Rail to Digital automated up to autonomous train operation

D13.1 – Moving Block Specifications applying a train-centric approach

Part 2 - System Specification (Release 3)

Due date of deliverable: 31/10/2024

Actual submission date: 07/07/2025

Leader/Responsible of this Deliverable: Bertrand Badot, ATSA

Reviewed: Y

Document status		
Revision	Date	Description
01	17/07/2023	First issue Chapter 8 to 10 are still draft (not to be reviewed)
02	03/10/2023	Second issue for Release 1 Comments on first issue answered Chapters 8 to 10 completed and available for review
03	31/01/2024	First issue for Release 2 Comments on document revision 2 answered
04	16/04/2024	Last issue for Release 2 with answers to the Reviewer's comments. Scope of work for Release 3 anticipated in chapter 2
05	05/06/2024	First intermediate issue for Release 3. **Chapter 6.11 Functional requirements for flank protection (*Risk Path*) is work in progress and should not be reviewed.**
06	08/08/2024	Second issue for Release 3.

		Update according to comments received on Revision 05. Chapter 5.10 and 6.11 updated for Flank Protection. **Flank protection is now ready for review.** Chapter 5.15 and related functions revisited for cooperative MP request.
07	15/10/2024	Last issue for Release 3 with answers to the Reviewer's comments.
08	05/12/2024	Updated according to TMT review.
09	20/01/2025	Names of authors and reviewers introduced
10	07/07/2025	Update according to Review Sheet consolidated D13.1 (ERA + external reviewers)

Project funded from the European Union's Horizon Europe research and innovation programme		
Dissemination Level		
PU	Public	X
SEN	Sensitiv – limited under the conditions of the Grant Agreement	

Start date: 01/12/2022 Duration: 42 months

ACKNOWLEDGEMENTS

This project has received funding from the Europe's Rail Joint Undertaking (ERJU) under the Grant Agreement no. 101102001. The JU receives support from the European Union's Horizon Europe research and innovation programme and the Europe's Rail JU members other than the Union.

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Bertrand Badot, Staffan Pettersson	ATSA	Author
Frank Skowron	DB	Author
Nader Nayeri, Thomas Naulin	GTSD	Author
Stephan Bischoff, Bettina Morman	SBB	Author
Lucia Blanco	ADIF (INECO)	Reviewer
Daniel Kolar	AZD	Reviewer
Eivind Lenschow	Bane NOR	Reviewer
Ivan Velado Martinez, Marta Garcia	CAF	Reviewer
Martin Woiton, Konstantinos Emmannouil, Petra Hubrig, Christian Sadowski	DB	Reviewer
Andreas Distler	DLR	Reviewer
Felix Schaber, Gerhard Wipplinger, Andrej Kiriviga	GTSD	Reviewer
Giuseppe Pagliarulo	MERMEC	Reviewer
Manuel Schleiffelder, Hubert Künig, Salome Christiani	OBB-Infra	Reviewer
Simon Chadwick, Craig McLellan	SMO	Reviewer
Adelaide Vitiello	STS	Reviewer
Anders Lindfelt	TRV (KTH)	Reviewer

Disclaimer

EXECUTIVE SUMMARY

This document specifies the signalling system, called Moving Block System, in particular the system capabilities, functions, interfaces, and the specific domain objects.

This document contains the System Specification for a train-centric signalling system providing high capacity with low cost and high reliability, enabling moving block operation.

This document is part of the Moving Block System specification deliverable.

ABBREVIATIONS AND ACRONYMS

For abbreviations and acronyms used in the ERTMS/ETCS specifications, please refer to /ETCS/ SUBSET-023 and SUBSET-026 chapter 7 for ETCS variables.

AoC	Area of Control
CCS	Control, Command and Signalling
DPS	Drive Protection Section
DPSG	Drive Protection Section Group
DR	Digital Register
ERJU	Europe's Rail Joint Undertaking
MBS	Moving Block System
MP	Movement Permission
mSFE	Min(imum) Safe Front End
MSFE	Max(imum) Safe Front End
mSRE	Min(imum) Safe Rear End
MSRE	Max(imum) Safe Rear End
PE	Plan Execution
R2DATO	Rail to Digital automated up to autonomous train operation
RB	Risk Buffer
RCA	Reference CCS Architecture
RP	*Risk Path*
SCI	Standard Communication Interface (EULYNX)
SCI-CMD	Standard Communication Interface – Command
SCI-P	Standard Communication Interface – Point
SCI-TDS	Standard Communication Interface – Train Detection System
S2R	Shift2Rail
TA	Trackside Asset
TACS	Trackside Asset Control and Supervision
TCCS	Transversal CCS (Control Command and Signalling)
TDS	Train Detection System
TEP	Track Edge Point
TES	Track Edge Section
TIMS	Train Integrity Monitoring System

TO	Train Object
TTD	Trackside Train Detection
UTO	Unresolved Trackbound Object

GLOSSARY

Note: Some of those terms are currently also defined in the Glossary of other documents (e.g., System Definition, Safety Analysis) of WP13. Therefore, as long as there is no separate Glossary document available, care must be taken to keep the definitions synchronised.

Term	Definition
Allocation Section	*Allocation Section*s express gauge clearance conflicts between different tracks. For example, *Allocation Sections* are associated to the representation of switchable Track Assets and further track connections like diamond crossings. The *Allocation Sections* are used in terms of granting a Movement Permission request as condition for clearance in a certain area. See also /FlankProtection/
Area of Control (AoC)	The Area of Control is the topologically limited extent used here for defining the technical and operational responsibility of one instance of MBS.
Domain Data	The *Domain Data* refers to use case specific configuration data for the MBS to define the specific application. These can be broadly classified as Map Data, Segment Profiles, and Parameter Data. As a part of configuration process, the MBS needs *Domain Data*. Potential updates of *Domain Data* will be realised by a centralised provisioning process incl. synchronous activation of the new data version. Source: /SD1DM/
Domain Object	A *Domain Object* is an abstract object for which a Domain (e.g. Moving Block System) has the main responsibility. There might be other Domains who are consumers of this object as well. In general, it is based on or linked to the *Domain Data*.
Drive Protection Section (DPS)	A *Drive Protection Section* is a linear contiguous stretch of track with a driveability (passage possible yes/no) state. A *Drive Protection Section* (DPS) represents a *Track Edge Section* that can be brought to different driveability states to ensure the driveability or safety of a track route. As such, it is an abstraction for any location on the railway network that may adopt different states due to Switchable Trackside Asset (e.g. points or level crossings). Source: RCA

MBS Operational State	*MBS Operational State* is the collection of all of *Domain Objects* instantiated by the MBS to manage its operations and supervise the train movements. This includes: • *Train Objects,* • *Unresolved Trackbound Objects,* • *Trackside Asset* Objects, • *Movement Permission,* • Etc...
MBS is operational	*MBS is operational* when it is in a state allowing the MBS to perform its fundamental function ensuring safe train movement and preventing railway accidents, incidents... From now on, communication sessions to the external systems (e.g., OBU, PE, etc.) can be established and supervised.
Movement Permission	The *Movement Permission* defines the part of the track that is reserved for the movement of a train. It includes: - *Movement Permission Extent* - *Risk Buffer* - *Risk Path* - Requested Maximum Speed - ETCS Movement Mode - List of DPS Groups that must not be used as flank protection measure
Movement Permission Extent	A *Movement Permission Extent* is a linear contiguous stretch of track that is reserved for the movement of a train. The *Movement Permission* is translated to an authorisation (e.g. Movement Authority) according to the /ETCS/ - SUBSET-026 that is transmitted to the train. The *Movement Permission Extent* is part of the Movement Permission. Source: RCA
Non-switchable Trackside Asset	A *Non-switchable Trackside Asset* is a Trackside Asset which provides information to the MBS (e.g. *Trackside Train Detection*) but cannot be controlled to a particular state.
Position is ambiguous	The position information contained in a Train Position Report (Position Report or SoM Position Report with status valid) can be considered as ambiguous in case MBS is not able to safely locate the train within the track layout. Since the Train Position Report only contains a (directed) distance to the LRBG, MBS might not be able to locate the train on the correct position in the track layout, e.g. in case of a zig-zag movement

	(see Hazard 0003 in /ETCS/ - SUBSET-113) or when there is a facing pair of points between the LRBG and the position of the train.
Risk Buffer	The *Risk Buffer* is a linear contiguous stretch of track that serves as the overrun protection and in the event of a rollback of a chased train. It is part of a Movement Permission. A *Risk Buffer* exists if there is a Danger Point or a safe margin (project specific) greater than zero. Source: RCA
Risk Path	A *Risk Path* is one potential path (a linear contiguous stretch of track) by which a non-permitted vehicle movement could result in a flank collision with a vehicle moving along the *Movement Permission Extent*. A Movement Permission can contain zero or more *Risk Paths*. Source: RCA
Switchable Trackside Asset	A *Switchable Trackside Asset* is a *Trackside Asset* which enables (e.g. points, derailers, movable bridges, gates) or allows (e.g. light signals at border, level crossings) the continuation of movement beyond this asset when this latter is controlled to particular state.
Topology Data	See entry for *Domain Data*
Track Edge (TE)	*Track Edge* is a linear object that defines an uninterrupted stretch of a railway track without divergence or convergence. A *Track Edge* is defined along the centre line of the 2D or 3D track alignment and has a finite length. The *Track Edges* have an implicit direction (from start to end). The start/end of *Track Edge* shall correspond to the location of a simple point, or any form of end of track. Source: RCA, /SD1DM/
Track Edge Point (TEP)	A *Track Edge Point* is a spot location on a *Track Edge*. Example usage: balise location Source: RCA, /SD1DM/
Track Edge Section (TES)	A *Track Edge Section* is a linear extent between two *Track Edge Points* on (the same) *Track Edge* and can be directed. Example usage: Track properties like gradient, SSP, DPS Source: RCA, /SD1DM/

Trackside Asset (TA))	*Trackside Asset*s are elements on or near the track which are used to monitor (using sensors) and/or control (using actuators) the movement of vehicles through the railway network. They can be switchable or non-switchable and are controlled by the actors *Trackside Asset Control and Supervision* (TACS). See also *Switchable Trackside Asset* and *Non-switchable Trackside Asset* definition.
Trackside Asset Control and Supervision (TACS)	The *Trackside Asset Control and Supervision* (TACS) is a subsystem supervising and controlling *Trackside Asset*s.
Trackside Train Detection (Section)	*Trackside Train Detection* is a system which determines the occupancy status of TTD sections. TTD section may be a Track Circuit or an Axle Counting system. EULYNX synonym: Track Vacancy Proving Section (TVPS)
Train Location	*Train Location* is the MBS interpretation of the unambiguous location of the train, based on Train Position Reports, Validated Train Data and other inputs if available, e.g. TTD. *Train Location* is a linear contiguous stretch of track that has a front and a rear. X2R5 source: Train Location RCA source: rMOB extent
Train Object	*Train Object* is the object needed by the MBS to manage the connected trains currently performing their mission. Note: This *Train Object* could nevertheless correspond to a train not (yet) localised by MBS. If a Train Object is referenced as a geometric extent, the extent is the extent of the Train Location. RCA source: (rMOB)
Train Position Report	The term *Train Position Report* refers to either Position Report packet (packet number 0) or Position Report based on two balise groups packet (packet number 1) according to /ETCS/ - SUBSET-026, chapter 7.
Unresolved Trackbound Object	*Unresolved Trackbound Object* is the object needed by the MBS to manage a contiguous track area where track vacancy is not proven and cannot be linked to any connected train (*Train Object*). RCA source: uMOB X2R5 source: Unknown Track Status Area (partly)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The task 13.2 “Moving Block Specification – Requirements, engineering and operational rules” within the WP13 of the project FP2 – R2DATO has got the objective to develop a Moving Block Specification.

As a result of this task, the present document specifies the Moving Block System, as firstly defined in the Moving Block System Definition (document /SysDef/).

This specification focuses on the functional requirements. Non-functional requirements are considered in a later release of this document.

This document is related to the following work packages:

- WP13: Task 13.3: Moving Block Safety Analysis
- WP14: Moving Block ETCS Level 3 – Prototype development & Analysis
- WP44-45: Moving Block ETCS L3 Demonstrator – Specification

2 SCOPE OF WORK

The scope of release 3 of the System Specification is limited as follows[1]:

Capability:

- Start up the system
- Load *Domain Data* at start-up
- Control the *Trackside Assets* (SCI-P only)
- Establish, maintain and terminate communication session with *Trackside Asset*s
- Manage track path allocation (including Release allocated portion of track path which has been passed by the train and Release allocated portion of track in front of the train)
- Manage authorisations for train movement (Movement Authority, Request to Shorten MA)
- Manage the current trackside state and determine the state of the track from information given during runtime by trains and *Trackside Asset*s within its *Area of Control*
- Store an up-to-date, reliable and consistent *MBS Operational State* and provide this to consuming systems (PE only)
- Establish, maintain and terminate communication session with OBU

Interface with

- *Trackside Assets* (SCI-P and SCI-TDS) via *Trackside Asset Control and Supervision* (TACS) instances
- Plan Execution (PE)
- ETCS On-board (OBU)
- Digital Register (DR)

The following needs are covered:

- Flank Protection
- Splitting, joining, turning (with/without Cold Movement Detection)
- DPS Group
- Propagation of UTOs
- Train length (L_TRAIN) reliability

All other interfacing systems according to /SysDef/ are out of scope for this release.

For *Trackside Asset*, only SCI-P and TTD sections are considered.

[1] Only underlined text is new compared to previous releases

(Degraded) operational scenarios are not defined/analysed/covered (e.g. odometry issues, reset of axle counters, etc…)

Override is out of scope

Only the ETCS modes SB, FS, OS are covered inside the AoC.

Transitions (from/to adjacent interlockings, RBC, and MBS) are out of scope.

2.1 GENERAL LIMITATIONS

This chapter contains general limitations that are valid for all releases of the System Specification.

- Disclaimer: this specification is not yet part of a complete safety analysis.
- As the System Specification also contains the functionality of an RBC, the MBS shall be able to perform all the functions of the RBC Basic Interoperability Constituent (IC). Instead of repeating the /ETCS/, this document focuses on the essential functions of the MBS rather than specifying each function in detail of the RBC functionality.
- This System Specification does not explicitly specify the rules to provide national values, position report parameters and MA request parameters to the OBU. This depends on e.g. the operational rules and therefore is assumed to be application specific.
- This System Specification focus on functional requirements.
- The swinging overlaps are currently not supported (see REQ-SC_DPS_RB).
- The System Version 2.1 of /ETCS/ is only supported by the MBS.
    - Justification: This System Specification is used by the demonstrators using OBUs. But there are no OBUs available yet supporting a newer System Version than 2.1. In later editions of the System Specification newer System Versions will be supported.
- This System Specification does not explicitly specify how the cryptographic artefacts (e.g. KMACS) for the communication between MBS and the trains are made known to the MBS.

Justification: According to chapter 2 this interface is out of scope of this System Specification.

3 APPROACH AND METHODOLOGY

The Moving Block System specification is developed according to the following inputs sources:

- Moving Block System Definition (ref. /SysDef/), which
  - defines the System capabilities to be performed.
  - defines the external actors and the interfaces (System Boundaries).
- The EULYNX Standard (ref. /EULYNX/)

  It is used for the interface with the *Trackside Asset* (I_TACS interface, see chapter 7.1)
- The CCS TSI (ref. /CCSTSI/),
  - for the ETCS concepts and functionality
  - for the interface with OBU (I_OBU interface, see chapter 7.3)
  - for the interface with adjacent system (I_AS interface, see chapter in a later release)
  - for the interface with Security Service (I_SEC interface, see chapter in a later release)
- RCA (ref. /RCA/)
- Shift2Rail Moving Block (ref. /S2R/)
- System Pillar – Global system architecture – input expected for a further release
- System Pillar – Operational scenario – input expected for a further release
- System Pillar – OpCon Operational Vision (ref. /OpCon/)
- System Pillar TCCS SD1 Data Model (ref. /SD1DM/) for the *Domain objects* description
- Requirement writing (ref. /SempR2/ and /SempR3/)
- Alignment with the Demonstrator Work Packages FP2-WP44 and FP2-WP45
- Alignment with the Digital Register Work Package FP2-WP27
- Alignment with the Plan Execution Work Package FP1-WP17
- Approved list and description of operational scenarios which have to be covered by the System Specification.
  - Note: As long as there are no operational scenarios available from System Pillar Operational Design Domain, the work bases on the operational scenarios to be covered by the Moving Block Demonstrator (WP44).

The goal of the System Specification is the derivation of the System Requirements from the System Capabilities.

The approach to derive the System Requirements for the MBS is as follows:

Step	Description	Chapter
1	The main concepts of /RCA/ and /S2R/ are evaluated and consolidated. Afterwards the consolidated concepts are described in detail in separate concept papers to be able to apply	none

	it later for the specification of the System Requirements. A justification is provided for each of the consolidated concepts.	
2	Then the System Capabilities (as listed in the /SysDef/) related to the operational scenarios are detailed. Afterwards this detailing is used to derive sequence diagrams depicting the interactions of the MBS with neighbouring systems connected to it. The sequence diagrams are additionally utilised to derive the necessary System Functions. The same System Function may be used by several capabilities or scenarios.	Chapter 5
3	Subsequently the derived System Functions are described and the specific requirements for them are listed considering the consolidated concepts (in step 1), if applicable.	Chapter 6
4	Based on the scenarios, the interface needs (e.g., messages, etc.) are described considering existing standards and the concepts, if applicable.	Chapter 7

4 MBS OVERVIEW

An overview of the environment and boundaries of the Moving Block System (MBS) is shown in the following figure with the mentioned technological systems, environment, humans and other railway duty holders.

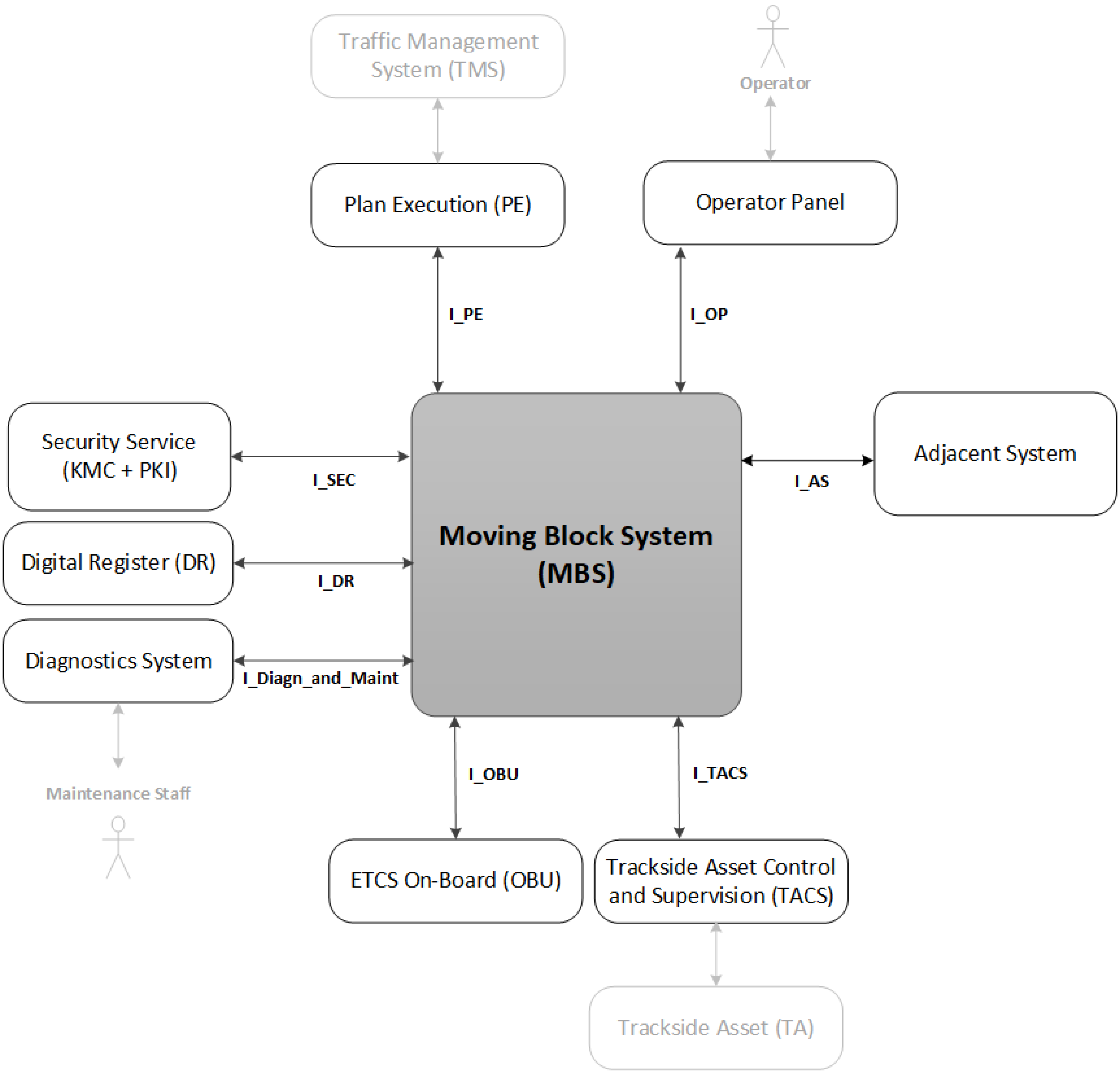


Figure 1 – System Boundaries

Note: The interface to the Operator Panel, amongst others, is not standardised yet and has to be defined. The Figure 1 considers two options. As this design decision is not clear yet, this is highlighted in red.

For more information about the system boundaries, please refer to the System Definition (ref. /SysDef/) chapter 3.

5 SYSTEM CAPABILITIES SPECIFICATION

This chapter further details the system capabilities defined in /SysDef/.

The following table provides a mapping from the system capabilities listed in /SysDef/ to the system capabilities detailed in this System Specification.

System Capability as listed in /SysDef/	Chapter(s) in System Specification
MBS manages communication sessions with *Trackside Assets* (TA) via specified interfaces within its *Area of Control* (AoC).	5.6 SysC: Start communication with one TACS
MBS manages communication sessions with trains via specified interfaces within its AoC and adjacent areas where trains are supposed to establish or terminate a communication session.	5.7 SysC: Respond to initiation of communication session by OBU 5.14 SysC: Terminate Train Mission
MBS controls all TAs within its AoC.	5.8 SysC: Control *Switchable Trackside Assets*
MBS manages the current trackside state and determines the state of the track from information given during runtime by trains and TAs within its AoC.	5.12 SysC: Start of Train 5.10 SysC: Update MBS *Operational State* 5.14 SysC: Terminate Train Mission
MBS manages all track path allocations for all trains and vehicles within its AoC. This contains an adequate and risk-based protection of requested pieces of track for an intentional train movement.	5.13 SysC: Provide MA to Train
MBS issues authorisations for train movements based on requested and accepted track path allocations.	5.13 SysC: Provide MA to Train
MBS supervises trains and TAs to prevent railway accidents. This includes especially any collision, derailment or over-speeding.	Out of scope for current releases
MBS stores an up-to-date, reliable and consistent current *Operational State* and provides this Operational State to systems connected to MBS.	5.10 SysC: Update MBS *Operational State* 5.11 SysC: Report *MBS Operational State*
MBS manages *Domain Data* changes (e.g., by introducing new parts and/or changes of the track)	5.2 SysC: Preload Topology Data 5.3 SysC: Approve Topology Data activation 5.4 SysC: Activate Topology Data

MBS handles a safe transition of train movement from and to adjacent systems.	Out of scope for current releases

Different scenarios outlining the MBS behaviour are defined for each capability.

Please refer to “Annex 2: Template” for explanation of the following capability tables and sequence diagrams.

5.1 SysC: Start and Maintain MBS

5.1.1 Communication patterns

MBS has communication sessions to its actors according to the following list. For every actor it is described why there is the initiator/responder role:

(MBS as session initiator)

- *DR*: *DR* is a service which provides topology data to its clients. It therefore acts in a server role which means that clients (like *MBS*) establish the communication to the server.
- *TACS*: Defined by EULYNX, the interlocking (here: *MBS*) is responsible to initiate the communication.

(MBS as session initiation responder)

- *PE*: *MBS* is a service to *PE* which serves requests to set *Switchable Trackside Asset*s and grant *Movement Permission*s. *MBS* therefore acts in a server role which means that *PE* establishes the communication to the server (*MBS*).
- *OBU*: It initiates the communication as *MBS* won’t know all trains in its area until they connect (/ETCS/ - SUBSET-026 §3.5.3.4 of /ETCS/).

MBS also supervises the communication so it can react to a loss of communication.

If MBS is the session initiator, it means whenever a supervision function of *MBS* detects that there is no communication, it establishes a communication (which might be the very first establishment at start of *MBS* or a re-establishment after a communication loss):

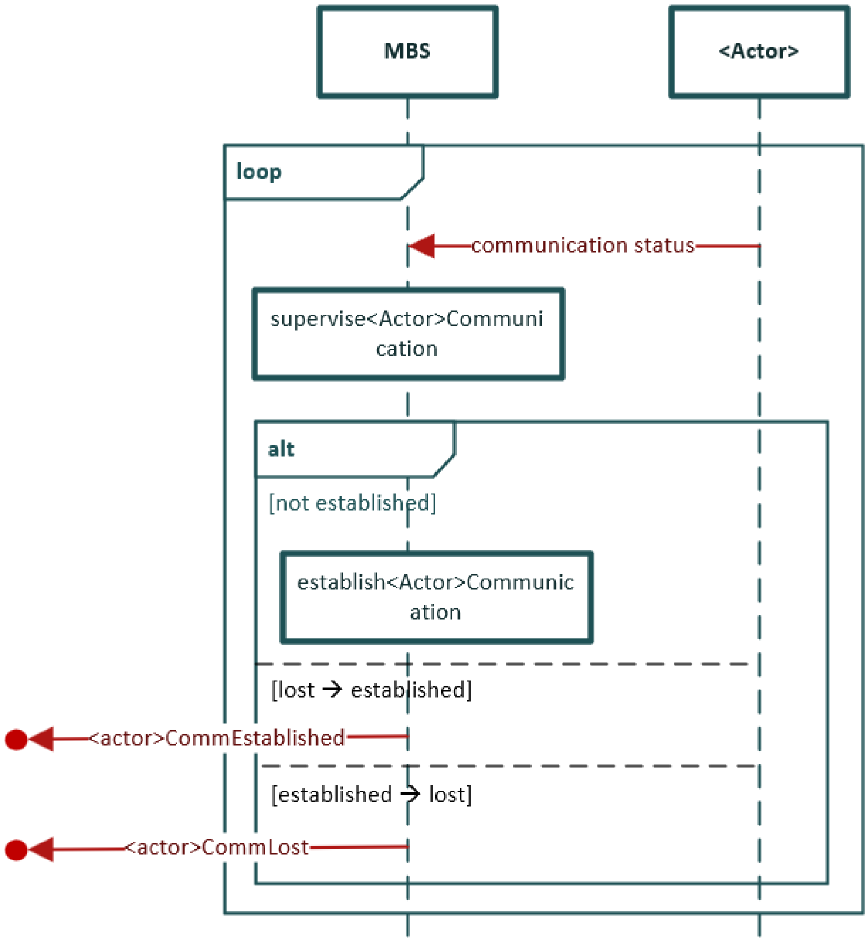


Figure 2 – Scenario pattern: Initiate communication

<Actor> can be DR or TACS.

If *MBS* is the session responder, it needs not to care for re-establishment (but the actor):

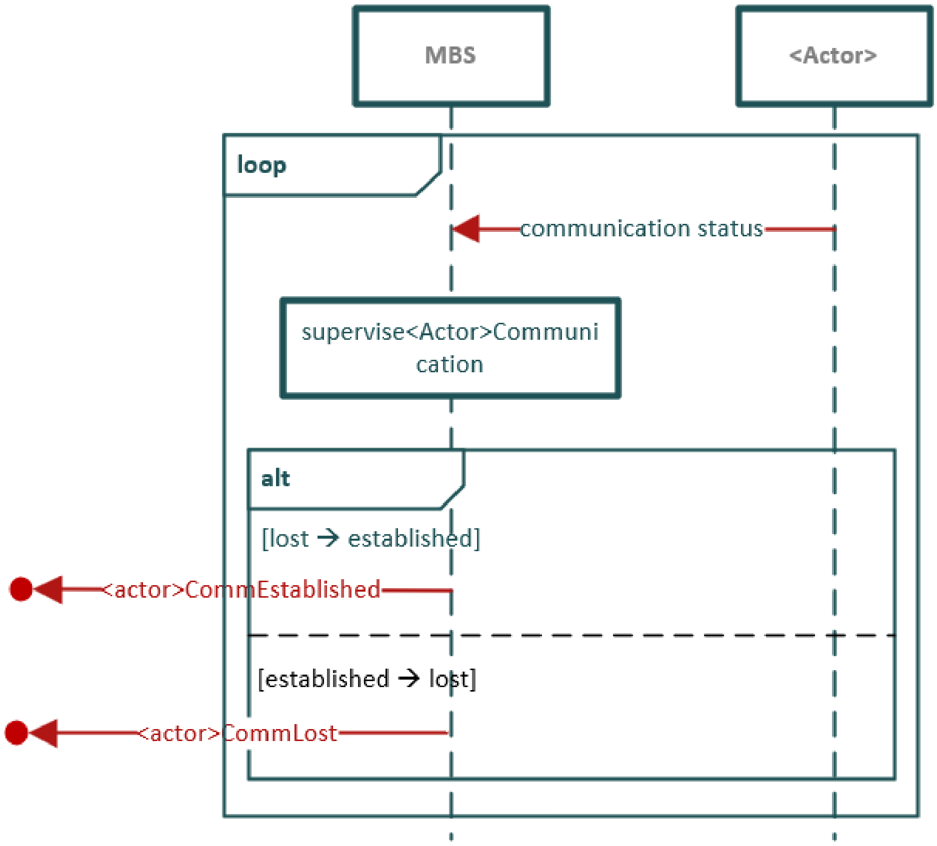


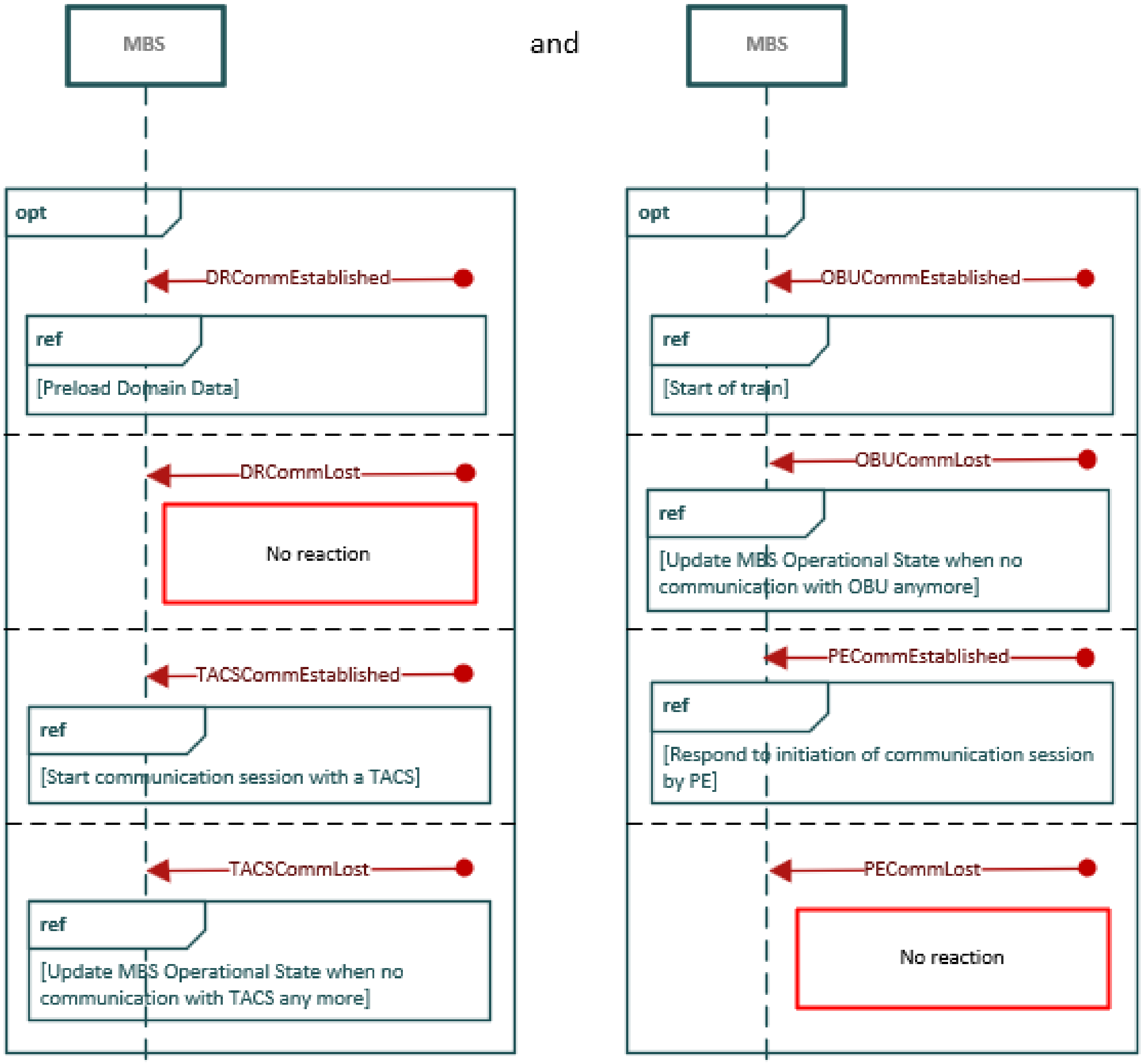
Figure 3 – Scenario pattern: Respond to communication initiation

<Actor> can be PE or OBU.

The <actor>CommEstablished event can be used to trigger further scenarios like the synchronisation of TACS in case of <actor> == TACS or initialisation of a related state.

The <actor>CommLost event can be used to trigger further scenarios like setting (a) related *Domain Object*(s) to the safe state.

With this, *MBS* can react independently on the raised internal events:



5.1.2 Capability

The named communication pattern is applied to *MBS* in order to supervise communication to actors ((re-)establish/maintain communication).

Table 1 – Description of SysC: Start and Maintain MBS

Description	This capability allows to start and maintain *MBS* communication to actors.
Goal	*MBS is operational*
Precondition(s)	None
Postcondition(s) (Success)	The Moving Block System has been started and is operational.
Postcondition(s) (Failure)	The Moving Block System is not operational.
Involved actor(s)	*DR*, *PE, OBU, TACS*
Trigger(s)	*MBS* is started
Main Sequence	1. *MBS* supervises the communication to actors (This is done in a continuous loop.)
Alternate Sequence	None
Failure Sequence	Only for release 2..4: 1. If loading or checking the *Topology Data* fails, the start procedure terminates.
Comments	MBS could either be started by an external event or automatically when recovering from a failure for example. The communication patterns raise events *<actor>CommEstablished* and *<actor>CommLost* for every actor <actor> (UML: *lost message*). Other capabilities can react (UML: *found message*) to these events and react accordingly (e.g. initialising a safe state).

5.1.3 Scenario: Start and Maintain MBS

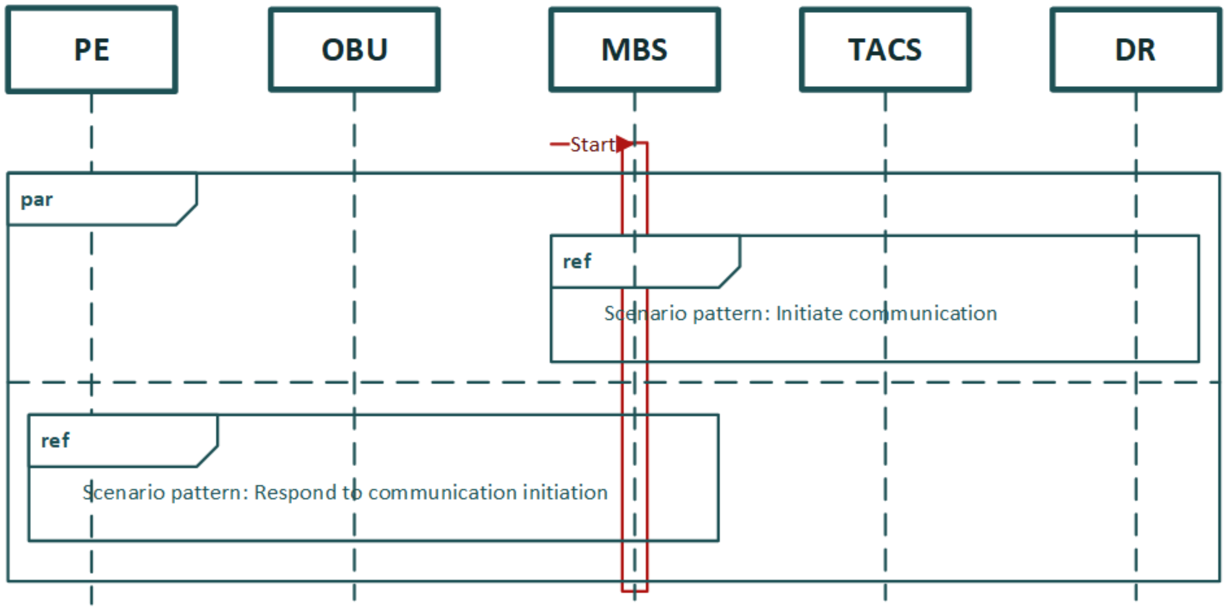


Figure 4 - Scenario: Start and Maintain MBS

5.2 SysC: Preload Topology Data

Description	This capability allows to provide *MBS* with *Topology Data* initially. This finally results into topology-related *Domain Object*s
Goal	*MBS* has loaded (initial or new version of) *Topology Data* and related *Domain Objects*
Precondition(s)	No *Topology Data* available (no *Topology Data* loaded) at startup
Postcondition(s) (Success)	Up to release 4: *MBS* has loaded, approved, and activated *Topology Data* *MBS is operational*0
	From release 5 on (more granular steps so this capability only does preloading): *MBS* has loaded *Topology Data* *MBS is operational*0
Postcondition(s) (Failure)	*MBS* state related to *Topology Data* has not changed *MBS* is not operational0
Involved actor(s)	*DR*
Trigger(s)	1. *MBS starts up* 2. (For further release) *MBS* receives the *Topology Data* from *DR*
Main Sequence	Up to release 4: 1. *MBS* establishes a communication session with *DR*. 2. *MBS* requests *Topology Data* from *DR* 3. *MBS* receives *Topology Data* and activates them
	From release 5 on: 1. *MBS* establishes a communication session with *DR*. 2. *MBS* requests *Topology Data* from *DR* 3. *MBS* receives *Topology Data* and pre-loads them. 4. *MBS* approves the activation of *Topology Data* 5. *MBS* activates *Topology Data*
Alternate Sequence	From release 5 on: At any point in time, DR can send *Topology Data* to *MBS* (continues then from 3. on)
Failure Sequence	4. *MBS* rejects the approval when there are e.g. conflicting *Movement Permission*s (for further release)
Comments	Before release 5, there are the following restrictions • The scope of *Topology Data* is the full *Area of Control* (so no partial update) • *Topology Data* are loaded only once at startup and remain unchanged (so no update during run-time) • It is assumed that neither connecting to *DR*, nor loading the *Topology Data* from there fails (exclusion of unhappy paths) The scenario will thus widen in a later release: data are not only loaded and immediately activated, but pre-loaded, approved, and activated. In order to save work already knowing the future state, the function to load *Topology Data* is already named ‘preload’ and not only ‘load’. The term ‘preloaded’ can be read as ‘loaded’.

5.2.1 Scenario: Preload *Topology Data*

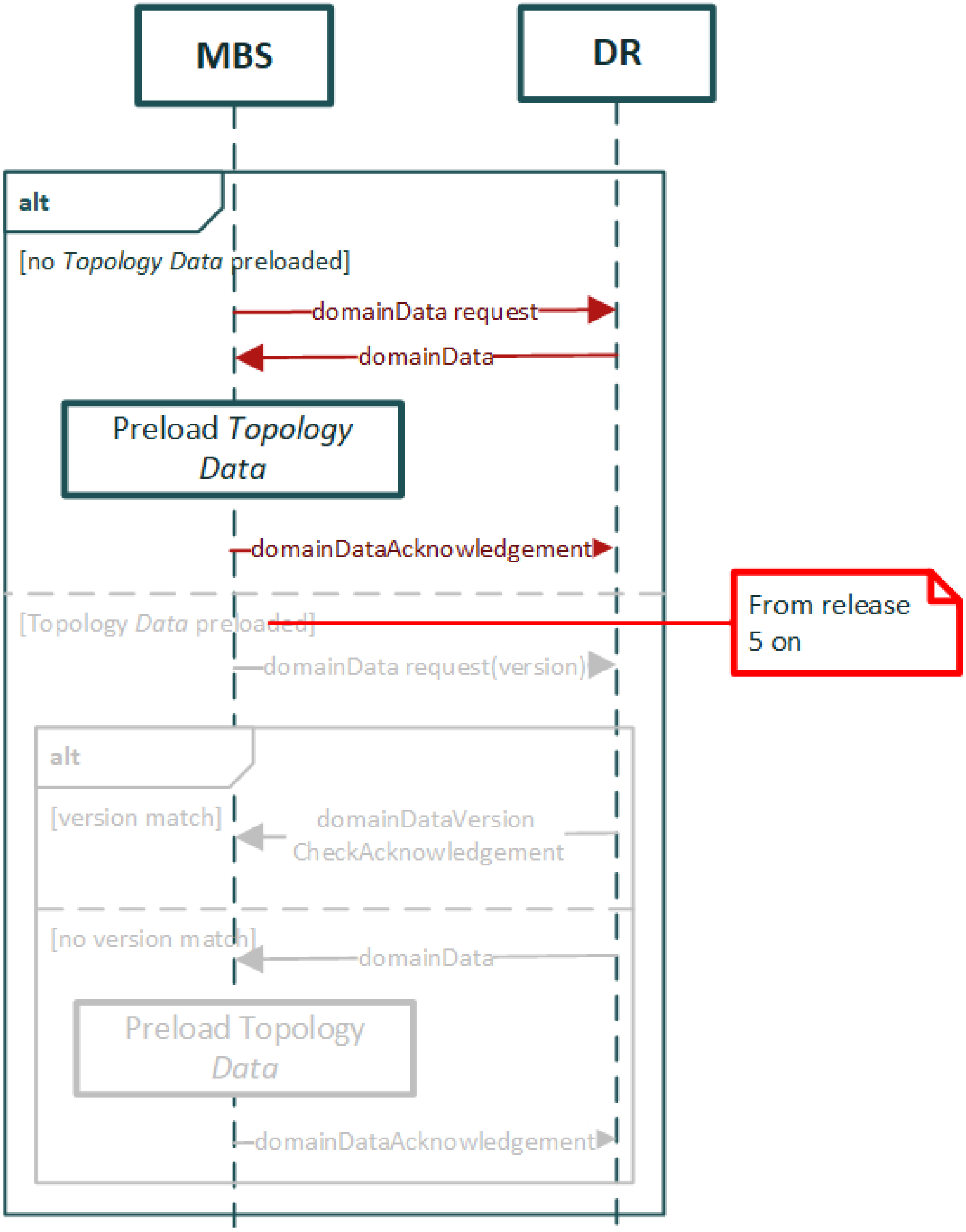


Figure 5: Scenario to pre-load *Topolgy Data*

5.3 SysC: Approve Topology Data activation

Note: This capability checks if data in the to-be-updated area can be approved from *MBS* point of view (e.g. no *Movement Permission*s are in conflict) and will be part of a further release. Until then, there is no such check and data are regarded as approved already within function 'Preload Topology Data'.

