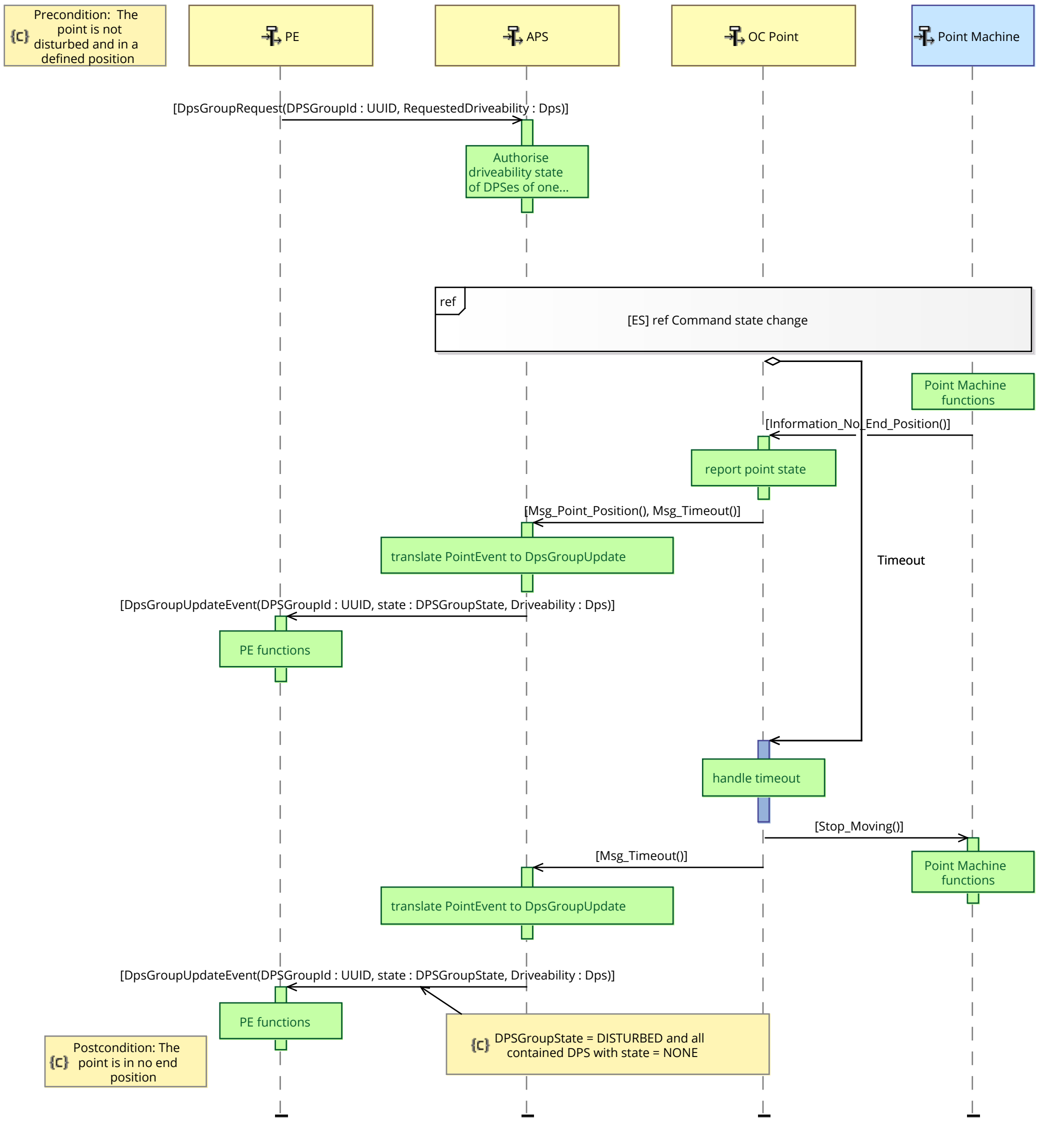

Precondition: The point is not disturbed and in a defined position
PE
APS
OC Point
Point Machine
[DpsGroupRequest(DPSGroupId : UUID, RequestedDriveability : Dps)]
Authorise driveability state of DPSes of one...
ref
[ES] ref Command state change
Point Machine functions
[Information_No_End_Position()]
report point state
[Msg_Point_Position(), Msg_Timeout()]
translate PointEvent to DpsGroupUpdate
Timeout
[DpsGroupUpdateEvent(DPSGroupId : UUID, state : DPSGroupState, Driveability : Dps)]
PE functions
handle timeout
[Stop_Moving()]
[Msg_Timeout()]
Point Machine functions
translate PointEvent to DpsGroupUpdate
[DpsGroupUpdateEvent(DPSGroupId : UUID, state : DPSGroupState, Driveability : Dps)]
PE functions
DPSGroupState = DISTURBED and all contained DPS with state = NONE
Postcondition: The point is in no end position

Figure 5: [ES] Set field element - timeout element setting

4.3.6.4 Further failed request after timeout

When a point reported timeout after a request, the *DPSGroupState* is DISTURBED and both DPSes are in state NONE.

If PE wants to request a new state again and it wouldn´t succeed again, there would be no state change. With the approach of only reporting state changes and with the approach of APS only doing safety critical checks and thus not checking, if the request succeeded after some time, it needs to be PE (or above), who monitors the failure of a second request.

To be investigated	The need of PE for a status update is under discussion.

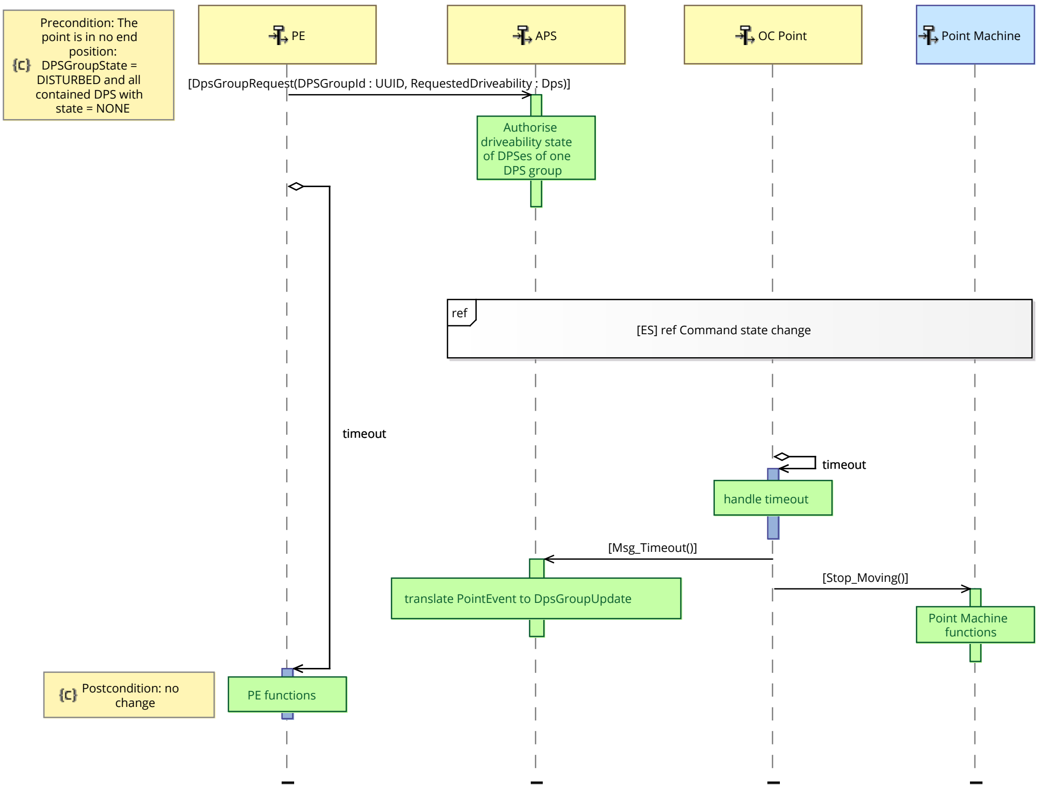

Precondition: The point is in no end position: DPSGroupState = DISTURBED and all contained DPS with state = NONE
PE
APS
OC Point
Point Machine
[DpsGroupRequest(DPSGroupId : UUID, RequestedDriveability : Dps)]
Authorise driveability state of DPSes of one DPS group
ref
[ES] ref Command state change
timeout
timeout
handle timeout
[Msg_Timeout()]
[Stop_Moving()]
translate PointEvent to DpsGroupUpdate
Point Machine functions
Postcondition: no change
PE functions

Figure 6: [ES] Set field element - timeout observation by PE

4.3.6.5 Communication loss

If APS detects a communication loss for the interface to/from *Object Controllers*, it notifies this to PE by sending a DPSGroupUpdateEvent, indicating that the DPSes in that group are all in state "NONE" now, the DPSGroupState is in "DISTURBED".

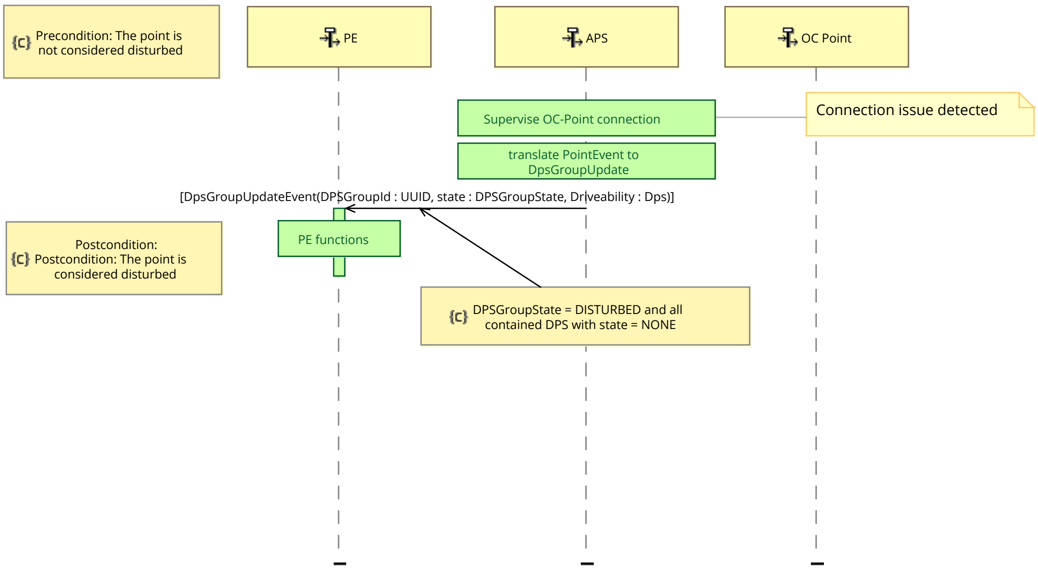

Precondition: The point is not considered disturbed
PE
APS
OC Point
Supervise OC-Point connection
Connection issue detected
translate PointEvent to DpsGroupUpdate
[DpsGroupUpdateEvent(DPSGroupId : UUID, state : DPSGroupState, Driveability : Dps)]
Postcondition: Postcondition: The point is considered disturbed
PE functions
DPSGroupState = DISTURBED and all contained DPS with state = NONE

Figure 7: [ES] Field element status - network issue

4.3.6.6 State change requested, but no network connection available

When the interface between APS and ocPoint is interrupted and a state change is requested by PE for the given point, all checks are performed. But when translating the request to a point-specific command, the request is rejected.

