

Rail to Digital automated up to autonomous train operation

D14.3 – Updated Moving Block Specification

Part 2 –Moving Block System Specification

Due date of deliverable: 30/04/2026

Actual submission date: 20/04/2026

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	<p>Second issue for Release 3.</p> <p>Update according to comments received on Revision 05.</p> <p>Chapter 5.10 and 6.11 updated for Flank Protection.</p> <p>Flank protection is now ready for review.</p> <p>Chapter 5.15 and related functions revisited for cooperative MP request.</p>
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	27/06/2025	First issue for Release 4
11	12/09/2025	<p>Second issue for Release 4.</p> <p>Update according to comments received on Revision 10.</p>
12	28/01/2026	First issue for Release 5
13	16/03/2026	<p>Second issue for Release 5.</p> <p>Update according to comments received on Revision 12.</p> <p>Operational rules and engineering rules are deleted in all requirements.</p>
14	20/04/2026	Update according to TMT review (chapter executive summary updated).

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 in WP14
Bertrand Badot Staffan Pettersson	ATSA	Author
Frank Skowron Martin Woiton	DB	Author
Nader Nayeri, Thomas Naulin Matthias Ruppert	GTSD	Author
Stephan Bischoff Martin Kemkemer	SBB	Author
Alfonso Lorenzo Lucia Blanco	ADIF (INECO)	Reviewer
Marta Garcia	CAF	Reviewer
Matthias Ruppert Felix Schaber Andrej Kiviriga Gerhard Wipplinger	GTSD	Reviewer
Daniel Kolar	AZD	Reviewer
Leon Walsh-Bijkerk Craig McLellan	SMO	Reviewer
Andreas Distler	DLR	Reviewer
Adelaide Vitiello	STS	Reviewer
Anders Lindfeldt	TRV (KTH)	Reviewer

Disclaimer

Funded by the European Union. Views and opinion expressed are however those of the author(s) only and do not necessarily reflect those of the European union. Neither the European Union nor the granting authority can be held responsible for them. The project FP2-R2DATO is supported by the Europe's Rail Joint Undertaking and its members."

EXECUTIVE SUMMARY

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

This document presents the **Updated System Specification of the Moving Block System (MBS)** developed within the *Rail to Digital – Automated up to Autonomous Train Operation (R2DATO)* programme.

It defines the **functional capabilities, system behaviour, interfaces, and core domain concepts** required to enable **train-centric ETCS-based moving-block operation**.

The Moving Block System is designed to deliver **higher network capacity, increased operational flexibility, and reduced lifecycle cost** while maintaining a high level of safety.

It achieves this by dynamically allocating track space to trains based on real-time train localisation, train integrity, and trackside information rather than relying on fixed block sections.

Within the ETCS framework, the MBS fulfils the role of an **RBC Basic Interoperability Constituent**, while extending beyond a conventional RBC by integrating trackside asset control, track path allocation, flank protection, and conflict management.

Interfaces are specified to ETCS On-Board Units, Trackside Asset Control and Supervision (EULYNX-based), Plan Execution, Operator Panel, and Digital Register.

This specification provides a **stable and comprehensive functional foundation** for demonstrators, prototype implementations, and safety analyses, and represents a key step toward a harmonised European Moving Block System capable of supporting progressively automated and autonomous railway operations.

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
CRE	Confirmed Rear End
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
OP	Operator Panel
PE	Plan Execution
R2DATO	Rail to Digital automated up to Autonomous Train Operation
RB	Risk Buffer
RCA	Reference CCS Architecture
RP	<i>Risk Path</i>
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
SP	Shunting Permission
SysC	System Capability
SysF	System Function
S2R	Shift2Rail
TA	Trackside Asset
TACS	Trackside Asset Control and Supervision
TCCS	Transversal CCS (Control Command and Signalling)

TDP	Train Detection Point
TDS	Train Detection System
TE	Track Edge
TEP	Track Edge Point
TES	Track Edge Section
THR	Tolerable Hazard rate
TIMS	Train Integrity Monitoring System
TO	Train Object
TTD	Trackside Train Detection
TVPS	Track Vacancy Proving Section (via /EULYNX/)
URA	Usage Restriction Area
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 WP14. Therefore, as long as there is no separate Glossary document available, care must be taken to keep the definitions synchronised.

Term	Definition
Allocation Section	<p><i>Allocation Sections</i> express gauge clearance conflicts between different tracks.</p> <p>For example, <i>Allocation Sections</i> are associated to the representation of switchable Track Assets and further track connections like diamond crossings.</p> <p>The <i>Allocation Sections</i> are used in terms of granting a MP request as condition for clearance in a certain area.</p> <p>See also /FlankProtection/</p>
Ambiguous position	<p>The position information contained in a Position Report (e.g. the SoM Position Report with status valid, or a Train Position Report message) can be considered as ambiguous in case MBS is not able to safely locate the train within the track layout. Since the 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.</p>
Area of Control	<p>The Area of Control is the topologically limited extent used here for defining the technical and operational responsibility of one instance of MBS.</p>
Assumed (train) position	<p>This is the position provided by the signaller in the Operator Panel for a train which the MBS cannot locate the train because its position is ambiguous or unknown.</p>
Authorisation	<p><i>Authorisation</i> refers to a permission granted to a train to proceed along a defined part of a track under specific conditions. Examples for such an Authorisation are an FS Movement Authority or a SR Authorisation.</p>
Demand	<p>See <i>Request</i></p>
Domain Data	<p>The <i>Domain Data</i> 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 <i>Domain Data</i>. Potential updates of <i>Domain Data</i> will be realised by a centralised provisioning process incl. synchronous activation of the new data version.</p> <p>Source: /SD1DM/</p>

Domain Object	<p>A <i>Domain Object</i> 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.</p> <p>The MBS Domain Object includes the MBS <i>Domain Data</i> and the <i>MBS Operational State</i>.</p>
Drive Protection Section	<p>A <i>Drive Protection Section</i> is a linear contiguous stretch of track with a driveability (passage possible yes/no) state.</p> <p>A <i>Drive Protection Section</i> represents a <i>Track Edge Section</i> 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).</p> <p>Source: RCA</p>
Known position	<p>The position reported by a train is known and unambiguous to the MBS, i.e. there is no doubt about where the front of the train is located in the MBS Area of Control.</p>
MBS Operational State	<p><i>MBS Operational State</i> is the collection of all of <i>Domain Objects</i> instantiated by the MBS to manage its operations and supervise the train movements.</p> <p>This includes:</p> <ul style="list-style-type: none"> • <i>Train Objects</i>, • <i>Unresolved Trackbound Objects</i>, • <i>Trackside Asset Objects</i>, • <i>Movement Permission</i>, • <i>Usage Restriction Areas</i>, • Etc...
MBS is operational	<p><i>MBS is operational</i> 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.</p>
Movement Permission	<p>The <i>Movement Permission</i> defines the part of the track that is reserved for the movement of a train.</p> <p>It includes:</p> <ul style="list-style-type: none"> - <i>Movement Permission Extent</i> - <i>Risk Buffer</i> - <i>Risk Path</i> - Requested Maximum Speed

	<ul style="list-style-type: none"> - ETCS Movement Mode - List of DPS Groups that must not be used as flank protection measure
Movement Permission Extent	<p>A <i>Movement Permission Extent</i> is a linear contiguous stretch of track that is reserved for the movement of a train. The <i>Movement Permission</i> is translated to an authorisation (e.g. Movement Authority) according to the /ETCS/ - SUBSET-026 that is transmitted to the train.</p> <p>The <i>Movement Permission Extent</i> is part of the Movement Permission.</p> <p>Source: RCA</p>
Non-switchable Trackside Asset	<p>A <i>Non-switchable Trackside Asset</i> is a Trackside Asset which provides information to the MBS (e.g. <i>Trackside Train Detection</i>) but cannot be controlled to a particular state.</p>
Operator	<p><i>Operator</i> is a generic term being an alias for e.g. Signaller, Dispatcher</p>
Request	<p><i>Request</i> and <i>demand</i> are messages towards MBS that require an action. While a <i>request</i> undergoes all syntax and safety checks (and is rejected if one fails), a <i>demand</i> has fewer checks to fulfil. Violated checks are reported back.</p>
Risk Buffer	<p>The <i>Risk Buffer</i> is a linear contiguous stretch of track that serves as the overrun protection and includes a safety margin for the overhang of vehicles and for the event of a rollback of a chased train. It is part of a Movement Permission.</p> <p>A <i>Risk Buffer</i> exists if there is a Danger Point or a safe margin (project specific) greater than zero.</p> <p>Source: RCA</p>
Risk Path	<p>A <i>Risk Path</i> 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 <i>Movement Permission Extent</i>.</p> <p>A Movement Permission can contain zero or more <i>Risk Paths</i>.</p> <p>Source: RCA</p>
Shunting Limit	<p>A <i>Shunting Limit</i> exists today usually at an entry signal at a station or between the last point and the entry signal. Such a limit will still be needed so that the <i>Shunting Permission</i> does not have to end at a shunting signal of another station (if this signal exists at all).</p>
Shunting Permission	<p>A <i>Shunting Permission</i> defines the part of track that is reserved for a shunting movement. It starts at a shunting signal and ends at another shunting signal, <i>Buffer Stop</i> or a <i>Shunting Limit</i>. A <i>Shunting Permission</i> reflects a movement that is supervised by a signaller in contrast to a shunting area where the movement is controlled and supervised by the</p>

	shunting personnel on site. Such shunting areas are currently out of scope of MBS.
Switchable Trackside Asset	A <i>Switchable Trackside Asset</i> is a <i>Trackside Asset</i> which enables (e.g. points, derailleurs, 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 <i>Domain Data</i>
Track Edge	<p><i>Track Edge</i> is a linear object that defines an uninterrupted stretch of a railway track without divergence or convergence. A <i>Track Edge</i> is defined along the centre line of the 2D or 3D track alignment and has a finite length.</p> <p>The <i>Track Edges</i> have an implicit direction (from start to end).</p> <p>The start/end of <i>Track Edge</i> shall correspond to the location of a simple point, or any form of end of track.</p> <p>Source: RCA, /SD1DM/</p>
Track Edge Point	<p>A <i>Track Edge Point</i> is a spot location on a <i>Track Edge</i>.</p> <p>Example usage: balise location</p> <p>Source: RCA, /SD1DM/</p>
Track Edge Section	<p>A <i>Track Edge Section</i> is a linear extent between two <i>Track Edge Points</i> on (the same) <i>Track Edge</i> and can be directed.</p> <p>Example usage: Track properties like gradient, SSP, DPS</p> <p>Source: RCA, /SD1DM/</p>
Trackside Asset	<p><i>Trackside Assets</i> 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 <i>Trackside Asset Control and Supervision</i>.</p> <p>See also <i>Switchable Trackside Asset</i> and <i>Non-switchable Trackside Asset</i> definition.</p>
Trackside Asset Control and Supervision	The <i>Trackside Asset Control and Supervision</i> is a subsystem supervising and controlling <i>Trackside Assets</i> .
Trackside Train Detection (Section)	<p><i>Trackside Train Detection</i> is a system which determines the occupancy status of TTD sections. TTD section may be a Track Circuit or an Axle Counting system.</p> <p>EULYNX synonym: Track Vacancy Proving Section.</p>

Train Detection Point	<p>The function which reports the passing of a train, using a Detection point. It can be used for activation of level crossings or hot box detectors and further functions. Depending on configuration, the TDP can report for a given direction or all directions.</p> <p>Source: EULYNX Glossary</p>
Supervised at standstill	<p>A train is <i>supervised at standstill</i> if the train is at standstill and the Movement Permission extent ends at the train front.</p>
Train Location	<p><i>Train Location</i> is the MBS interpretation of the location of the train, based on Position Reports, Validated Train Data and other inputs if available, e.g. TTD. <i>Train Location</i> is a linear contiguous stretch of track that has a front and a rear.</p> <p>X2R5 source: Train Location</p> <p>RCA source: rMOB extent</p>
Train Object	<p><i>Train Object</i> is the object needed by the MBS to manage a connected train.</p> <p>Note: This <i>Train Object</i> could nevertheless correspond to a train not (yet) localised by MBS.</p> <p>If a <i>Train Object</i> is referenced as a geometric extent, the extent is the extent of the <i>Train Location</i>.</p> <p>RCA source: (rMOB)</p>
Position Report	<p>The term <i>Position Report</i> 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.</p>
Unambiguous position	<p>See “Known position”.</p>
Unknown position	<p>The position reported by a train is not known to the MBS, either because the train indicates its position as unknown or invalid in the SoM Position Report, or because the identity of the LRBG is not known to the MBS.</p>
Unresolved Trackbound Object	<p><i>Unresolved Trackbound Object</i> 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 (<i>Train Object</i>).</p> <p>RCA source: uMOB</p> <p>X2R5 source: Unknown Track Status Area (partly)</p>

Usage Restriction Area	A <i>Usage Restriction Area</i> limits or constraints operation on a part within the Area of Control. A <i>Usage Restriction Area</i> can be created according to an Operational Plan (e.g. for enabling construction works) or in response to an incident (e.g. as a mitigation measure). There are various limitations possible for A <i>Usage Restriction Area</i> , e.g. speed restriction, full track closure or deactivate automatic operation
------------------------	--

TABLE OF CONTENTS

Acknowledgements.....	3
Report Contributors.....	3
Executive Summary	5
Abbreviations and Acronyms	6
Glossary	8
Table of Contents.....	14
List of Figures	17
List of Tables	19
1 Introduction	20
2 Scope of work	21
2.1 Limitations	22
3 Approach and methodology.....	26
4 MBS Overview	28
5 System Capabilities Specification.....	29
5.1 SysC: Start and Maintain MBS.....	30
5.2 SysC: Preload Topology Data.....	35
5.3 SysC: Approve Topology Data activation	37
5.4 SysC: Activate Topology Data	37
5.5 SysC: Respond to initiation of communication session by PE/OP	38
5.6 SysC: Start communication with one TACS	39
5.7 SysC: Respond to initiation of communication session by OBU	40
5.8 SysC: Control <i>Switchable Trackside Assets</i>	43
5.9 SysC: Overwrite DPS State	44
5.10 SysC: Revoke Overwrite DPS State	46
5.11 SysC: Shutdown MBS	47
5.12 SysC: Update <i>MBS Operational State</i>	47
5.13 SysC: Report <i>MBS Operational State</i>	53
5.14 SysC: Start of Train	54
5.15 SysC: Provide Authorisation to Train	56
5.16 SysC: Terminate Train Mission.....	59
5.17 SysC: Shorten MA cooperatively	63
5.18 SysC: Supervise Trains and Trackside Assets	64
5.19 SysC: Revoke or restrict authorisation.....	66
5.20 SysC: Continue after Train Trip	69
5.21 SysC: Recovering Degraded TTD Situations.....	70

5.22	SysC: Manage Usage Restriction Area	77
5.23	SysC: Authorise Shunting.....	84
5.24	SysC: Set Shunting Permission.....	85
5.25	SysC: Supervise Shunting Permission	86
5.26	SysC: Update Shunting Permission.....	88
5.27	SysC: Handle Emergency Stop for Shunting Signal	90
5.28	SysC: Revoke Shunting Permission	91
6	System Function specifications	93
6.1	General requirements	96
6.2	SysF Report <i>MBS Operational State</i>	97
6.3	SysF Authorise TA State Request.....	98
6.4	SysF Translate TA State request to TACS command	107
6.5	SysF Send TACS command	108
6.6	SysF Authorise DPS Overwrite Demand.....	108
6.7	SysF Execute DPS Overwrite Demand.....	110
6.8	SysF Authorise Revoke DPS Overwrite Demand.....	110
6.9	SysF Execute Revoke DPS Overwrite Demand	111
6.10	SysF Update <i>Domain Object</i> state	113
6.11	SysF Preload Topology Data.....	117
6.12	SysF Assign a safe value to a <i>Domain Object</i>	118
6.13	SysF Create <i>Train Object</i>	119
6.14	SysF Localise Train.....	121
6.15	SysF Manage Unresolved Trackbound Object	143
6.16	SysF Authorise MP Request	165
6.17	Authorise Cooperative Shortening Request.....	205
6.18	SysF Translate MP Request to Movement Authority	209
6.19	SysF Translate MP Request to SR Authorisation	214
6.20	SysF Translate Cooperative Shortening Request to Request to Shorten MA	216
6.21	SysF Delete <i>Train Object</i>	217
6.22	SysF Supervise Trains and Trackside Assets.....	220
6.23	SysF Revoke or restrict authorisation	222
6.24	SysF Authorise Stop Train Request	228
6.25	SysF Authorise Release Stop Train Request.....	230
6.26	SysF Update Movement Permission.....	231
6.27	SysF Check TTD Section Failure Status	235
6.28	SysF Reset TTD section by MBS	238

6.29	SysF Reset TTD section by Operator	239
6.30	SysF Supported Reset of TTD section by Operator	240
6.31	SysF Reset of TTD section by Operator using Sweeping	242
6.32	SysF Supervise<Actor>Communication	243
6.33	SysF Establish<Actor>Communication.....	244
6.34	SysF Authorise Create URA	245
6.35	SysF Create URA.....	247
6.36	SysF Authorise Delete URA	248
6.37	SysF Delete URA	249
6.38	Provide SH Confirmation Request.....	250
6.39	Authorise Shunting	250
6.40	SysF Authorise SP Request	251
6.41	SysF Update Shunting Signal.....	259
6.42	SysF Update Shunting Permission	262
6.43	SysF Authorise Shunting Signal Stop Demand.....	270
6.44	SysF Supervise Shunting Permission.....	270
6.45	SysF Set Shunting Signal to Stop.....	272
6.46	SysF Authorise Revoke SP Demand	274
6.47	SysF Revoke Shunting Permission	277
7	Interface Specifications	278
7.1	Description of the external interface I_TACS	278
7.2	Description of the external interface I_PE	280
7.3	Description of the external interface I_OBU	282
7.4	Description of the external interface I_DR.....	283
7.5	Description of the external interface I_OP.....	285
7.6	Description of the external interface I_AS	288
7.7	Description of the external interface I_SEC.....	288
7.8	Description of the external interface I_Diagn_and_Maint	288
8	References.....	289
	Annex 1: templates	290

LIST OF FIGURES

Figure 1 – System Boundaries	28
Figure 2 – Scenario pattern: Initiate communication.....	31
Figure 3 – Scenario pattern: Respond to communication status.....	32
Figure 4 - Scenario: Start and Maintain MBS	35
Figure 5: Scenario to pre-load Topology Data.....	37
Figure 6 - Scenario: Respond to Initiation of communication session by PE/OP	39
Figure 7 - Scenario: Start communication session with a TACS.....	40
Figure 8 - Scenario: Respond to initiation of communication session by OBU.....	42
Figure 9 - Scenario: Control <i>Switchable Trackside Assets</i>	44
Figure 10 - Scenario: Overwrite Switchable Trackside Asset State	46
Figure 11 - Scenario: Revoke Overwrite DPS State	47
Figure 12 - Scenario 1: Update <i>MBS Operational State</i> when TA state report is received.....	49
Figure 13 - Scenario 2: Update <i>MBS Operational State</i> when Position Report or validated train data are received	50
Figure 14 - Scenario 3: Update of status when no communication with TACS anymore	51
Figure 15 - Scenario 4: Update of <i>MBS Operational State</i> when no communication with OBU anymore	52
Figure 16 - Scenario 5: Update <i>MBS Operational State</i> when a request for an assumed train position is received.....	53
Figure 17 - Scenario: Report of <i>MBS Operational State</i> when triggered.....	54
Figure 18 - Scenario 1: Start of Train	56
Figure 19 - Scenario : Provide MA to Train	58
Figure 20 - Scenario : Provide SR Authorisation to Train	59
Figure 21 - Scenario 1: Train End of Mission	61
Figure 22 - Scenario 2: Termination of communication session by OBU	62
Figure 23 - Scenario 3: end mission when no communication anymore with an OBU	62
Figure 24 - Scenario 1: Shorten MA cooperatively	64
Figure 25 Scenario 1 MBS supervises the issued authorisation and detects that at least one safety check of an already issued authorisation is violated.	66
Figure 26 Scenario 1 Revoke or restrict authorisation due to a command received by OP.....	68
Figure 27 Scenario 2 Revoke or restrict authorisation due to a violation of a safety check.....	69
Figure 28 - Scenario : Train Trip	70
Figure 29 - Scenario 1: Automatic Reset TTD Section	73
Figure 30 - Scenario 2: Manual Reset TTD Section with Manual Operational Clearance	74
Figure 31 - Scenario 3: Supported Reset TTD Section with Using Restriction Area	75
Figure 32 - Scenario 4: Reset TTD Section with TTD capability Sweeping.....	76

Figure 33: Illustration of URA effect.....	78
Figure 34: Scenario to create Usage Restriction Area (by PE).....	80
Figure 35: Scenario to create Usage Restriction Area (by OP).....	81
Figure 36: Scenario to delete Usage Restriction Area	82
Figure 37: Scenario: Authorise Shunting.....	85
Figure 38 - Scenario : Set Shunting Permission	86
Figure 39 - Scenario : Supervise Shunting Permission	88
Figure 40 - Scenario : Update Shunting Permission	90
Figure 41 - Scenario : Handle Emergency Stop for Shunting Signal.....	91
Figure 42 - Scenario : Revoke Shunting Permission	92
Figure 43: Terms used for Train Location	122
Figure 44: Train Location from Start of Mission Position Report.....	125
Figure 45: Front of Train Location updated from new Position Report.....	127
Figure 46: Rear of Train Location updated from new Position Report, Integrity Confirmed.....	128
Figure 47: Train Location when receiving Validated Train Data during Start of Mission	129
Figure 48: Train Location when receiving Validated Train Data, L_TRAIN decreased.....	130
Figure 49: Train Location when receiving Validated Train Data, L_TRAIN increased.....	131
Figure 50: Train with Train Integrity confirmed Sweeping the Train Location of a chased Train with integrity not confirmed	132
Figure 51: Shortening of front of Train Location due to clear TTD	133
Figure 52: No shortening of front of Train Location due to clear TTD	134
Figure 53: Shortening of rear of Train Location due to clear TTD.....	135
Figure 54: No shortening of rear of Train Location due to clear TTD	135
Figure 55 Extension of Train Location when train passes TTD limit	136
Figure 56 Moving of Train Location by Cleared TTD	137
Figure 57 Extension of Train Location after Mute Timer has expired by Occupied TTD	140
Figure 58: Train Location after confirmation of Train Integrity	148
Figure 59: UTO creation when receiving Validated Train Data, L_TRAIN decreased	149
Figure 60: Unresolved Trackbound Object remains when Front Train after Splitting leaves	150
Figure 61: Train with Train Integrity confirmed Sweeping an <i>Unresolved Trackbound Object</i>	152
Figure 62: Existing <i>Unresolved Trackbound Object</i> swept by a passing train	152
Figure 63: Existing <i>Unresolved Trackbound Object</i> cannot be swept by the train	153
Figure 64: UTO created by rear moving forward for a train with Integrity not confirmed	154
Figure 65: Short Unresolved Trackbound Object at crossover	155
Figure 66: Creation of Unresolved Trackbound Object for unexpected Clear TTD	160
Figure 67: UTO propagation with a train in the same direction.	161
Figure 68: UTO propagation with a train in the opposite direction.	162

Figure 69: UTO propagation over a diverging point.....	162
Figure 70: UTO propagation over a converging point.....	163
Figure 71: UTO creation for a non-integer train.....	164
Figure 72 - Scenario: Template Scenario.....	292

LIST OF TABLES

Table 1 – Description of SysC: Start and Maintain MBS.....	34
Table 2 – Description of SysC: Respond to initiation of communication session by PE/OP.....	38
Table 3 – Description of SysC: Start communication with one TACS.....	39
Table 4 – Description of SysC:.....	43
Table 5 – Description of SysC: Overwrite DPS State.....	44
Table 6 – Description of SysC: Revoke Overwrite DPS State.....	46
Table 7 – Description of SysC: Update <i>MBS Operational State</i>	47
Table 8 – Description of SysC: Report <i>MBS Operational State</i>	53
Table 9 – Description of SysC: Provide Authorisation to Train.....	56
Table 10 – Description of SysC: Terminate Train Mission.....	59
Table 11 – Description of SysC: Shorten MA cooperatively.....	63
Table 12 – Description of SysC: Supervise train and trackside assets.....	65
Table 13 – Description of SysC: Revoke or restrict authorisation.....	67
Table 14 – Description of SysC: Set Shunting Permission.....	85
Table 15 – Description of SysC: Update Shunting Permission.....	88
Table 16 – Description of SysC: Emergency Stop for Shunting Signal.....	90
Table 17 – Description of SysC: Revoke Shunting Permission.....	91
Table 18 – Reasons to create or move <i>Train Location</i>	123
Table 19 – Reasons to delete <i>Train Location</i>	123
Table 20 – Reasons to create or extend Unresolved Trackbound Object.....	144
Table 21 – Reasons to remove (even partly) Unresolved Trackbound Object.....	144
Table 22 – <i>Unresolved Trackbound Object</i> Stored Data.....	146
Table 23 – Flank Protection measures configuration.....	168
Table 24 - Description of SysC: <Template>.....	290

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.

The work is continued in the task 14.4 “Moving Block - Update of Moving Block Specification”. It is organized in two new releases (release 4 and 5).

As a result of these tasks, 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 5 of the System Specification is defined as follows¹:

Capabilities:

- Start up the system
- Load *Domain Data* at start-up
- Establish, maintain and terminate communication session with *Trackside Assets*
- Establish, maintain and terminate communication session with ETCS on-board
- Control the *Trackside Assets* (SCI-P, SCI-TDS, SCI-LS for SH Light Signals)
- 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 movement (Movement Authority, SR authorisation, SH authorisation, 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 Assets* within its *Area of Control*
- Store an up-to-date, reliable and consistent *MBS Operational State* and provide this to consuming systems (PE and OP)
- Supervise trains and *Trackside Assets* to prevent railway accidents (collision, derailment, over-speeding)
- Manage Usage Restriction Area

Interface with

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

The following needs are covered:

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

¹ Only underlined text is new compared to previous releases

- 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, SCI-TDS and SCI-LS for SH Signals are considered.

2.1 LIMITATIONS

This chapter contains 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).
- 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.

2.1.1 General limitations

The following interfaces according to /SysDef/ are out of scope for this release:

- I_SEC: interface to Security Service (KMC+PKI)
- I_Diagn_and_Maint: interface to Diagnostics System
- I_AS: interface to Adjacent System
- I_TACS: for interface to TACS, only SCI-P and SCI-TDS and SCI-TDS for SH Signals are considered
- For interfaces I_PE, I_DR, and I_OP, Protocol level and Application level are not specified.

On-line partial update of the Topology data is out of scope

Only System Version 2.1 of /ETCS/ is supported for the current release.

- 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.

Transitions (from/to adjacent interlockings, RBC, and MBS) are out of scope. This excludes ETCS modes UN, SN for the current release.

2.1.2 No/late availability of System Pillar input documents

Due to no/late availability of System Pillar documents, they were not used as a formal input of WP13 and WP14.

2.1.3 Operational rules and engineering rules are excluded

Operational rules and engineering rules have not been analysed and are not part of the MBS Specification.

2.1.4 No THR objective defined

No THR objectives are given in the MBS specification.

The scope of the MBS is broader than that of an RBC as it also includes functions that are outside the ETCS reference architecture (e.g. an RBC is not responsible for managing points or for checking for conflicting routes).

The THR_{Trackside} in Subset-091 applies only the ETCS trackside and excludes failures of functions that are considered to be outside the reference architecture.

It has not been analysed which functions of the MBS are considered to be part of the reference ETCS architecture and therefore covered by the THR_{Trackside} defined in Subset-091.

2.1.5 Trailed point may apply a safety reaction

Due to vibrations caused by the train itself while the points are being traversed, the detection that the points are in the required position may be temporarily lost.

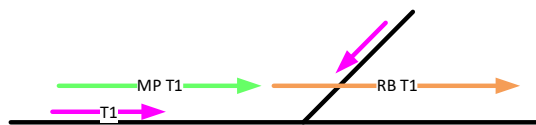
Therefore, some infrastructure managers decided that RBC has to evaluate first whether this has been caused by the train itself or not before taking any action. This is requested at least by Spain as well as DB customer explicitly in their customer requirement specifications today.

This aspect is not covered in MBS specification. A trailed point inside an Movement may cause a safety reaction and the train may apply emergency brakes.

2.1.6 Flank Protection is not performed for the Risk Buffer

Protection is excluded on the Risk Buffer in the current Release (see chapter 6.15.1.1. Flank Protection)

This may not meet the safety principles currently applied in some countries. Even if the authorised movement does not exceed its MP extent, it could nonetheless be put into danger by an unauthorised/uncontrolled movement entering at the risk buffer. E.g. consider a set of facing points close to the start of the risk buffer. An unauthorised vehicle could trail through the points and enter the path of the authorised train. See example below.



Safety risk should be evaluated as this seems to add protection (flank protection) on a margin (risk buffer).

2.1.7 Train length delay is not considered for URA type eoaExclusion

In the current edition it is not foreseen that a distinction is made whether the train has fully left a URA of this type or only its front end.

While for a Radio Hole it is sufficient, it might be desirable to check that the full train extent has left the URA in order to fulfil its constraint (example: train completely left a bridge covered by an eoaExclusion URA to avoid stopping on the bridge).

2.1.8 CR 1370 (TSI 2023) considered as mandatory for Moving Block

CR 1370 (Relocation without Linking) shall be considered essential for safe Moving Block operation.

If CR 1370 is not implemented in ETCS onboard system, the odometry error may be wrongly re-evaluated when a train passes over a balise group and no linking information is available onboard.

Such behaviour can lead to:

- Incorrect determination of the Train Confirmed Rear End,
- Incorrect computation of the Minimum Safe Rear,
- Potential issuance of an over-extended Movement Authority (MA) to a following train in Moving Block.

Therefore, to ensure the safety and correctness of train positioning within Moving Block, CR 1370 shall be implemented in the ETCS onboard system.

2.1.9 Train Integrity confirmed by driver is out of scope

Train integrity confirmed by driver is not implemented in MBS Specification as it is not possible to guarantee that the information provided by the driver is safe.

2.1.10 Means for revocation of SR Authorisations

Practically, the SR authorisation can be revoked also with sending new $D_SR = 0$.

This revocation option does not exist in the current release.

Closing the cabin or UES are the only options available today to reroute a train in SR.

2.1.11 No additional protection against supervised train overpassing the Movement Permission end

MBS will allow two trains to be routed directly towards each other, even at high speed, on the same track, possibly even with overlapping risk buffers.

This needs to be analysed and to be accepted by national safety authorities, even if the risk buffers are not overlapping. It would be difficult to argue that the risks are being controlled so far as is reasonably practicable (or whatever criteria the NSA uses as the basis for risk acceptance)

Additional controls may be considered in the future for such cases, such as limitations on the speed, or requiring additional safety margins to ensure the risks are adequately controlled.

2.1.12 Management of Shunting movements

SH Areas are out of scope, only SH Permissions (used to allocated route for SH movement and set the aspect of SH Signals) are managed.

Note that SH Signal always shows stop if there is no SP Request (i.e. SH Signal showing stop only means that train shall not pass the signal in SH mode), the setting of SH signal to dark is not foreseen for other train movements. So, SH Signal shall be ignored by the driver in other mode than SH (e.g. FS, OS, SR).

No risk buffer is possible today beyond the Shunting Signal for SP Permission. This means that there is no additional provision/margin taken against a shunting train passing the Shunting Signal.

Mode SH is never given by Trackside (no MA with Mode Profile SH is sent by MBS), Shunting shall be selected by driver.

Mode SM is out of scope, as ETCS System Version 2.1 is considered for the current release.

2.1.13 ATO is out of scope

Modes AD is out of scope as ETCS System Version 2.1 is considered for the current release

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.

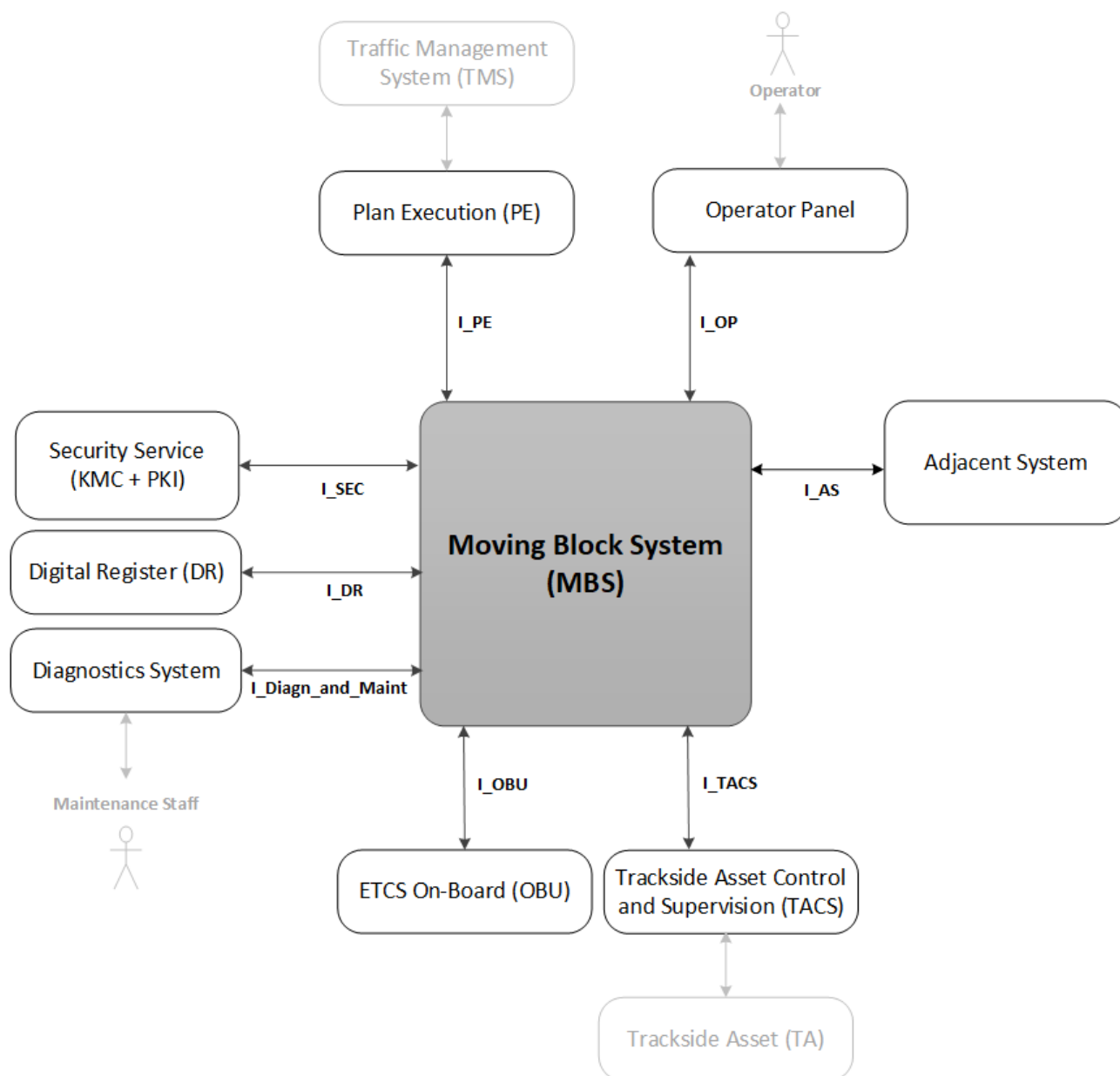


Figure 1 – System Boundaries

Note: Systems/Actors shown in grey have no direct interface with the Moving Block System.

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 <i>Trackside Assets</i> (TA) via specified interfaces within its <i>Area of Control</i> (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 5.16 SysC: Terminate Train Mission
MBS manages communication sessions with PE and OP via their specific interfaces.	5.5 SysC: Respond to initiation of communication session by PE
MBS controls all TAs within its AoC.	5.8 SysC: Control <i>Switchable Trackside Assets</i> 5.9 SysC: Overwrite DPS State 5.10 SysC: Revoke Overwrite DPS State 5.21 SysC: Recovering Degraded TTD Situations
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.	5.14 SysC: Start of Train 5.12 SysC: Update MBS Operational <i>State</i>
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.	5.15 SysC: Provide Authorisation to Train 5.17 SysC: Shorten MA cooperatively 5.20 SysC: Continue after Train Trip
MBS issues authorisations for train movements based on requested and accepted track path allocations.	5.15 SysC: Provide Authorisation to Train 5.23 SysC: Authorise Shunting 5.24 SysC: Set Shunting Permission
MBS supervises trains and TAs to prevent railway accidents. This includes especially any collision, derailment or over-speeding.	5.18 SysC: Supervise Trains and Trackside Assets 5.19 SysC: Revoke or restrict authorisation 5.25 SysC: Supervise Shunting Permission

	5.26 SysC: Update Shunting Permission 5.27 SysC: Handle Emergency Stop for Shunting Signal 5.28 SysC: Revoke Shunting Permission
MBS stores an up-to-date, reliable and consistent current <i>Operational State</i> and provides this Operational State to systems connected to MBS.	5.13 SysC: Report <i>MBS Operational State</i>
MBS manages <i>Domain Data</i> 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
<i>MBS</i> manages restrictions of track usage and trackside asset operation (Usage Restriction Area – URA).	5.22 SysC: Manage Usage Restriction Area
MBS handles a safe transition of train movement from and to adjacent systems.	Out of scope for current releases
Not Applicable	5.1 SysC: Start and Maintain MBS 5.11 SysC: Shutdown MBS

The following capabilities are not defined in the current further release:

- 5.3 SysC: Approve Topology Data activation
- 5.4 SysC: Activate Topology Data
- 5.11 SysC: Shutdown MBS

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

Please refer to “Annex 1: 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*: Depending on the configuration, *MBS* is responsible to initiate the communication.

(MBS as session initiation responder)

- *PE* and *OP*: *MBS* is a service to *PE* and *OP* which serves requests to set *Switchable Trackside Assets* and grant *Movement Permissions*. *MBS* therefore acts in a server role which means that *PE* and *OP* establish 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/).
- *TACS*: Depending on the configuration, *TACS* is responsible to initiate the communication.

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):

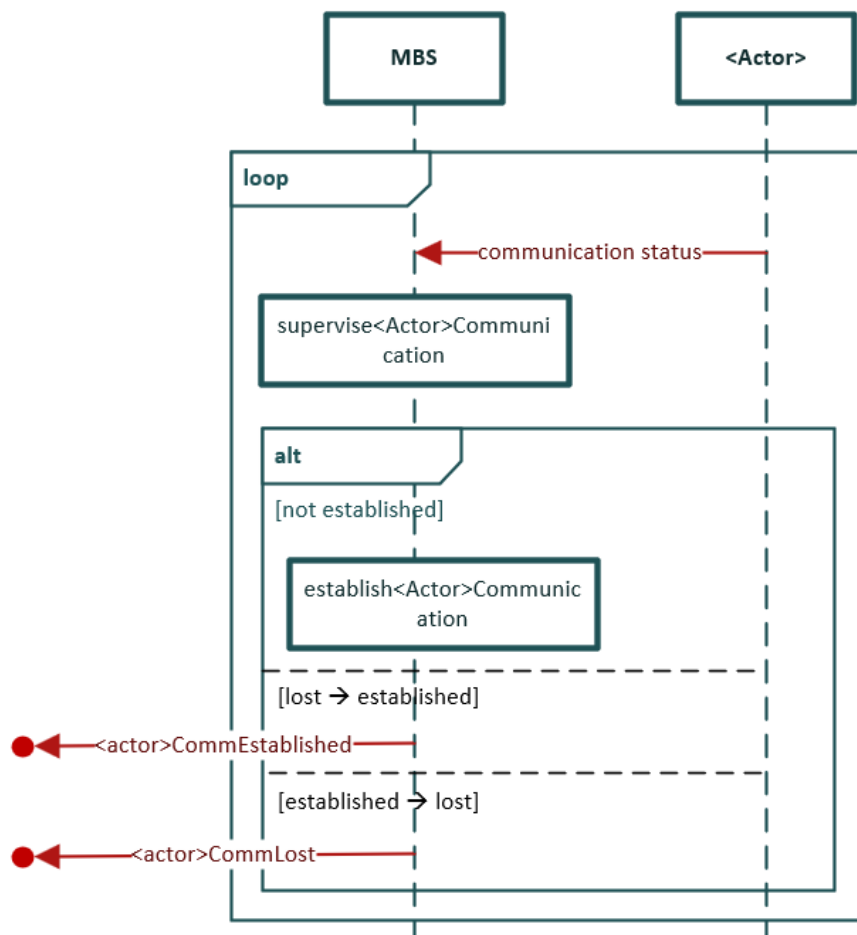


Figure 2 – Scenario pattern: Initiate communication

<Actor> can be DR or TACS.

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

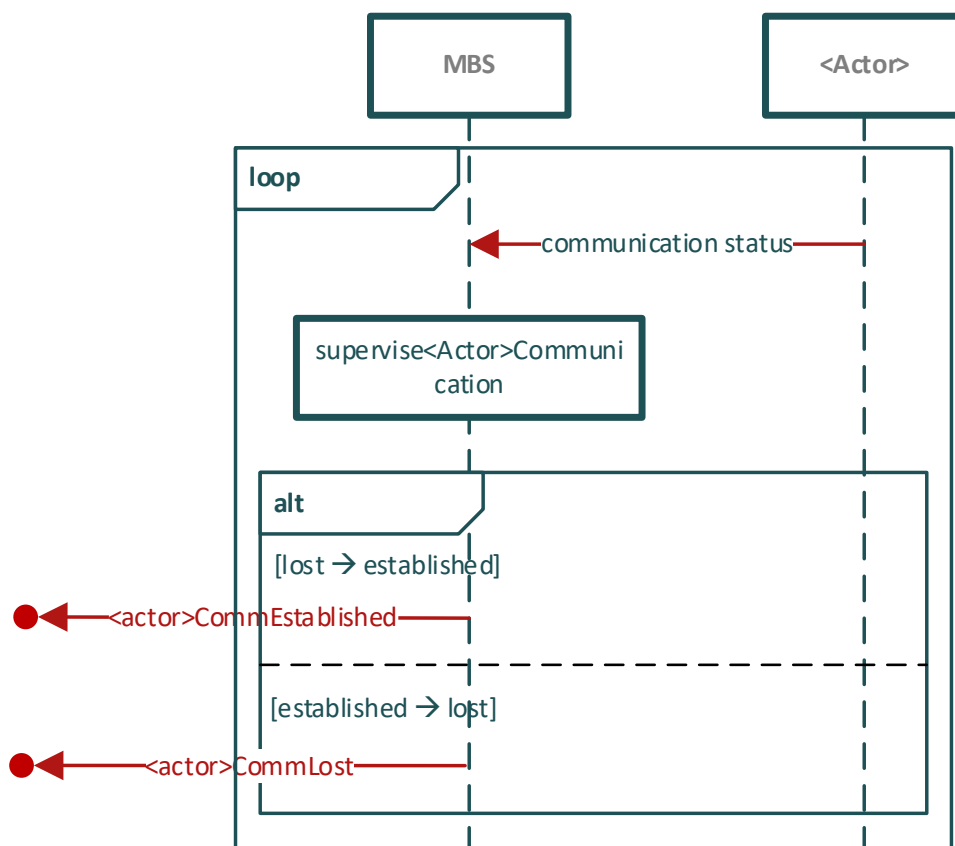


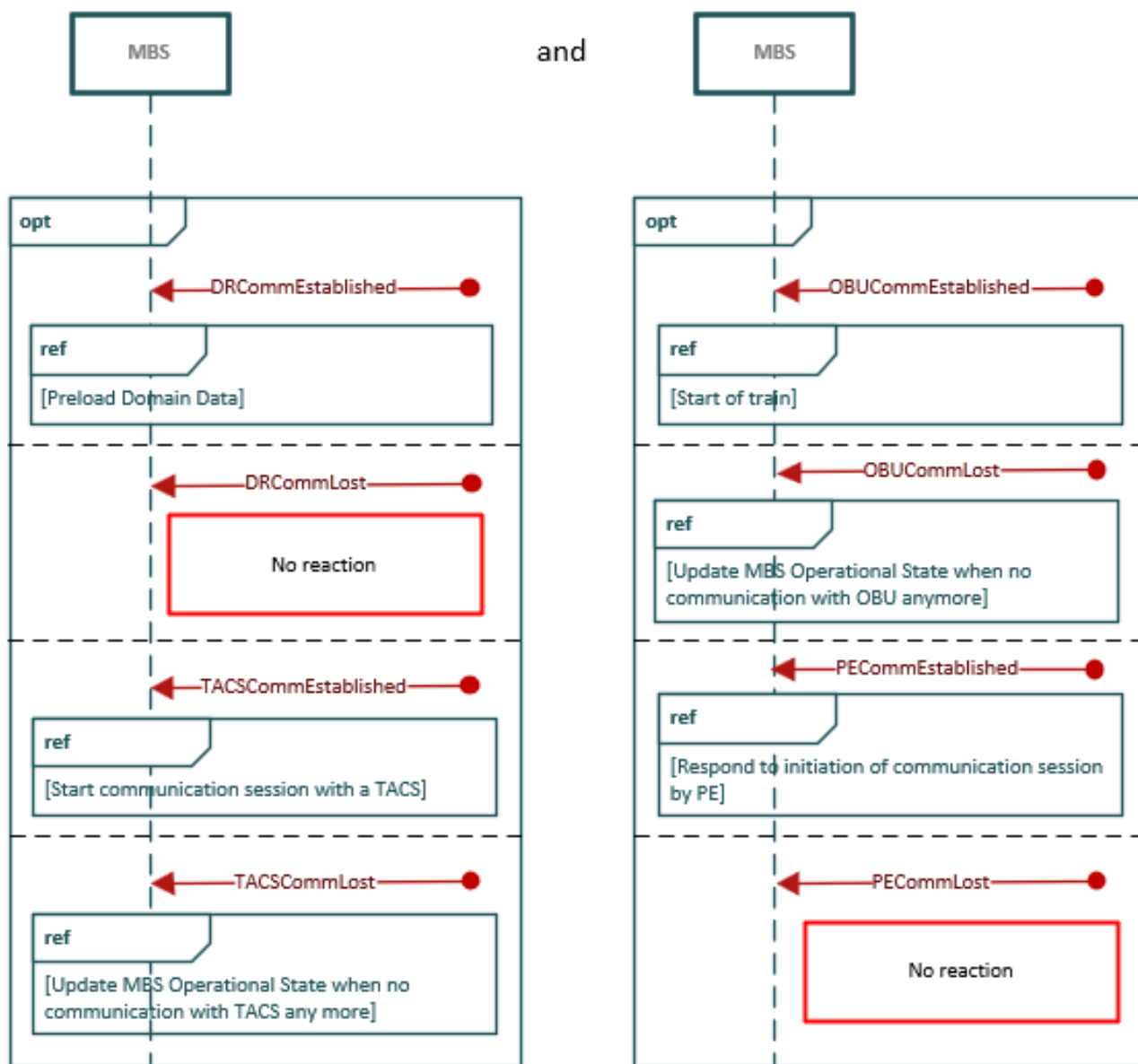
Figure 3 – Scenario pattern: Respond to communication status

<Actor> can be PE, OP, TACS 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 <i>MBS</i> communication to actors.
Goal	<i>MBS is operational</i>
Precondition(s)	None
Postcondition(s) (Success)	The Moving Block System has been started and is operational.
Postcondition(s) (Failure)	
Involved actor(s)	DR, PE, OP, OBU, TACS
Trigger(s)	<i>MBS</i> is started
Main Sequence	<ol style="list-style-type: none"> 1. <i>MBS</i> supervises the communication to actors <p>(This is done in a continuous loop.)</p>
Alternate Sequence	None
Failure Sequence	If loading or checking the <i>Topology Data</i> fails, the start procedure terminates.
Comments	<p>MBS could either be started by an external event or automatically when recovering from a failure for example.</p> <p>The communication patterns raise events <i><actor>CommEstablished</i> and <i><actor>CommLost</i> for every actor <i><actor></i> (UML: <i>lost message</i>). Other capabilities can react (UML: <i>found message</i>) to these events and react accordingly (e.g. initialising a safe state).</p>

5.1.3 Scenario: Start and Maintain MBS

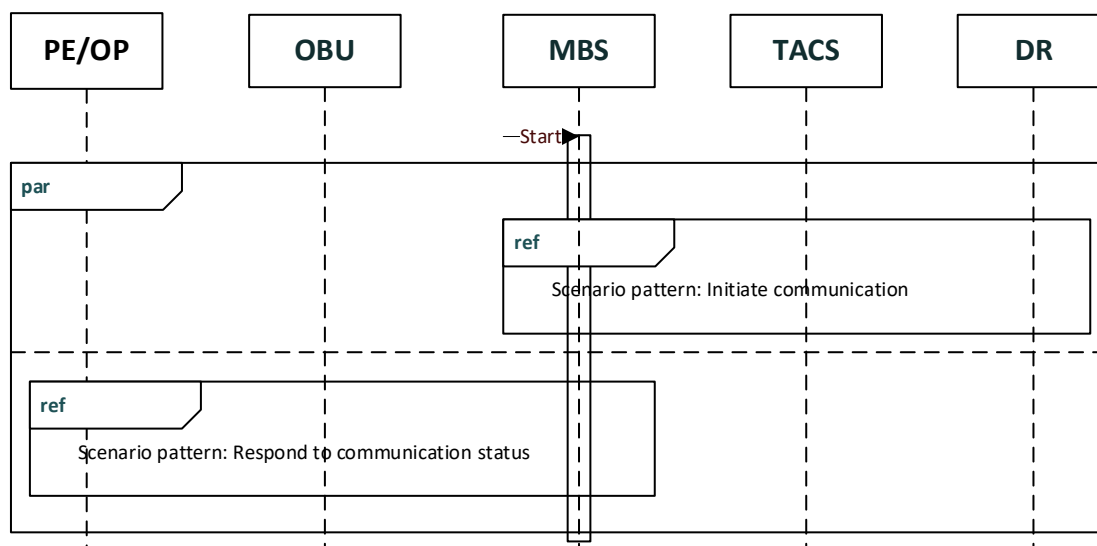


Figure 4 - Scenario: Start and Maintain MBS

5.2 SYSC: PRELOAD TOPOLOGY DATA

Description	This capability allows to provide <i>MBS</i> with <i>Topology Data</i> initially. This finally results into topology-related <i>Domain Objects</i>
Goal	<i>MBS</i> has loaded (initial or new version of) <i>Topology Data</i> and related <i>Domain Objects</i>
Precondition(s)	No <i>Topology Data</i> available (no <i>Topology Data</i> loaded) at startup Communication session with <i>DR</i> established
Postcondition(s) (Success)	<i>MBS</i> has loaded, approved, and activated <i>Topology Data</i> <i>MBS</i> is operational
Postcondition(s) (Failure)	<i>MBS</i> state related to <i>Topology Data</i> has not changed <i>MBS</i> is not operational
Involved actor(s)	<i>DR</i>
Trigger(s)	1. <i>MBS</i> starts up 2. (For further release) <i>MBS</i> receives the <i>Topology Data</i> from <i>DR</i>
Main Sequence	For current release: 1. <i>MBS</i> requests <i>Topology Data</i> from <i>DR</i> 2. <i>MBS</i> receives <i>Topology Data</i> and activates them For a further release: 1. <i>MBS</i> requests <i>Topology Data</i> from <i>DR</i> 2. <i>MBS</i> receives <i>Topology Data</i> and pre-loads them 3. <i>MBS</i> approves the activation of <i>Topology Data</i> 4. <i>MBS</i> activates <i>Topology Data</i>
Alternate Sequence	From release 5 on:

	At any point in time, DR can send <i>Topology Data</i> to MBS (continues then from 3. on)
Failure Sequence	4. MBS rejects the approval when there are e.g. conflicting <i>Movement Permissions</i> (for further release)
Comments	<p>Before release 5, there are the following restrictions</p> <ul style="list-style-type: none"> • The scope of <i>Topology Data</i> is the full <i>Area of Control</i> (so no partial update) • <i>Topology Data</i> 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 <i>Topology Data</i> from there fails (exclusion of unhappy paths) <p>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 <i>Topology Data</i> is already named 'preload' and not only 'load'. The term 'preloaded' can be read as 'loaded'.</p>

5.2.1 Scenario: Preload Topology Data

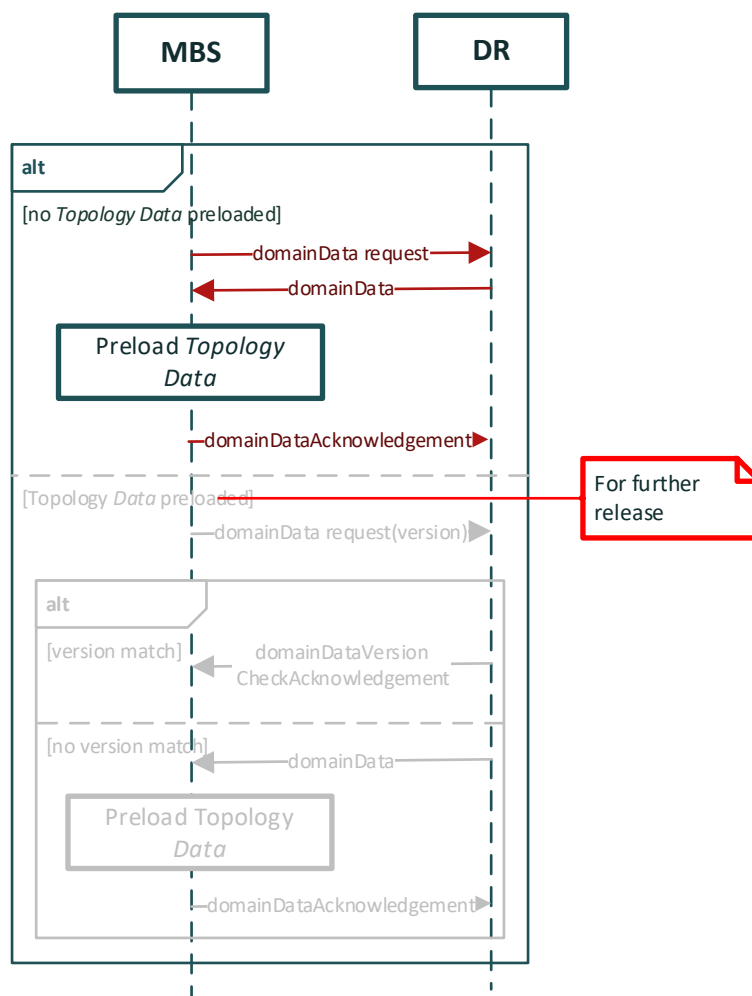


Figure 5: Scenario to pre-load Topology Data

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 Permissions* 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/OP

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

Description	<p>This capability responds to the communication session establishment by <i>PE</i> or <i>OP</i>.</p> <p>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 <i>MBS Operational State</i> (e.g., state of <i>Trackside Assets</i>) to <i>PE</i> and <i>OP</i>.</p>
Goal	<i>MBS</i> has distributed its <i>MBS Operational State</i> to <i>PE/OP</i> .
Precondition(s)	<i>MBS is operational</i>
Postcondition(s) (Success)	The <i>MBS Operational State</i> is synchronised with <i>PE/OP</i>
Postcondition(s) (Failure)	No communication session to <i>PE/OP</i>
Involved actor(s)	<i>PE</i> , <i>OP</i>
Trigger(s)	Event <i>PECommEstablished/OPCommEstablished(OPId)</i>
Main Sequence	1. <i>MBS</i> distributes its <i>MBS Operational State</i> to <i>PE/OP</i> .
Alternate Sequence	None
Failure Sequence	1. <i>MBS</i> cannot distribute the <i>MBS Operational State</i> to <i>PE/OP</i> <i>MBS</i> closes the communication session
Comments	<p>This capability may be triggered after start of <i>MBS</i> or when the communication session to the <i>PE</i> or <i>OP</i> needs to be re-established for any reason.</p> <p>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.</p>

5.5.1 Scenario: Respond to initiation of communication session by PE/OP

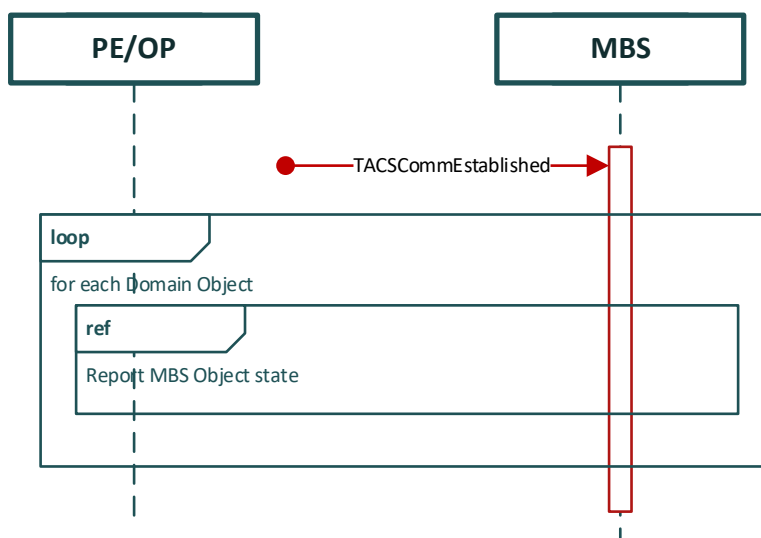


Figure 6 - Scenario: Respond to Initiation of communication session by PE/OP

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	<p>This capability responds to the communication session establishment between the <i>MBS</i> and one <i>TACS</i>; the capability is applied <u>for each TACS</u>.</p> <p><i>MBS</i> performs the synchronisation with <i>TACS</i>, updates the related <i>Domain Objects</i> and distributes their state to <i>PE/OP</i> (by capability 'Report <i>MBS Operational State</i>')</p>
Goal	<i>Domain Objects</i> of <i>MBS</i> are synchronised with <i>TACS</i> and subsequently <i>MBS</i> has distributed the corresponding <i>Domain Object</i> state to <i>PE/OP</i> .
Precondition(s)	<i>MBS is operational</i>
Postcondition(s) (Success)	<i>MBS</i> has distributed the corresponding <i>Domain Object</i> state to <i>PE/OP</i> .
Postcondition(s) (Failure)	No communication session to <i>TACS</i>
Involved actor(s)	PE, OP, TACS
Trigger(s)	Event <i>TACSCommEstablished(TACSId)</i>
Main Sequence	<ol style="list-style-type: none"> 1. <i>MBS</i> synchronises with <i>TACS</i>. 2. <i>MBS</i> updates and distributes the corresponding <i>Domain Objects</i> state to <i>PE</i> and <i>OP</i> (according to the capability 'Update <i>MBS Operational State</i>')
Alternate Sequence	None

Failure Sequence	1. The synchronisation with TACS failed <i>MBS</i> closes the communication session
Comments	This capability may be triggered after start of <i>MBS</i> 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

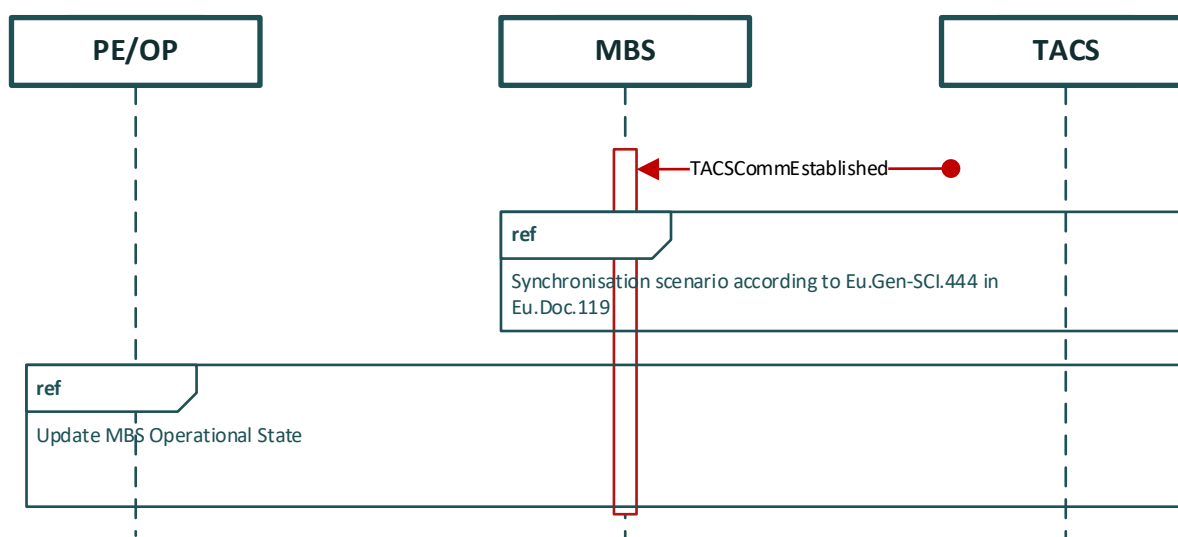


Figure 7 - Scenario: Start communication session with a TACS

This capability 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 <ul style="list-style-type: none"> 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)	<i>MBS is operational</i>

Postcondition(s) (Success)	A communication session with an OBU is established.
Postcondition(s) (Failure)	A communication session with an OBU could <u>not</u> be established.
Involved actor(s)	OBU, PE, OP
Trigger(s)	An OBU requests to set-up a safe radio connection with the MBS.
Main Sequence	<p>1. MBS sets-up a safe radio connection and communication session according to /ETCS/ considering using System Version 2.1.</p> <p>MBS creates a <i>Train Object</i> for this OBU and subsequently informs PE/OP about this through the capability 'Update <i>MBS Operational State</i>'.</p>
Alternate Sequence	None.
Failure Sequence	<p>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.</p>
Comments	<p>The failure sequence may be triggered e.g. in the following case:</p> <ul style="list-style-type: none"> • There is no key (KMAC) available within MBS for this OBU.