5.4 SysC: Activate Topology Data

Note: This capability finally activates the data and will be part of a further release. Until then, there is no such procedure and data are regarded as activated already within function 'Preload Topology Data'.

5.5 SysC: Respond to initiation of communication session by PE

Table 2 – Description of SysC: Respond to initiation of communication session by PE

Description	This capability responds to the communication session establishment by *PE*. This communication session is crucial to e.g., be able to receive requests for Movement Permissions for trains. After the communication session is established, the MBS distributes its *MBS Operational State* (e.g., state of *Trackside Assets*) to *PE*.
Goal	*MBS* has distributed its *MBS Operational State* to *PE*.
Precondition(s)	*MBS is operational*
Postcondition(s) (Success)	The *MBS Operational State* is synchronised with *PE*
Postcondition(s) (Failure)	No communication session to *PE*
Involved actor(s)	*PE*
Trigger(s)	Event *PECommEstablished*
Main Sequence	1. *MBS* distributes its *MBS Operational State* to *PE*.
Alternate Sequence	None
Failure Sequence	1. *MBS* cannot distribute the *MBS Operational State* to *PE* *MBS* closes the communication session
Comments	This capability may be triggered after start of *MBS* or when the communication session to the *PE* needs to be re-established for any reason. When – in failure case – the communication session is closed, the capability 'Start and Maintain MBS' will re-establish the session and this triggers this capability again.

5.5.1 Scenario: Respond to initiation of communication session by PE

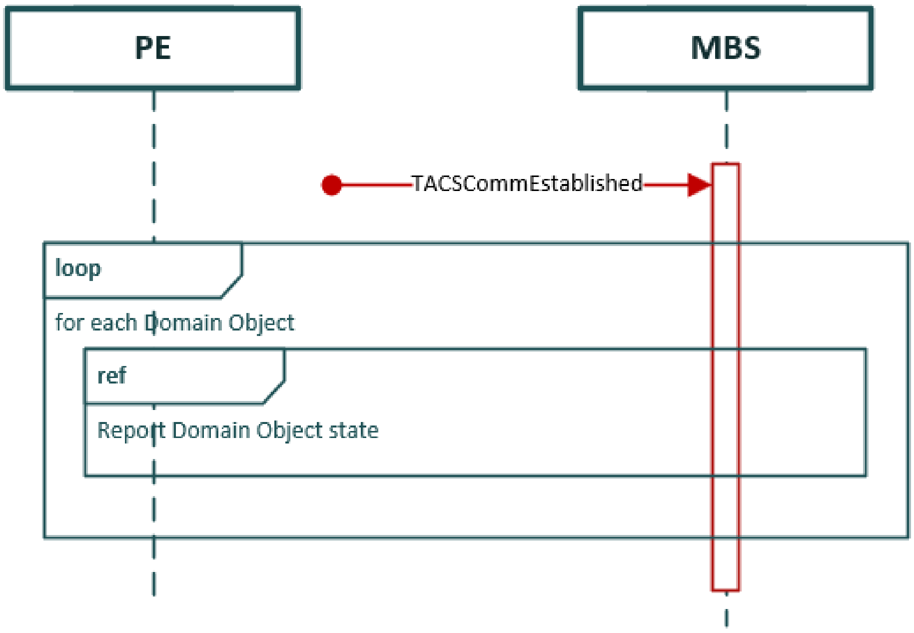


Figure 6 - Scenario: Respond to Initiation of communication session by PE

This system capability is not detailed further since there is no defined interface specification (e.g. SCI-CMD) yet.

Currently it is assumed that the initiation of the communication session is triggered by *PE* whereupon *MBS* shall be able to receive commands from *PE* and provide information (e.g. *MBS Operational State*) to *PE*.

5.6 SysC: Start communication with one TACS

Table 3 – Description of SysC: Start communication with one TACS

Description	This capability responds to the communication session establishment between the *MBS* and one *TACS*; the capability is applied <u>for each TACS</u>. MBS performs the synchronisation with TACS, updates the related *Domain* Objects and distributes their state to *PE* (by capability 'Report *MBS Operational State*')
Goal	*Domain Object*s of *MBS* are synchronised with *TACS* and subsequently *MBS* has distributed the corresponding *Domain Object* state to *PE*.
Precondition(s)	*MBS is operational*)
Postcondition(s) (Success)	*MBS* has distributed the corresponding *Domain Object* state to *PE*.
Postcondition(s) (Failure)	No communication session to *TACS*
Involved actor(s)	*PE*, *TACS*
Trigger(s)	Event *TACSCommEstablished(TACSId)*
Main Sequence	1. *MBS* synchronises with *TACS*.

	2. *MBS* updates and distributes the corresponding *Domain Objects* state to *PE* (according to the capability 'Update *MBS Operational State*')
Alternate Sequence	None
Failure Sequence	1. The synchronisation with *TACS* failed *MBS* closes the communication session
Comments	This capability may be triggered after start of *MBS* or when the communication session to a *TACS* was re-established for any reason. When – in failure case – the communication session is closed, the capability 'Start and Maintain MBS' will re-establish the session and trigger this capability again.

5.6.1 Scenario: Start communication session with a TACS

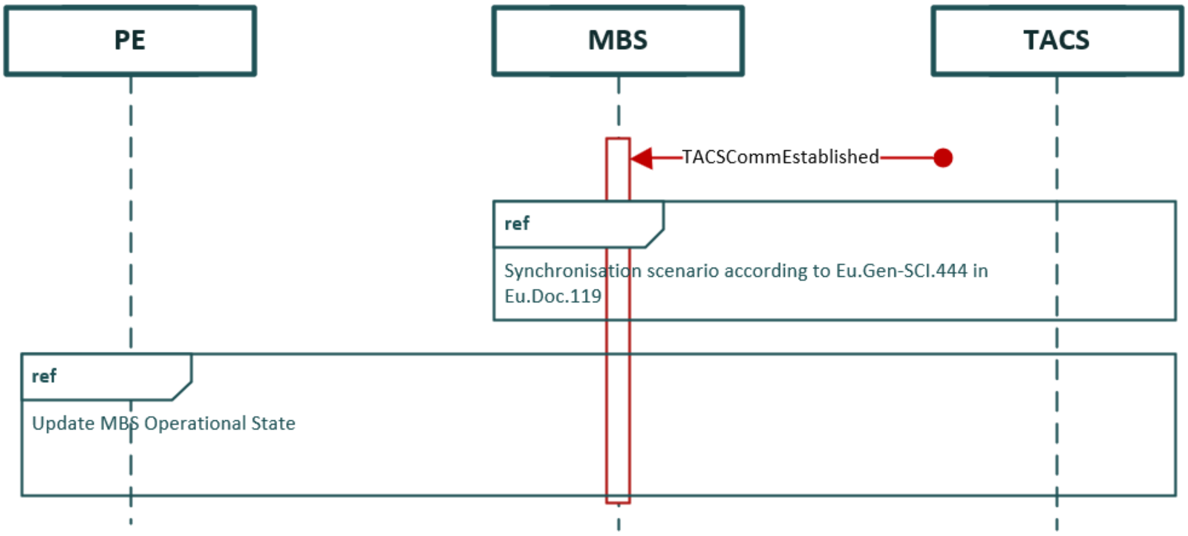


Figure 7 - Scenario: Start communication session with a TACS

The capability "Establish communication session with a TACS" is responsible for establishing a communication session with a TACS. Generally, when MBS detects that there is no communication session with the TACS, the MBS shall establish a communication session with a TACS. This capability is not further detailed in this chapter. Instead the details are described in chapter 7.1 of this document.

5.7 SysC: Respond to initiation of communication session by OBU

Description	This capability manages the establishment of the communication session between the MBS and an OBU considering the requirements of • chapter 3.5.3 (Establishing a communication session) of /ETCS/ - SUBSET-026. • /ETCS/ - SUBSET-037.
Goal	A communication session with an OBU is established.

Precondition(s)	*MBS is operational*
Postcondition(s) (Success)	A communication session with an OBU was established.
Postcondition(s) (Failure)	A communication session with an OBU could not be established.
Involved actor(s)	OBU, PE
Trigger(s)	An OBU requests to set-up a safe radio connection with the MBS.
Main Sequence	1. MBS sets-up a safe radio connection and communication session according to /ETCS/ considering using System Version 2.1. MBS creates a *Train Object* for this OBU and subsequently informs PE about this through the capability 'Update *MBS Operational State*'.
Alternate Sequence	None.
Failure Sequence	1. If a condition to establish a safe connection or communication session is not fulfilled, then MBS ends the procedure to set-up a safe radio connection and communication session by terminating the safe connection, if any.
Comments	The failure sequence may be triggered e.g. in the following case : • There is no key (KMAC) available within MBS for this OBU.

5.7.1 Scenario: Start communication session with an OBU

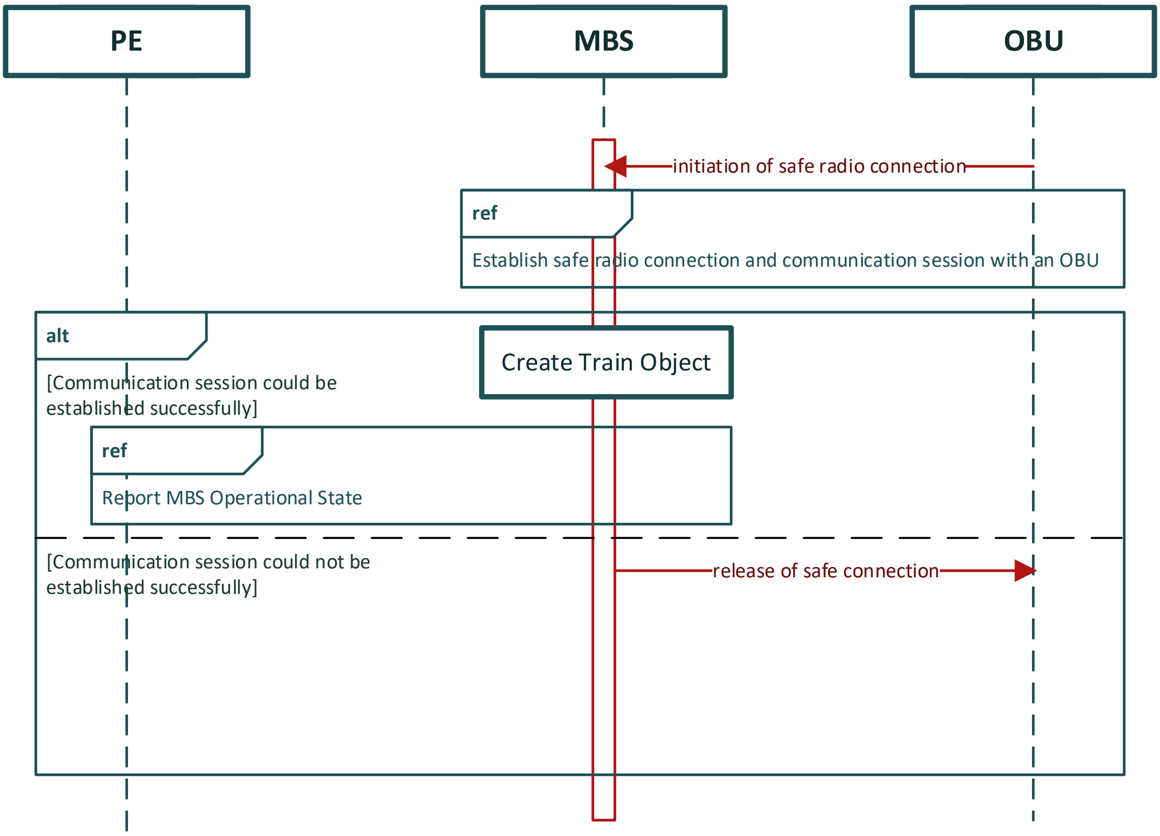


Figure 8 - Scenario: Start communication session with an OBU

The capability "Establish safe radio connection and communication session with an OBU" referenced in the scenario is responsible for managing the safe radio connection and communication session establishment between MBS and an OBU considering the requirements of:

- Chapter 3.5.3 (Establishing a communication session) of /ETCS/ - SUBSET-026 and
- /ETCS/ - SUBSET-037.

This capability is not detailed further on since the requirements are already provided in the /ETCS/ as stated above.

5.8 SysC: Control *Switchable Trackside Assets*

Table 4 – Description of SysC: Control *Switchable Trackside Assets*

Description	This capability allows *PE* to change the state of a *Switchable Trackside Asset* by sending a corresponding TA State Request to *MBS*. *MBS* has to verify if the request is valid. If it is valid, *MBS* carries it out by sending the corresponding command to the *TACS* related to the *Switchable Trackside Asset*.
Goal	Due to a request from *PE*, a *Switchable Trackside Asset* is commanded to change its state by sending a command to its *TACS*.

Preconditions	*MBS is operational* 5.1.2
Postcondition (Success)	Granting of request is indicated to *PE*. Command for changing its state is sent to *TACS*.
Postcondition (Failure)	Rejecting of a valid request from *PE*. Command for changing its state is not sent to *TACS*.
Involved Actors	*PE*, *TACS*
Trigger	Request from *PE* to change the position of a *Switchable Trackside Asset* via its *TACS*.
Main Sequence	A valid request is granted and carried out by *MBS* (see: Scenario: Control *Switchable Trackside Assets*) and MBS informs PE about granting this request
Alternate Sequence	
Failure Sequence	An invalid request is rejected by *MBS* (see: Scenario: Control *Switchable Trackside Assets*) and MBS informs PE about rejecting this request.
Comments	None

5.8.1 Scenario: Control *Switchable Trackside Assets*

The figure below contains the main sequence and the failure sequence of the SysC Control *Switchable Trackside Asset*.

When the *MBS* receives a TA State Request, it performs the safety checks (Function: Authorise TA State Request) for the request.

If the safety checks are successful, *MBS* responds to *PE* the granting of the request and translates the request to a *TACS* command (Function: Translate TA State Request to TACS Command). The *TACS* command is then sent to the related *TACS* (Function: Send TACS Command).

If the safety checks fail, *MBS* responds to *PE* system the rejecting of the request and performs no further actions for the request.

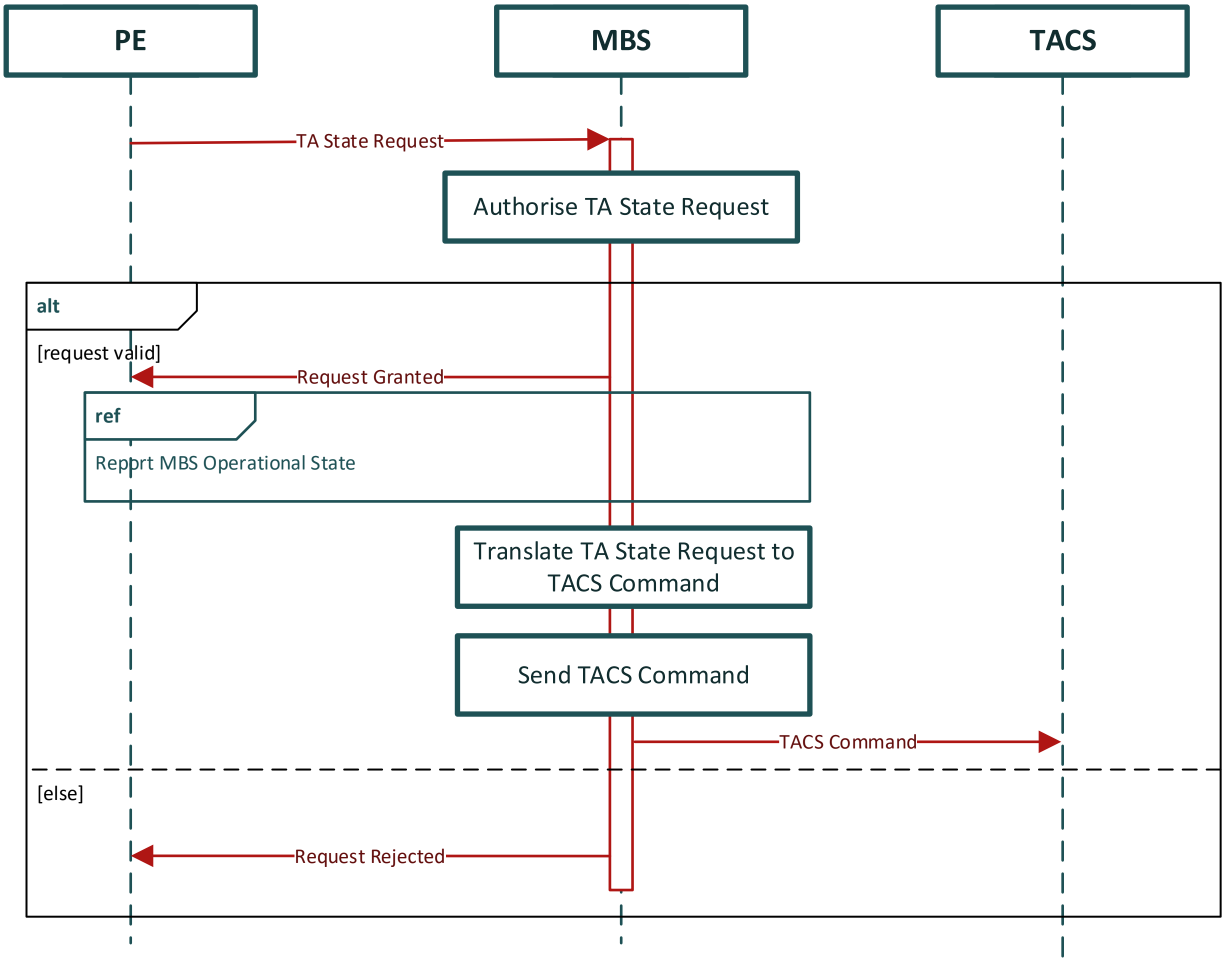


Figure 9 - Scenario: Control *Switchable Trackside Assets*

Note that the response from the *Switchable Trackside Asset* is not shown here, it is asynchronously sent (refer to the next section).

5.9 SysC: Shutdown MBS

Out of scope for this release

5.10 SysC: Update MBS *Operational State*

Table 5 – Description of SysC: Update MBS *Operational State*

Description	This capability updates the *MBS Operational State*.
Goal	Update the state of *MBS Operational State*
Precondition	*MBS is operational)*
Postcondition (Success)	MBS has updated its *MBS Operational State*
Postcondition (Failure)	None (no failure)
Involved Actors	• TACS • OBU • PE
Trigger	• Any change of *MBS Operational State* is detected (inexhaustive list):

	• MBS receives a state update report from the TACS • MBS detects that there is no communication with TACS anymore • MBS receives a position report from OBU • MBS receives validated train data from OBU • The communication between MBS and an OBU is established • MBS detects that there is no communication with OBU anymore
Main Sequence	Scenario 1: Update *MBS Operational State* when TA state report is received Scenario 2: Update *MBS Operational State* when a train position report or validated train data are received
Alternate Sequence	Scenario 3: Update *MBS Operational State* when no communication with TACS anymore Scenario 4: Update *MBS Operational State* when no communication with OBU anymore
Failure Sequence	None
Comments	None

5.10.1 Scenario 1: Update *MBS Operational state* when TA state report is received

This scenario covers the nominal scenario (all communications are established), when a TA state report is received from a TACS.

Train Location or Unresolved Trackbound Object are updated when a TTD section status changes.

Risk Path, part of the Movement Permission, may be updated when a Point status changes.

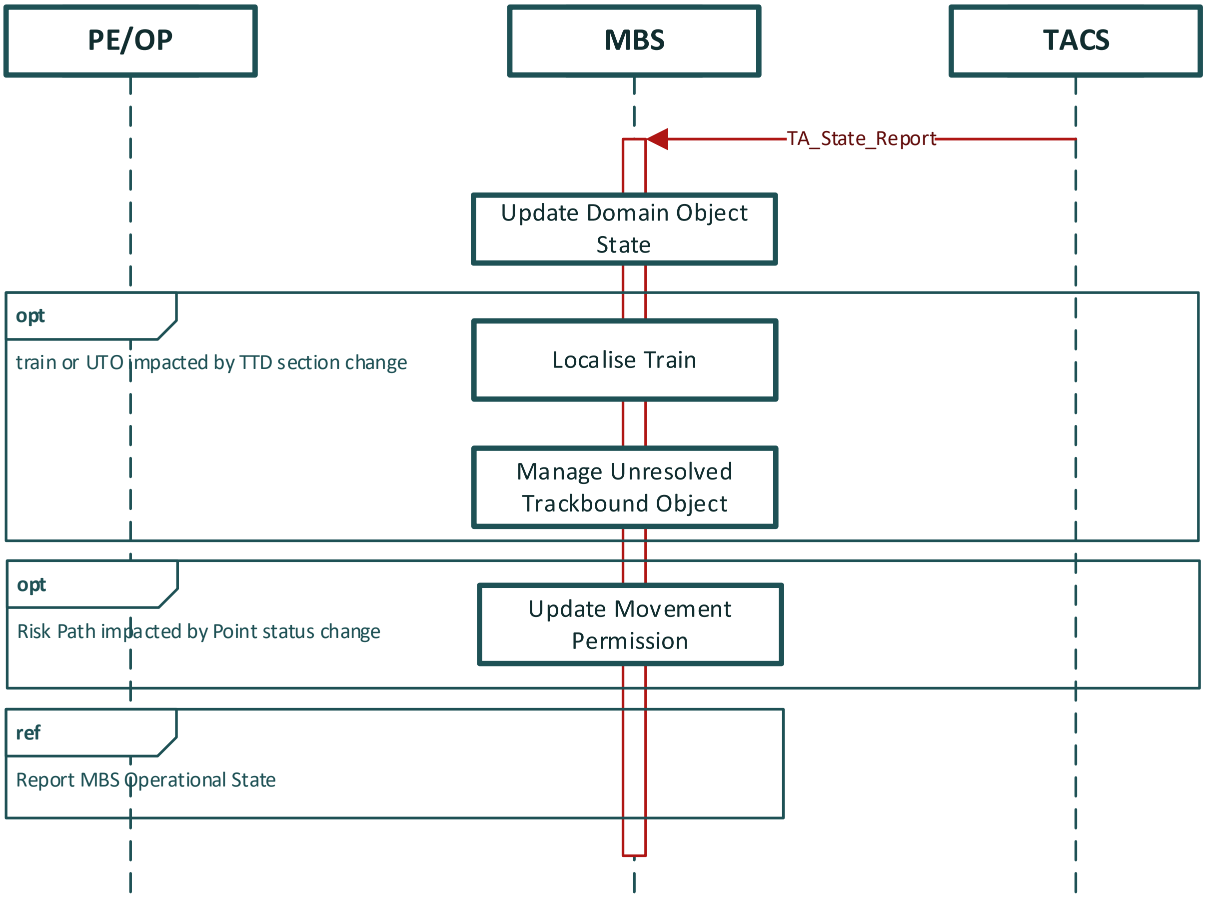


Figure 10 - Scenario 1: Update *MBS Operational State* when TA state report is received

5.10.2 Scenario 2: Update *MBS Operational State* when a train position report or validated train data are received

This scenario covers the nominal scenario (all communications are established), when a position report or validated train data are received from the train.

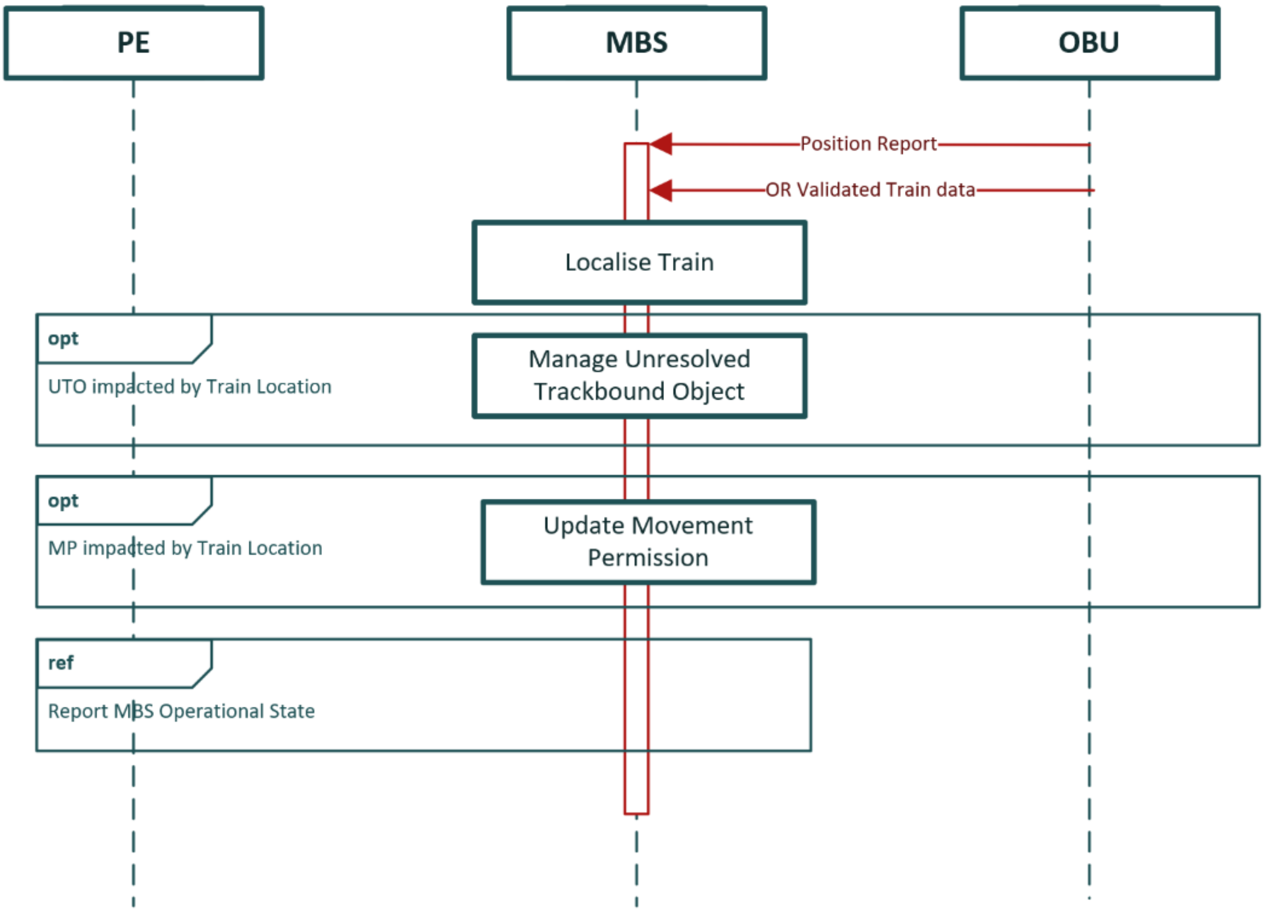


Figure 11 - Scenario 2: Update *MBS Operational State* when train position report or validated train data are received

5.10.3 Scenario 3: Update *MBS Operational State* when no communication with TACS anymore

This scenario covers the status to be reported when the communication with the TACS is lost.

When the MBS detects that the communication with a TACS is lost, the MBS sets and reports the safe value of the related *Domain Object* to the PE, *Train Location* and UTO are also updated if impacted by a TTD section change.

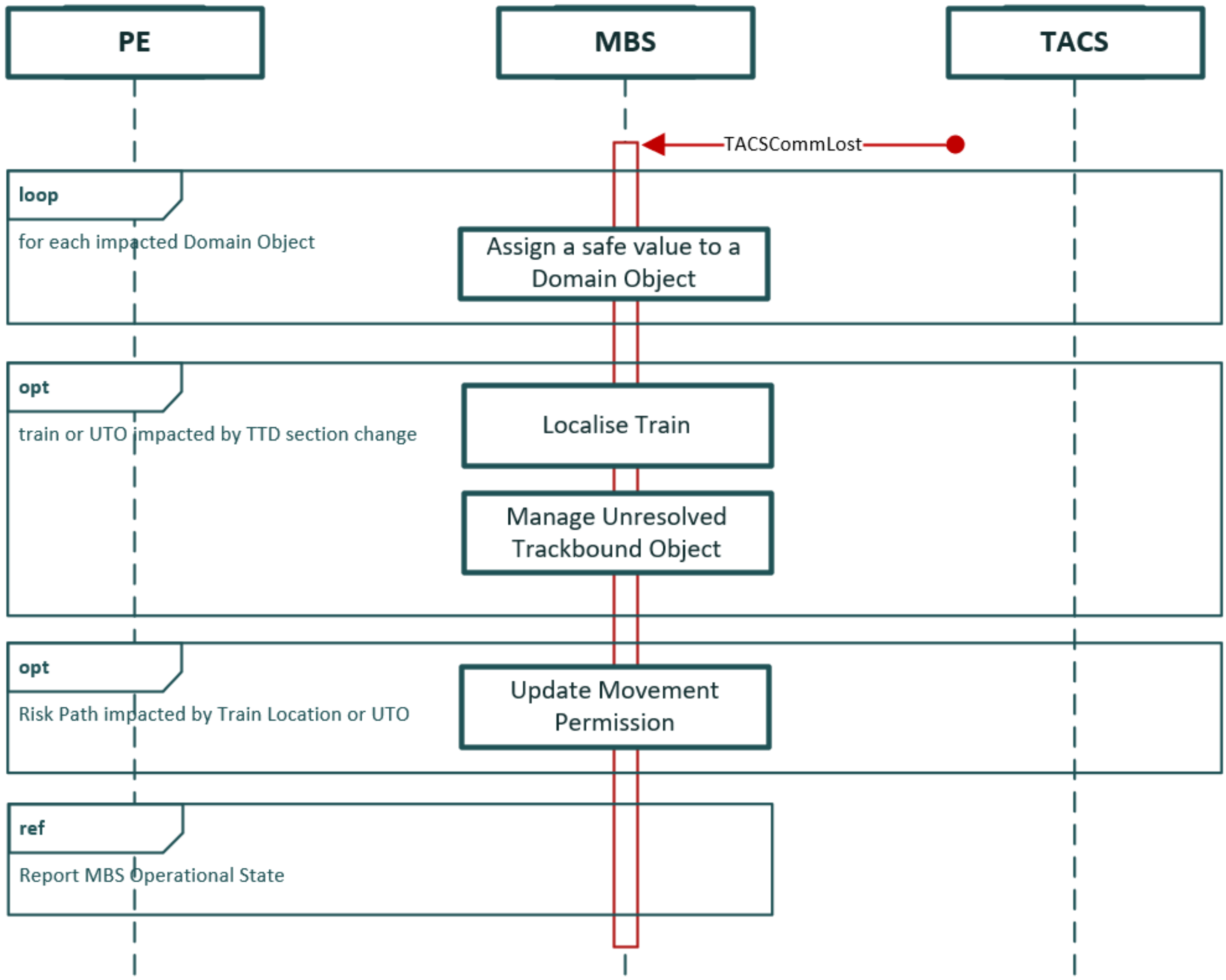


Figure 12 - Scenario 3: Update of status when no communication with TACS anymore

5.10.4 Scenario 4: Update *MBS Operational State* when no communication with OBU anymore

This scenario covers the status to be reported when the communication with the OBU is lost.

When the MBS detects that the communication with the OBU is lost, the MBS reports this information to the PE in the Train Object.

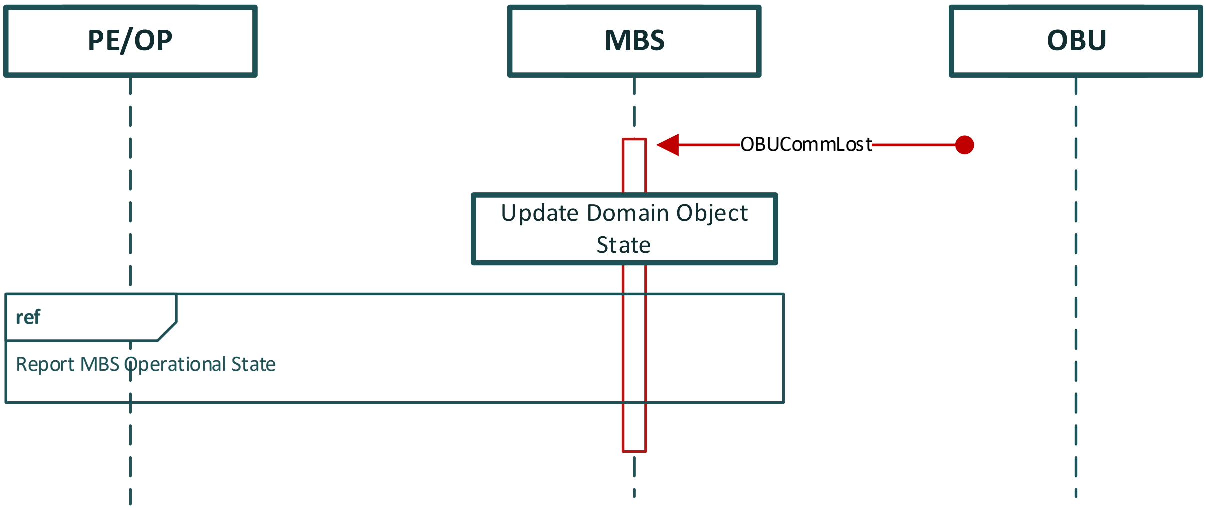


Figure 13 - Scenario 4: Update of *MBS Operational State* when no communication with OBU anymore

5.11 SysC: Report *MBS Operational State*

Table 6 – Description of SysC: Report *MBS Operational State*

Description	When triggered, this capability reports the *MBS Operational State*.
Goal	Report the state of *MBS Operational State*
Precondition	*MBS is operational*5.1.2
Postcondition (Success)	PE has received the *MBS Operational State* for the given *Domain Object* Instance
Postcondition (Failure)	None (no failure)
Involved Actors	• PE
Trigger	Triggered for a given *Domain Object* Instance by other capabilities
Main Sequence	Scenario: Report of *MBS Operational State*
Alternate Sequence	
Failure Sequence	None
Comments	None

5.11.1 Scenario: Report of *MBS Operational State* when triggerred

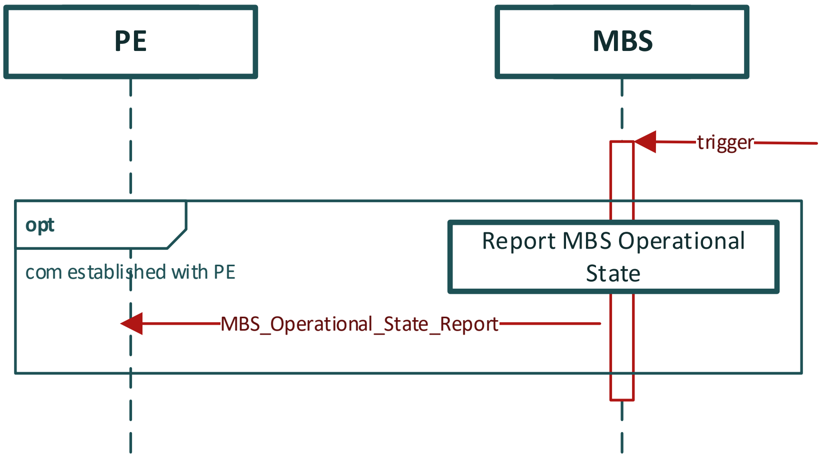


Figure 14 - Scenario: Report of *MBS Operational State* when triggered

5.12 SysC: Start of Train

Description	Start of Train
Goal	A train successfully has started up according to /ETCS/ and MBS has subsequently sent an Authorisation Requested message to PE.
Precondition(s)	*MBS is operational* 5.1.2
Postcondition(s) (Success)	MBS has sent an Authorisation Requested message to PE after receiving a first MA request during the Start of Mission procedure.
Postcondition(s) (Failure)	None
Involved actor(s)	OBU, PE
Trigger(s)	MBS receives a SoM Position Report message from an OBU.
Main Sequence	1. MBS determines that the position is valid and unambiguous. MBS updates the *Train Object*.
	2. MBS receives Train Data, Train Running Number from OBU and subsequently acknowledges the train data to the OBU. MBS updates the *Train Object*.
	3. MBS receives an MA Request from OBU. MBS provides an Authorisation Requested message to PE.
Alternate Sequence	1.a) MBS receives a SoM Position Report with invalid / unknown position. MBS updates the *Train Object* indicating that the position is invalid / unknown and sends Train Accepted to OBU. Afterwards the flow continues with step 2 of the main sequence.

	1.b) MBS receives a SoM Position Report with a valid position, but the *position is ambiguous*. MBS updates the *Train Object* indicating that the *position is ambiguous* and continues with step 2 of the main sequence.
Failure Sequence	None
Comments	Please consider that mode change to SH is currently excluded by the scope of the document and thus there is no failure sequence aborting this capability in such case. The same also applies for using the 'Override' function. Additionally, it is also not foreseen yet to revalidate the train position (using the SoM Position Report Confirmed message) since this may depend on the operational procedures which are not available yet.

5.12.1 Scenario: Start of Train

Please consider that during this scenario after each Train Position Report (packet number 0 or packet number 1), respectively after receiving the SoM Position Report, MBS updates the *Train Object* by the capability "Update *MBS Operational State*" and reports this to the PE. This handling of Train Position Reports is not explicitly illustrated in the figure to limit the sequence diagram to the Start of Train capability.

During this scenario, after the acknowledgment of Train Data, it is possible (when the OBU is equipped with a TIMS) that the MBS receives the first Train Position Report with integrity confirmed. Then especially the extent of the *Train Location* using the confirmed rear end is updated.

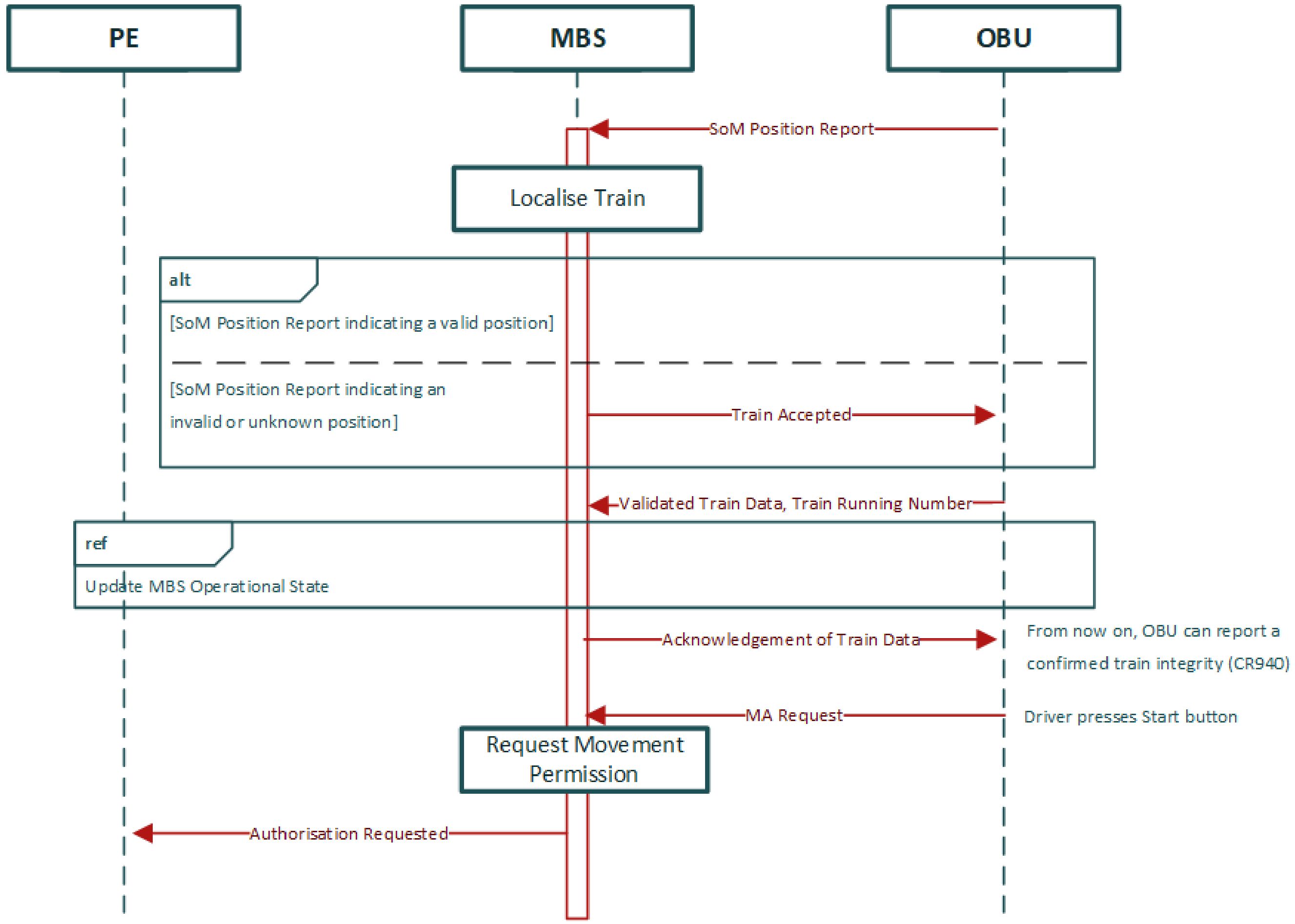


Figure 15 - Scenario 1: Start of Train

5.13 SysC: Provide MA to Train

Table 7 – Description of SysC: Provide MA to Train

Description	This capability generates a Movement Permission for a dedicated train run and issues an Authorisation for a particular OBU.
Goal	After receiving an MP request from PE, MBS checks all safety constraints, generates a Movement Permission for a dedicated train run and translates it into an Authorisation which is sent to the OBU.
Precondition	None
Postcondition (Success)	Authorisation issued by MBS to the OBU corresponding to the *Train Object*; Movement Permission reported to PE.
Postcondition (Failure)	None
Involved Actors	• OBU • PE
Trigger	• MBS receives a Movement Permission Request

Main Sequence	When all checks are successful, MBS indicates this to PE, updates the *Train Object* with the Movement Permission and issues an Authorisation to OBU based on the Movement Permission Request received from PE.
Alternate Sequence	None
Failure Sequence	When at least one check fails, MBS reports a Request Rejected to PE indicating the reason why the Movement Permission Request could not be granted.
Comments	•

5.13.1 Scenario: Provide MA to Train

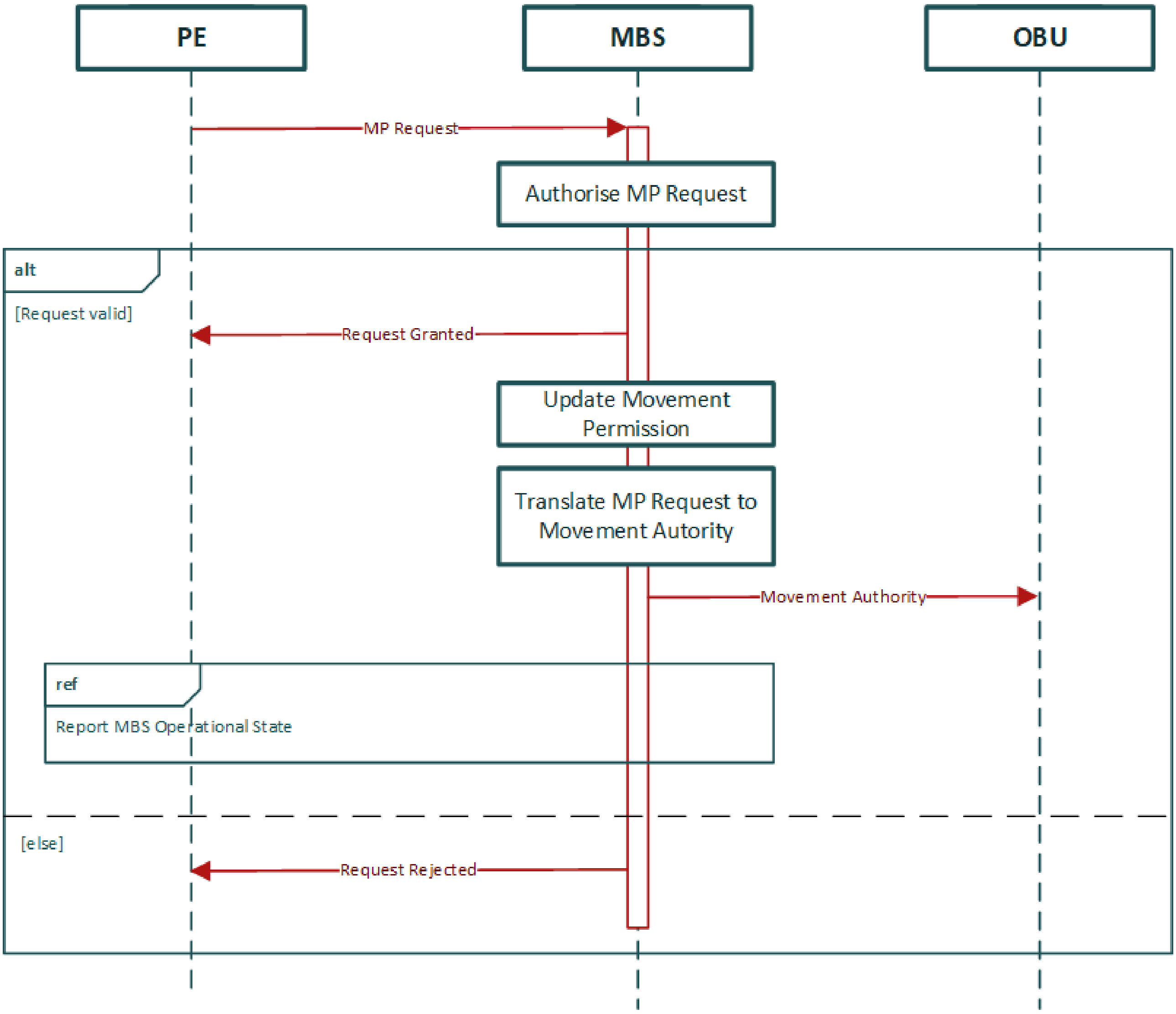


Figure 16 - Scenario : Provide MA to Train

5.14 SysC: Terminate Train Mission

Table 8 – Description of SysC: Terminate Train Mission

Description	This capability manages the termination of the mission of a train. It manages: • End of mission according to /ETCS/ - SUBSET-026 chapter 5.5 • Termination of the communication session according to /ETCS/ - SUBSET-026 chapter 3.5.5. • Loss of communication It converts the *Train Object* into an *Unresolved Trackbound Object* (needed by the MBS to manage the occupied area and a further start of mission for this train). It reports the information to the PE
Goal	Terminate the mission of a given train
Precondition	Communication between the OBU and the MBS is established
Postcondition (Success)	Communication between the OBU and the MBS is terminated. *Train Object* is converted into *Unresolved Trackbound Object*
Postcondition (Failure)	
Involved Actors	• OBU • PE
Trigger	• A message triggering the order to terminate the communication session is received from OBU (see scenario 1) • Message "termination of communication session" is received from OBU (see scenario 2) • Communication with OBU is lost for more than Session Timeout (see scenario 3)
Main Sequence	Scenario 1: Train End of Mission
Alternate Sequence	Scenario 2: Termination of communication session by OBU Scenario 3: end mission when no communication anymore with an OBU
Failure Sequence	
Comments	

5.14.1 Scenario 1: Train End of Mission

This scenario covers the nominal scenario when a message triggering the order to terminate the communication session is received from the OBU.