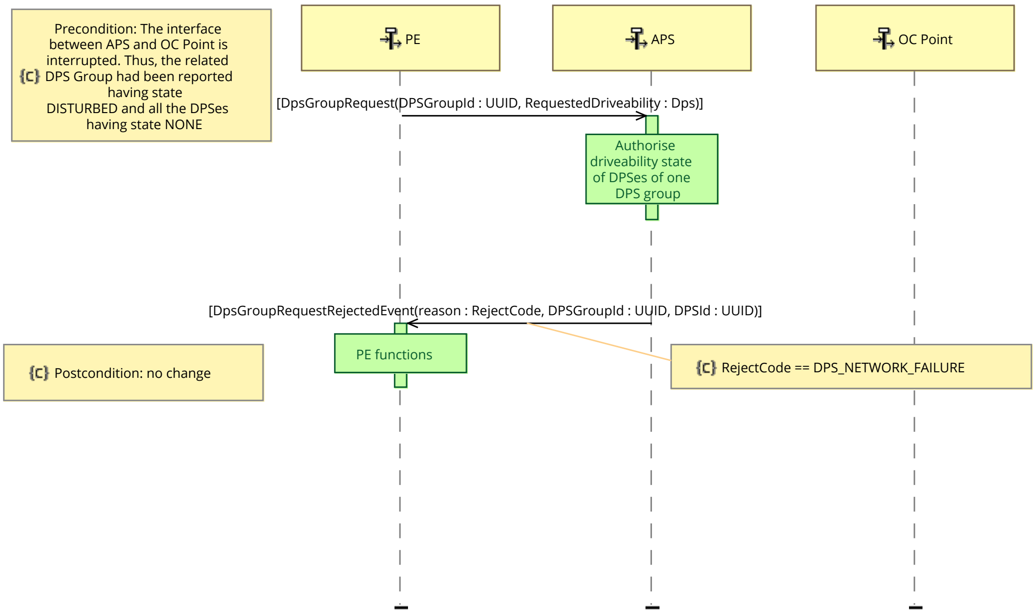

Precondition: The interface between APS and OC Point is interrupted. Thus, the related DPS Group had been reported having state DISTURBED and all the DPSes having state NONE
PE
APS
OC Point
[DpsGroupRequest(DPSGroupId : UUID, RequestedDriveability : Dps)]
Authorise driveability state of DPSes of one DPS group
[DpsGroupRequestRejectedEvent(reason : RejectCode, DPSGroupId : UUID, DPSId : UUID)]
Postcondition: no change
PE functions
RejectCode == DPS_NETWORK_FAILURE

Figure 8: [ES] Set field element - network issue

4.3.6.7 Trailed point

When a point is trailed, this is reported to APS by the *Object Controller*. APS translates this into a DPSGroupUpdateEvent, indicating, that the DPSes in that group are all in state "NONE" now and that the DPSGroupState is "DISTURBED".

It might be a variation point of APS if in consequence there is a specific behaviour (e.g. creating a *Usage Restriction Area* over a trailed point).

Independent from this (and not shown in the diagram), OC Point also reports the trailed status via SDI-P to Diagnostics & Monitoring.

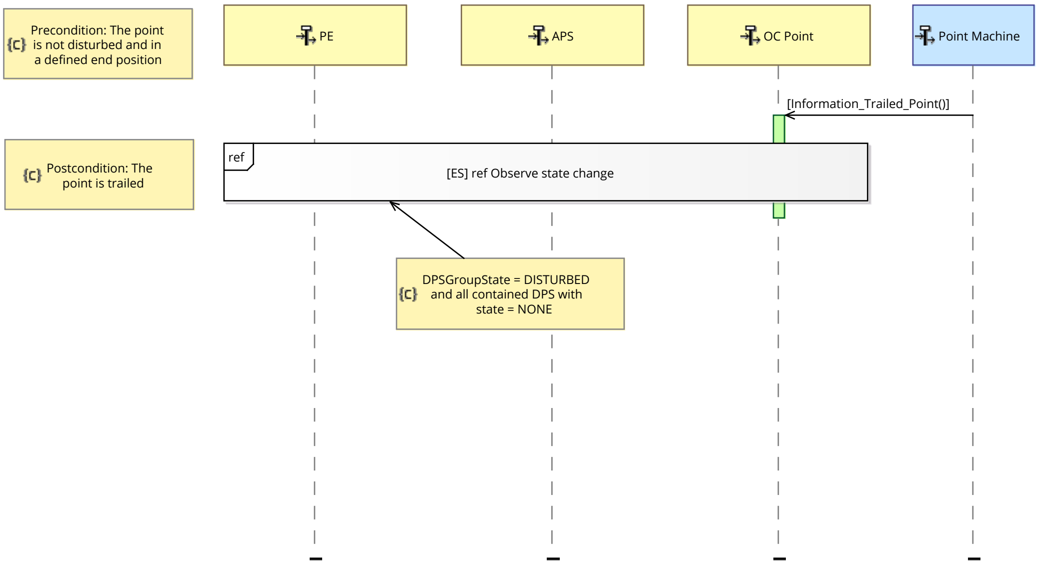

Precondition: The point is not disturbed and in a defined end position
PE
APS
OC Point
Point Machine
[Information_Trailed_Point()]
Postcondition: The point is trailed
ref
[ES] ref Observe state change
DPSGroupState = DISTURBED and all contained DPS with state = NONE

Figure 9: [ES] Field element status - trailed point

4.3.6.8 Loss of supervision

If Point Machine reports to ocPoint, that the blades are no more in any end position, this is reported via ocPoint to APS, where it´s translated to a DPSGroupUpdateEvent to PE, indicating, that the DPSes in that group are all in state "NONE" and the DPSGroupState being in state "DISTURBED".

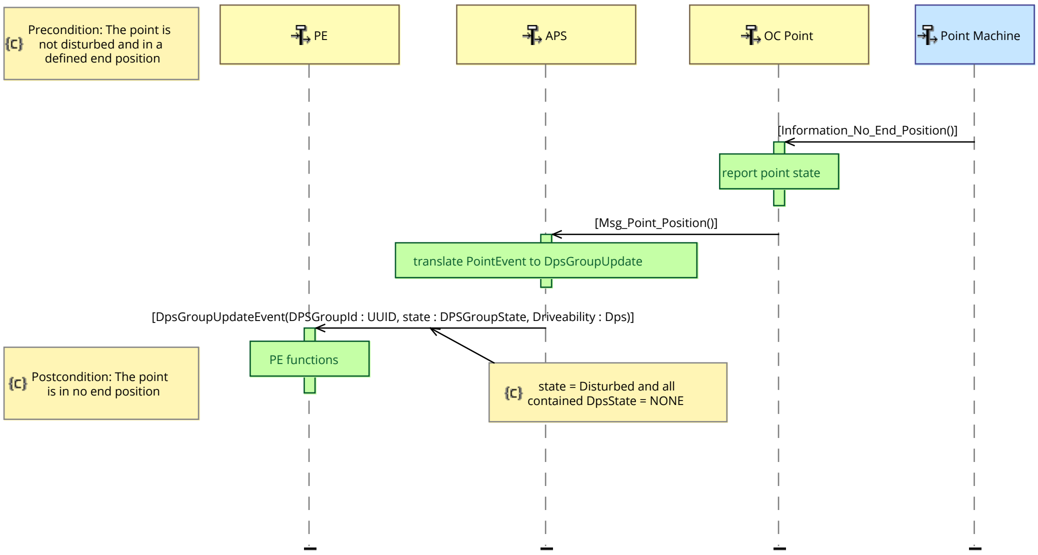

Precondition: The point is not disturbed and in a defined end position
PE
APS
OC Point
Point Machine
[Information_No_End_Position()]
report point state
[Msg_Point_Position()]
translate PointEvent to DpsGroupUpdate
[DpsGroupUpdateEvent(DPSGroupId : UUID, state : DPSGroupState, Driveability : Dps)]
PE functions
Postcondition: The point is in no end position
state = Disturbed and all contained DpsState = NONE

Figure 10: [ES] Field element status - loss of supervision

4.4 Configurability of behaviour

It is a general aim to avoid variability as far as possible. Operational harmonisation will support this.

In the functional area of setting switchable Field Elements the following variability is envisaged:

- Safety check to allow switching of a point used in another Risk Buffer in trailing direction: allowed/not allowed
- Configurability of the behaviour if a trailed point is detected (e.g. creating a *Usage Restriction Area* over a trailed point)

5 Measures to mitigate the risk of a flank collision

5.1 Scope

To ensure a collision-free movement of a train, there are the protection targets to safeguard the train from (other) following movements, encountering movements, and flank movements.

In normal operation, all movements of trains are controlled at the defined accepted risk level:

- In advance: Not granting any Movement Permission that would illegitimately overlap other Movement Permissions (APS);
- During execution: Supervising every Movement Permission (derived Movement Authority) on-board to ensure that its limits are adhered to (OBU).

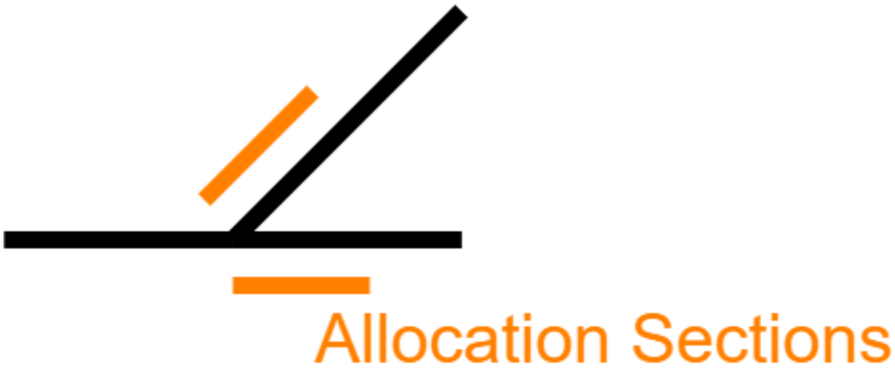
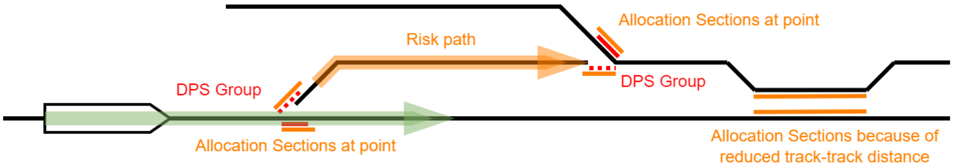
Hence, normal operation is characterised as the operational mode with the highest technical safety level. In contrast, degraded situation can occur where the movement is neither controlled nor planned. Derived from that split, different modes of operation are present. According to /RCA.Doc.63/, these can be accommodated by defining operational categories (supervised train or shunting movement (during the migration phase) following a secured route path or 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 conceptual analysis of defining measures to mitigate the risk of a flank collisions, mainly three modes of operation must be considered:

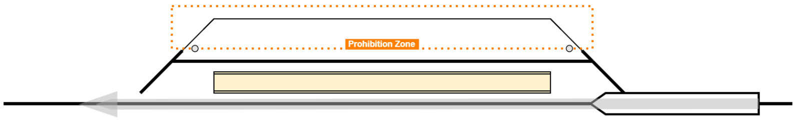
- Planned controlled movements
- Planned uncontrolled movements
- Unplanned uncontrolled movements

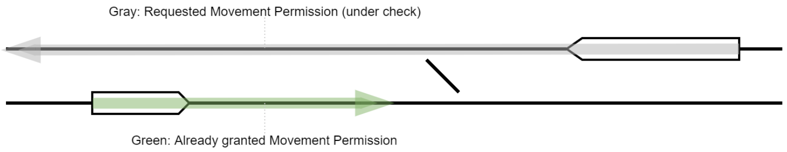
This means that for controlled movements safety is already ensured by these measures. In the target vision of APS, also today's planned uncontrolled movements, i.e. shunting manouvers, will be controlled (by support of needed paradigm game changers defined by ERA). That is, flank protection can not only be ensured by the on-board supervision of the Movement Permission (derived Movement Authority) but further measures have to be taken until all movements can be controlled (by overcoming the lack of incapable train sets) one day. However, for the migration of APS, with its different and early implementations plateaus, there will be planned uncontrolled movements (e.g. shunting, or maintenance vehicles). Furthermore, regardless of the migration phase, the occurance of unplanned uncontrolled movements (referred to as free movements in /RCA.Doc.63/) cannot be ruled out.

This concept introduces the conceptual approach of providing flank protection in areas where uncontrolled vehicle movements can occur during railway operation and thus, the risk of a flank collision with controlled and supervised train movements has to be mitigated.

5.2 Terms

Term	Explanation
Flank collision hazards	Flank hazards are endangering movements of vehicles on the track (e.g. vehicles, trains) that a Physical Train Unit (see /RCA.Doc.67/) which is moving on its cleared and authorised path needs to be protected against.
Allocation Section	The end of Allocation Sections mark the locations where the hazard of a flank collision can occur: This can be • at a tracknode like a point, crossing, or slip point or • at further places where Allocation Sections indicate the risk for lack of clear profile between conflicting movements. These situations trigger the need for a Risk Path. 
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.  Allocation Sections at point Risk path DPS Group DPS Group Allocation Sections at point Allocation Sections because of reduced track-track distance For instance, a Drive Protection Section Group (see /RCA.Doc.61/) or Movement Permission (see /RCA.Doc.63/) could be used for limiting the Risk Path. The Risk Path is defined as a Contiguous Track Area.