5.7.1 Scenario: Respond to initiation of communication session by OBU

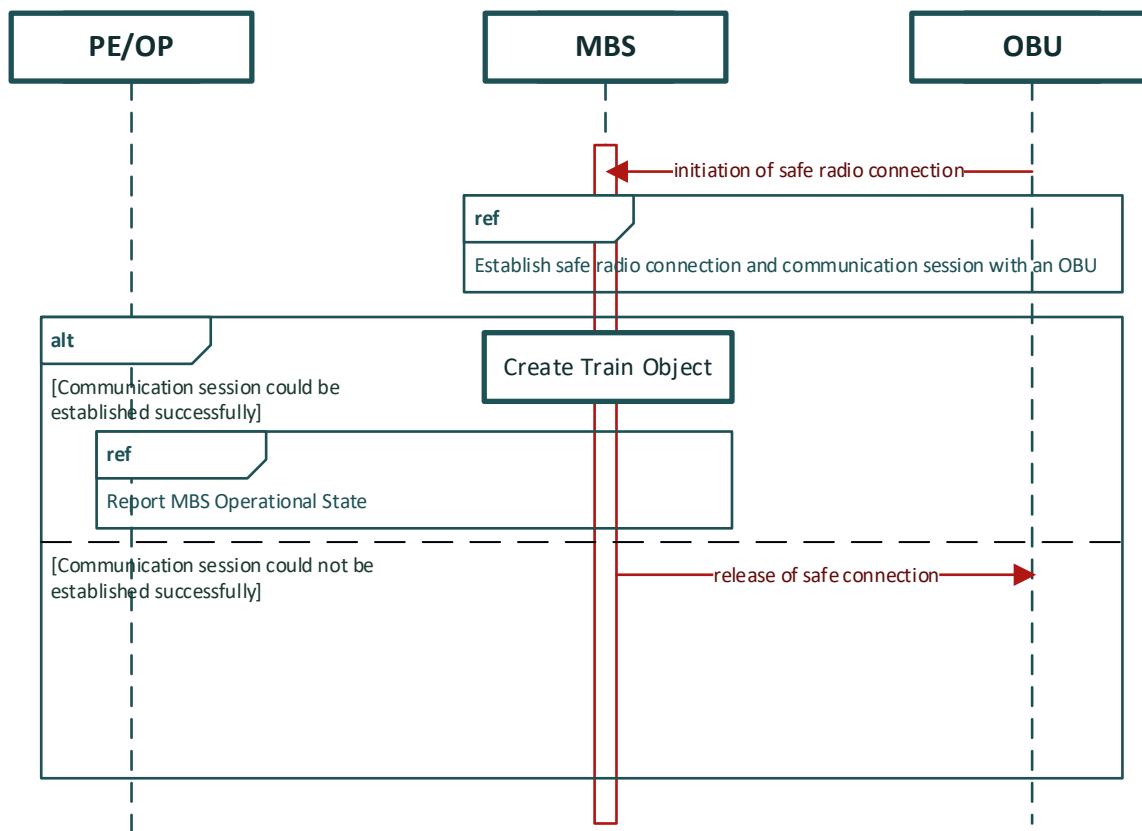


Figure 8 - Scenario: Respond to initiation of communication session by OBU

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:

Description	This capability allows <i>PE</i> and <i>OP</i> to change the state of a <i>Switchable Trackside Asset</i> by sending a corresponding TA State Request to <i>MBS</i> . <i>MBS</i> has to verify if the request is valid. If it is valid, <i>MBS</i> carries it out by sending the corresponding command to the <i>TACS</i> related to the <i>Switchable Trackside Asset</i> .
Goal	Due to a request from <i>PE</i> or <i>OP</i> , a <i>Switchable Trackside Asset</i> is commanded to change its state by sending a command to its <i>TACS</i> .
Preconditions	<i>MBS</i> is operational
Postcondition (Success)	Granting of request is indicated to <i>PE</i> or <i>OP</i> . Command for changing its state is sent to <i>TACS</i> .
Postcondition (Failure)	Rejecting of a valid request from <i>PE</i> or <i>OP</i> . Command for changing its state is not sent to <i>TACS</i> .
Involved Actors	<i>PE</i> , <i>OP</i> , <i>TACS</i>
Trigger	Request from <i>PE</i> or <i>OP</i> to change the position of a <i>Switchable Trackside Asset</i> via its <i>TACS</i> .
Main Sequence	A valid request is granted and carried out by <i>MBS</i> (see: Scenario: Control <i>Switchable Trackside Assets</i>) and <i>MBS</i> informs <i>PE</i> or <i>OP</i> about granting this request
Alternate Sequence	
Failure Sequence	An invalid request is rejected by <i>MBS</i> (see: Scenario: Control <i>Switchable Trackside Assets</i>) and <i>MBS</i> informs <i>PE</i> or <i>OP</i> 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* or *OP* 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* or *OP* system the rejecting of the request and performs no further actions for the request.

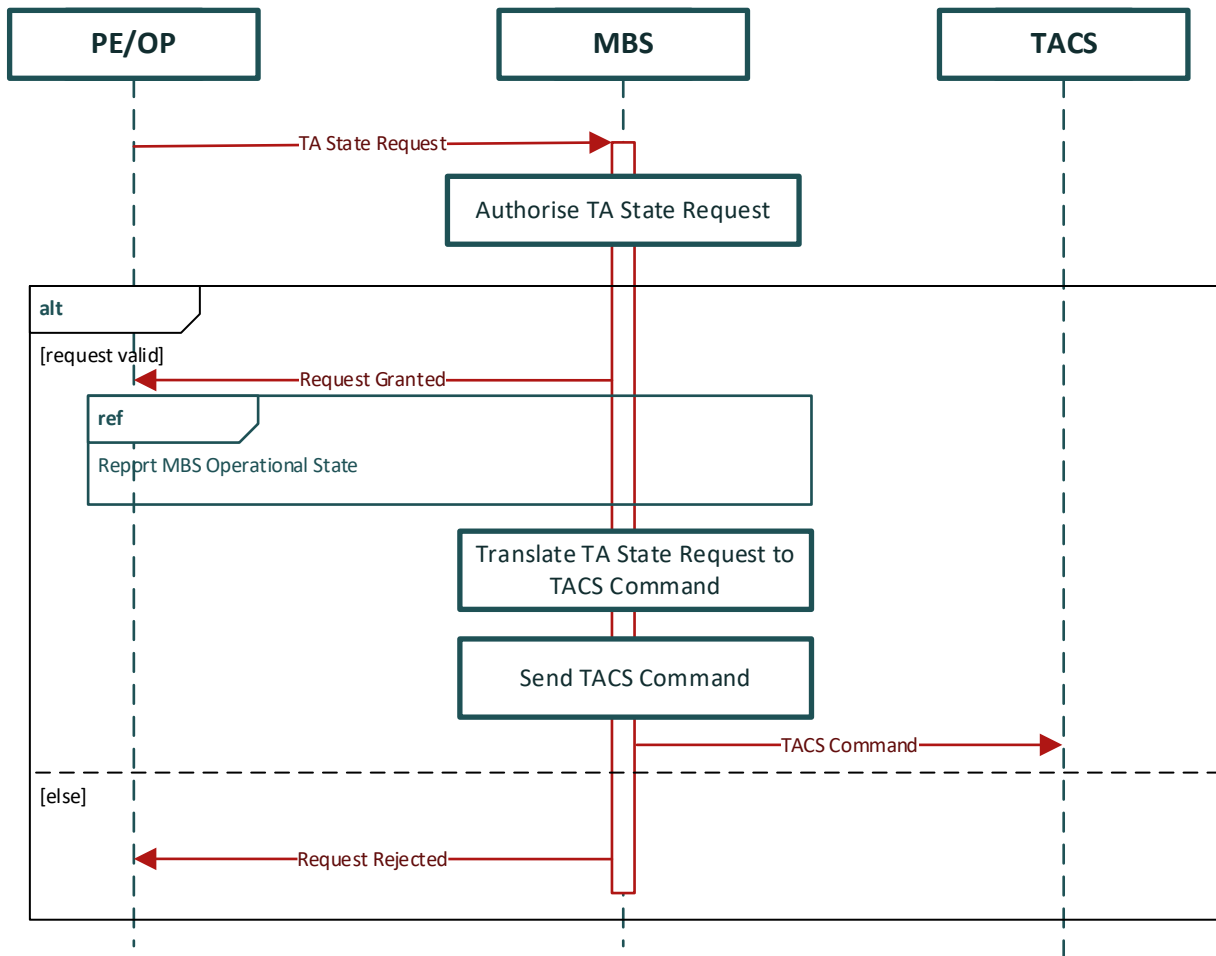


Figure 9 - Scenario: Control *Switchable Trackside Assets*

Note that the response from the *Switchable Trackside Asset* is not shown here, it is asynchronously sent (refer to section 5.12.1).

5.9 SysC: OVERWRITE DPS STATE

Table 5 – Description of SysC: Overwrite DPS State

Description	This capability allows the operator to force a DPS to be considered as drivable although the state reported from the Switchable Trackside Asset is different.
Goal	<p>MBS assumes a DPS as drivable irrespective of the state reported by TACS.</p> <p>Note: As the DPS is set as drivable, Movement Permission in FS can be set over the DPS. This of course implies that the drivability is guaranteed by other means and a physical lock shall be installed prior this procedure.</p> <p>If other restrictions are operationally needed (e.g. reduced speed), a URA shall be created by the Operator to reflect this.</p>

Preconditions	<i>MBS is operational</i> A URA with the restriction property nonSwitchable has been set over all DPS of this DPS Group
Postcondition (Success)	Granting of a demand is indicated to <i>OP</i> . The DPS(s) of a DPS Group which should be drivable are considered drivable irrespective of the currently reported <i>Trackside Asset</i> state.
Postcondition (Failure)	Rejecting of a demand is indicated to <i>OP</i> .
Involved Actors	OP
Trigger	DPS Overwrite Demand sent to MBS from OP.
Main Sequence	A valid demand is granted and carried out by <i>MBS</i> (see Scenario: Overwrite DPS State) and MBS informs OP about granting this request
Alternate Sequence	None
Failure Sequence	An invalid request is rejected by <i>MBS</i> and <i>MBS</i> informs OP about rejecting this request.
Comments	None

5.9.1 Scenario: Overwrite DPS State

The figure below contains the sequence and the failure sequence of one scenario of the SysC Overwrite DPS Group State.

When the *MBS* receives a DPS Overwrite Demand, it performs the safety checks (Function: Authorise DPS Overwrite Demand) for the demand.

If the safety checks are successful, *MBS* responds to *OP* the granting of the demand and reports the target state of the DPS Group as the current state (Function Execute DPS Overwrite Demand)

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

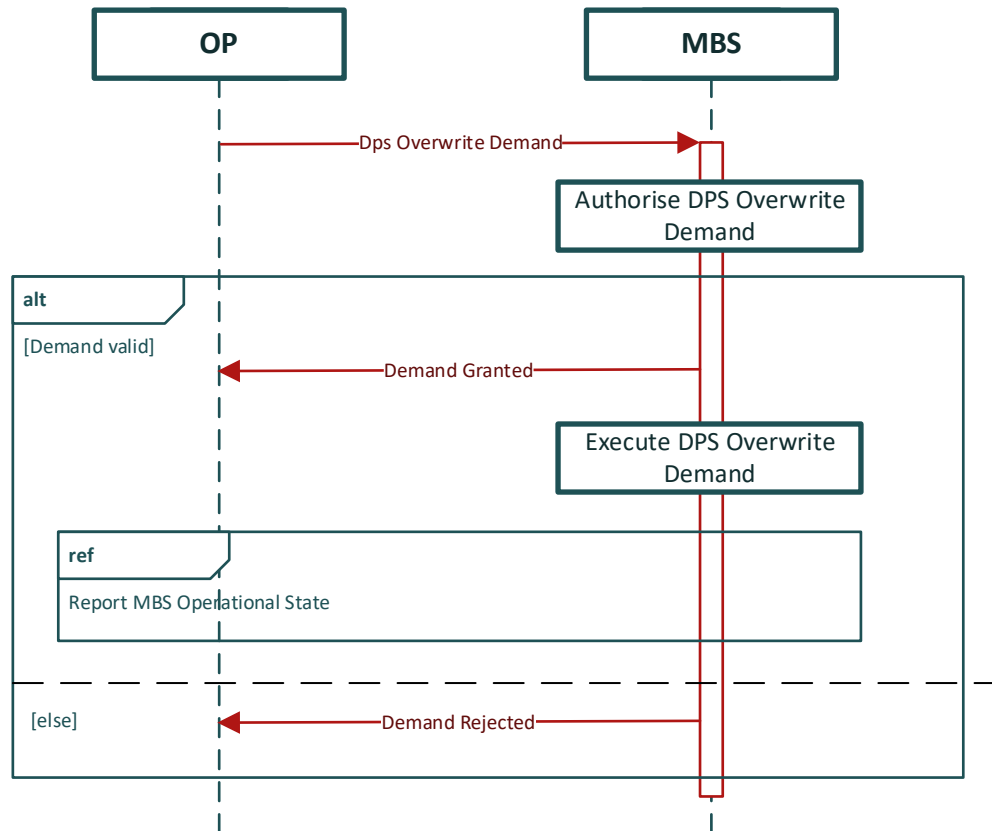


Figure 10 - Scenario: Overwrite Switchable Trackside Asset State

5.10 SysC: REVOKE OVERWRITE DPS STATE

Table 6 – Description of SysC: Revoke Overwrite DPS State

Description	This capability allows the operator to revoke the overwriting of a DPS state returning to the currently known state reported by the Trackside Asset.
Goal	MBS assumes a DPS again as reported by the Trackside Asset.
Preconditions	<i>MBS is operational 5.1.2</i>
Postcondition (Success)	MBS assumes a DPS again as reported by the Trackside Asset.
Postcondition (Failure)	Rejecting of a demand from <i>OP</i> .
Involved Actors	OP
Trigger	Demand from <i>OP</i> to revoke the overwrite of the DPS in a DPS Group.
Main Sequence	A valid request is granted and carried out by <i>MBS</i> (see: Scenario: Revoke Overwrite DPS State) and MBS informs OP about granting this demand
Alternate Sequence	None
Failure Sequence	An invalid demand is rejected by <i>MBS</i> (see: Scenario: Control <i>Switchable Trackside Assets</i>) and MBS informs OP about rejecting this demand.
Comments	None

5.10.1 Scenario: Revoke Overwrite DPS State

The figure below contains the sequence and the failure sequence of the SysC Revoke Overwrite DPS state.

When the *MBS* receives a Revoke DPS Overwrite Demand it performs the safety checks (Function: Authorise Revoke DPS Overwrite Demand) for the demand.

If the safety checks are successful, *MBS* responds to *OP* the granting of the demand and assumes again the state reported by the Trackside Asset for the DPS and DPS Group states.

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

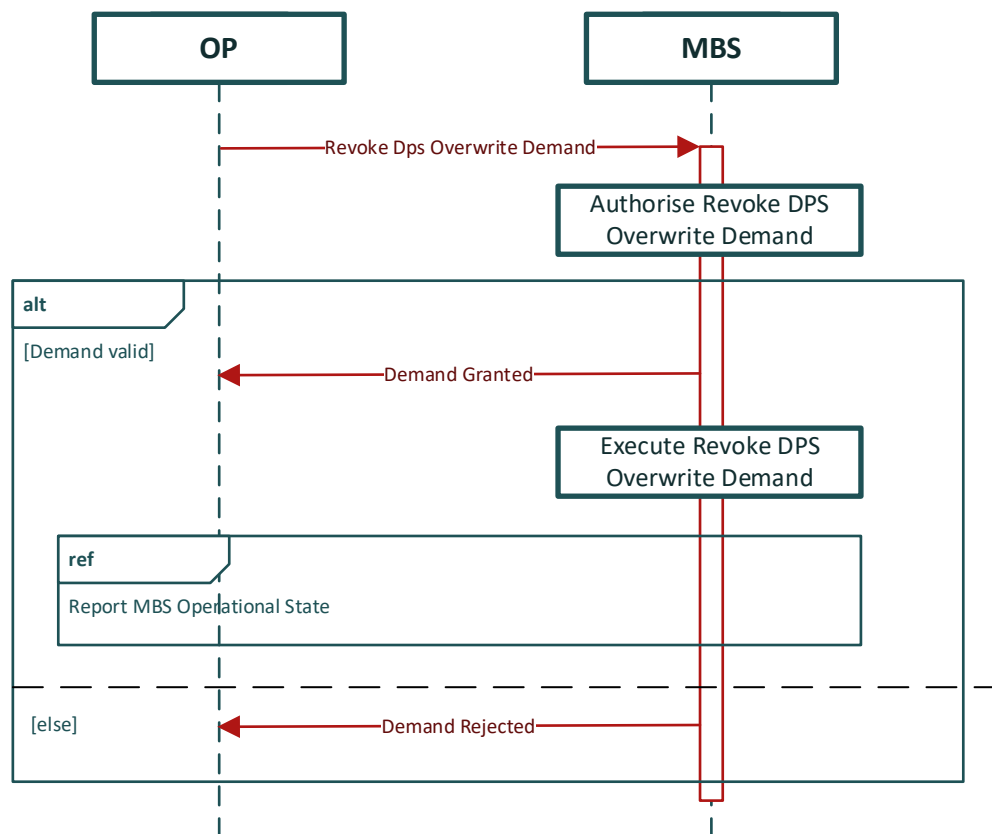


Figure 11 - Scenario: Revoke Overwrite DPS State

5.11 SysC: SHUTDOWN MBS

Out of scope for this release

5.12 SysC: UPDATE *MBS OPERATIONAL STATE*

Table 7 – Description of SysC: Update *MBS Operational State*

Description	This capability updates the <i>MBS Operational State</i> .
Goal	Update the state of <i>MBS Operational State</i>
Precondition	<i>MBS is operational</i>
Postcondition (Success)	MBS has updated its <i>MBS Operational State</i>
Postcondition (Failure)	None (no failure)
Involved Actors	OBU, PE, OP
Trigger	<ul style="list-style-type: none"> Any change of <i>MBS Operational State</i> is detected (inexhaustive list): <ul style="list-style-type: none"> 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 <i>MBS Operational State</i> when TA state report is received Scenario 2: Update <i>MBS Operational State</i> when a Position Report or validated train data are received
Alternate Sequence	Scenario 3: Update <i>MBS Operational State</i> when no communication with TACS anymore Scenario 4: Update <i>MBS Operational State</i> when no communication with OBU anymore
Failure Sequence	None
Comments	None

5.12.1 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.

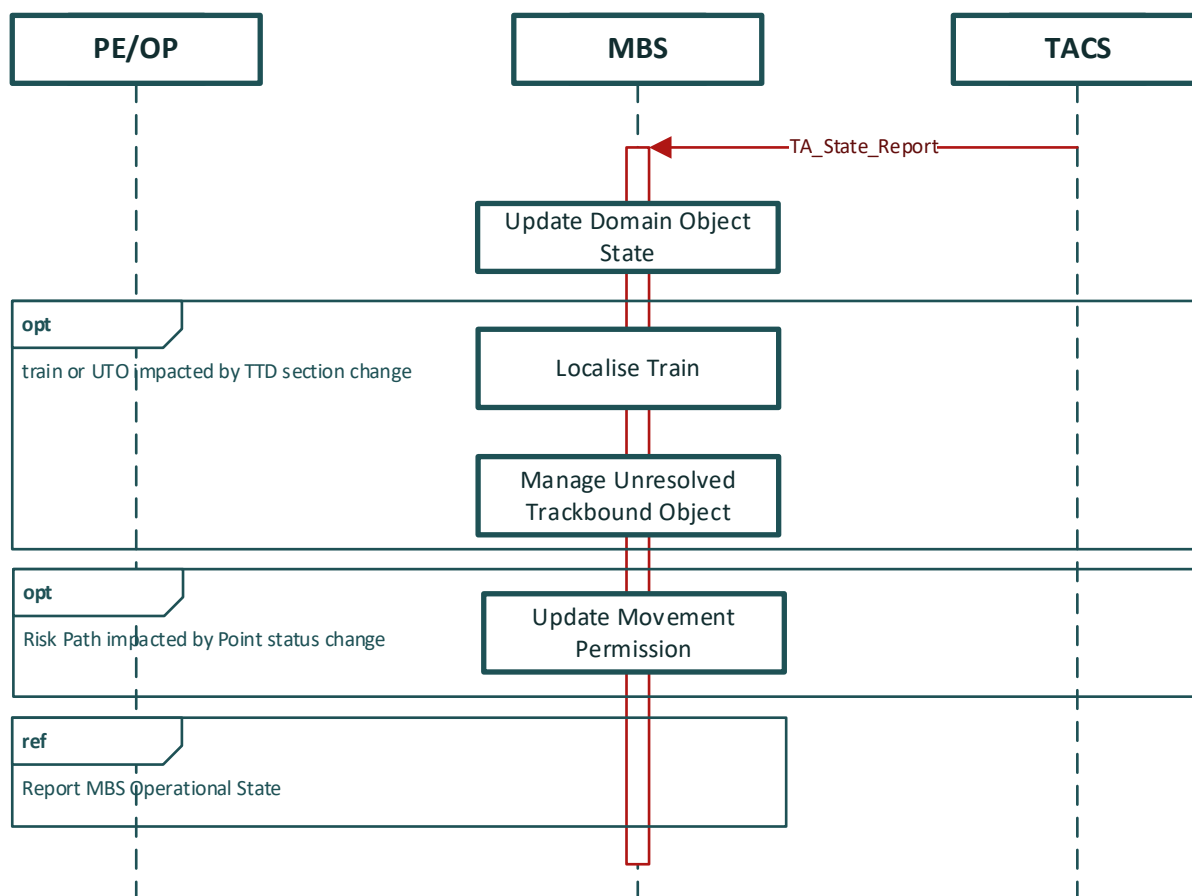


Figure 12 - Scenario 1: Update *MBS Operational State* when TA state report is received

Note: A TA_State_Report may also be sent to MBS e.g. in case of an unexpected TTD occupation or a point status change which may have impact to already issued authorisations. Those cases are detailed in the capabilities ‘Supervise trains and trackside assets’ and ‘Revoke or restrict authorisation’.

5.12.2 Scenario 2: Update *MBS Operational State* when a 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.

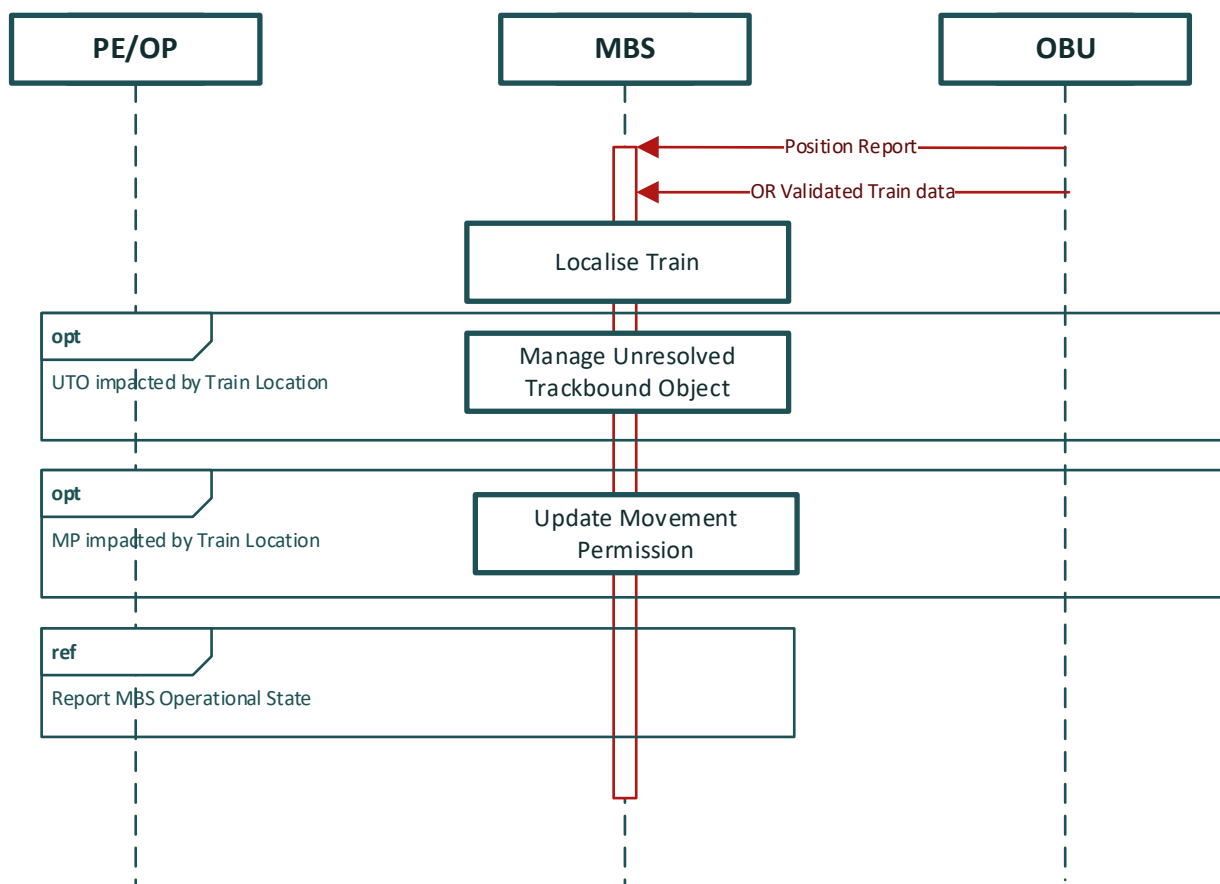


Figure 13 - Scenario 2: Update *MBS Operational State* when Position Report or validated train data are received

5.12.3 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.

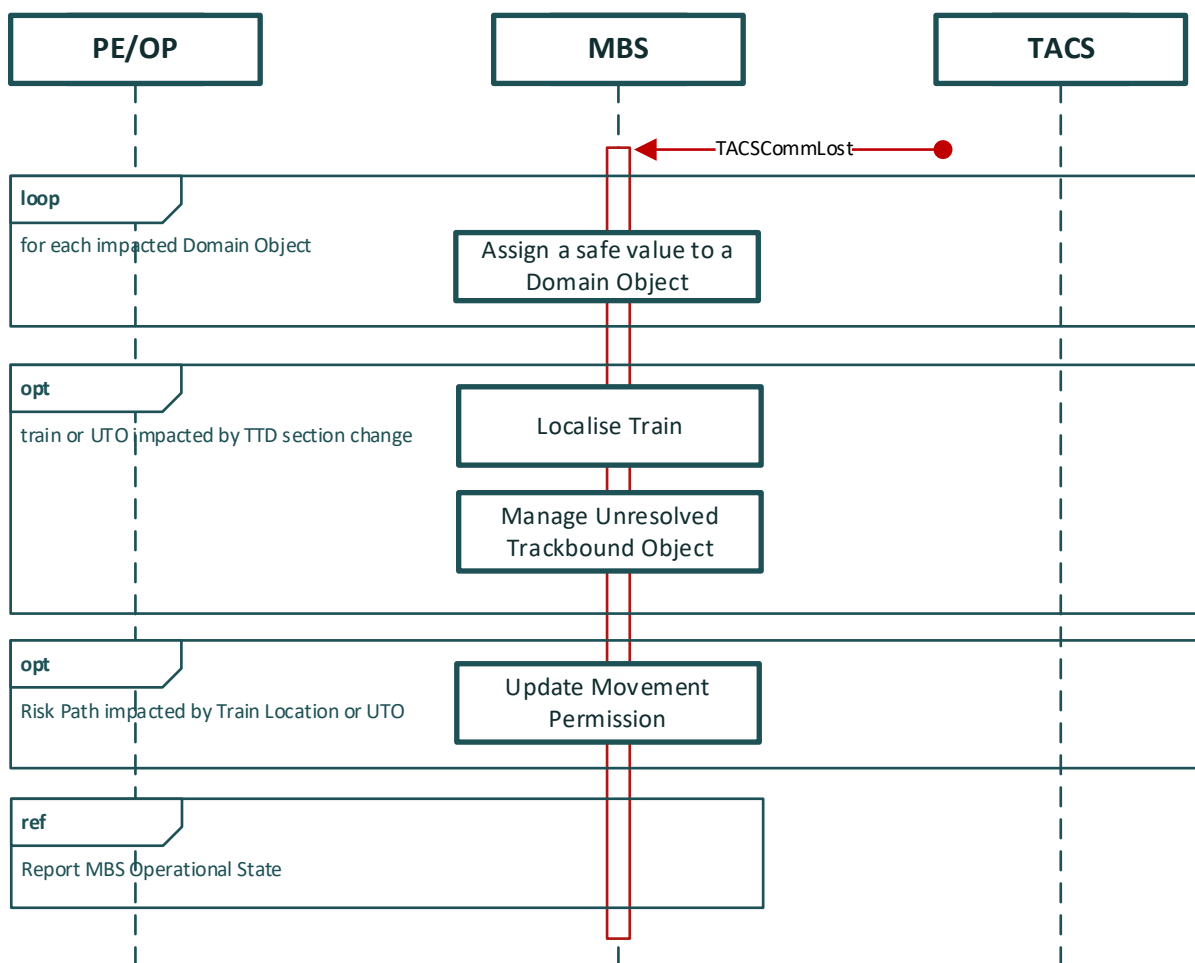


Figure 14 - Scenario 3: Update of status when no communication with TACS anymore

5.12.4 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 PE/OP in the Train Object.

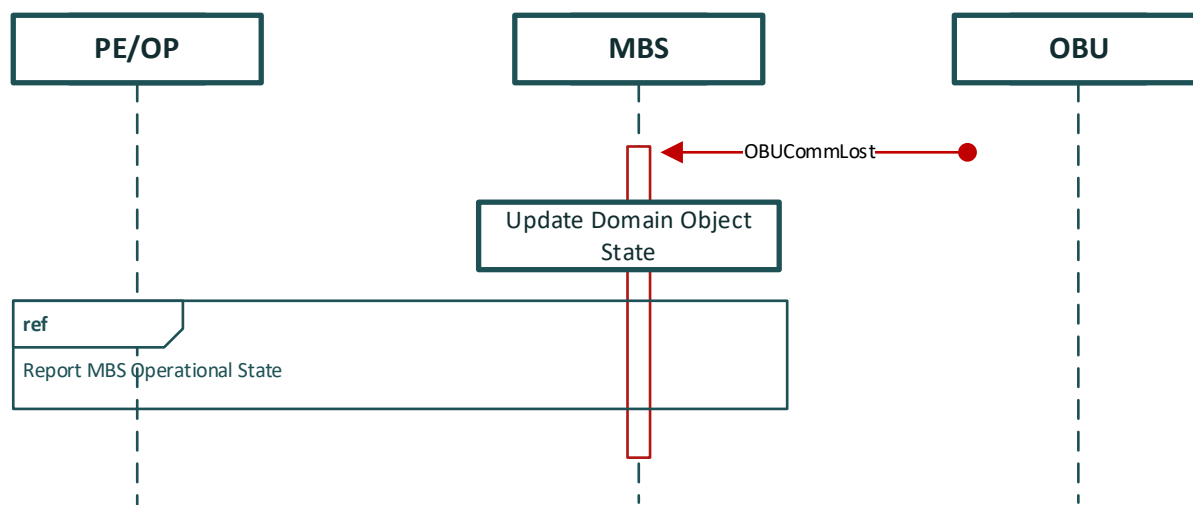


Figure 15 - Scenario 4: Update of *MBS Operational State* when no communication with OBU anymore

5.12.5 Scenario 5: Update *MBS Operational State* when a request for an assumed train position is received

This scenario covers the creation of an *Assumed Train Location* based on a request from OP for a train having reported a position unknown or ambiguous position to the MBS, e.g. at Start of Mission. The *Assumed Train Location* is created from the assumed position provided from OP and the length the associated train has reported in its validated Train Data. The assumed position is reported as a reference position with a direction, an (optional) offset from this position and whether the train front is in the same or the reverse direction.

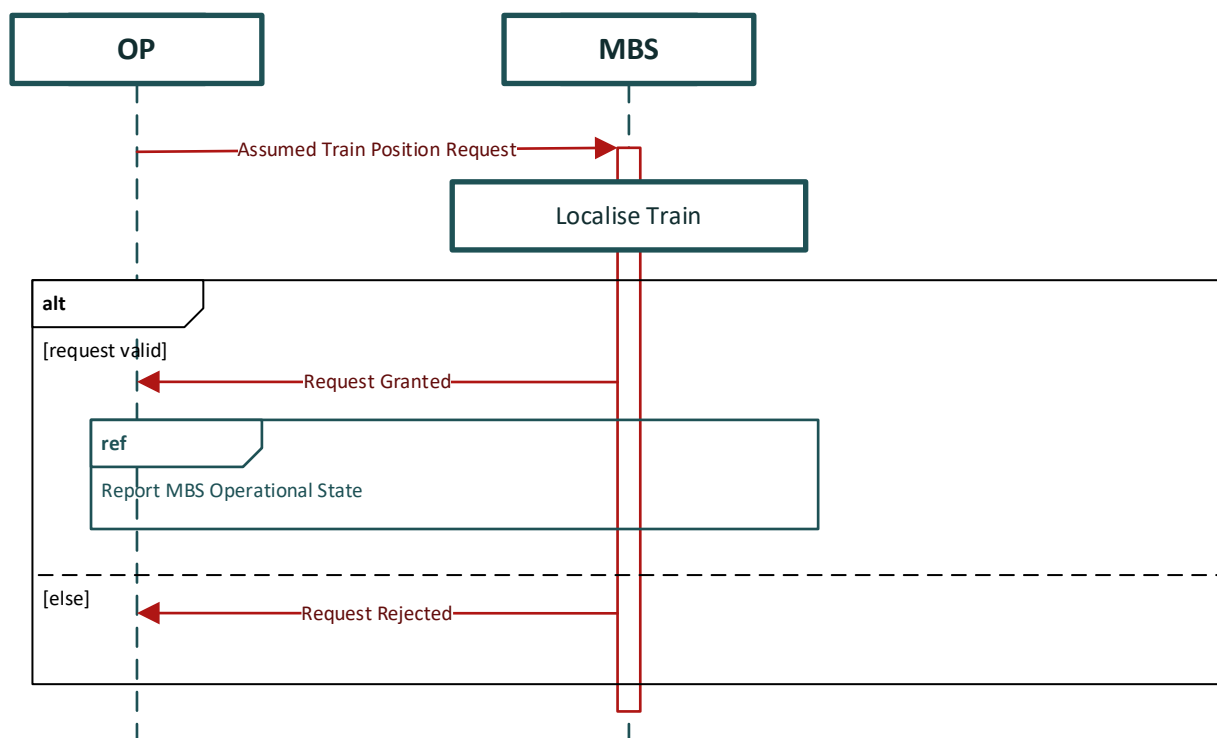


Figure 16 - Scenario 5: Update *MBS Operational State* when a request for an assumed train position is received

5.13 SysC: REPORT *MBS OPERATIONAL STATE*

Table 8 – Description of SysC: Report *MBS Operational State*

Description	When triggered, this capability reports the <i>MBS Operational State</i> .
Goal	Report the state of <i>MBS Operational State</i>
Precondition	<i>MBS is operational</i>
Postcondition (Success)	PE and OP has received the <i>MBS Operational State</i> for the given <i>Domain Object Instance</i>
Postcondition (Failure)	None (no failure)
Involved Actors	PE, OP
Trigger	A change of an <i>MBS Domain Object Instance</i> is detected
Main Sequence	Scenario: Report of <i>MBS Operational State</i>
Alternate Sequence	
Failure Sequence	None
Comments	None

5.13.1 Scenario: Report of *MBS Operational State* when triggered

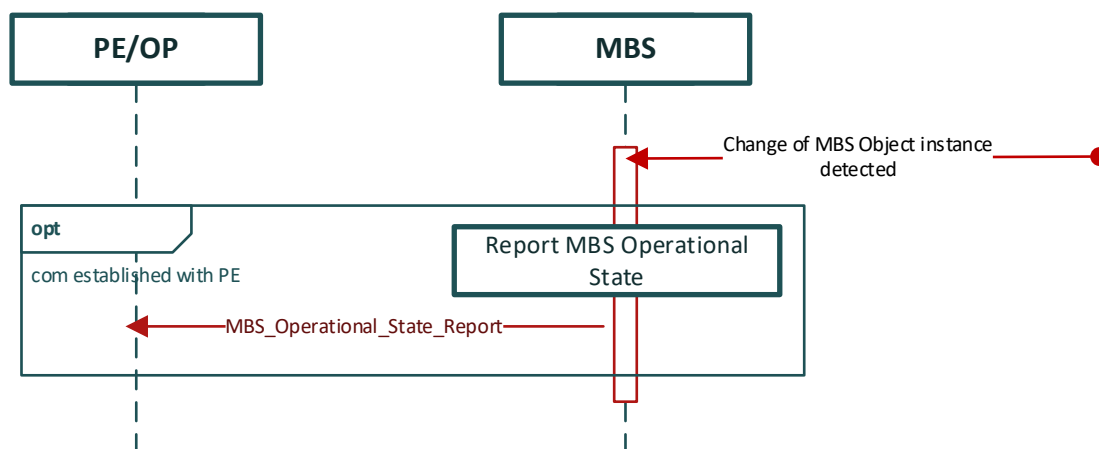


Figure 17 - Scenario: Report of *MBS Operational State* when triggered

5.14 SysC: START OF TRAIN

Description	Start of Train
Goal	A train successfully has started up according to /ETCS/ and MBS has subsequently updated the MBS Operational State.
Precondition(s)	<i>MBS is operational 5.1.2</i>
Postcondition(s) (Success)	MBS has updated the MBS Operational State after receiving a first MA request during the Start of Mission procedure.
Postcondition(s) (Failure)	None
Involved actor(s)	OBU, PE, OP
Trigger(s)	MBS receives a SoM Position Report message from an OBU.
Main Sequence	<ol style="list-style-type: none"> MBS determines that the position is valid and unambiguous. MBS updates the <i>Train Object</i> and the <i>MBS Operational State</i>. MBS receives Validated Train Data, Train Running Number from OBU and subsequently acknowledges the train data to the OBU. MBS updates the <i>Train Object</i> and the <i>MBS Operational State</i>. MBS receives an MA Request from OBU. MBS updates the <i>Train Object</i> and the <i>MBS Operational State</i>.
Alternate Sequence	<ol style="list-style-type: none"> a) MBS receives a SoM Position Report with invalid / unknown position. MBS updates the <i>Train Object</i> and the <i>MBS Operational State</i>, indicating that the position is invalid / unknown and sends Train

	Accepted to the OBU. Afterwards the flow continues with step 2 of the main sequence.
	<p>1.b) MBS receives a SoM Position Report with a valid position, but the <i>position is ambiguous</i> for the MBS.</p> <p>MBS updates the <i>Train Object</i> and the <i>MBS Operational State</i>, indicating that the <i>position is ambiguous</i>. Afterwards the flow continues with step 2 of the main sequence.</p>
	<p>1.c) MBS receives a SoM Position Report with a valid position, but the LRBG is unknown to the MBS.</p> <p>MBS updates the <i>Train Object</i> and the <i>MBS Operational State</i>, indicating that the position is unknown. Afterwards the flow continues with step 2 of the main sequence.</p>
Failure Sequence	None
Comments	<p>Please consider that mode change to SH is currently excluded from the scope of the document and thus there is no failure sequence aborting this capability in case step 3 does not occur. The same also applies for using the 'Override' function.</p> <p>Additionally, it is also not foreseen yet to revalidate the train position (using the SoM Position Report Confirmed message) since this may depend on operational procedures which are not available yet.</p>

5.14.1 Scenario: Start of Train

Please consider that during this scenario after each 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 PE and OP. This handling of Position Reports is not explicitly illustrated in the figure to limit the sequence diagram to the Start of Train capability.

The system function Localise Train also deals with trains which the MBS cannot locate from the SoM Position Report, i.e. trains reporting that the status of their position is invalid or unknown, or a position which is ambiguous to the MBS. A train with an unknown or ambiguous position in the Operational State will trigger the OP to request a Signaller to provide an assumed position for this train.

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

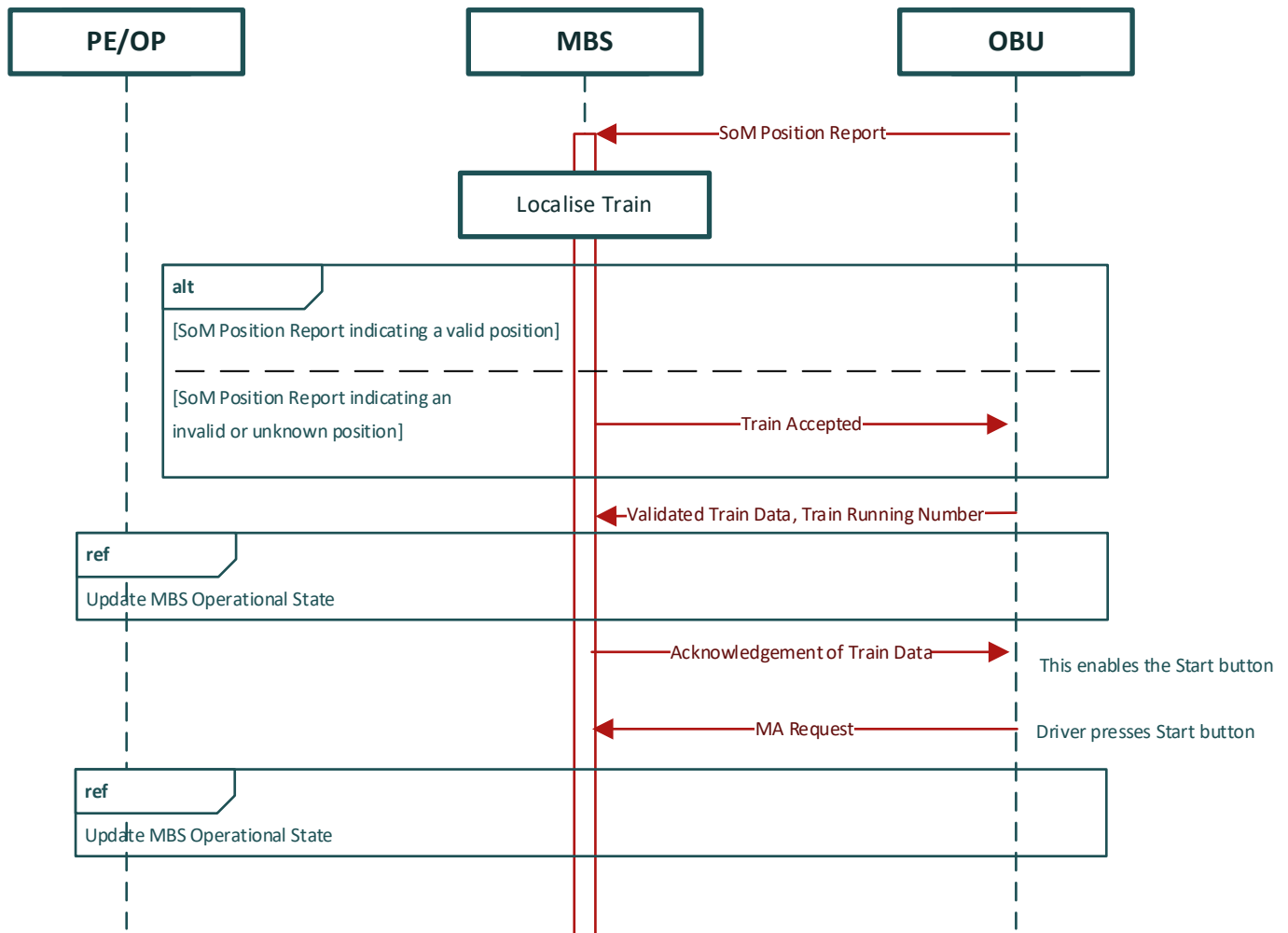


Figure 18 - Scenario 1: Start of Train

5.15 SysC: PROVIDE AUTHORISATION TO TRAIN

Table 9 – Description of SysC: Provide Authorisation 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 or OP, 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	<i>MBS is operational</i> Communication between the requesting entity, PE or OP, and the MBS is established
Postcondition (Success)	Authorisation issued by MBS to the OBU corresponding to the <i>Train Object</i> ; Movement Permission reported to PE and OP via the <i>MBS Operational State</i> .
Postcondition (Failure)	None

Involved Actors	OBU, PE, OP
Trigger	<ul style="list-style-type: none"> MBS receives an MP Request
Main Sequence	<p>When all checks are successful, MBS indicates this to PE or OP respectively, updates the <i>Train Object</i> with the Movement Permission and issues a Movement Authority or an SR Authorisation to the OBU based on the MP Request received from PE or OP, respectively.</p> <p>MP Request for SR Authorisation can only be given by OP.</p>
Alternate Sequence	None
Failure Sequence	<p>When at least one check fails, MBS reports a Request Rejected to the requesting entity, PE or OP, indicating the reason why the MP Request could not be granted.</p>
Comments	<p>SR Authorisation is given to a train when an MA is not possible, but as soon as it is possible to give an MA, PE will send an MP Request for this.</p>

5.15.1 Scenario: Provide MA to Train

This scenario shows the creation of a Movement Permission and sending of MA to a train, based on an MP Request from PE for this train.