Following messages are considered:

- message End of Mission is sent by the onboard to the MBS when the driver closes the desk, (including a change of mode to SB).

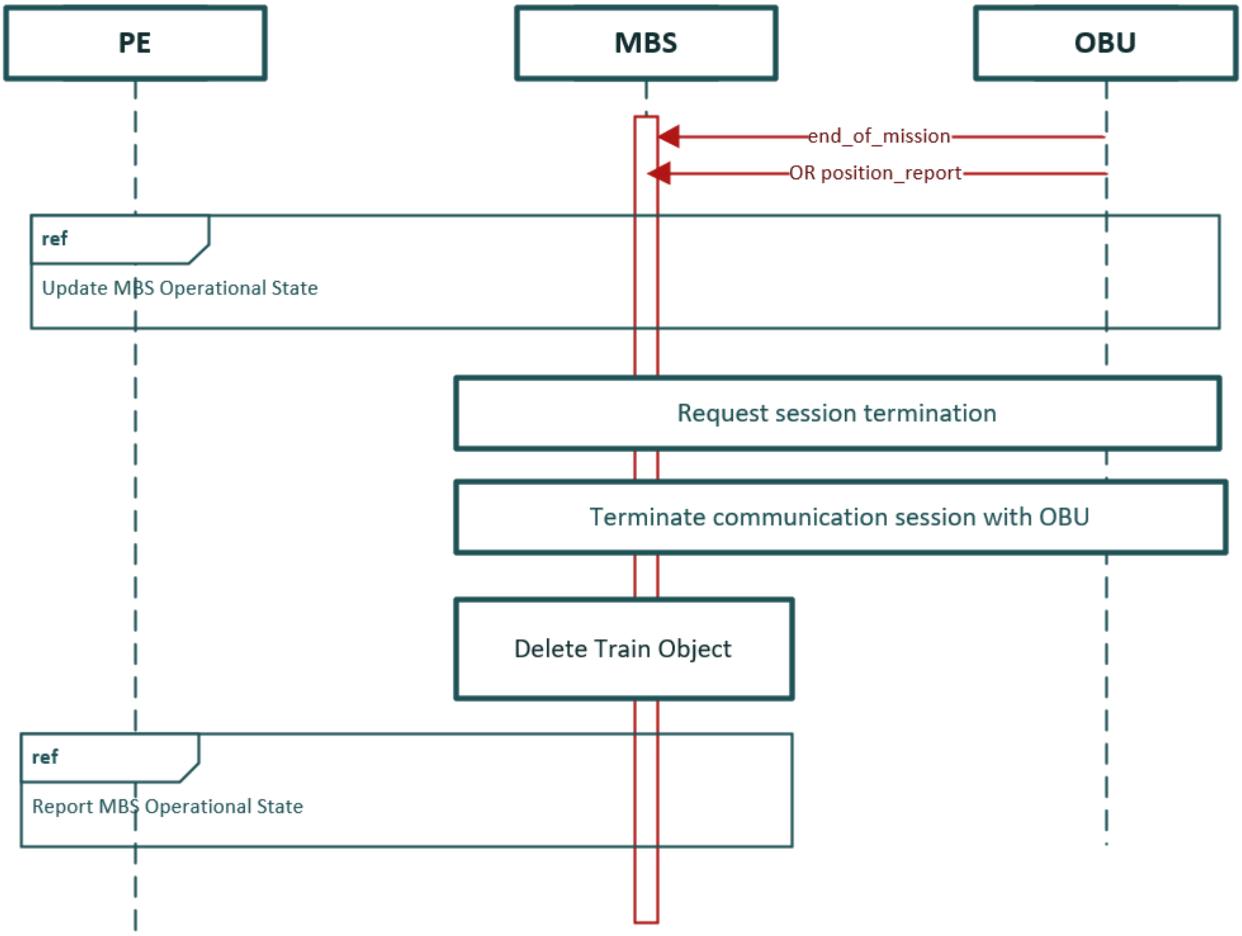


Figure 17 - Scenario 1: Train End of Mission

The functions "Request Session Termination" and "Terminate communication session with OBU" referenced in the scenarios are not further detailed in this document as the behaviour is specified in in /ETCS/ SUBSET-026 chapter 3.5.5.

5.14.2 Scenario 2: Termination of communication session by OBU

This scenario covers the case when a message "termination of communication session" is directly received from the OBU.

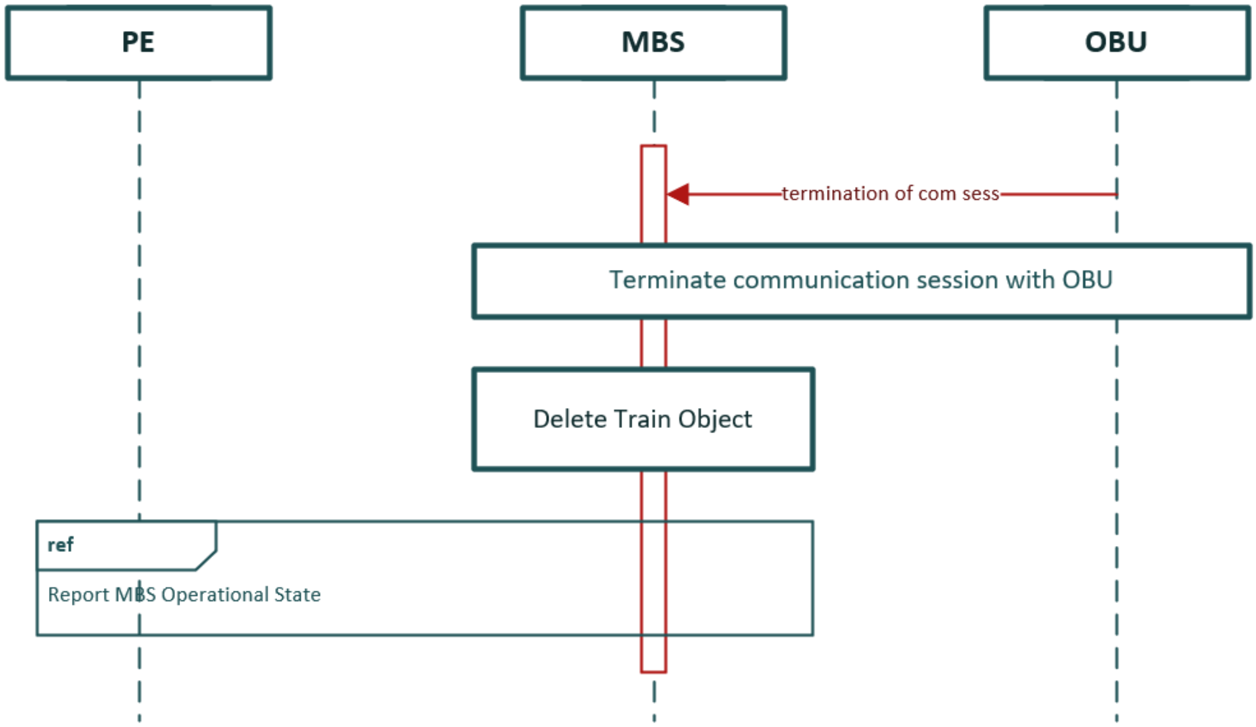


Figure 18 - Scenario 2: Termination of communication session by OBU

5.14.3 Scenario 3: end mission when no communication anymore with an OBU

This scenario covers the degraded scenario when communication with the OBU is lost for more than a configured Session Timeout.

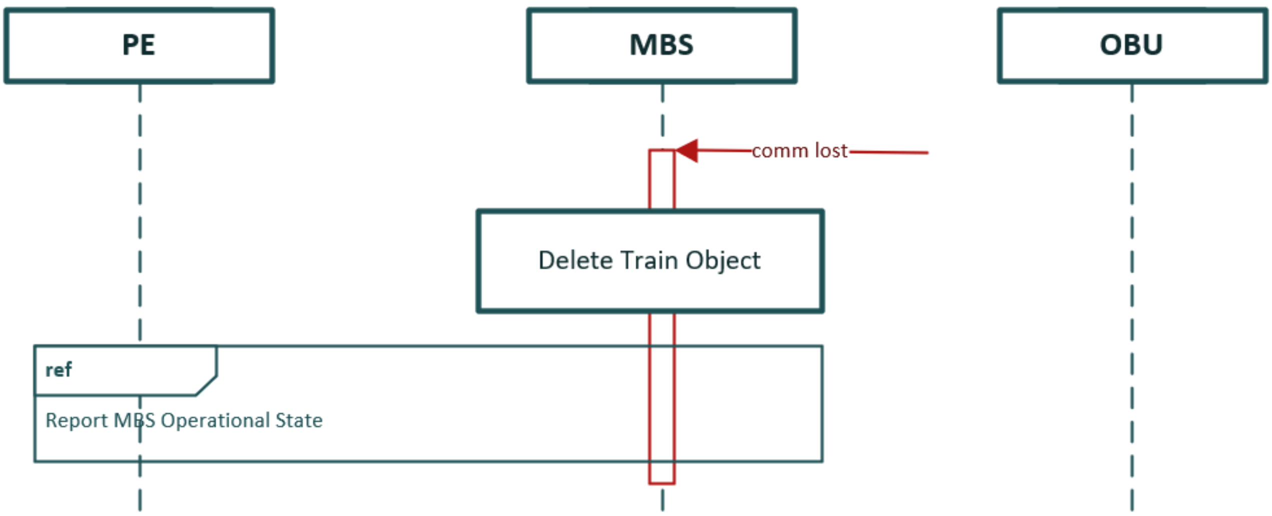


Figure 19 - Scenario 3: end mission when no communication anymore with an OBU

The functions "Request Session Termination" and "Terminate communication session with OBU" referenced in the scenarios are not further detailed as the behaviour is specified in the /ETCS/

5.15 SysC: Revoke MA cooperatively by PE

Description	The purpose of this capability is to perform a co-operative shortening of MA, applying the principles of /ETCS/ - SUBSET-026, chapter 3.8.6 (/ETCS/). This may be necessary for the operational scenarios "Joining" or to reschedule train movements.
Goal	After receiving a cooperative shortening request indicating that it is requested to cooperatively shorten the MA from PE, MBS checks all safety constraints and subsequently performs the cooperative shortening of MA with the OBU.
Precondition	None
Postcondition (Success)	After the OBU has accepted the new MA and has informed MBS about this, the MBS has updated the Movement Permission and informs PE about the success of the cooperative shortening of MA procedure.
Postcondition (Failure)	Failure 1: After the OBU has rejected the new MA and has informed MBS about this, the MBS informs PE about the failure of the cooperative shortening of MA procedure. The previously received MA remains valid on-board. Failure 2: The MBS has rejected the Cooperative Shortening Request.
Involved Actors	• OBU • PE
Trigger	• MBS receives a Cooperative Shortening Request from PE indicating that it is requested to co-operatively shorten the MA.
Main Sequence	1. When all checks are successful, then MBS indicates this to PE and subsequently sends a Request to Shorten MA message to the OBU based on the Cooperative Shortening Request received from PE.
	2. When MBS receives the Request to shorten MA is granted message from the OBU, then MBS indicates this to the PE. Subsequently the *Train Object* (including the Movement Permission) is updated and PE is also informed about that.
Alternate Sequence	None
Failure Sequence	1.a) When at least one check is not successful, then the MBS indicates this to PE. The co-operative shortening of MA procedure is aborted.
	2.a) When MBS receives the Request to shorten MA rejected message from the OBU, then MBS indicates this to PE. The co-operative shortening of MA procedure is finished.
Comments	None

Table 9 – Description of SysC: Revoke MA cooperatively by PE

5.15.1 Scenario: Revoke MA cooperatively by PE

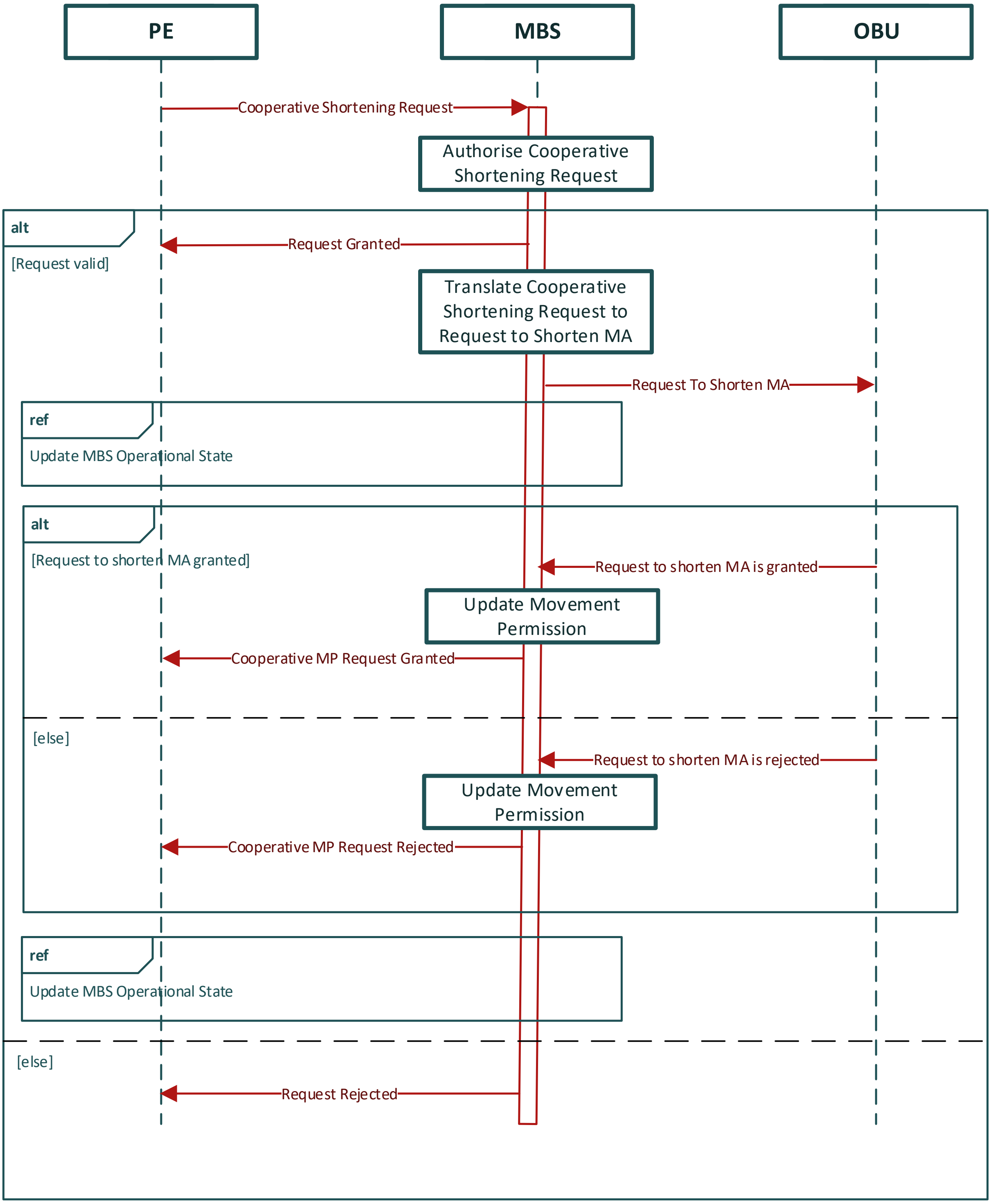


Figure 20 - Scenario 1: Revoke MA cooperatively by PE

6 SYSTEM FUNCTION SPECIFICATIONS

This chapter further details the functions introduced in the scenario of the System Capabilities.

For each function, an overview, the inputs, the outputs and the functional requirements are described.

The following table provide a mapping between the System Capabilities and the functions that are used by these capabilities inside the scenario.

System Capability as listed in chapter 5	Used function as listed in chapter 6
5.1 SysC: Start and Maintain MBS	6.19 SysF Supervise<Actor>Communication 6.20 SysF Establish<Actor>Communication
5.2 SysC: Preload Topology Data	6.6 SysF Preload Topology Data
5.3 SysC: Approve Topology Data activation	
5.4 SysC: Activate Topology Data	
5.5 SysC: Respond to initiation of communication session by PE	
5.6 SysC: Start communication with one TACS	
5.7 SysC: Respond to initiation of communication session by OBU	6.8 SysF Create Train Object
5.8 SysC: Control Switchable Trackside Assets	6.2 SysF Authorise TA State Request 6.3 SysF Translate TA State request to TACS command 6.4 SysF Send TACS command
5.9 SysC: Shutdown MBS	
5.10 SysC: Update MBS Operational State	6.5 SysF Update Domain Object state 6.7 SysF Assign a safe value to a Domain Object 6.9 SysF Localise Train 6.10 SysF Manage Unresolved Trackbound Object 6.18 SysF Update Movement Permission
5.11 SysC: Report MBS Operational State	6.1 SysF Report MBS Operational State
5.12 SysC: Start of Train	6.9 SysF Localise Train 6.16 SysF Request Movement Permission

5.13 SysC: Provide MA to Train	6.11 SysF Authorise MP Request 6.13 SysF Translate MP Request to Movement Authority
5.14 SysC: Terminate Train Mission	6.15 SysF Delete Train Object
5.15 SysC: Revoke MA cooperatively by PE	6.12 Authorise Cooperative Shortening Request 6.14 SysF Translate Cooperative Shortening Request to Request to Shorten MA 6.18 SysF Update Movement Permission

6.1 SysF Report *MBS Operational State*

6.1.1 Overview

MBS Operational State for a given *Domain Object* Instance has to be reported to the PE*.*

6.1.2 Inputs

- *MBS Domain Object*

6.1.3 Outputs

- *MBS Operational State report* according to I_PE interface

6.1.4 Functional requirements

REQ-0001

When this function is triggered for a given *MBS Domain Object* Instance, *MBS* shall send the state of the *MBS Domain Object* instance (*MBS Operational State*) to PE according to I_PE.

Rationale: Update of (changed) information OR provision of information as result of the previous request to provide the state.

Guidance: None

Operational Rules: None

Engineering Rules: None

6.2 SysF Authorise TA State Request

6.2.1 Overview

This function executes a series of safety checks on the received TA State Request.

The purpose of these Safety checks is to ensure that the requested state of the TA and the application of the corresponding TACS command by the MBS will not cause any hazards.

6.2.2 Input

- TA State Request message according to I_PE
- *MBS Operational State*

6.2.3 Outputs

- Message “request granted” according to I_PE
- Message “request rejected” according to I_PE

6.2.4 Functional requirements

REQ-SAFETY

The MBS shall perform a series of checks in the sequence given by the following ordered list of requirement references when it receives a DPS Group Request through I_PE:

1. REQ-SC_SYNTAX
2. REQ-SC_DPSG_EXISTS
3. REQ-SC_DPS_EXISTS
4. REQ-SC_DPS_DPSG
5. REQ-SC_DPSG_REACHABLE
6. REQ- SC_DPSG_CHANGE
7. REQ-SC_DPSG_STATE
8. REQ-SC_DPS_TO
9. REQ-SC_DPS_UTO
10. REQ-SC_DPS_MP
11. REQ-SC_DPS_RB
12. REQ-SC_DPS_RP

Rationale: The purpose of these checks is to ensure that the requested state of the TA and the application of the corresponding TACS command by the MBS will not cause any hazards

Guidance: This is the head requirement for all safety checks.

Operational Rules: None

Engineering Rules: None

REQ-0004

The MBS shall abort checking a DPS Group Request received through I_PE if any performed safety check failed.

Rationale: If a check for example discovers a message syntax error, further checks might lead to illegal function calls within MBS.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-SC_SYNTAX

If the syntax of the DPS Group Request message is not in accordance with the I_PE interface, MBS shall send a “SYNTAX” reject code.

Rationale: The MBS must be able to decode the request from PE.

Guidance: An invalid command syntax might lead to invalid state.

Operational Rules: None

Engineering Rules: None

REQ-SC_DPSG_EXISTS

MBS shall check that the DPS Group referenced in the DPS Group Request is known to MBS and if the check fails, MBS shall send a “DPS_UNKNOWN” reject code.

Rationale: The MBS must know the TA to be able to send a command to the corresponding TACS.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-SC_DPS_EXISTS

MBS shall check that every DPS referenced in the DPS Group Request is known to MBS and if the check fails, MBS shall send a “DPS_UNKNOWN” reject code.

Rationale: The MBS must know the TA to be able to send a command to the corresponding TACS.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-SC_DPS_DPSG

MBS shall check that every DPS referenced in the DPS Group Request is associated with the DPS Group referenced in the DPS Group Request and if the check fails, MBS shall send a “DPS_UNKNOWN” reject code.

Rationale: A DPS that is referenced shall be part of a DPS Group, otherwise a check could be performed for a DPS on another DPS Group.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-SC_DPSG_REACHABLE

MBS shall check that the TACS associated with the DPS Group referenced in the DPS Group Request are connected to MBS and able to receive commands and if the check fails, MBS shall send a “DPS_GROUP_NOT_READY” reject code.

Rationale: The MBS must be in communication with the TACS to be able to send a command to the corresponding TACS.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ- SC_DPSG_CHANGE

MBS shall check that the DPS states in the DPS Group Request are different to the target states currently in the referenced DPS Group and if the check fails, MBS shall send a “DPS_GROUP_NO_CHANGE” reject code

Rationale: MBS rejects the request if the DPSs are already in the state requested in the command. If all other safety checks would pass, MBS would set the reported state of all DPS to NONE and the DPS Group state to PROCESSING.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-SC_DPSG_STATE

MBS shall check that the combination of requested drivability states for each DPS referenced in the DPS Group Request matches one of the allowed combinations of the DPS Group and if the check fails, MBS shall send a “INVALID_COMBINATION” reject code.

Rationale: The MBS must be able to translate the state of the TA into a valid command for the corresponding TACS. The MBS checks that the requested state is allowed for this TA by the *Domain Data* (see *Drive Protection Section* Group in System Pillar TCCS SD1 Data Model /SD1DM/).

Guidance: None.

/SD1DM/

Operational Rules: None

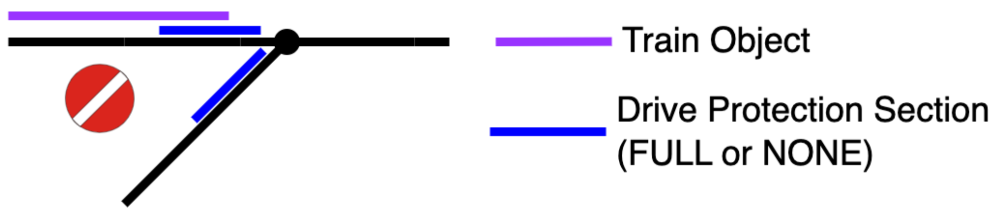
Engineering Rules: None

REQ-SC_DPS_TO

MBS shall check that no DPS of the DPS Group referenced in the DPS Group Request overlaps with a *Train Location* of a *Train Object* and if the check fails, the MBS shall send a “DPS_OCCUPIED” reject code.

Rationale: To move a TA, it must be free for state change (not occupied by a train).

Guidance:



Operational Rules: None

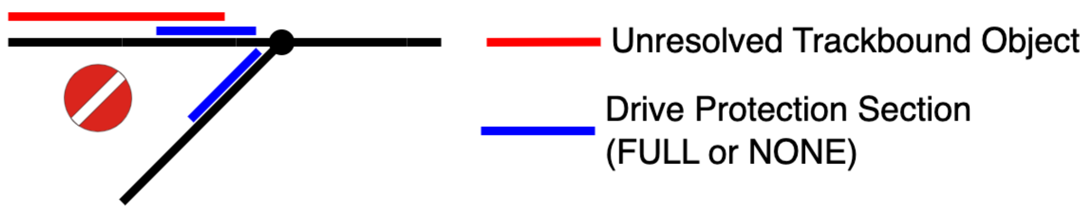
Engineering Rules: None

REQ-SC_DPS_UTO

MBS shall check that no DPS of the DPS Group referenced in the DPS Group Request overlaps with an Unresolved Trackbound Object and if the check fails, the MBS shall send a “DPS_OCCUPIED” reject code.

Rationale: To move a TA, it must be free for state change (not possibly occupied by a train).

Guidance:



Operational Rules: None

Engineering Rules: None

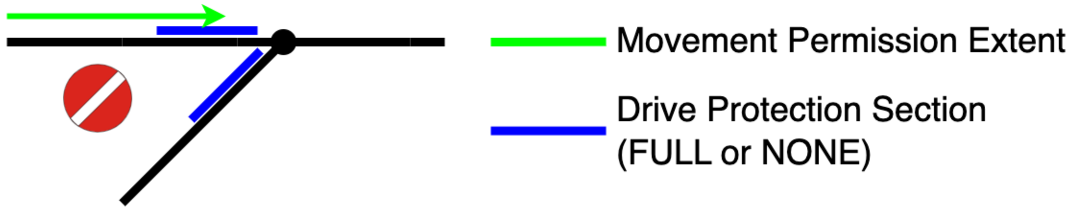
REQ-SC_DPS_MP

MBS shall check that no DPS of the DPS Group referenced in the DPS Group Request overlaps with a *Movement Permission Extent* and if the check fails, the MBS shall send a “DPS_LOCKED” reject code.

Rationale: To move a TA, it must not be allocated to any Movement Permission.

Guidance:

In the following figure, a *Movement Permission* overlaps a DPS of a DPS Group associated with the TA point, it is forbidden to move the point as this could cause a derailment. The same principle is also applied to other *Trackside Asset* types.



Operational Rules: None

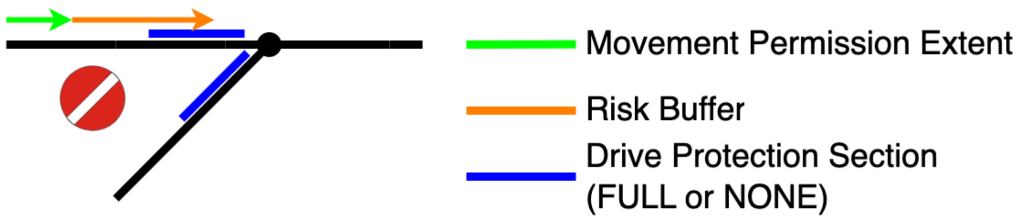
Engineering Rules: None

REQ-SC_DPS_RB

MBS shall check that no DPS of the DPS Group referenced in the DPS Group Request overlaps with a *Risk Buffer* and if the check fails, the MBS shall send a “DPS_LOCKED” reject code.

Rationale: To move a TA, it must not be allocated to any Movement Permission or locked in *Risk Buffer*. This implies that swinging overlaps are currently not supported.

Guidance:



Operational Rules: None

Engineering Rules: None

REQ-SC_AS_RP

MBS shall check that no *Risk Path* is terminated on a DPS belonging to this TA according to REQ-SC_RP_TERM_DPS and if this check fails, MBS shall send a "DPS_SECURING_RISKPATH" rejected code.

Rationale: To move a TA, it must not be providing flank protection.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-0005

If the DPS Group Request is not rejected, then MBS shall grant the request from PE to change the state of a *Switchable TA* and send the message "request granted" to PE.

Rationale: The request needs an answer to be sent to the PE.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-0003

If the DPS Group Request is not rejected, then MBS shall set the currentDriveability for all associated DPS to NONE and the dpsGroupState to PROCESSING.

Rationale: When command is in progress, DPS driveability is set to a safe state (NONE) immediately after granting the request as this DPS cannot be used until the reported state is equal to the requested state.

Guidance: None.

Operational Rules: None

Engineering Rules: None

6.3 SysF Translate TA State request to TACS command

6.3.1 Overview

The requested state of the abstracted *Switchable TA* is being translated into a specific command for the real trackside element controller (TACS).

6.3.2 Inputs

Requested state of the *Switchable TA.*

6.3.3 Outputs

TACS command according to I_TACS

6.3.4 Functional requirements

REQ-0006

If the request to change the state of a *Switchable TA* has been authorised, then MBS shall translate the request to a command to change the TA state to the requested one, according to the I_TACS interface.

Rationale: Once the TA State Request has been successfully checked, this TA State Request is translated into a TACS command to be sent to the corresponding TACS.

Guidance: None

Operational Rules: None

Engineering Rules: None

6.4 SysF Send TACS command

6.4.1 Overview

When this function is triggered by a translated TACS command, it sends the corresponding message to the requested TACS according to the I_TACS interface.

6.4.2 Inputs

TACS command.

6.4.3 Outputs

See I_TACS.

6.4.4 Functional requirements

REQ-0007

If a TACS command is translated, MBS shall send this TACS command to the corresponding TACS according to the I_TACS interface.

Rationale:	To be able to operate a *Switchable TA.*
Guidance:	/ReqSubsP/
Operational Rules:	None
Engineering Rules:	None

6.5 SysF Update *Domain Object* state

6.5.1 Overview

This function translates the TA and its state from a valid TACS report to the related *Domain Object* and updates its state.

Note: The state change of a *Domain Object* in case of communication loss is handled by the capability SysC: Update *MBS Operational State*.

6.5.2 Input

- TACS report
- OBUCommLost, *OBUCommEstablished*

6.5.3 Output

- *Domain Object* state

6.5.4 Functional requirements

REQ-0008

When a TACS report is received, MBS shall check the syntactical correctness of the message according to the I_TACS interface and if the check fails, the message shall be discarded.

Rationale:	To be able to operate a *Switchable TA.*
Guidance:	None
Operational Rules:	None
Engineering Rules:	None

Open point: check safety relevance (is discarding a safe measure?). Note: if a message is discarded at application layer, can the communication status still be considered established or is it needed to be torn down as safety reaction? [SAFETY_ANALYSIS]

REQ-0009

When a TACS report is decoded, MBS shall discard the message if this TACS does not exist in the *Domain Objects*.

Rationale: For a message received on a given communication channel, MBS should know the name of the TACS and the corresponding TACS type (e.g., Points, Level Crossing)

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-0011

When a TACS report is decoded, *MBS* shall update the related *Domain Object* reported state according to the TACS report.

Rationale: Keep the *MBS Operational state* up to date.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-0061

When a TACS report for a Switchable TA is received and no command is in progress (dpsGroupState is not PROCESSING), *MBS* shall update the DPS state according to the TACS report.

Rationale: Keep the *MBS Operational state* up to date. When no command is in progress, the reported state is always considered.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-0062

When a TACS report for a Switchable TA is received and a command is in progress (dpsGroupState is PROCESSING), *MBS* shall update the DPS state according to the TACS report only if the reported state corresponds to the requested state.

Rationale: When a command is in progress, the DPS driveability is updated only if it corresponds to the requested state..

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-0035

If a *Switchable TA* is now in the state requested, then MBS shall consider that a command is no more in progress and set (dpsGroupState to READY) for the corresponding *Switchable TA*.

Rationale: Once the TA is in the requested state, the command is no more in progress.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-0094

When MBS detects that the safe connection with an OBU is lost or (re)established, MBS shall update the connection status of the corresponding Train Object.

Rationale: The connection status of OBU must be reported to other systems.

Guidance: None

Operational Rules: None

Engineering Rules: None

6.6 SysF Preload Topology Data

6.6.1 Overview

With this function, *MBS* processes *Topology Data* received from *DR* (stores them, builds the *Domain Objects* within *MBS*).

6.6.2 Input

- *Topology Data* from *DR* in message *Domain Data*

6.6.3 Output

- Message *Domain Data Request*
- Message *Domain Data Acknowledgement*

6.6.4 Functional requirements

REQ-0018

When *MBS* has no *Topology Data*, it shall send the message *Domain Data Request* according to I-DR to *DR* to get initial *Topology Data*. The parameter *version* is not used.

When *MBS* has *Topology Data*, it shall send the message *Domain Data Request* according to I-DR to *DR* to check if available *Topology Data* still are in the required version. The parameter *version* refers to the version of the existing data.

Rationale: None

Guidance: It is up to the implementation if *MBS* stores *Topology Data* persistently or not. If it does not store it, it would request *Topology Data* with every (re)start. If it stores *Topology Data* persistently, it has to assure while restoring them, that stored data have not been falsified.

Operational Rules: None

Engineering Rules: None

REQ-0017

When *MBS* receives the message *Domain Data* from *DR*, *MBS* shall convert the received data into *Domain Object*s.

Upon **successful** conversion and storage, *MBS* shall send the message *Domain Data Acknowledgement* according to I_DR to *DR* with parameter *preLoadingStatus == success.*

Up to release 4: The *Topology Data* shall be considered active immediately and *MBS* be considered operational.

Rationale: None

Guidance: The correctness check covers for example the following aspects: Syntax, integrity, authenticity, version etc.

Operational Rules: None

Engineering Rules: None

REQ-0019

When *MBS* receives the message *Domain Data* from *DR*, *MBS* shall convert the received data into *Domain Object* data.

Upon **unsuccessful** conversion and storage, *MBS* shall discard the data and send the message *Domain Data Acknowledgement* according to I_DR to *DR* with parameter *preLoadingStatus == failure.*

Rationale: None

Guidance: None

Operational Rules: None

Engineering Rules: None

6.7 SysF Assign a safe value to a *Domain Object*

6.7.1 Overview

This function assigns a safe value to a *Domain Object*.

6.7.2 Inputs

- *Domain Object*

6.7.3 Outputs

- *Domain Object State*

6.7.4 Functional requirements

REQ-0020

When created, a *Domain Object* shall be initialised with a safe value.
When *MBS* cannot receive an up-to-date information from the related real-world object, it shall set the *Domain Object* to a safe value.

Rationale: *MBS* must assume the safe value when it cannot know the real value.

Guidance: Setting the safe value is needed during *MBS* (re)start and when *MBS* detects that the communication session to the provider of the original information is lost.

The safe value for a switchable *Trackside Asset* is NONE for all related DPSs and OCCUPIED for a TVPS.

Operational Rules: None

Engineering Rules: None

REQ-0028

When MBS starts up, the MBS shall create one or several *Unresolved Trackbound Objects* covering the complete AoC.

Rationale:

This is to start with the most restrictive state.

Guidance:

To consider the AoC as unresolved, the MBS creates one or several *Unresolved Trackbound Objects* covering the complete AoC.

Operational Rules: None

Engineering Rules: None

REQ-0029 FOR FURTHER RELEASE [X2R5 REQ-TrackInit-2]

The MBS shall utilise valid Stored Information to enable faster initialisation.

Rationale:

Historic information on the state of the railway from before the MBS was restarted can enhance the Initialisation process.

Guidance:

The location of all trains in communication prior to the restart, along with the extent of any MAs issued will be valuable information to be utilised.

The validity of the information used must be carefully considered, as if the MBS has been offline for some time the State of the Railway is likely to have changed.

Criteria for considering Stored information as valid are project dependent e.g. during MBS Initialisation, if the time passed is smaller than a configured value.

Operational Rules: None

Engineering Rules: ENG-TrackInit-1

REQ-0030 FOR FURTHER RELEASE [X2R5 REQ-TrackInit-3]

The MBS shall, if configured, provide a means for the person responsible for the MBS Initialisation to confirm that the procedure is completed.

Rationale:

If Stored Information is not valid, the person in charge of initialising the MBS has to confirm when the procedure is completed. They have the authority to confirm that all the obstacles on the railway are known to the MBS.

Guidance:

If Stored information is used to initialise the MBS, this confirmation is not needed and it is project specific to implement it.

Operational Rules: OPE-TrackInit-4

Engineering Rules: ENG-TrackInit-2

6.8 SysF Create *Train Object*

6.8.1 Overview

When MBS has successfully established a communication session with an OBU, then a *Train Object* for this OBU is established in the MBS. This *Train Object* subsequently covers all train-related information (e.g. Train Data, *Train Location*, etc.) as soon as this information is available.

6.8.2 Inputs

Successfully established communication session between MBS and an OBU

6.8.3 Outputs

Train Object

6.8.4 Functional requirements

REQ-CreateTrain-0001

As soon as there is an established communication session between MBS and an OBU, the MBS creates a *Train Object* for this OBU.

Rationale: None

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-TrainLoc-2

The MBS shall store a *Train Object* for all communicating trains within its Area of Control. When available, the following information shall be stored:

1. Train ID (NID_ENGINE)
2. Train Data (including L_TRAIN)
3. Most recent Train Position Report information
4. *Train Location* (when determined)
5. Time when the stored information was last valid
6. Train Running Number

Rationale:

This ensures that MBS has an up-to-date image of all train-related information. Most recent Train Position report information is used to e.g. store detailed position information (e.g. mSFE).

Guidance:

The time when the stored information was last valid is required in order to enable the possible use of the stored information during Trackside Initialisation.

Operational Rules: None

Engineering Rules: None

6.9 SysF Localise Train

6.9.1 Overview

This function localises a communicating train within the Area of Control. The *Train Location* information is stored in the *Train Object*.

Within the MBS, the *Train Location* for a train is the MBS interpretation of the location of the train, based on Train Position Reports, Validated Train Data and other inputs if available, e.g. TTD sections.

A *Train Location* has a front and a rear:

> The front of the *Train Location* is the MBS view of the furthest position for the front of the train, based on Train Position Reports and other inputs, e.g. TTD sections.
>
> The rear of the *Train Location* is the MBS view of the furthest position for the rear of the train, based on Train Position Reports, Validated Train Data, and other inputs, e.g. TTDs.

The different terms used within this section to determine a *Train Location* are summarised in Figure 21.