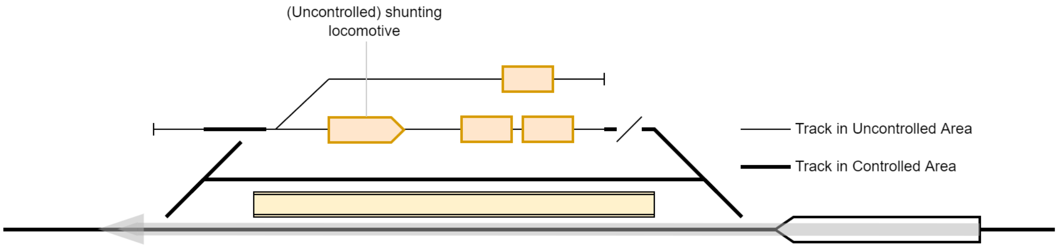
Term	Explanation
Controlled Area	A Track Area within the Area of Control where exclusively controlled objects, typically Physical Train Units (PTU), can be present: These objects can be controlled by trackside (APS providing non-overlapping Movement Permissions) and on-board (ETCS OBU supervising the related Movement Authority when using ETCS). Additional measures against flank collision risks by these objects are not required.
Uncontrolled Area	A Track Area within the Area of Control where non-controlled objects can be present (e.g. uncontrolled shunting units or stabled vehicles): These objects cannot (or only insufficiently) be controlled by trackside (APS) and on-board (in case of ETCS, no OBU present for wagons or choaches) and measures against flank collision risks by these objects must be taken, as these areas are usually connected to Controlled Areas.
Prohibition Zone	 A special Usage Restriction Area ewhere operational rules (can) forbid shunting or stabling of vehicles to provide flank protection if other measures cannot be taken or would not be taken for cost reasons. The area can be statically engineered in the Map data.
Repelling State	State of a flank protection providing element in which it actually does provide flank protection or a sufficient method that provides flank protection through its characteristics.
Trap point	If a flank movement can be prevented by a point (in its repelling position), this is used as a flank protection providing element. Points which are specifically designated only for this purpose are called trap points. They can usually be found at the end of a siding, protecting the main track.
Catch point (derail point), Derailer	This type of point is located directly in the track which is supposed to bear a movement with the risk for flank collision. Catch points (derail points) deflect in their repelling position the movement away from the Fouling Point and usually cause a derailment. Derailers are a simpler way: They do not deflect by forcing the movement off the straight track but have a deflector on the rail which will cause a derailment.

Term	Explanation
Granted and requested Movement Permission	The graphical representations and their meaning are explained in /RCA.Doc.52/. It should be repeated here that there is a graphical distinction between (already) granted and (currently) requested Movement Permissions:  Gray: Requested Movement Permission (under check) Green: Already granted Movement Permission

5.3 Problem description

5.3.1 High-level functionality

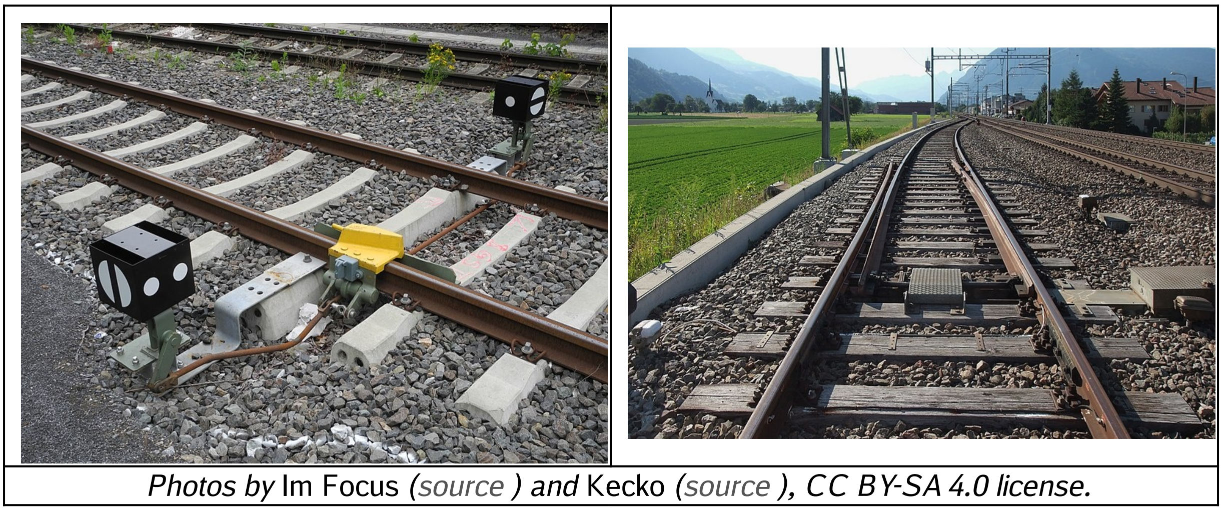
Physical Train Units (e.g. the train on the lower track in the figure below) have to be protected from flank collision hazards (e.g. vehicles on the upper tracks in the figure below) when they perform an authorised movement.


(Uncontrolled) shunting locomotive
Track in Uncontrolled Area
Track in Controlled Area

The basic assumption (see preconditions below) is that no controlled object can be endangered by another controlled object: Train protection (by trackside APS and on-board ETCS) safely prevents any hazard for flank collision amongst these objects.

However, non-controlled objects cannot be supervised and additional measures need to be taken (by trap points, derailers/catch points, and other measures). These measures need to be taken into account by the infrastructure planner in tracks where non-controlled objects can operate (Uncontrolled Areas, usually secondary tracks).

The photos show a derailer (left) and a catch point (right):



Photos by Im Focus (*source*) *and* Kecko (*source*), *CC BY-SA 4.0 license.*

Delimitation	In the target vision of RCA, all movements are controlled: Every single vehicle can be localised and shunting becomes a supervised (train) movement - in fact, there won't be any longer a distinction between shunting and train movements. However, in this edition of the document, the current operation with stabled vehicles and shunting movements is still assumed for different plateaus for installation and enabling fallback operations.

5.3.2 Current Solutions

The following sections give an overview of today's approach of flank protection in the UK, Switzerland, and Germany. The aim of this chapter is not to analyse all current flank protection laws and measures in Europe but to show the difference in approaching the topic on a national level.

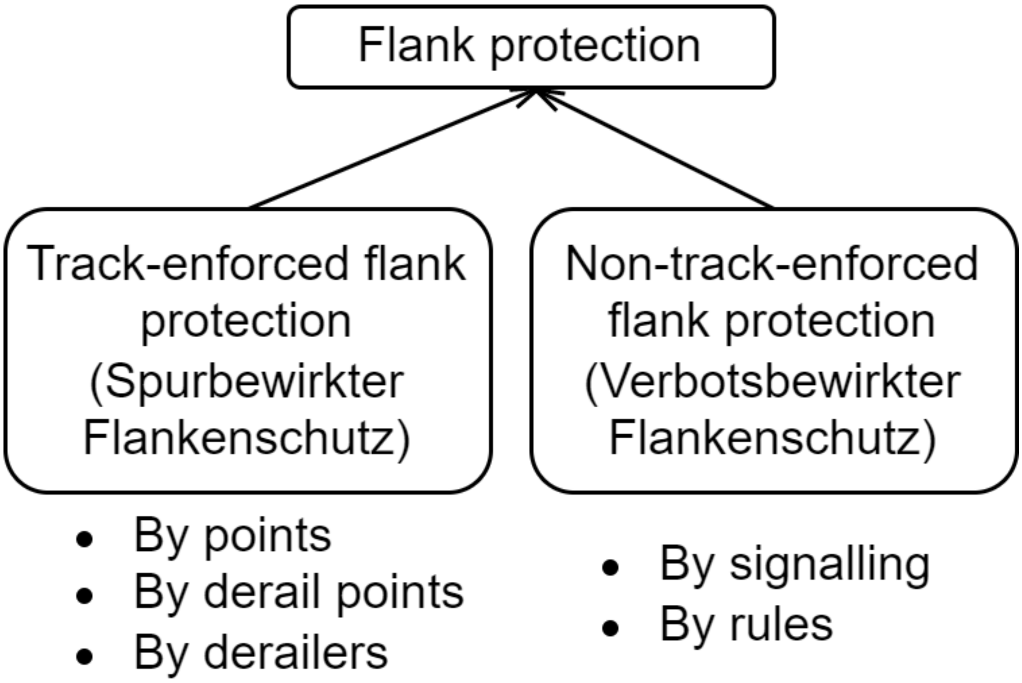
5.3.2.1 Network Rail (NR)

For UK the railway safety systems shall be designed in such a way that the risk of collision between train and shunting movements and runaway rolling stock is limited to an acceptable level (ALARP - As Low As Reasonably Practicable as consideration of costs vs. consequence). NR standards define the rules for the provision of protection, with these having evolved over time in the UK into two main types of protection generally being provided.

- Trapping protection - protection required to be given to authorised movements from areas such as sidings and lines on which rail vehicles are left unattended for long periods of time. These areas are considered at higher risk of rail vehicles moving without authorisation (i.e. rolling away) or moving beyond the authorised area (ie. signal overrun). This protection requires the setting of points or derailers to be provided to divert the rail vehicles (and potentially derail them) away from authorised movements. In some cases the need for a point or derailer can be waived if for example track gradient or operational rules mitigate the hazards of un-attended or shunting movements.
- Flank protection - setting of points not in the authorised route body of a train to protect the authorised trains from signal overrun or other unauthorised train movements on lines that could conflict with the authorised train. This protection historically would normally have checked that point detection of the 'flank point' was checked to be in protecting position before a protected route signal would clear. Recent changes now allow points to be only 'set' to a position, with detection only checked in higher risk areas or if a train is on or using the failed point. Detection now is generally only required if points within overlap or a defined 'overrun distance' from a signal and this inhibits two train movements being made at the same time in the event of a point detection failure. The UK engineering process includes, that each protecting signal will be assessed if the overrun mitigation (e.g. 'trapping' a movement) is suitable.

In UK a 'Clearance point' is provided that is a safety distance away from the 'Fouling point'. This distance helps to mitigate stretching or role back of trains into a protected route.

5.3.2.2 Schweizerische Bundesbahnen (SBB)


Flank protection
Track-enforced flank protection (Spurbewirkter Flankenschutz)
Non-track-enforced flank protection (Verbotsbewirkter Flankenschutz)
• By points
• By derail points
• By derailers
• By signalling
• By rules

SBB - Flank protection

By Swiss law /AB-EBV/, the railway safety systems shall be designed in such a way that the risk of collision between train and shunting movements and runaway rolling stock is limited to an acceptable level. The regulation states that flank movements can be prevented in particular by protective points, flank protection devices (like derailment devices) or the train control system.

Flank protection by means of protective points or derailment devices is to be preferred and are to be used

- On tracks for speeds above 120 km/h;
- On tracks for speeds above 80 km/h, at points of conflict where, both train movements and shunting movements take place during normal operation;
- On all tracks from which runaway rail vehicles are to be expected.

An exemption permit can be obtained if the speeds are (marginally) exceeded but providing flank protection would mean a disproportionate effort (only SBB).

The Swiss engineering rules /RTE25053/ detail the implementation of the regulation to achieve an acceptable risk level of collisions with flank movements.

The probability that a flank protection violation occurs depends on:

- Number of train movements at the conflict point;
- Number of shunting movements at the conflict point;

- Probability of vehicles running away against the conflict point. This is influenced by the
    - Gradient against the conflict point,
    - Type of movements towards the conflict point (e.g. regular pushing or pushing off or running off of vehicles),
    - Likelihood of improper movement of vehicles (e.g., by private loaders),
    - Local wind conditions,
    - Type of vehicles (wagons, coaches, groups of wagons/coaches, locomotives, multiple units, etc.).
- The extent of damage to be expected depends mainly on the speed of train travel at the point of conflict, the frequency of dangerous goods transports (and type of dangerous goods), the mode of operation of the flank protection.