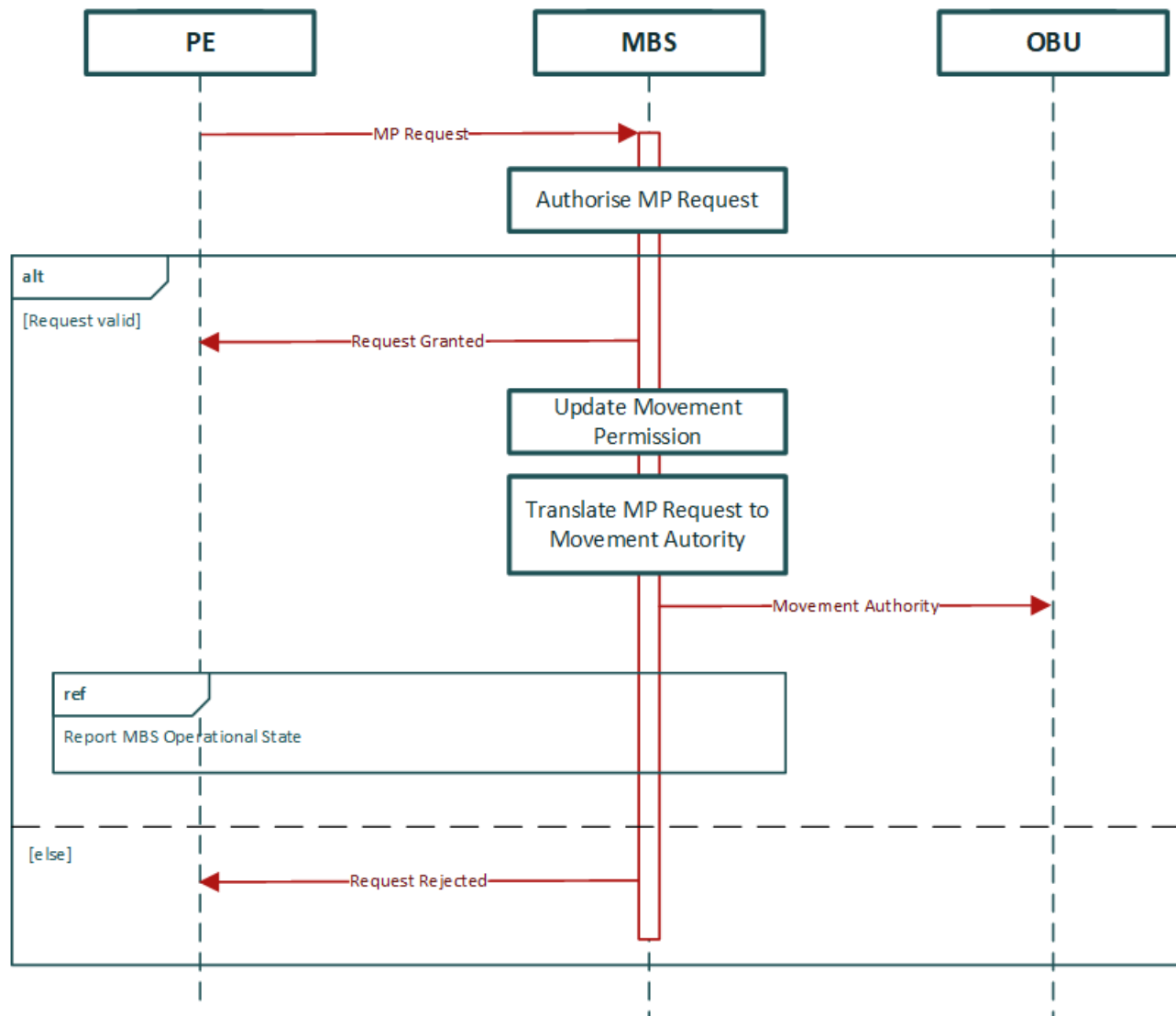


Figure 19 - Scenario : Provide MA to Train

5.15.2 Scenario: Provide SR Authorisation to Train

This scenario shows the creation of a Movement Permission and sending of an SR Authorisation to a train, based on an MP Request from OP for this train. The train must have a known or assumed position to be authorised.

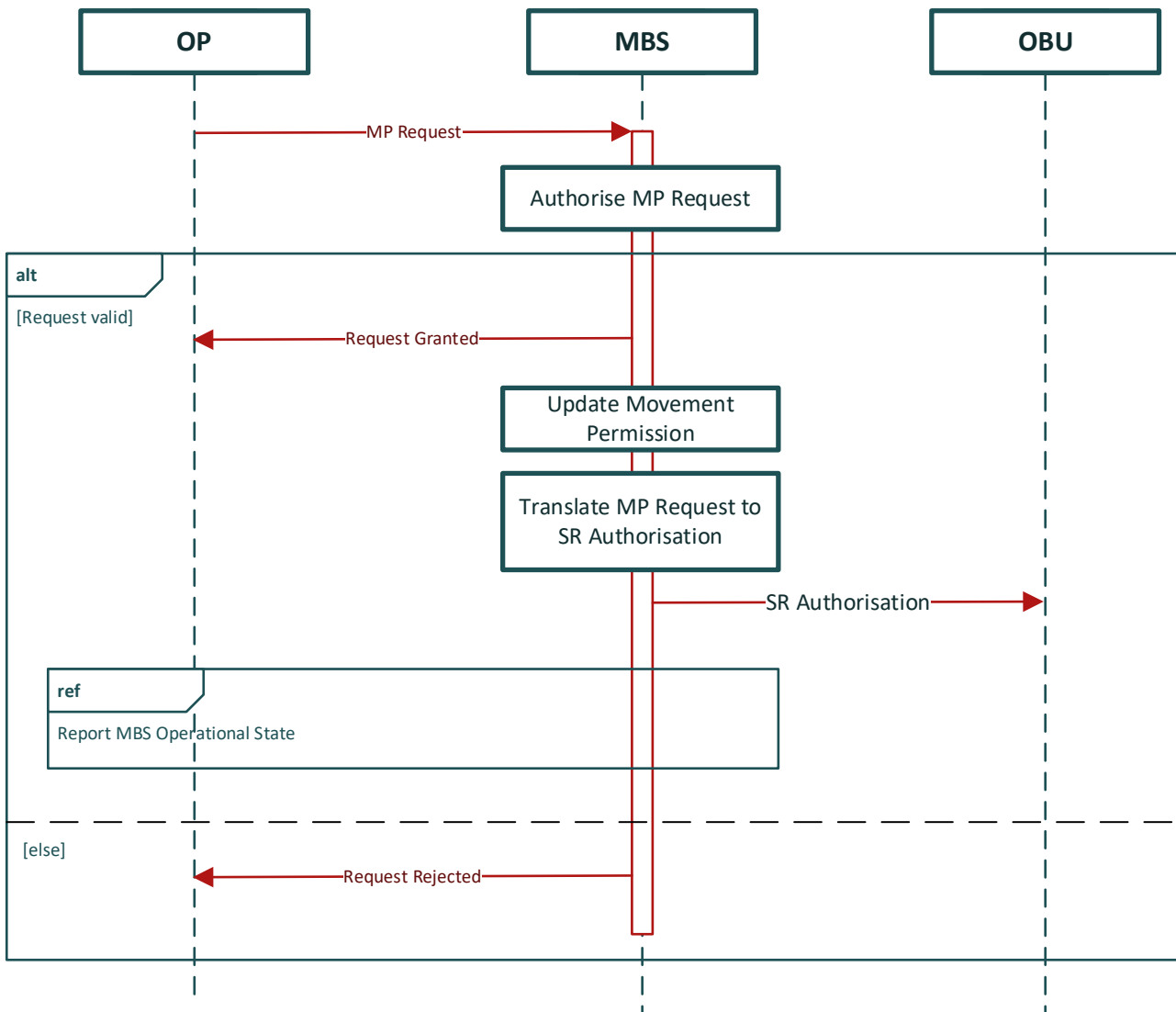


Figure 20 - Scenario : Provide SR Authorisation to Train

5.16 SysC: TERMINATE TRAIN MISSION

Table 10 – Description of SysC: Terminate Train Mission

Description	<p>This capability manages the termination of the mission of a train. It manages:</p> <ul style="list-style-type: none"> • 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 <i>Train Object</i> into an <i>Unresolved Trackbound Object</i> (needed by the MBS to manage the occupied area and a further start of mission for this train). It reports the information to PE/OP
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. <i>Train Object</i> is converted into <i>Unresolved Trackbound Object</i>
Postcondition (Failure)	none
Involved Actors	OBU, PE, OP
Trigger	<ul style="list-style-type: none"> • 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	

5.16.1 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).
- a Position Report indicating a change of mode to SB

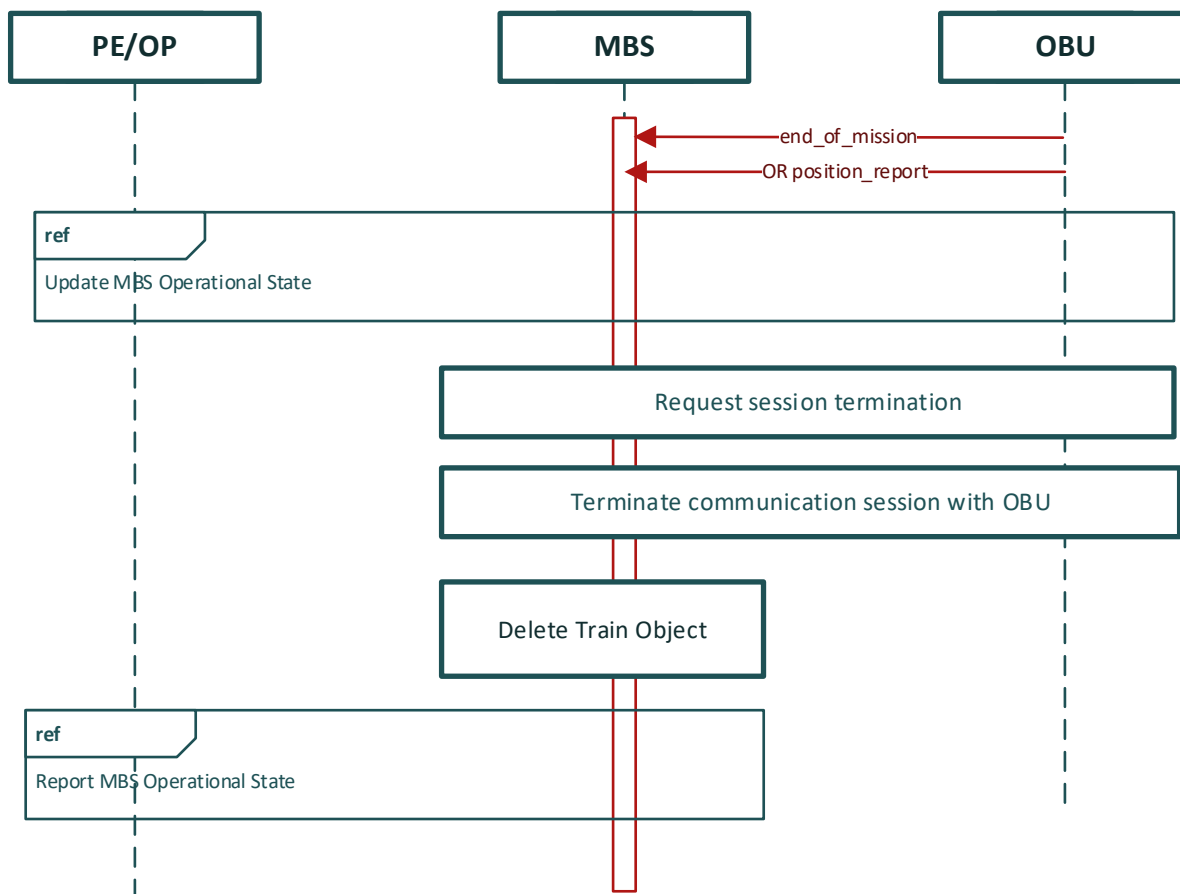


Figure 21 - Scenario 1: Train End of Mission

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.

5.16.2 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.

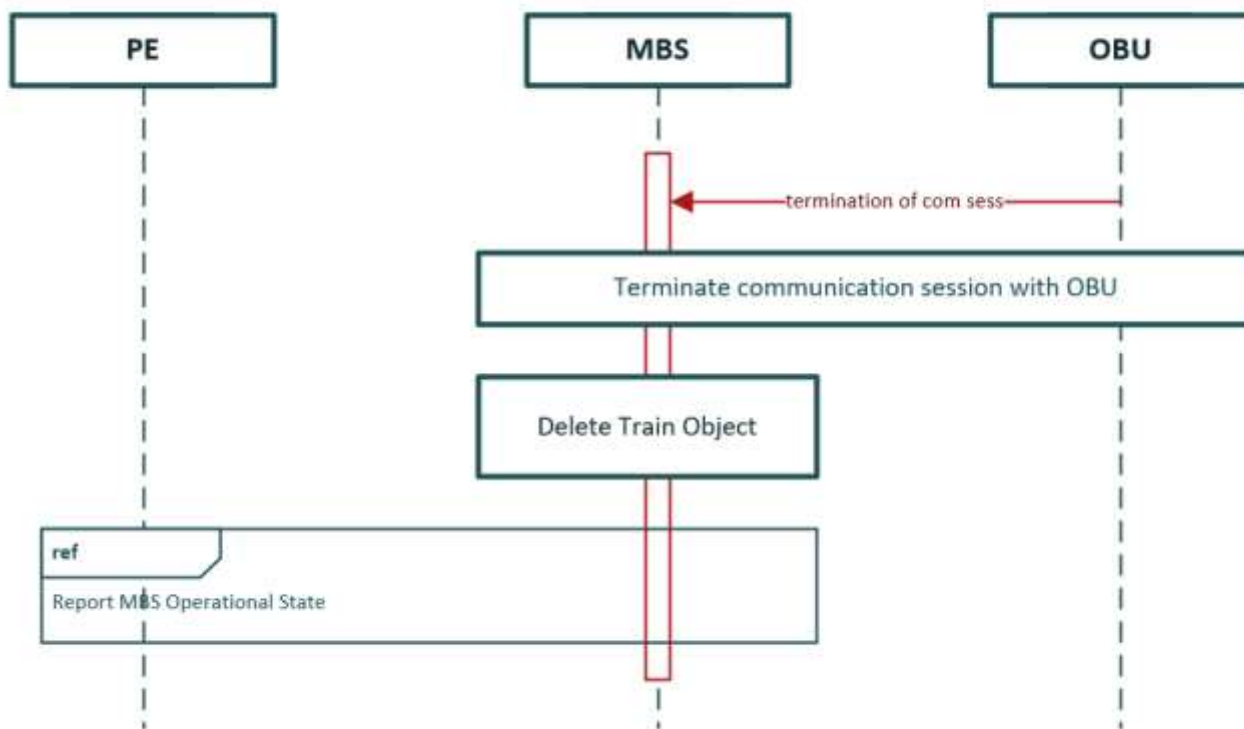


Figure 22 - Scenario 2: Termination of communication session by OBU

5.16.3 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.

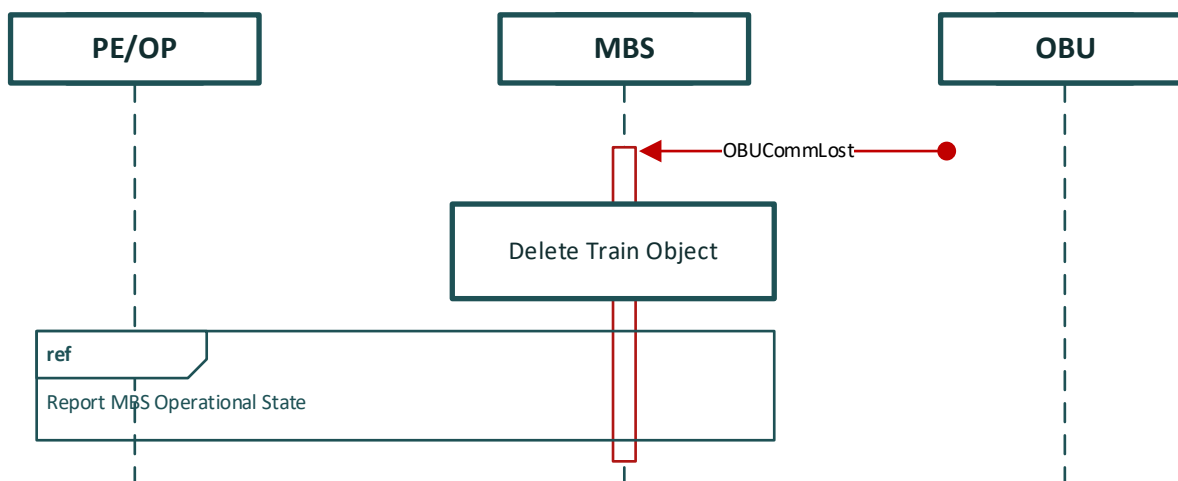


Figure 23 - Scenario 3: end mission when no communication anymore with an OBU

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/

5.17 SysC: SHORTEN MA COOPERATIVELY

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 or OP, MBS checks all safety constraints and subsequently performs the cooperative shortening of MA with the OBU.
Precondition	<i>MBS is operational</i>
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 or OP about the success of the cooperative shortening of MA procedure.
Postcondition (Failure)	<p>Failure 1: After the OBU has rejected the new MA and has informed MBS about this, the MBS informs PE or OP about the failure of the cooperative shortening of MA procedure. The previously received MA remains valid on-board.</p> <p>Failure 2: The MBS has rejected the Cooperative Shortening Request.</p>
Involved Actors	OBU, PE, OP
Trigger	<ul style="list-style-type: none"> MBS receives a Cooperative Shortening Request from PE or OP indicating that it is requested to co-operatively shorten the MA.
Main Sequence	<ol style="list-style-type: none"> When all checks are successful, then MBS indicates this to PE or OP and subsequently sends a Request to Shorten MA message to the OBU based on the Cooperative Shortening Request received from PE or OP When MBS receives the Request to shorten MA is granted message from the OBU, then MBS indicates this to the PE or OP. Subsequently the <i>Train Object</i> (including the Movement Permission) is updated and PE or OP is also informed about that.
Alternate Sequence	None
Failure Sequence	<ol style="list-style-type: none"> When at least one check is not successful, then the MBS indicates this to PE or OP. The co-operative shortening of MA procedure is aborted. When MBS receives the Request to shorten MA rejected message from the OBU, then MBS indicates this to PE or OP. The co-operative shortening of MA procedure is finished.
Comments	None

Table 11 – Description of SysC: Shorten MA cooperatively

5.17.1 Scenario: Shorten MA cooperatively

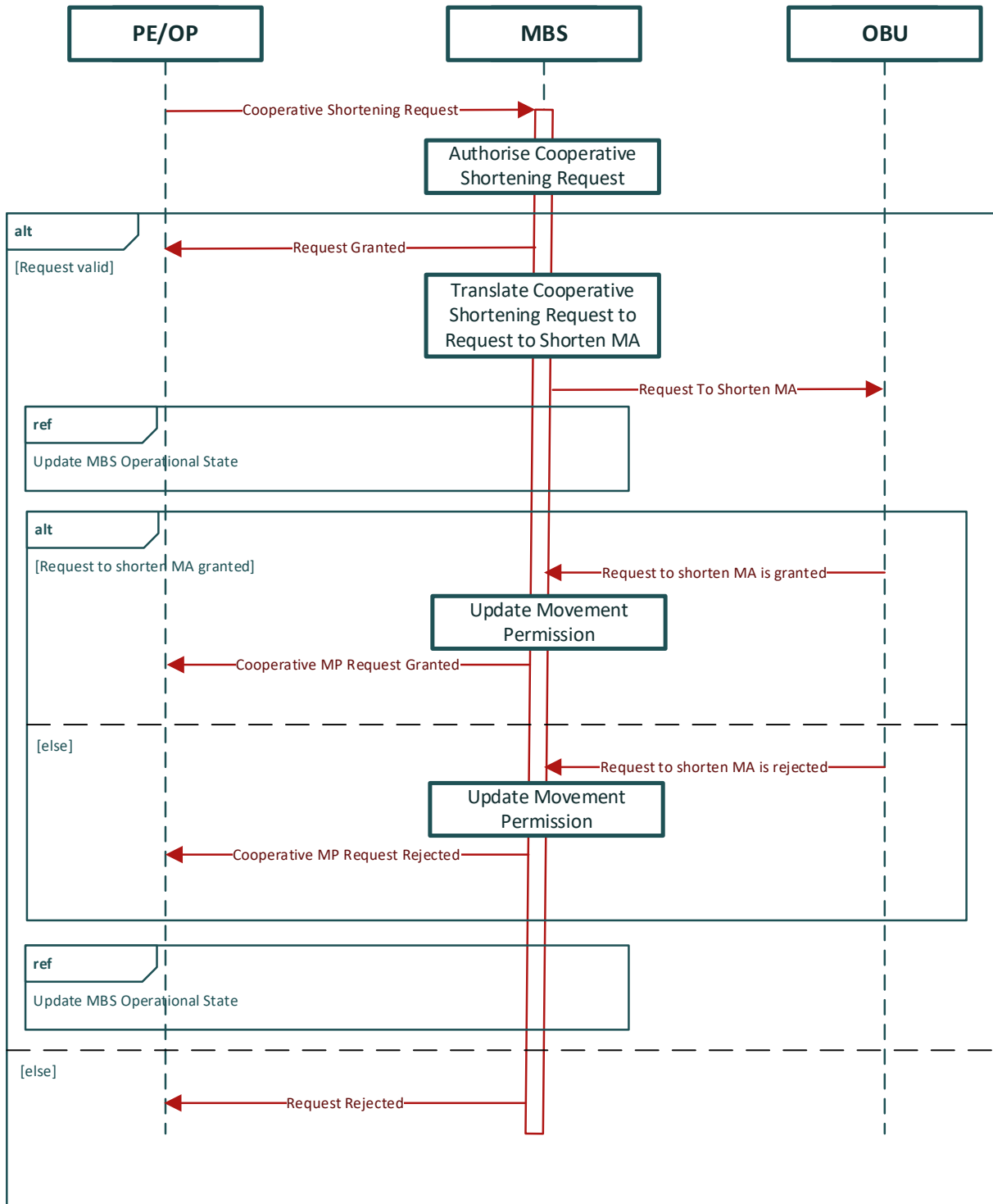


Figure 24 - Scenario 1: Shorten MA cooperatively

5.18 SysC: SUPERVISE TRAINS AND TRACKSIDE ASSETS

Description	The purpose of this capability is to continuously supervise for any issued authorisation (e.g. MA) whether the safety checks are still fulfilled.
-------------	---

Goal	MBS continuously monitors the issued authorisations. In the event of a violation of a safety check, appropriate measures are taken.
Precondition	MBS has already issued an authorisation to the OBU.
Postcondition (Success)	MBS detects that there is a violation of a safety check of a previously issued authorisation and subsequently MBS has triggered appropriate measures to mitigate any hazardous situations.
Postcondition (Failure)	None
Involved Actors	OBU, TACS
Trigger	<ul style="list-style-type: none"> An update of the MBS Operational State is detected.
Main Sequence	<ol style="list-style-type: none"> MBS supervises whether any issued authorisation is impacted by this update of the MBS Operational State. If at least one safety check of an issued authorisation is violated by the update of the MBS Operational State, then MBS triggers to revoke or restrict the authorisation.
Alternate Sequence	2.a) If no safety check is violated by the update of the MBS Operational State, then this capability is finished. It is triggered anew with the next update of the MBS Operational State.
Failure Sequence	None
Comments	None

Table 12 – Description of SysC: Supervise train and trackside assets

5.18.1 Scenario 1: MBS supervises the issued authorisation and detects that at least one safety check of an already issued authorisation is violated.

Note: In this exemplary figure below, it is assumed that the update of the MBS Operational State is triggered by a TA_State_Report. It should be noted that the same scenario could be also possible due to another type of update of the MBS Operational State, e.g. due to a Position Report, propagation of an UTO or creation of an URA.

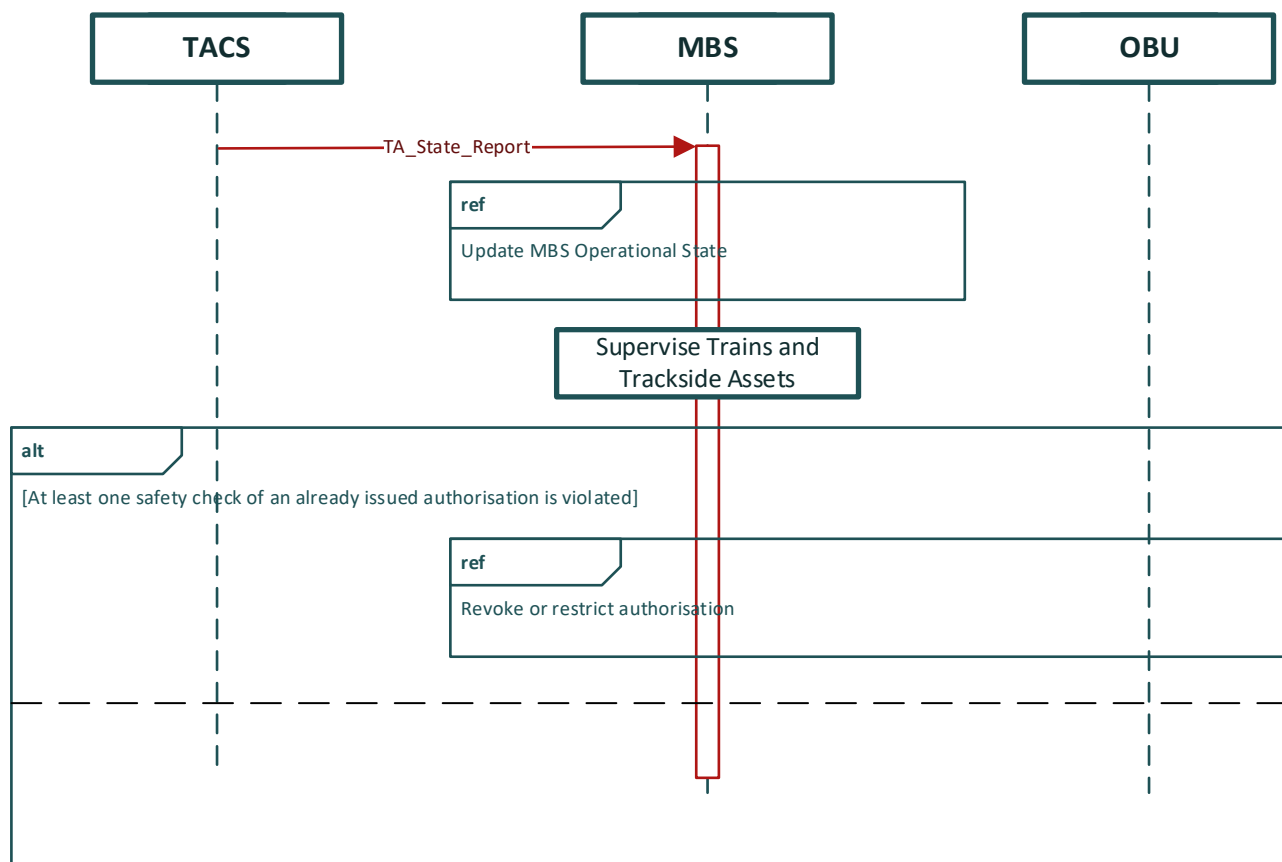


Figure 25 Scenario 1 MBS supervises the issued authorisation and detects that at least one safety check of an already issued authorisation is violated.

5.19 SysC: REVOKE OR RESTRICT AUTHORISATION

Description	The purpose of this capability is to revoke or restrict a granted authorisation for the OBU. This may be triggered by the operator or when the MBS detects that a safety check of an already granted authorisation is not fulfilled anymore.
Goal	MBS has successfully revoked or restricted an already granted authorisation provided to the OBU.
Precondition	MBS has already issued an authorisation to the OBU.
Postcondition (Success)	MBS has successfully revoked or restricted a previously granted authorisation provided to the OBU.
Postcondition (Failure)	The MBS has rejected the Stop Train Request (in case of a request from OP)
Involved Actors	OBU, PE, OP
Trigger	<ul style="list-style-type: none"> MBS has received a Stop Train Request from OP indicating that it is requested to stop a train (at a certain location) MBS detects that a safety check for an already granted authorisation is not fulfilled anymore. <ul style="list-style-type: none"> This is detected by the capability 'Supervise train and trackside assets'

Main Sequence	1. In case this capability is triggered by a request received from the OP, then MBS checks whether the request can be executed for the referenced train and indicates this to the OP.
	2. MBS revokes or restricts the authorisation to OBU.
	3. In case this capability has been triggered by a request from the OP and MBS has received Release Stop Train Request by Operator, then MBS is allowed to issue authorisations again and acknowledges this request to the OP.
Alternate Sequence	None
Failure Sequence	1.a) When at least one check is not successful, then the MBS indicates this to OP. This procedure to revoke or restrict an authorisation is aborted.
Comments	In case MBS uses emergency stop messages (Conditional or Unconditional Emergency Stop) to revoke or restrict an authorisation, those have to be revoked to allow a continuation of train movement. This is not in scope of this capability, but covered by the chapter "General requirements". The MP Extent is not updated. This is to ensure that for example points within the given MP are not moveable.

Table 13 – Description of SysC: Revoke or restrict authorisation

5.19.1.1 Scenario 1: Revoke or restrict authorisation due to a command received by OP

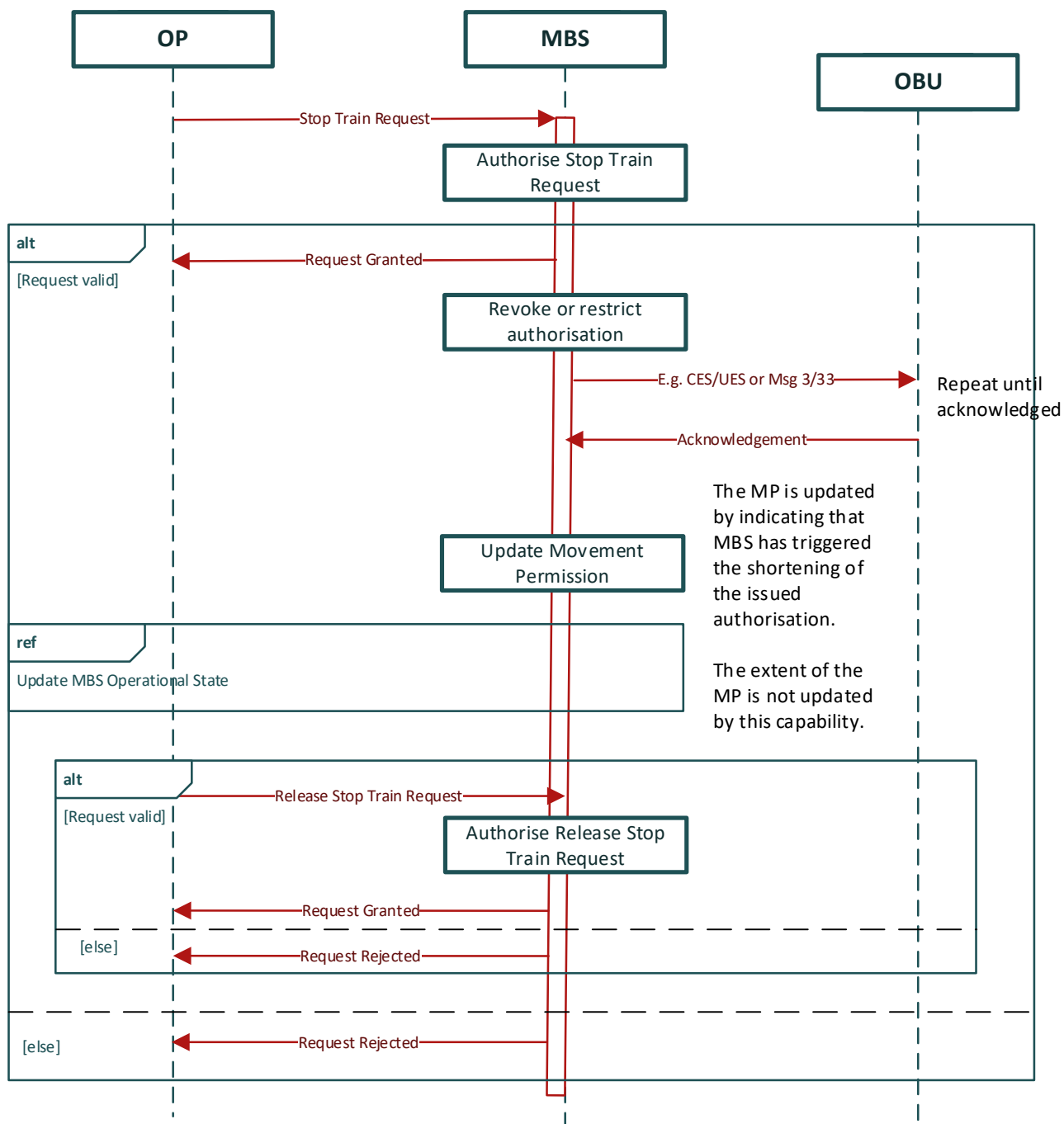


Figure 26 Scenario 1 Revoke or restrict authorisation due to a command received by OP

5.19.1.2 Scenario 2: Revoke or restrict authorisation due to a violation of a safety check of a previously issued authorisation

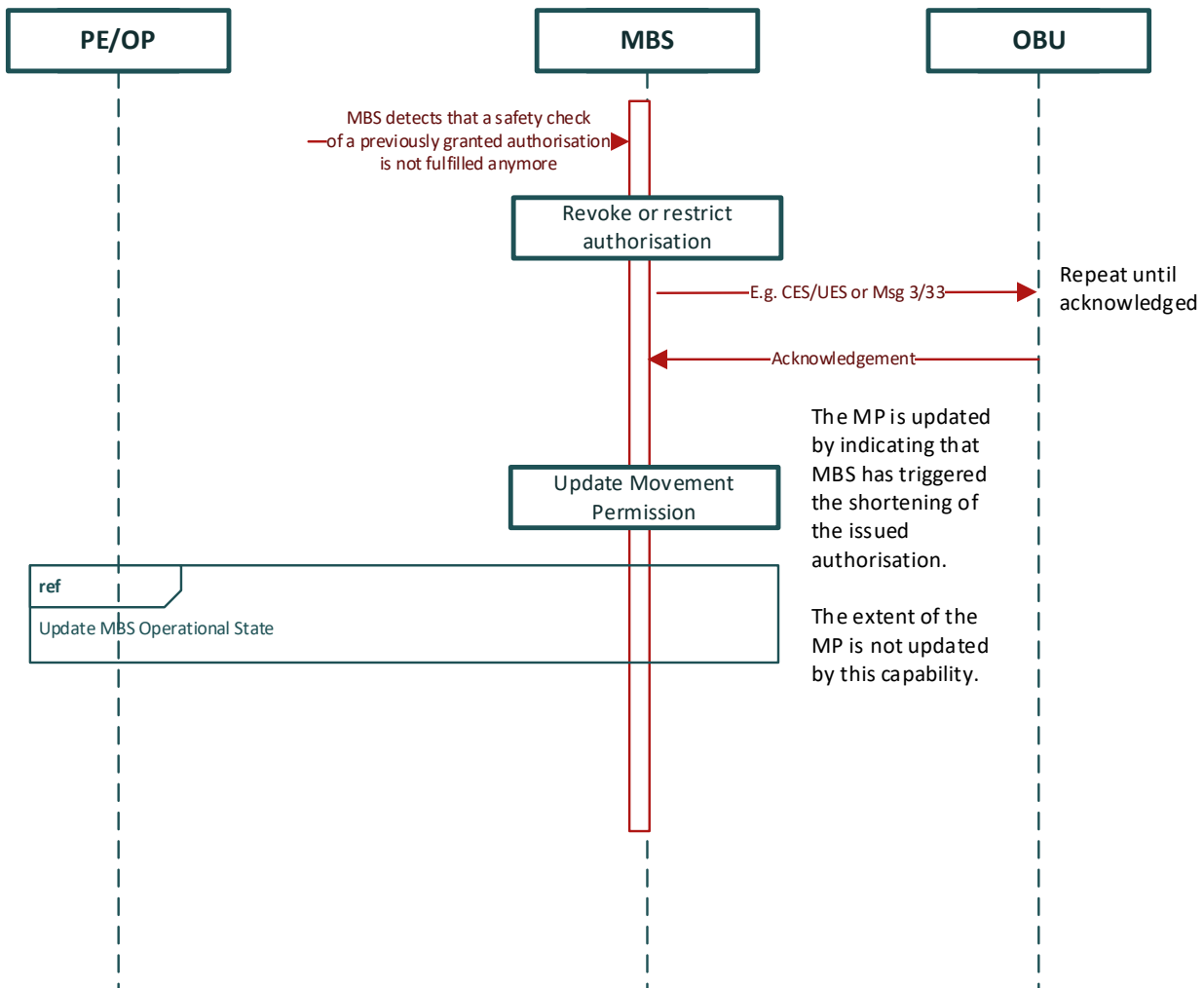


Figure 27 Scenario 2 Revoke or restrict authorisation due to a violation of a safety check

5.20 SysC: CONTINUE AFTER TRAIN TRIP

Description	This capability manages the procedure Train Trip according to /ETCS/ - SUBSET-026 chapter 5.11
Goal	Perform the Train Trip procedure to be able to continue the train mission after the Train Trip.
Precondition(s)	<i>MBS is operational</i>
Postcondition(s) (Success)	MBS has updated the MBS Operational State for a Train in PT mode, after that the Driver selects “Start”.
Postcondition(s) (Failure)	None
Involved actor(s)	OBU, PE, OP
Trigger(s)	MBS receives a Position Report message from an OBU in TR mode.

Main Sequence	Scenario: Train Trip
Alternate Sequence	None
Failure Sequence	
Comments	Please consider that mode change to SH is currently excluded by the scope of the document.

5.20.1 Scenario: Train Trip

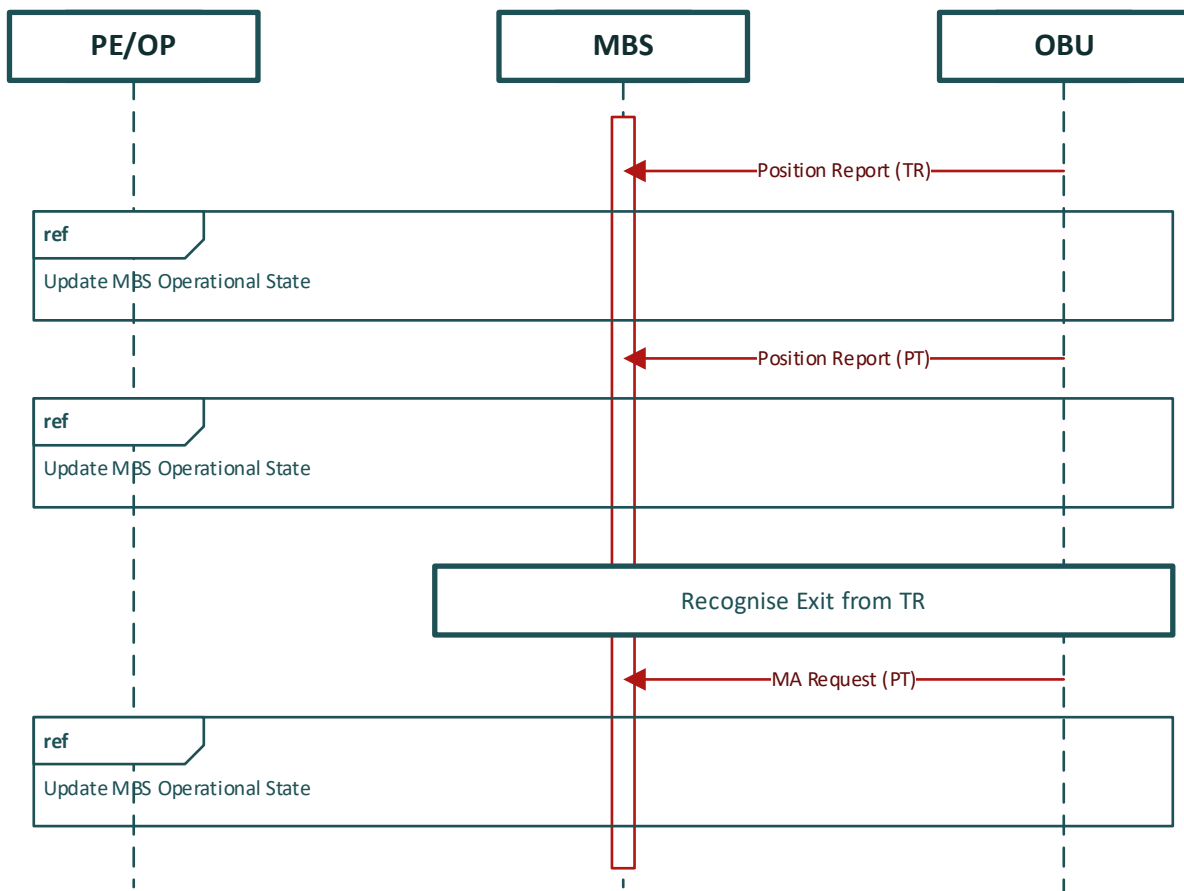


Figure 28 - Scenario : Train Trip

The function “Recognise Exit from TR” referenced in the scenario is not further detailed as the behaviour is specified in /ETCS/ SUBSET-026 5.11.

5.21 SysC: RECOVERING DEGRADED TTD SITUATIONS

Description	The purpose of this capability is to recover the MBS from trackside degraded situations concerning TTD, which hinder MBS from performing in full scale. Degraded situations are understood according to /OPETSI/
Goal	After receiving an operational failure state message from TACS, bring TACS back into normal operation

Precondition	<i>MBS is operational</i> TTD section is disturbed because of operational reasons (as defined in EULYNX)
Postcondition (Success)	TACS is operating in normal operation
Postcondition (Failure)	Failure 1: TACS is still in degraded situation
Involved Actors	TACS (TTD), PE, OP
Trigger	<ul style="list-style-type: none"> MBS receives a failure state message from TACS via I_TACS (SCI-TDS) due to operational reasons (negative counting, “-1”) MBS identifies a failure counting in a TTD section (positive counting, “+1”)
Main Sequence	<p>Scenario 1: MBS receives “TVPS Occupancy Status” with occupancy status is “TVPS is in state disturbed” and with “Disturbance is operational” and recovering is done fully automatic or</p> <p>Scenario 2: MBS receives “TVPS Occupancy Status” with occupancy status is “TVPS is in state disturbed” and with “Disturbance is operational” and recovering is done with full responsibility of the operator or</p> <p>Scenario 3: MBS receives “TVPS Occupancy Status” with occupancy status is “TVPS is in state disturbed” and with “Disturbance is operational” and recovering is supported by MBS with automatically issued URA after processing the reset command or</p> <p>Scenario 4: MBS receives “TVPS Occupancy Status” with occupancy status is “TVPS is in state disturbed” and with “Disturbance is operational” and recovering is supported by using TTD capability of sweeping</p>
Alternate Sequence	None
Failure Sequence	None (if recovering isn’t successful, degraded mode is still given)
Comments	All scenarios depend on the particular configuration of MBS. Scenario 1 can exist next of one the other scenarios. Scenario 2, scenario 3 and scenario 4 are mutually exclusive.

Hint: Using /EULYNX/ there are several possibilities to reset TTD sections. MBS acts as the “interlocking” part in /EULYNX/. A reset by or via MBS is therefore only possible, if the reported TTD system’s disturbance is “operational”. “TVPS Occupancy Status” is defined in /EULYNX/. The scenario 1 can be used in a very specific situation, in which MBS can reset fully automatically. If not configured, one of the other scenarios apply. The scenarios 2, 3 and 4 can exist in parallel to scenario 1 but not besides each other. They all describe that a TTD section reset is only possible through requests from OP. They are applicable for all kind of TTD section operational disturbances (last counted axle is in/unknown or out is not relevant). Scenario 2 provides no further assistance to OP. Every request from OP is executed without any check (besides general checks) inside of MBS if conditions are fulfilled to release the TTD section. If necessary, a restriction inside the TTD system is released without any further interaction between OP and MBS.

Scenario 3 provides assistance to OP: An URA forces a train movement in a mode in which the non-occupation of the track is supervised by the driver. The explorer train runs after resetting the disturbed TTD section. After the explorer train, every request is executed without any check (besides general checks) inside of MBS if conditions are fulfilled to release the TTD section.

Scenario 4 provides another kind of assistance: The /EULYNX/ capability of sweeping the TTD section forces a train movement in a mode in which the non-occupation of the track is supervised by the driver. The explorer train runs before resetting the disturbed TTD section. After this an acknowledgement is needed by OP, that the train passed the disturbed TTD section completely.

5.21.1 Scenario 1: Automatic Reset TTD Section

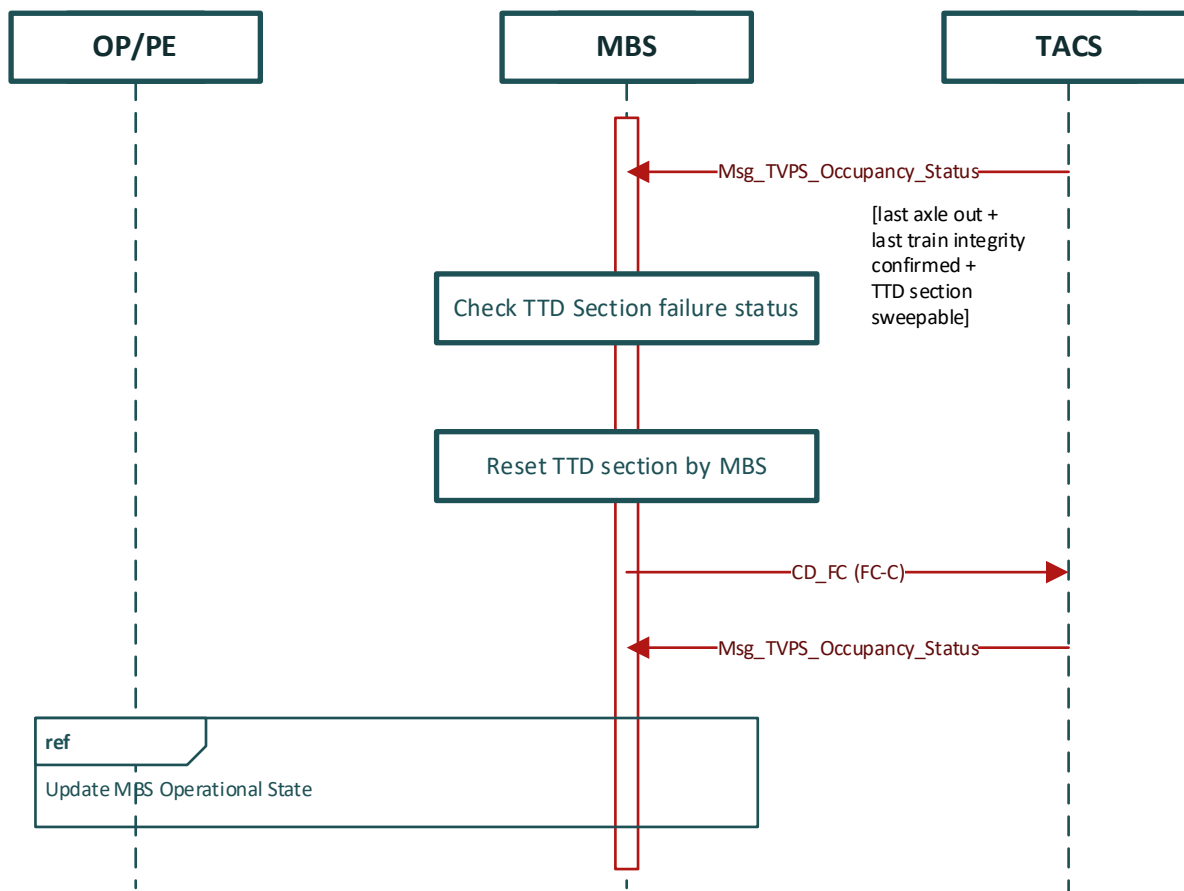


Figure 29 - Scenario 1: Automatic Reset TTD Section

5.21.2 Scenario 2: Manual Reset TTD Section with Explorer Train

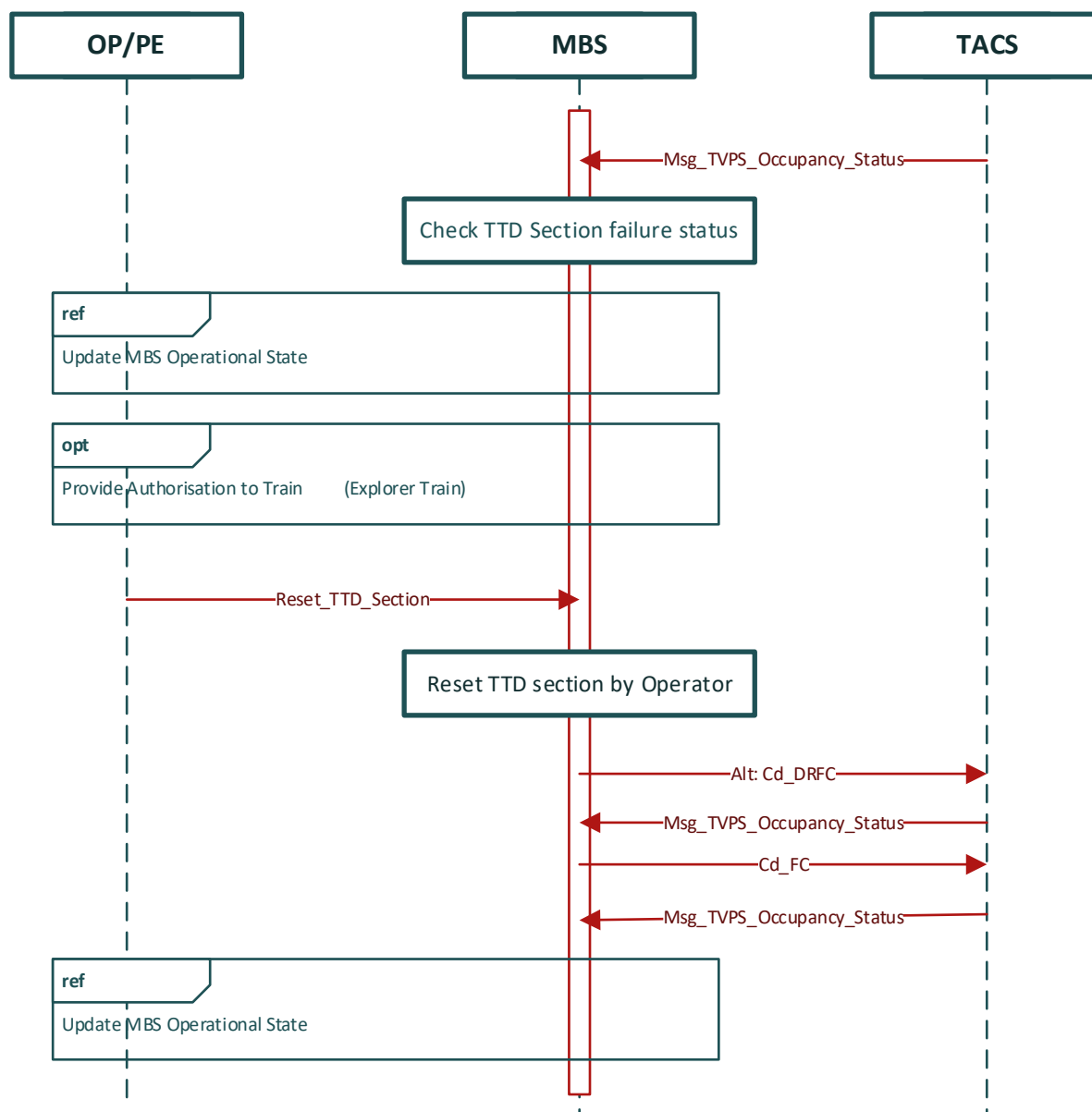


Figure 30 - Scenario 2: Manual Reset TTD Section with Manual Operational Clearance

5.21.3 Scenario 3: Supported Reset TTD Section with Explorer Train

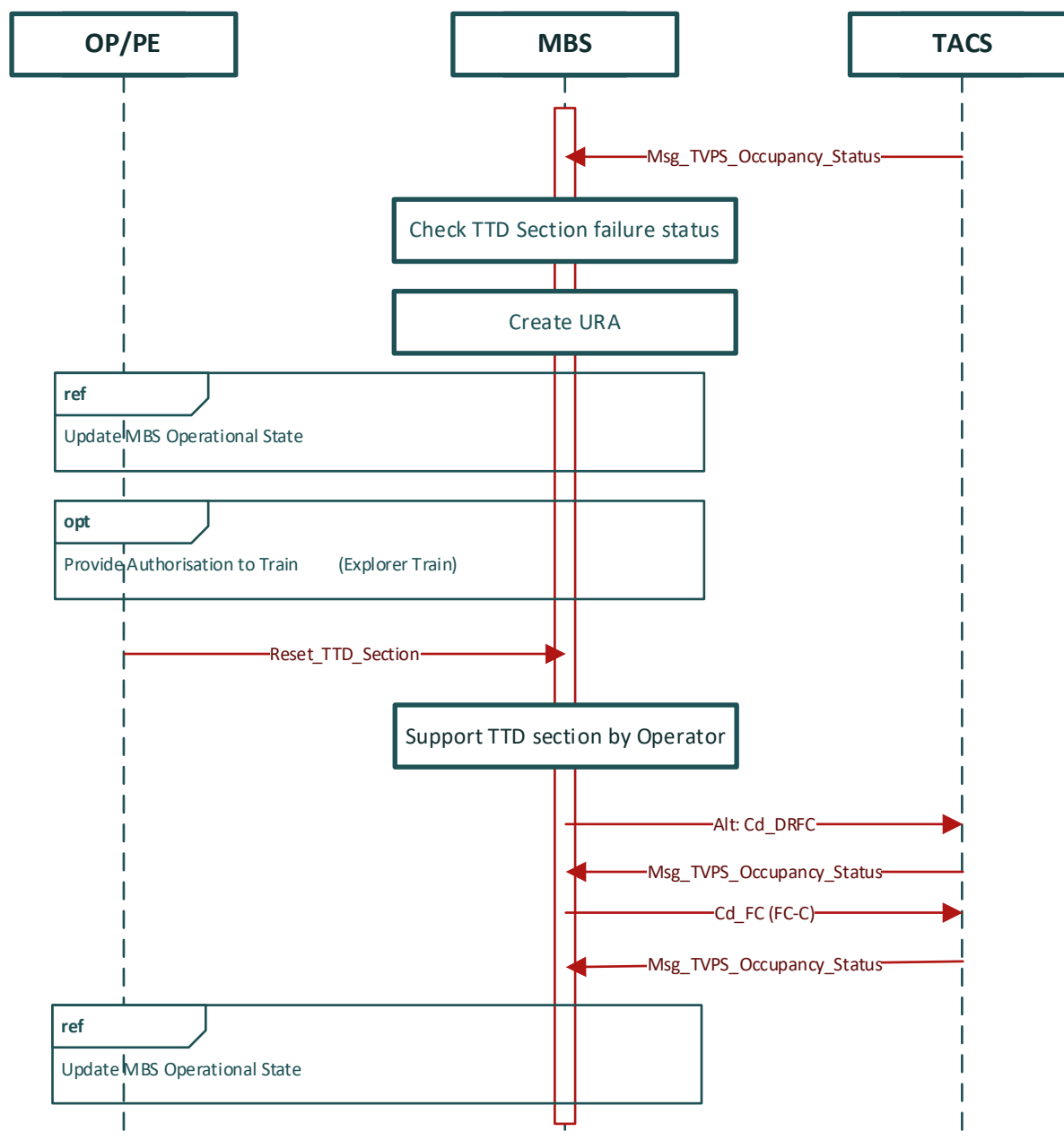


Figure 31 - Scenario 3: Supported Reset TTD Section with Using Restriction Area

5.21.4 Scenario 4: Reset TTD Section using TTD capability using Sweeping

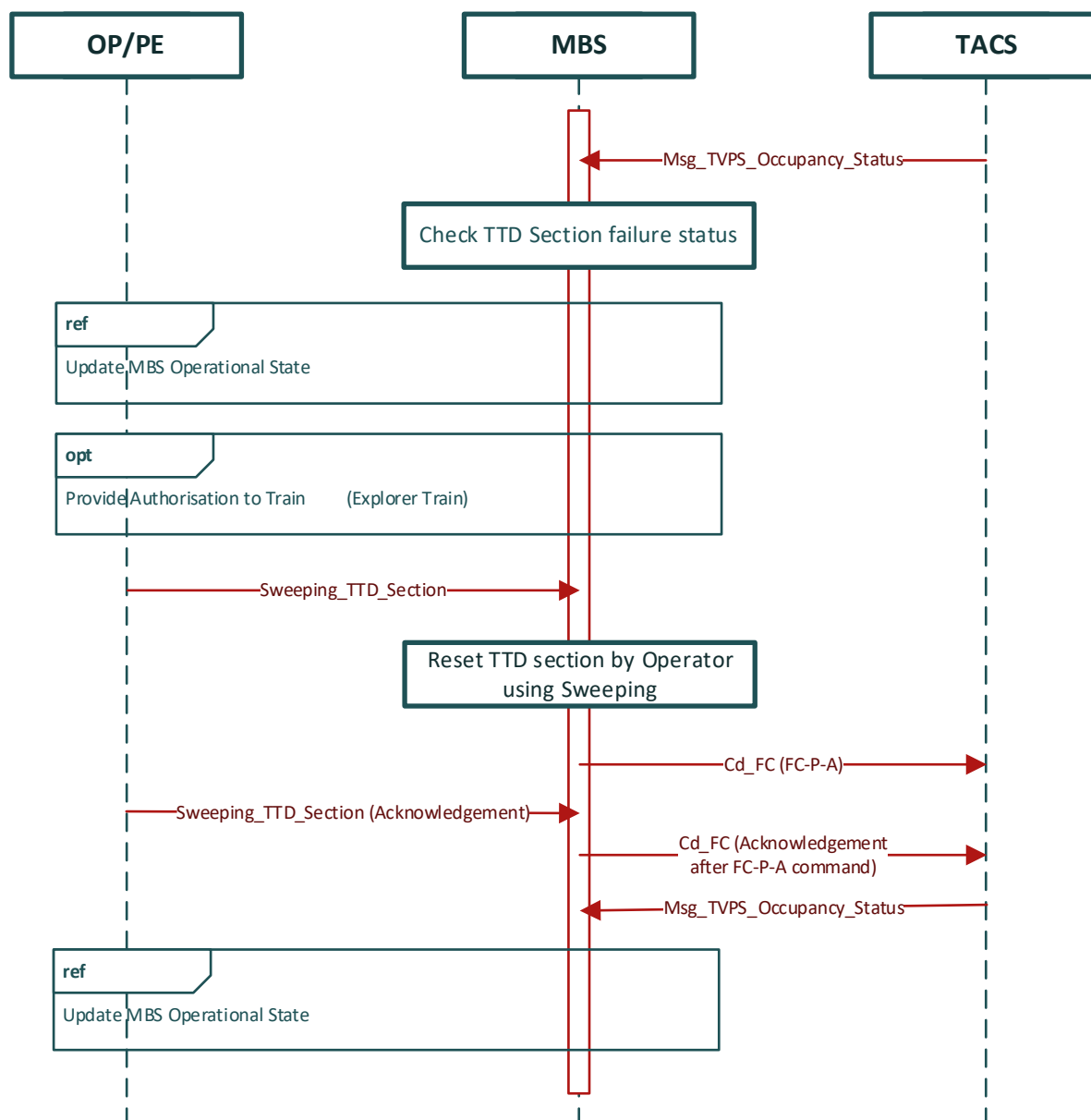


Figure 32 - Scenario 4: Reset TTD Section with TTD capability Sweeping

5.22 SYS C: MANAGE USAGE RESTRICTION AREA

Description	This capability allows to establish (create) or remove (delete) restrictions in an area (<i>Usage Restriction Area, URA</i>) on the track use (e.g. speed restriction), <i>switchable Trackside Assets</i> (e.g. disallow to switch), or operability of a <i>Track Area</i> (e.g. only allow local operation).
Goal	<i>MBS</i> has an updated <i>Domain Model</i> with all required restrictions. Note: To obey the effect of <i>URAs</i> is part of other capabilities.
Precondition(s)	<ul style="list-style-type: none"> • <i>MBS</i> is operational • Communication between <i>MBS</i> and <i>OP/PE</i> established
Postcondition(s) (Success)	Creation/deletion message is accepted and <i>Domain Model</i> updated.
Postcondition(s) (Failure)	Creation/deletion message is rejected and <i>Domain Model</i> unchanged.
Involved actor(s)	<i>PE, OP</i>
Trigger(s)	<i>MBS</i> receives a message to create/delete a <i>URA</i>
Main Sequence	<ol style="list-style-type: none"> 1. <i>MBS</i> checks conditions for <i>URA</i> creation/deletion 2. <i>MBS</i> accepts creation/deletion of <i>URA</i>
Alternate Sequence	None
Failure Sequence	<i>MBS</i> rejects creation/deletion of <i>URA</i>
Comments	From overall system point of view, <i>URAs</i> can be pre-configured in <i>Topology Data</i> (then they can simply be activated/deactivated) or dynamically created (then they are created/deleted on demand). However, if on system level a <i>URA</i> is activated, it will be requested to be created with <i>MBS</i> , and if on system level a <i>URA</i> is to be deactivated, it will be requested to be removed from <i>MBS</i> . Thus, from <i>MBS</i> point of view it is always a creation/deletion.