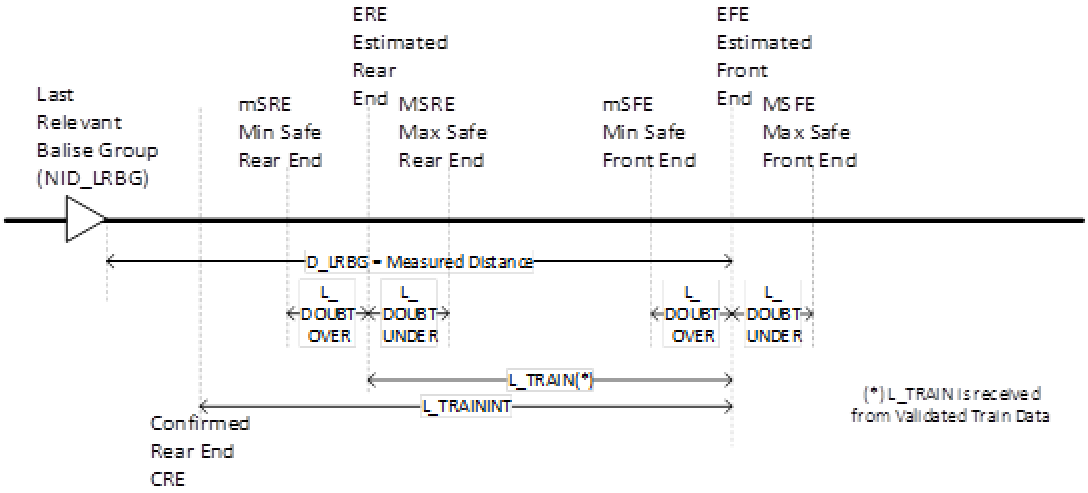


Figure 21: Terms used for Train Location

There are several reasons to create or move a *Train Location*, as shown in Table 10:

Create-move *Train Location* Reasons	Notes	Requirements
Train SoM position report received	*Train location* created from min Safe Front End to max Safe Front End (before having received train data)	REQ-TrainLoc-4
First Train Position Report	For example, PR without SoM process	REQ-TrainLoc-5

Update front by Train Max SFE	Front of the *Train Location* is updated using Max Safe Front End derived from the Train Position Report	REQ-TrainLoc-7
Update rear by Train CRE	Rear of the *Train Location* is updated using the Confirmed Rear End derived from the Train Position Report	REQ-TrainLoc-8 REQ-TrainLoc-9
Update rear with new value of Train Length	Rear of the *Train Location* is updated using the new value of Train Length	REQ-TrainLoc-6
Update front by clear TTD	Front of the *Train Location* is shortened using clear TTD section	REQ-TTD-2 REQ-TTD-4
Update rear by clear TTD	Rear of the *Train Location* is shortened using clear TTD	REQ-TTD-3 REQ-TTD-4
Update front by occupied TTD for mute train	Update front of the *Train Location* when a TTD becomes occupied for a mute train	REQ-TTD-5

Table 10 – Reasons to create or move *Train Location*

There are several reasons to delete a *Train Location*, as shown in Table 11:

Delete *Train Location* Reasons	Notes	Requirements
Train is no longer in communication	MBS considers that a train is no longer in communication	REQ-TrainLoc-10 REQ-0040

Table 11 – Reasons to delete *Train Location*

6.9.2 Inputs

- *Train Position Reports*
- *Validated Train Data*
- *Domain Data*
- *TTD section status (Domain Object* state)

6.9.3 Outputs

- *Train Location*

6.9.4 General *Train Location* Requirements

REQ-0063

To create or move a *Train Location*, the MBS shall perform the requirements sequentially in the order they are found in Table 10.

Rationale: For example, the position report requires the updating of the train front location prior the updating of the train rear location. Once the *Train Location* has been updated by the position report, it can be updated again by the clear TTD.

Guidance: None

Operational Rules: None

Engineering Rules: None

6.9.5 Requirements to create a *Train Location*

REQ-TrainLoc-5

The MBS shall create a *Train Location* for the *Train Object* from the Min Safe Front End to the Max Safe Front End derived from the Train Position Report if the following conditions are fulfilled:

- Train Position Report from an OBU where the reported position is unambiguous to the MBS is received, AND
- there is no *Train Location* for this OBU, AND
- mode is different from SB

Rationale:

This is to enable the MBS to record the *Train Location* of all communicating trains in the Area of Control.

Guidance:

The MBS will need to create a new *Train Location*:

- For an OBU which has started a communication session within the Area of Control, but which is not performing Start of Mission.
- For an OBU which has entered the Area of Control.

For a train which has started a communication session within the Area of Control, but which is not performing Start of Mission, the new *Train Location* will be from Max Safe Front End to Min Safe Front End, as there will be no train length provided yet.

For a train which has entered the Area of Control, and which has not confirmed Train Integrity, the new *Train Location* will be at least from the Max Safe Front End to the border of the Area of Control. This applies to both Handovers and Transitions.

How and when the first *Train Location* is established at the border to an Area of Control is project specific.

Note: When Train Data message is received for a train not yet localised (i.e. without existing *Train Location)*, the *Train Location* is created for the front of the train due to the Train Position Report contained in this message. The train rear is afterwards localised using the Train Length (L_TRAIN) contained in the Train Data message (see REQ-TrainLoc-6).

Operational Rules: None

Engineering Rules: None

REQ-TrainLoc-4

When receiving a Start of Mission Train Position Report which status is valid from a train where the reported position is unambiguous to the MBS, the MBS shall create a *Train Location* for that *Train Object* from the Min Safe Front End to the Max Safe Front End derived from the Train Position Report.

Rationale:

For a train which has a new connection to the MBS, the MBS must create a new *Train Location* for the reported position.

Guidance:

At Start of Mission, before the receipt of Validated Train Data, only the Estimated Front End and its Confidence Interval are known to the MBS. The *Train Location* is then only from Max Safe Front End to Min Safe Front End, as shown in Figure 22.

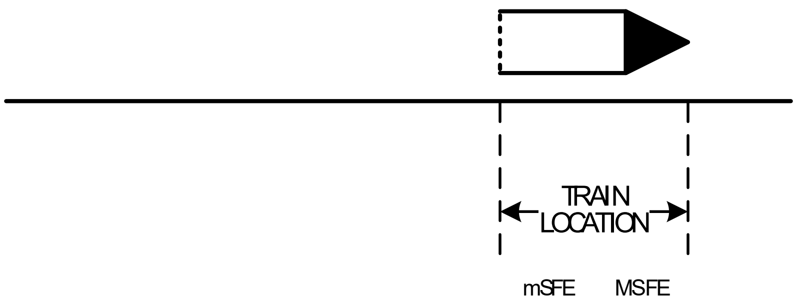


Figure 22: *Train Location* from Start of Mission Train Position Report

In Figure 22, the *Train Object* is shown with Train Integrity not confirmed. Train integrity cannot be confirmed until Validated Train Data has been acknowledged by the MBS.

How a *Train Location* which is partially outside the Area of Control is processed will be project specific.

There are other requirements (e.g. REQ-TMS-1) covering the situations when the reported location is invalid or unknown, or is valid but ambiguous to the MBS.

Operational Rules: None

Engineering Rules: None

REQ-TMS-1 FOR FURTHER RELEASE [X2R5 REQ-TMS-1]

The TMS shall provide means for a Signaller to assign a position to a train that is reporting a position during Start of Mission which is unknown or invalid, or a position which the MBS considers ambiguous.

Rationale:

This is to allow the MBS to locate a train in its Area of Control after a specific operational procedure.

Guidance:

How the Signaller enters the position of a train in the TMS is project specific, but the MBS cannot accept a position in a clear area of track.

The Signaller may need to contact the Driver to determine an estimated location for the train.

Operational Rules: OPE-SoM-4

Engineering Rules: None

6.9.6 Requirements to update a *Train Location*

REQ-TrainLoc-7

When receiving a Train Position Report from a train and the position is not ambiguous to the MBS, the MBS shall update the front of the *Train Location* for this train using the Max Safe Front End derived from the Train Position Report

Rationale:

The MBS uses the information in Train Position Reports to update the *Train Location* of trains in its area.

Guidance:

The front of the *Train Location* for a train can be updated with every position report received, including trains in RV mode, if the position is known to the MBS.

Figure 23 shows how the front of the *Train Location* is updated with a new train position report.

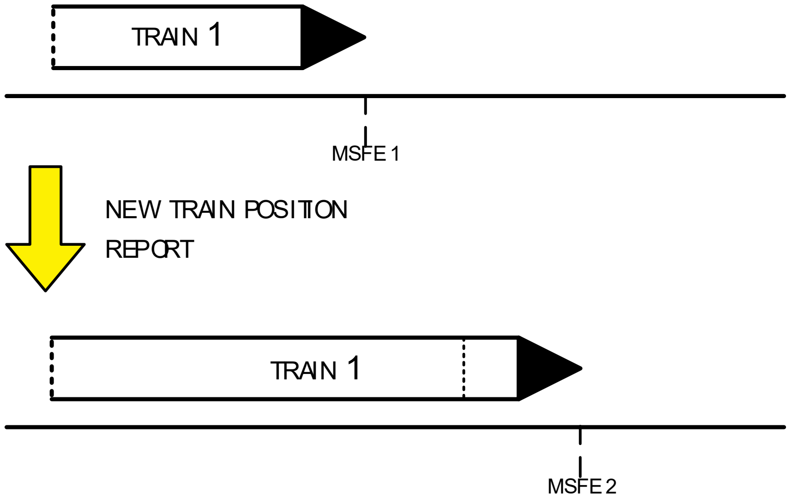


Figure 23: Front of *Train Location* updated from new Train Position Report

Operational Rules: None

Engineering Rules: None

REQ-TrainLoc-8

When receiving a Train Position Report from a train where:

- the position is not ambiguous to the MBS, AND
- there is a *Train Location* for that train, AND
- the train is in FS, OS or SB, AND
- Train Integrity is confirmed by external source,

then the MBS shall update the rear of the *Train Location* for this train using the Confirmed Rear End derived from the Train Position Report.

Rationale:

The MBS uses the information in Train Position Reports to maintain the *Train Location* of trains in its Area of Control.

Guidance:

The Confirmed Rear End is only known when receiving a Train Position Report with the Train Integrity confirmed. From the ladder the MBS can locate the confirmed rear end of the train.

Figure 24 shows how the CRE is updated with a new train position report with Train Integrity Confirmed.

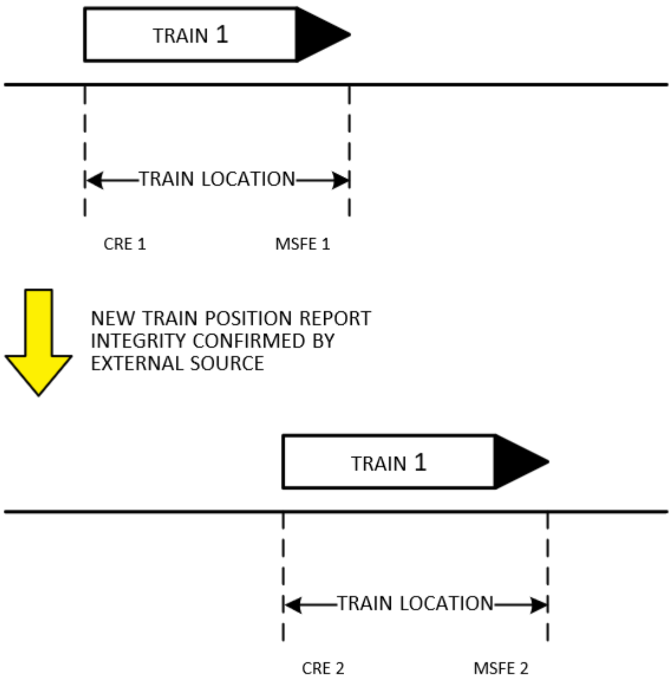


Figure 24: Rear of *Train Location* updated from new Train Position Report, Integrity Confirmed

Train Position Reports from trains in FS and OS will be from trains where linking is used. Train Position Reports from trains in SB allow for defining a *Train Location* at Start of Mission. Other modes, including SR, are excluded as there are issues with relocation.

Operational Rules: None

Engineering Rules: None

REQ-TrainLoc-9

When receiving a Train Position Report from a train where:

- the position is known to the MBS, AND
- there is a *Train Location* for that train, AND
- the train is in FS, OS or SB, AND
- Train Integrity is confirmed by Driver, AND
- the MBS is configured to accept Train Integrity confirmed by Driver,

then the MBS shall update the rear of the *Train Location* for this train using the Confirmed Rear End derived from the Train Position Report.

Rationale:

The MBS uses the information in Train Position Reports to update the *Train Location* of trains in its Area of Control.

Guidance:

The Confirmed Rear End is only known when receiving a Train Position Report with Train Integrity confirmed from which the MBS can locate the rear of the train.

If Train Integrity is confirmed by the driver, then the *Train Location* is only updated if the MBS is configured to accept this.

Train Position Reports from trains in FS and OS will be from trains where linking is used. Train Position Reports from trains in SB allow for defining a *Train Location* at Start of Mission. Other modes, including SR, are excluded as there are issues with relocation.

Operational Rules: OPE-Generic-3

Engineering Rules: ENG-LossTI-2

REQ-TrainLoc-6

When receiving a new value of Train Length in Validated Train Data from a train, the MBS shall update the Rear End of the *Train Location* for this train using the new value of Train Length.

Rationale:

The receipt of a new value of Train Length in Validated Train Data represents new information from the train, which must be used to update the *Train Location*.

Guidance:

The only information used from the Validated Train Data to determine *Train Location* is the train length (L_TRAIN).

A new value of L_TRAIN means either the first value received since the *Train Location* was created, or a changed value received at some later time.

If this is the first value for L_TRAIN received since the *Train Location* was created, then the *Train Location* is extended as shown in Figure 25.

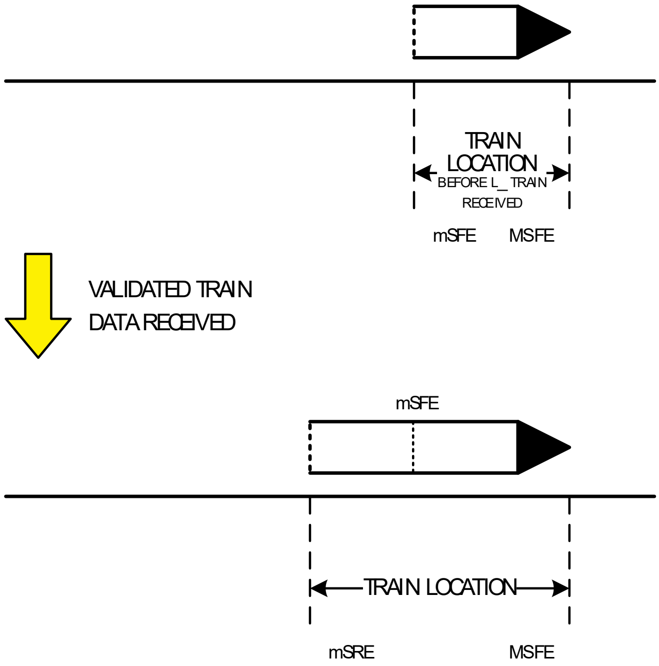


Figure 25: *Train Location* when receiving Validated Train Data during Start of Mission

If this is a changed value of L_TRAIN, then the new value of L_TRAIN could be shorter than the previous value, for example after Splitting, as shown in Figure 26. In this case, a UTO is also created according to requirement REQ-TrackStatus-25 to manage the missing part.

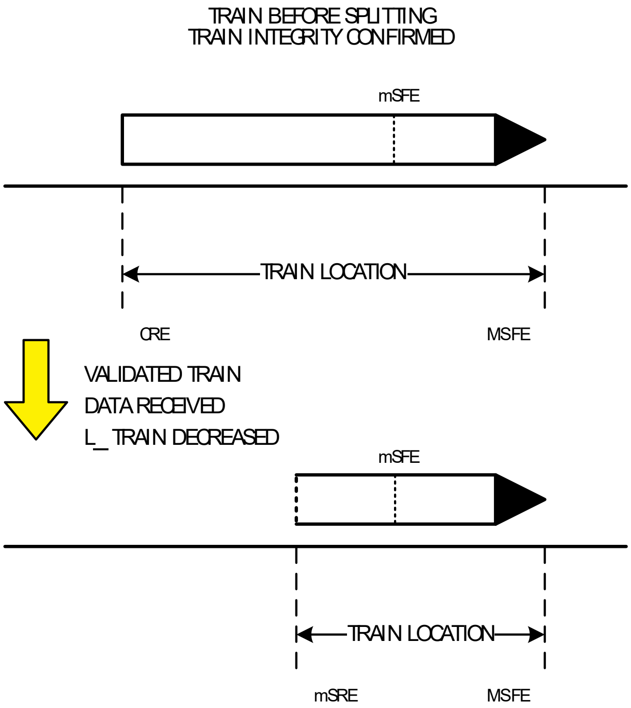


Figure 26: *Train Location* when receiving Validated Train Data, L_TRAIN decreased

If this is a changed value of L_TRAIN, then the new value of L_TRAIN could be longer than the previous value, for example after Joining, as shown in Figure 27.

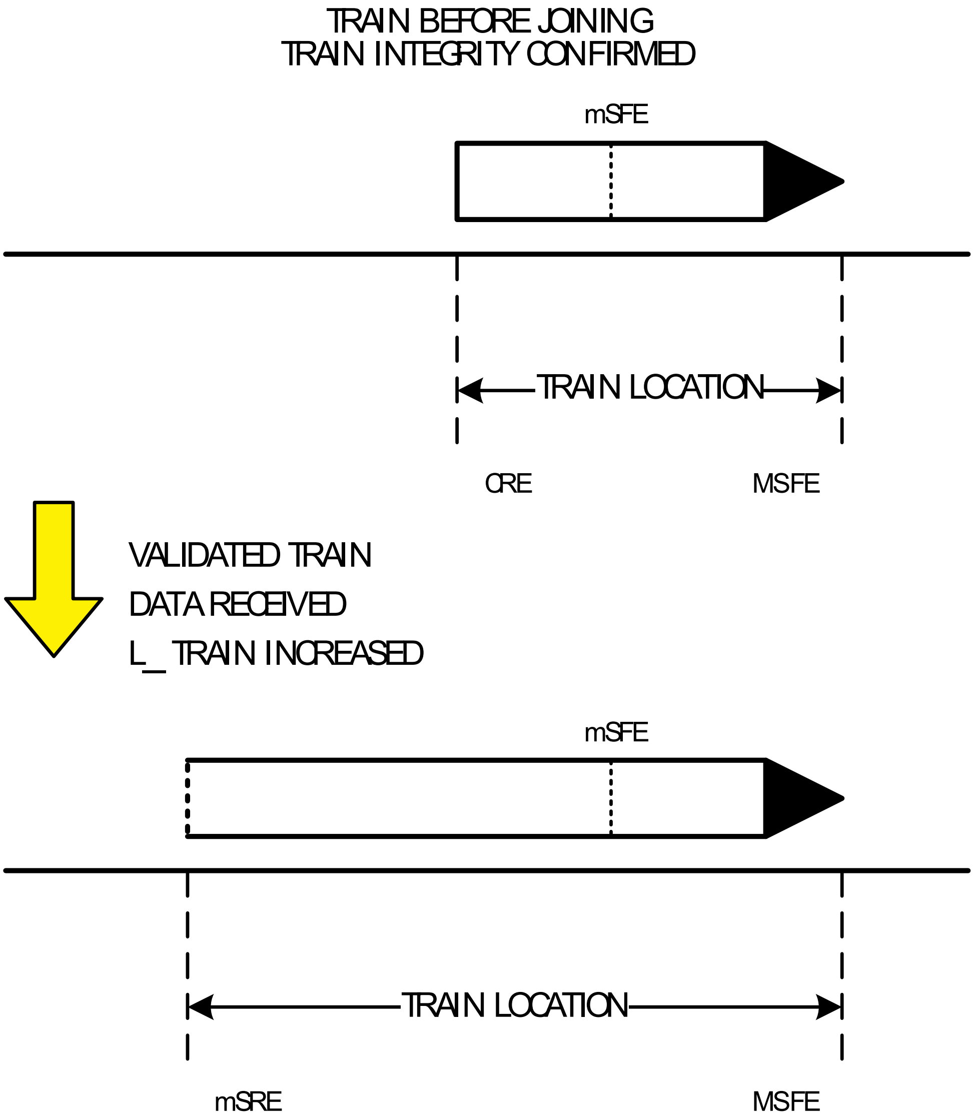


Figure 27: *Train Location* when receiving Validated Train Data, L_TRAIN increased

If the new *Train Location* extends outside the Area of Control, the handling is not managed in the current release.

Operational Rules: None

Engineering Rules: None

6.9.7 Reaction to Unexpected *Train Locations* – FOR FURTHER RELEASE

REQ-TrainLoc-12 FOR FURTHER RELEASE [X2R5 REQ-TrainLoc-12]

If a train reports a position that is unexpected or in conflict with other train movements, the MBS shall react to transition the system to a safe state.

Rationale:

The MBS is reliant upon trains reporting their position to separate traffic safely and the MBS must therefore react if it detects a potentially hazardous situation.

Guidance:

A train reporting an unexpected position can be a hazard even when there is TTD if more than one train is in the same TTD section, but the situation is more severe in an area without TTD.

The MBS will only be able to detect conflicts with other train movements which have been authorised by the MBS.

There are several situations where a position report from a train may require immediate action from the MBS to avoid a potential hazard, for example:

- a train reporting a position in an area previously considered clear, e.g. at Start of Mission, OR
- a train which has been allocated a Reserved Status Area reporting a position which cannot be linked with that Reserved Status Area, OR
- a train reporting a position locating it within a Reserved Status Area allocated to another train.

The specific reaction applied will depend on the situation and application specific requirements. Possible reactions include:

- shortening of the Movement Authority for the affected train(s),
- sending an Unconditional Emergency Stop message to the affected train(s).

Note that the *Train Location* is created or updated by other requirements.

Operational Rules: None

Engineering Rules: None

REQ-TrainLoc-13 FOR FURTHER RELEASE [X2R5 REQ-TrainLoc-13]

If a train reports a position that is unexpected or in conflict with other train movements, the MBS shall alert the PE to the situation.

Rationale:

This is to make the TMS and Signallers aware in case the reported position could be a real or potential hazard for other train movements.

Guidance:

A train reporting an unexpected position can be a hazard even when there is TTD if more than one train is in the same TTD section, but the situation is more severe in an area without TTD.

The MBS will only be able to detect conflict with other train movements which have been authorised by the MBS.

There are several situations where a position report from a train may require additional intervention from the TMS or Signaller to manage the degraded situation. For example:

- a train reporting a position in an area previously considered clear, e.g. at Start of Mission, OR
- a train reporting a position locating it within a Reserved Status Area allocated to another train.

Operational Rules: None

Engineering Rules: None

6.9.8 Impact from TTD on *Train Locations*

REQ-TTD-1

For a system using TTD, the MBS shall manage the asynchronicity between TTD section status and Train Position Reports for a communicating train.

Rationale:

It will occur that the train physically occupies a TTD section before it has reported its position within the TTD section (or vice versa). Similarly, the train may physically leave a TTD section before it has reported its position beyond the TTD section (or vice versa). The MBS must correlate these events.

Guidance:

The MBS must be designed to allow for:

- A TTD section becoming Occupied by a train before the train has reported a position within the TTD section.
- A train reporting a position within the TTD section before TTD section becomes Occupied.
- A TTD section becoming Clear after a train has left the TTD section before the train has reported a position clear of the TTD section.

- A train reporting a position clear of the TTD section before the TTD section becomes Clear.

The MBS could use a variety of technical solutions to correlate TTD occupancy to Train Position Reports. For example:

- Sending a Conditional Emergency Stop when a TTD is occupied, to stop a train that is approaching a boundary of the TTD if it is not the one that occupied the TTD.
- Use of a delay timer, to account for lack of synchronisation between Train Position Reports and TTD occupancy. If a train is still not detected when the timer expires, the MBS would react suitably.
- Tracking of TTD section occupancy and correlation with Train Position Reporting, to ensure a normal sequence is observed.

Note: a combination of these techniques may be used, depending on project specific requirements.

Operational Rules: None

Engineering Rules: None

REQ-TTD-2

For a system using TTD, if the Max Safe Front End reported by a train is located in a clear TTD section while the Min Safe Front End is not in this TTD section, then the MBS shall shorten the front of the *Train Location* for this train, by the extent of each TTD section that is detected Clear between the Min Safe Front End and the Max Safe Front End.

Rationale:

TTD information can be used to improve the MBS knowledge about the status of the track in the Area of Control, thus improving the performance of the system.

Guidance:

The effect of a Clear TTD section in the front part of a *Train Location* is to update the front of the *Train Location*.

This can be used to avoid locking points and level crossings in front of the train. Both the reception of TTD status and the receiving of a Train Position Report can be the trigger for updating the *Train Location*.

A clear TTD section in front of a train can shorten the front part of the *Train Location* of the train, as shown in Figure 28:

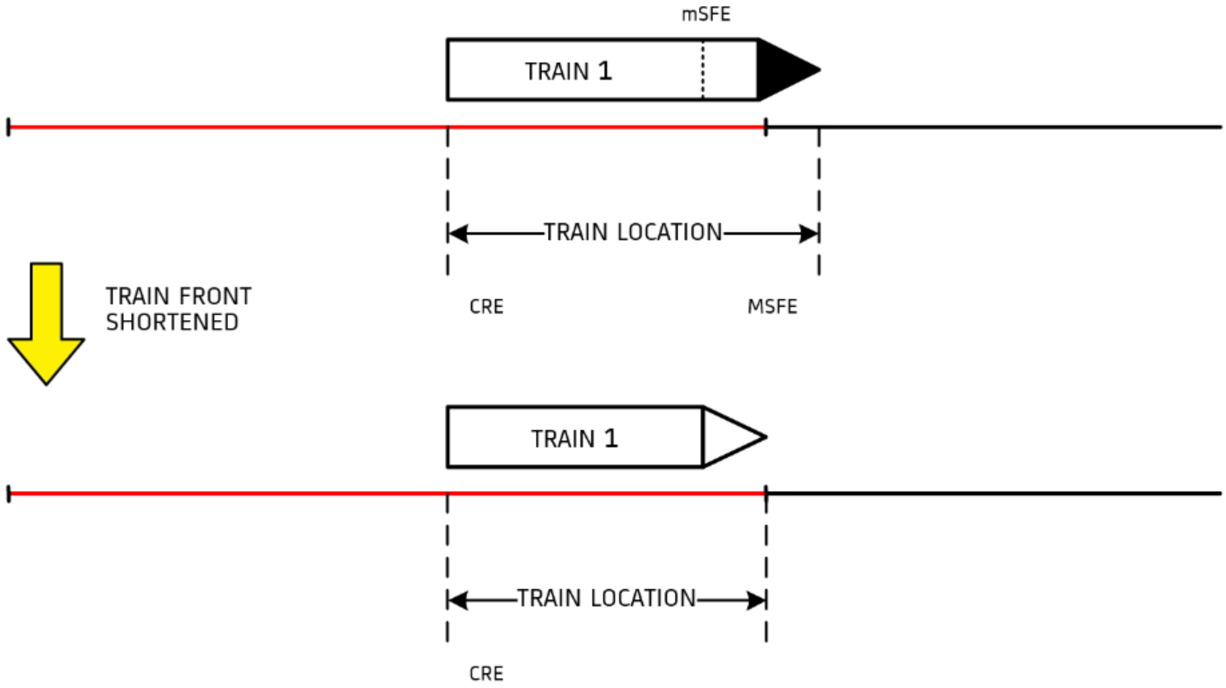


Figure 28: Shortening of front of *Train Location* due to clear TTD

Figure 29 shows the situation where the min Safe Front End is reported within the same Clear TTD as the Max Safe Front End, and therefore no shortening:

Figure 29: No shortening of front of *Train Location* due to clear TTD

Operational Rules: None

Engineering Rules: ENG-Generic-4

REQ-TTD-3

For a system using TTD, if the Rear End of the *Train Location* is located in a clear TTD section while the Max Safe Rear End is not in this TTD section, then the MBS shall shorten the rear of the *Train Location* for this train, by the extent of each TTD section that is Clear between the Rear End of the *Train Location* and Max Safe Rear End.

Rationale:

TTD information can be used to improve the MBS knowledge about the status of the track in the *Area of Control*, thus improving the performance of the system.

Guidance:

The effect of the Clear TTD section in the rear part of the *Train Location* is to update the rear of the *Train Location*.

This could be used to release points and level crossings faster. Both the reception of TTD section status and the receiving of a Train Position Report can be the trigger for updating the *Train Location*.

Care must be taken to allow for the overhang of vehicles at the boundary between an occupied and a clear TTD section.

A clear TTD section in rear of a train can shorten the rear part of the *Train Location* of the train, as shown in Figure 30:

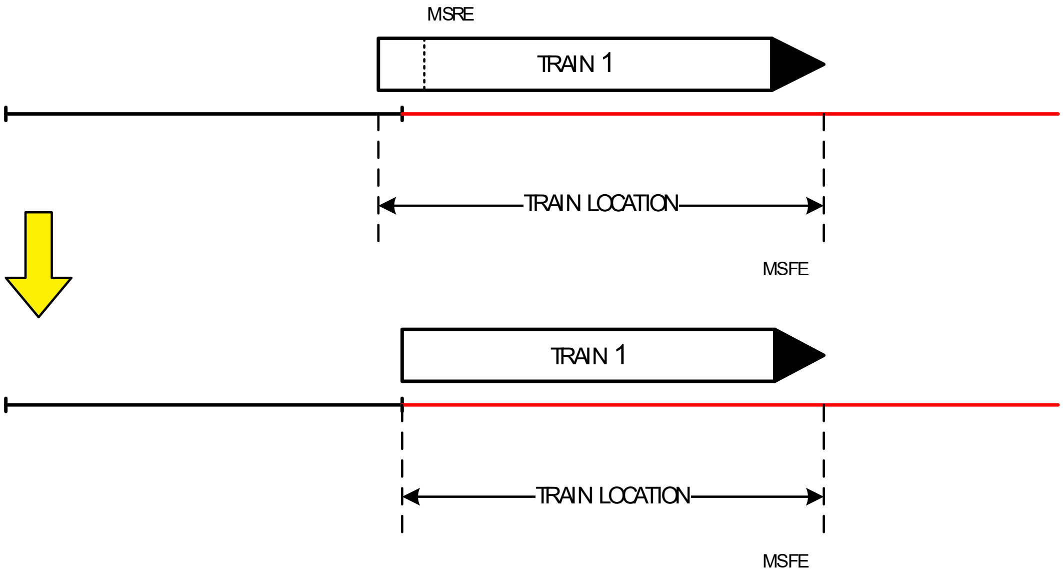


Figure 30: Shortening of rear of *Train Location* due to clear TTD

Figure 31 shows the situation where the Max Safe Rear End is reported within the same Clear TTD section as the Min Safe Rear End, and there is no shortening:

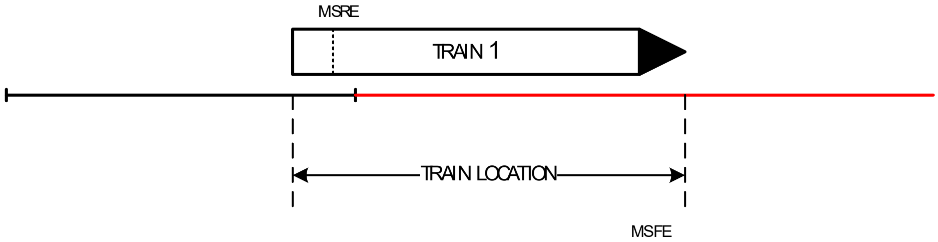


Figure 31: No shortening of rear of *Train Location* due to clear TTD

Operational Rules: None

Engineering Rules: ENG-Generic-4

REQ-TTD-4 FOR FURTHER RELEASE [X2R5 REQ-TTD-4]

For a system using TTD, when using Clear TTD sections to shorten a *Train Location*, the MBS shall ensure that the length of the reduced *Train Location* is not shorter than the length of the train.

Rationale:

Applying shortening should not result in the extent of the remaining *Train Location* being less than the length of the train.

Guidance:

If the application of shortening the *Train Location* results in the length of the *Train Location* being less than the length of the train, it is project specific what alternative action the MBS takes. For example, an application may decide to not apply any shortening to the *Train Location*, or to apply equal shortening to the front and rear.

At boundaries, projects might decide to truncate the *Train Location* and as a result, Train Location could be shorter than length of the train.

Operational Rules: None

Engineering Rules: None

REQ-TTD-5 FOR FURTHER RELEASE [X2R5 REQ-TTD-5]

For a system using TTD, when detecting an expected TTD occupancy within the Movement Permission allocated to a train, after its Mute Timer has expired, the MBS shall extend the *Train Location* of the train up to the closest of:

- the end of the Movement Permission's *Risk Buffer*, OR
- the next boundary of this Occupied TTD section

Rationale:

The MBS can use TTD occupation to extend the *Train Location* of a train where the Mute Timer has expired and is moving along the railway within the Movement Permission allocated to it, thus maintaining the link between the *Train Location* and the train, thereby facilitating recovery if communication is re-established.

Guidance:

A train where the Mute Timer has expired can move forward within the Movement Permission allocated to that train and occupy a previously clear TTD. That occupation can be attributed to a normal train movement. The MBS can adjust the knowledge about where the train might be by extending the *Train Location* of this train.

Figure 32 shows how the *Train Location* is extended within an existing Movement Permission when a train proceeds into a previously clear TTD after a loss of communication.

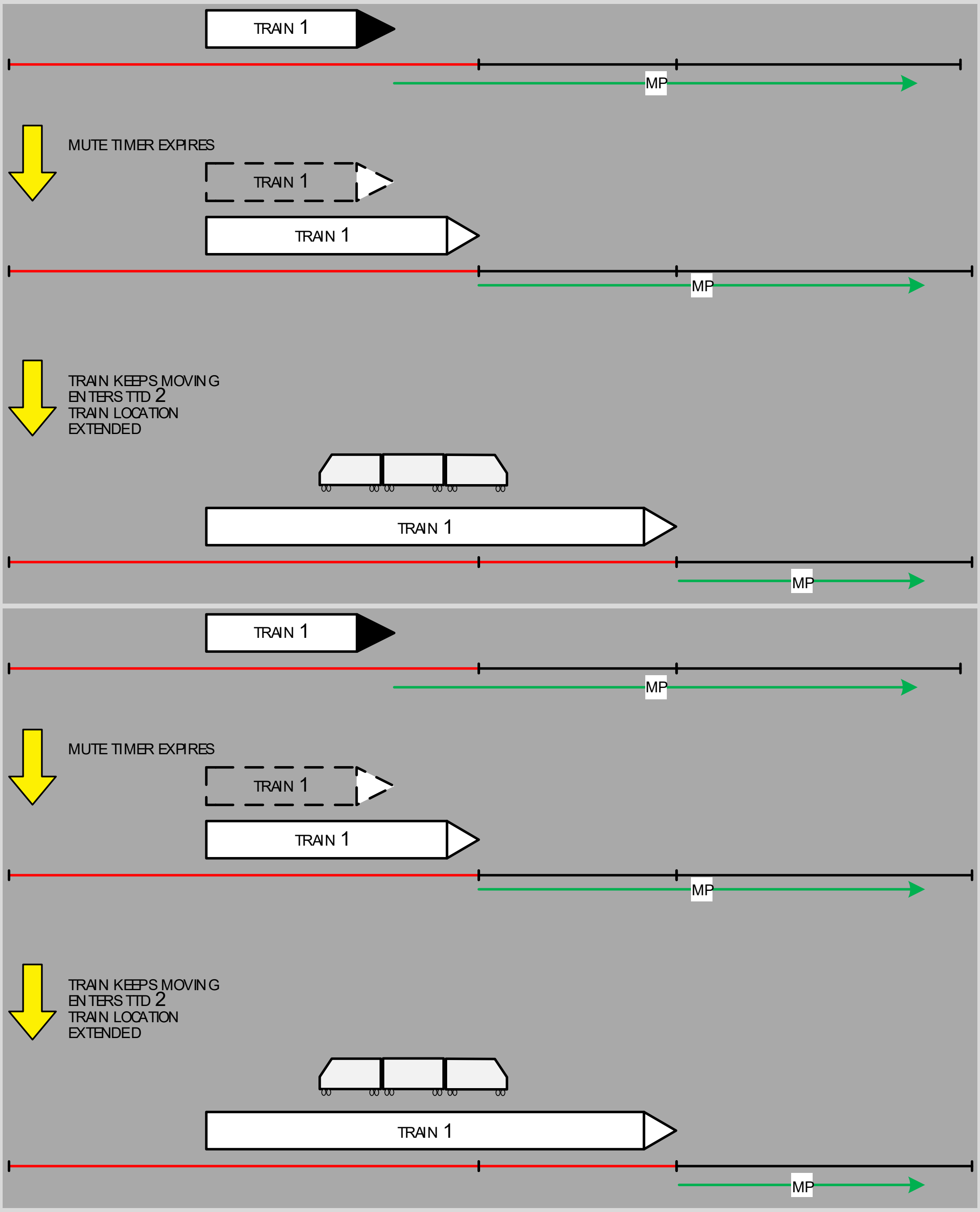


Figure 32 Extension of *Train Location* after Mute Timer has expired by Occupied TTD

Operational Rules:	None
Engineering Rules:	None

REQ-0037 FOR FURTHER RELEASE [X2R5 REQ- LossComms-1]

The MBS shall, if configured, for each train with which it has an active communication session supervise a defined timeout (a Mute Timer) after which the communication with this train is considered lost.

Rationale:

This is to enable the MBS to react faster to the potential loss of communication with an OBU than the timeout in the ETCS specifications. The ETCS specification timer of 5 minutes might be considered too long for some ETCS Level 3 systems.

Guidance:

This Requirement is mandatory if the Mute timer is used.

This is an optional functionality to be defined at application level based on the needs of the system. The value of the Mute timer will be longer than the variable T_NVCONTACT and shorter than the communication session expiry, as defined in [SS026].

Operational Rules: None

Engineering Rules: ENG-LossComms-1

REQ-0038 FOR FURTHER RELEASE [X2R5 REQ-LossComms-2]

When receiving a message from a train and if the use of a Mute Timer is configured, the MBS shall (re-)start the Mute Timer for this train.

Rationale:

This is for the MBS to be able to react if a message from the train is not received within a configured time.

Guidance:

This Requirement is mandatory if the Mute timer is used.

If a Mute Timer is configured it is only active when there is a communication session with the train.

Operational Rules: None

Engineering Rules: ENG-LossComms-1

REQ-0039 FOR FURTHER RELEASE [X2R5 REQ-LossComms-3]

When the Mute Timer expires for a train which has not entered an announced Radio Hole, and which was not reporting in RV mode, then the MBS shall convert the *Train Object* into an *Unresolved Trackbound Object*. The *Unresolved Trackbound Object* area shall correspond to the *Train Location* extended to the end of the Movement Permission or the end of the MA, whichever is shorter.

Rationale:

This is the area where the non-communicating train could be located, and as such needs to be protected.

Guidance:

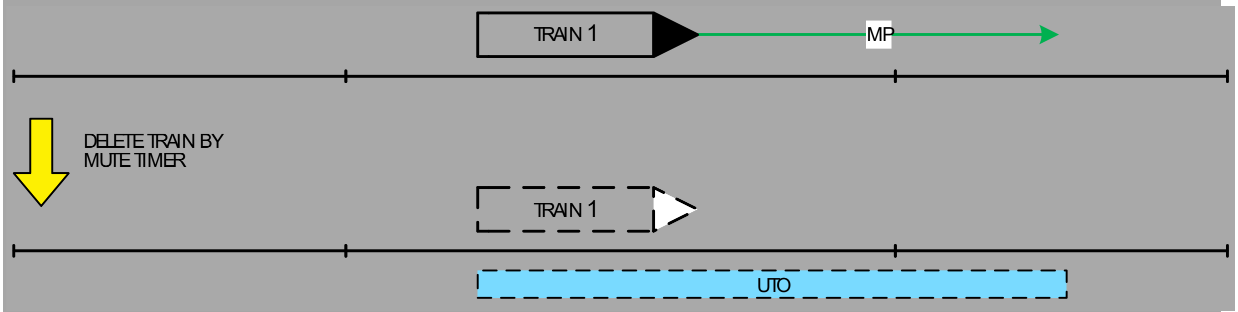
This Requirement is mandatory if the Mute timer is used.

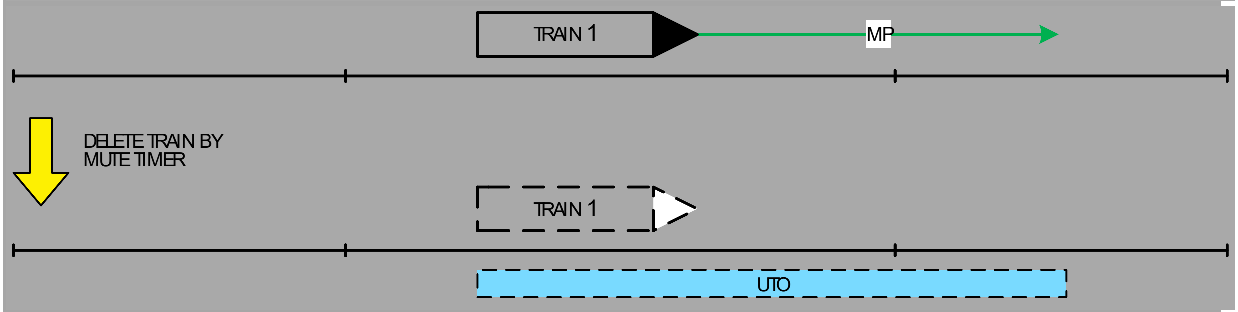
If the extent of the MA sent to the train is less than the Movement Permission, then the extension of the *Unresolved Trackbound Object* may only be to the end of the MA sent to the train.

The criteria for establishing whether a train has entered a Radio Hole are project specific and could include the train having received radio hole track condition information from the MBS.

Once a train is reporting in RV mode, it is not able to move forwards without performing EoM, Start of Mission, so it is not necessary to extend the *Unresolved Trackbound Object* to the end of the Reserved Status Area or MA.

The MBS will maintain the communication session with OBU as active even when the Mute timer has expired until the maximum time to maintain a communication session as specified in SUBSET-026 [BL3 R2] has elapsed.





Operational Rules: None

Engineering Rules: None

6.9.9 Requirements to delete *Train Location* and to create Unresolved Trackbound Object

REQ-0036 FOR FURTHER RELEASE [X2R5 REQ-EoM-4]

The MBS shall be able to cope with differences in the confidence interval provided in the position report of a train that reported EoM even when related to the same train position.

Rationale:

This is due to an ambiguity in the ETCS specifications around how to calculate the *Train Location* accuracy when linking information is deleted due to the change to SB mode.

See REQ-EoM-4

Guidance:

This issue is the subject of CR1318 in the ERA CCM Process [CRProcess]. The MBS must be able to deal with On-boards which have not applied the solution to CR1318.

Operational Rules: None

Engineering Rules: None

REQ-0040 FOR FURTHER RELEASE [X2R5 REQ-LossComms-4]

If the Mute Timer is not considered for use on a particular application, the MBS shall react when the session timer expires by converting the *Train Object* into an *Unresolved Trackbound Object*. The *Unresolved Trackbound Object* shall correspond to the *Train Location* extended to the end of the Movement Permission, except if the train was reporting in RV mode.

Rationale:

This is so that, even for applications not utilising the Mute timer functionality, the Trackside is protected when communications with a train expire according to the existing session expiry timer in the ETCS specifications [BL3 R2].

Guidance:

Whether or not to use the Mute Timer will depend on whether it is required to detect loss of communication before expiry of the session timer. This in turn will depend on traffic density and the typical speed of trains.

Once a train is reporting in RV mode, it is not able to move forwards without performing EoM and Start of Mission, so it is not necessary to extend the *Unresolved Trackbound Object* to the end of the Movement Permission.

For a system using TTD, there may be clear TTDs ahead of the train within the Movement Permission. In this case, the *Unresolved Trackbound Object* can be extended to the least distant position of the next TTD that is clear. This is equivalent to extending the *Unresolved Trackbound Object* up to the end of the MA, in accordance with this requirement, and then clearing those parts in accordance with TTD requirements.

Important note: this requirement assumes that the train is at standstill (or low speed) when the session timer expires.

Operational Rules: None

Engineering Rules: None

/ETCS/

6.9.10 Requirements for train integrity

REQ-0027

When receiving a position report from a train with the information 'Train Integrity is confirmed by External Source', then the MBS shall mark the *Train Object* associated to this train as "integrity confirmed".