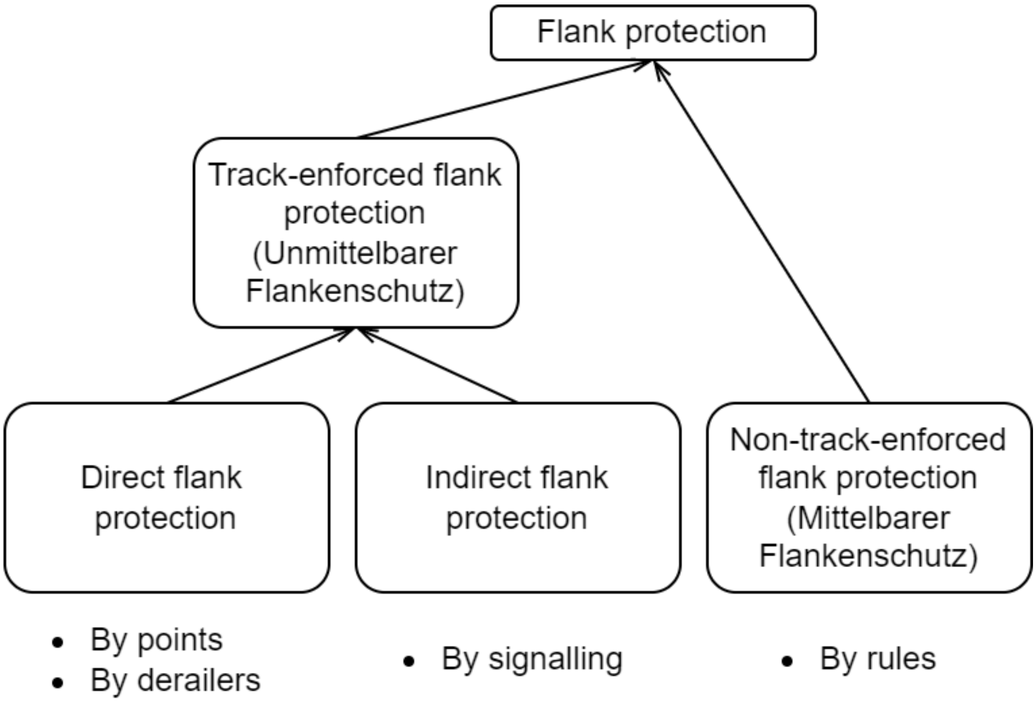
SBB uses decision trees taking these factors into account to decide on an appropriate flank protection measure (track enforced flank protection or flank protection by prohibitions), see the following points 1-3:

1. No track enforced flank protection possible meaning that reduced speed has to be signalled
2. Non-track enforced flank protection
    1. Minimum variant is to follow the regulations i.e. reduce the maximum speed to 80 km/h, no sidings/ramps/free loading sidings AND no slope towards the risk area/conflict point
    2. Shunting signals have to show stop aspect
    3. Shunting prohibited by shunt-stop signal
    4. Changing operative mode from "shunting permitted" (vmax=80 km/h) to "shunting not permitted"
3. Track-enforced flank protection
    1. Derailment points
    2. Derailer, only on tracks with a maximum allowed speed of 80 km/h
    3. Selective protective points: Dual called points (DE: Zwieschutzweiche)

Note: The scope of the engineering guidelines are unattended rolling stock and shunting movements being stopped belatedly.

EULYNX introduced in /Eu.Doc.36/ a degraded position for movable elements if the overall position cannot be detected absolutely. This enables the usage of points for specific operational situations, e.g. for flank protection. This is currently not implemented in the national operational processes but SBB is interested in the possible higher operational availability.

5.3.2.3 Deutsche Bahn (DB)


Flank protection
Track-enforced flank protection (Unmittelbarer Flankenschutz)
Direct flank protection
Indirect flank protection
Non-track-enforced flank protection (Mittelbarer Flankenschutz)
• By points
• By derailers
• By signalling
• By rules

DB - Flank protection

By regulation (Eisenbahn-Bau- und Betriebsordnung - EBO, §14 (11)), flank protection measures are demanded for passenger trains on main lines and secondary lines travelled with > 50km/h. With speed > 160km/h, flank protection points are demanded unconditionally.

Within DB flank protection is divided into track-enforced and non-track-enforced:

- Non-track-enforced flank protection is based on human communication and operational rules, that are used to ensure that movements towards the protecting worthy point have no permission (e.g. prohibition of shunting);
- Track-enforced flank protection is split into direct and indirect, where indirect means that the protection is ensured by the trackside asset (e.g. signal used for flank protection), which denies the permission for moving towards the protecting worthy point. For applying direct flank protection, the path to the protecting worthy point is secured by interrupting it with trackside elements (e.g. attached derailer or point in its Repelling State).

Only recently (end 2021), the regulation SBIV22 (in force since 1993) was updated to the new regulation 413.2002. The cause was a demand by the national German Federal Railway Authority (EBA) after two accidents. The authority's requirement was to re-evaluate the SBIV22 and check the updated regulation on the whole German network for sufficient presence of flank protection points.

The flank protection must be checked by the Infrastructure Manager. For this, the input beside the tracknet data (topology, including falling gradients) is

- Permitted maximum speed of the track of the endangered train

- Traffic according to operational plan:
    - For the track of the endangered train ("factor X") - number and typical speed
    - For the track of the endangering train ("factor Y") - number and shunting movements (being instances of endangering trains with/without train control)
- Local special situation ("factor Z") - gradients and factors increasing the effect of a hazard (e.g. bridge piers)

Traffic is derived from operational plan on a typical working day (Thursday is suggested), considering seasonal peaks above a defined threshold and future prospects of traffic increase.

The need for track-enforced flank protection is checked for each Fouling Point with a computation based on the risks represented by the mentioned input, yielding a risk value $F = X*Y*Z$:

- $0 \leq$ risk value < 5000: No flank protection point needed - an anual re-evaluation if traffic *per station* has changed and might result in a new risk value
- $5000 \leq$ risk value < 6000: A flank protection point might be needed - an annual re-evaluation of risk value per point/crossing is needed
- $6000 <$ risk value: Flank protection point needed - no annual re-evaluation

Summary: risk values are determined as static values on a per-day based traffic analysis, depending mainly on speed. Three stages of Accepted Risk Values exist to yield the need for flank protection points. Annual re-calculations are demanded very recently (and it appears challenging how the organisation can cope with this).

5.3.3 Problems with current solution

The short analysis of current solutions to mitigate the risk of flank collisions in the previous chapters shows some characteristica of today's measures:

- The risk of the occurance of a flank collision is assessed e.g. explicitely by a risk value or through a decision tree.
- The measure to prevent a flank collision is chosen according to the determined risk level.
- Generally, the higher the risk, a mitigation measure in the form of a piece of infrastructure is used, e.g. derailers or points.
- The mitigation measures are used at different points in time during the railway production meaning that in some cases the risk can be reduced to such a level that no further flank protection measure must be taken. As an example, in the UK flank protection already considered in the overrun risk assessment in the engineering process when planning protective signals.
- Additional safety assurance effort due to need of proving compliance to engineering rules (or providing the proof necessary to be exempted from implementing flank protection) is necessary.

In general it can be concluded, that the current measures implemented to mitigate the risk of flank collision range from interrupting the track path to the endangered train movement (e.g. direct flank protection) to applying operational rules (e.g. prohibition of shunting). The risk of a flank collision is highly depending on the operational and topological conditions in the area. Due to the diversity of national laws and engineering rules, the level of risk of a flank collision and the derived rules when a certain measure is appropriate are different and not harmonised. These rules are not dynamic, meaning that they are applied to fixed routes and block sections. This means also, that every change in the operating conditions, e.g. increase of speed limit, or the change in topology requires a new safety proof of having mitigated the risk of flank collisions to an acceptable level. The resulting high project engineering costs and the additional safety management effort have a negative impact on the overall lifecycle cost of the railway.

The question arises if the current (national) needs for flank protection will still be appropriate for the future railway system due to the continuous development of new and advanced technologies to automate and enhance the performance of today's railway. Considering the new game changers defined by ERA (e.g. trains are 'always on and always reporting'), it becomes evident that the risk levels of flank collisions are influenced. Also introducing technologies like ATO into the railway operation can mean that today's rules to determine the appropriate flank protection measure can be 'relaxed' depending on the migration plateau. This means, that it would be beneficial to define a generic ruleset that is capable to deal with evolving railway technologies as well as reduces safety assessment effort.

5.4 Solution summary

In the context of RCA, the possibility arises to introduce such generic rules for determining appropriate measures for flank protection, because of the application of abstract concepts like Drive Protection Sections, Movements Permissions, and Movable Objects being placed on a unified topology. Therefore, the design principles of how the measures to mitigate the risk of flank collisions are implemented have to be abstracted as well.

The concept to solve the problems outlined in the last section is based on the A.P.M. business targets (see /RCA.Doc.50/), the derived objectives for APS and PE listed in /RCA.Doc.53/, and the APS requirements derived in /RCA.Doc.51/ (the tracing of those APS requirements can be found in the appendix to RCA.Doc.52). Mainly the following two aspects of the APS objectives were used to derive the solution concept:

- Safe granting of movements on any topology considering the operational needed safety level and the possible risk mitigation measures
- Seperation of business logic (PE) and safety logic (APS)

The solution proposes a functional split in providing flank protection in the form of Risk Paths between PE and APS in the following way:

- Requesting safe but optimal Risk Paths.
- Checking if requested actually chosen Risk Paths are really safe and no Risk Path was forgotten.

Risk Paths as a measure to mitigate the risk of flank collisions are needed for each allocation section along the Movement Permission extent (and optionally of the Risk Buffer extent).

The concept of Risk Paths is introduced in /RCA.Doc.63/ as part of the Movement Permission and describes, how Risk Paths are checked once they are allocated in the context of ensuring all conditions for granting a safe train movement are met. This concept though focuses on the safety logic of how Risk Paths are found in the topology, built and allocated.

The idea is to determine the needed level of flank protection based on the nature of movements allowed in one area, i.e. if only controlled movements are allowed in a track area or if also non-controlled movements are allowed during normal operation. In case the need arises to perform uncontrolled movements in a controlled area during operation so-called Prohibition Zones can be established. Then, appropriate objects for providing flank protection are being searched, taking into account the shift from fixed light signals (limiting fixed blocks) to flexible end of Movement Permissions. Thus, the new approach results to also use moving (in the sense of dynamic) objects as flank protection element that can delimit the Risk Path. Please refer to the following sections for more details.

The behaviour of flank protection measures can be configured (see section Configurability below) to match national needs.

5.5 Prerequisites

5.5.1 Safety level of flank protection

Hint	Today, interlockings have no complete safety case which allows them to rely completely on the adherence to the (abstract) authorisation of movement (granted by lineside light signals or cab signalling). Therefore, nowadays a number of stricter measures are being taken (see the situation for some Infrastructure Managers described above), some of these reaching back to former times when there was no Train Protection System. With APS with its new and complete safety case and final European authorisation, it can be assumed to change this.

Amongst controlled movements - regular operation - the safety case is assumed to prove that the adherence to the Movement Permission (Movement Authority) will provide sufficient flank protection.

For uncontrolled movements (until they exist) and their potential dangerous impact - degraded operation - additional measures will be taken (see below).

5.5.2 All train movements are controlled

Trackside APS ensures non-overlapping Movement Permissions and ETCS OBU both supervises the adherence to the related Movement Authority and standstill if there is no Movement Authority. That means that the construction of a Movement Permission considers any remaining risk (at the accepted risk level) that a train could violate the limits of the permission to move. This is especially true for the Risk Buffer after the Movement Permission extent.

With this prerequisite, no controlled train movement can endanger another controlled train movement from the flank.

Note: Degraded modes of controlled train movements, e.g. loss of train supervision, are not analysed in this iteration of the document. The safe reaction of the system and handling regarding flank protection has to be aligned with the overall Incident Management Strategy.

Note: In addition see section All Risk Paths in Controlled Area.

Delimitation	Only measures to mitigate the risk of flank collisions are considered that are present at the time before granting the train movement. Scenarios of changing conditions that impact the flank protection of a train movement, e.g. moving trains on the topology, are not covered in this edition of the document.

5.5.3 Handling of non-controlled movements

In tracks (usually secondary tracks) where non-controlled movements can occur (shunting, stabling of vehicles with remaining rollaway risk), the Infrastructure Manager has to ensure that appropriate measures are available:

- Trap points, catch points/derailers;
- Prohibitions of shunting and stabling;
- Equipment with TTD (as otherwise non-controllable objects cannot be detected; see chapter: Unresolved Trackbound Movable Object).

Note: In addition see chapter: Risk Paths in(to) an Uncontrolled Area)

5.5.4 Technical standardisation

As concluded in the description of current situation above, the variety of national laws, engineering rules and operational processes for flank protection are a major impediment for the implementation of a straightforward flank protection solution. Therefore, changes of national legislation through harmonisation activities are a prerequisite to apply the following working principles in railway operation.