5.22.1 Overview: Usage Restriction Area

URAs can be created according to an *Operational Plan* (e.g. for enabling construction works) or in response to an incident (e.g. as a mitigation measure).

Their restriction will affect:

1. *Movement Permissions* (e.g. restricted speed; *URA* type: **Restricted MP**),
2. *Switchable Trackside Assets* (e.g. switching not allowed; *URA* type: **Restricted sTA**), or
3. the operability of an area (e.g. remote/local operation of both *MPs* and *sTAs*; *URA* type: **Restricted operability**).

Some of these restrictions can already be realised as track properties/track conditions in the pre-engineered *Topology Data*. However, also for these there can be the need for their temporary presence (creation/deletion). As well, these restrictions can be pre-configured in the *Topology Data* but they have to be activated (and later deactivated) so they are not permanent.

It is important to understand that from *MBS* point of view, there is no distinction of dynamically created or semi-permanently, pre-configured restrictions: Also, the latter will be created (when to be activated) or deleted (when to be deactivated) in *MBS* on request by *MBS*' actors like *PE*.

The effect of restrictions is illustrated below by the example of *URAs* which effect the *Movement Permission*:

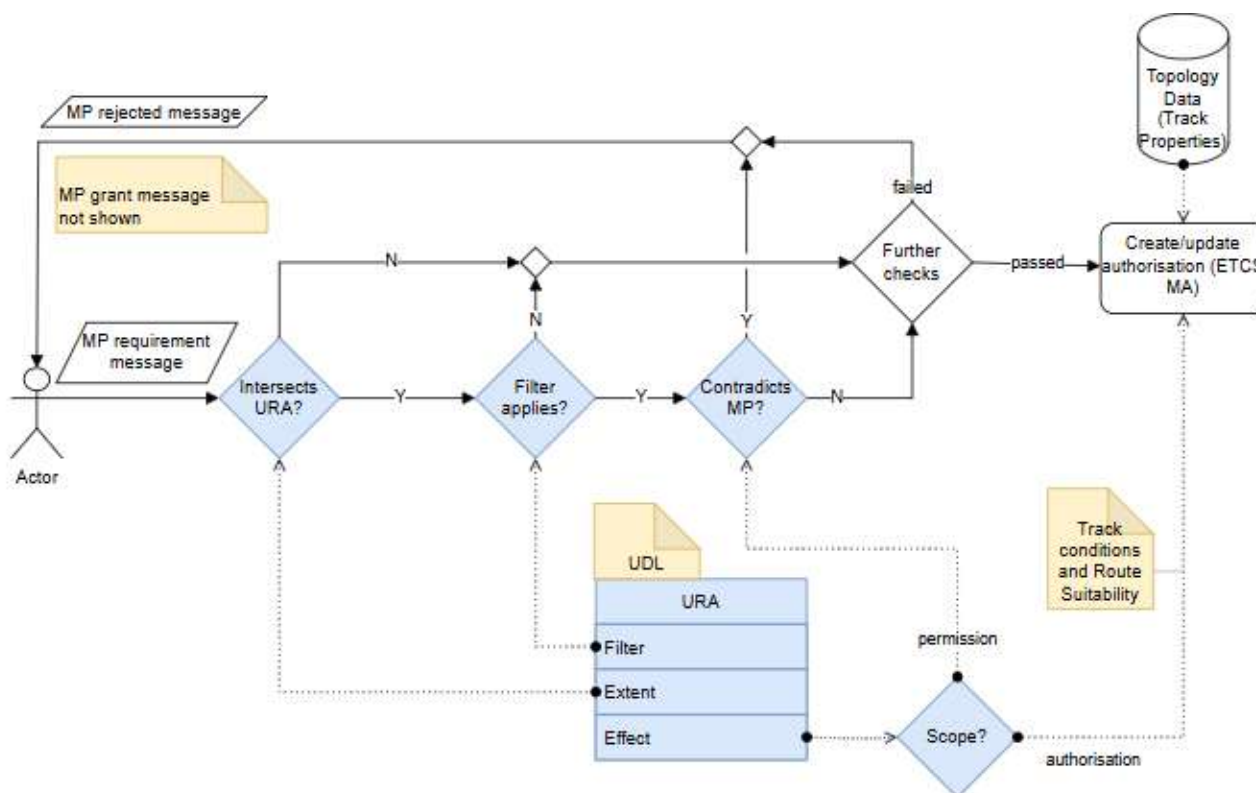


Figure 33: Illustration of URA effect

Note: the application of a *Create URA Demand* over an existing *Movement Permission* may result in a safety reaction.

A *URA* is described by the *URA Definition Language (UDL)* which has amongst ,header information (e.g. ID of the *URA*) three major constituents:

- *Extent* (Track Area, mandatory): geometric extent within the AoC where the restriction applies (e.g. some parallel tracks within a station);
- *Filter* (optional): specification for which *Train Objects* the restriction altogether applies (e.g. only to a certain train category or train running number); and
- *Effect* (mandatory): specification of the restriction as to the restricted property (e.g. speed). The effect can lead both to the rejection of an *MP* request (upper part of the figure) or to the consideration within the authorisation (ETCS *Movement Authority*, right part of the figure, so the supervision of the effect is delegated to the *OBUs*).

The *UDL* will be described in detail in the SCI-(S)CMD interface specification.

The operational use cases for a *URA* can be manifold, for example:

- The speed needs to be temporarily lowered (this is a 'classical TSR). The effect is that a reduced static speed profile is considered in the *MA*;
- A track (area) has to be closed. The effect is that an *MP* request intersecting the *URA* extent is rejected;
- A track might only be entered in a certain ETCS mode. The effect is that an *MP* request intersecting the *URA* with a mode profile different than the specified one will be rejected;
- A track walker needs to be protected from trains from the back but trains from front are allowed (directional *URA*). The effect is that an *MP* request in the wrong direction is rejected.
- A track condition applies temporarily, like a temporary radio hole. The effect is that the related ETCS Track Condition is considered in the *MA*;
- Track workers of a construction area have to be safeguarded. For the construction site itself, the passage and the remote switching of points is forbidden, and for the adjacent tracks a speed restriction is demanded. The effects are that an *MP* request intersecting the *URA* (for the construction site) will be rejected, requests to switch the *sTAs* within are rejected, and the reduced speed of the *URA* for the adjacent tracks is considered in the *MA*;
- Trained or defective *Points* shall not be switched. The effect is that requests to switch the *sTA(s)* within the *URA* are rejected;
- An area within the *AoC* shall only be operated manually. The effect is that requests for *MPs* intersecting the *URA* extent and requests to switch *sTAs* within the *URA* extent are rejected.

The following scenarios contain the creation/deletion of *URAs*. The *URA* can be found in these functions:

1. Restricted *MP*

- SysF Authorise MP Request
- SysF Translate MP Request to Movement Authority

2. Restricted *sTA*

- SysF TA State Request

3. Restricted operability

- Further release (no related capabilities defined yet)

5.22.2 Scenario: Create Usage Restriction Area

A *URA* can be created by a request on the SCI-CMD interface, originated by PE. The request can be rejected if needed conditions are not fulfilled:

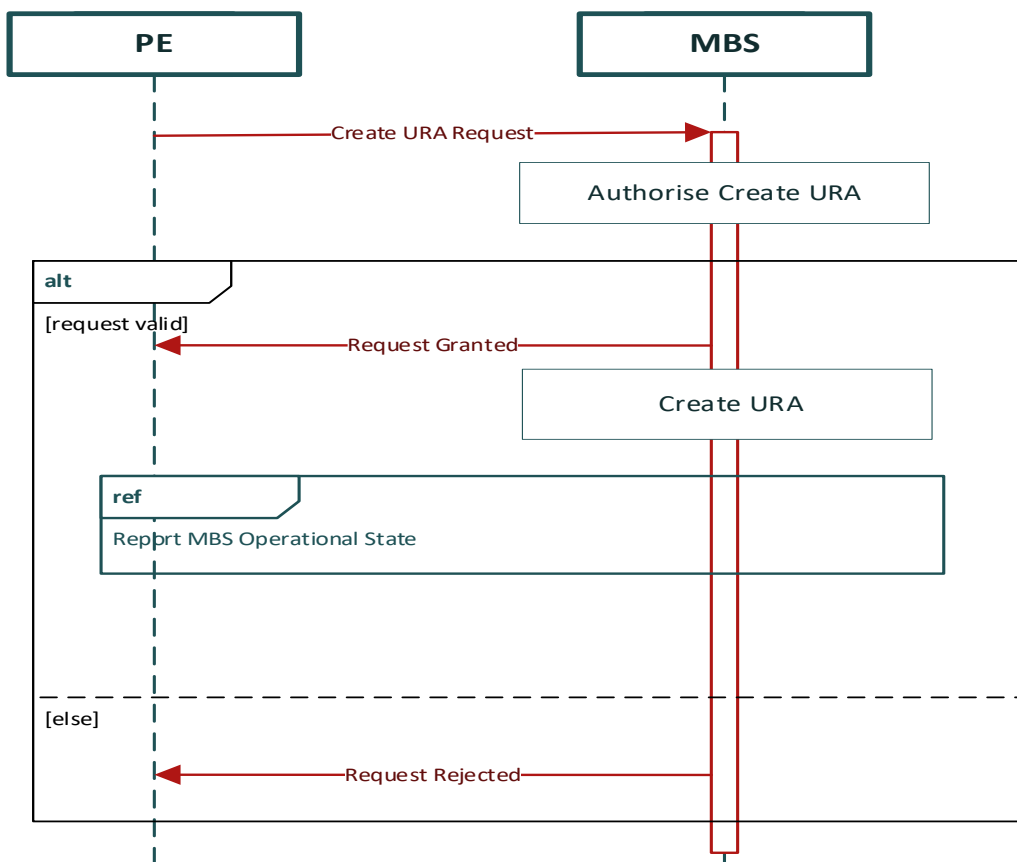


Figure 34: Scenario to create Usage Restriction Area (by PE)

Or it can be created by a request on the SCI-SCMD interface, originated by the operator on the OP. If no safety check fails, the request will be executed and the URA created.

If a safety check would fail, the request will be rejected with the reason.

The operator can decide to by-pass some safety check by applying a demand instead of a request.

Note: the application of a *Create URA Demand* over an existing *Movement Permission* may result in a safety reaction according to requirement REQ-SUPERVISE, due to the violation of the requirement REQ-SC_MP_URA.

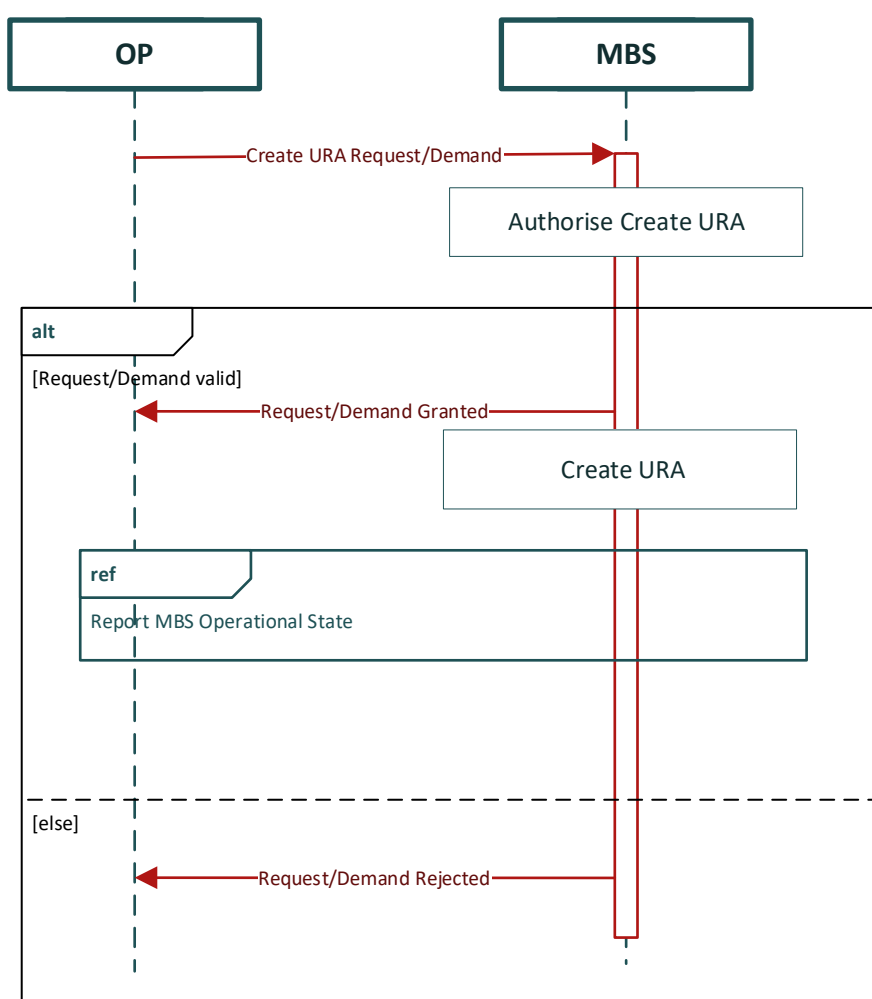


Figure 35: Scenario to create Usage Restriction Area (by OP)

5.22.3 Scenario: Delete Usage Restriction Area

A *URA* can be only deleted by a request on the SCI-SCMD interface, originated by the operator on the OP:

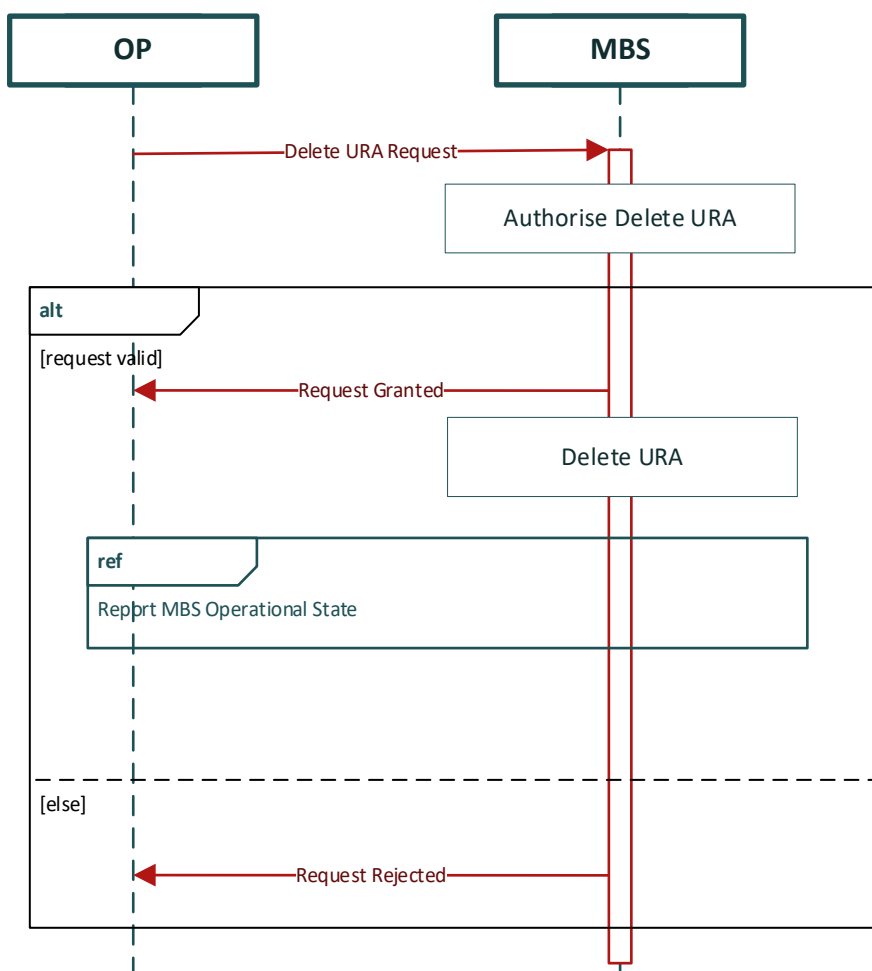


Figure 36: Scenario to delete Usage Restriction Area

5.22.4 Overview of URA usage

The following table gives an overview about the possible restriction properties and originator of a URA and refers to the related requirements.

Restriction property	PE	OP	MBS	REQUIREMENTS	Impacts
speed*	X	X		REQ-SC_MP_URA	MP is rejected
mode*	X	X	X	REQ-SC_MP_URA REQ-SC_SP_URA REQ-SUPERVISE_TRAILED_MOVEMENT*** REQ-0091***	MP/SP is rejected
Track condition		X		REQ-0057	Track description in MA
Route suitability		X		REQ-0057	Track description in MA
Adhesion factor		X		REQ-0057	Track description in MA
noPassage*		X		REQ-SC_MP_URA REQ-SC_SP_URA	MP/SP is rejected
eaExclusion*		X		REQ-SC_MP_URA	MP is rejected
nonSwitchable**		X		REQ-SC_DPS_URA_LOCKED REQ-SC_DPSOD_URA	DPS request and demand rejected
safetyCritical**			X	REQ-SC_DPS_URA_SAFETY_CRITICAL REQ-SUPERVISE_TRAILED_DPSG_DEMAND***	DPS request rejected
<i>manualOperation</i> *-**		X		REQ-SC_DPS_URA_MANUAL_OPS_PE REQ-SC_DPS_URA_MANUAL_OPS_OP REQ-SC_MP_URA REQ-SC_SP_URA	DPS request/MP/SP request rejected
<i>preventAutomaticShuntingRouteRelease</i>		X		REQ-USP-2 REQ-USP-3	Prevents removal of SP
<i>preventProceed</i>		X		REQ-SIG-5 REQ-SIG-6 REQ-SIG-7	Prevents a proceed aspect
<i>preventSignalAspect</i>		X		REQ-SIG-3	Prevents

* = restrictions on Movement Permission (Movement Permission can be rejected due to URA conflict)

** = restrictions on DPS Group (DPS Group command can be rejected due to URA conflict)

*** = requirement to create a URA by MBS (URA is directly created by MBS without URA creation command from OP)

X = System that originated the URA

5.23 SysC: AUTHORISE SHUNTING

Description	This capability confirms a shunting request for a particular OBU.
Goal	After receiving a Request for Shunting message from OBU, MBS forwards this request to PE and OP. As soon as MBS receives the confirmation by PE or OP it confirms the shunting request by sending the message SH Authorised to OBU.
Precondition	<i>MBS is operational</i>
Postcondition (Success)	MBS has confirmed the shunting request.
Postcondition (Failure)	MBS has refused the shunting request.
Involved Actors	OBU, PE, OP
Trigger	<ul style="list-style-type: none"> MBS receives a Request for Shunting message from OBU
Main Sequence	<ol style="list-style-type: none"> MBS forwards the request for shunting to PE and OP by sending an SH Confirmation Request to PE and OP. As soon as MBS receives the Shunting Request Confirmed message from PE or OP, MBS sends SH Authorised to OBU.
Alternate Sequence	None
Failure Sequence	2. When MBS receives Shunting Request Rejected message from PE or OP, MBS sends SH Refused to OBU.
Comments	Currently there are no harmonised procedures available in regards to shunting. Therefore, MBS does not perform any further checks (e.g. is train position known, inside the AoC, etc.) before authorising Shunting.

5.23.1 Scenario: Authorise Shunting

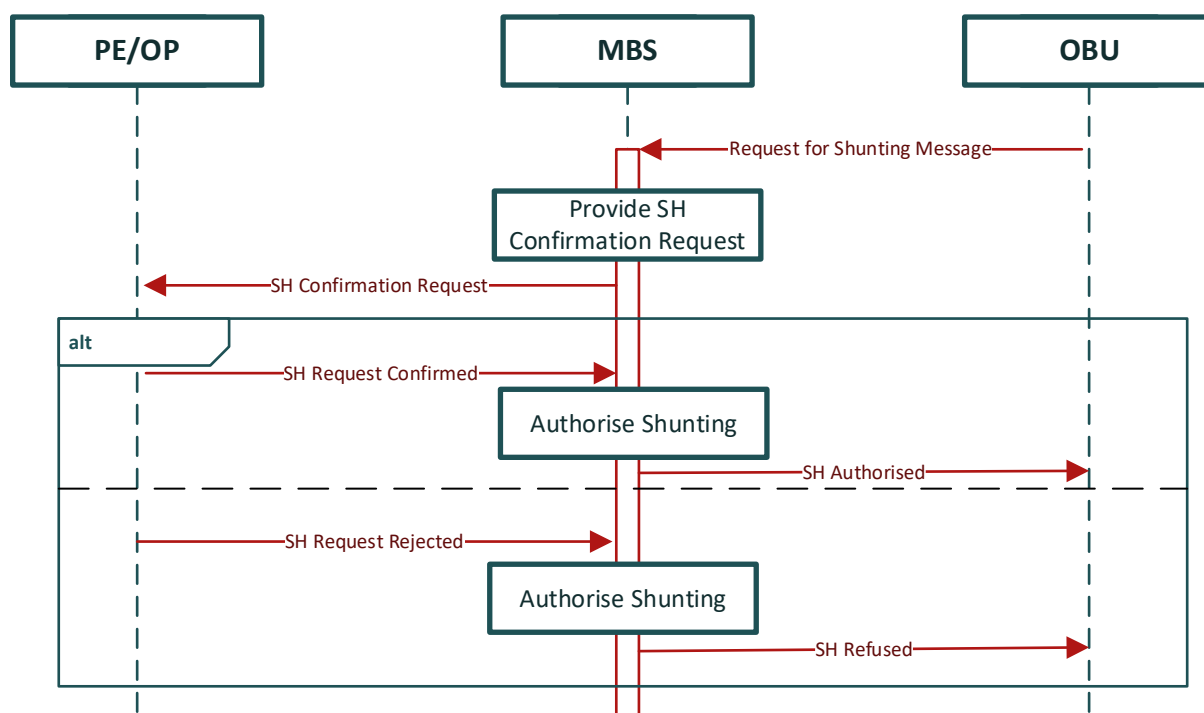


Figure 37: Scenario: Authorise Shunting

5.24 SysC: SET SHUNTING PERMISSION

Table 14 – Description of SysC: Set Shunting Permission

Description	This capability generates a Shunting Permission and updates the signal aspects for shunting signals
Goal	After receiving a SP request, from PE or OP, MBS checks all safety constraints, generates a Shunting Permission and updates the shunting signals as needed.
Precondition	<i>MBS is operational</i>
Postcondition (Success)	Shunting signals are in the desired state and the shunting movement can start; Shunting Permission reported to PE and OP via the <i>MBS Operational State</i> .
Postcondition (Failure)	<i>SP request is rejected</i>
Involved Actors	TACS (Shunting Signal), PE, OP
Trigger	<ul style="list-style-type: none"> MBS receives a SP Request
Main Sequence	When all checks are successful, MBS indicates this to PE or OP respectively, creates a Shunting Permission in the Operational State and sets the shunting signals as required.
Alternate Sequence	None
Failure Sequence	When at least one check fails, MBS reports a Request Rejected to the requesting entity, PE or OP, indicating the reason why the SP Request could not be granted.

Comments	In SH, the driver is responsible for remaining inside the shunting area defined by the aspect of the shunting signals.
----------	--

5.24.1 Scenario: Set Shunting Permission

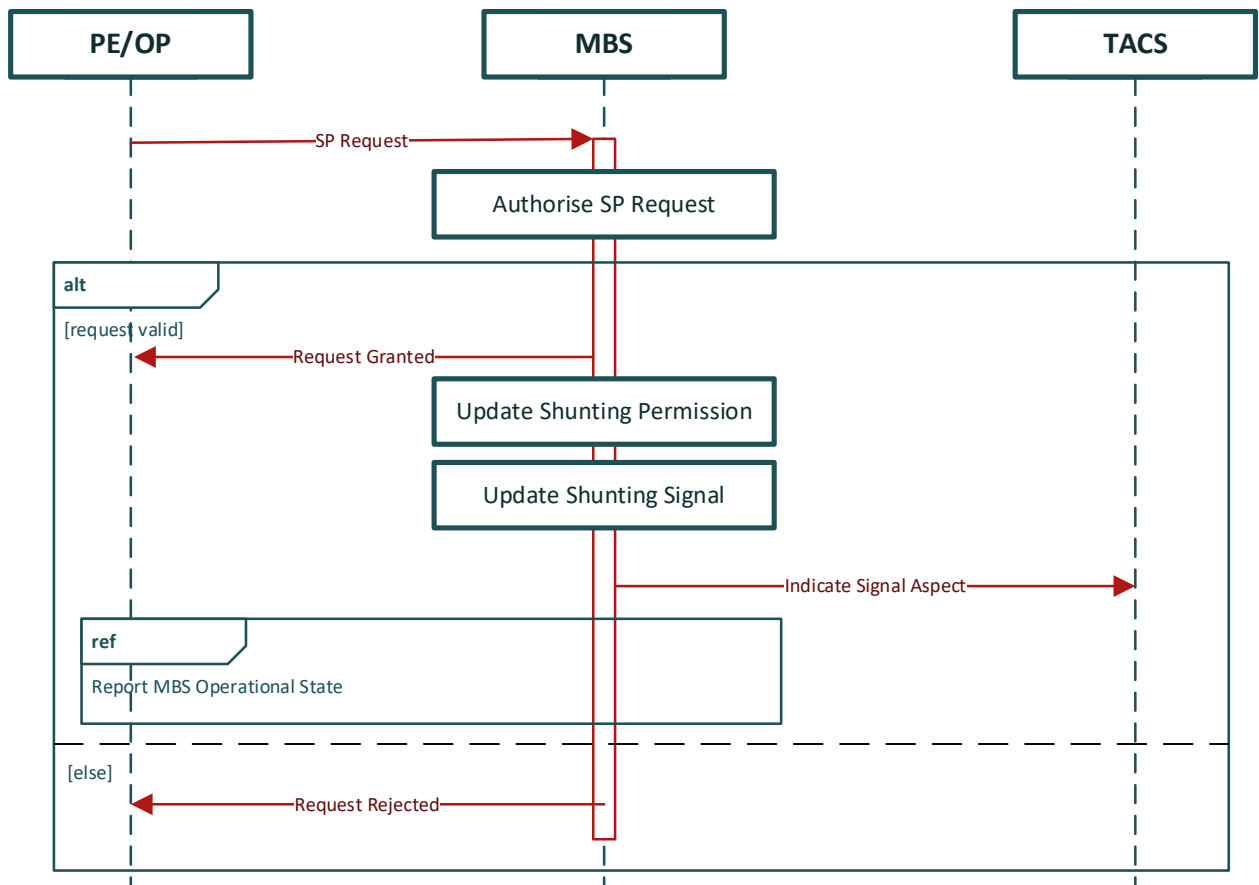


Figure 38 - Scenario : Set Shunting Permission

5.25 SysC: SUPERVISE SHUNTING PERMISSION

Description	The purpose of this capability is to continuously supervise Shunting Permissions whether the safety checks are still fulfilled.
Goal	MBS continuously monitors authorised Shunting Permissions. In the event of a violation of a safety check, appropriate measures are taken.
Precondition	MBS has authorised at least one Shunting Permission.
Postcondition (Success)	MBS has detected that there is a violation of a safety check of a previously authorised Shunting Permission and subsequently MBS triggered appropriate measures to mitigate any hazardous situations.

Postcondition (Failure)	None
Involved Actors	TACS, OP, PE
Trigger	<ul style="list-style-type: none"> An update of the MBS Operational State is detected.
Main Sequence	<p>1. MBS supervises whether any authorised Shunting Permission is impacted by this update of the MBS Operational State.</p> <p>2. If at least one safety check of an established Shunting Permission is violated by the update of the MBS Operational State, then MBS sets the corresponding Shunting signals to stop.</p>
Alternate Sequence	2.a) If no safety check is violated by the update of the MBS Operational State, then this capability is finished.
Failure Sequence	None
Comments	In SH, the driver is responsible for remaining inside the shunting area defined by the aspect of the shunting signals.

5.25.1 Scenario 1: MBS supervises the authorised Shunting Permission and detects that at least one safety check is violated.

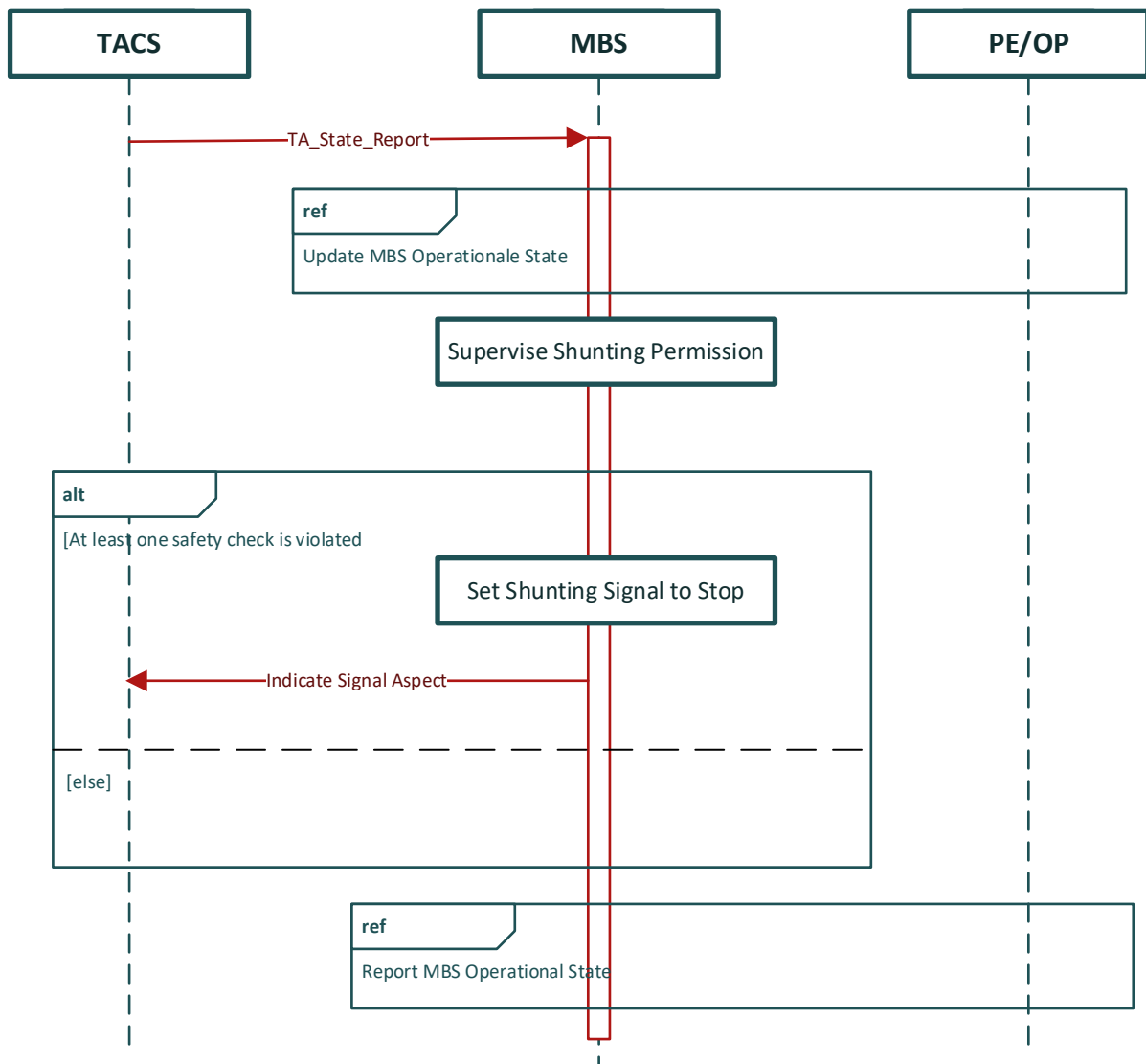


Figure 39 - Scenario : Supervise Shunting Permission

5.26 SysC: UPDATE SHUNTING PERMISSION

Table 15 – Description of SysC: Update Shunting Permission

Description	This capability updates a Shunting Permission and the signal aspects for shunting signals.
Goal	After a TA state report has been received, the Shunting Permission is modified according to the received event.
Precondition	<i>MBS is operational</i>

Postcondition (Success)	The Shunting Permission is updated to reflect the influence from the train to the existing permission.
Postcondition (Failure)	None
Involved Actors	TACS, PE, OP
Trigger	<ul style="list-style-type: none"> MBS receives a TA state report
Main Sequence	After the state report has been received, the Shunting Permission has to be altered. Additionally, a shunting signal might have to be set to a stop aspect.
Alternate Sequence	None
Failure Sequence	None
Comments	<p>Violations of safety checks of the granted Shunting Permission and the corresponding reaction by MBS are covered by capability 'Supervision Shunting Permission'.</p> <p>In SH, the driver is responsible for remaining inside the shunting area defined by the aspect of the shunting signals.</p>

5.26.1 Scenario: Update Shunting Permission

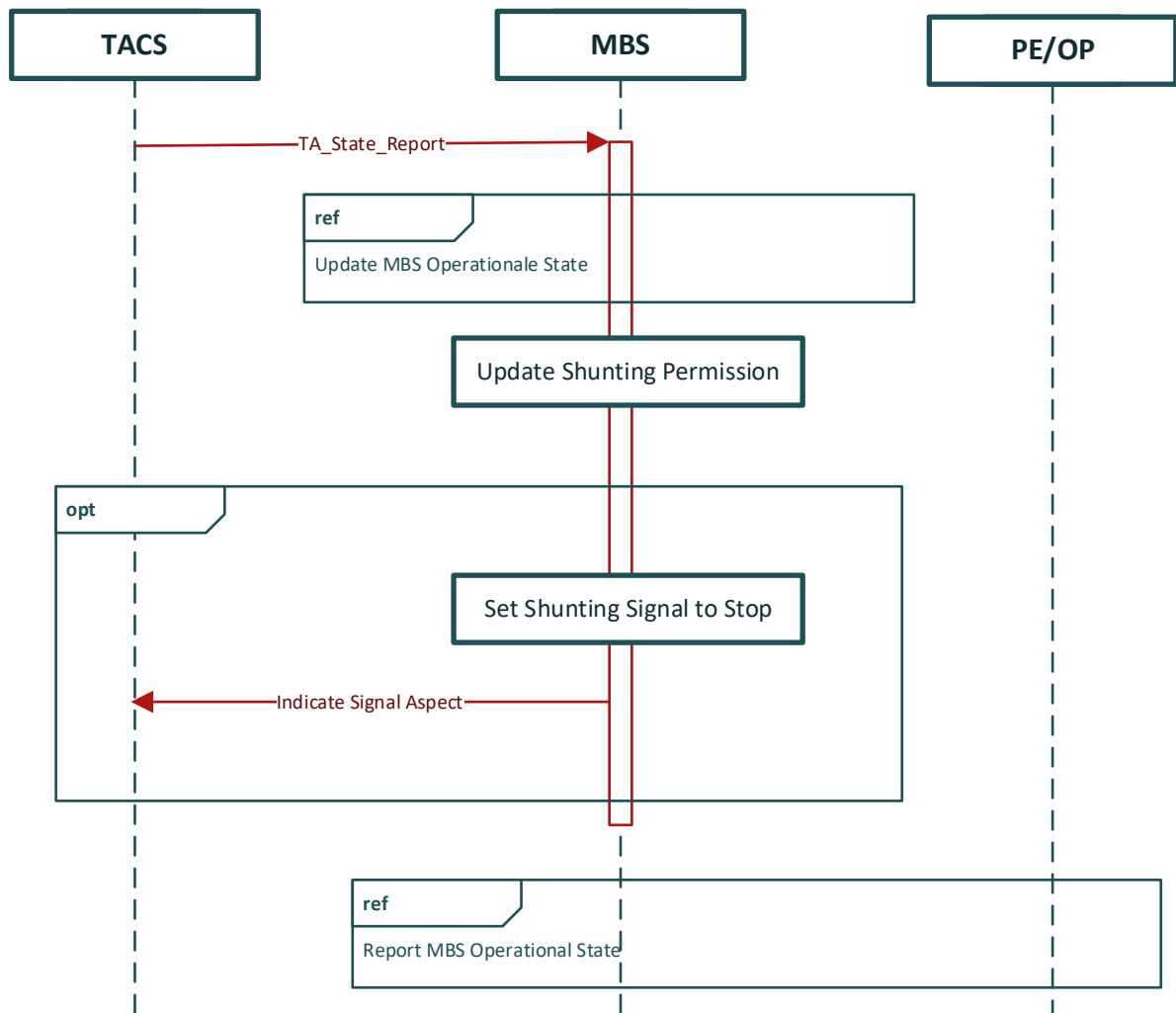


Figure 40 - Scenario : Update Shunting Permission

5.27 SysC: HANDLE EMERGENCY STOP FOR SHUNTING SIGNAL

Table 16 – Description of SysC: Emergency Stop for Shunting Signal

Description	This capability sets a shunting signal to a stop aspect if requested from the operator.
Goal	After receiving an Shunting Signal Stop Demand from OP, MBS checks all safety constraints and sets the shunting signal to stop.
Precondition	<i>MBS is operational</i>
Postcondition (Success)	The shunting signal is set to a stop aspect.
Postcondition (Failure)	None
Involved Actors	TACS, OP
Trigger	<ul style="list-style-type: none"> MBS receives an EmergencyStopDemand

Main Sequence	When all checks are successful, the corresponding signal is set to stop and other shunting signal's aspects are adjusted if needed.
Alternate Sequence	None
Failure Sequence	None
Comments	In SH, the driver is responsible for remaining inside the shunting area defined by the aspect of the shunting signals.

5.27.1 Scenario: Emergency Stop for Shunting Signal

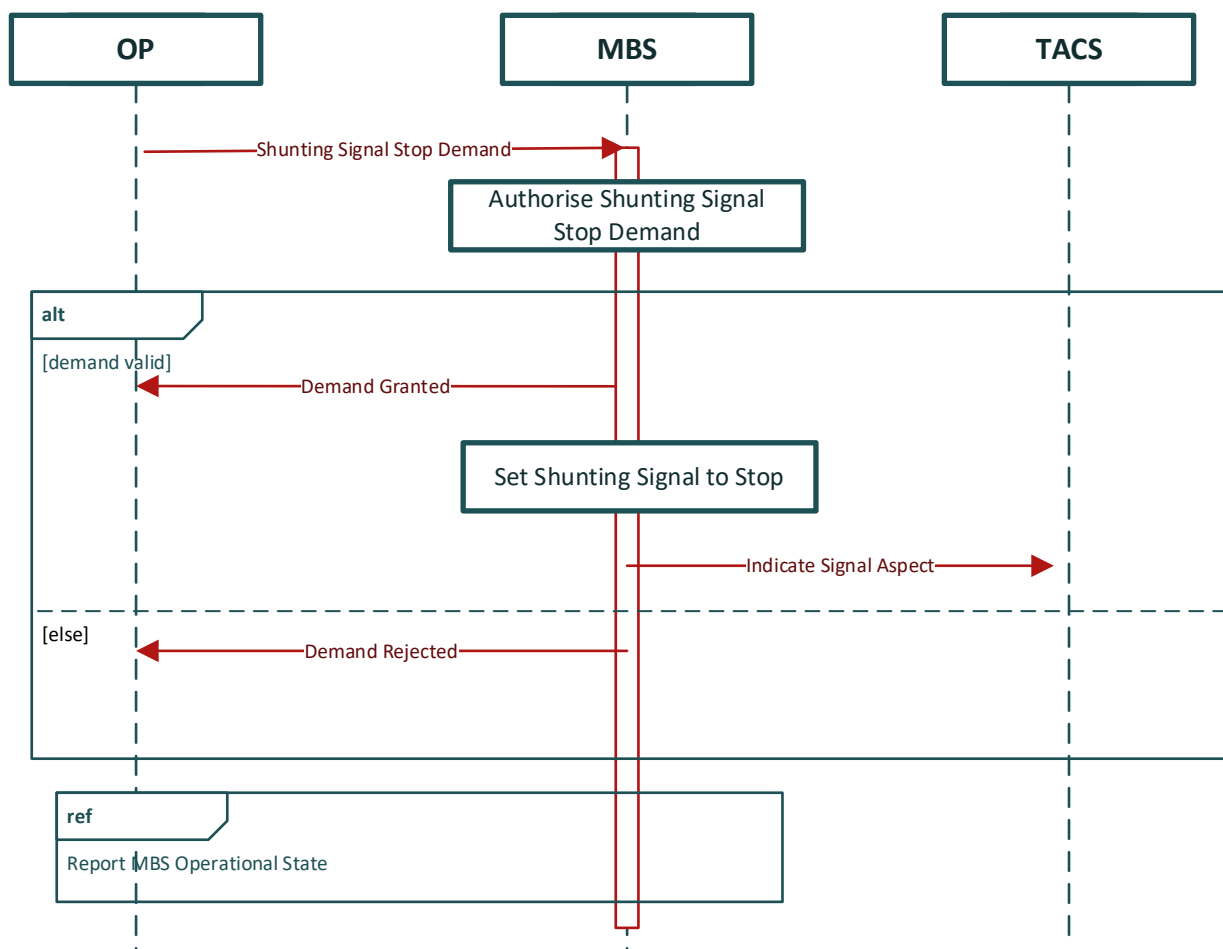


Figure 41 - Scenario : Handle Emergency Stop for Shunting Signal

5.28 SysC: REVOKE SHUNTING PERMISSION

Table 17 – Description of SysC: Revoke Shunting Permission

Description	This capability revokes a Shunting Permission.
Goal	After a demand to revoke a Shunting Permission has been received, the Shunting Permission is revoked.

Precondition	<i>MBS is operational</i>
Postcondition (Success)	The Shunting Permission is removed from the <i>MBS Operational State</i>
Postcondition (Failure)	None
Involved Actors	OP, PE, TACS
Trigger	<ul style="list-style-type: none"> MBS receives a Revoke SP Demand
Main Sequence	When all checks are successful, MBS indicates this to OP and removes the Shunting Permission from the <i>MBS Operational State</i> .
Alternate Sequence	None
Failure Sequence	When at least one check fails, MBS reports a Request Rejected to OP, indicating the reason why the Revoke SP Demand could not be granted.
Comments	None

5.28.1 Scenario: Revoke Shunting Permission

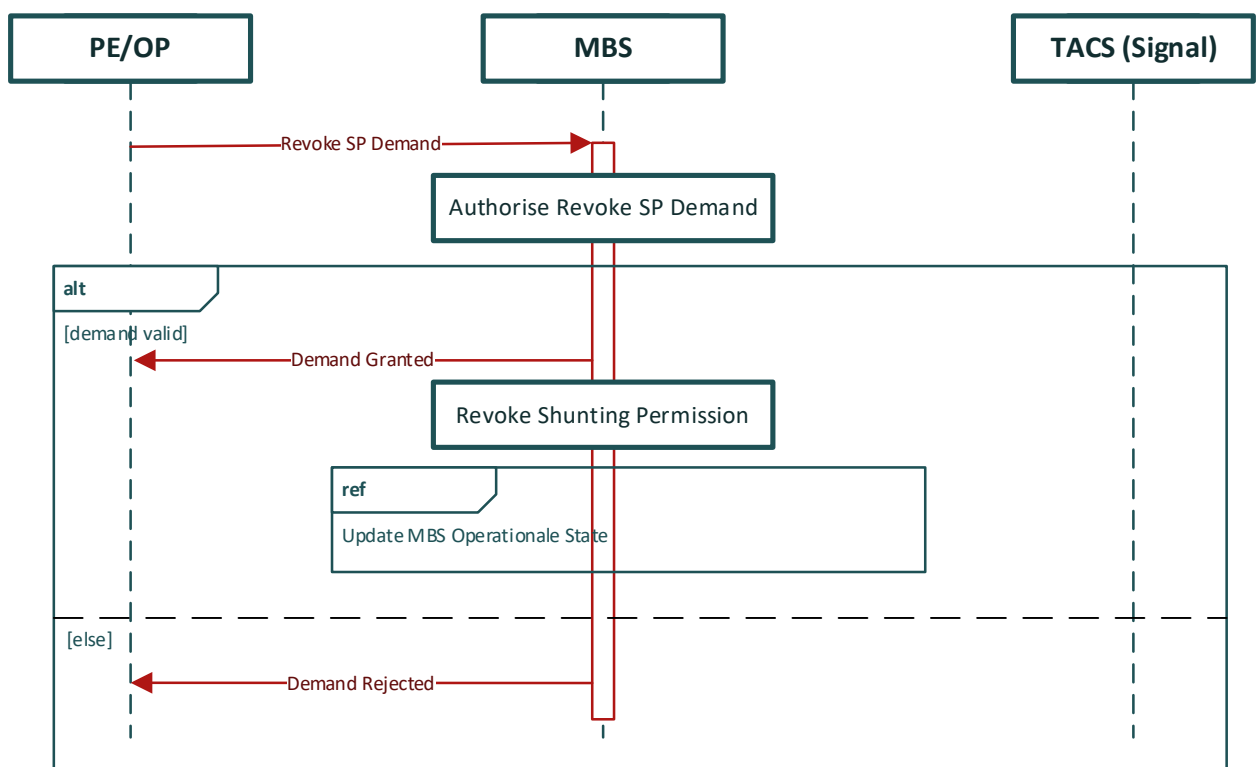


Figure 42 - Scenario : Revoke Shunting Permission

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 5.23
5.1 SysC: Start and Maintain MBS	6.32 SysF Supervise<Actor>Communication 6.33 SysF Establish<Actor>Communication
5.2 SysC: Preload Topology Data	6.11 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/OP	
5.6 SysC: Start communication with one TACS	
5.7 SysC: Respond to initiation of communication session by OBU	6.13 SysF Create Train Object
5.8 SysC: Control <i>Switchable Trackside Assets</i>	6.3 SysF Authorise TA State Request 6.4 SysF Translate TA State request to TACS command 6.5 SysF Send TACS command
5.9 SysC: Overwrite DPS State	6.6 SysF Authorise DPS Overwrite Demand 6.7 SysF Execute DPS Overwrite Demand
5.10 SysC: Revoke Overwrite DPS State	6.8 SysF Authorise Revoke DPS Overwrite Demand 6.9 SysF Execute Revoke DPS Overwrite Demand
5.11 SysC: Shutdown MBS	
5.12 SysC: Update <i>MBS Operational State</i>	6.10 SysF Update <i>Domain Object</i> state 6.12 SysF Assign a safe value to a <i>Domain Object</i> 6.14 SysF Localise Train

	6.15 SysF Manage Unresolved Trackbound Object 6.26 SysF Update Movement Permission
5.13 SysC: Report <i>MBS Operational State</i>	6.2 SysF Report <i>MBS Operational State</i>
5.14 SysC: Start of Train	6.14 SysF Localise Train
5.15 SysC: Provide Authorisation to Train	6.16 SysF Authorise MP Request 6.25 SysF Authorise Release Stop Train Request 6.18 SysF Translate MP Request to Movement Authority 6.19 SysF Translate MP Request to SR Authorisation
5.16 SysC: Terminate Train Mission	6.21 SysF Delete <i>Train Object</i>
5.17 SysC: Shorten MA cooperatively	6.17 Authorise Cooperative Shortening Request 6.20 SysF Translate Cooperative Shortening Request to Request to Shorten MA 6.26 SysF Update Movement Permission
5.18 SysC: Supervise Trains and Trackside Assets	6.22 SysF Supervise Trains and Trackside Assets
5.19 SysC: Revoke or restrict authorisation	6.23 SysF Revoke or restrict authorisation 6.24 SysF Authorise Stop Train Request 6.25 SysF Authorise Release Stop Train Request 6.26 SysF Update Movement Permission
5.20 SysC: Continue after Train Trip	
5.21 SysC: Recovering Degraded TTD Situations	6.27 SysF Check TTD Section Failure Status 6.28 SysF Reset TTD section by MBS 6.29 SysF Reset TTD section by Operator 6.30 SysF Supported Reset of TTD section by Operator 6.31 SysF Reset of TTD section by Operator using Sweeping
5.22 SysC: Manage Usage Restriction Area	6.34 SysF Authorise Create URA

	6.35 SysF Create URA 6.36 SysF Authorise Delete URA 6.37 SysF Delete URA
5.23 SysC: Authorise Shunting	6.38 Provide SH Confirmation Request 6.39 Authorise Shunting
5.24 SysC: Set Shunting Permission	6.40 SysF Authorise SP Request 6.41 SysF Update Shunting Signal 6.42 SysF Update Shunting Permission
5.25 SysC: Supervise Shunting Permission	6.45 SysF Set Shunting Signal to Stop 6.44 SysF Supervise Shunting Permission
5.26 SysC: Update Shunting Permission	6.42 SysF Update Shunting Permission 6.45 SysF Set Shunting Signal to Stop
5.27 SysC: Handle Emergency Stop for Shunting Signal	6.43 SysF Authorise Shunting Signal Stop Demand
5.28 SysC: Revoke Shunting Permission	6.46 SysF Authorise Revoke SP Demand 6.47 SysF Revoke Shunting Permission

6.1 GENERAL REQUIREMENTS

REQ-GENERAL-1

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

REQ-GENERAL-2

Whenever MBS has sent a Conditional Emergency Stop message and this emergency stop was accepted by the OBU or MBS has sent an Unconditional Emergency Stop message, the MBS shall revoke this emergency stop by sending a Revocation of Emergency Stop message to the OBU.