Rationale:

When the train is confirmed by External Source, the information about train integrity for the *Train Object* needs to be updated.

Guidance:

None.

Operational Rules: None

Engineering Rules: None

REQ-LossTI-2

When receiving a position report from a train with the information 'Train integrity lost', the MBS shall mark the *Train Object* associated with this train as "integrity not confirmed".

Rationale:

In this situation, the status for the *Train Location* of the train changes to integrity not confirmed, while the extent of the *Train Location* is updated by other requirements, changing the front end from the information in the position report while the rear end is maintained.

Guidance:

None

Operational Rules: None

Engineering Rules: None

REQ-LossTI-7

If the MBS receives Validated Train Data for a train with a train length different from previously reported within the same communication session, then the MBS shall mark the *Train Object* as "integrity not confirmed".

Rationale:

If the train reports loss of Train Integrity because of joining or splitting, then this will already result in the *Train Object* marked as "integrity not confirmed". This requirement is to cover the situation where the new train length is received before the loss of Train Integrity.

Guidance:

When new train data is entered, the OBU will not confirm Train Integrity until the new train data is acknowledged by the MBS. This behaviour is as defined in Change Request 940 [CR940].

Operational Rules: None

Engineering Rules: None

REQ-LossTI-4

The MBS shall mark the *Train Object* as "integrity not confirmed " when 'No train integrity information' is reported longer than a configurable time (Integrity Wait Timer).

Rationale:

This is to provide to other consumers entity as PE the information about the train integrity.

Guidance:

Once Train Integrity is considered Lost by the MBS, the mechanism in REQ-LossTI-2 is applied.

It is application specific whether to implement this function. The timer will have a special value that means the function is disabled.

Note that using this timer the Driver will not be aware of the train Integrity being treated as Lost by the MBS and as such cannot be expected to react in any manner.

If the MBS is configured not to accept Train Integrity confirmed by Driver, and Train Integrity confirmed by Driver is reported, then the MBS will treat this as "No train integrity information".

There is no specific relation between the length of the Mute Timer and the Integrity Wait timer.

Operational Rules: None

Engineering Rules: ENG-LossTI-1

REQ-LossTI-5

When the Integrity Wait Timer is configured, the MBS shall start/restart it with every message from the train with the information 'Train integrity confirmed by external source'.

Rationale:

This is for the MBS to implement an appropriate reaction in case a train does not send a position report with integrity confirmed by external source within the configured time.

Guidance:

The MBS does not start/restart the Integrity Wait Timer when driver confirms integrity.

It is application specific whether to implement the Integrity Wait Timer.

Operational Rules: None

Engineering Rules: ENG-LossTI-1

6.10 SysF Manage Unresolved Trackbound Object

6.10.1 Overview

The MBS must be aware of all parts of the track that are potentially occupied.

- For communicating trains that are localised, the occupancy is managed by the *Train Location* inside *Train Object*. The MBS will create and update a *Train Object* for each communicating train.
- For all other situations, the (potential) occupancy is managed by *Unresolved Trackbound Object*. The MBS will create and update *Unresolved Trackbound Object* in these cases.

An *Unresolved Trackbound Object* may exist for a specific train, but may also exist for another reason, not associated with a specific train.

There are several reasons to create or extend an *Unresolved Trackbound Object*, as shown in Table 12:

Unresolved Trackbound Object Reasons	Notes	Requirements
Reporting train with a shorter value of L_TRAIN	MBS is receiving Train Position Reports, and has also received a new shorter value of L_TRAIN (splitting is assumed). A new UTO is created for the missing length	REQ-TrackStatus-25, REQ-TrackStatus-10
Train is no longer in communication	MBS considers that a train is no longer in communication	REQ-TrainLoc-10 REQ-0040

Unresolved Trackbound Object Reasons	Notes	Requirements
Unresolved Trackbound Object created by MBS at Initialisation	At initialisation of the MBS, the status of the complete Area of Control is unknown	REQ-0028
Unexpected TTD section occupancy	A TTD section is unexpectedly Occupied	REQ-TTD-9, REQ-TTD-10
Unexpected TTD section clearance	A TTD section is unexpectedly Cleared	REQ-TTD-12
UTO propagation	UTO is propagated until the TTD limit or until *Train Location* limit.	REQ-TrainLoc-14, REQ-TrainLoc-15, REQ-TrainLoc-16, REQ-TrainLoc-17

Table 12 – Reasons to create or extend Unresolved Trackbound Object

There are several reasons to remove (even partly) an *Unresolved Trackbound Object*, as shown in Table 13:

Unresolved Trackbound Object Reasons	Notes	Requirements
UTO is replaced by *Train Location*	UTO is removed when it is replaced by the *Train Location* of a (newly) connected train. This is performed if the total recorded length of the UTOs to be replaced is matching the length (L_TRAIN) of the connected train	REQ-TrackStatus-9
UTO is shortened by *Train Location*	UTO is shortened when it is partly replaced by the *Train Location* of a (newly) connected train. This is performed if the recorded length of the UTO is greater than the length of the connected train.	REQ-TrackStatus-10
Sweeping UTO under the train	Remove the part of UTO between the min Safe Front End to the Max Safe Rear End of the train, i.e. under the train	REQ-TrackStatus-12 REQ-TrackStatus-15
Sweeping UTO by train front	Remove the part of UTO from the previous min Safe Front End up to the new min Safe Front End of the train	REQ-TrackStatus-14
Remaining UTO is too small	Remove UTO for which the extent is less than a configurable minimum length	REQ-TrackStatus-19 REQ-TTD-8
Removed by clear TTD	Remove all or part of UTO corresponding to a TTD section which is clear	REQ-TTD-7

Table 13 – Reasons to remove (even partly) Unresolved Trackbound Object

6.10.2 Propagation concept

The concept of propagation is based on the idea that an *Unresolved Trackbound Object* needs to be increased, possibly after a period of time, to allow for the fact that any railway vehicles in the *Unresolved Trackbound Object* area may move without knowledge of the MBS.

Within a signalling system with 100% *Trackside Train Detection* (TTD), any movement which crosses a TTD boundary is likely to be detected (see REQ-TTD-9, REQ-TTD-10, REQ-TTD-12).

In case of loss of communication, the Movement Permission is also considered as a possible envelope for movements of non-reporting vehicles (see REQ-TrainLoc-10).

Without TTD or if the TTD is already occupied, movements of non-reporting rail vehicles will not be detected by the MBS.

For stationary vehicles, the period of time before propagation is applied could be associated with the length of time for which railway vehicle brakes can be expected to remain active, and so keep the vehicle(s) stationary.

Measures are generally put in place at railway project level to prevent or detect and mitigate the risk of rolling vehicles moving such that they conflict with other movements:

- Use of trap points or derailers in station areas and/or sidings
- Use of *Trackside Train Detection* in station areas and/or sidings

If hazard analysis on a particular railway identifies that the remaining risk of unexpected vehicle movement causing a collision is still not acceptable, MBS includes a propagation algorithm within TTD (see REQ-TrainLoc-14, REQ-TrainLoc-15 and REQ-TrainLoc-16) to mitigate this risk.

6.10.3 Storage requirements

REQ-TrackStatus-26 FOR FURTHER RELEASE [X2R5 REQ-TrackStatus-26]

If an *Unresolved Trackbound Object* is created that is within a *Movement Permission* allocated to a train, then the MBS shall react to transition the system to a safe state.

Rationale:

A new *Unresolved Trackbound Object* within a *Movement Permission* allocated to a train may require urgent action from the MBS in order to avoid a hazard.

Guidance:

The specific reaction applied will depend on the scenario and application specific requirements. Possible reactions include shortening of the Movement Authority for another train; sending an Unconditional Emergency Stop to one or multiple trains etc.

Operational Rules: None

Engineering Rules: None

REQ-TrackStatus-27

The MBS shall store and update data for each *Unresolved Trackbound Object* within its Area of Control in accordance with the following table:

Data item	Type or Possible Values	Notes
Extent	Definition of the extent of the *Unresolved Trackbound Object*	The extent of the *Unresolved Trackbound Object*.
Recorded Train Length	As for L_TRAIN	The length of train associated with this *Unresolved Trackbound Object*, if any. Note: this length is not the same as the extent of the UTO.
Train ID	As for NID_ENGINE	The NID_ENGINE of the train associated with this UTO, if any.
Reason	From enumerated list see Table 12.	The reason why the UTO was created. There might be more than one reason.

Table 14 – *Unresolved Trackbound Object* Stored Data

Rationale:

The Stored Data will be used by recovery mechanisms, for example at Start of Mission, recovery after loss of communication, etc.

Stored Information can also aid with initialising the MBS after a restart.

Guidance:

The Train ID stored will be the NID_ENGINE of the train associated with the *Unresolved Trackbound Object*, if any.

There may be more than one reason for an *Unresolved Trackbound Object*.

Stored Data for *Unresolved Trackbound Object* can be used in the following situations:

a) Joining/Splitting: The Length of trains involved in Splitting and Joining is recorded, and the MBS ensures that the full length is accounted for before and after the procedure

b) Start of Mission: Comparing the new train length to the stored train length for an *Unresolved Trackbound Object*, and removing the *Unresolved Trackbound Object* if the train lengths match

c) Recovery after loss of communication (new session): New train length received is compared with that stored to check that it is the same train reconnecting.

The enumerated list of reasons for an *Unresolved Trackbound Object* will include the reasons listed in Table 12.

Operational Rules: None

Engineering Rules: None

REQ-TrackStatus-3 [X2R5 REQ-TrackStatus-3]

When at Start of Mission a *Train Location* has been created for a train with the min Safe Front End located within an *Unresolved Trackbound Object*, then this *Train Location* shall be associated with this *Unresolved Trackbound Object* if the following conditions are fulfilled:

- The min Safe Front End is located inside exactly one *Unresolved Trackbound Object*, and
- There is a recorded train length for this *Unresolved Trackbound Object*, and
- The *Unresolved Trackbound Object* is not associated to any train.

Rationale:

This is to manage the reduction or removal of the associated *Unresolved Trackbound Object* when the train confirms integrity (see for example REQ-TrackStatus-9).

Guidance:

In case there are several UTO overlapping the *Train Location*, it is project specific to decide on which one of them the Train Location shall be associated with, if any.

Operational Rules: None

Engineering Rules: None

6.10.4 Requirements to update Unresolved Trackbound Objects

REQ-TrackStatus-8 FOR FURTHER RELEASE [X2R5 REQ-TrackStatus-8]

The MBS shall alert the PE to the situation if:

- the MBS has updated the *Train Location* for a train, AND
- the rear of the Train has moved backward AND
- there are no adjacent *Unresolved Trackbound Object* where the rear of the train is localised.

Rationale:

If a train has reported new Validated Train Data where the train length has increased, and the increase in length cannot be accounted for by the Recorded Train Length in some adjacent *Unresolved Trackbound Object*, then there may have been an error when updating the length of this or another train, which should be brought to the attention of the PE.

Guidance:

The increase in the train length for the *Train Location* will be because the MBS has received Validated Train Data with an increased value of L_TRAIN.

A train is expected to send Validated Train Data with an increased value of L_TRAIN if it has performed a joining operation. In this case, there should be one or more adjacent *Unresolved Trackbound Object*, where the additional Recorded Train Length(s) can account for the increased train length.

If there are no adjacent *Unresolved Trackbound Object* which can account for the increased train length, then some error has occurred, and the TMS will be alerted.

An inconsistency in the reported length from a train and the length stored by the MBS could be due to an error in the stored data, or failure in the application of Operational Rules. The MBS may decide to take a protective reaction, such as extending an *Unresolved Trackbound Object* to cover the *Train Location*. This reaction is project specific.

Operational Rules: None

Engineering Rules: None

REQ-TrackStatus-9

When Train Integrity is confirmed by External Source for a train associated with an *Unresolved Trackbound Object* and the length of this train (L_TRAIN) is equal to the recorded length of the UTO, then the MBS shall delete the *Unresolved Trackbound Object*.

When Train Integrity is confirmed by External Source for a train associated with an *Unresolved Trackbound Object* and the total recorded length of this UTO plus all other UTOs overlapping this latter matches the length of the train (L_TRAIN), then MBS shall delete all UTOs matching the length of this train.

Rationale:

The *Unresolved Trackbound Object* is “replaced” by the Train Location of the *Train Object* in this case. It is assumed that when a train confirms its train integrity then the MBS can trust the length of this train (L_TRAIN). L_TRAIN matches the real length of the train (considering stretching).

Guidance:

The length of the train could be longer than what is recorded for the *Unresolved Trackbound Object* in case two trains were joined after performing EoM and the joined train is associated with one of two *Unresolved Trackbound Object*.

Projects may decide to allow for some tolerance in matching the length of a train with what is recorded for the *Unresolved Trackbound Object*. In that case, the tolerance can be the configurable minimum length of *Unresolved Trackbound Object*, as defined in ENG-Generic-3. Projects may also decide to check if there is another *Unresolved Trackbound Object* nearby that could explain the new longer Train Length and to alert the TMS if this is not the case.

Figure 33 shows the relationship between *Train Location* and the associated *Unresolved Trackbound Object* for an individual train with Train Integrity, one where the length of the train is the same as that recorded for the *Unresolved Trackbound Object* and one where the length *is* longer (e.g after joining.

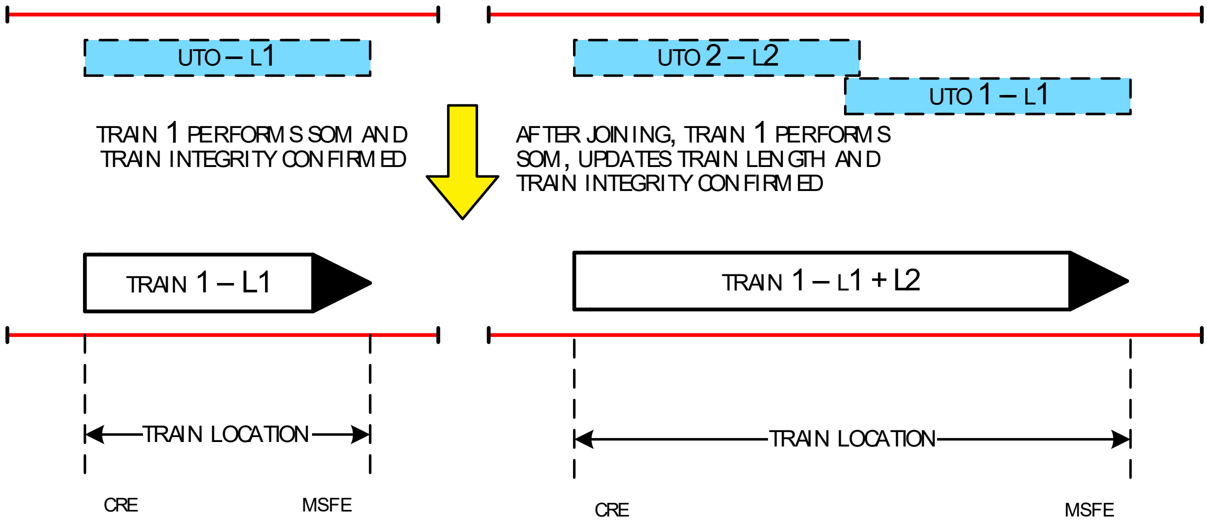


Figure 33: *Train Location* after confirmation of Train Integrity

In the righthand example, there is a step missing when the *Train Location* is updated with the Train Length after receiving Validated Train Data. In the end, when the total length matches the length of the 2 UTOs, the result is the same as in the lefthand figure (i.e. both UTOs are deleted by the established *Train Location*).

Operational Rules: None

Engineering Rules: ENG-Generic-3

REQ-TrackStatus-25

When receiving Validated Train Data from a train indicating that the train length has been decreased, then MBS shall, before applying REQ-TrackStatus-10

- create an Unresolved Trackbound Object from the rear of the *Train Location* (considering the old train length) to the max safe rear end position of the train (considering the new train length)
- associate the *Unresolved Trackbound Object* to this train
- store the old Train Length (L_TRAIN) in the created *Unresolved Trackbound Object* if the train is marked as integrity confirmed,

Rationale:

As the *Train Location* is shortened according to REQ-TrainLoc-6, it is necessary to create an UTO to manage the remaining length of the train that is now unresolved. It is assumed that when a train confirms its train integrity then the MBS can trust the length of this train (L_TRAIN). L_TRAIN matches the real length of the train (considering stretching).

Guidance:

If this is a changed value of L_TRAIN, then the new value of L_TRAIN could be shorter than the previous value, for example after Splitting, as shown in Figure 34.

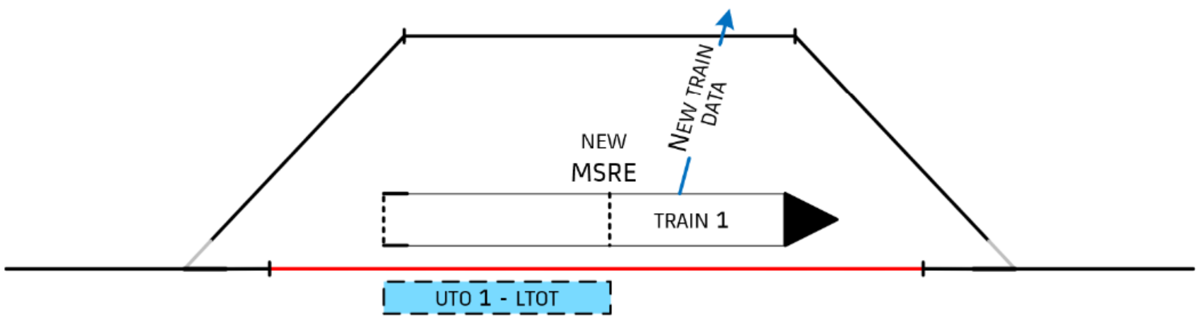


Figure 34: UTO creation when receiving Validated Train Data, L_TRAIN decreased

The created UTO will then be updated according to REQ-TrackStatus-10 (update of the Recorded Length).

Operational Rules: None

Engineering Rules: None

REQ-TrackStatus-10

When Train Integrity is confirmed by External Source for a train associated with an *Unresolved Trackbound Object* and the length (L_TRAIN) of this train is less than the Recorded Train Length, then the MBS shall:

- remove the part of the *Unresolved Trackbound Object* between the Min Safe Front End to the Max Safe Rear End of the train if the front ends do not overlap with the rear ends, AND
- reduce the Recorded Train Length of the remaining *Unresolved Trackbound Object* by the length of the train that confirmed Train Integrity, AND
- dissociate the *Unresolved Trackbound Object* from this train

Rationale:

This is required for the MBS to maintain the *Unresolved Trackbound Object* within its Area of Control when all the train length recorded for an *Unresolved Trackbound Object* is not accounted for by a train confirming integrity.

Guidance:

An *Unresolved Trackbound Object* cannot be fully recovered if the reported train length does not account for all the train length recorded for that area. In this case, the *Unresolved Trackbound Object* must remain with the recorded train length reduced by the length of the train that confirmed integrity.

The extent of the *Unresolved Trackbound Object* will also be reduced because the new *Train Location* will sweep the part of the *Unresolved Trackbound Object* from its Min Safe Front End to the Max Safe Rear End. This could result in this area being split in two, depending on the *Train Location*. In that case the recorded train length is the same for both *Unresolved Trackbound Object*.

Figure 35 shows an example of a train accounting for part of the length recorded for an *Unresolved Trackbound Object* after splitting and that area being split by the train when it confirms integrity. Here, the Front Train After Splitting, train 1 in the figure, confirms integrity and leaves before the rear part has performed SoM. As the train moves away, it sweeps the part of the *Unresolved Trackbound Object* at the front of the train, while the overlapped part at the rear becomes visible.

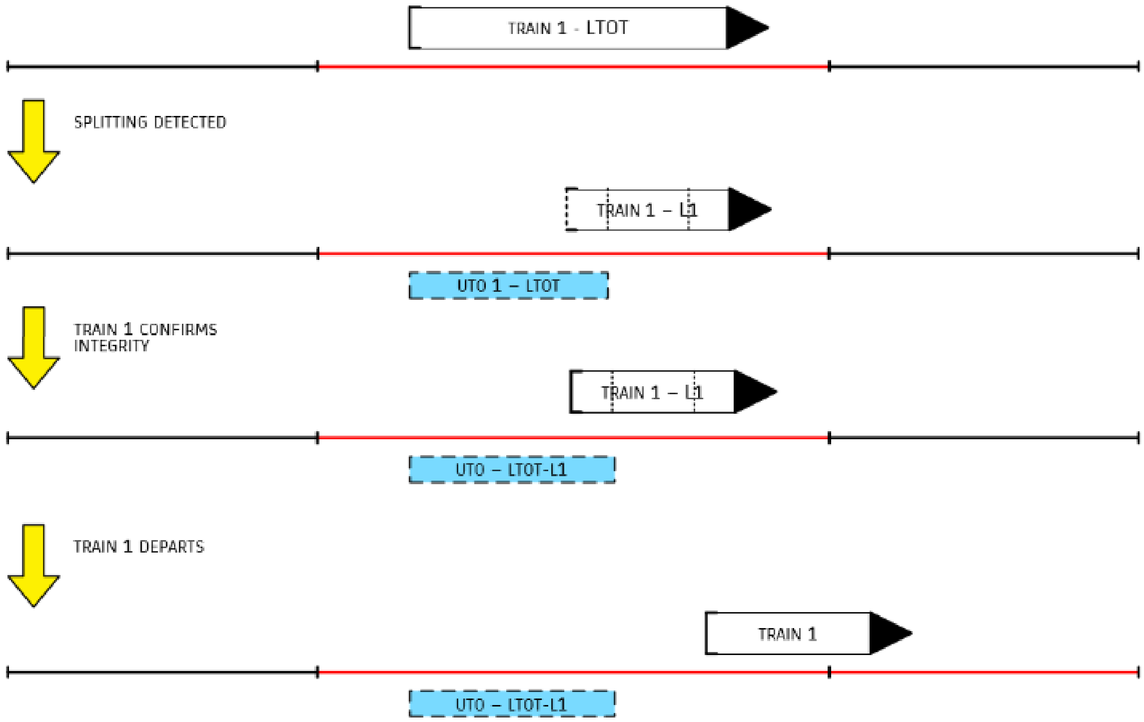


Figure 35: *Unresolved Trackbound Object* remains when Front Train after Splitting leaves

The process above is repeated if another train performs Start of Mission in the remaining *Unresolved Trackbound Object*. After splitting, any end could perform Start of Mission first, but the handling is the same.

Projects may decide to allow for some tolerance in matching the length of a train with what is recorded for the *Unresolved Trackbound Object*. In that case, the tolerance can be the configurable minimum length of *Unresolved Trackbound Object*, as defined in ENG-Generic-3.

Additionally, projects may decide to additionally remove the UTO in front of the train in case the MBS can unambiguously determine that there is no other (part of a) train in front, e.g. by comparing the Train ID from the UTO with the Train ID from the train performing Start of Mission.

Additionally, after splitting, very short UTO may be removed according to requirement TrackStatus-19.

Operational Rules: None

Engineering Rules: ENG-Generic-3

REQ-TrackStatus-11

When an *Unresolved Trackbound Object* is split and this has a Recorded Train Length, then the MBS shall store this length for all *Unresolved Trackbound Object* resulting from this split.

Rationale:

This is to avoid that some train and/or waggons are lost to the MBS when an *Unresolved Trackbound Object* is split.

Guidance:

Unresolved Trackbound Object can be split by a TTD section detected clear or by a train . In some situations, e.g. over a set of points, an *Unresolved Trackbound Object* could even be split in more than two parts.

If the split is due to a train which confirms integrity, this requirement is performed after REQ-TrackStatus-10.

Even if the extents of the split areas are very different, the MBS cannot safely judge if one of them should have more of the recorded length than the other and what that length should be. This is the same situation as if an *Unresolved Trackbound Object* is split by a clear TTD section.

Figure 35Operational Rules: None

Engineering Rules: None

REQ-TrackStatus-12 FOR FURTHER RELEASE [X2R5 REQ-TrackStatus-12]

If the MBS is configured to accept Train Integrity confirmed by Driver, when Train Integrity is confirmed by Driver for a train associated with an *Unresolved Trackbound Object*, and the length (L_TRAIN) of this train is less than the Recorded Train Length of the *Unresolved Trackbound Object*, then the MBS shall:

- reduce the Recorded Train Length of the *Unresolved Trackbound Object* by the length of the train that confirmed Train Integrity

Rationale:

An *Unresolved Trackbound Object* cannot be fully removed if a reported train length does not account for all the Recorded Train Length of that area.

Guidance:

Figure 36 shows an example of a train accounting for part of the length recorded for an *Unresolved Trackbound Object* after splitting when its Driver has confirmed integrity.

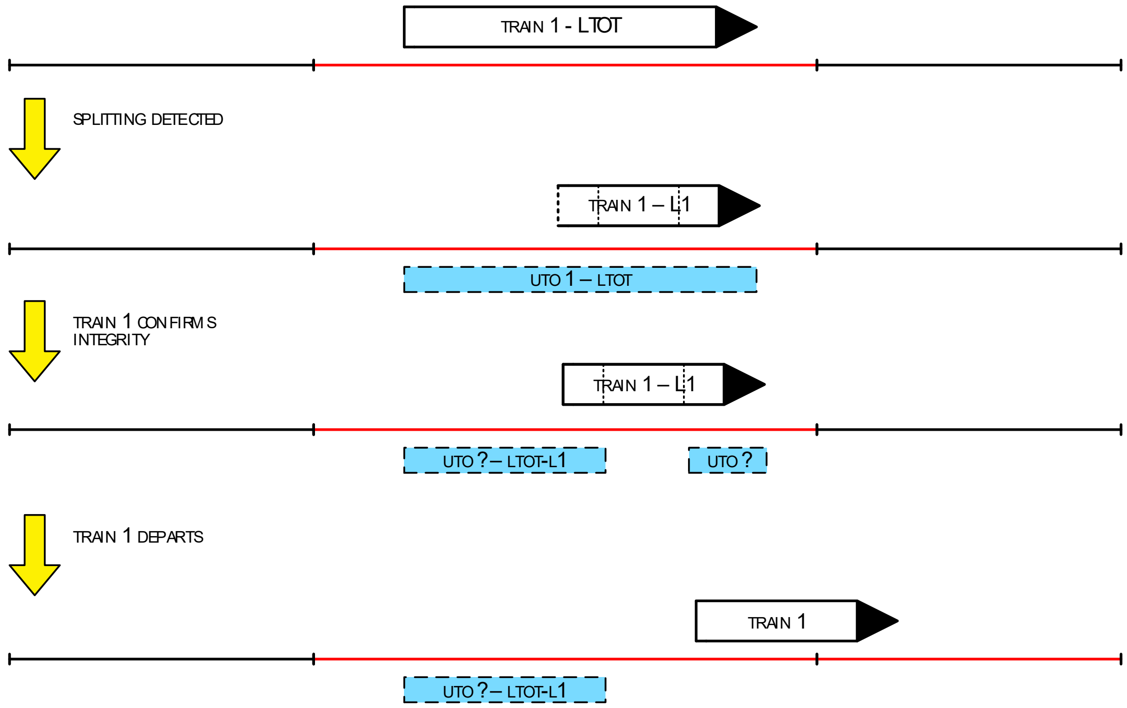


Figure 36: *Unresolved Trackbound Object* updated after integrity confirmed by Driver

Operational Rules: None

Engineering Rules: None

REQ-TrackStatus-13 FOR FURTHER RELEASE [X2R5 REQ-TrackStatus-13]

When Train Integrity is confirmed for a train associated with an *Unresolved Trackbound Object* located within an Activated Temporary Shunting Area, then the MBS shall reduce the Recorded Train Length of the *Unresolved Trackbound Object* associated with the Shunting Area by the length of the train that confirmed Train Integrity.

Rationale:

This is required for the MBS to maintain the Track Status within its Area of Control.

Guidance:

If all the train length recorded for an Active Shunting Area is accounted for when the area is deactivated, then the *Unresolved Trackbound Object* that was associated with the Shunting Area can be removed, else it will remain but be Sweepable.

Operational Rules: None

Engineering Rules: None

REQ-TrackStatus-14

When the front of the train has passed a part or all of an *Unresolved Trackbound Object* that existed before the *Train Location* was updated, then the MBS shall reduce that *Unresolved Trackbound Object* for the part of it from the previous min Safe Front End up to the new min Safe Front End of the train.

Rationale:

This is to enable sweeping of the area passed between received position reports.

Guidance:

Sweeping is performed by the Min Safe Front End (mSFE) of a train, as it cannot be guaranteed that there is no obstruction between the mSFE and the Max Safe Front End (MSFE) which is the Confidence Interval where the front of the train can be.

Figure 37 shows the sweeping by *Train Location* for a train with Train Integrity confirmed in a *Sweepable Unresolved Trackbound Object* ahead of the train.

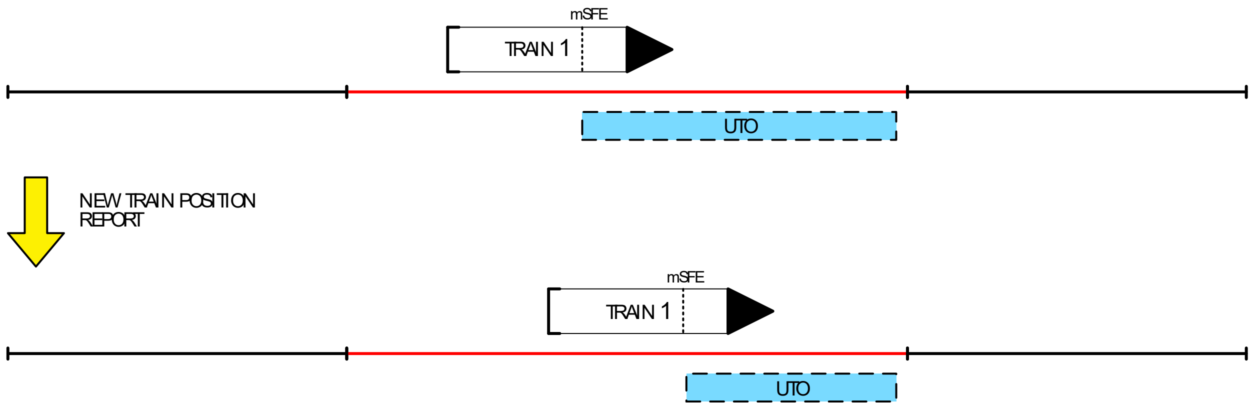


Figure 37: Train with Train Integrity confirmed Sweeping an *Unresolved Trackbound Object*

Figure 38 below shows a train having passed a sweepable *Unresolved Trackbound Object* between a new and the previous *Train Location*. The train sweeps that *Unresolved Trackbound Object*.

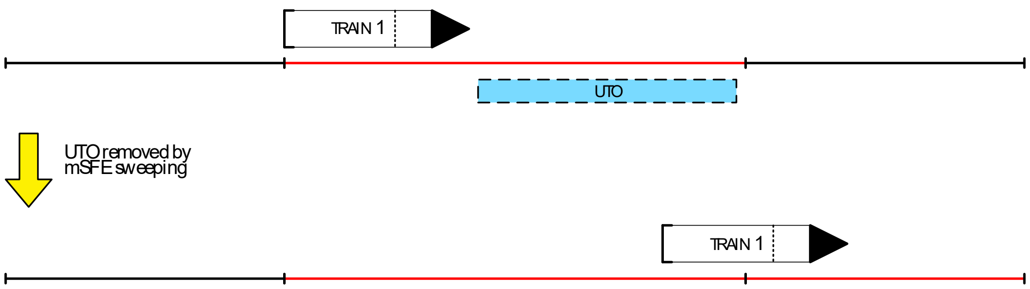


Figure 38: Existing *Unresolved Trackbound Object* swept by a passing train

The passage of a train through a Sweepable *Unresolved Trackbound Object* sweeps that *Unresolved Trackbound Object*.

Sweeping will not be applied when a train reports in RV. A reversing train will not sweep *Unresolved Trackbound Object*. However, the Max Safe Front end is updated as the train reports while reversing.

Operational Rules: None

Engineering Rules: None

REQ-TrackStatus-15

When a *Train Location* is updated and this train has passed a part or all of an *Unresolved Trackbound Object* that did not exist before the *Train Location* was updated, then the MBS shall reduce that *Unresolved Trackbound Object* for the part of it between the Min Safe Front End and the Max Safe Rear End of the train.

Rationale:

This is to enable (partial) sweeping of an *Unresolved Trackbound Object* that was created between received position reports.

Guidance:

Sweeping is performed by the Min Safe Front End (mSFE) of a train, as it cannot be guaranteed that there is no obstruction between the mSFE and the Max Safe Front End (MSFE) which is the Confidence Interval where the front of the train can be.

A hazardous situation may arise if an *Unresolved Trackbound Object* is swept by a train if this *Unresolved Trackbound Object* was created only after the train had passed it.

Figure 39 below shows a train having passed a Sweepable *Unresolved Trackbound Object* between a new and the previous *Train Location*. As the area did not exist before the *Train Location* was updated, it only sweeps that *Unresolved Trackbound Object* from the new min Safe Front End and the new Max Safe Rear End of the train.

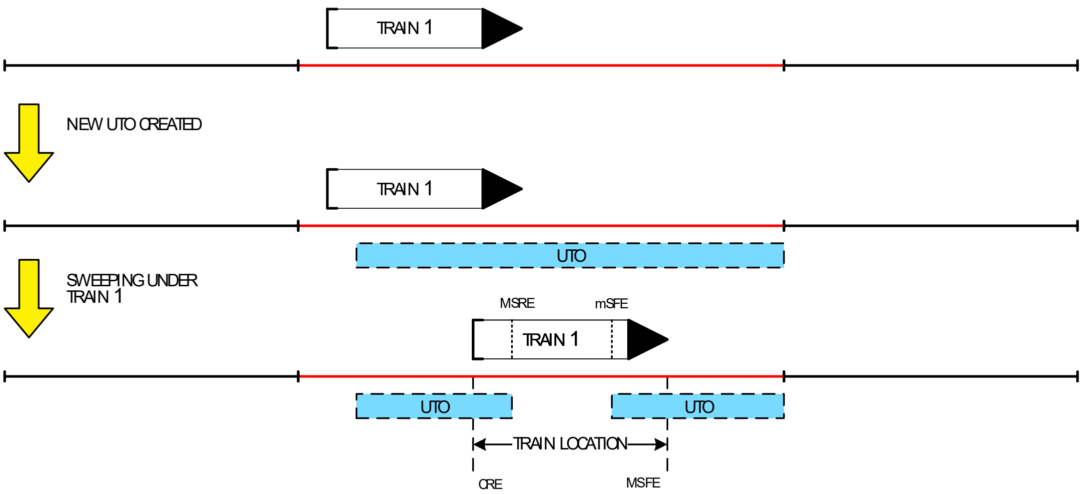


Figure 39: New *Unresolved Trackbound Object* swept by a passing train

Operational Rules: None

Engineering Rules: None

REQ-TrackStatus-16 FOR FURTHER RELEASE [X2R5 REQ-TrackStatus-16]

When the MBS considers the communication session with a train is terminated, the MBS shall convert the *Train Location* to an *Unresolved Trackbound Object*, except if the train is completely located inside an Active Shunting Area.

Rationale:

This is the area where the train could be located, and as such needs to be protected by an *Unresolved Trackbound Object*.

Guidance:

This requirement applies at EoM for trains not inside an Active Shunting Area.

For a train located completely inside an Active Shunting Area, there is no need for an *Unresolved Trackbound Object* since there is already an *Unresolved Trackbound Object* associated with the Active Shunting Area which will protect the train.

If a train is partially located inside an Active Shunting Area, it is project specific whether the MBS authorises the transition to Shunting Mode. Similarly, it is project specific how the MBS subsequently manages the overlapping *Unresolved Trackbound Object* that is created for the location of this train.

For a train leaving the MBS Area, another requirement deals with the relevant *Unresolved Trackbound Object* that could be removed when the train has left the area, i.e. before the communication session has been terminated.

Loss of communications is handled by other requirements.

Operational Rules: None

Engineering Rules: None

6.10.5 Removing an Unresolved Trackbound Object

REQ-TrackStatus-19

The MBS shall automatically remove *Unresolved Trackbound Object* for which the extent is less than or equal to a configurable minimum length.

Rationale:

This is to avoid having small *Unresolved Trackbound Object* that have to be swept when it is known that there cannot be a vehicle inside them.

Guidance:

Small *Unresolved Trackbound Object* could arise from splitting and joining procedures, or from sweeping.

For example, this requirement could apply to cross-over areas, as in Figure 40:

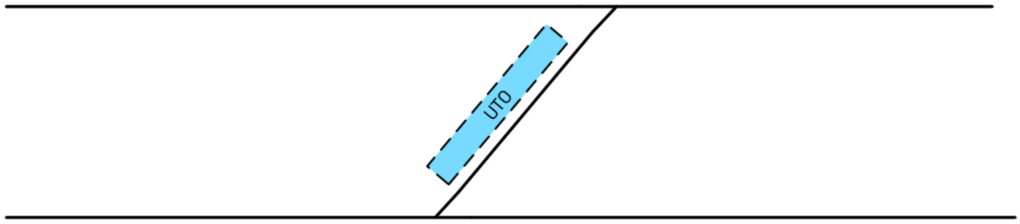


Figure 40: Short *Unresolved Trackbound Object* at crossover

The configurable minimum length could be related to the length of the shortest vehicle that could be running on the line. The *Unresolved Trackbound Object* can be removed, regardless of the status of adjacent areas.

In case an *Unresolved Trackbound Object* is split in two, e.g. by a clear TTD section, and if one of these areas is shorter than the configured minimum distance, then it can be removed even if it has a Recorded Train Length because that length is also recorded in the other area. Thus, there is no risk of trains and/or waggons becoming lost.

Operational Rules: None

Engineering Rules: ENG-Generic-3

6.10.6 Impact from TTD on Unresolved Trackbound Objects

REQ-TTD-7

For a system using TTD, the MBS shall remove all or part of a Unresolved Trackbound Object, corresponding to a TTD section which is Clear.

Rationale:

TTD information can be used to clear the track under degraded situations.

Guidance:

TTD can assist with recovery as there is no need to sweep clear TTD sections.

Only the part of the Unresolved Trackbound Object corresponding to the Clear TTD section can be removed according to this requirement. This might mean that part of the Unresolved Trackbound Object may remain.

Operational Rules: None

Engineering Rules: None

REQ-TTD-8

For a system using TTD, if the MBS has shortened the extent of an *Unresolved Trackbound Object*, then the MBS shall ensure the resulting *Unresolved Trackbound Object* is not shorter than the Recorded Train Length stored for it.

Rationale:

Applying shortening could result in the extent of the remaining Unresolved Trackbound Object being less than the Recorded Train Length.

An *Unresolved Trackbound Object* with an extent shorter than the stored train length could represent a hazard.

Guidance:

When the application of shortening the *Unresolved Trackbound Object* results in the length of the *Unresolved Trackbound Object* being less than Recorded Train Length, it is project specific what alternative action the MBS takes. For example, an application may decide to not apply any shortening to the *Unresolved Trackbound Object*, or to apply equal shortening to the front and rear whilst maintaining the length of the Recorded Train Length.

If an *Unresolved Trackbound Object* is one part of an Unresolved Trackbound Object which has been split, for example by a clear TTD, then project-specific rules may be needed, as the Recorded Train Length will be recorded in two Unresolved Trackbound Objects; see REQ-TrackStatus-11.

Operational Rules: None

Engineering Rules: None

REQ-TTD-9

For a system using TTD, when detecting a TTD occupancy not associated with any expected train movement, the MBS shall create a Unresolved Trackbound Object for that TTD section (if there is not UTO to be extended from the next TTD according to requirement REQ-TTD-10).

Rationale:

A TTD occupancy not associated with any expected train movement should be considered a potential hazard.

Guidance:

Unexpected TTD occupancy also includes a TTD remaining Occupied when it might be expected to become Clear. For example, a TTD remaining Occupied behind a train which has sent a Train Position Report which gives a position clear of the TTD might indicate the presence of a Ghost Train. Implementation of such a function is project-specific and will likely require the use of a timer to compensate for the latency between Train Position Reports and TTD inputs.

If the TTD section is a short TTD section protecting a boundary of the MBS Area of Control, then projects may decide to create a larger Unresolved Trackbound Object if the TTD becomes unexpectedly occupied. This would require engineering, to determine the size of the Unresolved Trackbound Object to be created if the short boundary TTD becomes unexpectedly occupied.

There are other requirements relating to reactions for expected TTD occupancy.

Operational Rules: None

Engineering Rules: None

REQ-TTD-10

For a system using TTD, when detecting a TTD occupancy not associated with any movement permission and adjacent to a TTD containing an existing Unresolved Trackbound Object which has a Recorded Train Length greater than zero, the MBS shall extend the Unresolved Trackbound Object up to the next boundary of this TTD section.

Rationale:

A TTD occupancy not associated with any expected train movement should be considered a potential hazard.

Guidance:

A train which is not communicating can move and occupy a previously clear TTD. That occupation can be attributed to the train in the adjacent TTD. The MBS can adjust the knowledge about where the train might be by extending the existing Unresolved Trackbound Object.

Unexpected TTD occupancy also includes a TTD remaining Occupied when it might be expected to become Clear. For example, a TTD remaining Occupied behind a train which has sent a Train Position Report which gives a position clear of the TTD might indicate the presence of a Ghost Train. Implementation of such a function is project-specific and will likely require the use of a timer to compensate for the latency between Train Position Reports and TTD inputs.

There are other requirements relating to reactions for expected TTD occupancy.

Operational Rules: None

Engineering Rules: None

REQ-TTD-11 FOR FURTHER RELEASE [X2R5 REQ-TTD-11]

For a system using TTD, on request from the TMS, the MBS shall be able to remove an Unresolved Trackbound Object caused by a faulty TTD.

Rationale:

This will allow the MBS to help restore normal operation on the line.

Guidance:

This function could be used to improve the reliability of the system and overrule false occupation reported by TTD (e.g. malfunctioning axle counters).

In MBS operations, when all train movements are supervised by OBU with train position reporting and train integrity confirmation, a faulty TTD could be detected, e.g. dependent on the states of the neighbouring TTDs and position reports.

The implementation of this requirement will need to prevent a new Unresolved Trackbound Object being created whilst the TTD remains Occupied.

Operational Rules: OPE-Generic-1, OPE-Generic-2

Engineering Rules: ENG-Generic-7

REQ-TTD-12

For a system using TTD, when detecting a TTD clearance which cannot be associated with any regular train movement or *Train Location*, the MBS shall create an *Unresolved Trackbound Object* for each adjacent area if the adjacent area is not completely covered by UTO, or is known as cleared (by TTD if available).

Rationale:

A TTD clearance which cannot be associated with any regular train movement or *Train Location*, should be considered a potential hazard, as such the MBS needs to protect other train movements by either creating or extending Unresolved Trackbound Objects.

Guidance:

A TTD becoming unexpectedly clear might be due to several reasons. For example, a non-communicating train is moved such that the TTD becomes clear.

The MBS must react, for example by creating an additional Unresolved Trackbound Objects to protect the movement of trains.

Figure 41 shows the creation of Unresolved Trackbound Objects adjacent to a Clear TTD which has become unexpectedly Clear.