5.6 Solution details

5.6.1 Elements where flank protection is needed

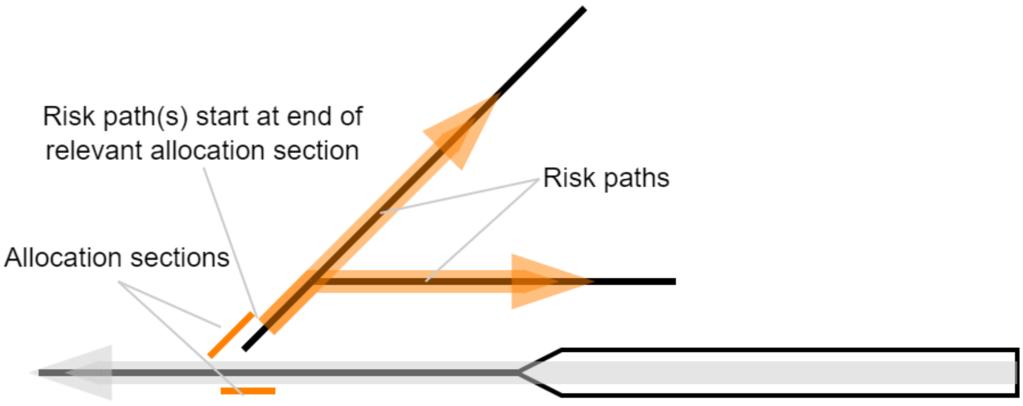
The risk of a flank movement can occur at each end of the relevant Allocation Section of points (including slip points) and crossings or at further places where Allocation Sections indicate the risk for lack of clear profile between conflicting movements.

Delimitation	Other movable Field Elements like turntables or traversers are out of scope in this edition of the document.

5.6.2 Methods for providing flank protection

To actually provide flank protection, APS defines, in contrast to today's solely track-enforced and non-track-enforced flank protection methods, a number of element types that can be used to limit a requested Risk Path.

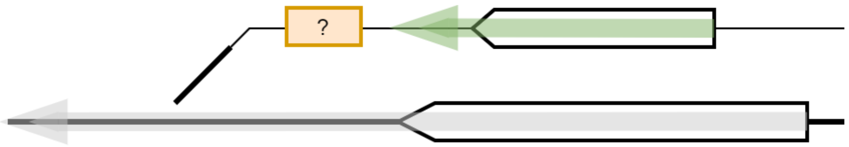
In the following sections, these element types will be described and the Risk Paths are depicted like this:



For simplification of the figures, the Allocation Sections will not always be depicted.

5.6.2.1 Movement Permission and Movable Object

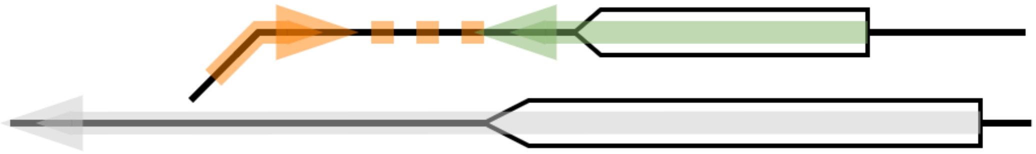
As stated in the preconditions, it is ensured that controlled objects don't impose flank collision risks on each other. That means they are all elements providing flank protection.

Delimitation	These elements are **not** providing flank protection **if** they are located in an Uncontrolled Area, as a non-controlled object can be between them and the end of a relevant Allocation Section: 

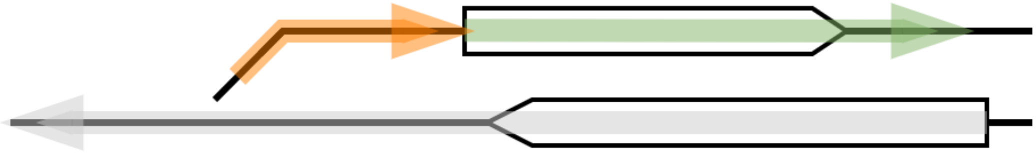
To be investigated	It must be prevented that the MOB leaves the controlled state (i.e. changes from FS/OS mode) or the train integrity is lost. Both will be the task of a safety manager function within APS, continuously supervising if all needed conditions are still met.

5.6.2.1.1 Movement Permission

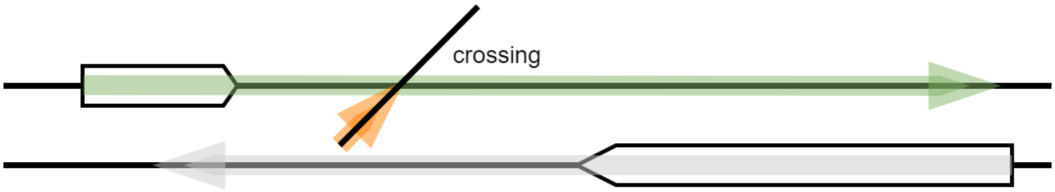
The Risk Buffer of a facing Movement Permission can delimit the Risk Path as well as the tail of a Movement Permission can:



or



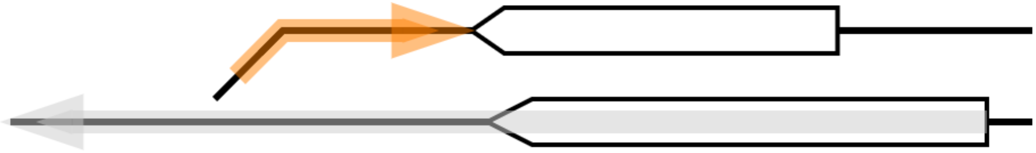
A Movement Permission or the MOB itself can delimit the Risk Path:



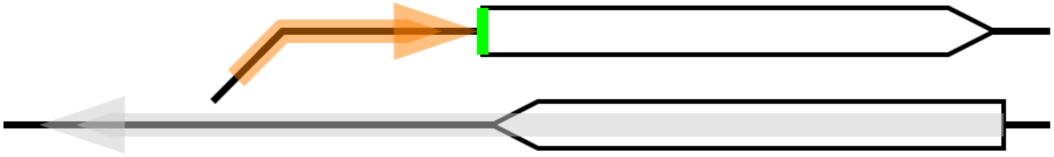
Repelling State: Unconditional (the existence of the Movement Permission).

5.6.2.1.2 Resolved Trackbound Movable Object without Movement Permission

A Resolved Trackbound Movable Object (rMOB) without a Movement Permission cannot move because it is supervised for standstill by on-board according to the accepted risk level; it can therefore delimit the Risk Path:

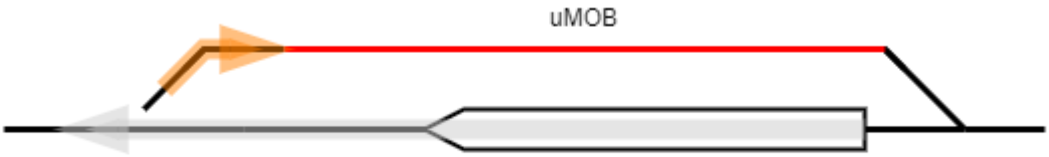


or



Repelling State: Unconditional the existence of the Resolved Trackbound Movable Object rMOB (Normal operation with train integrity or locomotive needs to be located at the front of the train composition):

5.6.2.1.3 Unresolved Trackbound Movable Object

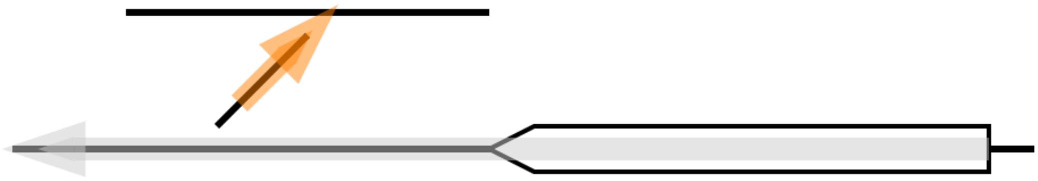


An Unresolved Trackbound Movable Object (uMOB) can limit a Risk Path in a **TTD area**. The rationale behind this is the consideration of today's safety principles: An occupied TVPS is protected by a signal showing stop aspect without knowledge what is occupying the track section (e.g. uncontrolled vehicle, train not reporting its integrity). The risk is deemed acceptable in the current railway system. Transfering this working principle to APS, the uMOB extent prevents setting of an MP into an occupied track section that is limited by TTD. In other word, APS protects the track path using occupancy information derived by the TVPS (analogous to today's interlocking minus the need for trackside signalling).

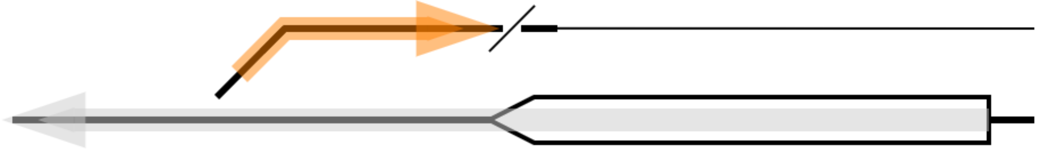
Note: For OTD areas, uMOBs should be a rare occasion. Whether they can provide flank protection has to be analysed after the overall risk analysis considering potential safety reaction of other subsystems and actors.

Repelling State: Unconditional (the existence of the Unresolved Trackbound Resolved Movable Object).

5.6.2.2 Point from trailing side, derailer/catch point



or

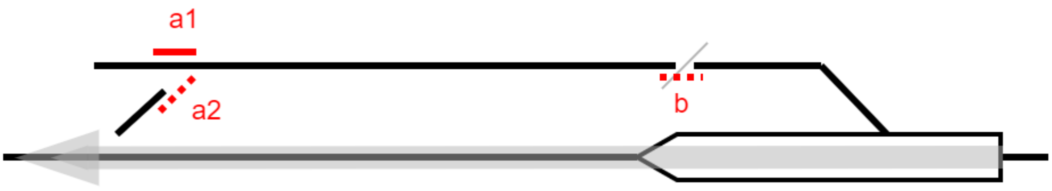


These are the 'classical' elements to provide flank protection by preventing the movement into the Risk Path.

Repelling State: Repelling position of the point/derailer.

5.6.2.2.1 Introduction: Drive Protection Section (DPS) abstraction

The elements in this concept will be described from their true nature of being a point, derailer, ... - not referring to the abstraction of DPS in /RCA.Doc.61/. Taking into account the DPS abstraction, each DPS must be configured in Map with the property of providing flank protection for a potential Risk Path approaching another DPS within the same DPS Group:

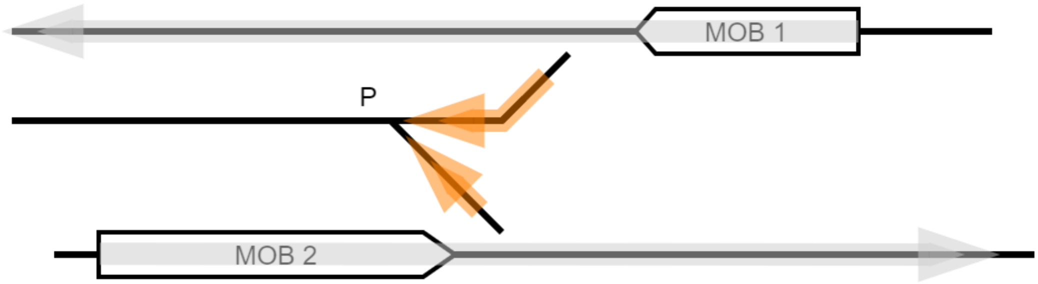


The from the point abstracted DPS Group {a1, a2} has the dependency that if a1 == FULL, it provides flank protection for a Risk Path search via a2 (along a2 only if in the direction towards the related Track Edge Point) and therefore terminates the Risk Path search.

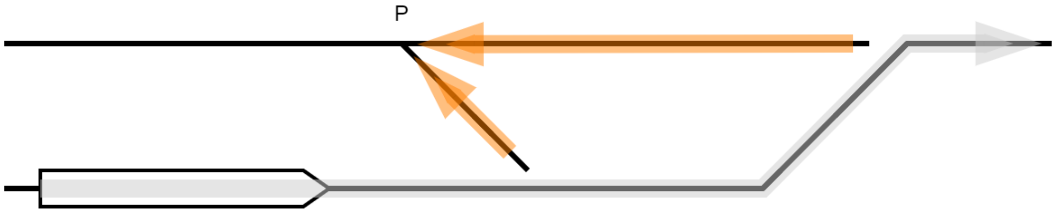
The from the derailer abstracted DPS Group (b) has the dependency that if b == NONE, it provides flank protection for a Risk Path search via b (depending on the type of derailer only in one or even in both directions) and therefore terminates the Risk Path search.