Rationale: The OBU won't accept any further Movement Authority issued by the MBS as long as the emergency stop has not been revoked yet.

Guidance: When revoking an emergency stop, the MBS has to consider that OBU will accept the Revocation of Emergency Stop message only in some modes (when certain conditions are fulfilled), see also chapter 4.8.4, Subset-026 in /ETCS/.

Additionally, the MBS has to consider that some mode transitions cause the deletion of an emergency stop on-board.

REQ-GENERAL-3

MBS shall provide the National Values as defined in the Domain Data for the AoC before or when a first authorisation is issued by the MBS.

Rationale: This is to avoid that the default National Values are applied on OBU, because these do not include the most restrictive national values, e.g. for M_NVCONTACT, T_NVCONTACT or V_NVSTFF.

Guidance: None

REQ-GENERAL-4

MBS shall provide the MA Request parameters and Position Report parameters to OBU as defined in the Domain Data.

Rationale: This is to ensure that the valid MA Request and Position Report parameters are on-board in-time.

Guidance: Actually, this is not a safety-related requirement and thus this may be also sent by an external system via MBS to the OBU. But this alternative is not considered as less complex than if MBS simply sends those packets by itself.

REQ-GENERAL_SYNTAX

If the syntax of a message received from the PE or the OP is not in accordance with the I_PE or I_OP interface, then the MBS shall send a “SYNTAX” reject code.

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

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

REQ-GENERAL_EXISTANCE

The MBS shall check that the element (e.g. a Train Object, a DPS or DPS Group) referenced in a message received from the PE or OP exists and if the check fails, the MBS shall send an “UNKNOWN_ELEMENT” reject code.

Rationale: The MBS must know the element to be able to process the message received from PE or OP.

Guidance: None

6.2 SysF Report *MBS OPERATIONAL STATE*

6.2.1 Overview

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

6.2.2 Inputs

- *MBS Domain Object*

6.2.3 Outputs

- *MBS Operational State report* according to I_PE and I_OP interfaces, respectively

6.2.4 Functional requirements

REQ-0001

When detecting a change to any 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 and to OP according to I_OP.

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

Guidance: None

6.3 SYSF AUTHORISE TA STATE REQUEST

6.3.1 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.

6.3.2 Input

- DPS Group Request according to I_PE
- DPS Group Request according to I_OP
- DPS Group Demand according to I_OP
- *MBS Operational State*

6.3.3 Outputs

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

6.3.4 Functional requirements

REQ-DPSG_PE_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-GENERAL_SYNTAX
2. REQ-GENERAL_EXISTANCE
3. REQ-SC_DPS_DPSG
4. REQ-SC_DPS_URA_LOCKED
5. REQ-SC_DPS_URA_SAFETY_CRITICAL
6. REQ-SC_DPS_URA_MANUAL_OPS_PE
7. DPSG_REACHABLE
8. REQ- SC_DPSG_CHANGE
9. REQ-SC_DPSG_STATE
10. REQ-SC_DPS_TO
11. REQ-SC_DPS_UTO
12. REQ-SC_DPS_MP
13. REQ-SC_DPS_RB
14. 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.

REQ-DPSG_OP_REQUEST_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_OP:

1. REQ-GENERAL_SYNTAX
2. REQ-GENERAL_EXISTANCE
3. REQ-SC_DPS_DPSG
4. REQ-SC_DPS_URA_LOCKED
5. REQ-SC_DPS_URA_SAFETY_CRITICAL
6. REQ-SC_DPS_URA_MANUAL_OPS_OP

7. REQ- SC_DPSG_CHANGE

8. REQ-SC_DPSG_STATE

9. REQ-SC_DPS_TO

10.REQ-SC_DPS_UTO

11.REQ-SC_DPS_MP

12.REQ-SC_DPS_RB

13.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.

REQ-DPSG_OP_DEMAND_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 Demand through I_OP:

1. REQ-GENERAL_SYNTAX
2. REQ-GENERAL_EXISTANCE
3. REQ-SC_DPS_DPSG
4. REQ-SC_DPS_URA_LOCKED
5. REQ-SC_DPS_URA_SAFETY_CRITICAL
6. REQ-SC_DPS_URA_MANUAL_OPS_OP
7. REQ- SC_DPSG_CHANGE
8. REQ-SC_DPSG_STATE
9. REQ-SC_DPS_TO
- 10.REQ-SC_DPS_UTO
- 11.REQ-SC_DPS_MP
- 12.REQ-SC_DPS_RB
- 13.REQ-SC_DPS_RP

unless the specific safety check is marked to be ignored in the request and is within the following list:

- REQ-SC_DPS_URA_SAFETY_CRITICAL
- REQ-SC_DPS_TO

- REQ-SC_DPS_UTO

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 only cause hazards accepted by the infrastructure manager and its operators.

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

REQ-DPSG_PE_ABORT

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

REQ-DPSG_OP_ABORT

The MBS shall abort checking a DPS Group Request or DPS Group Demand received through I_OP 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

REQ-SC_DPS_DPSG

MBS shall check that every DPS referenced in the DPS Group Request or Demand 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.

REQ-SC_DPSG_REACHABLE

MBS shall check that the TACS associated with the DPS Group referenced in the DPS Group Request or Demand 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.

REQ-SC_DPS_URA_LOCKED

MBS shall check that if a DPS in the DPS Group Request or Demand overlaps an URA, the URA shall not have the restriction property *nonSwitchable* and if the check fails, MBS shall send a “DPS_URA_CONFLICT” reject code.

Rationale: A DPS Group locked into that position by an URA, shall not be moved in any case.



Guidance: None

REQ-SC_DPS_URA_SAFETY_CRITICAL

MBS shall check that if a DPS in the DPS Group Request or Demand overlaps an URA, the URA shall not have the restriction property *safetyCritical* and if the check fails, MBS shall send a “DPS_URA_CONFLICT” reject code.

Rationale: A traileed point shall only be moved with explicit confirmation by the operator.



Guidance: None

REQ-SC_DPS_URA_MANUAL_OPS_PE

MBS shall check that if a DPS in the DPS Group Request overlaps an URA, the URA shall not have the restriction property *manualOperation* and if the check fails, MBS shall send a “DPS_URA_CONFLICT” reject code.

Rationale: If the DPS Group is exclusively under the control of I_OP, PE shall not be able to change the state of TA (DPS).



Guidance: This check only applies to requests received through I_PE

REQ-SC_DPS_URA_MANUAL_OPS_OP

MBS shall check that all DPS in the DPS Group Request or Demand overlap an URA with the restriction property *manualOperation* and if the check fails, MBS shall send a “DPS_URA_CONFLICT” reject code.

Rationale: If the DPS Group is exclusively under the control of I_PE (no URA with restriction property *manualOperation* being present), the Operator Panel shall not be able to request commands.



Guidance: This check only applies to requests received through I_OP. Consequently, the request may be permissible if exchanged through the I_PE interface instead.

REQ- SC_DPSG_CHANGE

MBS shall check that the DPS states in the DPS Group Request or Demand 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

REQ-SC_DPSG_STATE

MBS shall check that the combination of requested drivability states for each DPS referenced in the DPS Group Request or Demand 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/

REQ-SC_DPS_TO

MBS shall check that no DPS of the DPS Group referenced in the DPS Group Request or Demand 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:



REQ-SC_DPS_UTO

MBS shall check that no DPS of the DPS Group referenced in the DPS Group Request or Demand 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:



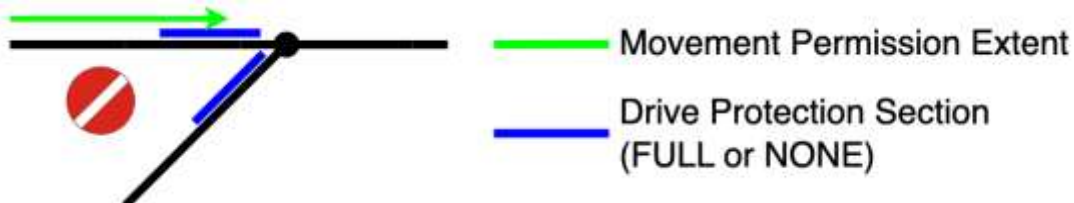
REQ-SC_DPS_MP

MBS shall check that no DPS of the DPS Group referenced in the DPS Group Request or Demand 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.



REQ-SC_DPS_RB

MBS shall check that no DPS of the DPS Group referenced in the DPS Group Request or Demand 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:



REQ-SC_DPS_RP

MBS shall check that no Risk Path is terminated at a DPS of the DPS Group referenced in the DPS Group Request or Demand 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.

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.

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.

6.4 SYSF TRANSLATE TA STATE REQUEST TO TACS COMMAND

6.4.1 Overview

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

6.4.2 Inputs

Requested state of the *Switchable TA*.

6.4.3 Outputs

TACS command according to I_TACS

6.4.4 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

6.5 SysF SEND TACS COMMAND

6.5.1 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.

6.5.2 Inputs

TACS command.

6.5.3 Outputs

See I_TACS.

6.5.4 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/

6.6 SysF AUTHORISE DPS OVERWRITE DEMAND

6.6.1 Overview

This function executes a series of safety checks on the received DPS Overwrite Demand.

In cases where a point is technically not supervised mechanically locked in one position and reported driveable by a maintainer, MBS shall allow movements over this point.

6.6.2 Input

- Dps Overwrite Demand according to I_OP
- *MBS Operational State*

6.6.3 Outputs

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

REQ-DPSOD_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 Overwrite Demand through I_OP:

1. REQ-DPS_OD_ABORT
2. REQ-GENERAL_SYNTAX
3. REQ-GENERAL_EXISTANCE
4. REQ-SC_DPSOD_URA

Rationale: The purpose of these checks is to ensure that the requested overwrite of the DPS Group will only cause hazards accepted by the infrastructure manager and its operator.

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

REQ-DPSOD_ABORT

The MBS shall abort checking a DPS Overwrite Demand received through I_OP if any performed safety check failed.

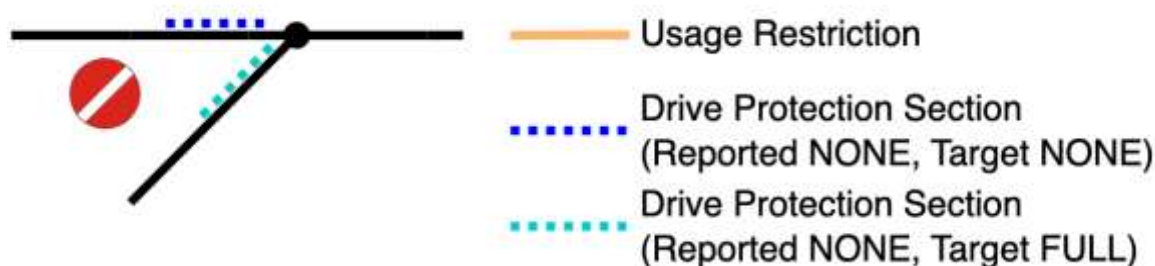
Rationale: If a check for example discovers a message syntax error, further checks might lead to illegal function calls within MBS.

Guidance: None

REQ-SC_DPSOD_URA

MBS shall check that all DPS referenced in the DPS Overwrite Demand are overlapped with a URA with the restriction property *nonSwitchable* and if the check fails, MBS shall send a “DPSOD_NOT_LOCKED” reject code.

Rationale: The state of a DPS Group must not change while its state is overwritten.



Guidance: None.

6.7 SysF EXECUTE DPS OVERWRITE DEMAND

6.7.1 Overview

After a DPS Overwrite Demand is granted, the internal state must be adapted to reflect the change.

6.7.2 Inputs

- *Requested Overwrite*
- *MBS Operational State*

6.7.3 Outputs

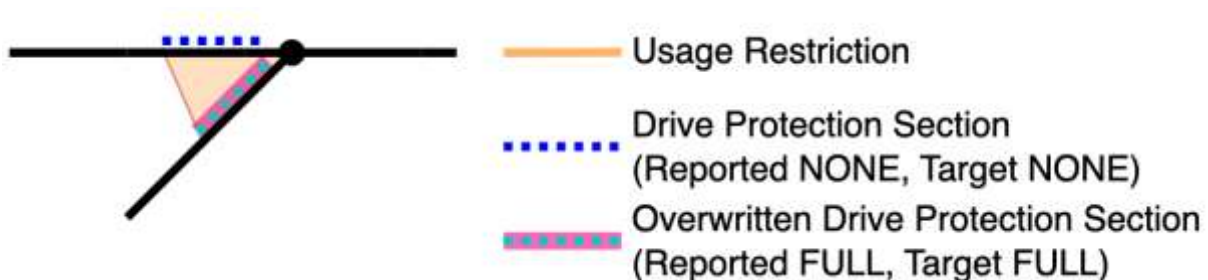
- *MBS Operational State*

6.7.4 Functional requirements

REQ-DPSOD_Overwrite

If the DPS Overwrite Demand has been authorised, MBS shall overwrite the current DPS state by the target state ignoring any state reported by the *Switchable Trackside Asset*.

Rationale:



Guidance: The MBS must keep the state overwritten as long as the overwrite is not revoked. This flag must not be persistent over a system failure or restart.

6.8 SysF AUTHORISE REVOKE DPS OVERWRITE DEMAND

6.8.1 Overview

This function executes a series of safety checks on the received Revoke DPS Overwrite Demand.

When an overwritten Switchable Trackside Asset is brought back into operation, the overwrite of its position shall be reverted.

6.8.2 Input

- Revoke DPS Overwrite Demand according to I_OP
- *MBS Operational State*

6.8.3 Outputs

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

REQ-DPSUD_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 Revoke DPS Overwrite Demand through I_OP:

1. REQ-DPSOD_ABORT
2. REQ-GENERAL_SYNTAX
3. REQ-GENERAL_EXISTANCE

Rationale: The purpose of these checks is to ensure that the Revoke DPS Overwrite Demand will only cause hazards accepted by the infrastructure manager and the operator.

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

REQ-DPSOD_ABORT

The MBS shall abort checking a Revoke DPS Overwrite Demand received through I_OP 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

6.9 SYSF EXECUTE REVOKE DPS OVERWRITE DEMAND

6.9.1 Overview

After a Revoke DPS Overwrite Demand is granted, the internal state must be adapted to reflect the change.

6.9.2 Inputs

- *Requested Overwrite*
- *MBS Operational State*

6.9.3 Outputs

- *MBS Operational State*

6.9.4 Functional requirements

REQ-DPSOD_RevokeOverwrite-1

If the Revoke DPS Overwrite Demand has been authorised and no command is in progress (dpsGroupState is not PROCESSING), MBS shall update the DPS state according to the Reported State Trackside Asset (memorised according to requirement REQ-0011).

Rationale:

As REQ-0062 and REQ-0035 are still performed when an DPS Overwrite is in progress, the DpsGroupState could have been set to READY (i.e. the TA State request command is no more in progress) during the Overwrite process.

Guidance:



REQ-DPSOD_RevokeOverwrite-2

If the Revoke DPS Overwrite Demand has been authorised and a TA State Request command is in progress (dpsGroupState is PROCESSING), MBS shall set the state for all associated DPS to NONE.

Rationale:

If the TA State request command is still in progress when the Overwrite process is finished, all reported DPS states must be set to NONE as this is the safe state.

Guidance:



6.10 SysF UPDATE *DOMAIN OBJECT* STATE

6.10.1 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*.

6.10.2 Input

- TACS report
- OBUCommLost, *OBUCommEstablished*

6.10.3 Output

- *Domain Object* state

6.10.4 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 and communication closed with the TACS.

Rationale: To be able to operate a TA. If a message is discarded, the communication is closed with the TACS to raise an alarm and change the TACS state to a safe value.

Guidance: None

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

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

REQ-0061

When a TACS report for a Switchable TA is received, no command is in progress (dpsGroupState is not PROCESSING) and no DPS Overwrite is in progress, 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

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

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

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

REQ-0044

When the MBS receives an MA Request message from the OBU, then the MBS shall update the *MBS Operational State* indicating the reason for this MA request (e.g. driver has pressed the start button)

Rationale:

This is necessary to indicate the reason behind the request, e.g. that the driver has pressed the start button or the time before reaching the perturbation location is reached.

Based on this information, PE may decide to send a Movement Permission to the MBS.

Guidance: None

REQ-AmbigPR-1

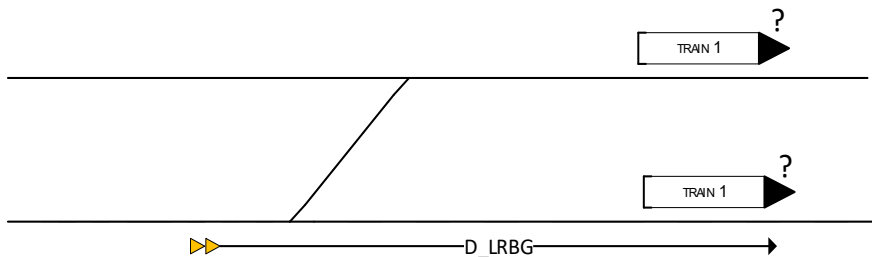
When receiving a SoM Position Report from an OBU where the status of the position is set to valid but which the MBS considers ambiguous, the MBS shall set the position qualifier in the Train Object related to this OBU to “ambiguous”.

Rationale: This is to inform the Signaller that there is a train that has started with a position which is ambiguous to the MBS.

Guidance:

This could happen if there is one or more points between the LRBG and the possible location of the front end of the train. The status of the position is part of the SoM Position Report parameters.

In the following example, if it is not possible for MBS to determine if the train is on the track up or down, the position qualifier is set to ambiguous even if the status of the position is set to valid inside the SoM Position Report message.



REQ-AmbigPR-2

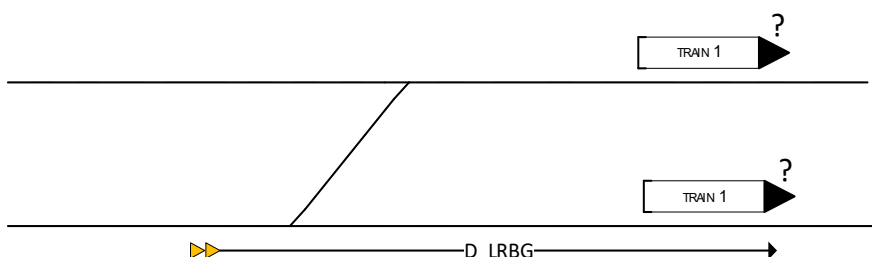
When receiving a Position Report from an OBU with a position which the MBS cannot locate unambiguously in the track, then the MBS shall set the position qualifier in the Train Object related to this OBU to “ambiguous”.

Rationale: This is to inform the Signaller that there is a train with an ambiguous position, also after the SoM Position Report.

Guidance:

This could happen if there is one or more points between the LRBG and the possible location of the front end of the train.

In the following example, if it is not possible for MBS to determine if the train is on the track up or down, the position qualifier is set to ambiguous.



Note: if the train was in a supervised mode with a received Movement Authorisation, the Movement Permission extent could have been used to solve the ambiguity.

REQ-Unknown-BG

When receiving a Position Report from an OBU in which the LRBG is not known to the MBS, then the MBS shall set the position qualifier in the Train Object related to this OBU to “unknown”.

Rationale: This is to inform the Signaller that there is a train with an unknown position.

Guidance: This could happen with a train approaching the border to the MBS Area, or a train that has been moved cold into the MBS Area.

6.11 SYSF PRELOAD TOPOLOGY DATA

6.11.1 Overview

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

6.11.2 Input

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

6.11.3 Output

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

6.11.4 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.

REQ-0017

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

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.

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

6.12 SysF ASSIGN A SAFE VALUE TO A DOMAIN OBJECT

6.12.1 Overview

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

6.12.2 Inputs

- *Domain Object*

6.12.3 Outputs

- *Domain Object State*

6.12.4 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.

REQ-SV_COMMLOSS

When *MBS* receives the event *TACSCommLost(TACSIId)*, it shall assign a safe value to the related *Domain Object*.

Rationale: Cf. REQ-0020

Guidance: Cf. REQ-0020

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.

6.13 SysF CREATE TRAIN OBJECT

6.13.1 Overview

When *MBS* has successfully established a communication session with an *OB*, then a *Train Object* for this *OB* 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.

6.13.2 Inputs

Successfully established communication session between *MBS* and an *OB*

6.13.3 Outputs

Train Object

6.13.4 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

REQ-0095

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 Position Report information
4. *Train Location* (when determined)
5. Time when the stored information was last valid
6. Train Running Number
7. Train Integrity status
8. Connection status
9. Position qualifier

Rationale:

This ensures that MBS has an up-to-date image of all train-related information. Most recent Position Report information is used to e.g. store detailed position information (e.g. mSFE) and to evaluate the status of the reported position.

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. The information about the most recent Position Report includes a parameter about the status of the position, similar to that in the SoM Position Report, which can be used to indicate if the MBS considers the position as ambiguous and thereby alert about the need to locate a train (e.g. at Start of Mission), or if a train has been given an assumed position by a signaller.

The position qualifier for a *Train Object* can be either *known*, *unknown*, *ambiguous* or *assumed*. This depends on the position reported at Start of Mission or during a mission and if the Signaller has provided an *assumed* position for a train that the MBS cannot locate itself.

The transitions between the states of the position qualifier defined by requirements as seen in the table below. Requirements being fulfilled below a state lead to a transition to the state in the same row to the right of that requirement and requirements fulfilled above a state lead to a transition to the state to the left of that requirement.

Unknown (default) REQ-Default-Pos	< REQ-Unknown-BG	< REQ-Unknown-BG	< REQ-Unknown-BG < REQ-OP-Delete-Pos
REQ-Known-Pos >	Known	< REQ-Known-Pos	< REQ-Known-Pos
REQ-AmbigPR-1 > REQ-AmbigPR-2 >	REQ-AmbigPR-2 >	Ambiguous	< REQ-AmbigPR-2
REQ-Assumed-Pos >	N/A	REQ-Assumed-Pos >	Assumed

6.14 SysF LOCALISE TRAIN

6.14.1 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 Position Reports, Validated Train Data and other inputs if available, e.g. TTD sections. If the MBS is not able to locate a communicating train itself, it can receive an assumed position from the *Operators Panel*. From this assumed position, the MBS can derive an assumed *Train Location*, which the MBS can use until the train has reported a position that is unambiguous to the MBS.

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 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 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 43.

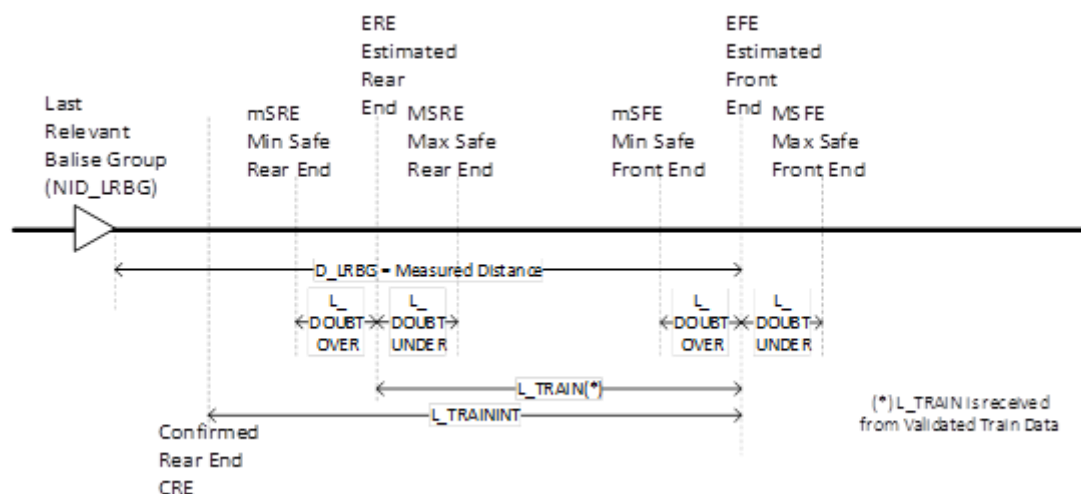


Figure 43: Terms used for Train Location

NB. The terms in the figure above does not apply for a train with an assumed *Train Location*, which is created based on the assumed position received from OP together with the reported *Train Length*.

There are several reasons to create or move a *Train Location*, as shown in the following table. This table also describes the sequence in which the requirements are executed (see REQ-0063).

Create-move <i>Train Location</i> Reasons	Notes	Requirements
Train SoM position report received	<i>Train location</i> created from min Safe Front End to max Safe Front End (before having received train data)	REQ-TrainLoc-4
First Position Report	For example, PR without SoM process	REQ-TrainLoc-5
Update front by Train Max SFE	Front of the <i>Train Location</i> is updated using Max Safe Front End derived from the Position Report	REQ-TrainLoc-7
Update rear by Train CRE	Rear of the <i>Train Location</i> is updated using the Confirmed Rear End derived from the Position Report	REQ-TrainLoc-8
Update rear with new value of Train Length	Rear of the <i>Train Location</i> is updated using the new value of Train Length	REQ-TrainLoc-6
Update front by clear TTD	Front of the <i>Train Location</i> is shortened using clear TTD section	REQ-TTD-2
Update rear by clear TTD	Rear of the <i>Train Location</i> is moved using clear TTD	REQ-TTD-3
Update rear by clear TTD	Rear updated by expected TTD clearance in accordance with the Movement Permission	REQ-TTD-6
Update front to the passed TTD limit	Update front of the <i>Train Location</i> when the passing of a TTD limit is detected	REQ-TTD-14

Update front by occupied TTD for mute train	Update front of the <i>Train Location</i> when a train becomes mute	REQ-TTD-15
Update front by occupied TTD for mute train	Update front of the <i>Train Location</i> when a TTD becomes occupied for a mute train	REQ-TTD-5
Update rear or front end to maintain the length of the train	Ensure that the length of the updated Train Location is not shorter than the length of the train	REQ-TTD-4
Sweeping Train Location by chasing train front	Remove the part of Train Location from the previous min Safe Front End up to the new min Safe Front End of the chasing train	REQ-TrackStatus-17
Receiving an assumed position	A request is received from the Operator Panel to locate the front of a train at the indicated position	REQ-OP-Assume-Pos
Update the front of an assumed Train Location	A train with an assumed Train Location is given an SR Authorisation or a TTD section within its Movement Permission becomes occupied.	REQ-SR-Extend-Assumed-Loc, REQ-TTD-16

Table 18 – Reasons to create or move *Train Location*

There is one reason to delete a *Train Location*, as shown in Table 19:

Delete <i>Train Location</i> Reasons	Notes	Requirements
Train is no longer in communication with MBS	MBS considers that a train is no longer in communication	REQ-TrainLoc-10 REQ-TrainLoc-18
Request to delete an assumed Train Location	A request is received from the Operator Panel to delete the assumed location for a train	REQ-OP-Delete-Pos
Train reports an LRBG which is unknown to the MBS	MBS cannot locate the train in its supervised area	REQ-Delete-Assumed-Location

Table 19 – Reasons to delete *Train Location*

For a system using TTD, the MBS is designed to manage the lack of synchronicity between TTD section status and Position Reports for a communicating train. 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 can correlate these events.

The MBS is designed to allow for:

- The passing of a TTD limit (detected by TDP or occupancy of the TTD) by a train before the train has reported a position within the TTD section i.e. train front is moved to the beginning of the occupied section in this case (see REQ-TTD-14).
- A train reporting a position within the TTD section before the passing of the TTD section becomes Occupied i.e. train front is updated according to the Min Safe Front End and Max Safe Front End derived from the Position Report, and according to the free TTD limit (see REQ-TrainLoc-7 and REQ-TTD-2).

- 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 i.e. train rear is moved to the end of the cleared TTD and train front is moved accordingly (see REQ-TTD-6 and REQ-TTD-4).
- A train reporting a position clear of the TTD section before the TTD section becomes Clear i.e. train rear is moved using the Confirmed Rear End derived from the Position Report (see REQ-TrainLoc-8).

6.14.2 Inputs

- *Position Reports*
- *Validated Train Data*
- *Domain Data*
- *TTD section status (Domain Object state)*
- *Assumed Train Position* (from OP: a reference position, its direction, an offset (optional) and whether the front of the associated train is in the same or the opposite direction)

6.14.3 Outputs

- *Train Location*

6.14.4 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 18.

Rationale: This is to ensure the correctness of the Train Location.

Guidance: 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.

REQ-Default-Position

When creating a *Train Object*, the MBS shall set the position qualifier for this *Train Object* to *unknown*.

Rationale: This is the default state of a train's position.

Guidance: The position qualifier can change when the train reports a position.

REQ-Known-Pos

The MBS shall set the position qualifier for a *Train Object* to *known* when receiving a Position Report from the associated train with a position which is unambiguous to the MBS and not reported as invalid in a SoM Position Report.

Rationale: This is to update the status of a train's position.

Guidance: This applies to any Position Report, also at Start of Mission but not if reported as invalid.

REQ-Assumed-Pos

When creating an assumed *Train Location* for a *Train Object*, the MBS shall set the position qualifier for this *Train Object* to *assumed*.

Rationale: This is to update the status of a train's position when positioned from the OP.

Guidance: None.

6.14.5 Requirements to create a *Train Location*

REQ-TrainLoc-4

When receiving a Start of Mission 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 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 the figure below.

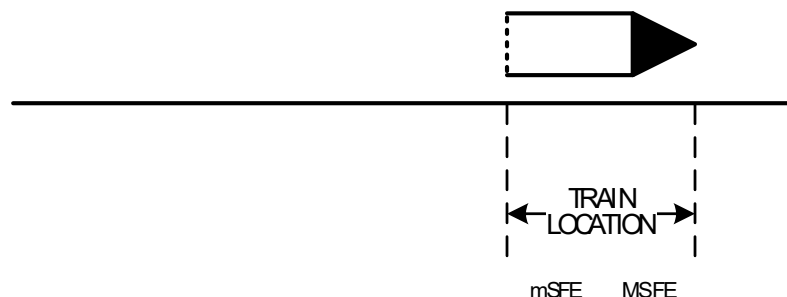


Figure 44: Train Location from Start of Mission Position Report

In the figure above, the location of the Train Object is shown with train length still unknown and with Train Integrity not confirmed. Train integrity cannot be confirmed until Validated Train Data has been acknowledged by the MBS.

There are other requirements covering the situations when the reported location is invalid or unknown, or is valid but ambiguous to the MBS.

REQ-TrainLoc-5

When receiving a Position Report, the MBS shall create a *Train Location* for the *Train Object* from the Min Safe Front End (or Min Safe Rear End if L_TRAIN is already available) to the Max Safe Front End derived from the Position Report if the following conditions are fulfilled:

- 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
- the mode of this OBU 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.

REQ-OP-Check-Pos1

The MBS shall check that the train indicated in a Request for Assumed Train Position from OP has no *Train Location* and if it has then the MBS shall reject this request and reply with the reject code "TRAIN_ALREADY_LOCATED".

Rationale: This is to check that the train in the OP request has no *Train Location*.

Guidance: If an assumed *Train Location* needs to be modified, it must first be deleted.

REQ-OP-Check-Pos2

The MBS shall check that at the position indicated in a Request for Assumed Train Position from OP there is at least one UTO and if there is none then the MBS shall reject this request and reply with the reject code "NO_UTO_AT_ASSUMED_POS".

Rationale: This is to check that there is a train at the indicated position.

Guidance: There must be a UTO at the indicated position, else there cannot be a train.

REQ-OP-Assume-Pos

If there is at least one UTO at the position indicated in a Request for Assumed Train Position from OP for a train without a *Train Location*, then the MBS shall create an assumed *Train Location* starting at the position indicated in the request and extending this in the opposite direction to that provided in the request for the known length of the train (L_TRAIN) or the train length stored for the UTO(s) at this location until the length is known.

Rationale: This is to create an assumed *Train Location* from the OP request.

Guidance: The assumed position can be given with an offset from a reference location.

The length of the train is either already known when the MBS is requested to position the train or updated by another requirement when it becomes known.

6.14.6 Requirements to update a *Train Location*

REQ-TrainLoc-7

When receiving a 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 Position Report

Rationale:

The MBS uses the information in 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 45 shows how the front of the *Train Location* is updated with a new Position Report.

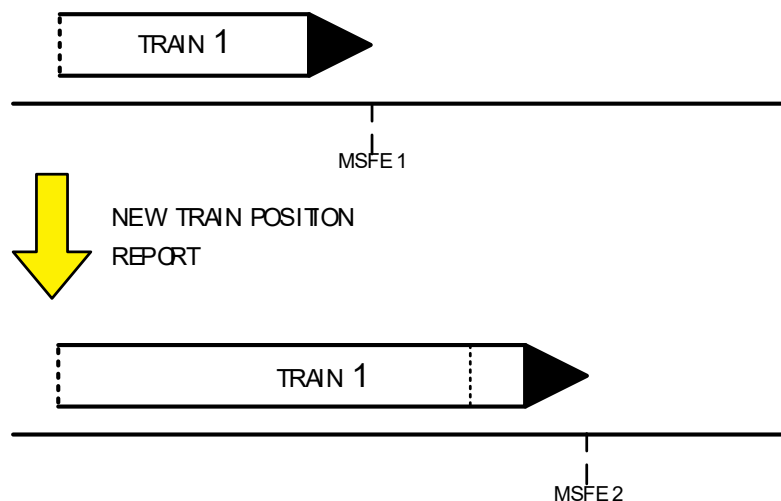


Figure 45: Front of Train Location updated from new Position Report

REQ-TrainLoc-8

When receiving a 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, SR 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 Position Report.

Rationale:

The MBS uses the information in 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 Position Report with the Train Integrity confirmed. From this, the MBS can locate the confirmed rear end of the train.

Figure 46 shows how the CRE is updated with a new Position Report with Train Integrity Confirmed.

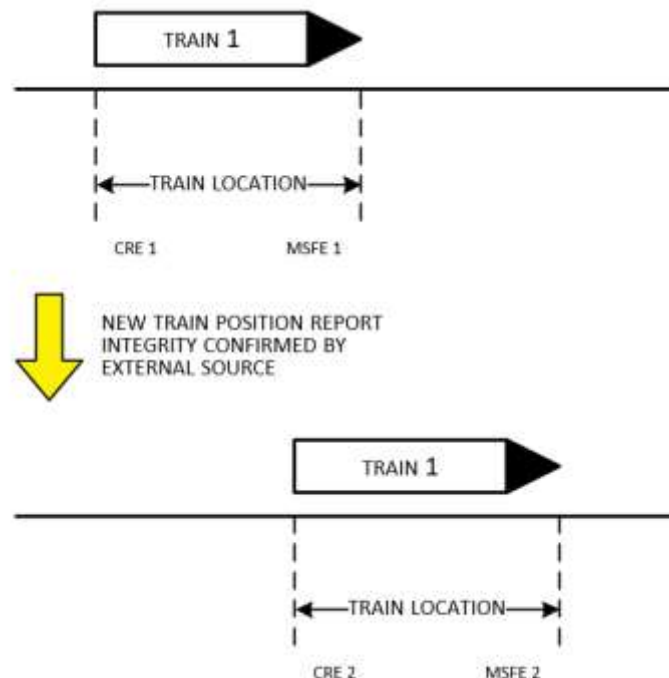


Figure 46: Rear of Train Location updated from new Position Report, Integrity Confirmed

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

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 47.

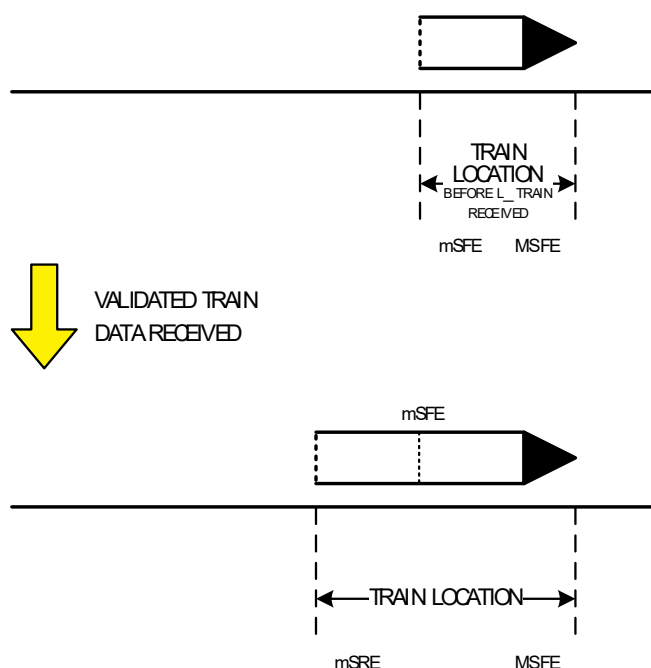


Figure 47: Train Location when receiving Validated Train Data during Start of Mission

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 48. In this case, a UTO is also created according to requirement REQ-TrackStatus-25 to manage the missing part.

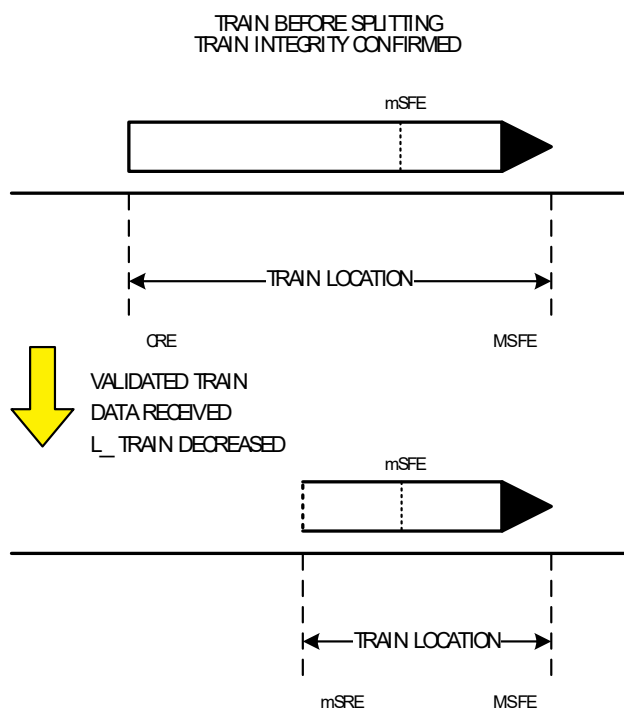


Figure 48: Train Location when receiving Validated Train Data, L_TRAIN decreased

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 49.

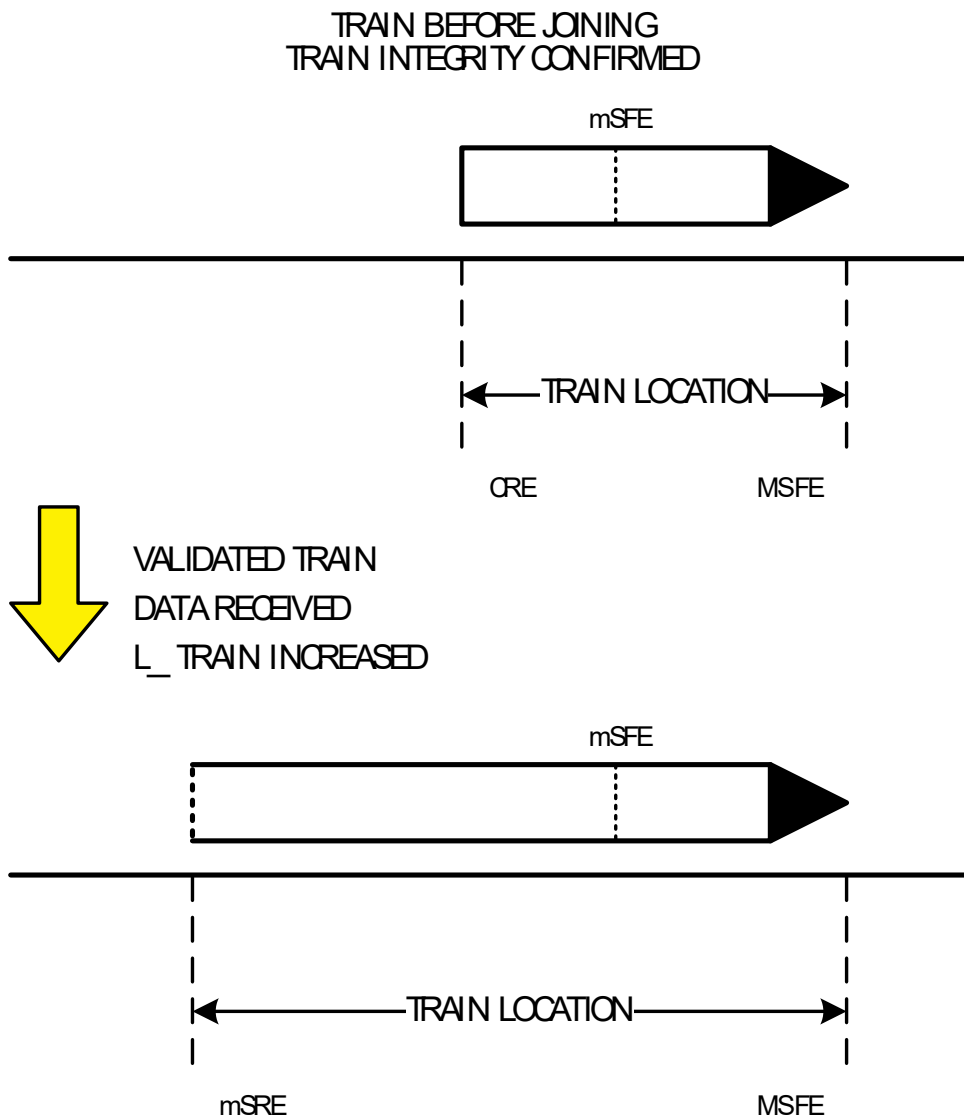


Figure 49: Train Location when receiving Validated Train Data, L_TRAIN increased

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

REQ-TrackStatus-17

When the front of a chasing train has passed a part a *Train Location* of a chased Train, then the MBS shall reduce that *Train Location* for the part of it from the previous min Safe Front End up to the new min Safe Front End of the chasing 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 61 shows the sweeping by *Train Location* for a train with Train Integrity confirmed in a *Train Location* ahead of the train.

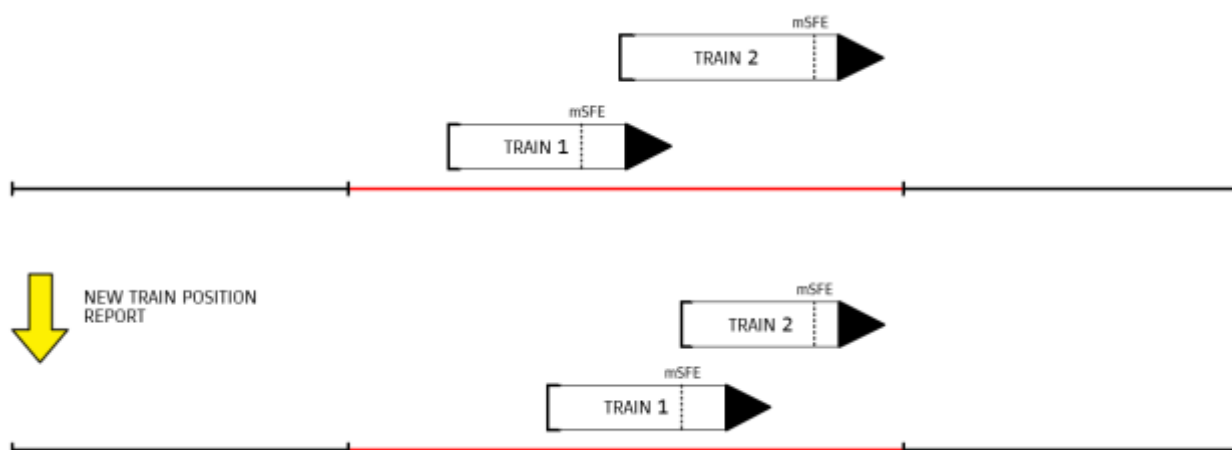


Figure 50: Train with Train Integrity confirmed Sweeping the Train Location of a chased Train with integrity not confirmed

REQ-SR-Extend-Assumed-Loc

When giving an SR authorisation to a train having an assumed *Train Location*, then the MBS shall extend the assumed *Train Location* of this train up to the closest of:

- the end of the Movement Permission's *Risk Buffer*, OR
- the next boundary of the first free TTD section in advance of the *Train Location*.

Rationale: This is to indicate where the train could be after authorised to move in SR.

Guidance: An assumed *Train Location* is affected by the given Movement Permission and information from the TTD sections within the Movement Permission. It can also be extended when an adjacent TTD section at its front end becomes occupied.

6.14.7 Impact from TTD on *Train Locations*

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 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 51:

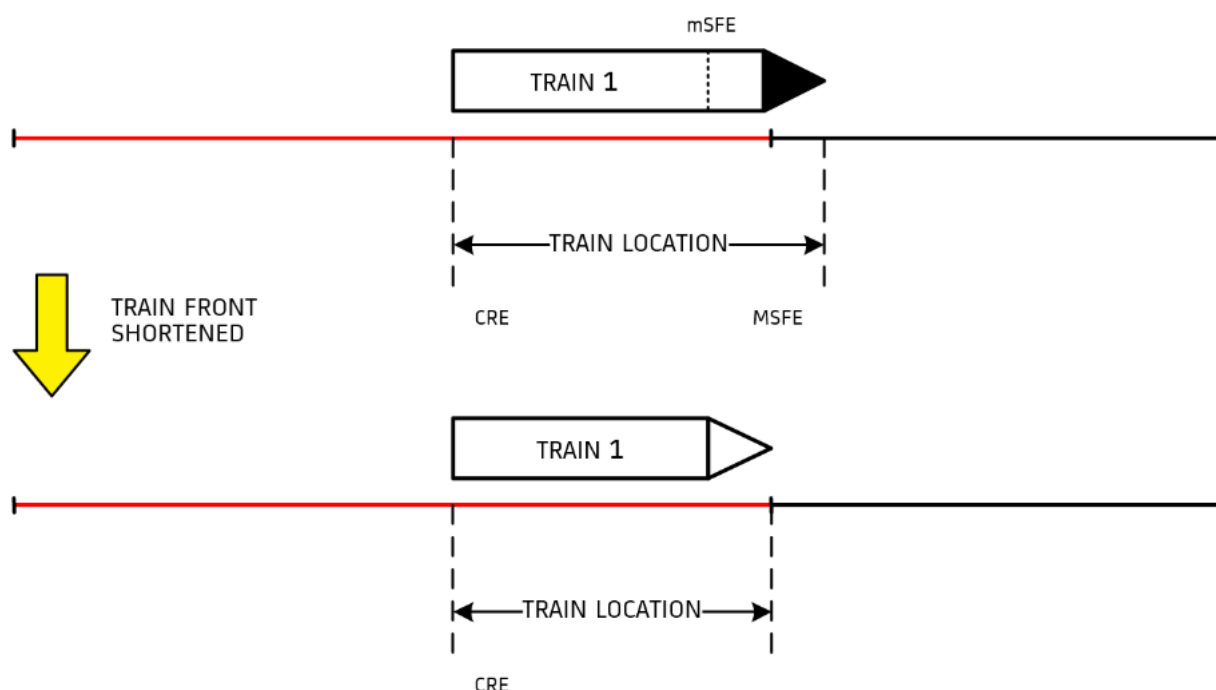


Figure 51: Shortening of front of Train Location due to clear TTD

Figure 52 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:

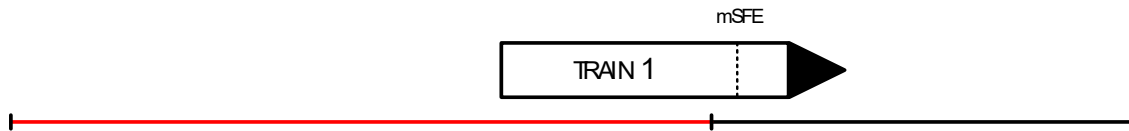


Figure 52: No shortening of front of Train Location due to clear TTD

This requirement is mainly used for a train at standstill with a large odometry error to avoid blocking a point in front of the train when the TTD is free.

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 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 53:

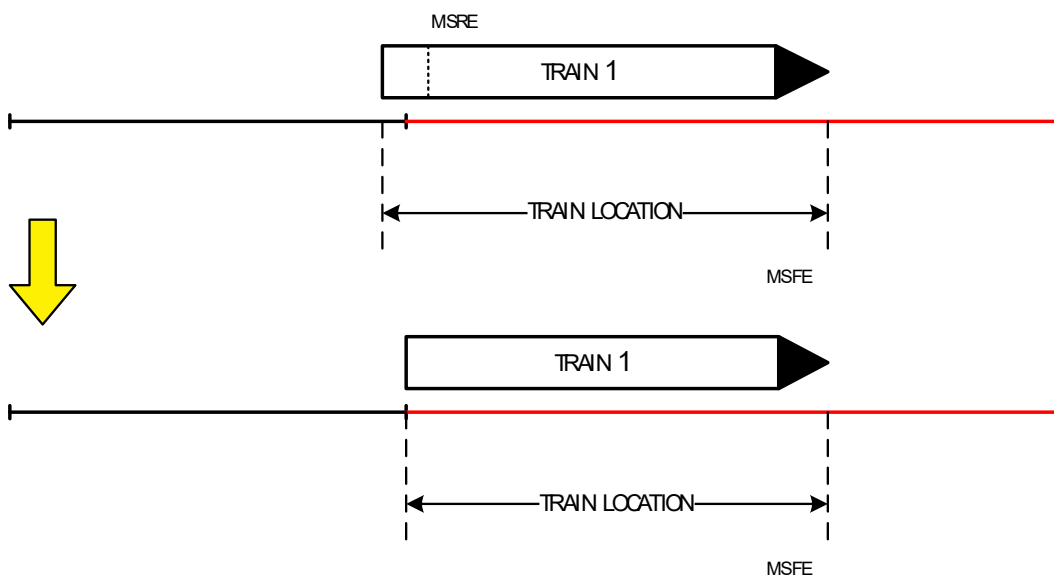


Figure 53: Shortening of rear of Train Location due to clear TTD

Figure 54 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:

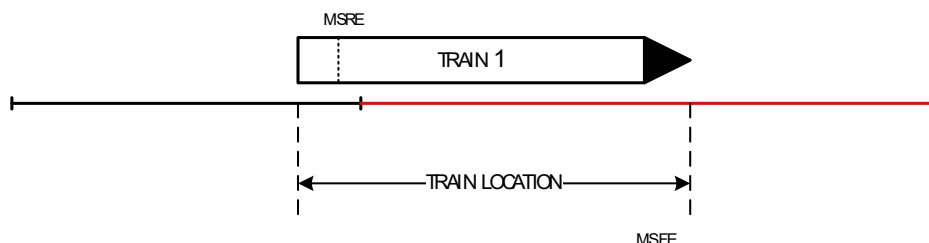


Figure 54: No shortening of rear of Train Location due to clear TTD

REQ-TTD-4

[X2R5 REQ-TTD-4]

For a system using TTD, when using mechanisms 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 move the front and rear.

Example: when train rear is moved according to REQ-TTD-6 or REQ-TrackStatus-17, train front can be moved accordingly.

REQ-TTD-14

For a system using TTD, when detecting an expected train movement passing a TTD limit the MBS shall move the front end of the Train Location forward to the passed TTD limit.

Rationale:

The MBS can use TTD information to extend the *Train Location* of a train that is moving along the railway within the Movement Permission allocated to it

Guidance:

A train can move forward within the Movement Permission allocated to that train and pass a TTD limit. The MBS can adjust the knowledge about where the train might be by extending the *Train Location* of this train.

The passing of a TTD limit can be detected by:

- Train Detection Point (TDP) function, this is the preferred solution for detecting the passing of a TTD limit as it can be detected even between 2 adjacent TTD sections that are already occupied.
- The occupancy of the next TTD.

Figure 57 shows how the *Train Location* is extended within an existing Movement Permission when a train proceeds into a previously clear TTD.