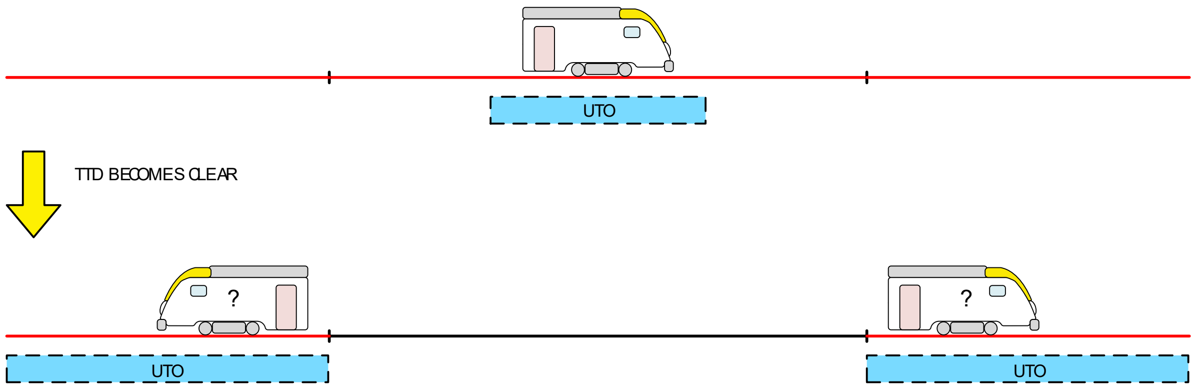


Figure 41: Creation of *Unresolved Trackbound Object* for unexpected Clear TTD

Projects should consider the impact of creation of the *Unresolved Trackbound Object* on railway operations.

Depending on the implementation, project-specific engineering rules may be required.

Operational Rules: None

Engineering Rules: None

REQ-TrainLoc-14

When the propagation timer of a UTO expires, the MBS shall extend the UTO in both directions:

- until the TTD section limit, or
- until the first Max Safe Rear End location found from the UTO to the TTD limit applicable in the same direction, or
- until the first Min Safe Front location found from the UTO to the TTD limit applicable in the opposite direction.

Rationale:

Due to the presence of a UTO, uncontrolled movements are possible inside the occupied TTD section, the UTO is then extended to the TTD limit or the first found *Train Location* (see chapter 6.10.2). Uncontrolled movements outside the currently occupied TTD are managed by other requirements.

Guidance:

The propagation time is configurable at Project level.

If the propagation time is set to 0, the propagation is performed immediately.

If the propagation time is set to the specific value “infinite”, the propagation is never performed.

Figure 42 below shows the propagation of the UTO when the propagation timer expires and a train is present in the same direction.

The UTO will be propagated every time the train 1 moves forward.

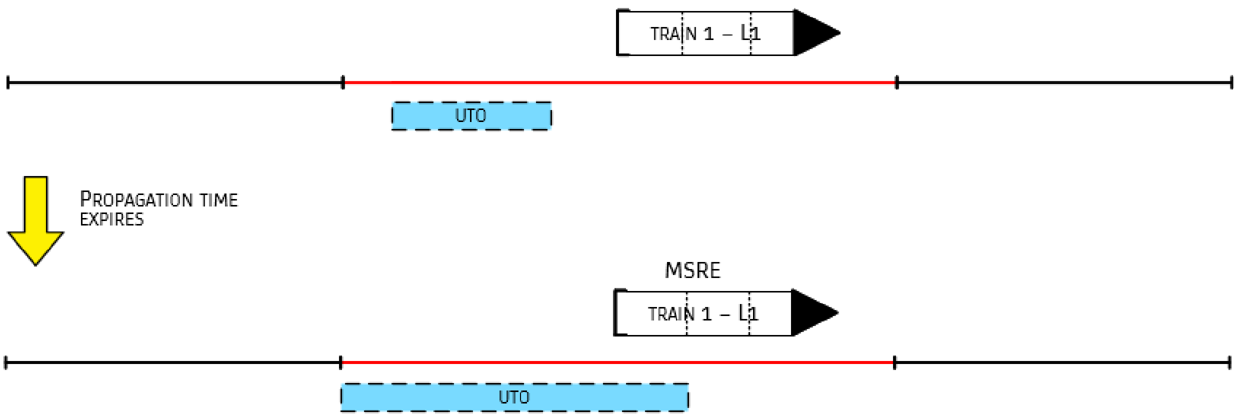


Figure 42: UTO propagation with a train in the same direction.

Figure 43 below shows the propagation of the UTO when the propagation timer expires with the presence of a train in the opposite direction.

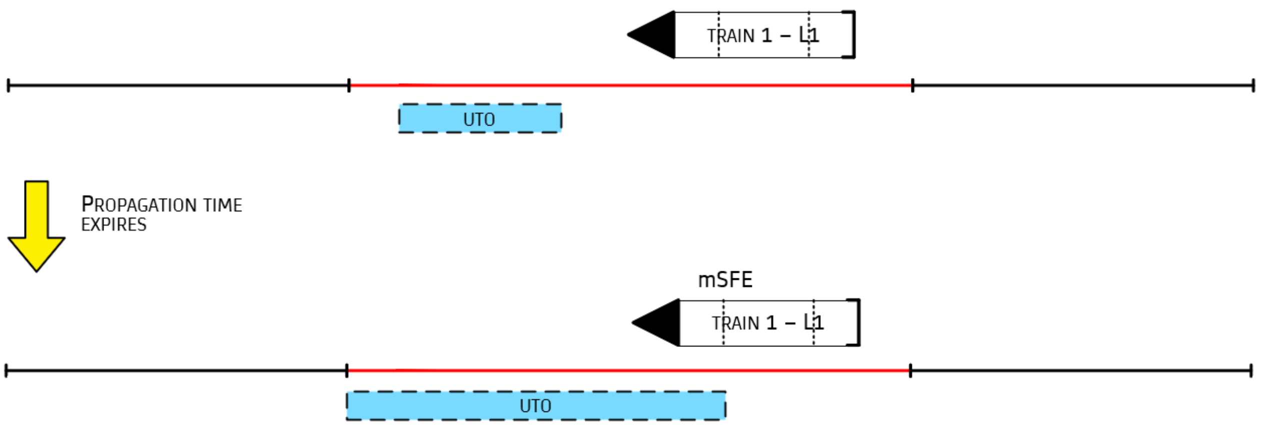


Figure 43: UTO propagation with a train in the opposite direction.

Operational Rules: None

Engineering Rules: None

REQ-TrainLoc-17

After the propagation timer of a UTO has expired, if the UTO is terminated at a Max Safe Rear End location of a Train Location, when this train moves, the MBS shall update the extent of the UTO to closest of:

- the new Max Safe Rear End location of the train, or
- the TTD limit.

Rationale:

When UTO has been propagated to the rear of a train according to REQ-TrainLoc-14, the UTO is propagated every time the train moves, until the rear of the train has passed the TTD limit.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-TrainLoc-15

When a *Train Object* is marked as “integrity not confirmed” for more than a given propagation time, then MBS shall create a UTO associated to this train from the Max Safe Rear End of the train up to the next TTD limit in reverse direction.

Rationale:

Due to the *Train Location* with integrity not confirmed, an uncontrolled roll-away movement is possible inside the occupied TTD section. A UTO is then created to the TTD limit. Uncontrolled movement outside the current occupied TTD are managed by other requirements. Max Safe Rear End is considered here according to splitting scenario.

Guidance:

Figure 44 below shows the creation of the UTO for a non-integer train when the propagation time expires

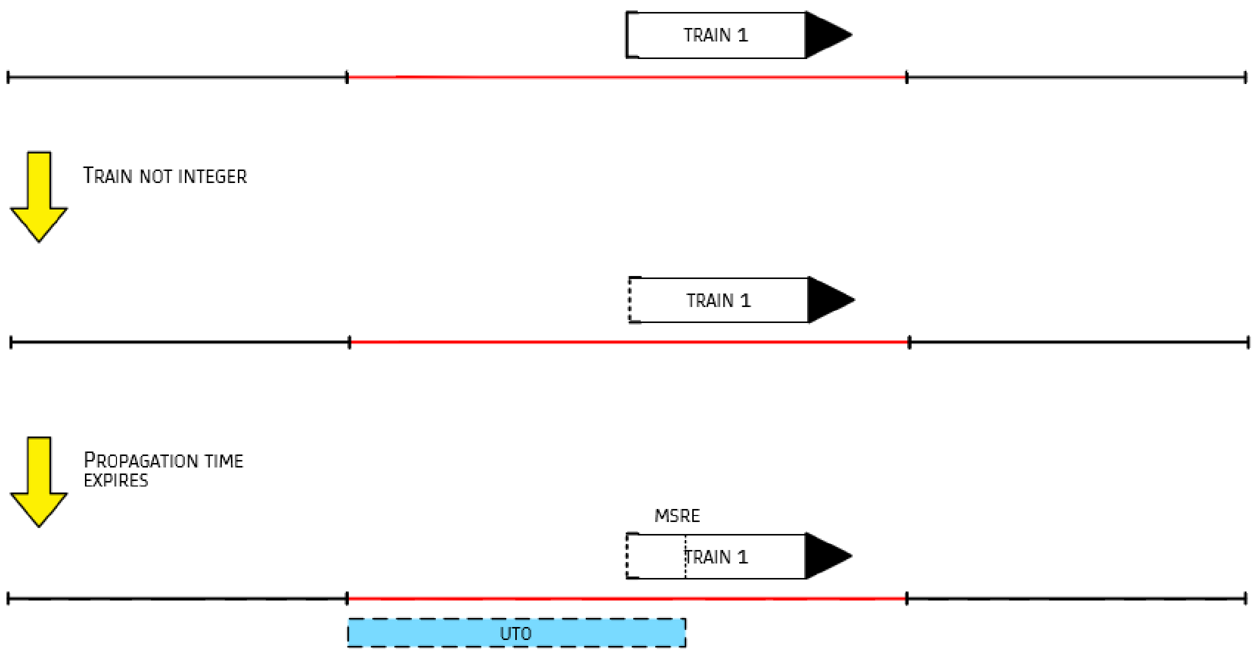


Figure 44: UTO creation for a non-integer train.

Operational Rules: None

Engineering Rules: None

REQ-TrainLoc-16

Once a UTO has been created according to requirement REQ-TrainLoc-15, the propagation time shall be considered as expired for this UTO.

Rationale:

Any movement of the train in front of the UTO should extent the current UTO by propagation immediately according to requirement REQ-TrainLoc-14.

Guidance: None

Operational Rules: None

Engineering Rules: None

6.10.7 Requirements related to Operator panel – FOR FURTHER RELEASE

REQ-TrackStatus-22 [X2R5 REQ-TrackStatus-22]

On request from the PE/Operator panel, the MBS shall create an *Unresolved Trackbound Object* flagged as Sweepable provided the area is longer than the configurable minimum length.

Rationale:

This is to allow the MBS to have all relevant information concerning obstructions.

Guidance:

For example, this can be used in the degraded situation of a non-communicating train. A train without communications has to be moved inside an *Unresolved Trackbound Object*, so that the MBS is aware that this area is protected for a specific train.

The *Unresolved Trackbound Object* may be created automatically by the TMS, or via dispatcher interaction with the TMS or Operator Panel.

Unresolved Trackbound Object can be created independently.

The Sweepable *Unresolved Trackbound Object* needs to be longer than the configurable minimum length for removal of Unresolved Trackbound Object, as defined in ENG-Generic-3.

Operational Rules: OPE-TrackInit-2; OPE-Generic-7; OPE-LossComms-1; OPE-LossTI-1

Engineering Rules: ENG-Generic-3

REQ-TrackStatus-23 [X2R5 REQ-TrackStatus-23]

On request from the PE/Operator Panel, the MBS shall create an *Unresolved Trackbound Object* flagged as Non-Sweepable.

Rationale:

When the PE/Operator Panel requests a Non-Sweepable *Unresolved Trackbound Object*, it may be for a reason that would make it unsuitable to be swept e.g. a known permanent obstacle on the line.

Guidance:

Non-Sweepable *Unresolved Trackbound Object* will only be cleared at the request of the TMS. The MBS will retain a Non-Sweepable *Unresolved Trackbound Object* after traversal by a train which has confirmed Train Integrity.

Unresolved Trackbound Object can be created independently, i.e. they can overlap existing *Unresolved Trackbound Object* or *Train Location*.

For example, creating *Unresolved Trackbound Object* in parts of the track might be due to external systems detecting fallen objects, or landslides.

Operational Rules: OPE-TrackInit-2, OPE-Generic-7; OPE-LossComms-1; OPE-LossTI-1

Engineering Rules: None

REQ-TrackStatus-24 [X2R5 REQ-TrackStatus-24]

On request from the PE/Operator Panel, the MBS shall remove, reduce or extend *Unresolved Trackbound Object*.

Rationale:

MBS must allow the TMS to remove, reduce or extend *Unresolved Trackbound Object* based on the result of operational procedures.

Guidance:

An *Unresolved Trackbound Object*, both Sweepable and Non-Sweepable, can be removed, reduced or extended by the PE/Operator Panel.

For example, some Infrastructure Managers may permit *Unresolved Trackbound Object* to be removed or reduced based on the observations of a Driver sweeping on an adjacent line.

Projects may, if providing the necessary information, allow the Dispatcher via PE/Operator Panel to remove or reduce parts of an *Unresolved Trackbound Object*, e.g. by stating a certain length to be removed.

In case there is a train length stored for an *Unresolved Trackbound Object* requested for removal, it is recommended that the MBS prevents removing this *Unresolved Trackbound Object* unless the removal is supported by some additional measure(s).

Robust operational procedures are required in order to permit the Dispatcher, via the PE/Operator Panel, to remove or reduce *Unresolved Trackbound Object*.

In case of overlapping *Unresolved Trackbound Object* conditions might be considered when removing an *Unresolved Trackbound Object*.

If the *Unresolved Trackbound Object* is Sweepable, the MBS will remove it if it is reduced to a length shorter than the configurable minimum length for removal of *Unresolved Trackbound Object*, as defined in ENG-Generic-3.

Operational Rules: OPE-Generic-2, OPE-Generic-7

Engineering Rules: None

6.11 SysF Authorise MP Request

6.11.1 Overview

This function is responsible to assess the safety of a request to alter the Authorisation of a *Train Object*. PE or the operator through the operator panel can request an Authorisation through the SCI-CMD interface which is then checked by MBS if it violates any safety constraint. The MBS shall not alter the request if certain parameters are incorrect (e.g. The operating state has changed during the message transmission between PE and MBS) but only report the failure to PE with the failure reason.

The MP Request shall contain the following information:

- *Train Object* Identifier
- Movement Permission

The Movement Permission shall have the following attributes

- *Risk Buffer* (LinkedPath)
- Extent (LinkedPath)
- Requested Maximum Speed in km/h (LinkedPath per different speed)
- ETCS Movement Mode (Linked Path per different mode)
- List of DPS Groups that must not be used as flank protection measure

6.11.1.1 Flank Protection Overview

Before authorizing an MP request, MBS evaluates if sufficient protections to limit the risk of side-on collision according to the safety analysis are in observed between the requested MP and any uncontrolled trackbound movement.

To find the flank protecting measures applicable to the MP request, MBS builds *Risk Path* Candidates that span from the end of the *Allocation Sections* up to the corresponding elements providing (or not) flank protection (see requirement REQ-RP_SEARCH).

Note: once a risk path has been created, it may also be updated/deleted without the reception of a new MP request (e.g. when a train is moving) through a continuous evaluation (see chapter 6.18).

For each *Risk Path* Candidate that has been built (according to REQ-SC_RP_SEARCH), the MBS evaluates if the *Risk Path* is correctly terminated (according to REQ-SC_RP_TERM) on an element authorised to provide flank protection.

The elements than can provide flank protections include:

- **Switchable Track element**

  Examples: point from trailing side, derailer/catch point, end of track, etc.

  The position of these points ensures that any uncontrolled trackbound movement approaching the side of the Movement Permission will be deviated or derailed.

- **Movement Permission**

The side of the Movement Permission is protected by another train supervised by a Movement Permission. As the ETCS on-board unit of the other train supervises the train movement, this reduces the risk that the train will exceed its authority to an extent that could result in a flank collision

- ***Train Object***

  The side of the Movement Permission is protected by another connected train. If the on-board unit guarantees that the train will not move without any authority, it is ensured that this train will not perform any movements that could result in a flank collision.

- **Protection by a sufficient distance**

  The side of the Movement Permission is detected as free over a sufficient distance to mitigate the risk a flank collision to an acceptable level.

- **Protection by Operational Rules**

  If the risk of flank collision cannot be mitigated by the preceding measures, the final option is to reduce the potential consequences of a flank collision if Operational Rules (vehicle should not be moved without permission) are violated.

  This imposes a reduced speed.

It is possible to configure within the MBS *Domain Data* the appropriate flank protection measures to be safely verified by the MBS according to Table 15.

Flank Protection by	Termination Requirement SC-RP_TERM_	Variable	Scope	Type	Description
Search Options	--	*fpSearch*	**G**	**BOOL**	TRUE if Flank Protection is required
		fpSearchOnDependentAs	**AS**	**BOOL**	TRUE if the dependent *Allocation Section* needs Flank Protection
		rpMaxSearchDistance	**G**	**UINT**	The length in meters after which the *Risk Path* search is finished
Switchable Track Element	DPS	*rpTermAtDpsOnly*	**AS**	**BOOL**	TRUE if a *Risk Path* originating at this *Allocation Section* can only be terminated at a DPS
		dps*ProvidesFlankProtection*	**DPS**	**BOOL**	TRUE if this DPS can provide flank protection
		dps*MaxFlankProtectionSpeed*	**DPS**	**UINT**	Speed in km/h up to which this DPS can provide Flank Protection
Movement Permission	RB MP	rpTermAllowedAtRbAndMp	**G**	**BOOL**	TRUE if Risk Paths terminated at a Movement Permission Extent or Risk Buffer can be used as a flank protection measure.
Train Object	TO	rpTermAllowedAtTo	**G**	**BOOL**	TRUE if Risk Path terminated at a Train Object can be used as a flank protection measure.

Flank Protection by	Termination Requirement SC-RP_TERM_	Variable	Scope	Type	Description
Sufficient Distance	DIST	*rpTermAllowedAfterMaxDistance*	**G**	**BOOL**	TRUE if Risk Path terminated after a defined search distance given in rpMaxSearchDistance can be used as flank protection measure.
Operational Rules (UTO found)	UTO	rpTermAllowedAtUto	**G**	**BOOL**	TRUE if Risk Path terminated at an Unresolved Trackbound Object can be used as flank protection measure.
		rpTermMaxSpeedUto	**G**	**UINT**	Max Speed for a Movement Permission at the *Allocation section* if a *Risk Path* originating from it terminates at a Unresolved Trackbound Object.

Table 15 – Flank Protection measures configuration

G = Global

AS = Configurable at every *Allocation Section*

DPS = Configurable at every *Drive Protection Section*

UINT = Unsigned Integer

BOOL = Boolean value (TRUE, FALSE)

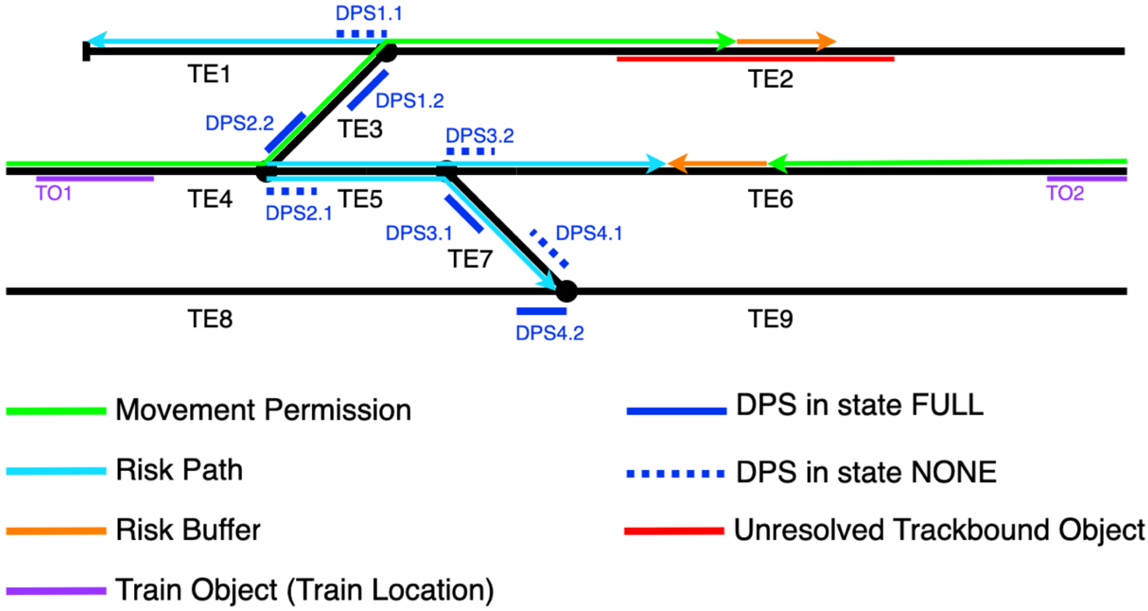
In tracks (usually secondary tracks) where non-controlled movements can occur (shunting, stabling of vehicles with remaining rollaway risk), the Infrastructure Manager has to ensure that appropriate measures are available:

- Trap points, catch points/derailers;
- Prohibitions of shunting and stabling;
- Equipment with TTD (as otherwise non-controllable movements cannot be detected).

The interface between MBS and PE is impacted by the flank protection as follows:

- For each granted Movement Permission, the MBS provides to PE the *Risk Path* as part of the Movement Permission.
- When requesting a Movement Permission, the PE is able to optionally provide a list of DPS that must not be used as flank protection measure.

6.11.1.2 Application Example



In the example above the maximum speed for TE3 and TE2 is equal, it is different for TE3 and TE4. The whole train running path of TO1 is split in three segments. The split between TE4 and TE3 would be due to the change in maximum speed. The split in TE2 is due to the mode change from FS to OS.

Note: the example is not exhaustive and does not show all possible starting conditions and terminations of a risk path (e.g. risk path termination by Train Object, risk path starting at a diamond crossing).

6.11.1.3 Safety Check Overview

Safety Checks performed for direct overlaps between two extents (the first column represents the received request to be checked, other columns represent the current state):

	MP	TO/UTO	RB	RP
MP	REQ-SC_MP_MP	FS Mandatory REQ-SC_MP_TO REQ-SC_MP_UTO	REQ-SC_MP_RB	Config REQ-SC_MP_RP
RB	REQ-SC_RB_MP	FS Mandatory OR Config REQ-SC_RB_TO REQ-SC_RB_UTO	Config REQ-SC_RB_RB	Config REQ-SC_RB_RP

Safety Checks performed for overlaps of extents within dependent *Allocation Sections*:

	MP	TO/UTO	RB	RP
MP	REQ-SC_MP_MP_AS	FS Mandatory REQ-SC_MP_TO_AS REQ-SC_MP_UTO_AS	REQ-SC_MP_RB_AS	
RB	REQ-SC_RB_MP_AS	FS Mandatory OR Config REQ-SC_RB_TO_AS REQ-SC_RB_UTO_AS	Config REQ-SC_RB_RB_AS	

Red = Check is always performed

Orange = Check is performed depending on operational situation

Yellow = Check is configuration dependent

Green = No Check

Additional safety checks for flank protection are performed by:

- Requirement REQ-RP_SEARCH, which search the elements providing (or not) flank protection
- Requirement REQ-SC_RP_TERM which check the found elements

6.11.2 Inputs

- MP Request message according to I_PE
- *Domain Object* State

6.11.3 Outputs

- Message “request granted” according to I_PE
- Requested and validated state of the *Movement Permission*
- Message “request rejected” according to I_PE

6.11.4 Functional requirements

REQ-SAFETY

The MBS shall perform a series of checks given by the following ordered list when it receives an Authorise MP Request through I_PE:

1. REQ-SYNTAX
2. REQ-TO_EXISTS
3. REQ-TO_RADY
4. REQ-TOPO1
5. REQ-TOPO2
6. REQ-TOPO3
7. REQ-TOPO4
8. REQ-TOPO5
9. REQ-TRANSLATE
10. REQ-SC_MP_SPEED
11. REQ-SC_RB_SPEED
12. REQ-SC_MP_SPEED_LOWER
13. REQ-SC_MODE
14. REQ-SC_MODE_MISMATCH
15. REQ-SC_MP_SHORTER
16. REQ-SC_RB_SHORTER
17. REQ-SC_MP_TO
18. REQ-SC_MP_UTO
19. REQ-SC_RB_TO
20. REQ-SC_RB_UTO
21. REQ-SC_MP_TO_AS
22. REQ-SC_MP_UTO_AS
23. REQ-SC_RB_TO_AS
24. REQ-SC_RB_UTO_AS
25. REQ-SC_MP_MP
26. REQ-SC_MP_RB
27. REQ-SC_MP_RP

28. REQ-SC_MP_MP_AS
29. REQ-SC_MP_RB_AS
30. REQ-SC_RB_MPPS
31. REQ-SC_RB_RB
32. REQ-SC_RB_RP
33. REQ-SC_RB_MP_AS
34. REQ-SC_RB_RB_AS
35. REQ-SC_RB_SIZE
36. REQ-SC_MPPS_DPS
37. REQ-SC_RB_DPS
38. REQ-RP_SEARCH
39. REQ-SC_RP_TERM
40. REQ-COOP_PENDING

Rationale: The request to allow a train movement shall be safeguarded.

Guidance: This is the top requirement for all (safety) checks.

Operational Rules: None

Engineering Rules: None

REQ-0032

The MBS shall abort checking an Authorise MP Request received through I_PE if any performed safety check fails and send a request rejected message.

Rationale: A safety check could require the correct execution of a previous safety check.

Guidance: If a check discovers a mismatch between the topology in PE and MBS, further checks might lead to illegal function calls within MBS as this part of the topology is not present in the current operating state of MBS.

Operational Rules: None

Engineering Rules: None

REQ-0033

If none of the safety checks fails, MBS shall send an “MP_REQUEST_GRANTED” reply.

Rationale: PE shall be informed about the successful check of the request.

Guidance: None

Operational Rules: None

Engineering Rules: None

6.11.4.1 General Safety Checks

REQ-SYNTAX

The MBS shall perform a syntax check on the received message and if the check fails, the MBS shall send a “SYNTAX” reject code.

Rationale: An invalid command syntax might lead to illegal state.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ- TO_EXISTS

The MBS shall check that the *Train Object* referenced in the request exists within the operating state of the MBS and if the check fails, the MBS shall send a “INCONSISTENT_WITH_TO” reject code.

Rationale: The train for which the Movement Permission shall be granted has to be present.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ- TO_READY

The MBS shall check that train data has been received and acknowledged for the train referenced in the request and if the check fails, the MBS shall send a “TO_NOT_READY” reject code.

Rationale: The OBU accepts a Movement Authority only if the train data has been acknowledged.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-TOPO1

The MBS shall check that every referenced topology element in the request exists in the currently active topology and if the check fails, the MBS shall send a “INVALID_TOPOLOGY” reject code.

Rationale: Referencing a different topology could possibly lead into a wrongly issued Movement Authority.

Guidance:

Every topology reference in the request (mainly *Track Edges*, *Track Edges Links* and *Track Edge Points*) shall match the currently active topology objects.

Operational Rules: None

Engineering Rules: None

REQ-TOPO2

MBS shall check that every LinkedPath in the request is well-formed (i.e. is truely a LinkedPath) and if the check fails, the MBS shall send a “INVALID_TOPOLOGY” reject code.

Rationale: Every Linked Path shall be correctly formed (contiguous non branching path on the network)

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-TOPO3

The MBS shall check that any attributes that can have different values along the Movement Permission are covering the full extent of the Movement Permission and if the check fails, the MBS shall send a “INVALID_TOPOLOGY” reject code.

Rationale:

Every attribute (like Movement Mode) shall cover the full *Movement Permission Extent*.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-TOPO4

The MBS shall check that the last *Movement Permission Extent Segment* in running direction and the *Risk Buffer* form a contiguous path and if the check fails, the MBS shall send a “INVALID_TOPOLOGY” reject code.

Rationale: The *Risk Buffer* has to be a direct extension of the end of the train’s running path and shall not branch off it or start somewhere along the path.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-TOPO5

The MBS shall check that the *Train Location* of the *Train Object* the MP Requests refers to, is completely overlapped by the *Movement Permission Extent* given within the request.

Rationale: If all Movement Permission Path Segment are outside the *Train Location* of the *Train Object*, the train could not move. Additionally, any switchable element below the *Train Objects* Location shall be in the proper state when a movement happens.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-TRANSLATE

The MBS shall translate the requested MP into an Authorisation as if it was granted. If the translation from a Movement Permission into an Authorisation fails, MBS shall send a “MA_CONSTRUCTION_FAILED” reject code.

Rationale: e.g. if the MP results in an Authorisation longer than 500 bytes. it shall not be accepted.

Guidance: None

Operational Rules: None

Engineering Rules: None

6.11.4.2 Speed and Mode related Safety Checks

REQ-SC_MP_SPEED

At every location along the *Movement Permission Extent*, the MBS shall check that the maximum speed given in the requested Movement Permission is equal to or lower than the maximum speed defined in the topology at that location for the concerned train and if the check fails, the MBS shall send a “SPEED_PROFILE” rejection code.

Rationale: The Movement Permission is to be translated into a Movement Authority and the train shall not exceed the maximum speed on the network for the concerned train (possibly considering the train cant deficiency, other train category, train axle load,…).

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-SC_RB_SPEED

At every location along the *Risk Buffer*, the MBS shall check that the maximum speed given in the requested Movement Permission is equal to or lower than the maximum speed defined in the topology at that location for the concerned train and if the check fails, the MBS shall send a “SPEED_PROFILE” rejection code.

Rationale: The Movement Permission is to be translated into a Movement Authority and the train shall not exceed the maximum speed on the network for the concerned train (possibly considering the train cant deficiency, other train category, train axle load, …). The Static Speed Profile has to defined until the SvL (i.e. the danger point inside the Risk Buffer).

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-SC_MP_SPEED_LOWER

If a Movement Permission is already present for a *Train Object*, the MBS shall check that the speed in the request is at every point equal to or higher than in the existing Movement Permission and if the check fails, the MBS shall send a "SPEED_LOWER" rejection code.

Rationale: If the speed in the new MP is lower than in the currently active MP, it is not guaranteed that the train is able to brake. Thus, MBS rejects the MP request if the requested speed is lower than the one already sent to the OBU.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-SC_MODE

The MBS shall check that the movement mode along the Movement Permission only consists of FS or OS and if the check fails, the MBS shall send a "SAFETY_RESPONSIBILITY_PROFILE_INVALID" reject code.

Rationale: Currently only FS and OS are in scope for the MBS.

Guidance: The current version of this requirement is only concerning train movements in Full Supervision and or On Sight.

Operational Rules: None

Engineering Rules: None

REQ-SC_MP_MODE_MISMATCH

If a Movement Permission is already present for a *Train Object*, the MBS shall check that the movement mode of the requested Movement Permission is either FS or equals the mode of the existing Movement Permission and if the check fails, the MBS shall send a "SAFETY_RESPONSIBILITY_PROFILE_MISMATCH" rejection code.

Rationale: If the train shall operate in a different mode, a change on time is not guaranteed.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-SC_MP_SHORTER

If a Movement Permission is already present for a *Train Object*, the MBS shall check that the requested *Movement Permission Extent* is equal to or longer than the existing *Movement Permission Extent* and if the check fails, the MBS shall send a "MP_SHORTER" rejection code.

Rationale: If the new Movement Permission is shorter than the currently active Movement Permission, it is not guaranteed that the train is able to break in rear of the new EoA when receiving a shorter MA.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-SC_RB_SHORTER

If a Movement Permission is already present for a *Train Object* and the Movement Permission Extent of the requested MP equals the Movement Permission Extent of the already present MP, the MBS shall check that the requested Risk Buffer is equal to or longer than the existing Risk Buffer and if the check fails, the MBS shall send a "MP_SHORTER" rejection code.

Rationale: If the new Risk Buffer would become shorter than the currently present Risk Buffer, the train might receive an emergency brake reaction.

Guidance: None

Operational Rules: None

Engineering Rules: None

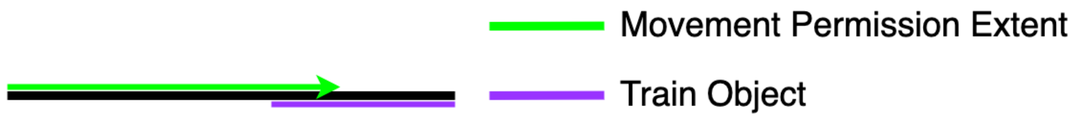
6.11.4.3 Vehicle related Safety Checks

REQ-SC_MP_TO

The MBS shall check that, if a Movement Permission overlaps another *Train Object* in advance of the mSFE of the train for which the Movement Permission is requested, the mode for that part is OS, and if the check fails, the MBS shall send a "PATH_OCCUPIED" reject code.

Rationale: The running path of a train shall be free of other vehicles if operating under FS.

Guidance:



The overlap of MP and TO is not allowed if the Authorisation Type of the Movement Permission Path Segment is set to FS.

Intersection in rear of the minimum Safe Front End is ignored to allow the first train to start in FS in case of splitting.

Operational Rules: None

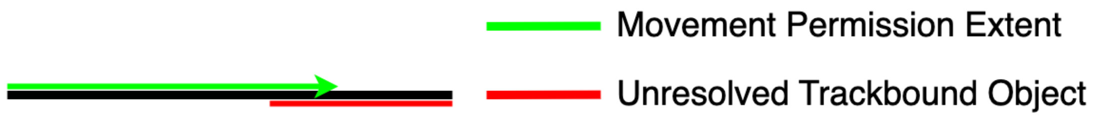
Engineering Rules: None

REQ-SC_MP_UTO

The MBS shall check that, if a Movement Permission overlaps an Unresolved Trackbound Object in advance of the mSFE of the train for which the Movement Permission is requested, the mode for that part is OS, and if the check fails, the MBS shall send a “PATH_OCCUPIED” reject code.

Rationale: The running path of a train shall be free of other vehicles if operating under FS.

Guidance:



The overlap of MP and UTO is not allowed if the Authorisation Type of the Movement Permission Path Segment is set to FS.

Intersection in rear of the minimum Safe Front End is ignored to allow the first train to start in FS in case of splitting.

Operational Rules: None

Engineering Rules: None

REQ-SC_RB_TO

The MBS shall check that the *Risk Buffer* of the requested MP shall not overlap the extent of another *Train Object*, if the requested mode at the end of the Movement Permission Extent is FS and this check is enabled in the configuration, and if the check fails, the MBS shall send a “RISK_BUFFER_OCCUPIED” reject code.

Rationale: The *Risk Buffer* shall be clear of any vehicles if the requested mode was FS at the end of the running path. In some countries the overlap area is not required to be clear of vehicles.

Guidance:

The overlap of *Risk Buffer* and TO is not allowed if the Authorisation Type at the end of the Movement Permission is set to FS.

Operational Rules: None

Engineering Rules: None

REQ-SC_RB_UTO

The MBS shall check that the *Risk Buffer* of the requested MP shall not overlap the extent of an Unresolved Trackbound Object, if the requested mode at the end of the Movement Permission is FS andifthis check is enabled in the configuration, and if the check fails, the MBS shall send a “RISK_BUFFER_OCCUPIED” reject code.

Rationale: The *Risk Buffer* shall be clear of any vehicles if the requested mode was FSat the end of the running path. In some countries the overlap area is not required to be clear of vehicles.

Guidance:

The overlap of *Risk Buffer* and UTO is not allowed if the Authorisation Type at the end of the Movement Permission is set to FS.

Operational Rules: None

Engineering Rules: None

REQ-SC_MP _TO_AS

The MBS shall check that if the extent of the Movement Permission overlaps an *Allocation Section*, all mutually exclusive *Allocation sections* shall not have an overlap with another *Train Object* and if the check fails, the MBS shall send an “AS_OCCUPIED” reject code.

Rationale: The fouling point shall be clear of other vehicles, otherwise a flank collision might result.

Guidance:

Having both *Risk Path* and a *Train Object* present in a conflicting *Allocation Section* is not allowed.

Operational Rules: None

Engineering Rules: None

REQ-SC_MP_UTO_AS

The MBS shall check that if the extent of the Movement Permission overlaps an *Allocation Section*, all mutually exclusive *Allocation sections* shall not have an overlap with an Unresolved Trackbound Object and if the check fails, the MBS shall send an “AS_OCCUPIED” reject code.

Rationale: The fouling point shall be clear of other vehicles, otherwise a flank collision might result.

Guidance:

Having both *Risk Path* and an Unresolved Trackbound Object present on a conflicting *Allocation Section* is not allowed.

Operational Rules: None

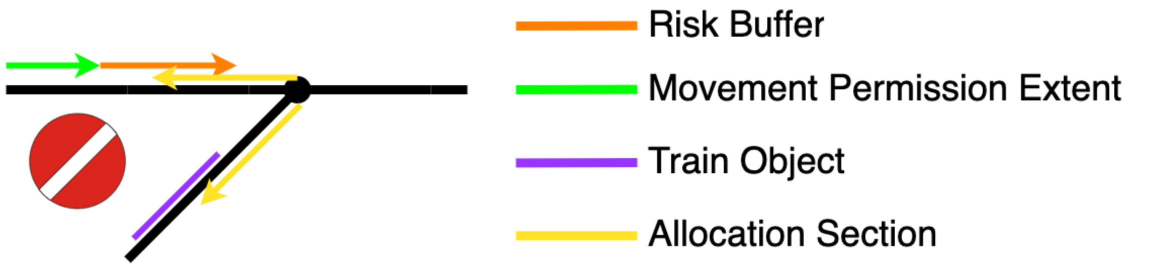
Engineering Rules: None

REQ-SC_RB_TO_AS

The MBS shall check that if the *Risk Buffer* of the Movement Permission overlaps an *Allocation Section*, all mutually exclusive *Allocation sections* shall not have an overlap with the extent of another *Train Object* and if the check fails, the MBS shall send an “AS_OCCUPIED” reject code.

Rationale: The fouling point of points shall be clear of other vehicles.

Guidance:



Having both *Risk Path* and *Train Object* present in a conflicting *Allocation Section* is not allowed.

Operational Rules: None

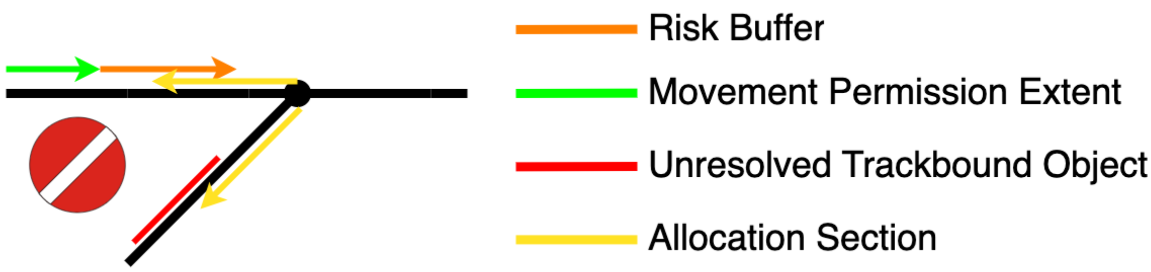
Engineering Rules: None

REQ-SC_RB_UTO_AS

The MBS shall check that if the *Risk Buffer* of the Movement Permission overlaps an *Allocation Section*, all mutually exclusive *Allocation sections* shall not have an overlap with an Unresolved Trackbound Object and if the check fails, the MBS shall send an “AS_OCCUPIED” reject code.

Rationale: The fouling point of points shall be clear of other vehicles.

Guidance:



Interne

Having both *Risk Path* and Unresolved Trackbound Object present in a conflicting *Allocation Section* is not allowed.

Operational Rules: None

Engineering Rules: None

6.11.4.4 Movement related Safety Checks

REQ-SC_MP_MP

The MBS shall check that the *Movement Permission Extent* in advance of the mSFE of the train for which the Movement Permission is requested shall not overlap with a *Movement Permission Extent* of another train unless the other train is supervised at standstill and if the check fails, the MBS shall send an “EXTENT_CONFLICT” reject code.

Rationale: Two trains should not be authorised to perform conflicting movements.

Guidance: The enforcement of OS for the overlap between the MP and the Train Object is covered in REQ-SC_MP_TO.

Operational Rules: None

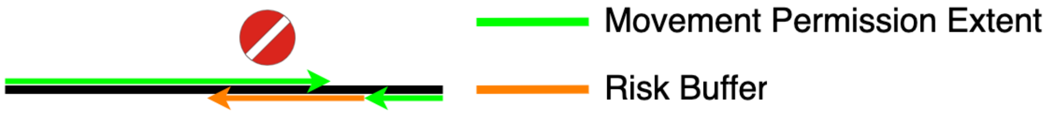
Engineering Rules: None

REQ-SC_MP_RB

The MBS shall check that the *Movement Permission Extent* of the requested MP shall not overlap with a *Risk Buffer* extent of another train and if the check fails, the MBS shall send an “EXTENT_CONFLICT reject code.

Rationale: The running path of a train shall be free of other vehicles.

Guidance: The current version of this requirement is only concerning train movements in FS or OS.



Operational Rules: None

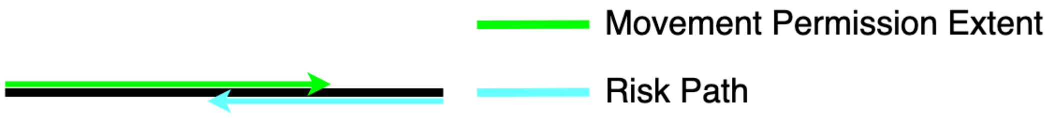
Engineering Rules: None

REQ-SC_MP_RP

The MBS shall check that if the global variable *rpTermAllowedAtRbAndMp* is set to TRUE, the *Movement Permission Extent* of the requested MP shall not overlap with a *Risk Path* extent of another train and if the check fails, the MBS shall send an “EXTENT_CONFLICT reject code.

Rationale: If a *Risk Path* is not allowed to terminate at a *Movement Permission* or *Risk Buffer*, permitting the request would lead to a safety reaction.

Guidance:



Operational Rules: None

Engineering Rules: None

REQ-SC_MP_MP_AS

The MBS shall check that any *Allocation Section* a *Movement Permission Extent* of the requested MP overlaps with, shall not have an overlap with a *Movement Permission Extent* of another train in all mutually exclusive *Allocation Sections* and if the check fails, the MBS shall send an “EXTENT_AS_CONFLICT reject code.

Rationale: The fouling point shall not be occupied by another train movement.

Guidance:

Operational Rules: None

Engineering Rules: None

REQ-SC_MP_RB_AS

The MBS shall check that an *Allocation Section* the *Movement Permission Extent* overlaps with, shall not have an overlap with a *Risk Buffer* of another train in all mutually exclusive *Allocation Sections* and if the check fails, the MBS shall send an “EXTENT_AS_CONFLICT reject code.

Rationale: The fouling point shall not be occupied by another train movement.