5.6.2.2.2 Special cases: Selective protective point and self-selective protective point

Selective protective point: In this special case, a point P potentially providing flank protection would be needed at the same time in two different (conflicting) positions:

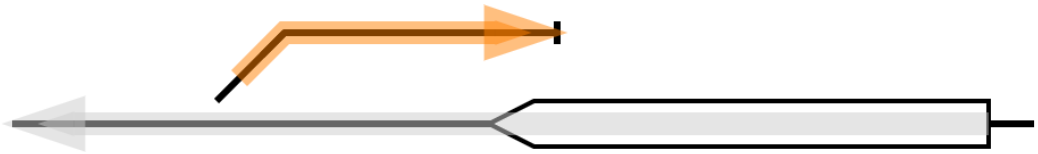


Self-selective protective point: A point P is needed in two different positions for providing flank protection for the *same* Movement Permission:



With the precondition of full control in the Controlled Area, both problems are no longer relevant : If any Risk Path starting from such an end of a relevant Allocation Section is terminated within the Controlled Area, it is even not needed to use these points as flank protection providing elements.

5.6.2.3 Buffer stop or end of tracknet



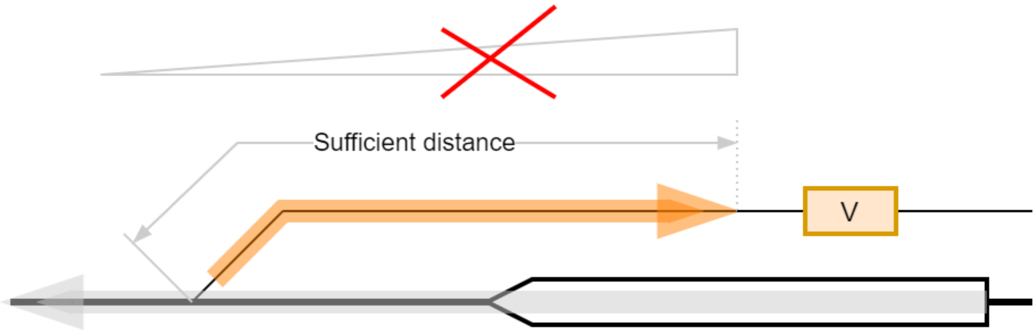
A buffer stop or an end of tracknet marks the last location of potential endangering risks and is therefore limiting the Risk Path search.

Repelling State: Unconditional (existence of the buffer stop).

Note: A switchable buffer stop is for this aspect similar to a derailer.

5.6.2.4 Sufficient distance inside Controlled Area or to Uncontrolled Area

As a further flank protection providing element, a sufficient distance can terminate a Risk Path (distance: configuration value). An additional precondition is not to allow a gradient falling against the direction of the Risk Path (zero gradient is acceptable). 'Sufficient' distance means that even if a vehicle is (rather) pushed into the Risk Path, APS will detect this (in Uncontrolled Area by TTD) and if the distance is sufficiently long, measures could be taken to stop the train of the endangered movement.



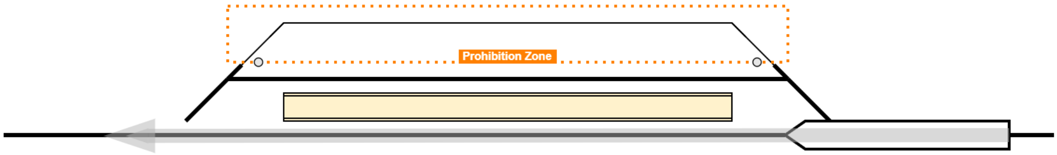
Repelling State: Unconditional (the existence of the distance with the static conditions named above).

5.6.2.5 Operational flank protection

Prohibitions are used where technical measures are not efficient from a cost perspective, and/or the risk for flank movements is low. Today it is left to regulations (prohibition) and eventually humans (operator, shunting staff) to enforce the adherence.

If APS is requested by PE to check a provided Risk Path, APS could not distinguish if the respective area is or is not protected by such a prohibition. In consequence, it would not be able to judge the safety of the provided Risk Path, and the Movement Permission request would be rejected.

A solution is to define a Prohibition Zone which makes this prohibition "visible" to APS:

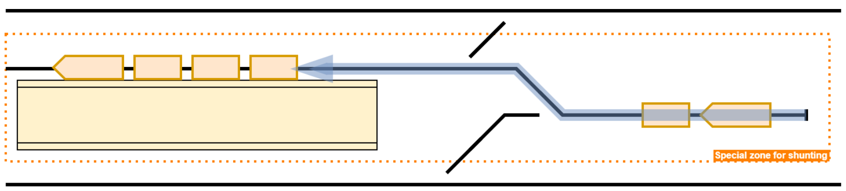


Repelling State: Prohibition Zone is in activated state.

Such a zone would typically be located in the Uncontrolled Area.

To be investigated	- Potentially this zone needs not only to be statically engineered and always active but could be switchable (active, inactive) and even creatable during run-time. - If a train requests a mode change which contradicts the characteristic/prohibition of the zone, APS would reject it if the Physical Train Unit is located in the zone and the zone's state is *deactivated.* - *Note: Shunting movements under full supervision (FS, no longer called shunting movements) - as in target view of RCA - would not fall under this restriction.*

Note: In addition see section *Risk Paths in(to) an Uncontrolled Area*.

To be investigated	In order to support shunting in the Controlled Area a special zone can be established with appropriate attributes (e.g. maximum speed of 25 km/h). **Example** Adding a wagon or coach to a train: 

5.6.2.6 Remote flank protection: Elements potentially providing flank protection but not in the Repelling State

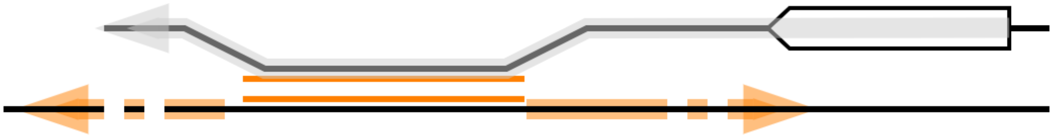
Obviously, if any of the aforementioned (potential) flank protection providing elements is found along the building of the Risk Path *and* it is *not* in the Repelling State, it cannot be used as a flank protection providing element.

The search is not terminated and will be continued until a (next) (potential) flank protection providing element is found (passed on, 'remote flank protection') or the search fails when reaching the search depth limit.

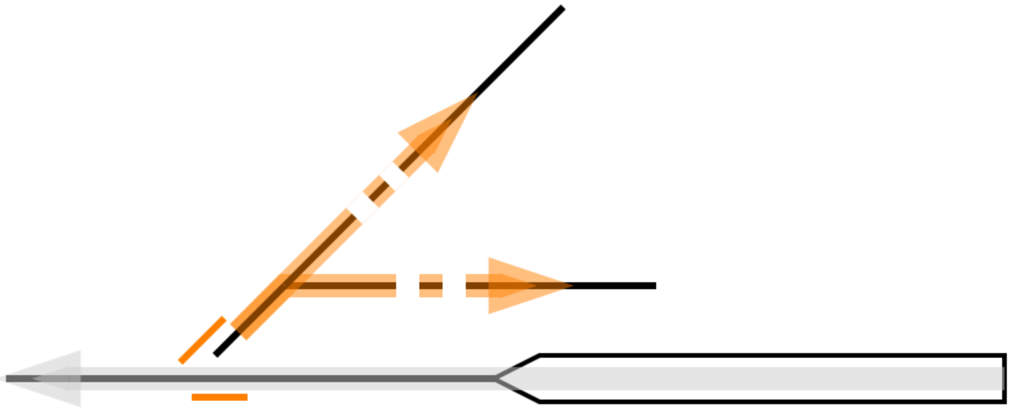
5.6.3 Determining the Risk Path(s)

To be investigated	The dynamic changes in the railway operation afterwards the MpRequest need to be considered in a further state of the concept.

Starting at every end of the relevant Allocation Section in the extent of the Movement Permission (including the Risk Buffer, if not opted out by other configuration, compare section *Configurability of behaviour* below), a set of Risk Paths is being determined, e.g.:



Each path will split up into two paths at points which are traversed from the facing side:

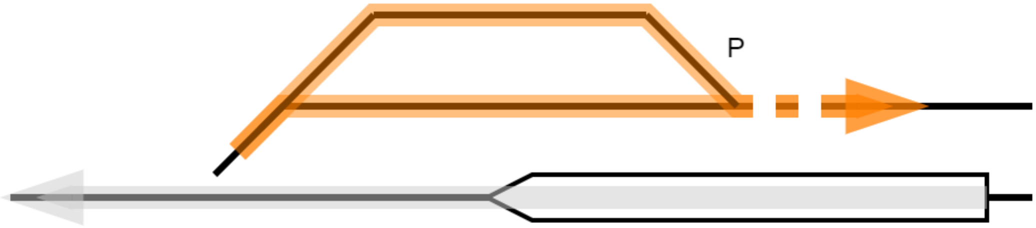


This means that the set of Risk Paths along the way traversed so far doubles, and each of the split Risk Paths is further traversed. A Risk Path is terminated through one of the listed methods above.

(In addition see section *All Risk Paths in Controlled Area).*)

To be investigated	The traversal could need to be continued beyond the limits of the Area of Control. As this area is not known to APS, searching for Risk Paths has to be done in co-operation with the neighbouring system. This will be investigated later in the course of the APS handover to/from another Area of Control.

It is not only the case that a Risk Path can be split - two (or more) Risk Paths can actually be joined in the end, if no flank protection providing element can be found before the joining point P, consider this example:



The consequence is that a Risk Path in its general representation needs to be a Contiguous Track Area (Linear Contiguous Track Area would not cover all cases).

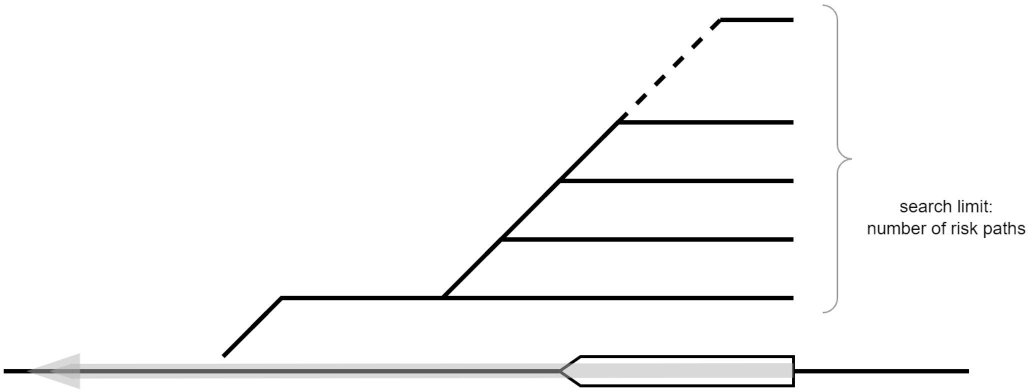
5.6.4 Remote flank protection (passing on flank protection demand)

The problem in current solutions of passing on flank protection demand when finding that the nearest element cannot provide flank protection ('remote flank protection') is built-in into the solution by the described split of the Risk Path.

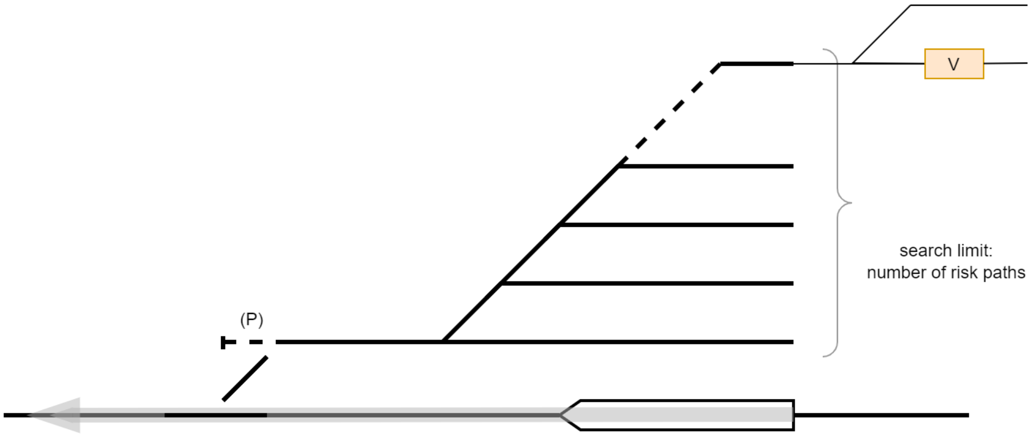
5.6.5 Risk Path search limit

It shall not happen that the search for Risk Paths starting from an Allocation Section is not terminating in sufficient extent and/or time because of frequent split by facing points. In practice, a configuration value (default value which is covered by the generic safety case) would limit the search (limit for number of Risk Paths). From today's computing performance point of view the search limit could be considerably big, however, there needs to be a limit.