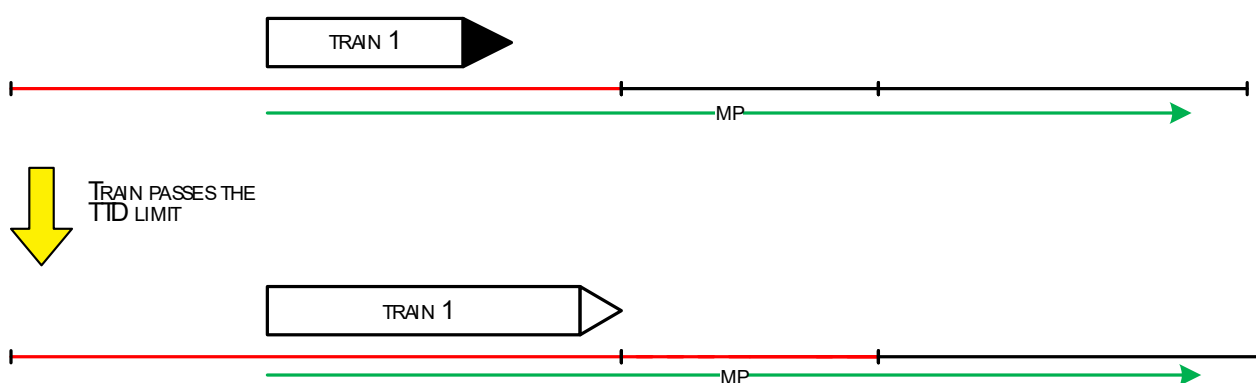


Figure 55 Extension of Train Location when train passes TTD limit

Implementation of such a function is project-specific and will likely require the use of timers to compensate for the latency between the Position Reports and TTD inputs.

Note: if the passing of a TTD limit is considered as unexpected, a UTO is created/extended according to REQ-TTD-9/REQ-TTD-10.

REQ-TTD-6

For a system using TTD, when detecting an expected TTD clearance in accordance with the Movement Permission allocated to a train, the MBS shall move the rear end of the Train Location forward to the end of the cleared TTD.

Rationale:

The MBS can use TTD clearance to move the *Train Location* rear of a train, equivalent to a route release mechanism.

Guidance:

A train can move forward within the Movement Permission allocated to that train and free a previously occupied TTD. That occupation can be attributed to a normal train movement. The MBS can adjust the knowledge about where the train might be by moving the *Train Location* of this train.

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

Figure 57 shows how the *Train Location* is moved within an existing Movement Permission when a train passes a TTD border and when the TTD clearance is received before Position Report. Note that the front of the train location may also be moved in this case in accordance with requirement TTD-4.

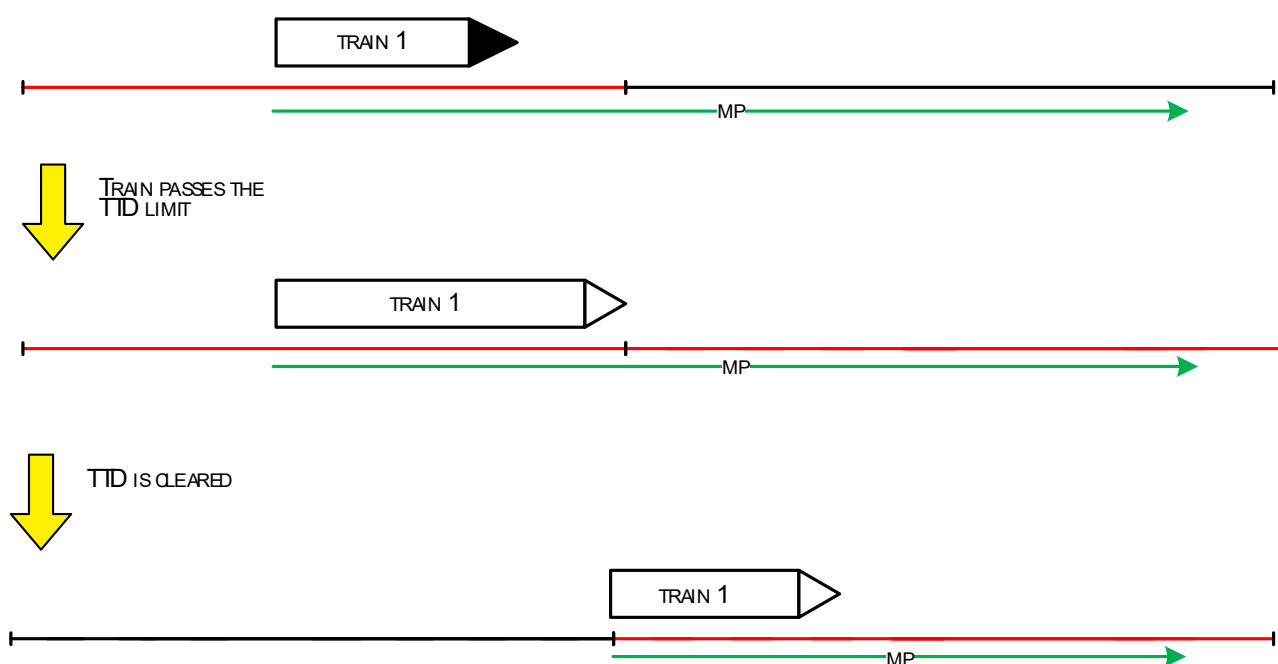


Figure 56 Moving of Train Location by Cleared TTD

REQ-0037

[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.

Guidance:

This is an optional functionality to be defined at application level based on the needs of the system.

REQ-0038

[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.

REQ-TTD-15

For a system using TTD, when Mute Timer expires, 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 the first free TTD section in advance of the current *Train Location*

Rationale:

When the train becomes mute, the front of the train is moved to its furthest possible location to give the information (to operator) that the train could be anywhere along the Movement Permission considering TTD information.

Guidance:

See REQ-TTD-5

REQ-TTD-5

[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 boundary of the next free TTD section

Rationale:

When the train is mute, the front of the train is moved to its furthest possible location to give the information (to operator) that the train could be anywhere along the Movement Permission considering TTD information.

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 57 shows how the *Train Location* is extended to the boundary of the first free TTD section when its Mute Timer expires and subsequently how it is extended within its existing Movement Permission when the train proceeds into a previously clear TTD section after a loss of communication.

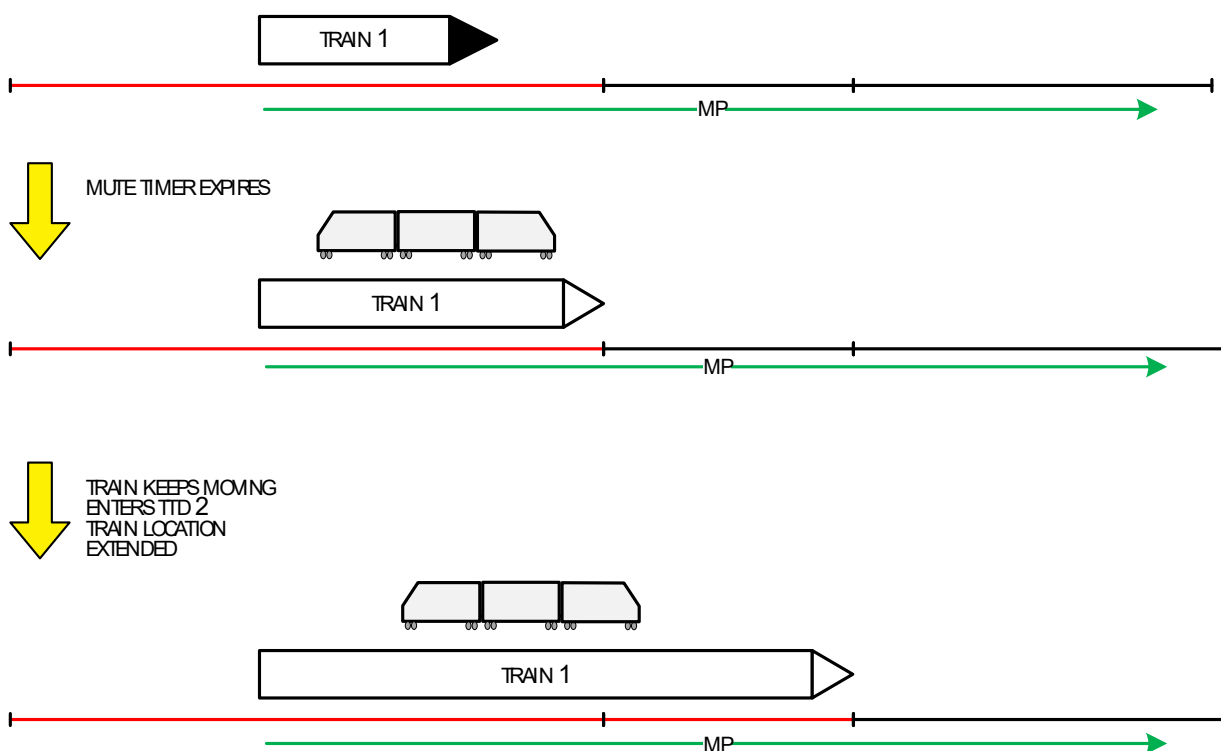


Figure 57 Extension of Train Location after Mute Timer has expired by Occupied TTD

REQ-TTD-16

For a system using TTD, when detecting an expected TTD occupancy within the Movement Permission allocated to a train with an assumed position, the MBS shall extend the assumed *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:

While a train has an assumed position, the front of the assumed Train Location is moved to its furthest possible location to give the information (to operator) that the train could be anywhere along the Movement Permission considering the TTD information.

Guidance:

A train with an assumed position can move forward within the Movement Permission allocated to that train and occupy a previously clear TTD section. 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 assumed *Train Location* of this train. This is similar to the possible movement of a train for which the Mute Timer has expired, as seen in the figure in REQ-TTD-5.

6.14.8 Requirements to delete *Train Location*

REQ-OP-Delete-Pos

MBS shall check that the train indicated in a Request for Delete Position from OP has an assumed train position and only if this is the case delete this position and set the position qualifier for this train to *unknown*, otherwise the MBS shall reject this request and reply with the reject code “INVALID_REQUEST”.

Rationale: This checks that the train in the OP request has an assumed *Train Location*.

Guidance: If an assumed *Train Location* needs to be modified, it must first be deleted.

Note that if the affected train has already been given an SR Authorisation, then deleting the assumed position will cause the MBS to send an Emergency Stop message to that train.

REQ-Delete-Assumed-Loc

MBS shall delete an assumed *Train Location* if the position qualifier for the associated *Train Object* changes to *unknown*.

Rationale: A position that is unknown cannot be associated with an assumed location.

Guidance: This should only happen if the assumed train position is deleted or if the train reports an LRBG which is not known to the MBS. Note that if the associated train has been given an SR Authorisation, the deletion of the assumed train location will cause the MBS to send Unconditional Emergency Stop message to this train.

6.14.9 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.

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

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].

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.

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

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.

6.15 SysF MANAGE UNRESOLVED TRACKBOUND OBJECT

6.15.1 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 20:

<i>Unresolved Trackbound Object</i> Reasons	Notes	Requirements
Reporting train with a shorter value of L_TRAIN	MBS is receiving 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 at standstill is no longer in communication	REQ-TrainLoc-10
Train is no longer in communication	MBS considers that a moving train is no longer in communication	REQ-TrainLoc-18
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

<i>Unresolved Trackbound Object Reasons</i>	<i>Notes</i>	<i>Requirements</i>
TTD section trespassing	A TTD section is unexpectedly trespassed	REQ-TTD-9, REQ-TTD-10
Unexpected TTD section clearance	A TTD section is unexpectedly Cleared	REQ-TTD-12
TTD remains occupied	A TTD remains occupied when it is expected to become Clear	REQ-TTD-13
UTO propagation	UTO is propagated until the TTD limit or until <i>Train Location</i> limit.	REQ-TrainLoc-14, REQ-TrainLoc-17
UTO creation/propagation for train with integrity not confirmed	UTO is created until the TTD limit or until <i>Train Location</i> limit when integrity is lost.	REQ-TrainLoc-15, REQ-TrainLoc-16
Train with integrity not confirmed	When the train rear is moved forward by a Train with integrity not confirmed, UTO is created (and then potentially removed by clear TTD).	REQ-0078

Table 20 – Reasons to create or extend Unresolved Trackbound Object

There are several reasons to remove (even partly) an *Unresolved Trackbound Object*, as shown in Table 21:

<i>Unresolved Trackbound Object Reasons</i>	<i>Notes</i>	<i>Requirements</i>
UTO is replaced by <i>Train Location</i>	UTO is removed when it is replaced by the <i>Train Location</i> 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
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 21 – Reasons to remove (even partly) Unresolved Trackbound Object

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

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 can correlate these events.

The MBS is designed to allow for:

- The passing of a TTD limit (detected by TDP or occupancy of the TTD) by a train before the train has reported a position within the TTD section i.e. no UTO is created in this case as the occupancy is expected (see REQ-TTD-9 and REQ-TTD-10).
- A train reporting a position within the TTD section before TTD section becomes Occupied i.e. no UTO is created in this case.
- 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 i.e. no UTO is created in this case as the clearing is expected (see REQ-TTD-12).
- A train reporting a position clear of the TTD section before the TTD section becomes Clear, i.e. UTO is not immediately created in this case as the clearing of the TTD is expected within a certain time (see REQ-TTD-13 guideline).

6.15.2 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 derailleurs 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.

6.15.3 Requirements to update Unresolved Trackbound Objects

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 <i>Unresolved Trackbound Object</i>	The extent of the <i>Unresolved Trackbound Object</i> .
Recorded Train Length	As for L_TRAIN	The length of train associated with this <i>Unresolved Trackbound Object</i> , 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 20.	The reason why the UTO was created. There might be more than one reason.

Table 22 – *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:

- 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
- 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
- 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 20.

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 with 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.

REQ-TrackStatus-9

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, if any, 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*.

Figure 58 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).

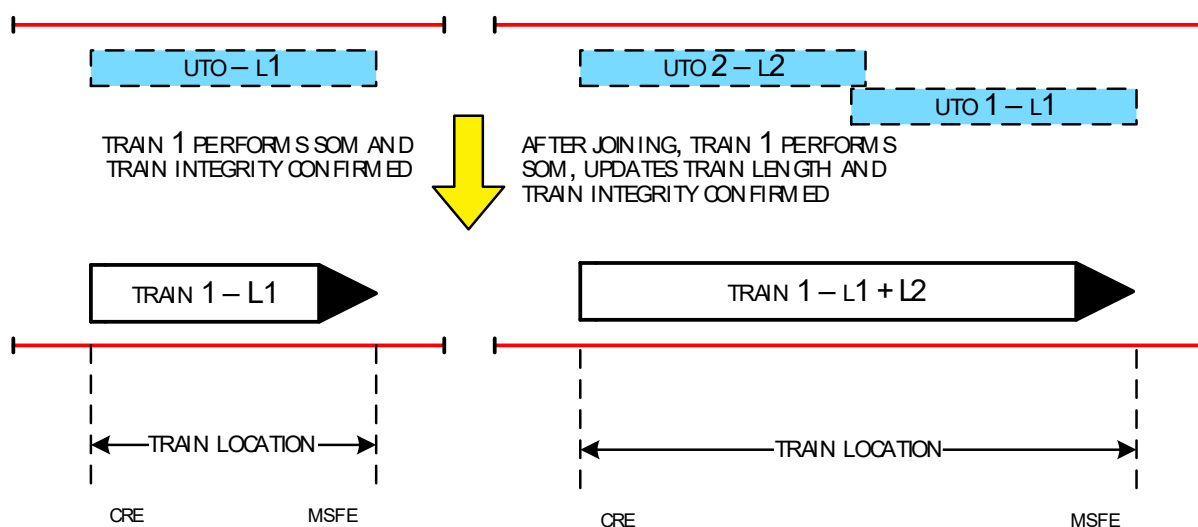


Figure 58: Train Location after confirmation of Train Integrity

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*).

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 59.

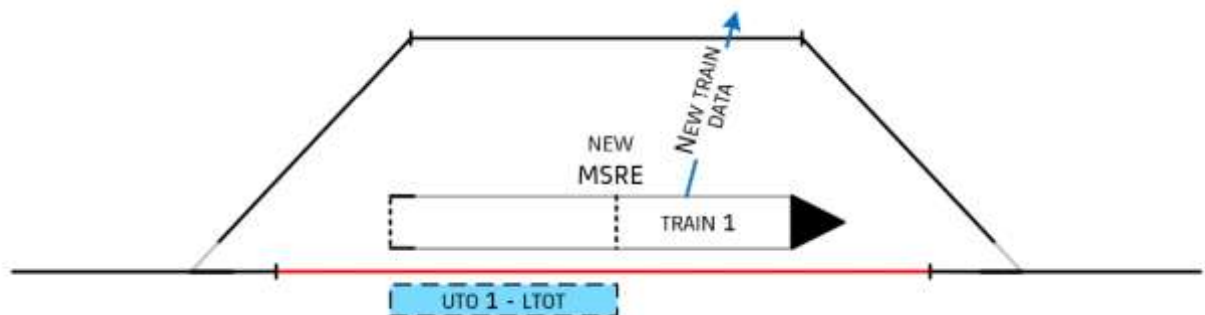


Figure 59: UTO creation when receiving Validated Train Data, L_TRAIN decreased

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

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:

- 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.

Figure 60 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.

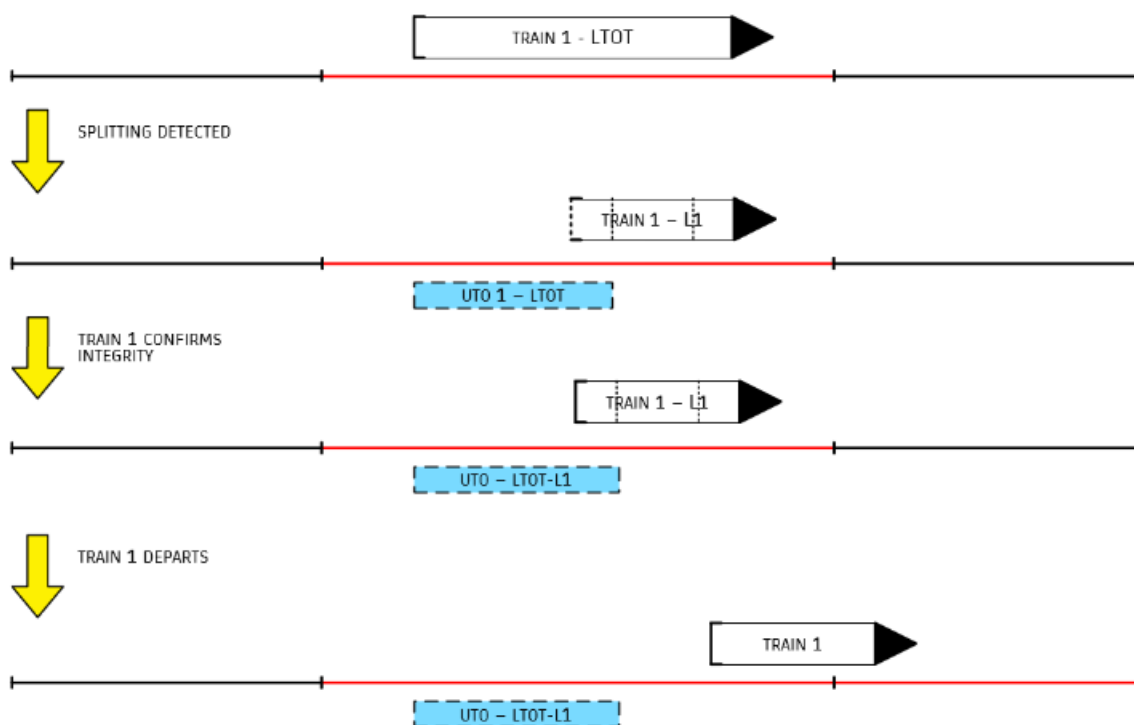


Figure 60: Unresolved Trackbound Object remains when Front Train after Splitting leaves

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*

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

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 waggon 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.

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

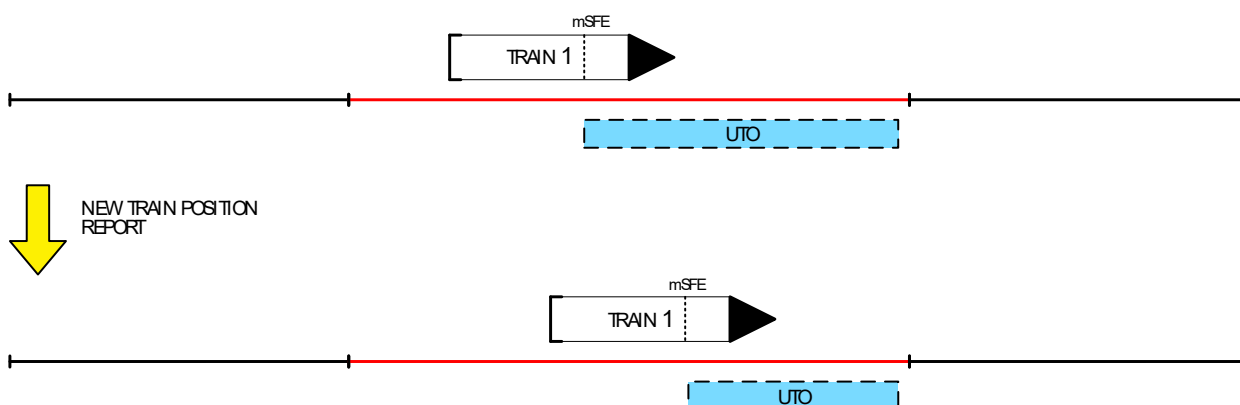


Figure 61: Train with Train Integrity confirmed Sweeping an *Unresolved Trackbound Object*

Figure 62 below shows a train having passed an *Unresolved Trackbound Object* between a new and the previous *Train Location*. The train sweeps that *Unresolved Trackbound Object*.

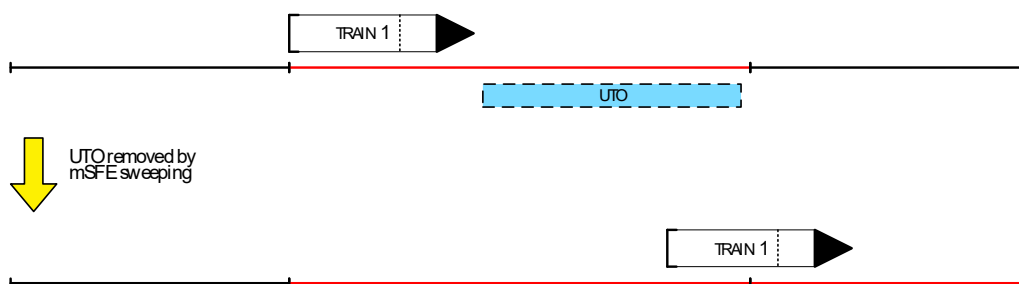


Figure 62: Existing *Unresolved Trackbound Object* swept by a passing train

The passage of a train through an *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.

This reduction must only be performed if the *Unresolved Trackbound Object* is not divided into two by this reduction as no UTO must be left backward the min Safe Front End during sweeping. In the following example, no sweeping is performed as a UTO would be left backward the min Safe Front End.

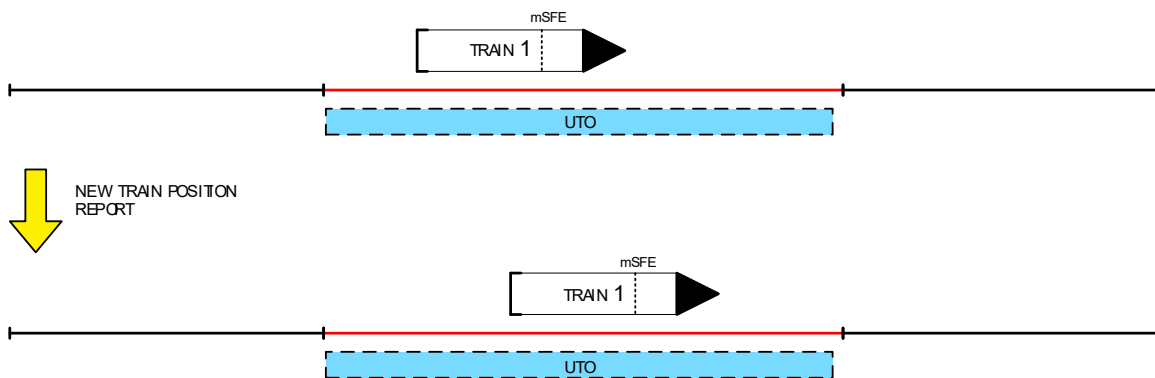


Figure 63: Existing *Unresolved Trackbound Object* cannot be swept by the train

REQ-0078

When MBS moves forward the rear of the *Train Location* for a Train with integrity not confirmed, the MBS shall create a UTO from the previous rear of the *Train Location* up to the new rear of the *Train Location*. This requirement shall be performed before requirement REQ-TTD-7.

Rationale:

When the *Train Location* rear of a train with integrity not confirmed moves forward (due to TTD clearance), the track vacancy is not proven for the zone vacated by the train, a UTO is then created covering the zone released by the *Train Location*.

Guidance:

Figure 64 below shows the update of the train rear due to track occupation clearance according to REQ-TTD-6. As train integrity is not confirmed for this train during this update, a UTO is created according to REQ-0078 and then partly removed according to REQ-TTD-7. The UTO remains on the first TTD as this TTD remains occupied.

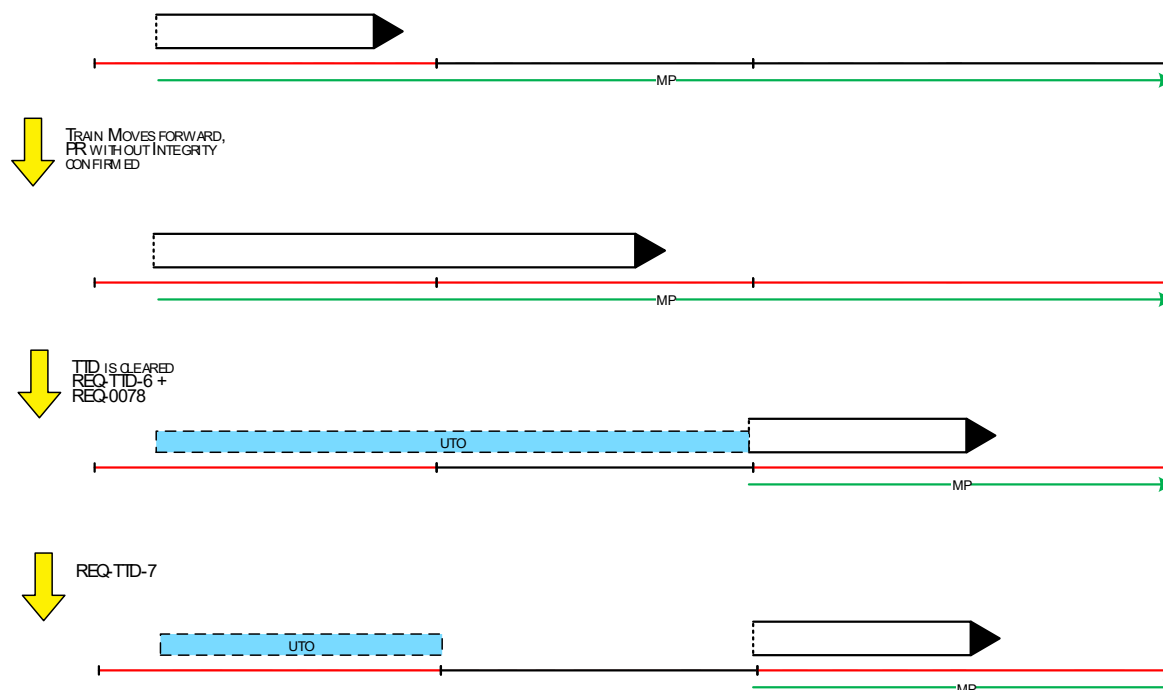


Figure 64: UTO created by rear moving forward for a train with Integrity not confirmed

Note: in case a UTO is already associated to the non-integer train as per REQ-TrainLoc-15 and REQ-TrainLoc-16, REQ-0078 could be not applied.

6.15.4 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 65:

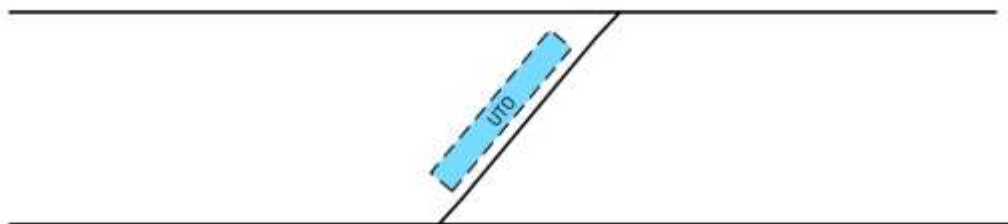


Figure 65: Short Unresolved Trackbound Object at crossover

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 waggon becoming lost.

6.15.5 Impact from TTD on Unresolved Trackbound Objects

REQ-TTD-7

For a system using TTD, the MBS shall remove all or part of an Unresolved Trackbound Object, corresponding to a TTD section which is detected cleared in accordance with a train movement or an operational procedure.

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.

If a clear TTD section cannot always be fully trusted (e.g. if it is possible for track circuits to fail in the clear state due to rail head contamination), specific conditions might be considered to remove the UTO (the clearance is expected according to train movements or during specific operational procedure, as MBS start-up).

Note: If the TTD is a track circuit and becomes cleared due to dust, TTD-7 is not applicable as the TTD section is not detected cleared in accordance with a train movement or an operational procedure. In this situation, the UTO remains on the cleared TTD section.

REQ-TTD-17

If a UTO has to be split into several UTOs, e.g. according to requirement REQ-TTD-7, the recorded length shall be deleted for all resulting UTOs.

Rationale:

Recorded train length information is not meaningful anymore for a UTO if it is split.

Guidance: None

REQ-TTD-18

When there is an overlap of UTOs and at least one of the UTO has no recorded train length, the MBS shall merge these UTO into one UTO without a recorded train length.

Rationale:

Recorded train length information is not meaningful anymore for an overlapping UTO if the other UTO has no recorded train length.

Guidance: None

REQ-TTD-19

When there is an overlap of UTOs and all these UTOs have a recorded train length, the MBS shall merge these UTO into one UTO to be reported to OP and PE through the MBS Operational State.

Rationale:

To simplify the OP/PE design, only one UTO is reported in this case.

Guidance: None

REQ-TTD-20

When UTO are merged according to REQ-TTD-19, then MBS shall store the sum of all recorded lengths of the UTOs.

Rationale:

The total train length to be considered is the sum of all train lengths.

Guidance: 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.

REQ-TTD-9

For a system using TTD, when detecting an unexpected passing of a TTD limit, the MBS shall create an *Unresolved Trackbound Object* for the trespassed TTD section (if there is no UTO to be extended according to requirement REQ-TTD-10).

Rationale:

The passing of a TTD limit not associated with any expected train movement should be considered a potential hazard.

Guidance:

The unexpected passing of a TTD limit can be detected by:

- Train Detection Point (TDP) function, this is the preferred solution for detecting the passing of a TTD limit as it can be detected even between 2 adjacent TTD sections that are already occupied.
- The occupancy of TTD (TTD is unexpectedly occupied, disturbed, or even becomes unexpectedly free – see TTD-12).

Implementation of such a function is project-specific and will likely require the use of timers to compensate for the latency between the 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 section is trespassed. This would require engineering, to determine the size of the Unresolved Trackbound Object to be created when the short boundary TTD section is trespassed.

Note: an expected passing of a TTD limit must be by a foreseen train movement within a given Movement Permission. This also applies for SR Authorisations.

REQ-TTD-10

For a system using TTD, when detecting an unexpected passing of a TTD limit from a TTD section in which an Unresolved Trackbound Object having a Recorded Train Length greater than zero exists, the MBS shall extend this Unresolved Trackbound Object up to the next boundary of the trespassed TTD section.

Rationale:

The passing of a TTD limit not associated with any expected train movement should be considered a potential hazard.

Guidance:

A train which is not communicating can move and cross a TTD limit. The MBS can adjust the knowledge about where the train might be by extending the existing Unresolved Trackbound Object.

This can also happen for a train with an assumed Train Location being authorised to move in SR when the assumed location of the train is wrong and it passes a TTD limit which is not within the given SR Authorisation.

The unexpected crossing of a TTD limit can be detected by:

- Train Detection Point (TDP), this is the preferred solution for detecting the passing of a TTD limit as it can be detected even between 2 adjacent TTD sections that are already occupied.
- The occupancy of a TTD section (becoming occupied or even becoming free).

REQ-TTD-11

For a system using TTD, when detecting an expected passing of a TTD limit along a Shunting Permission, the MBS shall create an Unresolved Trackbound Object in the entered section, if no Unresolved Trackbound Object is present at the TTD limit within the entered section.

Rationale:

After passing a TTD limit during shunting, there has to be an occupation in the target section.

Guidance: None

REQ-TTD-111

For a system using TTD, when detecting an expected passing of a TTD limit along a Movement Permission and the train has an Assumed Train Location, the MBS shall extend the Unresolved Trackbound Object into the entered section according to REQ-TTD-9.

Rationale:

After passing a TTD limit during a movement in SR with an *Assumed Train Location*, the next section has to be covered by a UTO as well.

Guidance: None

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.

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

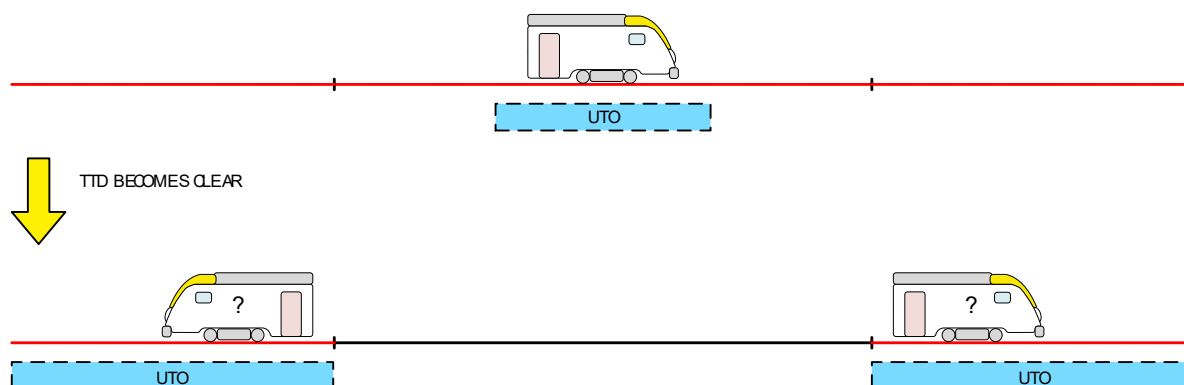


Figure 66: Creation of Unresolved Trackbound Object for unexpected Clear TTD

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.

Note 1: this requirement is used to mitigate the risk of a Trackbound Object that has passed the TTD limit of a TTD already occupied by a connected train (no UTO exists yet over the TTD as the occupation was explained by the Train Location of the connected train). In this case, a UTO is created on the already occupied TTD.

Note 2: if TDP are used, this requirement is not applicable, as the passing of the TTD limit is detected and a UTO is already present by the application of requirements REQ-TTD-9/REQ-TTD-10

REQ-TTD-13

For a system using TTD, when detecting a TTD being occupied which cannot be associated with any train movement or *Train Location*, the MBS shall create an Unresolved Trackbound Object covering the occupied TTD.

Rationale:

A TTD being occupied when it is expected to be clear indicates the possible presence of an unknown railway vehicle.

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 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 Position Reports and TTD inputs.

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 6.15.2). 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 67 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.

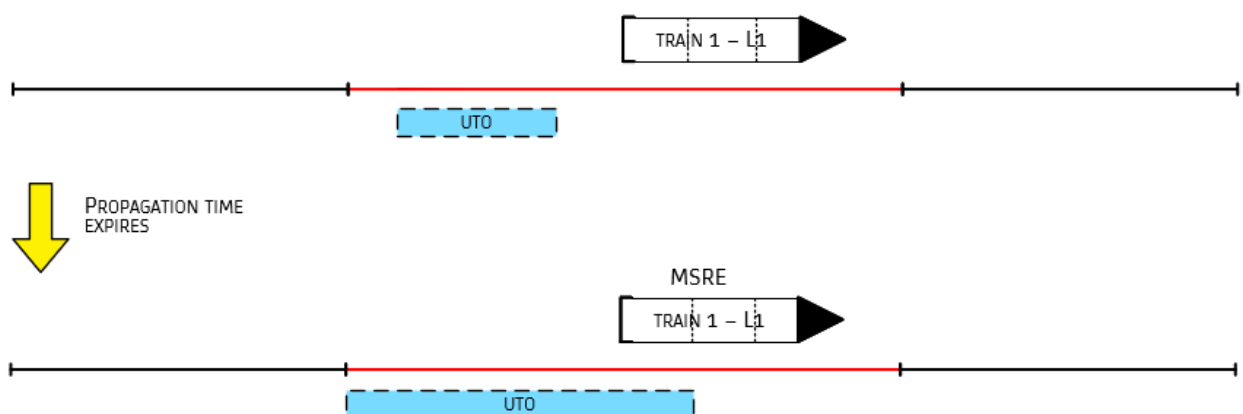


Figure 67: UTO propagation with a train in the same direction.

Figure 68 below shows the propagation of the UTO when the propagation timer expires with the presence of a train in the opposite direction.



Figure 68: UTO propagation with a train in the opposite direction.

If the UTO is propagated over a Track Edge End, the propagation is continued on adjacent Track Edge(s). If there are several adjacent Track Edges, the switch position (i.e. only one DPS in the state “FULL”) can be used to propagate on one Track Edge only.

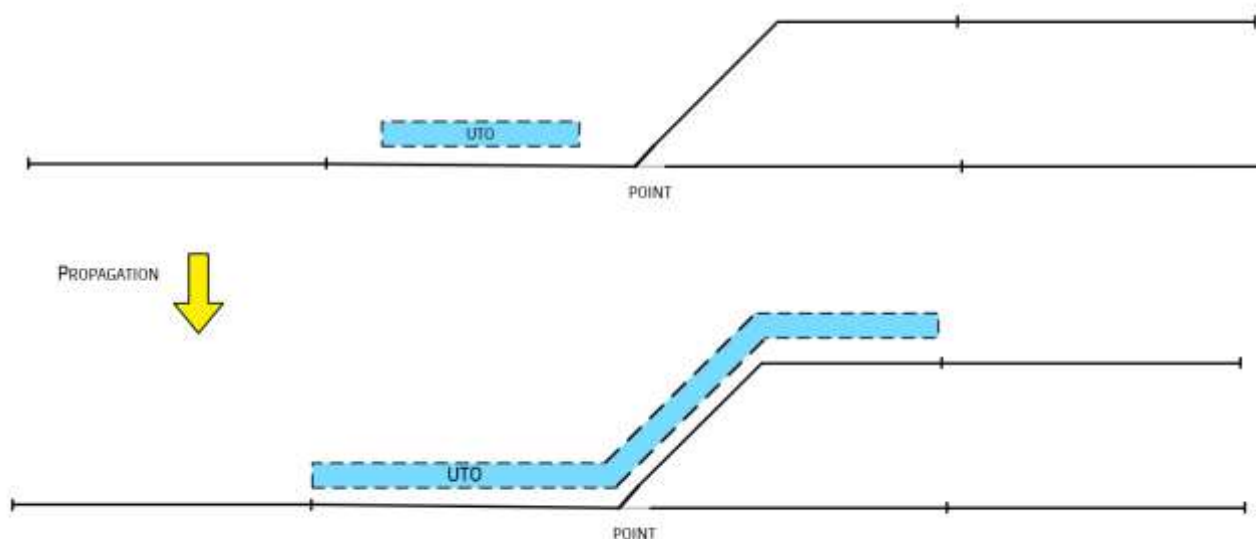


Figure 69: UTO propagation over a diverging point.

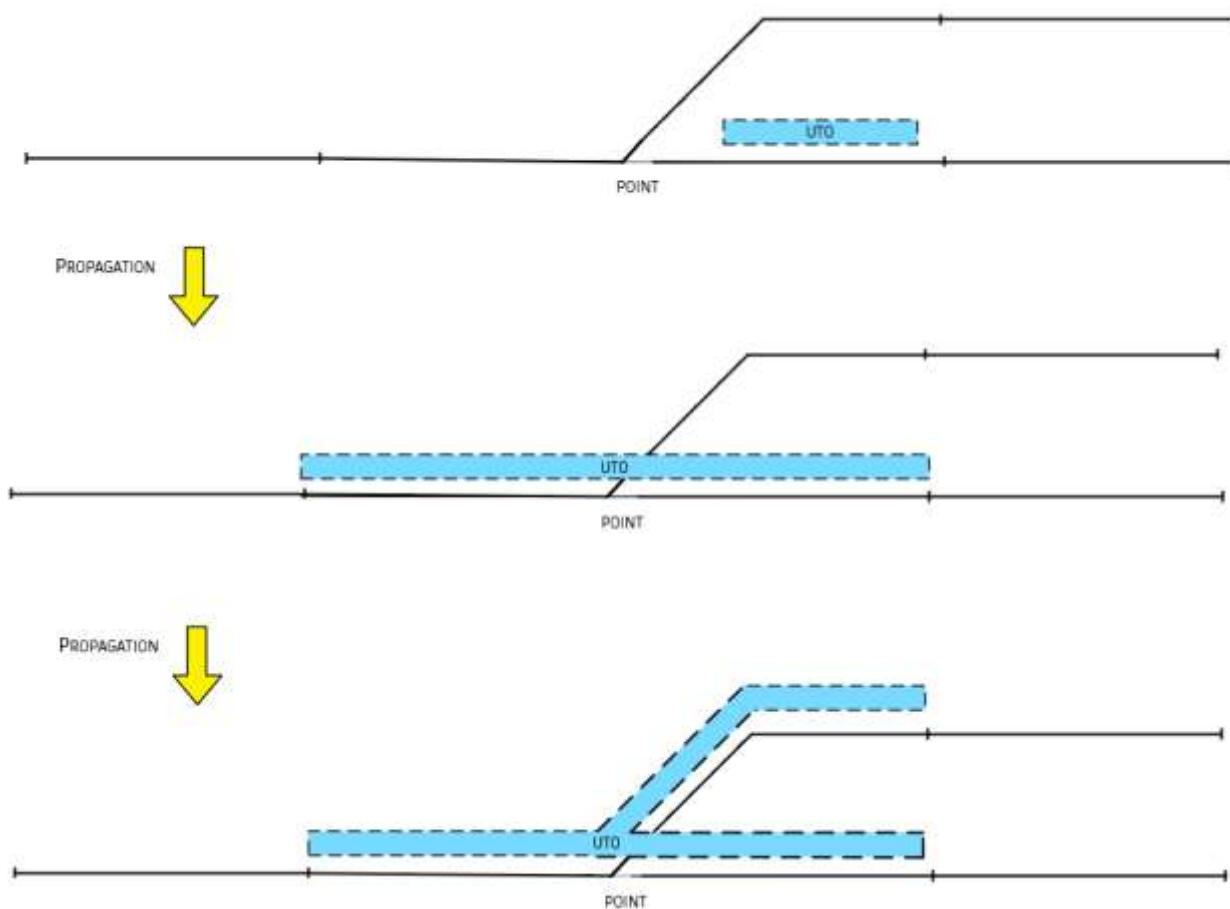


Figure 70: UTO propagation over a converging point.

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

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

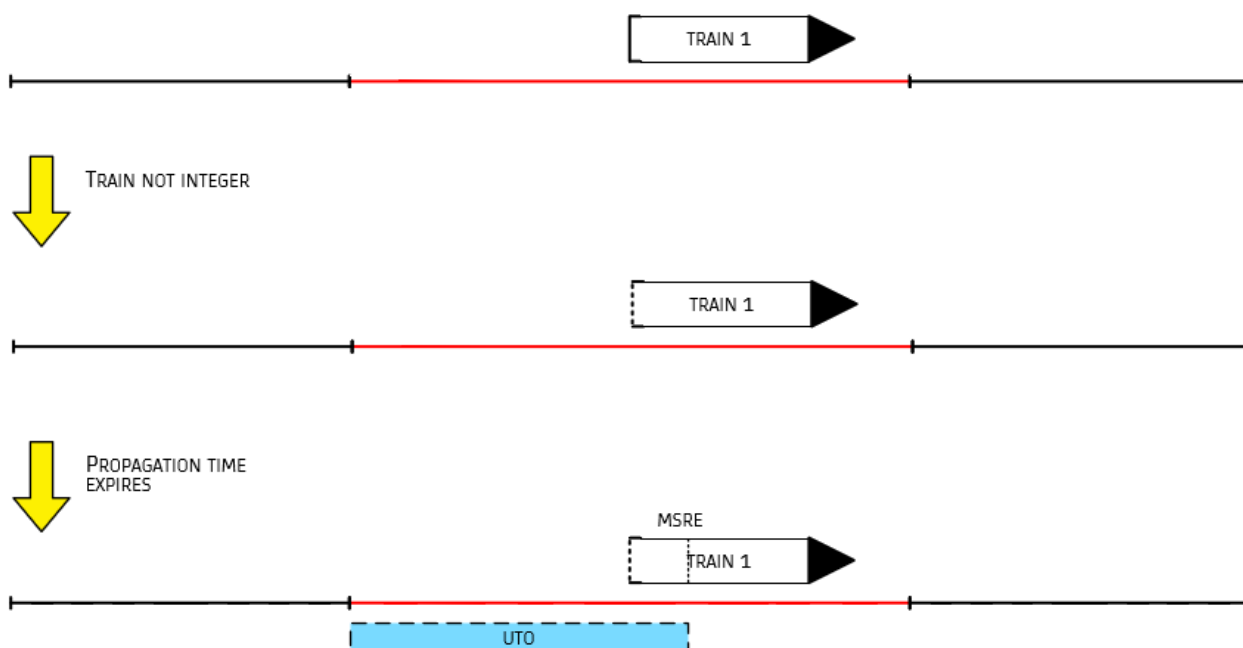


Figure 71: UTO creation for a non-integer train.

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

6.16 SysF AUTHORISE MP REQUEST

6.16.1 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 (OP) can request an Authorisation through the SCI-CMD interface (I_PE or I_OP), 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. if the operating state has changed during the message transmission between PE and MBS) but only report the failure to the requestor 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

6.16.1.1 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 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-MP).

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 6.22).

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.

For the current release, the search for flank protection along the Risk Buffer is excluded.

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 of 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 23.

Flank Protection by	Termination Requirement SC-RP_TERM_	Variable	Scope	Type	Description
Search Options	--	<i>fpSearch</i>	G	BOOL	TRUE if Flank Protection is required
		<i>fpSearchOnDependentAs</i>	AS	BOOL	TRUE if the dependent <i>Allocation Section</i> needs Flank Protection
		<i>rpMaxSearchDistance</i>	G	UINT	The length in meters after which the <i>Risk Path</i> search is finished
Switchable Track Element	DPS	<i>rpTermAtDpsOnly</i>	AS	BOOL	TRUE if a <i>Risk Path</i> originating at this <i>Allocation Section</i> can only be terminated at a DPS

Flank Protection by	Termination Requirement SC-RP_TERM_	Variable	Scope	Type	Description
		<i>dpsProvidesFlankProtection</i>	DPS	BOOL	TRUE if this DPS can provide flank protection
		<i>dpsMaxFlankProtectionSpeed</i>	DPS	UINT	Speed in km/h up to which this DPS can provide Flank Protection
Movement Permission	RB MP	<i>rpTermAllowedAtRbAndMp</i>	G	BOOL	TRUE if Risk Paths terminated at a Movement Permission Extent or Risk Buffer can be used as a flank protection measure.
<i>Train Object</i>	TO	<i>rpTermAllowedAtTo</i>	G	BOOL	TRUE if Risk Path terminated at a Train Object can be used as a flank protection measure.
Sufficient Distance	DIST	<i>rpTermAllowedAfterMaxDistance</i>	G	BOOL	TRUE if Risk Path terminated after a defined search distance given in <i>rpMaxSearchDistance</i> can be used as flank protection measure.
Operational Rules (UTO found)	UTO	<i>rpTermAllowedAtUto</i>	G	BOOL	TRUE if Risk Path terminated at an Unresolved Trackbound Object can be used as flank protection measure.
		<i>rpTermMaxSpeedUto</i>	G	UINT	Max Speed for a Movement Permission at the <i>Allocation</i> section if a <i>Risk Path</i> originating from it terminates at an Unresolved Trackbound Object.

Flank Protection by	Termination Requirement SC-RP_TERM_	Variable	Scope	Type	Description
Shunting Signal	SHUNT_SIG	provideFlankProtectionForTrainRuns	S	BOOL	TRUE if Shunting Signal provides flank protection
		rpTermMaxSpeedShuntSig	G	UINT	Max Speed for a Movement Permission at the <i>Allocation</i> section if a <i>Risk Path</i> originating from it terminates at a Shunting Signal.

Table 23 – 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)*

S = Configurable at every Shunting Signal

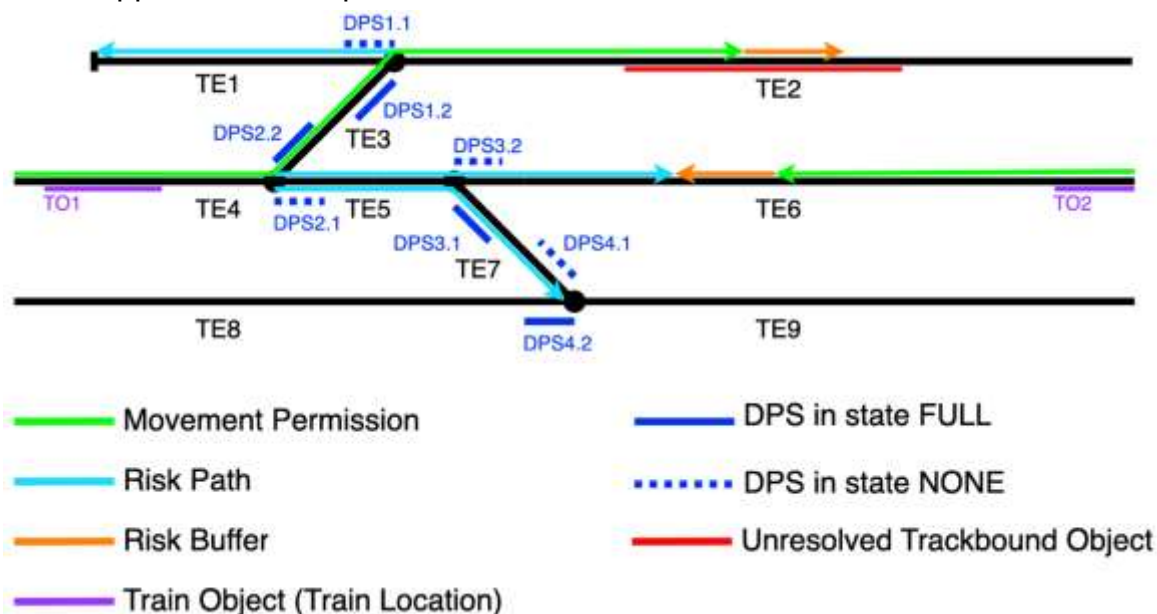
In tracks (usually secondary tracks) where non-controlled movements can occur (shunting, stabling of vehicles with remaining rollaway risk), the Infrastructure Manager has to ensure that appropriate measures are available:

- 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/OP is impacted by the flank protection as follows:

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

6.16.1.2 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).

6.16.1.3 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_RB_AS	

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

6.16.2 Inputs

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

6.16.3 Outputs

- Message “request granted” to the requestor, PE or OP, according to I_PE or I_OP
- Authorised Movement Permission
- Message “request rejected” to the requestor, PE or OP, according to I_PE or I_OP

6.16.4 Functional requirements

REQ-SAFETY-MP-REQ

The MBS shall perform a series of checks given by the following ordered list when it receives an MP Request from PE or OP:

1. REQ-GENERAL_SYNTAX
2. REQ-GENERAL_EXISTANCE
3. REQ-TO_READY
4. REQ-TO_MODE_READY
5. REQ-TO_MODE_READY_SR
6. REQ-TO_MODE_SR
7. REQ-TOPO1

- 8. REQ-TOPO2
- 9. REQ-TOPO3
- 10. REQ-TOPO4
- 11. REQ-TOPO5
- 12. REQ-POSITION_KNOWN
- 13. REQ-TRANSLATE
- 14. REQ-SC_MP_SPEED
- 15. REQ-SC_RB_SPEED
- 16. REQ-SC_MP_SPEED_LOWER
- 17. REQ-SC_MODE
- 18. REQ-SC_MODE_MISMATCH
- 19. REQ-SC_MP_SHORTER
- 20. REQ-SC_RB_SHORTER
- 21. REQ-SC_MP_TO
- 22. REQ-SC_MP_UTO
- 23. REQ-SC_RB_TO
- 24. REQ-SC_RB_UTO
- 25. REQ-SC_MP_TO_AS
- 26. REQ-SC_MP_UTO_AS
- 27. REQ-SC_RB_TO_AS
- 28. REQ-SC_RB_UTO_AS
- 29. REQ-SC_MP_MP
- 30. REQ-SC_MP_RB
- 31. REQ-SC_MP_RP
- 32. REQ-SC_MP_SP
- 33. REQ-SC_MP_MP_AS
- 34. REQ-SC_MP_RB_AS
- 35. REQ-SC_MP_SP_AS
- 36. REQ-SC_RB_MPPS
- 37. REQ-SC_RB_RB
- 38. REQ-SC_RB_RP

39.REQ-SC_RB_SP
40.REQ-SC_RB_MP_AS
41.REQ-SC_RB_RB_AS
42.REQ-SC_RB_SP_AS
43.REQ-SC_RB_SIZE
44.REQ-SC_MPPS_DPS
45.REQ-SC_RB_DPS
46.REQ-SC_MP_URA
47.REQ-RP_SEARCH-MP
48.REQ-SC_RP_TERM
49.REQ-COOP_PENDING
50.REQ-REV_OR_REST_PENDING
51.REQ-SR_TRAIN

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

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

REQ-0032

The MBS shall abort checking an MP Request 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 the request 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.