Guidance:

Operational Rules: None

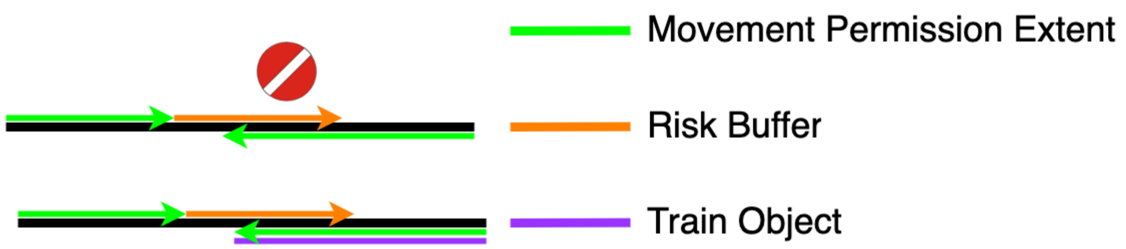
Engineering Rules: None

REQ-SC_RB_MP

The MBS shall check that the *Risk Buffer* of the requested MP shall not overlap with a *Movement Permission Extent* of another train unless the other train is supervised at standstill and if the check fails, the MBS shall send a "RISK_BUFFER_CONFLICT" reject code.

Rationale: The overrun protection area of a Movement Permission shall not be in conflict with another train movement.

Guidance: The enforcement of OS for the overlap between the MP and the Train Object is covered in REQ-SC_RB_TO.



Operational Rules: None

Engineering Rules: None

REQ-SC_RB_RB

If the safety check is enabled in the configuration, the MBS shall check that the *Risk Buffer* of the requested MP shall not overlap any *Risk Buffer* of another Movement Permission and if the check fails, the MBS shall send a "RISK_BUFFER_CONFLICT" reject code.

Rationale: The overrun protection area of a Movement Permission shall not be claimed by the *Risk Buffer* of another train.

Guidance:

Operational Rules: None

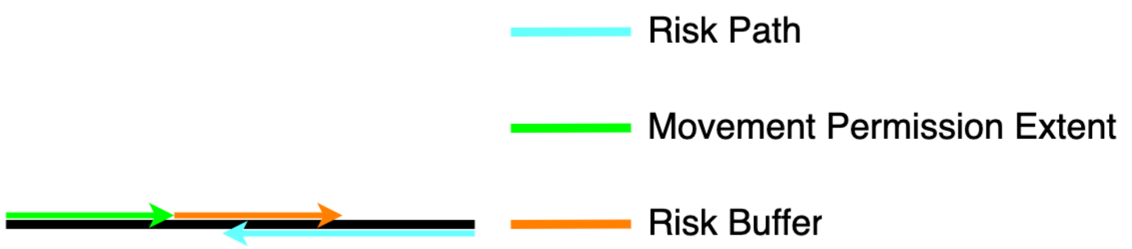
Engineering Rules: None

REQ-SC_RB_RP

The MBS shall check that if the global variable *rpTermAllowedAtRbAndMp* is set to TRUE, the *Risk Buffer* of the requested MP shall not overlap with a *Risk Path* extent of another train and if the check fails, the MBS shall send an "EXTENT_CONFLICT reject code.

Rationale: If a *Risk Path* is not allowed to terminate at a *Movement Permission* or *Risk Buffer,* permitting the request would lead to a safety reaction.

Guidance:



Operational Rules: None

Engineering Rules: None

REQ-SC_RB_MP_AS

The MBS shall check that any *Allocation Section* the *Risk Buffer* of the requested MP overlaps with, shall not have another overlap with a *Movement Permission Extent* of another train in all mutually exclusive *Allocation Sections* and if the check fails, the MBS shall send a "RISK_BUFFER_AS_CONFLICT" reject code.

Rationale: The fouling point shall not be occupied by another train movement.

Guidance:

Operational Rules: None

Engineering Rules: None

REQ-SC_RB_RB_AS

If the safety check is enabled in the configuration, the MBS shall check that any *Allocation Section* the *Risk Buffer* of the requested MP overlaps with, shall not have another overlap with a *Risk Buffer* of another train in all mutually exclusive *Allocation Sections* and if the check fails, the MBS shall send a “RISK_BUFFER_AS_CONFLICT” reject code.

Rationale: The fouling point shall not be occupied by another train movement.

Guidance:

Operational Rules: None

Engineering Rules: None

REQ-SC_RB_SIZE

The MBS shall check that the *Risk Buffer* for the requested MP is longer than or equal to the minimal length of the *Risk Buffer* according to the MBS configuration and if the check fails, the MBS shall send a “RISK_BUFFER_TOO_SHORT” reject code.

Rationale: The *Risk Buffer* includes the danger point and a safety margin to guarantee that the train never overpasses the end of the *Risk Buffer*, this assumes a minimum length for the *Risk Buffer*. See also REQ-0051.

Guidance: None.

Operational Rules: None

Engineering Rules: TBD how the concrete value shall be calculated. The absolute minimum size will be 6 meters for FS (overhang of vehicle front to first axle).

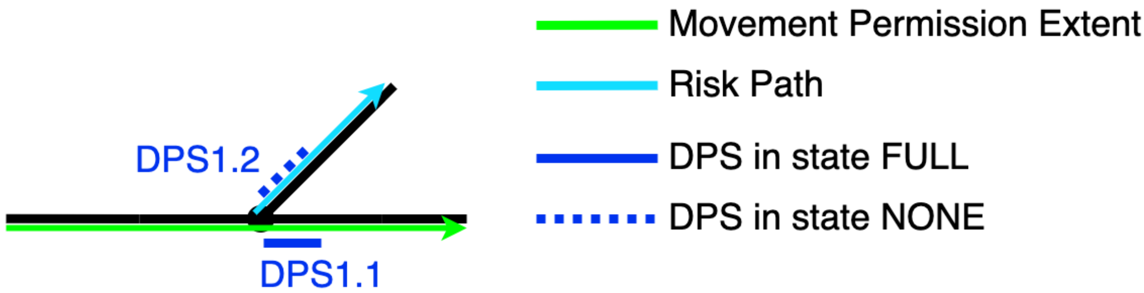
6.11.4.5 DPS related Safety Checks

REQ-SC_MP_DPS

The MBS shall check that all DPS that overlap with the *Movement Permission Extent* are in the state “FULL” and if the check fails, the MBS shall send a “DPS_INVALID_STATE” reject code.

Rationale: All *Switchable Trackside Assets* have to be secured in the correct position for a train movement.

Guidance:



Note: The *Risk Path* is only shown for completeness.

Operational Rules: None

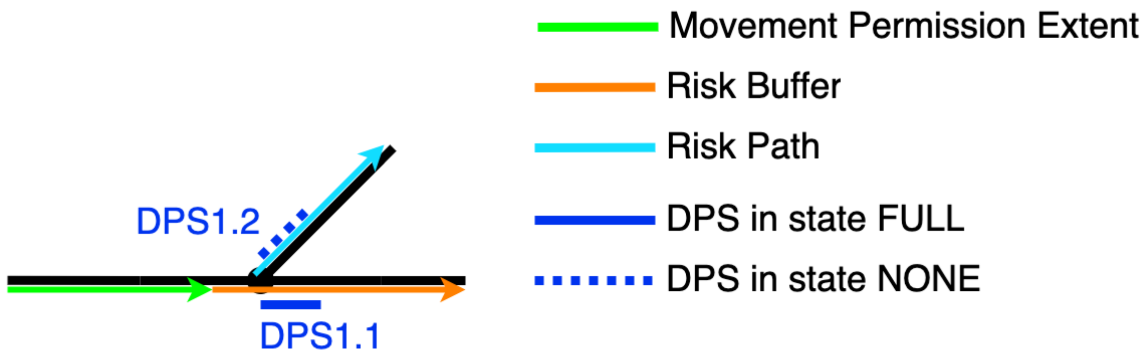
Engineering Rules: None

REQ-SC_RB_DPS

The MBS shall check that all DPS that overlap the *Risk Buffer* of the requested *Movement Permission Extent* are in the state “FULL” and if the check fails, the MBS shall send a “RISK_BUFFER_DPS_INVALID_STATE” reject code.

Rationale: All *Switchable Trackside Assets* have to be in the “secured” position in the overrun protection section of a train movement.

Guidance:



Note: The *Risk Path* is only shown for completeness.

Operational Rules: None

Engineering Rules: None

REQ-COOP_PENDING

The MBS shall check that there is no co-operative shortening of MA procedure is pending for the corresponding train and if the check fails, the MBS shall send a "COOP_PENDING" reject code.

Rationale: Sending MAs in parallel with Request to Shorten MA messages could result in inconsistent views between MBS and the on-board.

Guidance: None

Operational Rules: None

Engineering Rules: None

6.11.4.6 Flank Protection related Safety Checks

REQ-RP_SEARCH

If the global configuration variable *fpSearch* is set to TRUE and the attribute *fpSearchOnDependentAs* in the *Allocation Section* the *Movement Permission Extent* overlaps with is set to TRUE, MBS shall calculate at least one *Risk Path* starting at the end of each *Allocation Section* that is dependent to the *Allocation Section* the *Movement Permission Extent* overlaps with and set the end of the *Risk Path* according to the following list:

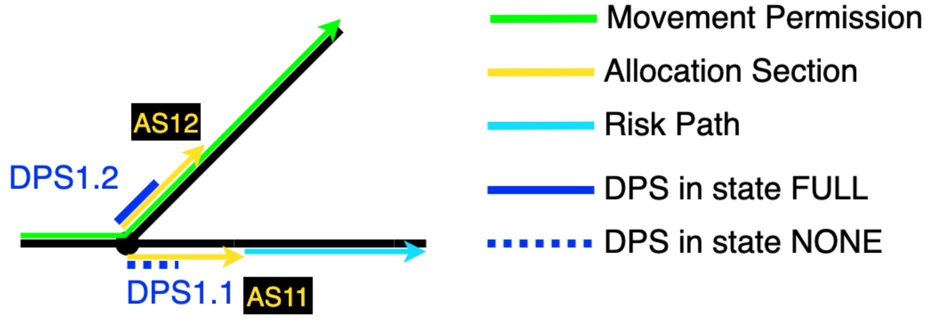
- REQ-RPS_DPS
- REQ-RPS_TO
- REQ-RPS_UTO
- REQ-RPS_MP
- REQ-RPS_RB
- REQ-RPS_TE
- REQ-RPS_DIST

, while obeying the following rules:

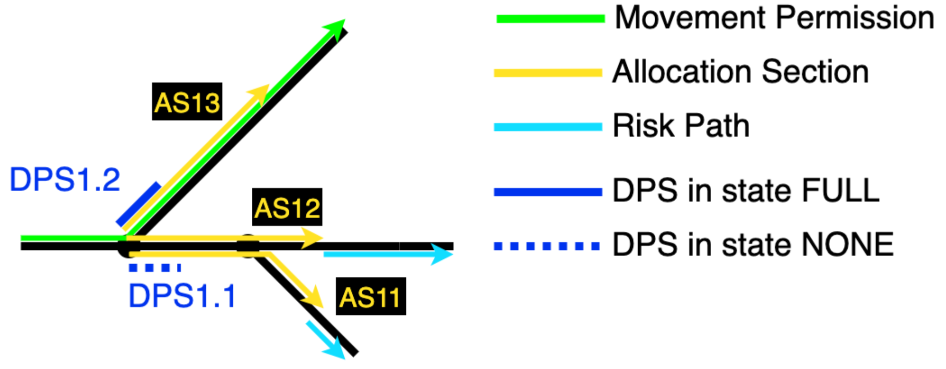
- REQ-RPS_NEAREST
- REQ-RPS_SPLIT

Rationale: An *Allocation Section* marks a stretch of track network where insufficient gauge clearance exists and there shall be no risk of movements against this point. As the risk buffer is used by the train only in degraded situations (i.e. the train overpasses its End of Authority), the risk buffer is intentionally excluded for the risk path search.

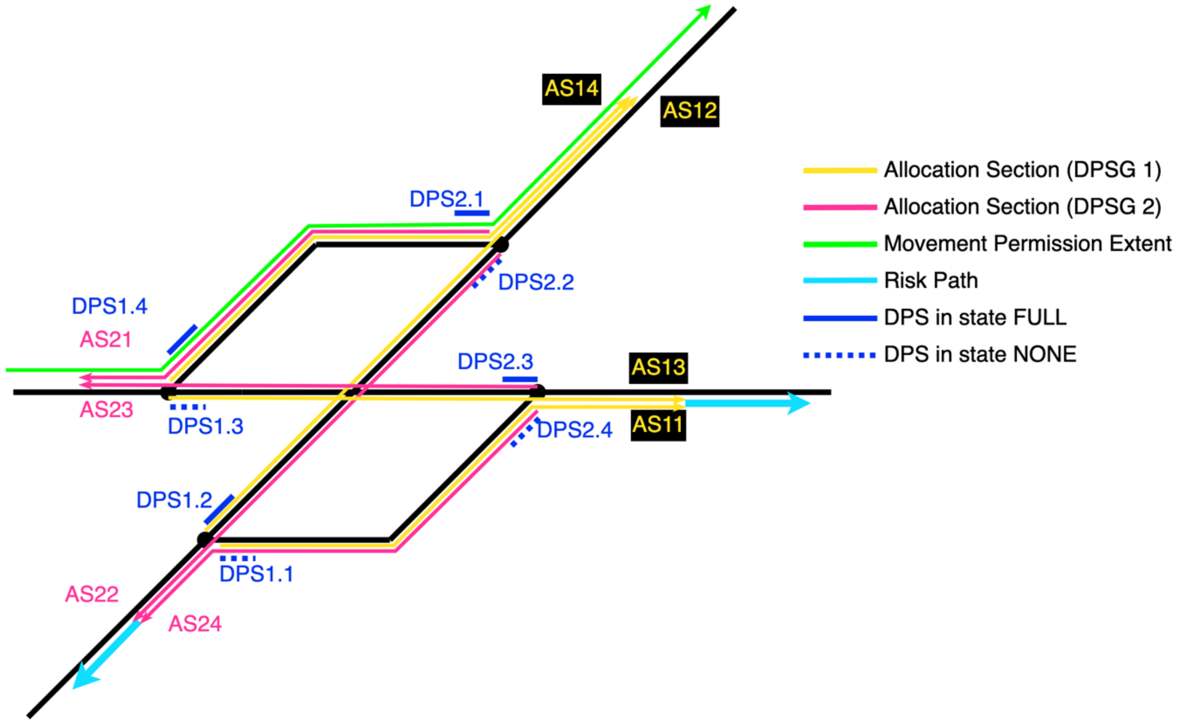
Guidance:



In this example AS11 is dependent to AS12 thus a *Risk Path* must emerge out of AS11 (if *fpSearchOnDependentAs* is set to TRUE for AS12).



In this example a second point is located in the right leg of the first point where the blades start inside the fouling point. The following dependencies exist in this example: AS11-AS13 and AS12-AS13. AS 11 and AS 12 are not dependent to each other.



In this reduced example of a double slip, the *Allocation Sections* of DPS Group 2 are shown in a different colour for clarity. The following dependencies exist: AS11 & AS12, AS13 & AS14, AS21 & AS22, AS23 & AS24. According to the rules a *Risk Path* is needed for AS11, AS13, AS22 and AS24. As the end locations of AS11 & AS13 as well as AS22 & AS24 are equal, only one *Risk Path* is needed per end location.

Operational Rules: None

Engineering Rules: None

REQ- RPS_TO

When the MBS builds a *Risk Path* and it finds a *Train Object* in the search direction, it shall set the end of the *Risk Path* at the border of the *Train Object* without overlapping it according to REQ_SC_RP_TO.

Rationale: A *Train Object* is a possible point for a *Risk Path* termination but the *Risk Path* shall not overlap a *Train Object*.

Guidance:

This requirement only concerns the building of the *Risk Path* Candidate that is then checked through the requirement REQ-SC_RP_TERM

Operational Rules: None

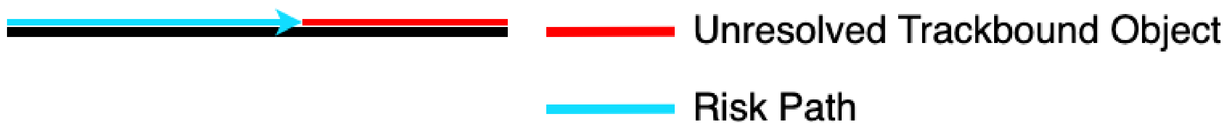
Engineering Rules: None

REQ- RPS_UTO

When the MBS builds a *Risk Path* and it finds an Unresolved Trackbound Object in the search direction, it shall set the end of the *Risk Path* at the border of the Unresolved Trackbound Object without overlapping it according to REQ_SC_RP_UTO.

Rationale: An Unresolved Trackbound Object is a possible point for a *Risk Path* termination but the *Risk Path* shall not overlap an Unresolved Trackbound Object.

Guidance:



This requirement only concerns the building of the *Risk Path* Candidate that is then checked through the requirement REQ-SC_RP_TERM

Operational Rules: None

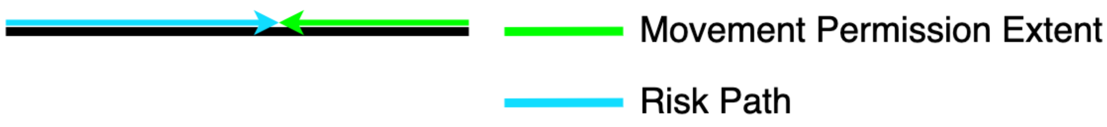
Engineering Rules: None

REQ- RPS_MP

When the MBS builds a *Risk Path* and it finds the end of a *Movement Permission Extent* in the search direction, it shall set the end of the *Risk Path* at the end of the *Movement Permission Extent* without overlapping it according to REQ_SC_RP_MP.

Rationale: The End of a *Movement Permission Extent* is a possible point for a *Risk Path* termination but the *Risk Path* shall not overlap a *Movement Permission Extent*.

Guidance:



This requirement only concerns the building of the *Risk Path* Candidate that is then checked through the requirement REQ-SC_RP_TERM.

Note: this situation is possible only if there is no Risk Buffer for the Movement Permission protecting the Risk Path.

Operational Rules: None

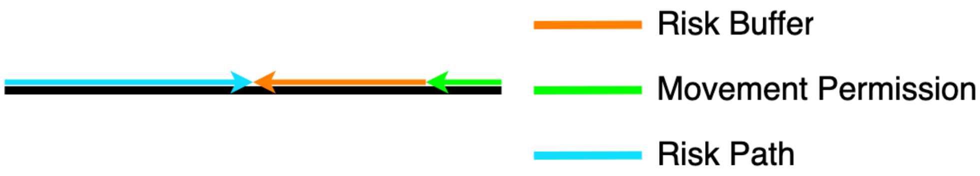
Engineering Rules: None

REQ- RPS_RB

When the MBS builds a *Risk Path* and it finds the end of a *Risk Buffer* in the search direction, it shall set the end of the *Risk Path* at the end of the *Risk Buffer* without overlapping it according to REQ_SC_RP_RB.

Rationale: The End of a *Risk Buffer* is a possible point for a *Risk Path* termination but the *Risk Path* shall not overlap a *Risk Buffer*.

Guidance:



This requirement only concerns the building of the *Risk Path* Candidate that is then checked through the requirement REQ-SC_RP_TERM

Operational Rules: None

Engineering Rules: None

REQ-RPS_DPS

When MBS builds a *Risk Path*, it shall set the end of the *Risk Path* to the end of a *Track Edge* if

- The requirements of SC_RP_TERM_DPS are fulfilled
- The DPS Group checked in SC-RP_TERM_DPS does not belong to the list of DPS Groups that shall not be used as a measure to mitigate the risk of flank collision for this Movement Permission

Rationale: For operational reasons, PE shall be able to mark certain DPS Groups that shall not be used for flank protection, so it remains flexible to be moved.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-RPS_ TE

When MBS builds a *Risk Path*, it shall set the end of the *Risk Path* to the end of a *Track Edge* if the *Track Edge* has no *Track Edge* Links.

Rationale: See SC_RP_TERM_TE

Guidance: See SC_RP_TERM_TE

Operational Rules: None

Engineering Rules: None

REQ-RPS_NEAREST

When MBS builds a *Risk Path*, it shall use the closest possible terminating element

Rationale: The search for flank protection shall not be extended beyond an element that is already providing protection unless it is operationally necessary (i.e. excluded by the MP request received from PE).

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-RPS_DIST

When the MBS builds a *Risk Path* and no element to terminate is found after the configured search length r*pMaxSearchDistance*, MBS shall set the end of the *Risk Path* at the location where the search distance is reached.

Rationale: See SC_RP_TERM_DIST

Guidance: See SC_RP_TERM_DIST

Operational Rules: None

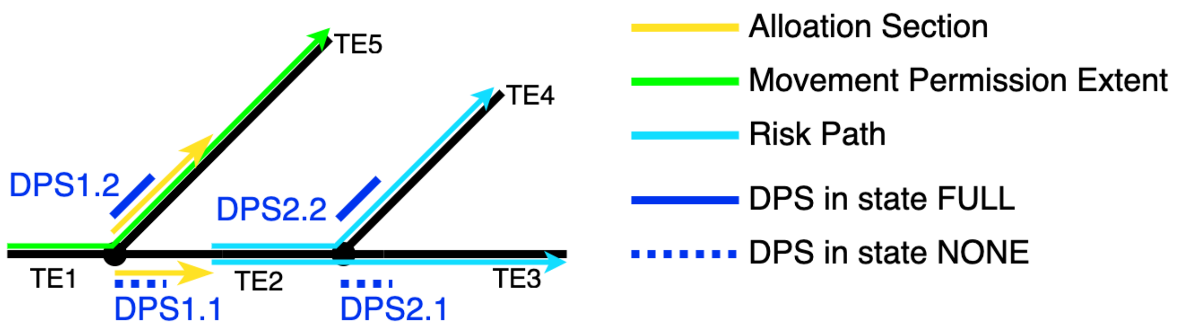
Engineering Rules: None

REQ-RPS_SPLIT

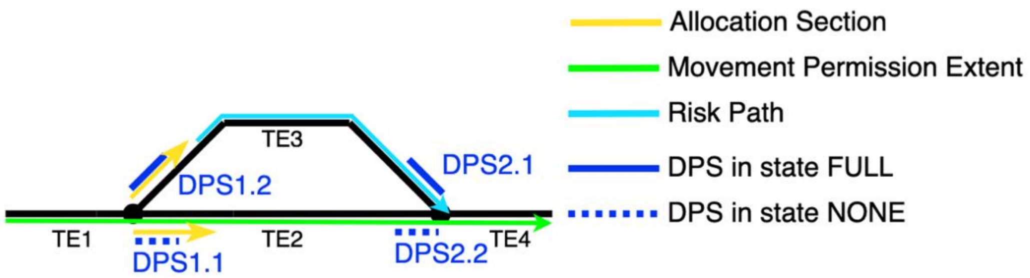
When MBS builds the *Risk Paths* for a Movement Permission, a *Risk Path* overlaps the end of a *Track Edge* and the *Risk Path* is not terminated at this *Track Edge*, MBS shall ensure that a *Risk Path* is present for every *Track Edge* linked by a *Track Edge* Link going in the same direction as the *Risk Path* unless the linked *Track Edge* is covered by the same *Movement Permission Extent*.

Rationale: If the head of a point is facing the requested Movement Permission, the *Risk Path* shall cover both legs of the point. MBS derives n (usually 2) *Risk Paths* if it encounters a *Track Edge* from which it can continue to n *Track Edges*.

Guidance:



TE2 is linked to TE3 and TE4, TE3 and TE4 have links to TE2 but not between them. As a *Risk Path* is present on TE2, one has to be present for *Track Edges* TE3 and TE4.



TE4 is linked to TE2 and TE3, TE2 and TE3 have links to TE4 but not between them. Although a *Risk Path* is present on TE3, none has to be present at TE4 as it is covered by the *Movement Permission Extent* itself.

Operational Rules: None

Engineering Rules: None

REQ-SC_RP_TERM

MBS shall check that all *Risk Paths* build by the MBS are terminated at one of the following termination options:

- SC_RP_TERM_DPS
- SC_RP_TERM_RB
- SC_RP_TERM_MP
- SC_RP_TERM_RP
- SC_RP_TERM_TO
- SC_RP_TERM_UTO
- SC_RP_TERM_DIST
- SC_RP_TERM_TE

and if the check fails, MBS shall send a "RP_TERMINATION_INSUFFICIENT" reject code.

Rationale: Every possible path that leads to a flank protection risk has to be excluded and thus an element has to be identified that provides the risk mitigation measure.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-SC_RP_TERM_DPS

A *Risk Path* is correctly terminated if the following conditions are met:

- The end of the *Risk Path* equals the end of the DPS
- The overlap length between the *Risk Path* and the DPS is greater than zero
- The overlapped DPS is in the state NONE
- The dependent DPS is in the state FULL
- The configuration attribute dps*ProvidesFlankProtection* is set to TRUE for the overlapped DPS
- The requested maximum speed at the location where the *Risk Path* originates from is equal to or lower than the speed configured in the attribute dps*MaxFlankProtectionSpeed* for the DPS that is providing flank protection.

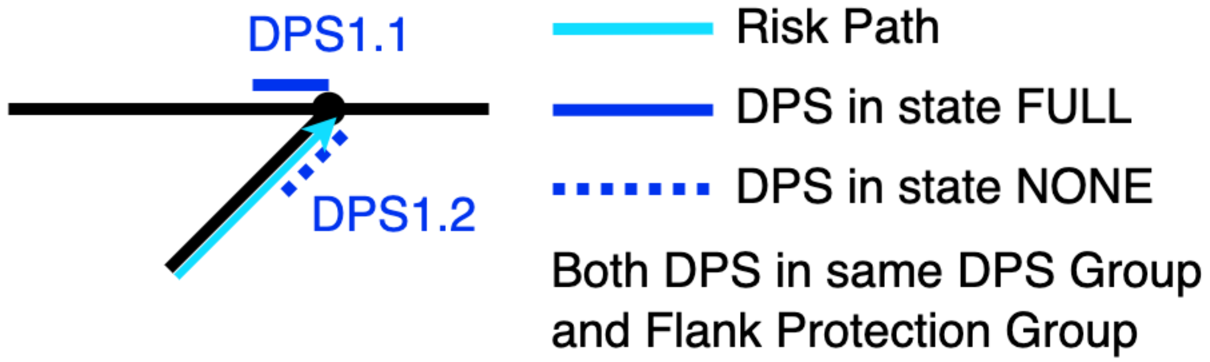
Rationale:

Points and derailers provide flank protection by means that no train can physically move towards the flank protection seeking element, if the path is set away from the side that needs protection (Check for FULL/NONE). In some cases, the abstracted DPS cannot physically provide flank protection (config variable flankProtection). For derailers a regulation exists (for example in Switzerland) that they must not be used if the speed of the to be protected train is higher than 120 km/h (variable maxFlankProtectionSpeed).

Guidance:

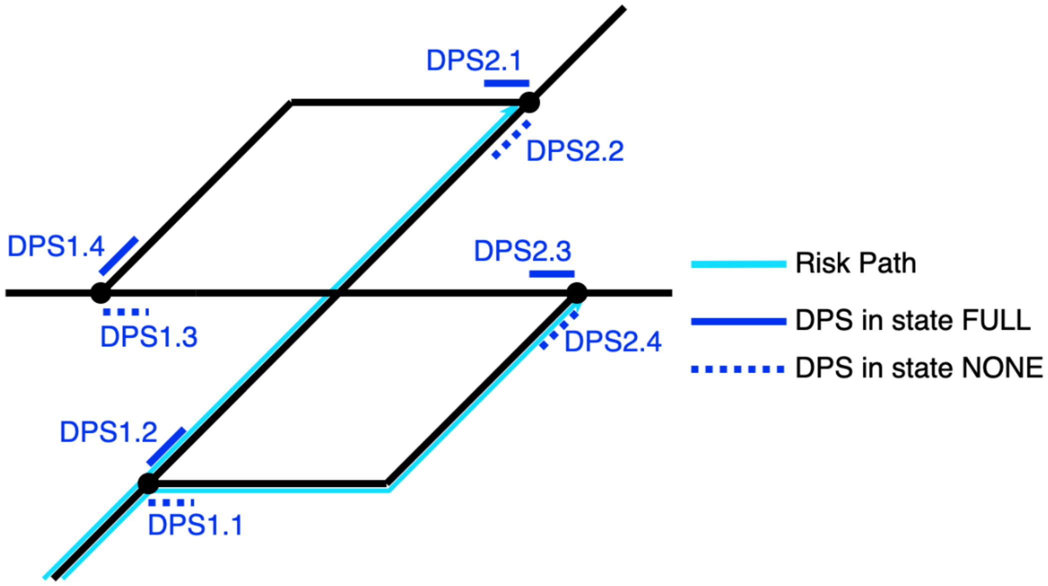
The termination of the *Risk Path* was chosen to be the “inner end” of the DPS to have a) a clear point to terminate, b) be able to perform an overlap check if the DPSG is allowed to move or locked as it serves as a flank protection element and c) to distinguish the cases of a DPSG where it is used as a flank protection measure (and thus not able to move) from being in the flank protection area (and thus allowed to move).

Simple Example of one set of points:

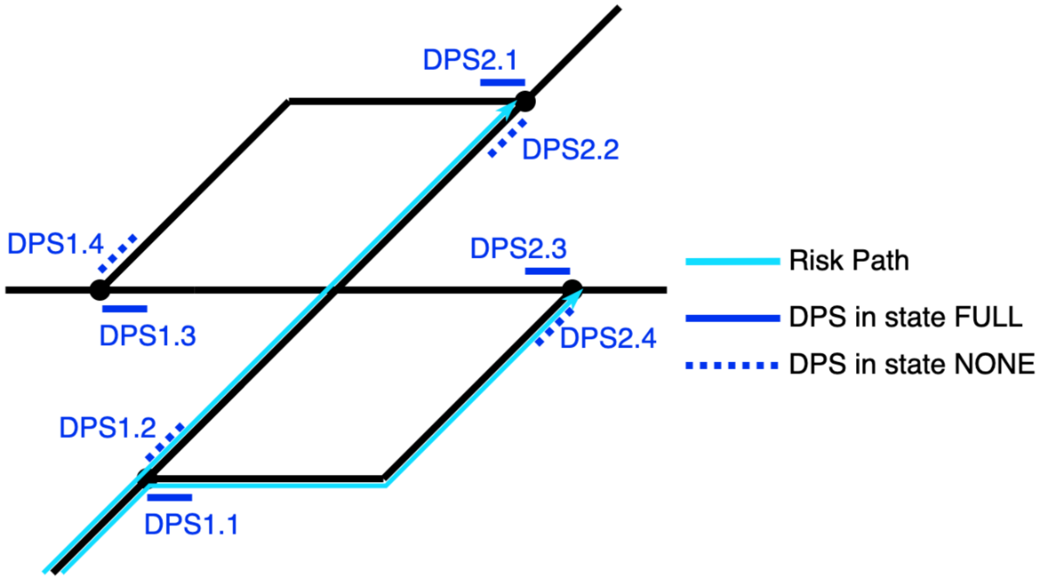


DPS 1.1 and 1.2 are in the same DPS Group and Flank Protection Group.

Complex example of double slips:



Example of a double slip: DPS 1.1, 1.2, 1.3 & 1.4 are in DPS Group 1, DPS 2.1, 2.2, 2.3 & 2.4 are in DPS Group 2. The DPS (1.1 & 1.2), (1.3 & 1.4), (2.1 & 2.2) and (2.3 & 2.4) are dependent to each other. The DPS (1.1 & 1.3), (1.2 & 1.4), (2.1 & 2.3) and (2.2 & 2.4) are mechanically linked.



Operational Rules: None

Engineering Rules: TBD

REQ-SC_RP_TERM_RB

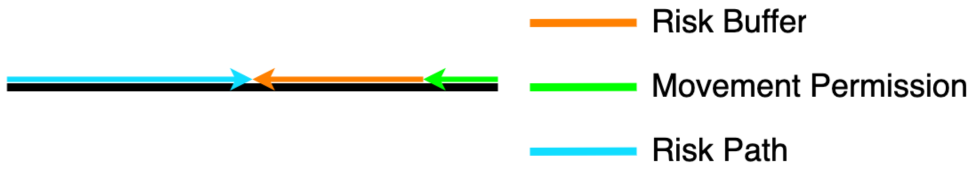
A *Risk Path* is correctly terminated if the following conditions are met:

- The end of the *Risk Path* equals the end of a *Risk Buffer*
- There is no overlap between the *Risk Path* and the *Risk Buffer*
- The global variable rpTermAllowedAtRbAndMp is set to TRUE

- The attribute *rpTermAtDpsOnly* is FALSE for the *Allocation section* the *Risk Path* originates from

Rationale: The other train movement is supervised to not overpass the end of the *Risk Buffer*.

Guidance:



Operational Rules: None

Engineering Rules: None

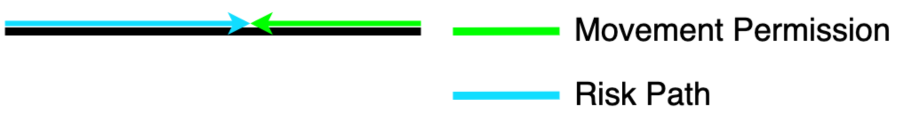
REQ-SC_RP_TERM_MP

A *Risk Path* is correctly terminated if the following conditions are met:

- The end of the *Risk Path* equals the end of a *Movement Permission Extent*
- There is no overlap between the *Risk Path* and the *Movement Permission Extent*
- The global variable rpTermAllowedAtRbAndMp is set to TRUE
- The attribute *rpTermAtDpsOnly* is FALSE for the *Allocation section* the *Risk Path* originates from

Rationale: The other train movement is supervised to not overpass the end of the Movement Permission Path Segment.

Guidance: None



Operational Rules: None

Engineering Rules: None

REQ-SC_RP_TERM_RP

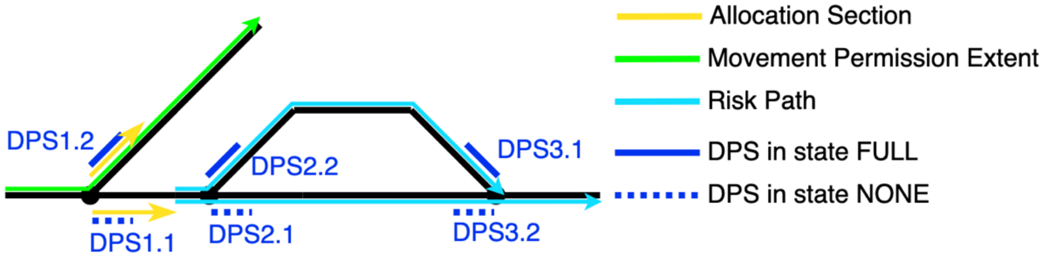
A *Risk Path* is correctly terminated if the following conditions are met:

- The end of the *Risk Path* equals the end of a *Track Edge*

- All other linked *Track Edges* are covered by a *Risk Path* of the same Movement Permission

Rationale: A *Risk Path* can be terminated at points if another *Risk Path* of the same Movement Permission is present on the other leg of the point and continues on the head side.

Guidance:



Operational Rules: None

Engineering Rules: None

REQ-SC_RP_TERM_TO

A *Risk Path* is correctly terminated if the following conditions are met:

- The end of the *Risk Path* equals one end of a *Train Object*
- There is no overlap between the *Risk Path* and the *Train Object*
- The global variable rpTermAllowedAtTo is set to TRUE
- The attribute *rpTermAtDpsOnly* is FALSE for the *Allocation section* the *Risk Path* originates from

Rationale: A *Train Object* is only created for trains that are communicating through ETCS and are thus supervised to not move unintentionally.

Guidance:

Operational Rules: None

Engineering Rules: None

REQ-SC_RP_TERM_UTO

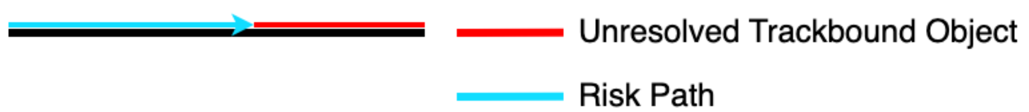
A *Risk Path* is correctly terminated if the following conditions are met:

- The end of the *Risk Path* equals one end of an *Unresolved Trackbound Object*
- There is no overlap between the *Risk Path* and the *Unresolved Trackbound Object*
- The requested maximum speed at the location where the *Risk Path* originates from is equal to or lower than a globally configured variable rpTermMaxSpeedUto
- The length of the *Risk Path* is equal to or greater than the minimal length required for the requested maximum speed at the location where the *Risk Path* originates from
- The global variable rpTermAllowedAtUto is set to TRUE
- The attribute *rpTermAtDpsOnly* is FALSE for the *Allocation section* the *Risk Path* originates from

Rationale: A parked vehicle not reporting to the MBS is not expected to move and thus the risk of a flank movement could be acceptable if the speed is low enough.

Guidance:

The minimal length for the *Risk Path* is configured in MBS with a lookup table with speed brackets and the minimum length as columns.



Operational Rules: None

Engineering Rules: None

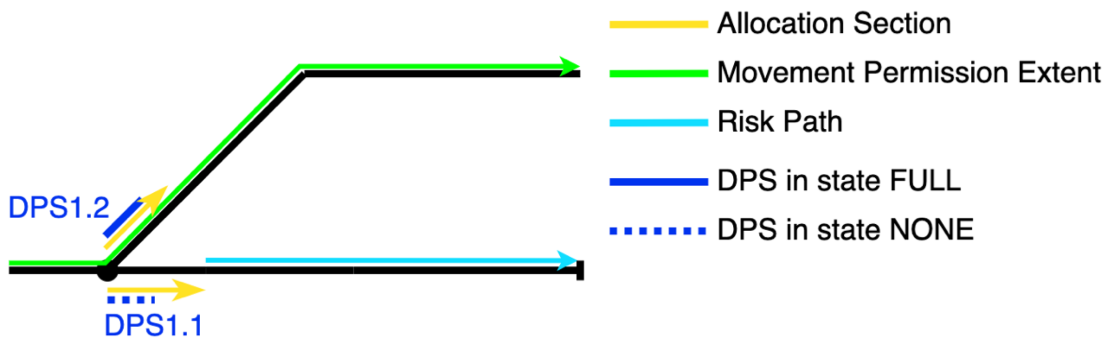
REQ-SC_RP_TERM_TE

A *Risk Path* is correctly terminated if the following conditions are met:

- The end of the *Risk Path* equals the end of a *Track Edge*
- The *Track Edge* has no *Track Edge* Links

Rationale: If the stretch between the *Allocation Section* and the track net is free of vehicles, the movement cannot be endangered.

Guidance:



Operational Rules: None

Engineering Rules: None

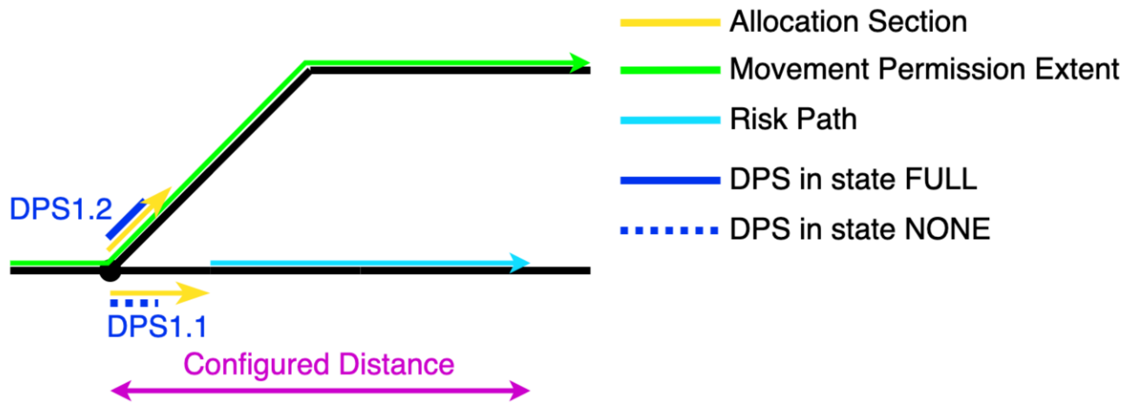
REQ-SC_RP_TERM_DIST

A *Risk Path* is correctly terminated if the following conditions are met:

- The maximum search distance according to the global variable *rpMaxSearchDistance* is reached
- The global variable *rpTermAllowedAfterMaxDistance* is set to TRUE

Rationale: An unterminated search could result in quite long search paths. If the distance is long enough, it is unlikely that a vehicle arriving from that side would endanger the train.

Guidance:



Operational Rules: None

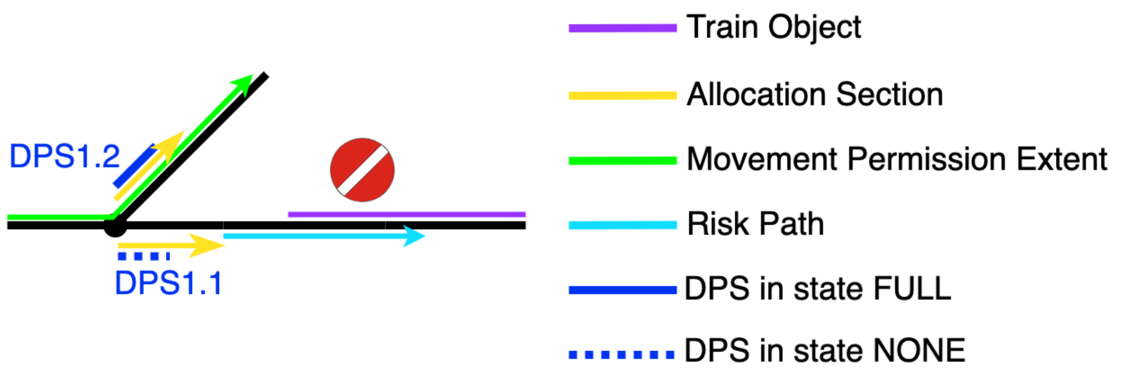
Engineering Rules: A safety consideration is to be done for the concrete value of the minimum distance.

REQ-SC_RP_TO

The MBS shall check that no *Risk Path* overlaps any *Train Location* of a *Train Object*.

Rationale: The area between the danger point and the flank protection providing element shall be clear of vehicles.

Guidance:



Note: The DPS states are only shown for completeness

Operational Rules: None

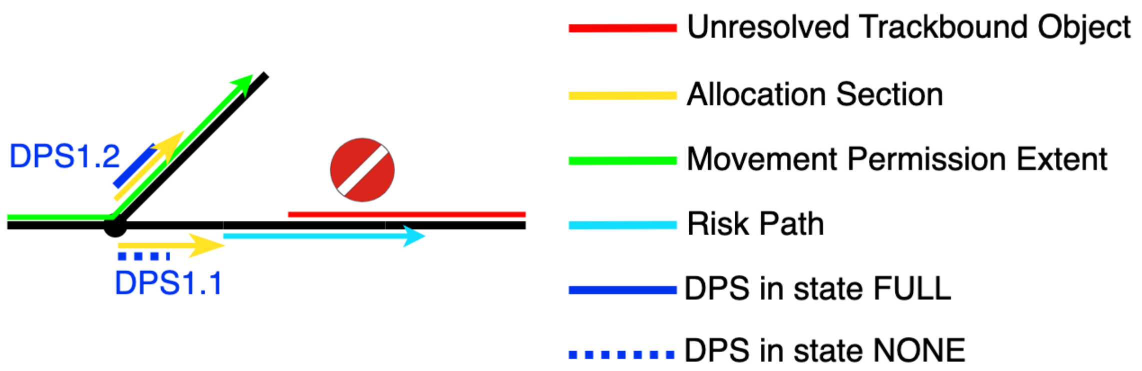
Engineering Rules: None

REQ-SC_RP_UTO

The MBS shall check that no *Risk Path* overlaps any Unresolved Trackbound Object.