If the search for Risk Paths terminates by the limit (i.e. does not find a flank protection providing element before) for at least one Risk Path, the entire search for flank protection fails.



The reason is that it can happen that right after the limitation of search there is a potential danger in an Uncontrolled Area (in the example: vehicle V). In such cases, the Infrastructure Manager must provide an alternative flank protection providing element within the search limit, in the example by a trap point P:



Note: The search limit matters, as later Movement Permission checks will demand the vacancy of any Risk Paths as well as the absence of occupancy claims - the bigger the search limit, the bigger the potential operational obstruction.

5.6.6 Functions

The following table gives an overview of the functions used to provide flank protection including the safety functions related to Risk Paths introduced in /RCA.Doc.63/ for the sake of completeness. As mentioned in the solution summary, only the functions concerning the provision of Risk Paths are described below since this concept focuses on these principles rather than how to check the allocated Risk Paths before granting the Movement Permission (refer to /RCA.Doc.63/ for that).

Function	Description	Remark
MpRequest syntax check, MpRequest existence check	See /RCA.Doc.63/	

Function	**Description**	**Remark**
Build Risk Paths	F or all ends of the relevant Allocation Sections in the extent of the Movement Permission (including the Risk Buffer, if not opted out by other configuration) a Risk Path(s) is determined. Note: Not all of the determined Risk Path might actually be needed, see function ' Check if all needed Risk Paths are provided'.	(For more details and examples see also section *Scenarios*)
Search limit	If the search for the limit of a Risk Path is not terminated within the search limit (configurable national value), the MpRequest is rejected.	Recall that Risk Paths are not needed within the Controlled Area. As the complexity is depending on facing points, the limit unit should be number of Risk Paths, not only distance.

Function	Description	Remark
Check if all needed Risk Paths are provided	Check that for every relevant Allocation Section a Risk Path is built and sufficiently providing flank protection. (see: Check needed Risk Paths' Repelling State) If the Allocation Section is within a Controlled Area and all possible Risk Paths for this Allocation Section remain within the Controlled Area, these Risk Paths are not needed to be further investigated, as the general characteristics of the Controlled Area are already providing sufficient flank protection. If for a Allocation Section a Risk Path need is found but PE requested no Risk Path for this Allocation Section, the MpRequest is rejected. Optional (configuration value): For every relevant Allocation Section in the Risk Buffer of a Movement Permission, the need for a Risk Path is determined.	Note: The setting of switchable Field Elements to the required state is already done before requesting a Movement Permission. For more details see /RCA.Doc.62/
Check needed Risk Paths' Repelling State	If a Risk Path is needed, the element providing flank protection at the end of the Risk Path must be in the Repelling State. Otherwise, the MpRequest is rejected.	If the flank protection providing element or method is not in the needed Repelling State, reject codes are delivered: • MOB_NOT_INTEGER • PROHIBTION_ZONE_NOT_ACTIVATED • SEARCH_LIMIT_REACHED

Function	Description	Remark
Route path clear proving for Risk Path Extent	See /RCA.Doc.63/	Geometrically, this means that no Movable Object and no Movement Permission must overlap any Risk Path.

5.6.7 Interaction between PE and APS

PE calculates the needed Movement Permission. This includes the *required* Risk Paths. For these, PE will calculate the Risk Paths according to the operational needs (if there is a choice).

Hint	For {allocationSection.name}}s where all potential Risk Paths remain within in the Controlled Area there is no need to consider flank protection (precondition!) and thus, PE would not need to request these Risk Paths.

There are two phases with two types of requests

1. DpsGroupRequest: PE will request here all needed positions of all switchable Field Elements, including those of the chosen Risk Paths. At this moment, APS cannot deduce whether a Field Elements is needed for a route, the Risk Buffer, or a Risk Path;
2. MpRequest: PE requests the Movement Permission, including the needed Risk Paths.

Only in the second phase, APS will check the Risk Paths.

The interaction between PE and APS is depicted in more detail in the figure below.

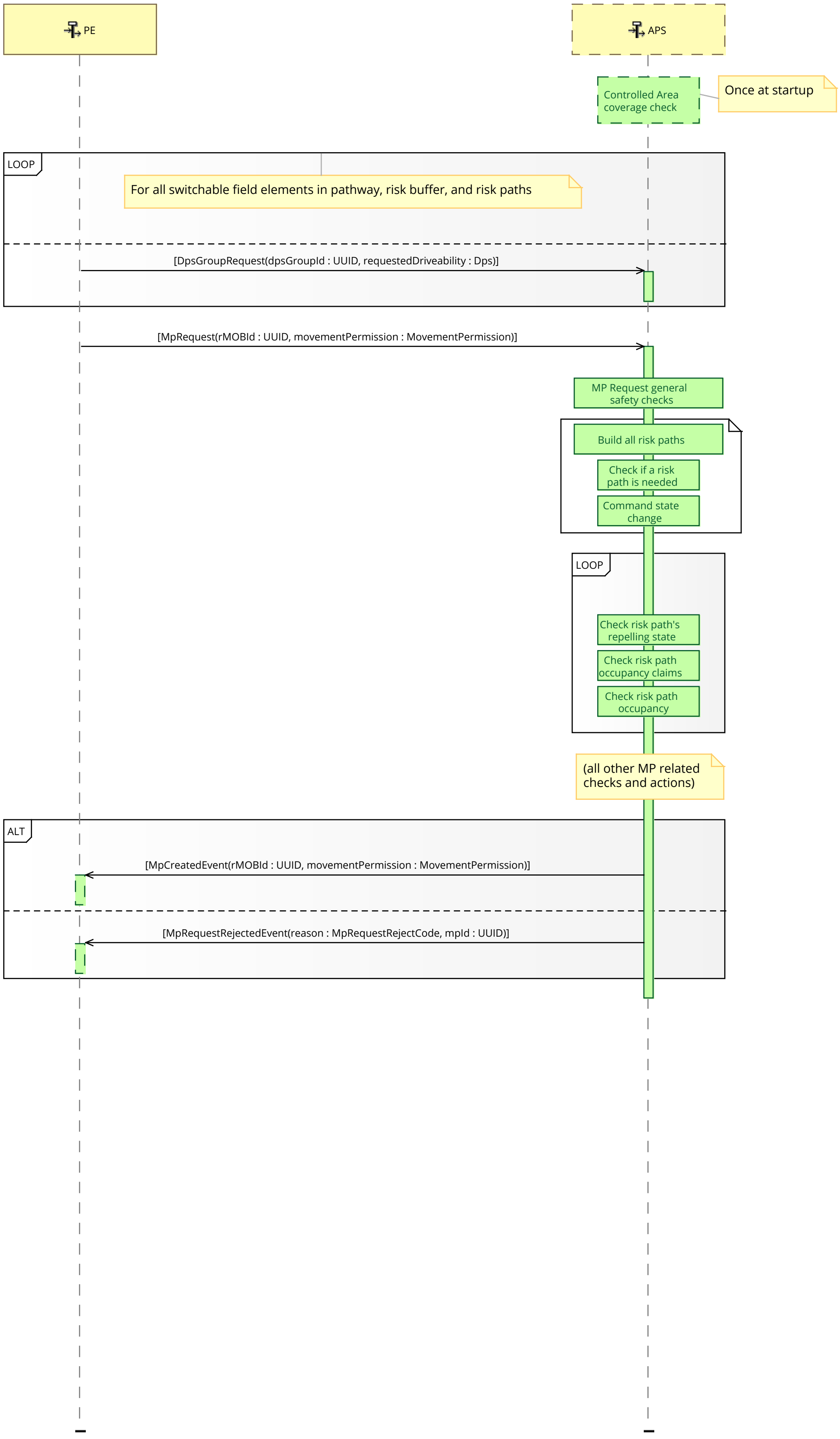

PE
APS
Controlled Area coverage check
Once at startup
LOOP
For all switchable field elements in pathway, risk buffer, and risk paths
[DpsGroupRequest(dpsGroupId : UUID, requestedDriveability : Dps)]
[MpRequest(rMOBId : UUID, movementPermission : MovementPermission)]
MP Request general safety checks
Build all risk paths
Check if a risk path is needed
Command state change
LOOP
Check risk path's repelling state
Check risk path occupancy claims
Check risk path occupancy
(all other MP related checks and actions)
ALT
[MpCreatedEvent(rMOBId : UUID, movementPermission : MovementPermission)]
[MpRequestRejectedEvent(reason : MpRequestRejectCode, mpId : UUID)]

Figure 40: [ES] Movement Permission - flank protection

The messages shown in the figure above are sent via the SCI-CMD interface (note that the reject code contains also non-flank protection reject reasons):

Messages		
Interface	**Exchange Item**	**Exchange Item Element : *Type***
SCI-CMD	**MpRequest** Request an inital Movement Permission.	**rMOBId : *UUID*** Identification of the MOB for which the initial Movement Permission shall be granted **movementPermission : *MovementPermission*** Specification of the Movement Permission to be initially granted
SCI-CMD	**MpCreatedEvent** The initial Movement Permission was successfully granted.	**rMOBId : *UUID*** Identification of the MOB for which the Movement Permission was granted **movementPermission : *MovementPermission*** Specification of the granted Movement Permission

Messages		
SCI-CMD	**MpRequestRejectedEvent** Sent if the authorisation to change the DPS drivability cannot be granted.	**reason :** ***MpRequestRejectCode*** More specific reason for the rejection • SYNTAX The requested MP does have syntax faults. • INCONSISTENT_WITH_MOB The requested MP does not correlated with the MOB mentioned. • INVALID_TOPOLOGY The requested MP covers parts not given on current topological data. • PATH_OCCUPIED Parts of the requested MP extent are occupied. • RISK_BUFFER_PATH_OCCUPIED Parts of the requested Risk Buffer extent are occupied. • AS_OCCUPIED Parts of the Allocation Sections in the requested MP are occupied. • EXTENT_CONFLICT The requested MP extent is in conflict with another MP. • EXTENT_AS_CONFLICT The requested MP extent is in conflict with Allocation Sectionss of another MP.

Messages		
		• RISK_BUFFER_CONFLICT The Risk Buffer of the requested MP is in conflict with another MP. • RISK_BUFFER_AS_CONFLICT The Risk Buffer of the requested MP is in conflict with Allocation Sections of another MP. • RISK_BUFFER_TOO_SHORT The Risk Buffer of the requested MP is too short. • SAFETY_RESPONSIBILITY_PROFILE_INVALID The requested Safety Responsibility Profile does not match with the current conditions. • SPEED_PROFILE_VIOLATION The requested Speed Profile does not match with the current conditions. • RISK_PATH_OCCUPIED Parts of the Risk Path in the requested MP are occupied. • RISK_PATH_CONFLICT Risk Path of the requested MP is in conflict with another MP • RISK_PATH_MISSING Risk Path in requested MP are incomplete.

		• UNPROTECTED_RISKPATH Risk Path of the requested MP does not got sufficient risk mitigiation measures for flank protection. • CHANGE_IN_EXTENSION The present MP is not covered by the requested MP for extension. • RECALCULATE_IN_EXTENTION The present MP of the requested MP extension differ in attributes. • UPGRADE_CONFLICT The requested MP for upgrade an existing MP violates the safety conditions. • URA_SPEED_VIOLATION The requested MP does not cover speed restrictions as temporarly active. • MOB_NOT_INTEGER The search for a flank protection providing element terminated at the rear end of an MOB. However, the MOB is not integer. • PROHIBITION_ZONE_NOT_ACTIVATED The search for a flank protection providing element terminated at a Prohibition Zone. However, the zone is not activated. • SEARCH_LIMIT_REACHED The search for a flank protection providing element did not terminate within the limits.