REQ-0033

If none of the safety checks for an MP Request fails, MBS shall send an "MP_REQUEST_GRANTED" reply.

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

Guidance: None

6.16.4.1 General Safety Checks

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

REQ-TO_MODE_READY

The MBS shall check that the train mode is SB, FS, SR, OS or PT and if the check fails, the MBS shall send a “TO_MODE_NOT_READY” reject code.

Rationale: The OBU rejects the Movement Authority in other modes according to /ETCS/ SUBSET-026 4.8.4.

Guidance: Note: modes UN, SN (relevant for an Entry into a Level 2 area), AD (from ETCS System Version 2.2) are excluded in the current release.

REQ-TO_MODE_READY_SR

When the MP Request is for SR mode, the MBS shall check that the train mode is SB, SR or PT and if the check fails, the MBS shall send a “TO_MODE_NOT_READY” reject code.

Rationale: The OBU rejects an SR Authorisation in other modes according to /ETCS/ SUBSET-026 4.8.4.

Guidance: None

REQ-TO_MODE_SR

When the MP Request is for SR mode, the MBS shall check that the request comes from OP.

Rationale: Only OP can request SR Authorisation.

Guidance: 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.

REQ-TOPO2

MBS shall check that every *LinkedPath* in the request is well-formed (i.e. is truly 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

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: The value of an attribute may change within the *Movement Permission Extent*.

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 or start somewhere along the path.

Guidance: None

REQ-TOPO5

For MP request in FS and/or OS mode, 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 and if the check fails, the MBS shall send a “INVALID_EXTENT” reject code.

Rationale: Any switchable element below the *Train Objects* Location shall be in the proper state when a movement happens.

Guidance: For MBS to give a *Movement Authority*, the train needs to be localised.

REQ-POSITION_KNOWN

For an MP Request in FS or OS, the MBS shall check that the position of the train is known and if the check fails, the MBS shall send a “POSITION_INVALID” reject code.

Rationale: Only trains with a Train Location known to the MBS can be given MA.

Guidance: 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: MBS must be able to build the MA from the MP Request.

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

REQ-COOP_PENDING

The MBS shall check that there is no co-operative shortening of MA procedure 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

REQ-REV_OR_REST_PENDING

The MBS shall check that there is no pending revocation or restriction for the corresponding train and if the check fails, the MBS shall send a “REVOCATION_OR_RESTRICTION_PENDING” reject code.

Rationale: Sending MAs in parallel with revocation or restriction messages (e.g. CES, UES or more restrictive MAs) could result in inconsistent views between MBS and the on-board.

Guidance: As long as the capability ‘Revoke or restrict an authorisation’ is running, MBS shall consider that there is a pending revocation or restriction ongoing for this train.

REQ-SR_TRAIN

The MBS shall check that at the start of a Movement Permission extent in an MP Request for SR Authorisation there is a *Train Location* and if there is none then MBS shall reply with a “NO_TRAIN_AT_SR_START” reject code.

Rationale: This is to check that there is a train where the SR Authorisation starts.

Guidance: There must be a train at the start of an SR Authorisation, else the authorisation could allow a train to move from an unknown location.

6.16.4.2 Speed and Mode related Safety Checks

REQ-SC_MP_SPEED

For MP request in FS and/or OS mode, 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, etc...).

Guidance: None

REQ-SC_RB_SPEED

For MP request in FS and/or OS mode, 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 be defined until the SvL (i.e. the danger point inside the Risk Buffer).

Guidance: 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

REQ-SC_MODE

For MP request in FS and/or OS 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: Modes FS and OS must not be mixed with SR.

Guidance: None

REQ-SC_MODE_MISMATCH

If a Movement Permission is already present for a *Train Object*, the MBS shall check that there is no downgrade of a mode (FS to OS, FS to SR, or OS to SR) within the overlap of the present Movement Permission and the requested Movement Permission and if the check fails, the MBS shall send a “SAFETY_RESPONSIBILITY_PROFILE_MISMATCH” rejection code.

Rationale: If a downgrade of mode is needed, the MBS must first revoke the current Movement Permission.

Guidance: 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

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

6.16.4.3 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: None



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.

For a train not localised, this check is performed on the completed Movement Permission Extent as there is no mSFE defined.

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 or SR, 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.

For a train not localised, this check is performed on the completed Movement Permission Extent as there is no mSFE defined.

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.

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 and if 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 UTO is not allowed if the Authorisation Type at the end of the Movement Permission is set to FS.

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.

REQ-SC_MP_UTO_AS

The MBS shall check that if the extent of the Movement Permission overlaps in FS mode 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.

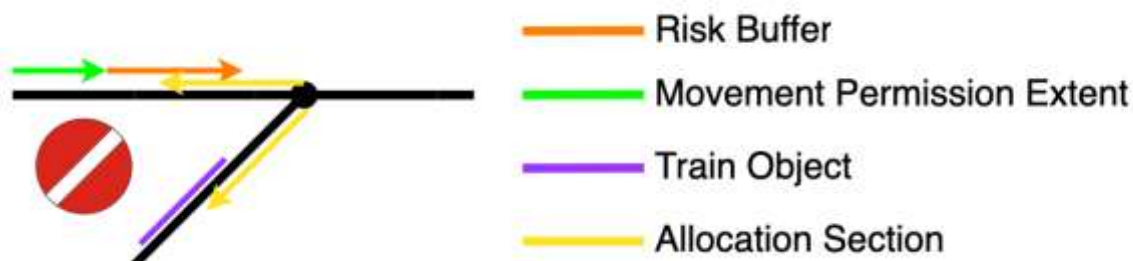
Note: only FS mode is considered here as it should be possible to pass in OS mode a UTO overlapping a switch. The UTO may occupy both allocation sections of the switch in this case.

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:



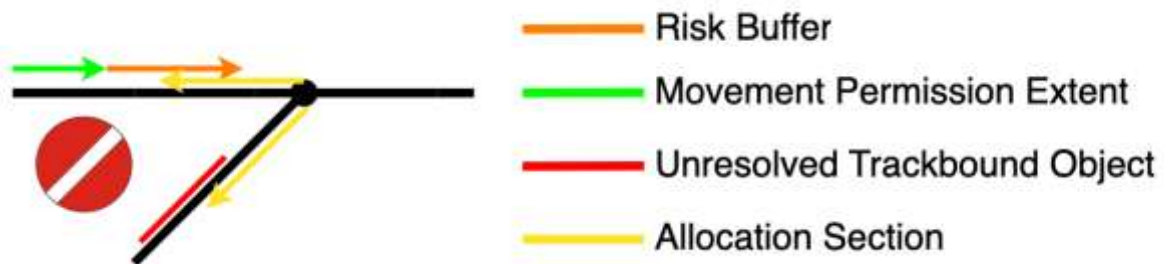
Having both *Risk Path* and *Train Object* present in a conflicting *Allocation Section* is not allowed.

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:



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

6.16.4.4 Movement related Safety Checks

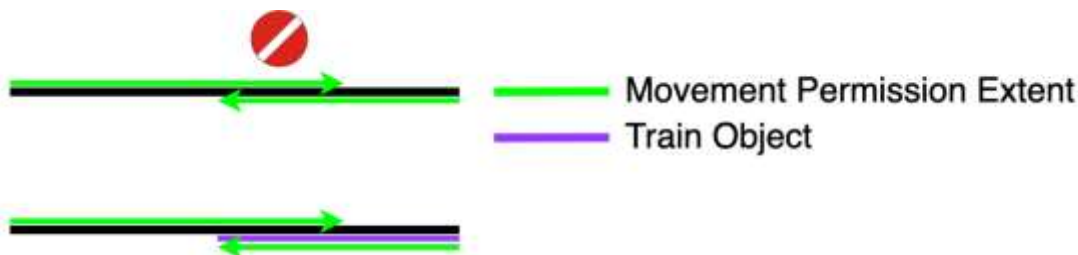
REQ-SC_MP_MP

For MP request in FS and/or OS mode, 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.



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:



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:



REQ-SC_MP_SP

The MBS shall check that the *Movement Permission Extent* of the requested MP shall not overlap with a *Shunting Permission* 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: 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:



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:

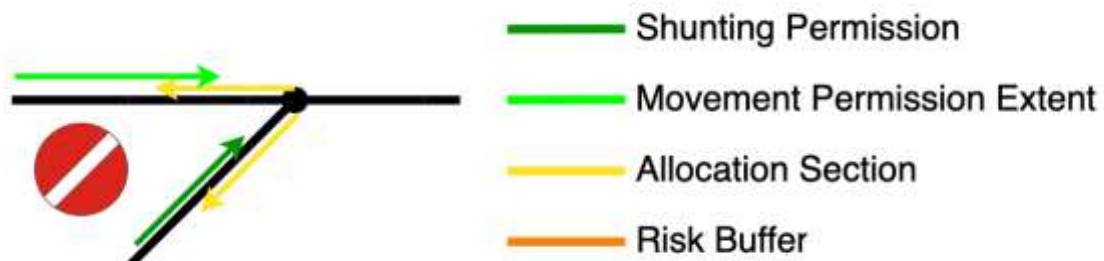


REQ-SC_MP_SP_AS

The MBS shall check that an *Allocation Section* the *Movement Permission Extent* overlaps with, shall not have an overlap with a *Shunting Permission* 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:



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.



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:

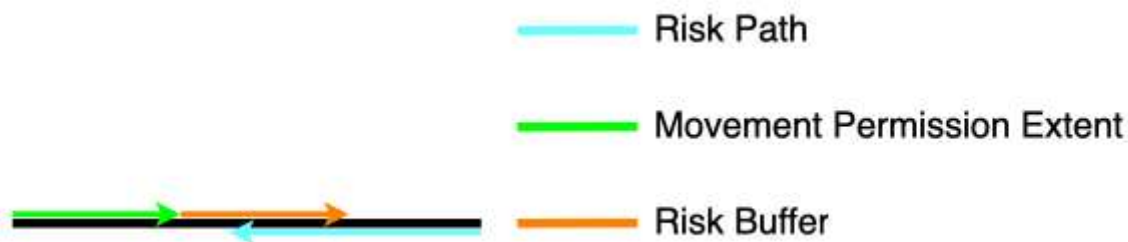


REQ-SC_RB_RP

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:



REQ-SC_RB_SP

The MBS shall check that the *Risk Buffer* of the requested MP shall not overlap with a *Shunting Permission* extent 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 a shunting movement.

Guidance:



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:



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:

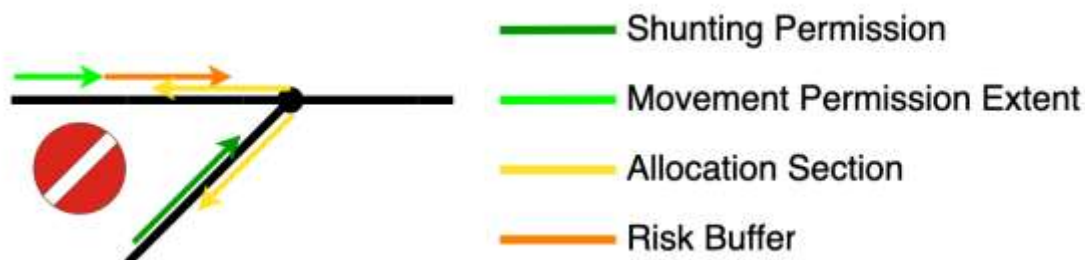


REQ-SC_RB_SP_AS

The MBS shall check that any *Allocation Section* the *Risk Buffer* of the requested MP overlaps with, shall not have another overlap with a *Shunting Permission* 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 shunting movement.

Guidance:



REQ-SC_RB_SIZE

The MBS shall check that the *Risk Buffer* for the requested MP is longer than or equal to the minimum 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: How the minimum length is determined (e.g. fixed value, specific function depending on speeds, gradients, etc.) is project specific. The absolute minimum length shall consider the overhang, i.e. the maximum distance between front / rear end of train and first / last axle according to /IF_CCS_OTHSUB/.

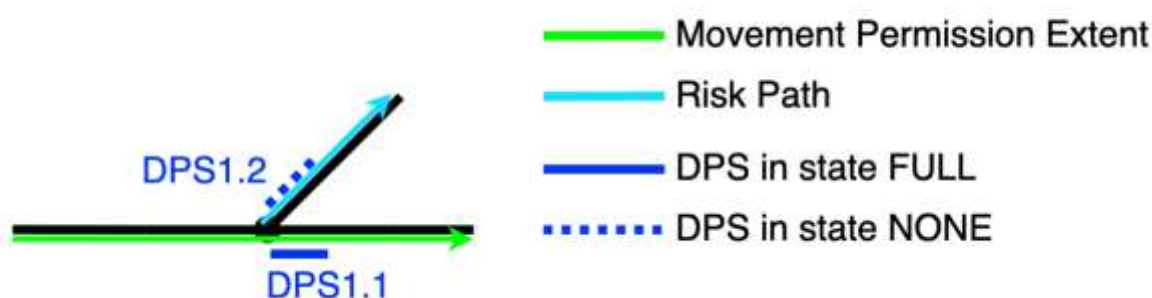
6.16.4.5 DPS related Safety Checks

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:



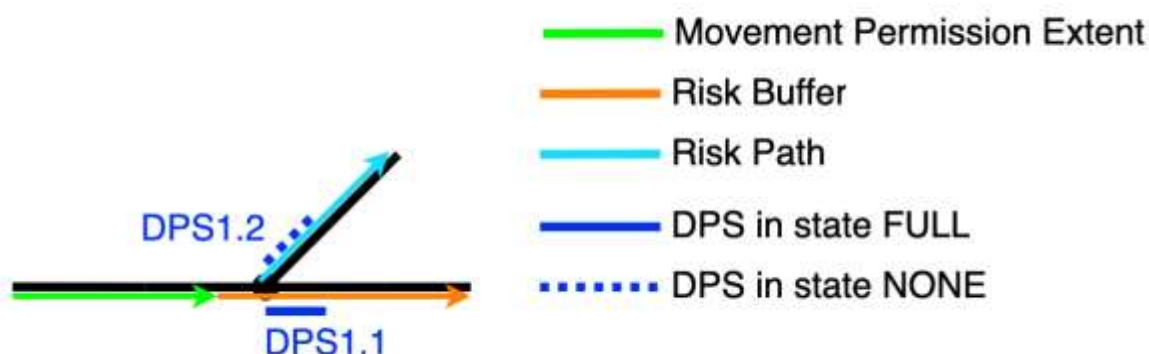
Note: The *Risk Path* is only shown for completeness.

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.

6.16.4.6 URA related Safety Checks

REQ-SC_MP_URA

When receiving an *MP Request* message where the *MP Extent* intersects a *URA* AND the *URA*

- demands a speed which is less than speed of the respective part of the *MP Speed Profile* (restriction property *speed*), OR
- demands a mode which is different from the mode in the respective part of the *MP Mode Profile* (restriction property *mode*), OR
- demands being non-passable (restriction property *noPassage*) OR
- demands not to stop (restriction property *eaExclusion*) but the EoA would be within the *URA* extent OR
- demands manual operation (restriction property *manualOperation*) but the request was received from PE

then *MBS* shall respond with *Request Rejected* message with reject code "MP_URA_CONFLICT".

Rationale: None

Guidance: None

6.16.4.7 Flank Protection related Safety Checks

REQ-RP_SEARCH-MP

If the global configuration variable *fpSearchForMp* 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:

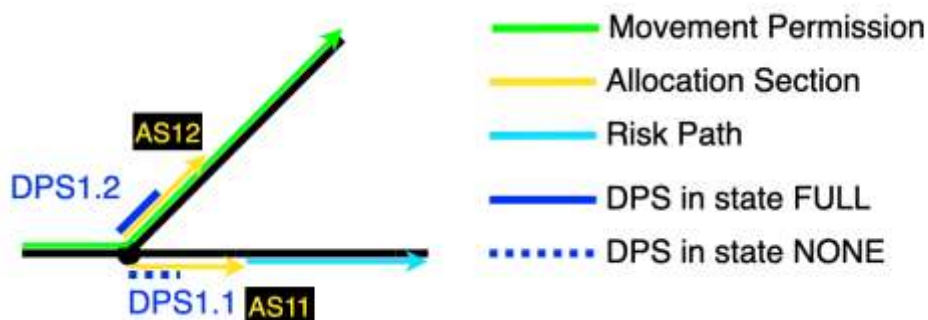
- REQ-RPS_DPS
- REQ-RPS_TO
- REQ-RPS_UTO
- REQ-RPS_MP
- REQ-RPS_RB
- REQ-RPS_SHUNT_SIG
- REQ-RPS_TE
- REQ-RPS_DIST

, while obeying the following rules:

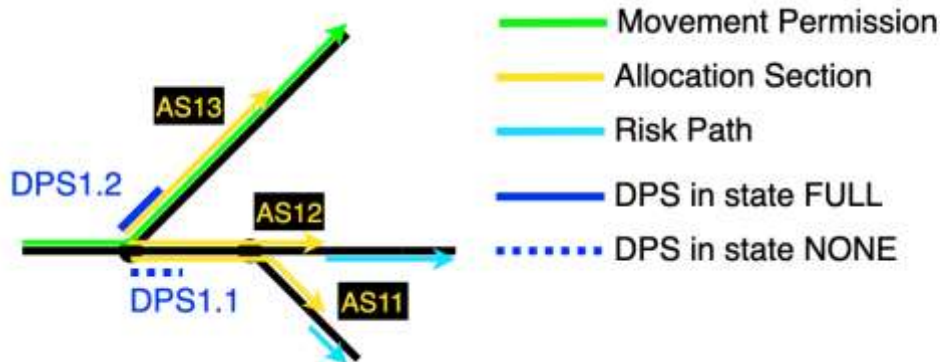
- REQ-RPS_NEAREST
- REQ-RPS_SPLIT

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.

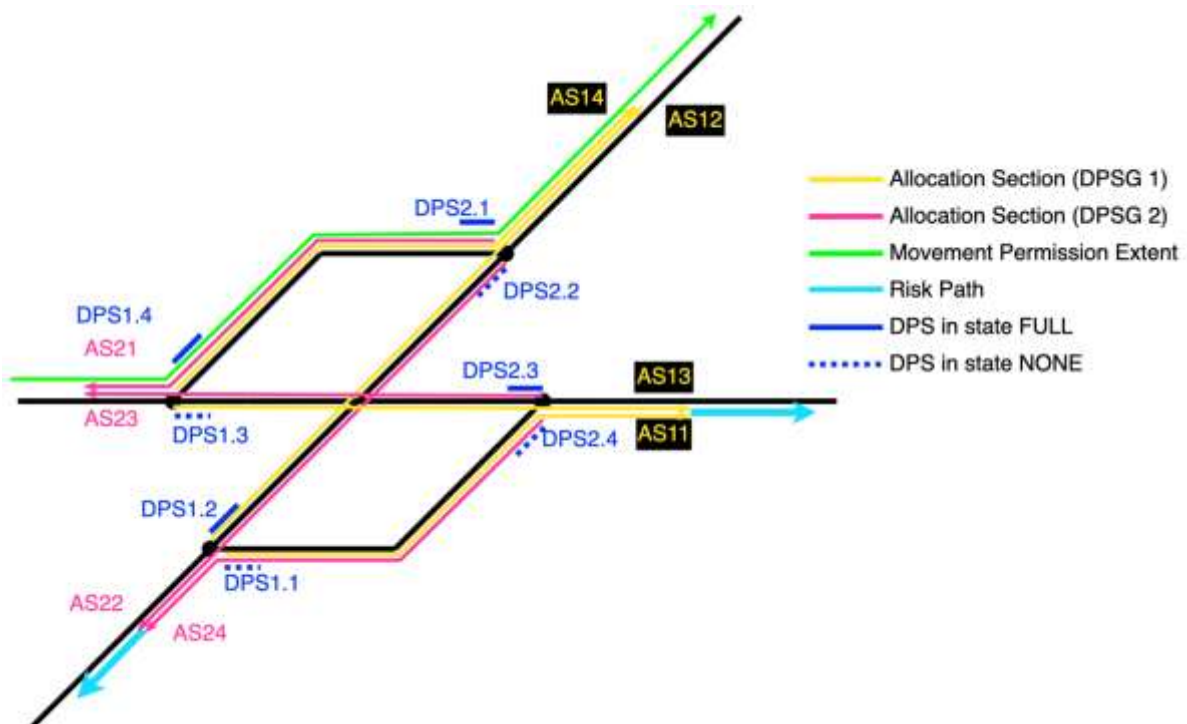
Guidance:



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.

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

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

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.

An End of a *Movement Permission Extent* in the search direction is considered as a valid end of the *Risk Path* because flank protection is also provided for this *Movement Permission*.

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

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

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 or Shunting 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

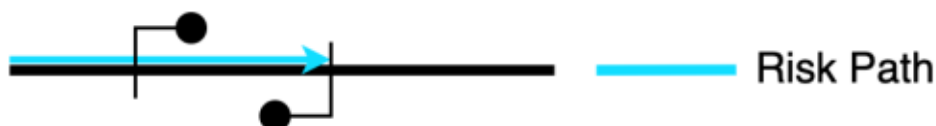
REQ- RPS_SHUNT_SIG

When the MBS builds a *Risk Path*, it shall set the end of the Risk Path to the location of a shunting signal if

- The application direction of the shunting signal is opposite to the search direction of the Risk Path
- The shunting signal does not belong to the list of shunting signals that shall not be used as a measure to mitigate the risk of flank collision for this Movement or Shunting Permission

Rationale: A shunting signal is a possible location for a *Risk Path* termination

Guidance:



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

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

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).

Guidance: None

REQ-RPS_DIST

When the MBS builds a *Risk Path* and no element to terminate is found after the configured search length *rpMaxSearchDistance*, 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

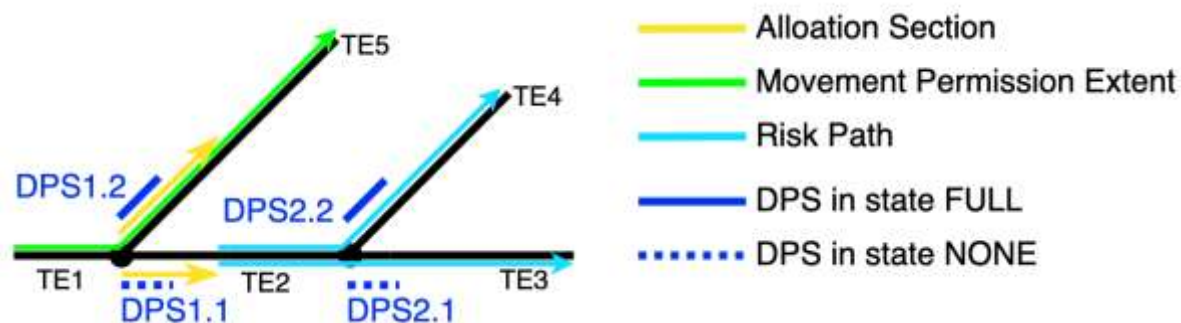
REQ-RPS_SPLIT

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*.

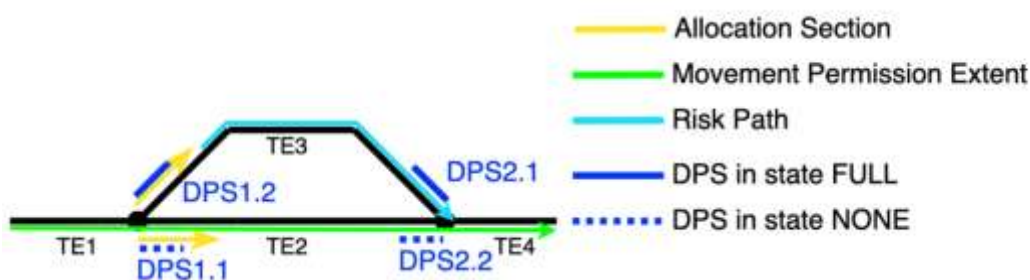
Rationale: If the head of a point is facing the requested Movement Permission, the *Risk Path* shall cover both legs of the point. MBS derives n (usually

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.

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_SHUNT_SIG
- 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

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 *dpsProvidesFlankProtection* 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 *dpsMaxFlankProtectionSpeed* for the DPS that is providing flank protection.

Rationale:

Points and derailleurs 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 derailleurs 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:

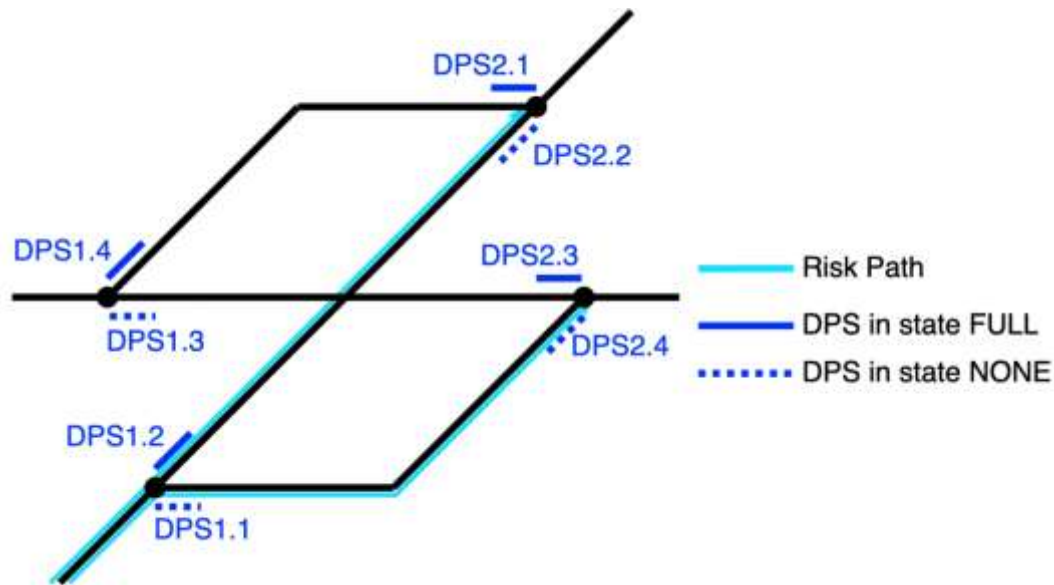
The termination of the *Risk Path* was chosen to be the “inner end” of the DPS to have a) a clear point to terminate, b) be able to perform an overlap check if the DPSG is allowed to move or locked as it serves as a flank protection element and c) to distinguish the cases of a DPSG where it is used as 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:

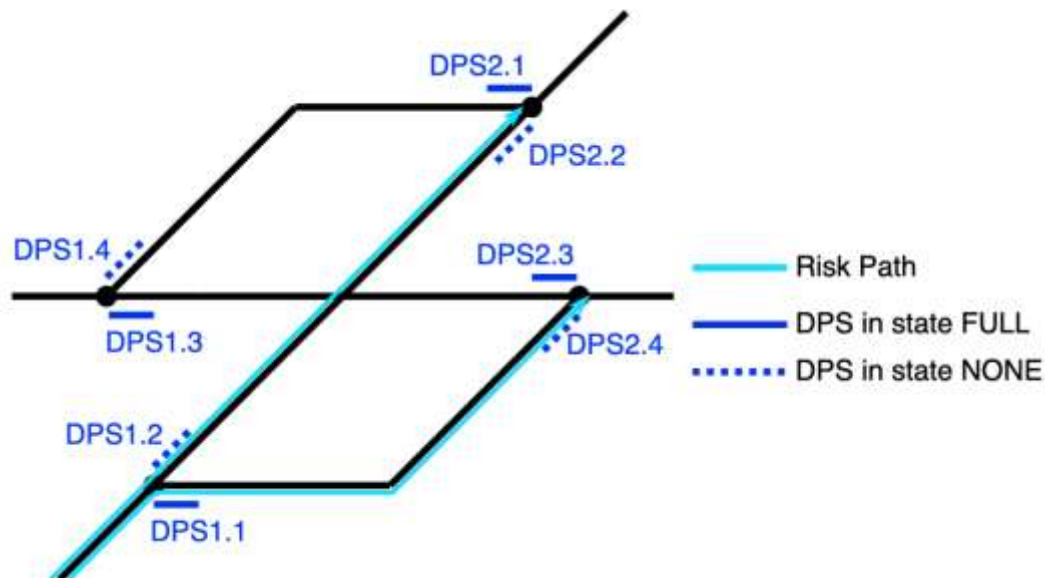


DPS 1.1 and 1.2 are in the same DPS Group and Flank Protection Group.

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.



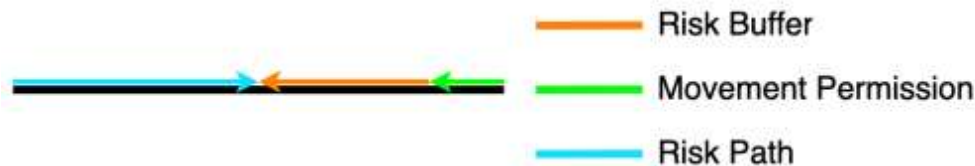
REQ-SC_RP_TERM_RB

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:



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



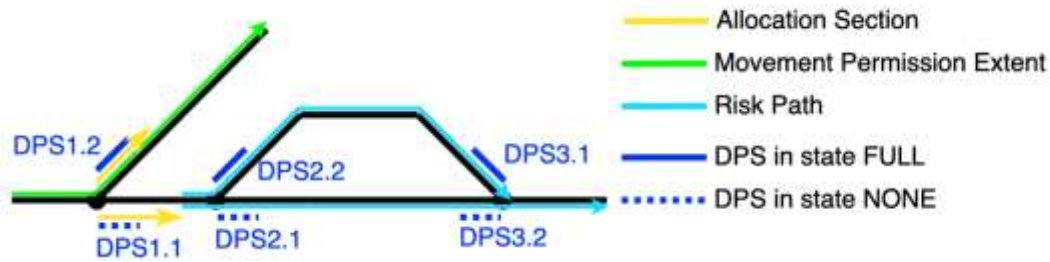
REQ-SC_RP_TERM_RP

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:



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:



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.



REQ-SC_RP_TERM_SHUNT_SIG

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

- The end of the *Risk Path* equals the location of the shunting signal
- If the *Risk Path* originates from a *Movement Permission Extent* or a *Risk Buffer*, the requested maximum speed at the location where the *Risk Path* originates from is equal to or lower than a globally configured variable `rpTermMaxSpeedShuntSig`
- If the *Risk Path* originates from a *Movement Permission Extent* or a *Risk Buffer*, the attribute `provideFlankProtectionForTrainRuns` on the shunting signal that should provide flank protection is set to TRUE
- The attribute `rpTermAtDpsOnly` is FALSE for the *Allocation section* the *Risk Path* originates from

Rationale: If set to a stop aspect, a shunting signal forbids shunting movements for in one direction thus it serves as a flank protection measure

Guidance:



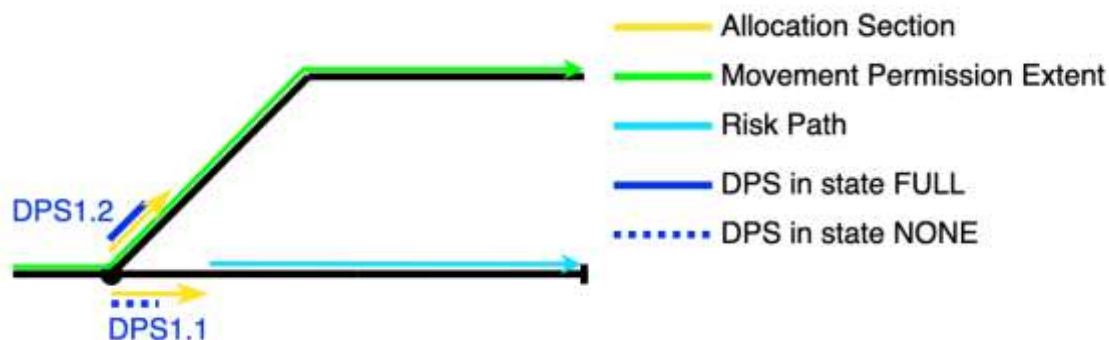
REQ-SC_RP_TERM_TE

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:



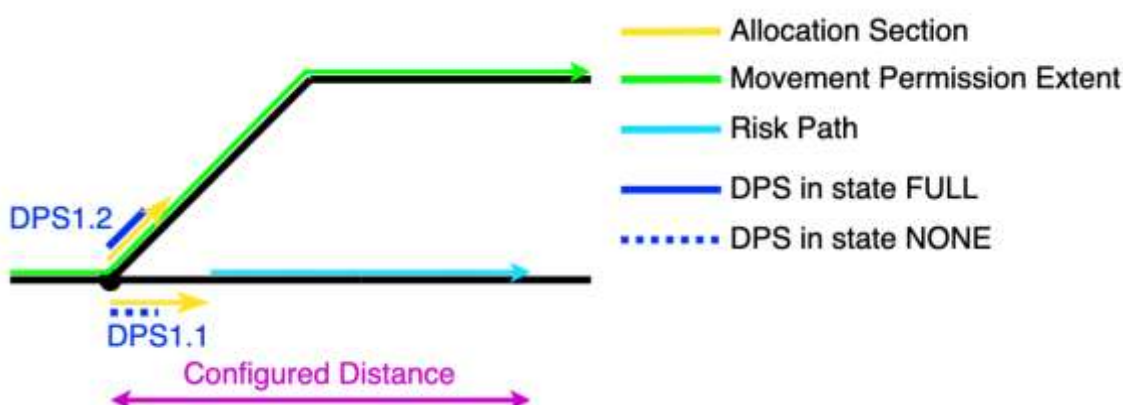
REQ-SC_RP_TERM_DIST

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

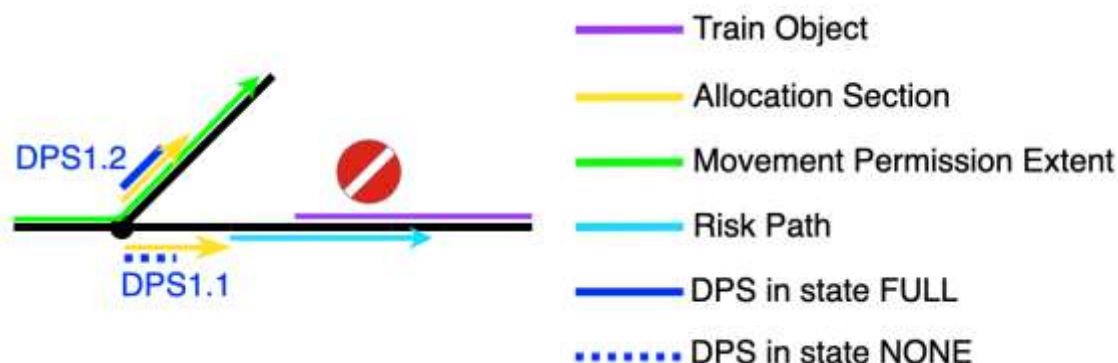


REQ-SC_RP_TO

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:



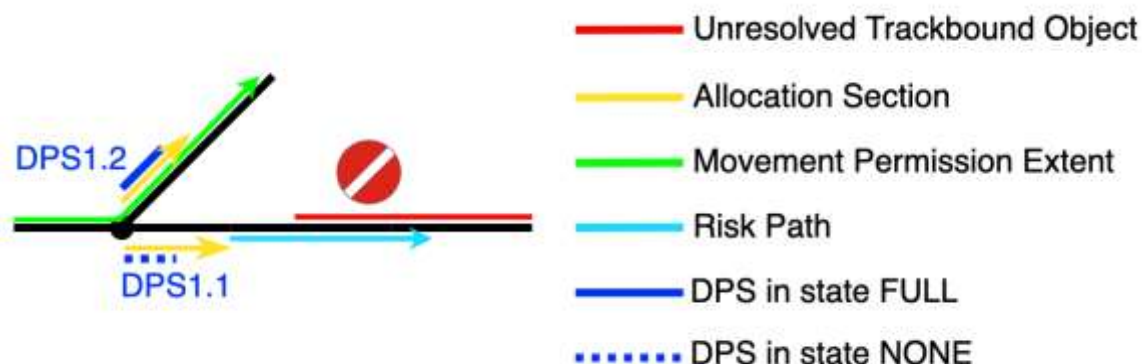
Note: The DPS states are only shown for completeness

REQ-SC_RP_UTO

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

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

Guidance:



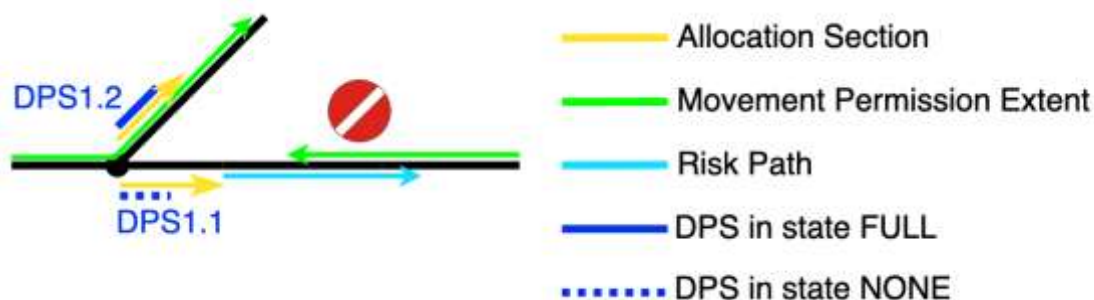
Note: The DPS states are only shown for completeness

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 danger point and the flank protection providing element shall be clear of movements.

Guidance:



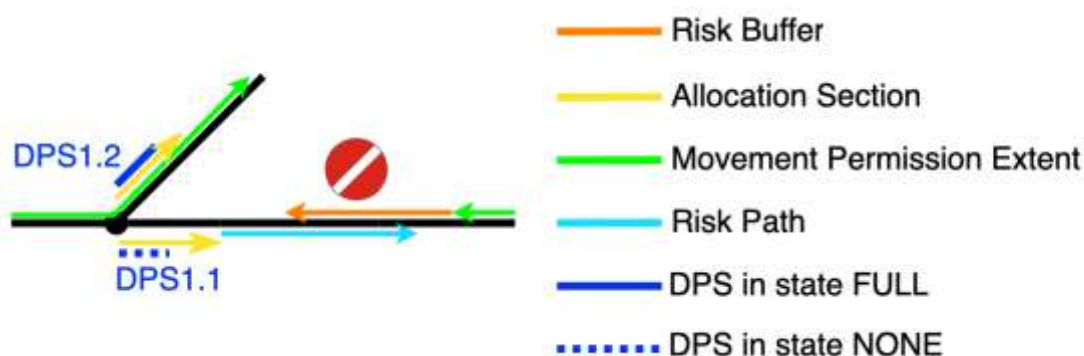
Note: The DPS states are only shown for completeness

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

6.17 AUTHORISE COOPERATIVE SHORTENING REQUEST

6.17.1 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 or OP with the failure reason.

The Cooperative Shortening Request shall contain the following information:

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

6.17.2 Inputs

- Cooperative Shortening Request message according to I_PE or I_OP

- *Domain Object State*

6.17.3 Outputs

- Message “request granted” according to I_PE or I_OP
- Message “request rejected” according to I_PE or I_OP
- Authorised Cooperative Shortening Request

6.17.4 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 or I_OP:

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

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

Guidance: This is the top requirement for all necessary checks.

REQ-COOP-FAILS

The MBS shall abort checking a Cooperative Shortening Request received through I_PE or I_OP 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

REQ-COOP-SUCCESSFUL

If none of the safety checks fails, MBS shall send an "REQUEST_GRANTED" reply.

Rationale: By this message, PE or OP is informed that the MBS accepts its request and sends the corresponding Request to Shorten MA message to the OBU.

Guidance: 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.

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

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

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 checks 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: The Risk Buffer related requirements to be considered are the one starting with REQ-SC_RB.

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

6.18 SYSF TRANSLATE MP REQUEST TO MOVEMENT AUTHORITY

6.18.1 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.

6.18.2 Inputs

- Authorised Movement Permission
- *Domain Object* State

6.18.3 Outputs

- Message Movement Authority according to I_OBU

6.18.4 Functional requirements

REQ-0048

When a valid MP Request is received for mode FS and/or OS, 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.

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.

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.

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*.

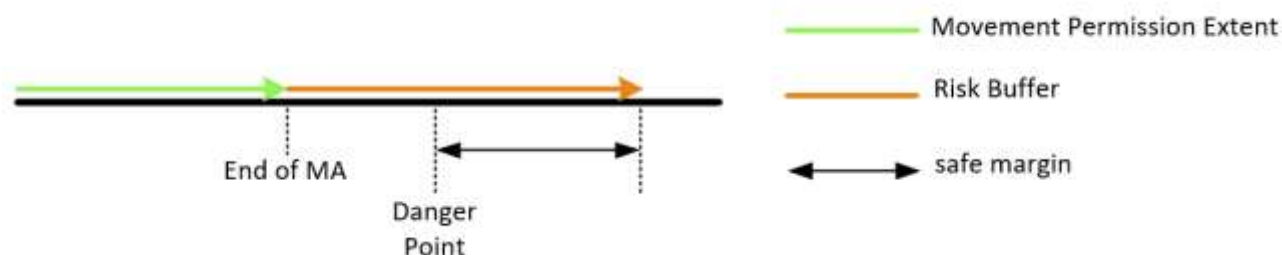
Rationale: The danger point is the Supervised Location that the train shall not overpass. A safe margin is nevertheless added to consider some degraded cases (see Guidance).

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).



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 determination of the Release Speed is Project Specific. 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.

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: MBS can determine that a train is at standstill by checking that the train does not move on consecutive Position Reports.

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.

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.

REQ-0057

The track description (excluding SSP) and linking information included inside the Movement Authority shall correspond to the *Domain Data* and any intersecting applicable *URA*, 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 (from both *Domain Data* and applicable *URA*).
- Optionally route suitability data (from both *Domain Data* and applicable *URA*).

- Optionally changed adhesion factor (from both *Domain Data* and applicable *URA*).

Linking information when available.

Axle load speed profile is ignored here as it will be covered by the SSP in the MBS solution (see REQ-SC_RB_SPEED).

When extending or modifying an existing MA, it is sufficient to only include the modified extended part not yet acknowledged by the OBU.

Track description may be adapted due to capacity constraints (e.g. Subset-040). In this case, the Track description may be refreshed when appropriate by MBS. This adaptation is project specific.

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.

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.

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.

6.19 SYSF TRANSLATE MP REQUEST TO SR AUTHORISATION

6.19.1 Overview

This function converts the authorised Movement Permission for SR mode into a SR Authorisation and transmits it to the on-board.

6.19.2 Inputs

- Authorised Movement Permission for SR mode
- *Domain Object State*

6.19.3 Outputs

- Message SR Authorisation according to I_OBU

6.19.4 Functional requirements

REQ-SR-1

MBS shall send the SR Authorisation resulting from the approved MP Request to the corresponding ETCS on-board equipment according to the I_OBU interface.

Rationale: SR Authorisations are needed to permit trains to move when it is not possible to give a Movement Authority.

Guidance: For a train with an assumed *Train Location*, the SR Authorisation should be long enough to reach at least one balise group.

REQ-SR-2

When MBS sends an SR Authorisation, Message 2, it shall include the authorised SR distance and a Packet 63 with the balises that can be expected within this SR distance.

Rationale: Packet 63 is to safeguard against moving in the wrong track and/or direction.

Guidance: The SR distance is deduced from the MP Request, while the balise groups to be included in Packet 63 are found in topology data (Domain Data) between the start and end of the LinkedPath in the MP Request.

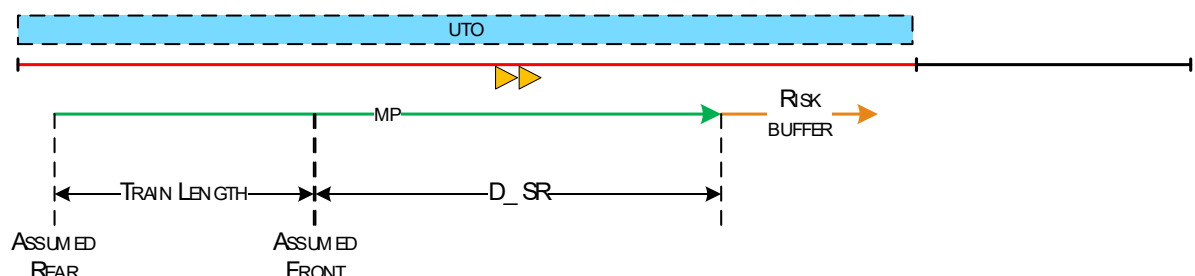
REQ-SR-3

MBS shall calculate the authorised SR distance as the length of the MP extent in the MP Request minus the length of the train stored for the Train Object with the same identity as in this MP Request.

Rationale: This is to limit the distance a train can run in SR mode.

Guidance:

The MP Extent starts at the rear end of the assumed location of the train and extends to the limit of where it is allowed to move in SR. Therefore, the length of the train must be subtracted from the length of the LinkedPath.



REQ-SR-4

MBS shall request the reception of the SR Authorisation message to be acknowledged by the ERTMS/ECS onboard.

Rationale: This is for MBS to know that the message has been received by the train.

Guidance: This is managed by setting the variable M_ACK to '1' in ETCS Message 2.

6.20 SysF TRANSLATE COOPERATIVE SHORTENING REQUEST TO REQUEST TO SHORTEN MA

6.20.1 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.

6.20.2 Inputs

- Authorised Cooperative Shortening Request
- *Domain Object* State

6.20.3 Outputs

- Message Request to Shorten MA according to I_OBU

6.20.4 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.

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.

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.

6.21 SYSF DELETE TRAIN OBJECT

6.21.1 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.

6.21.2 Inputs

- Trigger (by Terminate communication session with OBU)

6.21.3 Outputs

- *Train Object* (removed)
- *Train Location* (removed)
- *Unresolved Trackbound Object*

6.21.4 Functional Requirements

REQ-TrainLoc-10

[X2R5 REQ-TrainLoc-10]

When the communication session with a leading OBU that is reported at standstill is terminated for trackside, then the MBS shall, in the following sequence:

- create an *Unresolved Trackbound Object* corresponding to the *Train Location* extended to the end of the *Movement Permission* (risk buffer included).
- 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. If the train is confirmed at standstill, the *Train Location* and *Movement Permission* are replaced by a UTO and then deleted (End of mission at standstill).

Guidance:

Communication session is terminated for trackside according to /ETCS/ - SUBSET-26 chapter 3.5.5 (session terminated by the onboard) and 3.5.4.2.1 (session timer expires)

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.

Train is considered as reported at standstill only if its position is up to date (i.e., the last Position Report is recent).

Note that if the train is deleted according to the session timer, it should not be considered being at standstill as its position is no longer up to date (i.e. the last Position Report is not recent in this case).

This requirement applies also to a train with an (extended) assumed *Train Location*.

REQ-TrainLoc-18

When the communication session with a leading OBU that is not reported at standstill is terminated for trackside, then the MBS shall, in the following sequence:

- create an *Unresolved Trackbound Object* corresponding to the *Train Location* (risk buffer included).
- store the Train Length (L_TRAIN) in the created *Unresolved Trackbound Object* if the train is marked as integrity confirmed.
- create an *URA* of type “track closure” corresponding to the *Train Location* extended to the *Movement Permission* (Risk Buffer and Risk Paths included).
- create an *URA* of type “non switchable” corresponding to the *Train Location* extended to the end of the *Movement Permission* (Risk Buffer and Risk Paths included) and covering any sTA which served as *Risk Path* terminating element.
- delete the *Train Location* and the *Movement Permission*

Rationale:

URAs are created to avoid any movement and any sTA command in the area allocated to the train when it is deleted, and it is not confirmed standstill.

Guidance:

Communication session is terminated for trackside according to /ETCS/ - SUBSET-26 chapter 3.5.5 (session terminated by the onboard) and 3.5.4.2.1 (session timer expires)

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 and URA will remain.

A leading OBU is an OBU not in SL, NL.

Train is considered as reported at standstill only if the position of the train is up to date (i.e., the last Position Report is recent).

This requirement applies also to a train with an (extended) assumed *Train Location*.

REQ-0065

[X2R5 REQ-TrainLoc-10]

When the communication session is terminated for trackside, then the MBS shall delete the *Train Object*.

Rationale:

The MBS only maintains a *Train Object* for communicating trains.

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.

6.22 SysF SUPERVISE TRAINS AND TRACKSIDE ASSETS

6.22.1 Overview

The purpose of this function is to continuously supervise and monitor for all authorisations issued by MBS whether the previously fulfilled safety-checks are still fulfilled for this authorisation.

6.22.2 Inputs

Update of the MBS Operational State.

6.22.3 Outputs

Indication that a specific safety check is not fulfilled anymore for an authorisation issued by MBS.

6.22.4 Functional requirements

REQ-SUPERVISE

When MBS detects an update of the MBS Operational State, the MBS shall check whether any check (see REQ-SAFETY-MP-REQ) for a Movement Permission is violated by this update of the MBS Operational State and if the check fails, MBS shall revoke or restrict the given authorisation by applying the capability 'Revoke or restrict authorisation'

Rationale: This supervision is necessary to react in case of any violation of a safety-check to prevent or mitigate any hazardous situation, e.g. collision or derailment.

Guidance:

It has to be considered that a train itself may also cause an update of the MBS operational state, e.g. it has been observed by some IMs that a train passing a points causes a lot of vibrations. This can lead to a TACS report indicating that the points is not detected anymore for a short time. Thus, to prevent those cases when they occur, the MBS has to evaluate first whether this has been caused by the train itself or not.

Safety checks are the one defined in chapter 6.16.4.

REQ-SUPERVISE_TRAILED_MOVEMENT

When MBS detects that the reported position of a DPS Group of type point is not equal to the target position without a prior command to move the point, MBS shall create a URA covering the DPS with a *restriction property mode* only allowing mode SH.

Rationale: Except a movement to free point blades from vehicles, no other movement shall be allowed over a previously trailed point until it is cleared for operation again. The movement to free the point blade shall be done in mode SH.

Guidance:

There can be multiple reasons for this event to happen:

- OC-P reports "unintended position"
- OC-P reports "in no end position" without a movement command
- The connection to the OC-P is lost



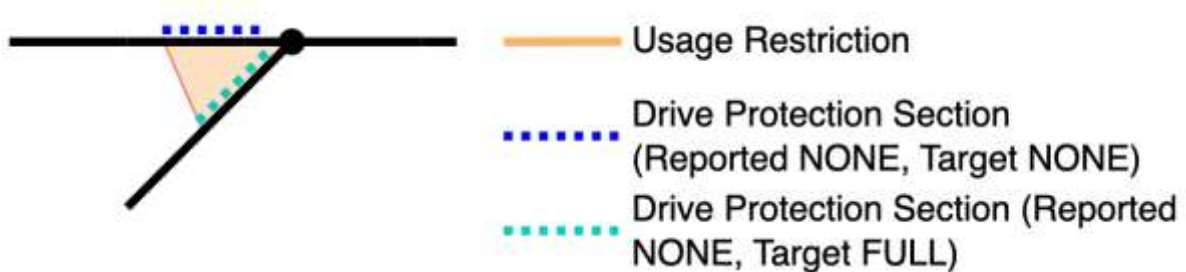
REQ-SUPERVISE_TRAILED_DPSG_DEMAND

When MBS detects that the reported position of a DPS Group of type point is not equal to the target position without a prior command to move the point, MBS shall create a URA covering the DPS with a restriction property *safetyCritical*.

Rationale: A safety critical command is mandatory to move the point.

Guidance: There can be multiple reasons for this event to happen:

- OC-P reports “unintended position”
- OC-P reports “in no end position” without a movement command
- The connection to the OC-P is lost



6.23 SysF REVOKE OR RESTRICT AUTHORISATION

6.23.1 Overview

6.23.1.1 Purpose

The purpose of this function is to revoke or restrict an authorisation previously issued by MBS due to

- a Stop Train Request received via I_OP OR
- MBS has detected that a safety check of a previously issued authorisation by MBS is not fulfilled anymore.
- an activation of a URA

6.23.1.2 Terminology

The term revocation means to completely invalidate the authorisation of a train. After receiving the revocation, a train has no valid authorisation to proceed further on.

The term restriction refers to a modification of the authorisation that:

- Reduces the extent of the trains' authorisation or
- Restricts the track constraints (e.g. speed) within the authorisation.

6.23.1.3 Means for revocation of Movement Authorities

To revoke a Movement Authority, the /CCSTSI/ provides two different solutions:

- A new MA is sent with a new EoA so that the mSFE is located in advance of the EoA when the train receives this new MA. Then the train performs a trip reaction.
- An Unconditional Emergency Stop (UES) is sent to the train. When the train accepts this UES, the train performs a trip reaction.

For revoking a Movement Authority, the MBS should generally use an Unconditional Emergency Stop message, because there are some situations when a train might not accept a Movement Authority (e.g. ETCS-H0019 hazard)

To reduce the extent of the trains' Movement Authority to a specific stop location, the /TSI/ /CCSTSI/ provides two different solutions (which are currently in operation and requested by the IMs)

- A new MA is sent with EoA at the new stop location.
- A Conditional Emergency Stop (CES) is sent with the emergency stop location at the stop location. If the train is in rear of the emergency stop location, the CES is accepted. In case the train has already passed the emergency stop location, the CES is rejected and trackside needs to send an UES to trip the train.

As both technical solutions for reducing the extent have drawbacks, which solution is applied is project specific.

6.23.1.4 Means for revocation of SR Authorisations

To revoke SR Authorisations, the /CCSTSI/ provides only one solution:

- An Unconditional Emergency Stop (UES) is sent to the train. When the train accepts this UES, the train performs a trip reaction.

6.23.2 Inputs

- Stop Train Request via I_OP
- Indication that a specific safety check is not fulfilled anymore for an authorisation issued by MBS
- Activation of URA which affects an already existing authorisation

6.23.3 Outputs

- A restriction or revocation of an authorisation issued by MBS.
 - o Note: In case MBS has detected that a safety check of a previously issued authorisation is violated, then the reaction towards OBU, e.g. CES, UES, a shortened or restrictive MA, etc. may depend on this violated safety check.