Rationale: The area between the endangerment point and the flank protection providing element shall be clear of vehicles.

Guidance:



Note: The DPS states are only shown for completeness

Operational Rules: None

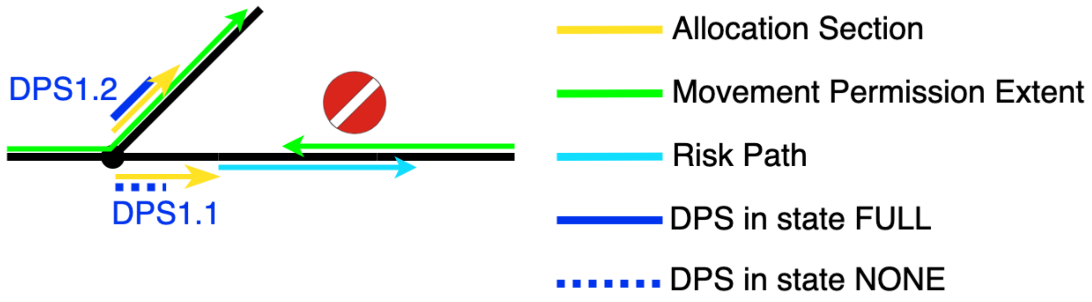
Engineering Rules: None

REQ-SC_RP_MP

The MBS shall check that no *Risk Path* overlaps any *Movement Permission Extent* of another train.

Rationale: The area between the endangerment point and the flank protection providing element shall be clear of movements.

Guidance:



Note: The DPS states are only shown for completeness

Operational Rules: None

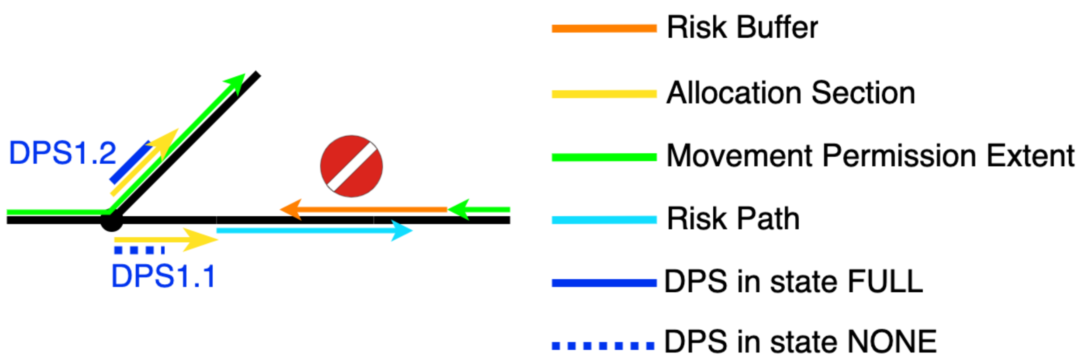
Engineering Rules: None

REQ-SC_RP_RB

The MBS shall check that no *Risk Path* overlaps any *Risk Buffer* of another train.

Rationale: The area between the danger point and the flank protection providing element shall be clear of movements.

Guidance:



Note: The DPS states are only shown for completeness

Operational Rules: None

Engineering Rules: None

6.12 AUTHORISE COOPERATIVE SHORTENING REQUEST

6.12.1 Overview

This function is responsible to assess the safety of a request to co-operatively shorten the Movement Authority of a train. The MBS shall not alter the request if certain parameters are incorrect but only report the failure to PE with the failure reason.

The Cooperative Shortening Request shall contain the following information:

- *Train Object* Identifier
- Requested Stop Location
- *Risk Buffer* (LinkedPath)

6.12.2 Inputs

- Cooperative Shortening Request message according to I_PE
- *Domain Object* State

6.12.3 Outputs

- Message “request granted” according to I_PE
- Message “request rejected” according to I_PE

6.12.4 Functional requirements

REQ-SAFETY-COOPERATIVE

The MBS shall perform a series of checks given by the following ordered list when it receives a Cooperative Shortening Request indicating a request to co-operatively shorten an MA through I_PE:

1. REQ-SYNTAX (see 'Authorise MP Request')
2. REQ-TOPO1 (see 'Authorise MP Request')
3. REQ-TOPO2 (see 'Authorise MP Request')
4. REQ-COOP_TO_EXIST
5. REQ-COOP_FS_OR_OS
6. REQ-STOP_LOCATION_IN_REAR_OF_EOA
7. REQ-COOP_TRANSLATE
8. REQ-COOP_RISK_BUFFER
9. REQ-COOP_PENDING

Rationale: The request to allow a train movement shall be safeguarded.

Guidance: This is the top requirement for all necessary checks.

Operational Rules: None

Engineering Rules: None

REQ-COOP-FAILS

The MBS shall abort checking a Cooperative Shortening Request received through I_PE if any performed safety check fails and send a "REQUEST_REJECTED" reply.

Rationale: A safety check could require the correct execution of a previous safety check.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-COOP-SUCCESSFUL

If none of the safety checks fails, MBS shall send an "REQUEST_GRANTED" reply.

Rationale: By this message, PE is informed that the MBS accepts its request and sends the corresponding Request to Shorten MA message to the OBU.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-COOP_TO_EXIST

The MBS shall check that the *Train Object* referenced in the Cooperative Shortening Request exists and if the check fails, the MBS shall send a “COOP_TO_NOT_EXISTENT” reject code.

Rationale: A co-operative shortening can be only applied to a train known to the MBS.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-COOP_FS_OS

The MBS shall check that the mode of the train is either FS or OS and if the check fails, the MBS shall send a “COOP_INVALID_MODE” reject code.

Rationale: The OBU does not accept a Request to Shorten MA message in other modes (supported by the MBS) according to chapter 4.8.4 (/ETCS/).

Guidance: According to chapter 4.8.4 (/ETCS/), an OBU would also accept a Request to Shorten MA message in the modes LS and AD, but those modes are not in scope of the System Specification of the MBS yet.

Operational Rules: None

Engineering Rules: None

REQ- STOP_LOCATION_IN_REAR_OF_EOA

The MBS shall check that the requested stop location of the Cooperative Shortening Request is located within the currently stored Movement Permission and if the check fails, the MBS shall send a COOP_NOT_IN_REAR reject code.

Rationale: According to chapter 4.8.4 (ETCS/), MBS should propose a shortened MA with an EOA closer to the train than the current EOA/LOA.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-COOP_TRANSLATE

The MBS shall translate the requested MP into a Request to Shorten MA message as if it was granted by the MBS and if the translation from a Movement Permission into a Request to Shorten MA message fails, MBS shall send a “COOP_MA_CONSTRUCTION_FAILED” reject code.

Rationale: The generation of a Request to Shorten MA may fail if e.g. the extent in the requested Movement Permission is located in rear of the current LRBG of the train (since a Request to Shorten MA message cannot be sent with a shifted location reference according to /ETCS/).

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-COOP_RISK_BUFFER

The MBS shall perform all checks related to the *Risk Buffer* contained in the Cooperative Shortening Request of the function 'Authorise MP Request' and if one of the check fails, the MBS shall send the corresponding reject code.

Rationale: The Cooperative Shortening Request can contain a *Risk Buffer* and therefore the (safety) checks for the *Risk Buffer* have to be performed.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-COOP_PENDING

The MBS shall check that there is no pending co-operative shortening for the referenced train in the Cooperative Shortening Request and if the check fails, the MBS shall send a "COOP_PENDING" reject code.

Rationale: It is considered as unlikely that PE would trigger several co-operative shortenings at the same time for one train. Thus, when MBS would allow this, this would unnecessarily the complexity of the MBS system.

Guidance: None

Operational Rules: None

Engineering Rules: None

6.13 SysF Translate MP Request to Movement Authority

6.13.1 Overview

To control the train movement in an ETCS based system, the on-board equipment shall receive a Movement Authority.

This function converts the authorised Movement Permission into a Movement Authority and transmits it to the on-board.

6.13.2 Inputs

- Authorised Movement Permission
- *Domain Object* State

6.13.3 Outputs

- Message Movement Authority according to I_OBU

6.13.4 Functional requirements

REQ-0048

When a valid Movement Permission is received, the MBS shall translate the Movement Permission into a Movement Authority.

Rationale: The MA is supplied to the on-board to allow the on-board equipment to control the train movement. The Movement Permission has to be supplied to the OBU as a Movement Authority in compliance with the interface I_OBU.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-0049

The End of Movement Authority shall be the location at the end of the *Movement Permission Extent*.

Rationale: The End of Movement Authority is the target of the Movement Permission and the *Risk Buffer* starts from there.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-0050

The Target Speed at the End of Movement Authority shall be zero.

Rationale: Target speed is set to 0 and *Risk Buffer* starts just after.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-0051

If a *Risk Buffer* is present in the Movement Permission, the Danger Point of the Movement Authority shall be a location at a fixed distance (safe margin) in rear of the end of the *Risk Buffer*.

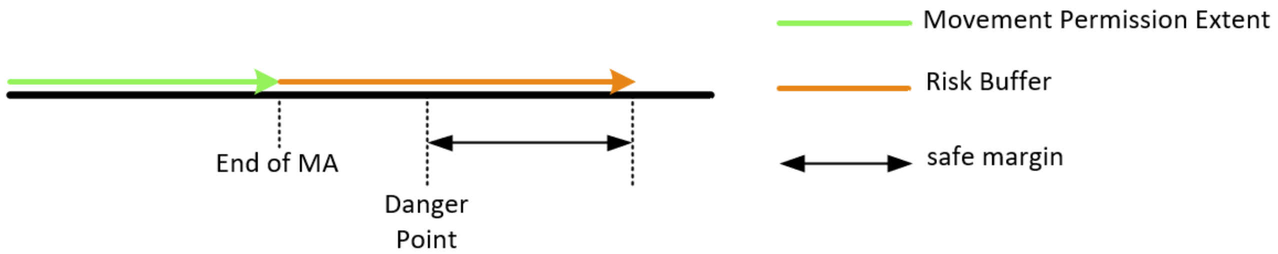
Rationale: The danger point is the Supervised Location that the train shall not overpass. A safe margin is nevertheless added to consider some degraded cases (see Guidance).

Guidance: The safe margin (defined at Project Level) considers that it is not always guaranteed that the train stops in rear of the Danger Point if certain assumptions are not fulfilled e.g.:

- That the available wheel-rail adhesion is better than or equal to that assumed in the ETCS braking curve calculation.
- That the train does not accelerate on approach to the EOA (release speed calculation assumes no acceleration).
- That the compensation of speed measurement inaccuracy is not inhibited by national value.

If any of these assumptions are not true, then the SvL protection is not guaranteed by the ETCS OBU. The safe margin provides a mitigation in case any of these assumptions is not fulfilled.

The safe margin also considers the risk associated with the potential rollback of a chased train and the train overhang (between the TTD border and the physical train end).



Operational Rules: None

Engineering Rules: None

REQ-0052

If a danger point is defined, the release speed shall be calculated (Project Specific) based on the information contained in the Movement Permission.

Rationale: The release speed as such is an operational decision.

Guidance: The release speed value impacts the length of the associated *Risk Buffer*.

For example, based on the Project decision, the Release speed can be:

- Set to 0 or to the specific value «calculated on board».
- Set to a value dependent on the Risk Buffer length and/or the train category.

Operational Rules: None

Engineering Rules: None

REQ-0053

Movement Authority shall be defined without an overlap.

Rationale: The use of overlap is considered as not needed. Once the train is at standstill, it should be possible for the PE to request to reduce the *Risk Buffer* by Cooperative Shortening Movement Authority if there is an operational need to do so.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-0055

Movement Authority shall be defined without section timers.

Rationale: No section timers are foreseen within an MA derived from a Movement Permission. The release of a Movement Permission must always be carried out by Cooperative Shortening Movement Authority

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-0056

The Mode Profiles defined inside the Movement Permission shall be included inside the Movement Authority.

Rationale: The mode profiles shall be transmitted to the on-board equipment to control the train movement (see /ETCS/ - SUBSET-026).

Guidance: The mode profile distance and length sent in the Movement Authority corresponds the mode extent defined in the Movement Permission. The other Mode Profile parameters are Project Specific.

Operational Rules: None

Engineering Rules: None

REQ-0057

The track description (excluding SSP) and linking information included inside the Movement Authority shall correspond to the *Domain Data*, that is entirely or partly covering the *Train Location* and *Movement Permission* (*Risk Buffer* included).

Rationale: Track description covering the minimum safe rear end (to avoid message entry in OS/FS) and the whole distance defined by the MA is supplied to the on-board to allow the on-board equipment to control the train movement. SSP is covered by requirement REQ-0066.

Guidance:

Track description includes the following information (see /ETCS/ - SUBSET-026 chapter 3.7)

- The gradient profile.
- Optionally Speed restriction to ensure a given permitted braking distance.
- Optionally track conditions.
- Optionally route suitability data.
- Optionally areas where reversing is permitted.
- Optionally changed adhesion factor.

Linking information when available.

Axle load speed profile is ignored here as it will be covered by the SSP in the MBS solution.

When extending or modifying an existing MA, it is sufficient to only include the modified extended part not yet acknowledged by the OBU.

Operational Rules: None

Engineering Rules: None

REQ-0066

The Static Speed Profile (SSP) included inside the Movement Authority shall correspond to the speed values given in the requested Movement Permission.

Rationale: Track description covering the minimum safe rear end (to avoid message entry in OS/FS) and the whole distance defined by the MA is supplied to the on-board to allow the on-board equipment to control the train movement.

The speed in the requested Moving Permission is safe since the requirements REQ-SC_MP_SPEED and REQ-SC_RB_SPEED have been successfully applied before.

Guidance: When extending or modifying an existing MA, it is sufficient to only include the modified extended part not yet acknowledged by the OBU.

Operational Rules: None

Engineering Rules: None

REQ-0058

MBS shall request acknowledgement of the reception of each Movement Authority (variable M_ACK is set to 1 inside the MA message).

Rationale: The Movement Authority has to be acknowledged by the OBU to confirm it is well received.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-0059

MBS shall send the translated Movement Authority to the corresponding ETCS on-board equipment according to the I_OBU interface.

Rationale: The MA is supplied to the train to allow the ETCS on-board equipment to control the train movement

Guidance: None.

Operational Rules: None

Engineering Rules: None

6.14 SysF Translate Cooperative Shortening Request to Request to Shorten MA

6.14.1 Overview

To co-operatively shorten the movement authority of a train, a Request to Shorten MA message shall be sent to the train.

This function converts the authorised Cooperative Shortening Request into a Request to Shorten MA message and transmits it to the on-board.

6.14.2 Inputs

- Authorised Cooperative Shortening Request
- *Domain Object* State

6.14.3 Outputs

- Message Request to Shorten MA according to I_OBU

6.14.4 Functional requirements

REQ-0067

When a valid Cooperative Shortening Request is received, the MBS shall translate the Movement Permission into a Request to Shorten MA message.

Rationale: To co-operatively shorten the movement authority of a train, a Request to Shorten MA message shall be sent to the train.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-0068

The MBS shall apply the requirements REQ-0049, REQ-0050, REQ-0051, REQ-0052, REQ-0053, REQ-0055, REQ-0056 from the function “Translate MP Request to Movement Authority” using the existing Movement Permission with the new stop location and the risk buffer for the translation of the Request to Shorten MA message.

Rationale: A Request to Shorten MA message sent by MBS contains packet 15 and optionally packet 80. Thus, only a subset of the requirements of “Translate MP Request to Movement Authority” is applied.

Guidance: None.

Operational Rules: None

Engineering Rules: None

REQ-0069

MBS shall send the translated Request to Shorten MA message according to the I_OBU interface.

Rationale: The Request to Shorten MA is supplied to the train to trigger the co-operative shortening of MA procedure to the ETCS on-board equipment.

Guidance: None.

Operational Rules: None

Engineering Rules: None

6.15 SYSF DELETE *TRAIN OBJECT*

6.15.1 Overview

When a *Train Object* inside the AoC is deleted from the MBS, the *Train Location* for this *Train Object* is replaced by an *Unresolved Trackbound Object* to manage the occupation of the track.

6.15.2 Inputs

- Trigger (by Terminate communication session with OBU)

6.15.3 Outputs

- *Train Object* (removed)
- *Train Location* (removed)
- *Unresolved Trackbound Object*

6.15.4 Functional Requirements

REQ-TrainLoc-10 [X2R5 REQ-TrainLoc-10]

When the communication session with a leading OBU is terminated for trackside, then the MBS shall:

- create an *Unresolved Trackbound Object* corresponding to the *Train Location* extended to the end of the *Movement Permission*.
- store the Train Length (L_TRAIN) in the created Unresolved Trackbound Object if the train is marked as integrity confirmed
- delete the *Train Location* and the *Movement Permission*

Rationale:

The MBS cannot determine the *Train Location* for a train when the communication session has been terminated or is considered terminated.

Guidance:

Communication session is terminated for trackside according to /ETCS/ - SUBSET-26 chapter 3.5.5 and 3.5.4.2.1

If the train was within or partially within the Area of Control when the communication session was closed, then even though the *Train Location* is removed, the *Unresolved Trackbound Object* for the train will remain.

A leading OBU is an OBU not in SL, NL.

Operational Rules: None

Engineering Rules: None

REQ-0065 [X2R5 REQ-TrainLoc-10]

When the communication session is terminated for trackside and when the *Train Location* has been deleted, then the MBS shall delete the *Train Object*.

Rationale:

The MBS cannot determine the *Train Location* for a train when the communication session has been terminated or is considered terminated.

Guidance:

Communication session is terminated for trackside according to /ETCS/ - SUBSET-26 chapter 3.5.5 and 3.5.4.2.1.

If the train was within or partially within the Area of Control when the communication session was closed, then even though the *Train Location* is removed, the *Unresolved Trackbound Object* for the train will remain.

Operational Rules: None

Engineering Rules: None

REQ-TrainLoc-11 FOR FURTHER RELEASE [X2R5 REQ-TrainLoc-11]

The MBS shall remove the *Train Location* for a train which has completely left the Area of Control.

Rationale:

The MBS does not need to maintain a *Train Location* for trains beyond its Area of Control.

Guidance:

This applies to both Handovers and Transitions.

How the removal is achieved is project specific. Options include:

- Monitoring the *Train Location* for a train which is leaving the Area of Control, until it is completely beyond the boundary of the Area of Control.
- Truncating the *Train Location* at the boundary for a train which is leaving the Area of Control, until it has zero length within the Area of Control.

It is also possible to use short TTD sections at boundaries of the Area of Control to determine when a train has left the area.

Projects may decide to maintain the *Train Location* beyond the border until ordering the train to terminate the communication session.

Projects may decide to implement different solutions at different borders of the Area of Control.

Operational Rules: None

Engineering Rules: None

6.16 SysF Request Movement Permission

6.16.1 Overview

When the MBS receives an MA Request message, then the OBU indicates that e.g., the driver has pressed the start button or that the time before reaching perturbation location is reached. In the first case, this additionally indicates that both the OBU and the driver are ready to accept authorisations (e.g. Movement Authority or SR Authorisation).).

Therefore, the MBS shall forward each MA Request message received from OBU to the PE by sending an Authorisation Requested message.

6.16.2 Inputs

MA Request message

6.16.3 Outputs

Authorisation Requested message

6.16.4 Functional requirements

REQ-0044

When the MBS receives an MA Request message from the OBU, then the MBS shall send an Authorisation Requested message to the PE indicating the reason for this request (e.g. driver has pressed the start button)

Rationale:

This is necessary to indicate to the PE that e.g., the driver has pressed the start button or the time before reaching perturbation location is reached.

Based on this information, the PE or TMS may decide to send a Movement Permission to the MBS or not.

Guidance: None

Operational Rules: None

Engineering Rules: None

6.17 General requirements

REQ-0045

The MBS shall be able to perform all the functions of the RBC Basic Interoperability Constituent (IC) in the Control-Command and Signalling Trackside Subsystem (see /BaInCon/)

Rationale: From ETCS point of view, the MBS is an RBC Basic Interoperability Constituent (IC). The MBS supplier shall supply an RBC-IC NoBo Certificate for his MBS Product.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-0010 FOR FURTHER RELEASE

MBS shall log all incoming and outgoing messages to the I_DIAG interface.

Rationale: This is requested for diagnostic.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-0046 FOR FURTHER RELEASE

If an OBU message has to be acknowledged (M_ACK = 1), MBS shall repeat this message periodically until the OBU acknowledgement is received. .

Rationale: MBS should send again a message if the OBU acknowledgement is not received after a period, because there is a risk that the OBU has not received the message.

Guidance: None

Operational Rules: None

Engineering Rules: None

6.18 SysF Update Movement Permission

6.18.1 Overview

6.18.2 Inputs

- *Train Location*
- “Request to shorten MA is granted message” according to I_OBU
- “Request to Shorten MA is rejected message” according to I_OBU

6.18.3 Outputs

- Movement Permission
- Message “Cooperative MP Request Granted” according to I_PE
- Message “Cooperative MP Request Rejected” according to I_PE

6.18.4 Functional requirements

REQ-0070

After MBS has granted a Movement Permission, it shall store the new Movement Permission as the current MP of the corresponding *Train Object*.

Rationale: A Movement Permission that has been granted shall become the currently active Movement Permission of a *Train Object*.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-0071

When there is an update of the *Train Location* then MBS shall modify the Movement Permission so that the start of the Movement Permission equals the rear of the *Train Location*.

Rationale: This ensures that any parts of the track that are not used by the train anymore can be (re-)used for train movements of other trains.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-0072

When MBS receives a “Request to Shorten MA is granted” message, then MBS shall modify the Movement Permission so that the end of the *Movement Permission Extent* equals the requested stop location and the *Risk Buffer* corresponds to the one received in the Cooperative Shortening Request, and subsequently informs PE by sending the “Cooperative MP Request Granted” message.

Rationale: When MBS has received the “Request to shorten MA is granted” message, then this implies that the train has accepted the new MA. Thus, the old part of the MA won’t be used by the train anymore and hence can be used for other train movements (e.g. for joining purposes)

The “Cooperative MP Request Granted” message is sent to explicitly inform PE that the co-operative shortening of MA was successful.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-0074

When MBS receives a “Request to Shorten MA is rejected” message then MBS shall provide this information by sending the “Cooperative MP Request Rejected” message to PE.

Rationale: As the OBU has not accepted the new MA in this case, the Movement Permission must not be updated. The message “Cooperative MP Request Rejected” is sent to explicitly inform PE that the co-operative shortening of MA was not successful.

Guidance: None

Operational Rules: None

Engineering Rules: None

6.18.5 Functional requirements for *Risk Path* update

REQ-0075

When any part of the Movement Permission is updated or deleted, if an *Allocation Section* does not overlap the *Movement Permission Extent* anymore, MBS shall delete the *Risk Paths* calculated from the dependent *Allocation Section* according to REQ-RP_SEARCH.

Rationale: Flank Protection is not needed anymore if the *Allocation Section* does not overlap the path anymore.

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-0076

MBS shall continuously monitor that every *Risk Path* is terminated according to REQ-SC_RP_TERM and if a *Risk Path* is not terminated correctly anymore, the *Risk Paths* of its associated Movement Permission shall be recalculated according to REQ-RP_SEARCH.

Rationale: If the risk mitigation method is not valid anymore, MBS shall search if other appropriate measures are still in place.

Guidance: This version of the requirement does not assume any degraded modes or violation of operational rules.

Operational Rules: None

REQ-0077

MBS shall continuously monitor that every *Risk Path* has no overlap according to

- REQ-SC_RP_TO
- REQ-SC_RP_UTO
- REQ-SC_RP_MP
- REQ-SC_RP_RB

and if an overlap is found, the *Risk Paths* of its associated Movement Permission shall be recalculated according to REQ-RP_SEARCH.

Rationale: If area between the *Allocation section* and the *Risk Path* terminating object is not free of vehicles or movements, the situation has to be reassessed.

Guidance: This version of the requirement does not assume any degraded modes or violation of operational rules.

Operational Rules: None

6.19 SysF supervise<Actor>Communication

Hint: <Actor> is a template for DR, TACS, PE, and OBU

6.19.1 Overview

This function supervises the communication state to the actor <actor>. It can detect, if the communication is established, lost (a communication never established is also considered as 'lost') established, and if there is change lost -> established or established -> lost.

6.19.2 Inputs

State of communication session between *MBS* and actor <actor>

6.19.3 Outputs

Events

- *<actor>CommEstablished* or
- *<actor>CommLost*

6.19.4 Functional requirements

REQ-1001

MBS shall observe the state of the communication between *MBS* and the actor *<actor>* and

- send the internal event *<actor>CommEstablished* when it detects that the communication session state changed from *lost* to *established;*
- send the internal event *<actor>CommLost* when it detects that the communication session state changed from *established* to *lost*.

Hint: For the OBU, the event *OBUCommLost* occurs when the communication session is lost in the sense of /ETCS/ SS026 3.5.4.2.1

Rationale: Central place to supervise communcation and let other capabilities react on this with the appropriate measure.

Guidance: The check can be performed by a *main loop* pattern centrally in *MBS*.

Operational Rules: None

Engineering Rules: None

6.20 SysF establish<Actor>Communication

Hint: <Actor> is a template for DR, TACS, PE, and OBU

6.20.1 Overview

This function establishes the communication state to the actor <actor> according to the related communication protocol.

6.20.2 Inputs

None

6.20.3 Outputs

(Changed) communication session state to <actor>.

6.20.4 Functional requirements

REQ-1002

When *MBS* detects that there is no communication established with actor <actor> AND *MBS* is in the role of the initiator of that communication, *MBS* shall establish the communication to <actor> actor according to the related communication protocol.

Rationale: None

Guidance: The check can be performed by a *main loop* pattern centrally in *MBS*.

Operational Rules: None

Engineering Rules: None

7 INTERFACE SPECIFICATIONS

7.1 DESCRIPTION OF THE EXTERNAL INTERFACE I_TACS

7.1.1 Role of the external interface

The interface I_TACS allows the Moving Block System:

- to send commands to the TACS to move switchable TAs to the required state, and
- to receive from the TACS the state of the TA.

Indeed, to enable a train run from A to B, the Moving Block System commands to the TACS the setting of the TA to the required state to allow the movement of the train from A to B.

To manage the train positioning and the movement of the trains, the Moving Block System also needs to acquire through the TACS the state of all the TA inside its *Area of Control* (AoC.)

The interface I_TACS covers the following interfaces defined in EULYNX:

- Subsystem – Train Detection System (SCI-TDS) if TTD is used
- Subsystem – Point (SCI-P)

7.1.2 Overview

REQ-0021

According to Project Configuration, the I_TACS interface shall implement TLS over TCP of the EULYNX Process data interface, as specified in the chapter 3 of /EuArch/.

Rationale: According to EULYNX, TACS communicates either by UDP or TLS over TCP. For new components, it is highly recommended to use TLS over TCP.

Guidance: None.

Operational Rules: None

Engineering Rules: None

7.1.3 Physical level

Not applicable, as the hardware definition of MBS is ouf of scope of the current specification.

7.1.4 Protocol level

REQ-0022

The lower layers (network layer, data link layer) of the I_TACS interface shall be compliant with /POS/.

Rationale: None

Guidance: None

Operational Rules: None

Engineering Rules: None

REQ-0023

The higher protocol layers (transport layer, safety, retransmission and redundancy layer and application layer) of the I_TACS interface shall be compliant with /POS//SCI/.

Rationale: I_TACS is according to the EULYNX specification

Guidance: None

Operational Rules: None

Engineering Rules: None

7.1.5 Application level

REQ-0024

The application layer of the I_TACS generic interface shall be compliant with /SCI-Gen/ and /SCI-GenIF/.

Rationale:	I_TACS is according to the EULYNX specification
Guidance:	None
Operational Rules:	None
Engineering Rules:	None

REQ-0025

The application layer of the of the I_TACS interface shall be compliant with /SCI-P/ for Point.

Rationale:	I_TACS is according to the EULYNX specification
Guidance:	None
Operational Rules:	None
Engineering Rules:	None

REQ-0026

The application layer of the I_TACS interface shall be compliant with /SCI-TDS/ for Train Detection System.

Rationale: None

Guidance: None

Operational Rules: None

Engineering Rules: None

7.1.6 Input Application Layer Messages

- EULYNX telegrams from TACS Point:
  - Msg_Point_Position : Message "Point Position"
  - Msg_timeout : Message "Timeout" – FOR FURTHER RELEASE
  - Msg_Ability_To_Move_Point : Message "Ability To Move Point" – FOR FURTHER RELEASE
- EULYNX telegrams from TACS Train Detection System:
  - Msg_TVPS_Occupancy_Status : Message "TVPS_Occupancy_Status"

7.1.7 Output Application Layer Messages

- EULYNX telegrams to TACS Point:
  - Cd_Move_point : Command "Move Point"

7.1.8 Implicit choices and justification

EULYNX protocol shall be implemented for I_TACS interface for the final target Baseline.

7.2 DESCRIPTION OF THE EXTERNAL INTERFACE I_PE

7.2.1 Role of the external interface

The interface I_PE allows the Moving Block System:

- to receive commands from the PE to supervise the TACS and trains according to the line operational needs defined by TMS, and
- to send information to PE to allow the line operation.

In the current version of the specifications, only the application layer messages are listed.

7.2.2 Overview

7.2.3 Physical level

Not applicable

7.2.4 Protocol level

Out of scope for this Release

7.2.5 Application level

Out of scope for this Release

7.2.6 Input Application Layer Messages

DPS Group Request

Movement Permission Request

Cooperative Shortening Request

7.2.7 Output Application Layer Messages

Request Granted (request id)

- This message indicates that a request has been successfully granted by MBS and is now being processed.

Request Rejected (request id, reason)

MBS Operational State Report (Object Id, reported state)

Authorisation Requested (Train Id, MA request reason)

Cooperative MP Request Granted

Cooperative MP Request Rejected

7.2.8 Implicit choices and justification

Not applicable

7.3 DESCRIPTION OF THE EXTERNAL INTERFACE I_OBU

7.3.1 Role of the external interface

The main objective of this interface is to provide movement authorities to allow the safe movement of trains on the Railway infrastructure area under the responsibility of the MBS.

In the current /ETCS/, this interface corresponds to the RBC - OBU interface.

The MBS can be interfaced to the FRMCS and/or GSM-R radio communication network(s).

7.3.2 Overview

7.3.3 Physical level

Not applicable

7.3.4 Protocol level

REQ-0047

The protocol layers of the I_OBU interface shall be compliant with /ETCS/ - SUBSET-037.

Rationale: None

Guidance: None

Operational Rules: None

Engineering Rules: None

7.3.5 Application level

REQ-0060

The application layer of the I_OBU generic interface shall be compliant with /ETCS/ - SUBSET-026, especially with Chapter 7 – ERTMS/ETCS language and Chapter 8 – Messages.

Rationale: I_OBU is according to the SUBSET-026 RBC - OBU interface.

Guidance: None

Operational Rules: None

Engineering Rules: None

7.3.6 Input Application Layer Messages

See /ETCS/ - SUBSET-026 chapter 8.6, Definition of Radio Messages from Train to Track

7.3.7 Output Application Layer Messages

See /ETCS/ - SUBSET-026 chapter 8.7, Definition of Radio Messages from Track to Train

7.3.8 Implicit choices and justification

Not applicable

7.4 DESCRIPTION OF THE EXTERNAL INTERFACE I_DR

7.4.1 Role of the external interface

By this interface, *MBS* gets the static *Topology Data*. This is the case both at startup and during run-time where there is the possibility to update existing *Topology Data* to a new version. Particularly it is possible to exchange a part of existing *Topology Data* e.g. as result of construction work.

7.4.2 Overview

Until release 4, *Topology Data* will cover the whole *Area of Control* and will immediately be valid (activated) after reception.

In a further release, *Topology Data* can cover an arbitrary part of the *Area of Control* and follow a lifecycle:

- First, they will be distributed (pre-loaded)
- Then, *MBS* will be asked for authorisation of the *Topology Data* activation where it checks for conflicting *Movement Permission*s and if there is no conflict, establishes a *Usage Restriction Area* to keep the updated area free of future *Movement Permission*s until the activation is finished
- Then, *Topology Data* become pre-activated and *MBS* can start to synchronise with the *TACS* (of changed or new *Trackside Asset*s)
- Finally, *MBS* is asked for activation, removes the *Usage Restriction Area* and uses the new data from now on

7.4.3 Physical level

Not applicable

7.4.4 Protocol level

Out of scope for current Release.

7.4.5 Application level

Out of scope for current Release.

All messages carry this generic header

- Parameter: messageNumber (unique identifier of the message type)
- Parameter: messageLength (total length of message)
- Parameter: dateTime (sending date and timestamp of message)

Further on, the parameter consumerId will be the unique identification of *MBS* (configurable value). The parameter DomainId is under discussion. It currently pretends that updateable *Topology Data* areas are fixed (pre-configured) but it shall be achieved that any sub-area, which cannot be pre-defined, shall be updateable. Until clarification it is used below, but the inherent future meaning shall be that the *Topology Data* themselves (parameter requestedDomainData are such that they allow identification of what sub-area they are replacing; the *DomainId* would then not be needed anymore.

Hint: for the mismatch of *Topology Data* and *Domain Data* (reflected in message names below) see the glossary entry for *Domain Data*.

7.4.6 Input Application Layer Messages

7.4.6.1 Domain Data

- Parameter: header
- Parameter: consumerId
- Parameter: DomainId

7.4.6.2 Domain Data Version Check Acknowledgement

- Parameter: header
- Parameter: DomainId (not used in current Release and under discussion)
- Parameter: DomainVersion (not used in current Release)

7.4.6.3 Activation Command

- Parameter: header
- Parameter: DomainId (not used in current Release and under discussion)
- Parameter: DomainVersion (not used in current Release)

7.4.6.4 Activation Commit Status

- Parameter: header
- Parameter: DomainId (not used in current Release and under discussion)
- Parameter: DomainVersion (not used in current Release)
- Parameter: activationCommitStatus

7.4.7 Output Application Layer Messages

7.4.7.1 Domain Data Request

- Parameter: header
- Parameter: consumerId
- Parameter: DomainId (not used in current Release and under discussion)
- Parameter: currentDomainVersion (not used in current Release)

7.4.7.2 Domain Data Acknowledgement

- Paramter: header
- Paramerter: DomainId (not used in current Release and under discussion)
- Parameter: DomainVersion (not used in current Release)
- Parameter: preLoadingStatus

7.4.7.3 Domain Data Usage Restriction Acknowledgement

- Parameter: header
- Parameter: DomainId (not used in current Release and under discussion)
- Parameter: DomainVersion (not used in current Release)
- Parameter: usageRestrictionStatus

7.4.7.4 Activation Acknowledgement

- Parameter: header

- Parameter: DomainId (not used in current Release and under discussion)
- Parameter: DomainVersion (not used in current Release)
- Parameter: activationAcknowledgement

7.4.8 Implicit choices and justification

Not applicable

7.5 Description of the external interface I_OP

For a further release.

7.6 Description of the external interface I_AS

For a further release.

7.7 Description of the external interface I_SEC

For a further release.

7.8 Description of the external interface I_Diagn_and_Maint

For a further release.

8 REFERENCES

/BaInCon/	Basic interoperability constituents in the Control-Command and Signalling Trackside Subsystem Table 5.2 in Legal framework of /CCSTSI/
/SysDef/	R2DATO D13.1 – Moving Block Specifications applying a train-centric approach Part 1 – System Definition
/CCSTSI/	Control Command and Signalling TSI Commission Implementing Regulation (EU) 2023/1695 of 10 August 2023
/ETCS/	ETCS Specifications Annex A for the /CCSTSI/ Set of Specifications (ETCS B4 R1)
/S2R/	S2R Moving Block Specification Release https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f58a710a&appId=PPGMS
/RCA/	RCA RCA Baseline 1 Release 0 https://public.3.basecamp.com/p/KeehzqFmXv5R2N7tGDjaEokq
/EULYNX/	EuLynx Baseline Set 4 Release 2 https://rail-research.europa.eu/system_pillar/system-pillar-outputs/trackside-assets-specifications/
/SD1DM/	SPT2-TransversalSystems TCCS SD1 - Data Model
/EuArch/	Eu.Doc.16 – EULYNX System architecture specification
/POS/	Eu.Doc.100 – Specification of Point of Service
/SCI/	Eu.Doc.92 – Interface definition SCI
/SCI-Gen/	Eu.Doc.93 – Interface specification SCI Generic
/SCI-P/	Eu.Doc.38 – Interface specification SCI-P
/SCI-TDS/	Eu.Doc.44 – Interface specification SCI-TDS

/SCI-LX/	Eu.Doc.112 – Interface specification SCI-LX
/SCI-GenIF/	Eu.Doc.119 – Generic interface and subsystem requirements for SCI
/ReqSubsP/	Eu.Doc.36 – Requirements specification for subsystem Point
/OpCon/	SP-CCS-TMS-CMS-Operational-vision.pdf (europa.eu) (?)
/RCA.Doc.61/	RCA APS Concept Operating State and APS Domain Objects
/RCA.Doc.62/	RCA APS Concept: Route setting and route protection
/GSL/	Geometric Safety Logic in a nutshell Note: this document already uses other abstract concepts than Drive Protection Section which are not yet agreed in the authors' working group. Please take them as indicative for understanding.
/FlankProtection/	ADI.023 Concept: Flank Protection (Allocation Section, *Risk Path*)
/SempR2/	SEMP Annex R2 - Requirements patterns syntax
/SempR3/	SEMP Annex R3 - Rules for writing textual requirements

Chapter	Reviewer	Comment	Answer	Meeting 21.11.2023
REQ-0010	Ivan	Only when it is discarded? Shouldn't all the messages be logged to the Diagnostic system?	TBD. I agree. Perhaps it would be better to consider an alarm (instead of event) in this case. This is in line with the comment of Bettina here after. This should be clarified within a general chapter "log and alarm" for a further release.	This should be clarified within a general chapter "log and alarm" for a further release. COMMENT TO BE KEPT
8.7 SYSF ESTABLISH COMMUNICATION SESSION WITH TACS	Daniel	from the requirements below, there are additional outputs: + order to establish a communication session + LOG of not established communication	TBD.	comment to be kept for further release, COMMENT TO BE KEPT
REQ-0016	Ivan	Should the establishment logged also in the Diagnosis interface? For analysing possible incidences, it can be interesting to know the time when the connection was established.		TBD. I agree, this should be clarified within a general chapter "log and alarm" for a further release. See previous comments. COMMENT TO BE KEPT
	Kostas	I would expect all operations to logged in for juridical reasons, Diagnostics would only log the abnormalities?	TBD. I agree, this should be clarified within a general chapter "log and alarm" for a further release. See previous comments	TBD. I agree, this should be clarified within a general chapter "log and alarm" for a further release. See previous comments. COMMENT TO BE KEPT

8.9 SYSF LOAD AND CHECK DOMAIN DATA	Kostas	[Minor] How about using the last validated data (if applicable) and triggering a rollback?	TBD. Not applicable to release 1 but for release 2 ?	COMMENT TO BE KEPT FOR FURTHER RELEASE

ANNEX 2: TEMPLATES

SysC: System Capability Template

Table 16 - Description of SysC: <Template>

Description	<Description of the capability to enable the reader to understand it>
Goal	<Short description what shall be achieved with the capability from a blackbox view>
Precondition(s)	- <Precondition1> - <Precondition…> - <Precondition n> Note: implicit preconditions are not mentioned here (e.g. when a position report received from the OBU is trigger for a capability, then it is obvious that the communication session is established)
Postcondition(s) (Success)	- <Postcondition 1> - <Postcondition…> - <Postcondition n> Note: Only show postconditions which are visible for external actors
Postcondition(s) (Failure)	- <Postcondition 1> - <Postcondition…> - <Postcondition n> Note: Only show postconditions which are visible for external actors
Involved actor(s)	- <Actor 1> - <Actor...> - <Actor n>
Trigger(s)	- <Trigger 1> - <Trigger...> - <Trigger n>
Main Sequence	<(Link to related scenario)>
Alternate Sequence	<(Link to related scenario)>
Failure Sequence	<(Link to related scenario)>
Comments	<Additional comment>

Scenario: Template Scenario

The scenario “Template Scenario” is shown. It contains a description of the elements to be used in the scenarios and some examples.

This Visio file template is available inside Project Place, directory "System Specification"

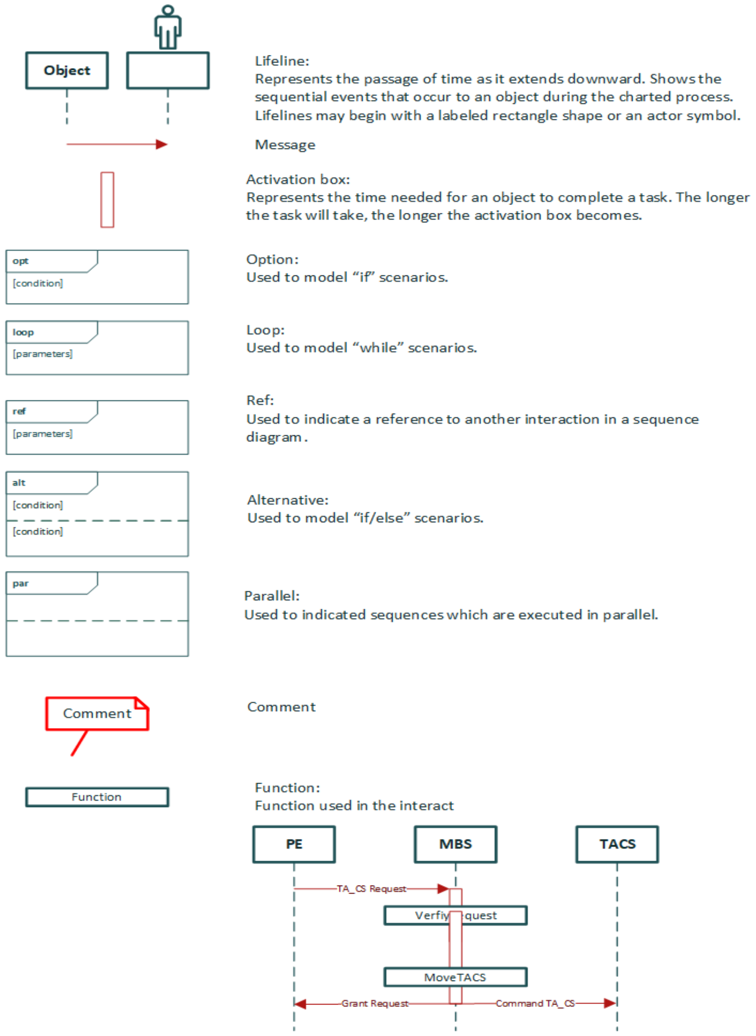


Figure 45 - Scenario: Template Scenario