Messages		
		• DPS_DRIVABILITY_CONFLICT None • MOB_SUITABILITY_FAILURE None **mpId :** ***UUID*** Identification of the rejected Movement Permission

5.7 Configurability of behaviour

It is a general aim to avoid variability as far as possible. Operational harmonisation will support this.

In the functional area of flank protection, the following variability is envisaged and can be configured for each Infrastructure Manager:

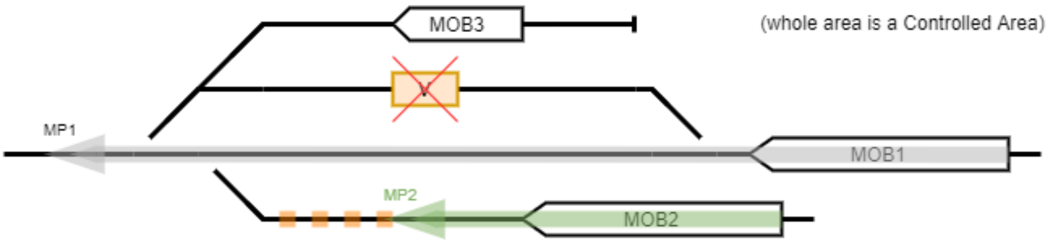
- The check for flank protection itself is optional (not every Infrastructure Manager needs flank protection)
- The check for flank protection within the Risk Buffer is optional
- Several configuration values (e.g. search depth when building the Risk Paths)

5.8 Scenarios

The following sections exemplify the provision of flank protection through the measures introduced in the previous chapters.

5.8.1 All Risk Paths in Controlled Area

In this example, Movement Permission MP1 is under check for Risk Paths which are all completely within the Controlled Area.



According to the precondition, there cannot be any object which endangers MP1; all these are self-controlled in a sufficient way:

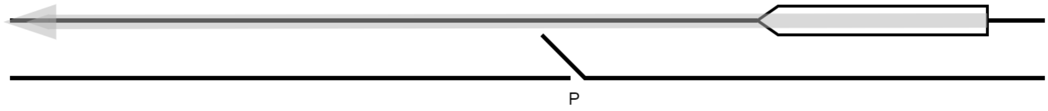
- MOB2 is supervised by its Onboard Unit adhering to the Movement Permission MP2 with a sufficient Risk Buffer
- MOB3 is supervised by its Onboard Unit for standstill (no Movement Permission) including the needed buffers (e.g. roll-away distance)

- Vehicle V cannot be there (otherwise, it's track would be in an Uncontrolled Area and would have to be secured by a flank protection providing element, like a derailer or a Prohibition Zone)

In this example, PE would not have requested any Risk Path and the granted Movement Permission MP1 would not contain any Risk Path. APS would check, however, all possible Risk Paths and would reject the request if it found any leading outside of the Controlled Area.

5.8.2 Waived point setting (for flank protection) in Controlled Area

In this situation, with all Risk Paths remaining within the Controlled Area:



PE could *(but does not have to)* request the setting of point P to its Repelling State (not leading into the Movement Permission) because for example, the distance of movements on the other track to the depicted Movement Permission is sufficiently large.. Additionally, according to the precondition, sufficient risk mitigation is given by the fact that only supervised movements (or MOBs without a Movement Permission) are present.

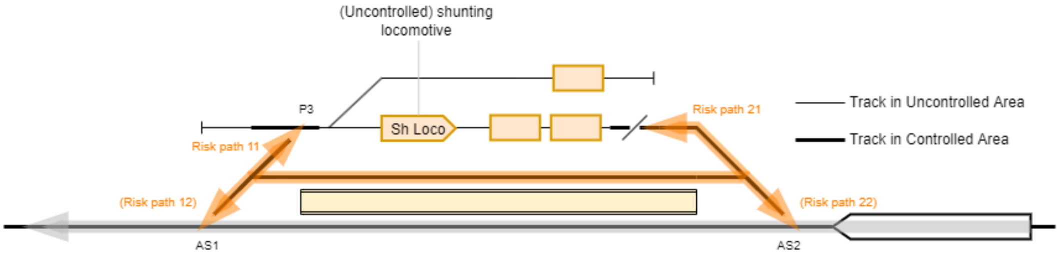
So PE could consider not setting the point P to its Repelling State for the reduction of switchings not needed from an operational and safety perspective.

Especially for the case of defective point P, today's restriction of decreasing the speed within the Movement Permission with the consequence of capacity decrease can be avoided. The possibility is also considered in the EULYNX requirements specification in /Eu.Doc.36/.

It has to be pointed out that the decision by PE would not be questioned by APS in this example - if PE provided a Risk Path terminating at point P, APS would not reject the Movement Permission request.

5.8.3 Risk Paths in(to) an Uncontrolled Area

In this example, a Movement Permission is under check for Risk Paths which are not all completely within the Controlled Area

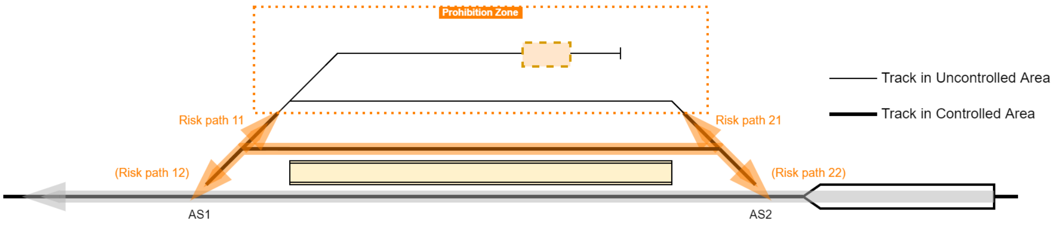


and terminate at the following flank protection providing elements (only listing those leaving the Controlled Area

- Allocation Section AS1
    - Risk Path 11 terminates at trap point P3

- Allocation Section AS2
    - Risk Path 21 terminates at derailer

If for cost reasons and low shunting traffic P3 (and the derailer) are not existing, a Prohibition Zone must be engineered.



If it is activated, Risk Paths 11 and 21 will both terminate at the activated zone. Otherwise (no such area engineered or engineered but not activated) the Movement Permission request will be rejected.

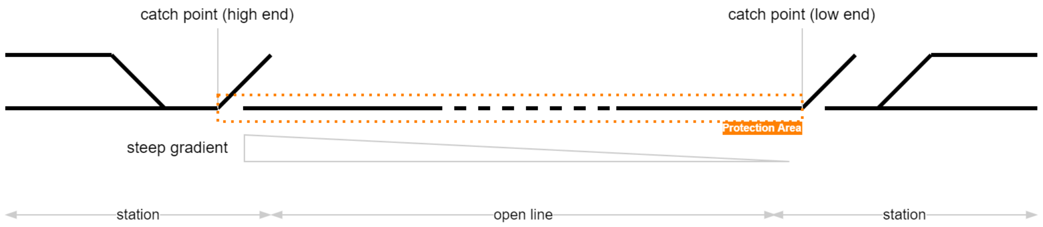
To be investigated	Depending on the type of the Prohibition Zone, vehicles may be in (prohibition for shunting) or not (prohibition for stabling). The adherence to the prohibition would be left to staff or for increased safety in case of prohibition of stabling, APS could check the occupancy state of the zone if it is equipped with TTD.

5.9 Future considerations

The following problem areas will be investigated further in a next edition. The sections below give an - incomplete - preview.

5.9.1 Catch points (steep gradients)

Catch points are a specific type of points that can also be used as measures to mitigate the risk of front-to rear collisions. They are used on lines with steep gradients. They prevent that vehicles can roll downhill out of a station - to the open line and into the next station. Therefore, they are situated both at the high end of the gradient at the end of the station and at the low end of the gradient at the beginning of the next station:



In the base (safe) position, they repell any movement away from the open line/station and shall always return to the safe position after a movement into the line/station.

Following topics are to be investigated in the next editions of this document:

- Requirement to reject the setting of the high end catch point into the station if it is not safe (no train in the Protection Area, high end catch point not set in safe position);
- Safety level of this requirement (can it be done in PE?);

- Supporting information to be attached at the two DPS groups (relationship, Track Area between them);
- Add the check if setting allowed to the *Set field element* part of this document.

5.9.2 Measures and levels of different flank protection methods

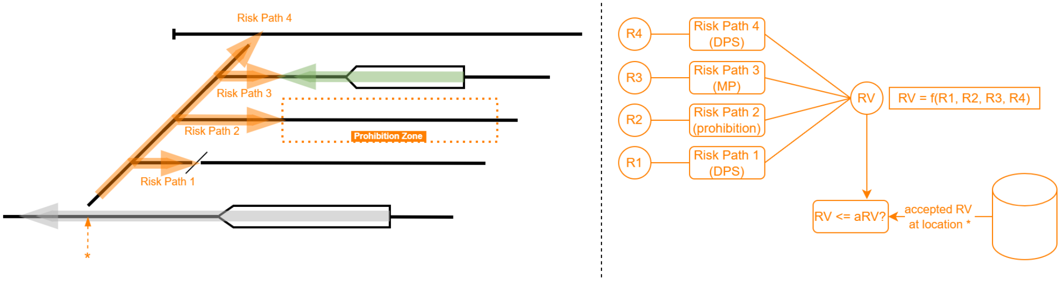
To be investigated	The dynamic changes in the railway operation afterwards the MpRequest need to be considered in a further state of the concept.

In general, APS needs to ensure that the Risk Paths are providing sufficient flank protection. As there are various methods for providing flank protection (see sections *Methods for providing flank protection*), where not all of them are equal in their characteristic, safety level, and methodology of fulfilling the flank protection demand, APS needs to have further measures for deciding about the potential risks for every Risk Path. For instance, a point in its Repelling State would presumptively have a lower risk value than an rMOB used for providing flank protection, based on a risk analysis.

One possible approach could be to rank the methods and let the IM decide through a configuration ('tool box'), which APS methods should be used for providing flank protection. A possible classification or ranking could be for instance:

1. APS uses infrastructure elements to interrupt the path to the protecting worthy point (point from trailing side, derailer/catch point, buffer stop or end of tracknet)
2. APS has the full control and state of information for ensuring the safeguarding that there is no Movement Permission towards the protecting worthy point (Movement Permission, Resolved Trackbound Movable Object without Movement Permission, sufficient distance inside Controlled Area)
3. APS has only partly control and state of information for ensuring the safeguarding that there is no permission to move towards the protecting worthy point (sufficient distance to Uncontrolled Area, Unresolved Trackbound Movable Object, operational flank protection)

Another possible approach would be to let each method (based on the national IM configuration) used for providing FP contribute with a risk value to a calculation of a risk tree (comparable to a fault tree). The value of that calculation would depend both on the risk value of the used methods and the situation (e.g. falling gradient towards the protecting worthy point), which then would be compared to a defined level it at least needs to fulfil.



In general, the following topics are to be further investigated in the next editions of this document:

- How to measure the risk of flank collision and distinguish between different levels of protection;
- Does the Risk Path needs to be statically or dynamically checked;
- How to cope with moving elements which can be used for flank protection and their special behaviours;
- Configurability and use of the flank protection methods by the IM;
- Handling of degraded situation.

6 Level crossings

The preparation of this topic is not yet mature enough for a concept. However, on the level of a position paper, /RCA.Doc.79/ can be consulted for first ideas on this subject.

7 Conclusion

Today's route setting and protection involves high engineering efforts to comply to national rules, technical solutions, and types of Field Elements. This concept gives an overview of new possibilities to set switchable Field Elements in order to ensure the trafficability of track sections and to provide flank protection measures using the principle of abstraction introduced by the layered RCA architecture.

Thus, switchable Field Elements are abstracted as DPS Groups to free the APS safety logic from considering specific Field Element types simplifying the safety checks and enabling longer, more stable life cycles.

The principle of abstraction also allows to abstract the measures to provide flank protection i.e. determining and limiting the Risk Paths starting at Allocation Sections along the requested MP. Furthermore, flank protection will be provided more efficiently: in order to mitigate the risk of flank collisions, it can be relied on the supervision of planned controlled movements in Controlled Areas, and additional measures for Uncontrolled Area like trap points, derailers, or Prohibition Zones can still be chosen where the supervision of conflicting movements is not available.

The switchable Field Elements considered in this concept are limited to (simple) points and derailers. The determination of the Risk Path is limited to the time until the MP is granted. While some degraded operative situations are being considered (e.g. loss of DPS supervision, unplanned uncontrolled movements), a full analysis of possible degraded train operation scenarios is not included in the current iteration of the document.