6.23.4 Functional requirements

REQ-REVOKE_GENERAL

When MBS has sent a revocation or restriction to the train, then this revocation or restriction has to be continuously repeated until acknowledged by the train.

Rationale:

It is not possible to exclude a message loss / delay on the radio interface and therefore this information needs to be repeated to ensure that the train will receive it.

Guidance: None

REQ-REVOKE_STOPREQUEST_IMMEDIATELY

When MBS has authorised a Stop Train Request received via I_OP indicating no stop location, then MBS shall immediately revoke the authorisation of the train.

Rationale:

MBS shall revoke the authorisation as requested by the Stop Train Request.

Guidance:

In such case the authorisation is usually revoked by sending an Unconditional Emergency Stop message to the train.

REQ-REVOKE_STOPREQUEST_WITH_STOP_LOCATION

When MBS has authorised a Stop Train Request received via I_OP indicating a stop location, then MBS shall immediately shorten the authorisation to the new stop location.

Rationale:

MBS shall shorten the authorisation as requested by the Stop Train Request.

Guidance: None

REQ-REVOKE_VEHICLE_RELATED_SAFETY_CHECK_VIOLATED

When MBS detects that one of the checks contained in chapter 'Vehicle related safety checks' is violated for a granted Movement Permission, then MBS shall revoke or restrict the corresponding authorisation of the train to mitigate or avoid any collision caused due to this overlap.

Rationale:

When one of the 'Vehicle related safety checks' is violated then this means that there is an overlapping of a Movement Permission with another Train Location or an UTO. In this case it cannot be excluded that the object causing the overlap does not move or roll further towards the train itself later on. Therefore, MBS has to revoke or restrict

the authorisation to avoid or mitigate any possible collision caused by such an overlap.

Guidance:

MBS must ensure that the authorisation is either appropriately shortened or invalidated, depending on the situation. For example, triggering an Unconditional Emergency Stop or shortening the authorisation.

REQ-REVOKE_DPS_RELATED_CHECK_VIOLATED

When MBS detects that one of the checks contained in chapter 'DPS related Safety Checks' is violated for a granted Movement Permission, then MBS shall shorten the authorisation so that the train has no authorisation over this DPS anymore.

Rationale:

When one of the 'DPS related Safety Checks' is violated, then a *Switchable Trackside Assets* (in the overrun protection section) is not secured in the correct position for a train movement anymore.

Guidance:

This must not be done if the violation of the corresponding safety check has been caused by the train itself. To ensure this, the function 'Supervise train and trackside

assets' has to evaluate first whether this check has been violated by the train itself or not.

REQ-REVOKE_FLANK_PROTECTION_RELATED_CHECK_VIOLATED

When MBS detects that one of the checks contained in chapter 'Flank protection related Safety Checks' is violated for a granted Movement Permission, then MBS shall shorten the authorisation to the begin of the Allocation Section of the corresponding DPS where the Risk Path, for which the safety check is violated, originates from.

Rationale:

The Allocation Section could be or become occupied by another object and therefore MBS has to shorten the authorisation to the begin of the Allocation Section.

Guidance:

A safety check of the 'Flank protection related Safety Checks' is considered as violated if one of the following conditions are fulfilled:

- The corresponding *Risk Path* is not terminated according to REQ-SC_RP_TERM anymore and it is not possible to recalculate the risk path successfully according to REQ-RP_SEARCH-MP.
- The corresponding *Risk Path* has an overlap (acc. to REQ-0077) and it is not possible to recalculate the risk path successfully according to REQ-RP_SEARCH-MP

It is project specific whether MBS shall perform this check and the corresponding reaction as in some countries today the 'Flank protection related Safety Checks' are only performed at the time when granting the authorisation.

REQ-REVOKE_URA_RELATED_CHECK_VIOLATED

When MBS detects that one of the checks contained in chapter 'URA related Safety Checks' is violated for a granted Movement Permission and the URA

- demands a speed which is less than the speed of the respective part of the MP Speed Profile OR
- demands a mode which is different from the mode in the respective part of the MP Mode Profile OR
- demands being non-passable,

then MBS shall update the authorisation so that the corresponding check is fulfilled again.

Rationale:

When one of the 'URA related Safety Checks' is violated, then a constraint provided by the *URA* is not ensured anymore.

Guidance:

The specific reaction of the MBS depends on the type of violation, e.g.

- In case the URA demands a speed, which is less than the speed of the respective part of the speed profile of the Movement Permission, then MBS shall send an updated authorisation considering the speed of the URA.
- In case the URA demands being non-passable, then the MBS shall shorten the authorisation to the begin of the URA, respectively unconditionally stop the train in case the train is already inside the URA.
- In case the URA requires to apply a Track Condition or a Route Suitability, MBS shall update the authorisation considering this track condition, respectively route suitability.

REQ-REVOKE-OTHER_CHECK_VIOLATED

When MBS detects that another check than mentioned in the requirements

- REQ-REVOKE_VEHICLE_RELATED_SAFETY_CHECK_VIOLATED
- REQ-REVOKE_DPS_RELATED_CHECK_VIOLATED
- REQ-REVOKE_FLANK_PROTECTION_RELATED_CHECK
- REQ-REVOKE_URA_RELATED_CHECK_VIOLATED

is violated, then MBS shall immediately revoke the authorisation of the train.

Rationale:

Due to the definition of the checks, it is not possible that any of those other checks is violated after having issued an authorisation based on an MP Request. But for robustness reasons, this requirement is introduced as an additional safety-net.

Guidance: None

REQ-Revoke-SR-Unknown-Loc

MBS shall revoke an SR authorisation for a train if its assumed *Train Location* is deleted on request from OP.

Rationale: This is to stop a train which is moving in an unexpected location.

Guidance: SR authorisations can only be revoked by Unconditional Emergency Stop. In case the *assumed Train Location* is deleted due to the train performing End of Mission, then there is no need to revoke the SR Authorisation.

REQ-Revoke-SR-Outside-MP

MBS shall revoke an SR authorisation for a train if it reports a known position which is not within its given SR authorisation.

Rationale: This is to stop a train which is moving in an unexpected location.

Guidance: SR authorisations can only be revoked by Unconditional Emergency Stop.

REQ-Revoke-SR-Wrong-Direction

MBS shall revoke an SR authorisation for a train if it reports a known position which is in the opposite direction of its given SR authorisation.

Rationale: This is to stop a train which is moving in the opposite direction.

Guidance: SR authorisations can only be revoked by Unconditional Emergency Stop.

6.24 SysF AUTHORISE STOP TRAIN REQUEST

6.24.1 Overview

This function is responsible to assess the safety of a request to stop a train (at a certain location). The MBS shall not alter the request if certain parameters are incorrect but only report the failure to OP with the failure reason.

The Stop Train Request shall contain the following information:

- *Train Object* Identifier
- Optional: Stop Location

6.24.2 Inputs

- Stop Train Request message according to I_OP
- *Domain Object* State

6.24.3 Outputs

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

6.24.4 Functional requirements

REQ-SAFETY-STOPREQUEST

The MBS shall perform a series of checks given by the following ordered list when it receives a Stop Train Request indicating a request to stop a train (at a certain location) through I_OP:

1. REQ-GENERAL_SYNTAX
2. REQ-GENERAL_EXISTANCE
3. REQ-STOPREQUEST_VALID_MODE
4. REQ-STOPREQUEST_LOCATION_IN_REAR_OF_EOA

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

Guidance: This is the top requirement for all necessary checks.

REQ-STOPREQUEST-FAILS

The MBS shall abort checking a Stop Train Request received through I_OP 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

REQ-STOPREQUEST-SUCCESSFUL

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

Rationale: By this message, OP is informed that the MBS has accepted its request and continues with executing this request.

Guidance: None

REQ-STOPREQUEST_AUTH_GRANTED

The MBS shall check that in case the Stop Train Request does not contain a stop location that the train is in a mode in which an Unconditional Emergency Stop message (UES) is accepted by the train.

Rationale: In case the Stop Train Request does not contain a Stop Location, an UES is used by MBS to revoke the authorisation (if any). The UES is accepted by the train not in all modes according to chapter 4.8.4 in Subset-026 in /ETCS/.

Guidance: None

REQ-STOPREQUEST_LOCATION_IN_REAR_OF_EOA

In case the Stop Train Request contains a stop location, the MBS shall check that the stop location is located within the currently stored Movement Permission Extent for this train and if the check fails, the MBS shall send a STOPREQUEST_NOT_IN_REAR reject code.

Rationale: The referenced stop location of the Stop Train Request has to within the Movement Permission to revoke or restrict the authorisation.

Guidance: None

6.25 SysF AUTHORISE RELEASE STOP TRAIN REQUEST

6.25.1 Overview

When it has been triggered to stop a train (at a certain) location by the OP via the Stop Train Request, the MBS won't issue any authorisation (with the exception of more restrictive authorisations) to this train anymore until this request has been released by the OP again. This function is responsible to release this command. After the request has been released, the MBS is allowed to issue authorisations to the corresponding train again.

The Release Stop Train Request shall contain the following information:

- *Train Object* Identifier

6.25.2 Inputs

- Release Stop Train Request message according to I_OP
- *Domain Object* State

6.25.3 Outputs

- Message "request granted" according to I_OP
- Message "request rejected" according to I_OP

6.25.4 Functional requirements

REQ-SAFETY-RELEASESTOPREQUEST

The MBS shall perform a series of checks given by the following ordered list when it receives a Release Stop Train Request indicating a request to release a previously authorised Stop Train Request for a train.

1. REQ-GENERAL_SYNTAX
2. REQ-GENERAL_EXISTANCE
3. REQ-RELEASESTOPREQUEST

Rationale: See checks.

Guidance: This is the top requirement for all necessary checks.

REQ-RELEASESTOPREQUEST-FAILS

The MBS shall abort checking a Release Stop Train Request received through I_OP 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

REQ-RELEASESTOPREQUEST-SUCCESSFUL

If none of the safety checks fails, MBS shall send an "REQUEST_GRANTED" reply.

Rationale: By this message, OP is informed that the MBS has accepted its request and continues with executing this request.

Guidance: None

REQ-RELEASESTOPREQUEST

The MBS shall check that MBS has already executed a Stop Train Request for the Train Object referenced in the Release Stop Train Request which has not been released yet and if the check fails, the MBS shall send a "RELEASE_STOPTRAIN_NOT_POSSIBLE" reject code.

Rationale: The request can be only released if a Stop Train Request has been previously executed for this train which has not been released yet.

Guidance: None

6.26 SysF UPDATE MOVEMENT PERMISSION

6.26.1 Overview

This function stores the Movement Permission in the *MBS Operational State* when MBS has granted the corresponding request. Additionally, this function updates a Movement Permission when necessary.

6.26.2 Inputs

- *Train Location*
- *Granted MP Request*
- “Request to shorten MA is granted message” according to I_OBU
- “Request to Shorten MA is rejected message” according to I_OBU

6.26.3 Outputs

- Movement Permission
- Message “Cooperative MP Request Granted” according to I_PE/I_OP
- Message “Cooperative MP Request Rejected” according to I_PE/I_OP

6.26.4 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

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

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: When applying this requirement, it must be ensured that wheel/rail adhesion is adequately considered.”

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

REQ-0080²

When MBS has successfully shortened the authorisation of a train, then MBS shall include the corresponding Stop Location in the Movement Permission until a new MP Request or Cooperative Shortening Request is accepted by MBS for this train.

Rationale: This stop location is used to inform the PE that the authorisation does not extend up to the end of the Movement Permission anymore.

Guidance: The MBS has successfully shortened the authorisation of a train, if the function ‘Revoke or restrict an authorisation’ has been completely executed.

REQ-0079

When there is an update of the Train Location indicating the entry into mode PT, then MBS shall delete the Movement Permission.

Rationale: All current MA and track description data are deleted onboard during the transition to TR mode according to /ETCS/ SS026 5.11.2.2 and the train is at standstill in PT mode.

Guidance: None

6.26.5 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-MP.

Rationale: Flank Protection is not needed anymore if the *Allocation Section* does not overlap the path anymore.

Guidance: 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-MP.

Rationale: If the risk mitigation method is not valid anymore, MBS shall search if other appropriate measures are still in place.

Guidance: 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-MP.

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: None.

6.27 SysF CHECK TTD SECTION FAILURE STATUS

6.27.1 Overview

When the MBS receives a failure status message via I_TACS, it has to evaluate if the conditions are fulfilled to reset the TTD section in failure by its own automatically or if the Operator has to be involved.

Hint: TTD Section (MBS) and TVPS (Track Vacation Proving Section / EULYNX) are describing the same piece of track. TTD (MBS) and TDS (EULYNX) are describing the same track occupancy proving functionality.

6.27.2 Inputs

- Msg_TVPS_Occupancy_Status via I_TACS with Occupancy Status = disturbed and Disturbance Status = Disturbance is operational
- *Train Integrity* state

6.27.3 Outputs

- MBS Domain Object State and
- Reset Qualifier

6.27.4 Functional Requirement

REQ-0081

For a system using TTD, when receiving a Msg_TVPS_Occupancy_Status

- with
 - Occupancy Status = disturbed and
 - Disturbance Status = Disturbance is operational and
- if applicable, while
 - a granted Movement Permission Extent spanning over the disturbed TTD section is not yet released and
 - the Train Object is
 - located in the disturbed section or
 - has already passed the disturbed section

the MBS shall release the used parts of the concerning Movement Permission Extent according to REQ-0071 before setting the Reset Qualifier to “manual” with a reference to the disturbed TTD section as referenced TA if REQ-0082 does not set the Reset Qualifier to “automatic”.

Rationale:

The MBS checks if the TTD section can be reset automatically. Before this is possible MBS shall wait until an eventually granted MP is released behind the train for which this MP is issued. This prevents unnecessary manual action before automatic reset is checked by MBS or before, if applicable, the supervision section of the TTD system can reset the disturbed section by its own.

See also Rationale of REQ-0082.

Guidance:

The reset qualifier is only for sorting purpose in the resetting process and only for requirement writing purpose. How this is solved in the MBS product is up to the supplier. It is up to the infrastructure manager or, if delegated, the supplier to specify which a manual TTD section request is possible for the operator.

If the message `Msg_TVPS_Occupancy_Status` with "Occupancy Status = disturbed" is received before the train, for which an MP exists spanning over the disturbed section, has entered the disturbed section, this shall be handled as incident and a safety reaction shall apply. The Reset Qualifier is set to "manual".

A disturbed TTD section can be operational in case of fail counting, means count one (or more) axles out of the section than counting previously in. Means typical -1 axle counting. A fail counting in the sense of having one axle left in the TTD section is then applicable in most cases in the very next TTD section next to -1 section. But having one axle left has to be assumed as not detected as disturbed by the TTD system. Detecting both cases is not part of MBS specification, for further information see /EULYNX/.

REQ-0082

For a system using TTD, when receiving a `Msg_TVPS_Occupancy_Status`

- with
 - Occupancy Status = disturbed and
 - Disturbance Status = Disturbance is operational and
 - Ability to be forced to clear = TVPS is able to be forced to clear and

- the *Train Integrity* of the very last previously *Train Object* passing the TTD section, before or while *Msg_TVPS_Occupancy_Status* is received, is confirmed and
- the disturbed TTD section is configured sweepable

the MBS shall set the Reset Qualifier to “automatic” with a reference to the disturbed TA representing the disturbed TTD section.

Rationale:

After receiving a message about a disturbed TTD section, MBS has to decide, whether all conditions are given for an automatic reset of the disturbed section or if the operator has to be involved due to safety reasons. The conditions given here are unique, so that an automatic reset by MBS is possible.

Guidance:

See REQ-0081

Out of Eu.Doc.43 “Requirement Specification for Subsystem TDS” the TTD system has to be configured as follows:

TTD system has to be configured with Variant B according to Eu.TDS.7152

TTS system has to be configured with *Con_t_Inhibition_Timer* according to Eu.TDS.1212 not greater than the Position Report time interval configured in MBS

When a TTD section is branching, it shall be configured sweepable, when there is no possibility to place vehicles (of any kind) between the TTD section border and the branching point (Axle counter has to be placed as nearest to the fouling point indicator).

REQ-0089

While Reset Qualifier is “manual”, MBS shall only be configured using one of the following three options:

1. REQ-0085 and REQ-0090 (SysF Reset TTD section by Operator) or
2. REQ-0086 and REQ-0091 (SysF Supported Reset of TTD section by Operator) or

3. REQ-0092 and REQ-0093 (SysF Reset of TTD section by Operator using Sweeping).

Rationale:

After receiving a message about a disturbed TTD section and the operator has to be involved due to safety reasons, the one of the three options have to be chosen which fits best into the given operational and safety framework of the infrastructure manager.

Guidance:

The reset qualifier is only for sorting purpose in the resetting process and only for requirement writing purpose. How the requirements linked in the MBS product is up to the supplier. It is up to the infrastructure manager or, if delegated, the supplier to specify which manual TTD section request is possible for the operator.

6.28 SysF RESET TTD SECTION BY MBS

6.28.1 Overview

When all conditions of REQ-0082 are given the MBS can reset TTD section without any operator interaction.

6.28.2 Inputs

Reset qualifier is “automatic”

6.28.3 Outputs

Reset message via I_TACS

TVPS is free and non-disturbed

6.28.4 Functional Requirement

REQ-0083

If configured, when Reset Qualifier for the referenced TA is detected “automatic”, MBS shall send “Cd_FC(FC-C)” to the referenced TA.

Rationale:

When all conditions are given, MBS shall relieve the operator and reset the failing TTD section by its own. As this is only for distinguished situations, this function can be chosen by MBS configuration.

Guidance:

An automatic reset is only possible in a very specific situation. One essential condition is the ability of the TTD section to be forced clear.

6.29 SysF RESET TTD SECTION BY OPERATOR

6.29.1 Overview

When at least one condition is not fulfilled of REQ-0082 the MBS cannot reset TTD section without operator interaction. The operator has to check if the TTD section is clear by operational measures without any support of MBS.

6.29.2 Inputs

Reset qualifier is “manual”

6.29.3 Outputs

Reset message via I_TACS

TVPS is free and non-disturbed

6.29.4 Functional Requirement

REQ-0085

If configured, when receiving Reset_TTD_Section request and

- Reset Qualifier is detected “manual” and
- Ability to be forced to clear of the referenced TA is “TVPS is unable to be forced to clear” and
- the checks
 - REQ-GENERAL_SYNTAX and
 - REQ-GENERAL_EXISTANCE are successful,

MBS shall send command Cd_DRFC via I_TACS to the referenced TA.

Rationale:

MBS shall support manual reset in case of reported TVPS failure. These requirements are smallest possible technical support. The check if it is permitted to reset the TTD section is fully up to the operator.

Guidance:

If the Ability to be forced to clear of the referenced TA is “TVPS is unable to be forced to clear” MBS command the TACS of the TTD section to deactivate the restriction to be forced clear without any further input from the Operator Panel.

The operator shall take operational measures to ensure, that the disturbed TTD section is physically free (no train in it, no further obstacle). If integrity of the previously passed train is confirmed (by train driver or via Position Report), this could be done by sending an explorer train.

REQ-0090

If configured, when receiving Reset_TTD_Section request and

- Reset Qualifier is detected “manual” and
- Ability to be forced to clear of the referenced TA is “TVPS is able to be forced to clear” and
- the checks
 - REQ-GENERAL_SYNTAX and
 - REQ-GENERAL_EXISTANCE are succesfull,

MBS shall send command Cd_FC (FC-C) via I_TACS to the referenced TA.

Rationale:

MBS shall support manual reset in case of reported TVPS failure. This requirement and REQ-0085 are the smallest possible technical support. The check if it is permitted to reset the TTD section is fully up to the operator.

Guidance:

No guidance necessary.

6.30 SysF SUPPORTED RESET OF TTD SECTION BY OPERATOR

6.30.1 Overview

When at least one condition is not fulfilled the MBS cannot reset TTD section without operator interaction. The operator has to prove if the TTD section is clear by operational measures. MBS supports this with technical measures: Add a URA to not allow MP with mode FS and use operational sweeping for the TTD section reset.

6.30.2 Inputs

Reset qualifier is “manual”

6.30.3 Outputs

Reset message via I_TACS

TVPS is free and non-disturbed

6.30.4 Functional Requirement

REQ-0086

If configured, when receiving Reset_TTD_Section request and

- Reset Qualifier is detected “manual” and
- Ability to be forced to clear of the referenced TA is “TVPS is unable to be forced to clear”

REQ-0085 applies.

Rationale:

See REQ-0085.

Guidance:

See REQ-0085.

REQ-0091

If configured, when receiving Reset_TTD_Section request and

- Reset Qualifier is detected “manual” and
- Ability to be forced to clear of the referenced TA is “TVPS is able to be forced to clear” and
- the checks
 - REQ-GENERAL_SYNTAX and
 - REQ-GENERAL_EXISTANCE are successful,

MBS shall

- send command Cd_FC (FC-C) via I_TACS to the referenced TA and
- create a pre-configured URA over to the full extent of the disturbed TTD section which prevents MBS to grant any MP request with mode FS (restriction property: mode ≠ FS).

Rationale:

As a further option MBS shall support releasing a disturbed TVPS. For this all movements in Full Supervision shall be prevented. This shall force PE and the operator to request only movements in a mode that requires train drivers' attention to supervise that the track is free.

Guidance:

Deletion of URA shall be done by Operator and according to REQ-DEL_URA_DO

- The operator shall take operational measures to ensure, that the disturbed TTD section is physically free (no train in it, no further obstacle). If integrity of the previously passed train is confirmed (by train driver or via Position Report), this could be done by sending an explorer train.
- Explorer train after resetting the TTD section has to be authorised to move in mode On Sight only.
- REQ-CR_URA_DO in 6.35 SysF Create URA has to be used to create the URA.

- If the TTD system allow supervisor section, this shall be used instead: if the counting failure occurs in an area of two sections which have in total a balanced number of axles counted, counting failure can be reset within the TTD system.

6.31 SysF RESET OF TTD SECTION BY OPERATOR USING SWEEPING

6.31.1 Overview

When at least one condition is not fulfilled the MBS cannot reset TTD section without operator interaction. The operator has to check if the TTD section is clear by operational measures. MBS supports this with technical measures: TTD section can only be reset by using an explorer train.

6.31.2 Inputs

Reset qualifier is “manual”

6.31.3 Outputs

Reset message via I_TACS

TVPS is free and non-disturbed

6.31.4 Functional Requirement

REQ-0092

If configured, when receiving Sweeping_TTD_Section request and

- Reset Qualifier is detected “manual” and
- the checks
 - REQ-GENERAL_SYNTAX and
 - REQ-GENERAL_EXISTANCE are successful,

MBS shall send a command Cd_FC (FC-P-A) to the referenced TA.

Rationale:

Before resetting the TTD section, the operator shall firstly authorise an explorer train using mode On Sight only and ask the train driver to confirm that the track is free. Using Cd_FC (FC-P-A), the operator is forced to send an explorer train to use the TTD system capability of sweeping.

Guidance:

An explorer train has to be authorised to move in mode On Sight only.

If the TTD system allow supervisor section, this shall be used instead: if the counting failure occurs in an area of two sections which have in total a balanced number of axles counted, counting failure can be reset within the TTD system.

REQ-0093

If configured, when receiving a Sweeping_TTD_Section (Acknowledgement) request and the checks

- REQ-GENERAL_SYNTAX and
- REQ-GENERAL_EXISTANCE

are successful, MBS shall send a command Cd_FC (Acknowledgement after FC-P-A command) to the reference TA.

Rationale:

After the explorer train swept the TTD section the operator has to confirm, that the train left the concerning TTD section with confirmed integrity.

Guidance:

No guidance necessary.

6.32 SysF SUPERVISE<ACTOR>COMMUNICATION

Hint: <Actor> is a template for DR, TACS, PE, and OBU

6.32.1 Overview

This function supervises the communication state to the actor <actor>. It can detect, if the communication is established or lost (a communication never established is also considered as 'lost'), and if there is change lost -> established or established -> lost.

6.32.2 Inputs

State of communication session between *MBS* and actor <actor>

6.32.3 Outputs

Events

- <actor>CommEstablished or
- <actor>CommLost

6.32.4 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 communication 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*.

6.33 SysF ESTABLISH<ACTOR>COMMUNICATION

Hint: *<Actor>* is a template for DR and TACS.

6.33.1 Overview

This function establishes the communication state to the actor *<actor>* according to the related communication protocol.

6.33.2 Inputs

None

6.33.3 Outputs

(Changed) communication session state to *<actor>*.

6.33.4 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*.

6.34 SysF AUTHORISE CREATE URA

6.34.1 Overview

This function checks if the *URA* fulfils a number of checks. If so, the *URA* can be created in the *Operational State* (see SysF *Create URA*) and a grant response is sent. Otherwise, a reject response is sent.

6.34.2 Inputs

- *Create URA Request* message according to I_PE or I_OP
- *Create URA Demand* according to I_OP

6.34.3 Outputs

- *Request Granted/Request Rejected* messages according to I_PE or I_OP
- *Demand Granted/Demand Rejected* messages according to I_OP

6.34.4 Functional requirements

REQ-SAFETY-CR_URA

The MBS shall perform a series of checks given by the following ordered list when it receives a *Create URA Request* message:

- a. REQ-GENERAL_SYNTAX
- b. REQ-GENERAL_EXISTANCE
- c. REQ-CR_URA_INCOMP

Rationale: The request to create a *URA* shall be safeguarded.

Guidance: This is the top requirement for all necessary checks.

REQ-SAFETY-CR_URA_DEMAND

The MBS shall perform a series of checks given by the following ordered list when it receives a *Create URA Demand* message:

- a. REQ-GENERAL_SYNTAX
- b. REQ-GENERAL_EXISTANCE

Rationale: The demand to create a *URA* skip the incompatibility check. This means that if the *URA* is not compatible with an existing *MP*, the *URA* is created and an emergency reaction will be applied to the train according to REQ-SUPERVISE.

Guidance: This is the top requirement for all necessary checks.

REQ-CR_URA_INCOMP

When receiving a valid (REQ-GENERAL_SYNTAX, REQ-GENERAL_EXISTANCE) *Create URA Request* message AND there exists a *Movement Permission (MP)* intersecting the *URA* extent AND the *URA*

- demands a speed which is less than speed of the respective part of the *MP Speed Profile* (restriction property *speed*), OR
- demands a mode which is different from the mode in the respective part of the *MP Mode Profile* (restriction property *mode*), OR
- demands being non-passable (restriction property *noPassage*) OR
- demands not to stop (restriction property *eaExclusion*) but the EoA would be within the *URA* extent OR
- demands manual operation (restriction property *manualOperation*)

then *MBS* shall send the *Request Reject* message with “INCOMPATIBLE_MP” reject code.

Rationale: A Create URA request should not cause a safety reaction. So, the request is rejected to avoid the application of safety reaction due to the violation of REQ-SC_MP_URA.

Guidance:

If an intersecting but compatible *MP* exist, further URA effects will not affect these *MPs*, as required URA effects only become effective with the next *MP* requests (SysF *Translate MP Request to Movement Authority* for Track Conditions/Route Suitability or SysF *Authorise MP Request* for total closure or EoA exclusion).

If the Operator accepts a safety reaction due to the creation of the URA, he can use a Create URA Demand which by-pass the current check.

REQ-0097

If none of the checks fails, MBS shall send a *Request/Demand Granted* reply.

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

Guidance: None

6.35 SysF CREATE URA

6.35.1 Overview

This function creates a *URA* in the *Operational State*, after the request to create a *URA* was granted (SysF *Authorise Create URA*).

6.35.2 Inputs

- *Create URA* message according to *URA Creation Request* or *URA Creation demand*

6.35.3 Outputs

- None (but see SysF *Report MBS Operational State*)

6.35.4 Functional requirements

REQ-CR_URA_DO

When receiving a valid *Create URA* message which is finally not rejected after further checks, then MBS shall create a corresponding *URA* in the *Operational State*.

Rationale: None

Guidance: This will also lead to the notification on the update of the *Operational State* by *SysF Report MBS Operational State*.

6.36 SYSF AUTHORISE DELETE URA

6.36.1 Overview

This function checks if the request fulfils a number of checks. If so, the *URA* is removed from the *Operational State* (see *SysF Delete URA*) and a grant response is sent. Otherwise, a reject response is sent.

At this time (edition of the document) there are no further checks foreseen prior to deletion which could be done by *MBS*. That could change in a next edition as in general, deletion is safety-critical as the lifting of a restriction might require preconditions (like track worker acknowledgement). This is currently out of scope and delegated to the operator (note below).

Note that it is only allowed that an operator (so on the *I_OP* interface), taking over responsibility, deletes a *URA*; it cannot be deleted by *PE* (on the *I_PE* interface the message does not exist).

6.36.2 Inputs

- *Delete URA Request* message according to *I_OP*

6.36.3 Outputs

- *Request Granted/Request Rejected* messages according to *I_OP*

6.36.4 Functional requirements

REQ-SAFETY-DEL_URA

The *MBS* shall perform a series of checks given by the following ordered list when it receives a *Delete URA Request* message:

1. REQ-GENERAL_SYNTAX
2. REQ-GENERAL_EXISTANCE
3. REQ-RM_URA_DEL_INVALID

Rationale: The request to create a *URA* shall be safeguarded.

Guidance: This is the top requirement for all necessary checks.

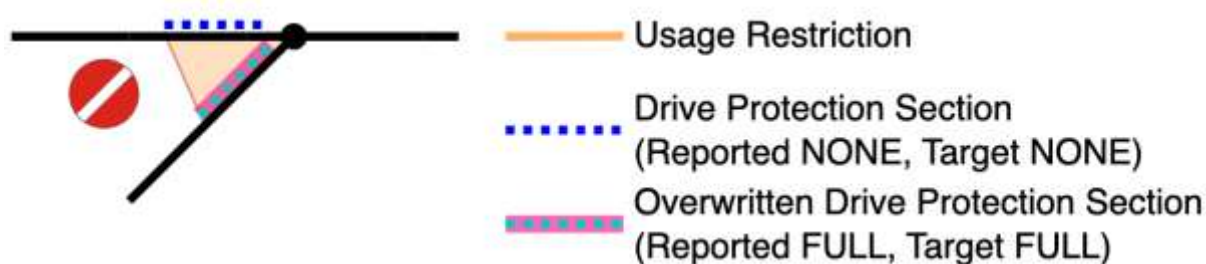
REQ- RM_URA_DEL_INVALID

When receiving a *Delete URA* message from *OP* where

- the *URA* overlaps a *DPS*
- and the restriction property equals *nonSwitchable*

- and the DPS Group the DPS belongs to is currently in the state *overwrite* the MBS shall send the *Request Rejected* message with “DPSG_OVERWRITTEN” reject code.

Rationale: When the state of the DPS Group is overwritten, the state must not be changed. The URA responsible for this behaviour must not be removed.



Guidance: None

REQ-0096

If none of the checks fails, MBS shall send a *Request Granted* reply.

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

Guidance: None

6.37 SysF DELETE URA

6.37.1 Overview

This function deletes the *URA* from the *Operating State*.

Note: It is up to *PE* to request afterwards a new *MP* without the *URA*'s effect (e.g. again a higher speed) if it needs so.

6.37.2 Inputs

- *Delete URA Request* message according to I_OP

6.37.3 Outputs

None (but see SysF Report MBS Operational State)

6.37.4 Functional requirements

REQ-DEL_URA_DO

When receiving a valid *Delete URA Request* message which is finally not rejected after further checks, then MBS shall delete the corresponding *URA* Domain Object.

Rationale: None

Guidance: This will also lead to the notification on the update of the Operational State by SysF Report *MBS Operational State*.

6.38 PROVIDE SH CONFIRMATION REQUEST

6.38.1 Overview

This function is responsible to provide an SH Confirmation Request to PE and OP when receiving a Request for Shunting message from OBU.

The SH Confirmation Request shall contain the following information:

- *Train Object* Identifier

6.38.2 Inputs

- Request for Shunting message according to I_OBU.

6.38.3 Outputs

- Message “SH Confirmation Request” according to I_PE or I_OP

6.38.4 Functional requirements

REQ-SHCONFREQUEST

The MBS shall send an SH Confirmation Request message to PE and OP if MBS receives a Request for Shunting message from an OBU.

Rationale: This request needs to be confirmed either by PE or OP before allowing any movement in mode SH.

Guidance: None

6.39 AUTHORISE SHUNTING

6.39.1 Overview

This function is responsible for either allowing or rejecting the transition to mode SH when it receives the response from PE/OP based on a previous SH Confirmation Request.

6.39.2 Inputs

- Message “SH Request Confirmed” according to I_PE or I_OP
- Message “SH Request Rejected” according to I_PE or I_OP

6.39.3 Outputs

- SH Authorised according to I_OBU
- SH Refused according to I_OBU

6.39.4 Functional requirements

REQ-SHCONFIRMED

The MBS shall send SH Authorised to OBU when MBS receives a Shunting Request Confirmed message from PE or OP.

Rationale: The answer of PE and OP indicates that MBS is allowed to confirm the SH request previously issued by the OBU.

Guidance: None

REQ-SHREFUSED

The MBS shall send SH Refused to OBU when MBS receives a Shunting Request Rejected message from PE or OP.

Rationale: The answer of PE and OP indicates that MBS is not allowed to confirm the SH request previously issued by the OBU and thus SH Refused has to be indicated to the OBU.

Guidance: None

6.40 SYSF AUTHORISE SP REQUEST

6.40.1 Overview

This function is responsible to assess the safety of a request to authorise a *Shunting Permission*.

The *Shunting Permission Request* message shall contain the following information:

- *Shunting Permission* extent

6.40.2 Inputs

- SP Request message according to I_OP

6.40.3 Outputs

- Message “request granted” according to I_OP
- Message “request rejected” according to I_OP
- Authorised *Shunting Permission*

6.40.4 Functional requirements

REQ-SAFETY-SP-REQ

The MBS shall perform a series of checks given by the following ordered list when it receives an SP Request from PE or OP:

1. REQ-GENERAL_SYNTAX
2. REQ-GENERAL_EXISTANCE
3. REQ-TOPO1
4. REQ-TOPO2
5. REQ-TOPO3
6. REQ-TOPO-SP1
7. REQ-TOPO-SP2
8. REQ-TOPO-SP3
9. REQ-SC_SP_TO
10. REQ-SC_SP_MP
11. REQ-SC_SP_RB
12. REQ-SC_SP_RP
13. REQ-SC_SP_SP
14. REQ-SC_SP_TO_AS
15. REQ-SC_SP_MP_AS
16. REQ-SC_SP_RB_AS
17. REQ-SC_SP_SP_AS
18. REQ-SC_SP_DPS
19. REQ-SC_SP_URA
20. REQ-RP_SEARCH-SP
21. REQ-SC_RP_TERM

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

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

REQ-SP-REQ-ABORT

The MBS shall abort checking an SP Request 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 the request 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.

REQ-SP-REQ-GRANTED

If none of the safety checks for a SP Request fails, MBS shall send an "SP_REQUEST_GRANTED" reply.

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

Guidance: None

REQ-TOPO-SP1

The MBS shall check the *Shunting Permission* starts at a shunting signal.

Rationale:

Guidance: None

REQ-TOPO-SP2

The MBS shall check the *Shunting Permission* end at a

- shunting signal
- OR a *Shunting Limit*
- OR at a Buffer Stop

Rationale: A shunting permission must end at a defined location that is also comprehensible for the shunting personnel.

Guidance: None

REQ-TOPO-SP3

The MBS shall check that there is no shunting signal along the *Shunting Permission*.

Rationale: The current concept for shunting in mode SH does not allow shunting signals "in transit"

Guidance: It is possible to combine several Shunting Permissions in sequence but they have to be requested individually.

REQ-SC_SP_TO

The MBS shall check that, if the global variable *spToOverlapAllowed* is set to FALSE, the Shunting Permission in the request does not overlap a Train Object, and if the check fails, the MBS shall send a “PATH_OCCUPIED” reject code.

Rationale: Depending on the accepted risk, a shunting movement is allowed to shunt into a train object

Guidance:

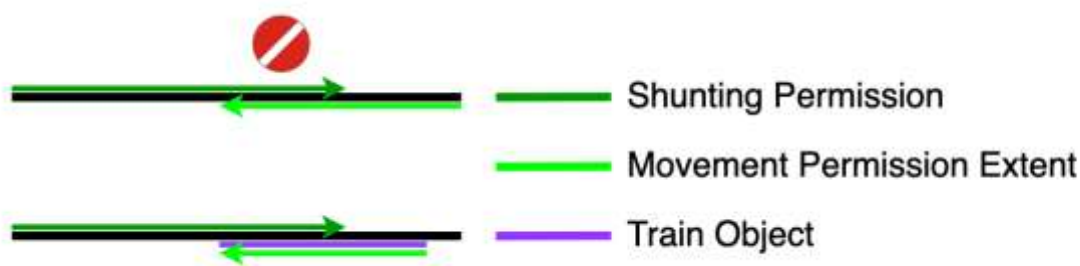


REQ-SC_SP_MP

The MBS shall check that the Shunting Permission does 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: A shunting movement shall not collide with another train.

Guidance:



REQ-SC_SP_RB

The MBS shall check that the *Shunting Permission* extent does not overlap with a *Risk Buffer* and if the check fails, the MBS shall send an “EXTENT_CONFLICT” reject code.

Rationale: A shunting movement shall not collide with another train.

Guidance:



REQ-SC_SP_RP

The MBS shall check that if the global variable *rpTermAllowedAtRbAndMp* is set to FALSE, the *Shunting Permission* extent does not overlap with a *Risk Path* 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:



REQ-SC_SP_SP

The MBS shall check that the *Shunting Permission* extent does not overlap with a *Shunting Permission* and if the check fails, the MBS shall send an “EXTENT_CONFLICT” reject code.

Rationale: A shunting movement shall not collide with another shunting movement.

Guidance:



Note: even if opposite Shunting Permissions are allowed in some countries, this is not allowed by MBS in the current release.

REQ-SC_SP_TO_AS

The MBS shall check that if the *Shunting Permission* extent overlaps an *Allocation Section*, all mutually exclusive *Allocation sections* shall not have an overlap with the extent of a *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.

REQ-SC_SP_MP_AS

The MBS shall check that any *Allocation Section* the *Shunting Permission* extent overlaps with, shall not have another overlap with a *Movement Permission Extent* in all mutually exclusive *Allocation Sections* and if the check fails, the MBS shall send EXTENT_AS_CONFLICT” reject code.

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

Guidance:



REQ-SC_SP_RB_AS

The MBS shall check that any *Allocation Section* the *Shunting Permission* extent overlaps with, shall not have another overlap with a *Risk Buffer* in all mutually exclusive *Allocation Sections* and if the check fails, the MBS shall send EXTENT_AS_CONFLICT” reject code.

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

Guidance:



REQ-SC_SP_SP_AS

The MBS shall check that any *Allocation Section* the *Shunting Permission* extent overlaps with, shall not have another overlap with a *Shunting Permission* Extent in all mutually exclusive *Allocation Sections* and if the check fails, the MBS shall send EXTENT_AS_CONFLICT” reject code.

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

Guidance:

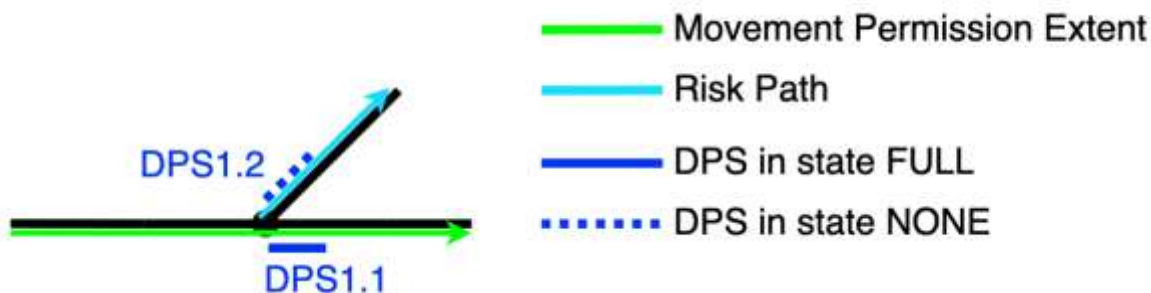


REQ-SC_SP_DPS

The MBS shall check that all DPS that overlap with the *Shunting 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 shunting movement.

Guidance:



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

REQ-SC_SP_URA

When receiving an *SP Request* message where the *Shunting Permission* overlaps a *URA* AND the *URA*

- forbids the mode SH (restriction property *mode*), OR
- demands being non-passable (restriction property *noPassage*) OR
- demands manual operation (restriction property *manualOperation*) but the request was received from PE

then *MBS* shall respond with *Request Rejected* message with reject code "MP_URA_CONFLICT".

Rationale: None

Guidance: None

REQ-RP_SEARCH-SP

If the global configuration variable *fpSearchForSp* 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 *Shunting 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_SHUNT_SIG
- 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: See REQ-RP_SEARCH-SP

6.41 SysF UPDATE SHUNTING SIGNAL

6.41.1 Overview

This function ensures the correct signalling after a *Shunting Permission* was authorised.

Note: this function excludes the setting to stop of a shunting Signal which is covered by function “SysF Set Shunting Signal to Stop”.

6.41.2 Inputs

- Domain Object State

6.41.3 Outputs

See I_TACS

6.41.4 Functional requirements

REQ-SIG-1

The MBS shall update the target signal aspect according to REQ-SIG-3, REQ-SIG-4, REQ-SIG-5 and REQ-SIG-6 when a *Shunting Permission* starts at a shunting signal and the signal is settable.

Rationale: After a *Shunting Permission* is granted, the shunting signal shall reflect the new state.

Guidance: None

REQ-SIG-2

The MBS shall set the shunting signal to not settable after the target state of the shunting signal was updated.

Rationale: A *Shunting Permission* must be removed before a signal can be cleared again.

Guidance: The signal aspect sent can also be stop.

REQ-SIG-3

If the *Shunting Permission* starting at the shunting signal overlaps a URA of type *preventSignalAspect*, MBS shall set the target aspect of the signal to stop.

Rationale: In some cases, only a route shall be secured but no immediate authorisation through a signal aspect shall take place,

Guidance: This example applies after a point has been trailed and the vehicle is to be removed, and the permission is only to be given through a written permission, but the

path shall be secured whatsoever. Setting the signal to not settable is still to be carried out.

REQ-SIG-4

If the global configuration variable *useCautionAndProceed* is set to FALSE, MBS shall set the target aspect to *proceed*.

Rationale: If there is only one aspect allowing a movement, there is no need to distinguish.

Guidance: Some countries do not use shunting signals with different signal aspects.

REQ-SIG-5

If the global configuration variable *useCautionAndProceed* is set to TRUE, MBS shall set the target state to *proceed* if

- the *Shunting Permission* ends at a shunting signal whose target and reported state is not equal to *stop*
- AND the *Shunting Permission* does not overlap a UTO
- AND the *Shunting Permission* does not overlap a *Train Object*
- AND the *Shunting Permission* does not overlap a URA of type *preventProceed*

Rationale: In order to show a proceed aspect, the following signal must show caution or proceed and there must be no expected obstacles.

Guidance: None

REQ-SIG-6

If the global configuration variable *useCautionAndProceed* is set to TRUE, MBS shall set the target state to *caution* if

- the *Shunting Permission* overlaps a URA of type *preventProceed*
- OR the *Shunting Permission* overlaps a UTO
- OR the *Shunting Permission* overlaps a *Train Object*
- OR the *Shunting Permission* ends at a target signal whose target state is *stop*

Rationale: If a *Shunting Permission* ends at a shunting signal showing stop or an obstacle is to be expected, the signal aspect is limited to caution

Guidance: The signal aspect sent can also be stop.

REQ-SIG-7

If the global configuration variable *useCautionAndProceed* is set to TRUE, MBS shall set the target state of a shunting signal to *proceed* if

- the *Shunting Permission* ends at a shunting signal whose target state was updated to *proceed* or *caution*
- AND the target and reported signal state of that shunting signal are equal
- AND the *Shunting Permission* did not overlap a URA of type *preventProceed* after the *Shunting Permission* was granted
- AND the *Shunting Permission* did not overlap a UTO after the *Shunting Permission* was granted
- AND the *Shunting Permission* did not overlap a *Train Object* after the *Shunting Permission* was granted

Rationale: When a *Shunting Permission* is prolonged, the shunting signals in rear can be updated to *proceed* if there was never a vehicle within this *Shunting Permission*.

Guidance: None

6.42 SysF UPDATE SHUNTING PERMISSION

6.42.1 Overview

This function stores the Shunting Permission in the MBS Operational State when MBS has granted the corresponding request- Additionally, this function updates a Shunting Permission after MBS receives a state change of the Trackside Train Detection System

6.42.2 Inputs

- Granted SP Request
- *TVPS Occupancy Status* or *TDP status* message according to I_TACS

6.42.3 Outputs

None (but see SysF Report MBS Operational State)

6.42.4 Functional requirements

REQ-USP-1

After MBS has granted a Shunting Permission, it shall store the new Shunting Permission in the *MBS Operational State*.

Rationale: A Shunting Permission has to be stored in the *MBS Operational State*.

Guidance: None

REQ-USP-2

After receiving a *TVPS Occupancy Status* or *TDP Status* message through I_TACS and

- a *TVPS Occupancy Status* message with status “TVPS is in state occupied” was received followed by a *TVPS Occupancy Status* message with status “TVPS is in state free” for the rearmost TVP section of a *Shunting Permission*
- AND a *TDP Status* message with status “passed” with a reference direction matching the direction of the *Shunting Permission* was received for both TDP covered by the *Shunting Permission*
- AND no *TDP Status* message with status “passed” with a reference direction opposite the direction of the *Shunting Permission* was received for any TDP covered by the *Shunting Permission*
- AND a *TDP Status* message with status “not passed” was received for both TDP covered by the *Shunting Permission*
- AND the rearmost TVP section is not overlapping a URA with the restriction property *preventAutomaticShuntingRouteRelease*

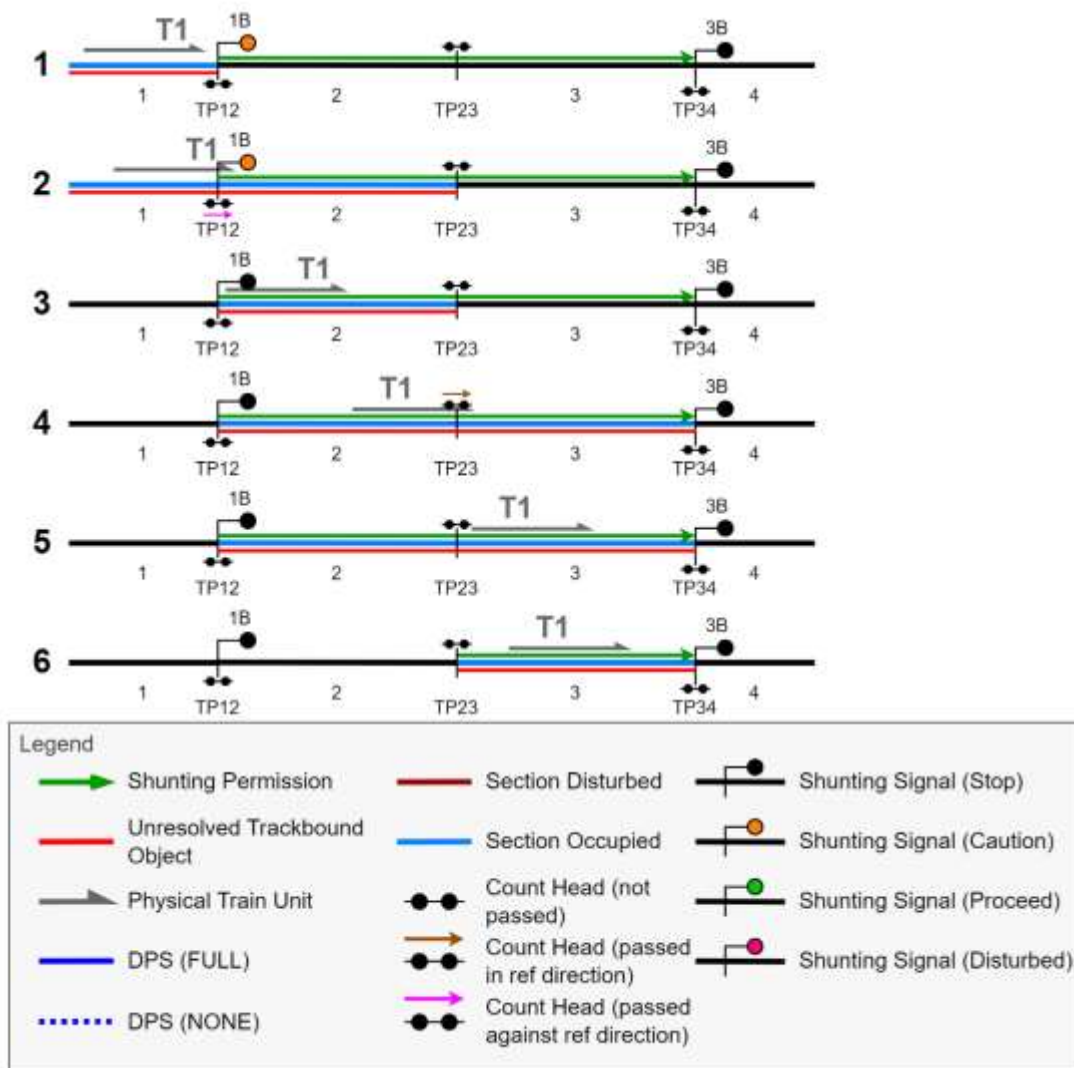
, MBS shall shorten the rear end of a *Shunting Permission* so that the new rear end of the *Shunting Permission* is at the next border of a section that does not yet satisfy the conditions above.

Rationale: A section of a *Shunting route* shall only be automatically removed if the desired movement was carried out. This is given when the rearmost section was occupied followed by being freed and a vehicle passing all TDP along the

Shunting Permission. Additionally when shunting with dangerous goods, the automatic route release must be prevented for security reasons.

Guidance:

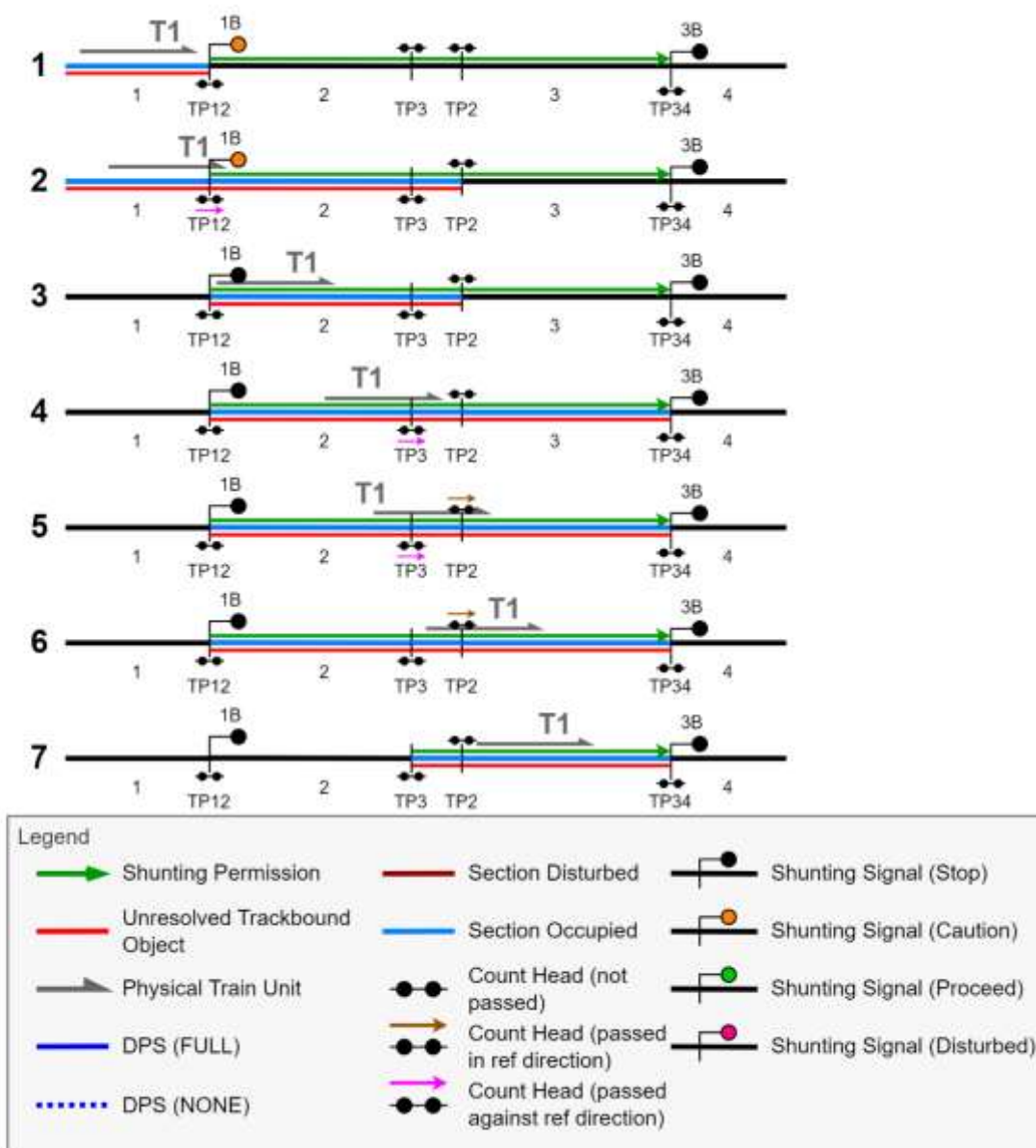
Scenario 1 Regular shunting, not overlapped sections



Depending on the rail where the count head is mounted, the reference direction of the axle counter changes. As in the example above the reference direction from TP12 and TP23 is different although the train runs in the same direction. Further note that

after the train has passed TP23 completely the time until TP23 reports not passed is shorter than for section 2 reporting vacant again.

Scenario 2 Regular shunting, overlapping sections



In this scenario the count heads for sections 2 and 3 are overlapping each other.

REQ-USP-3

After receiving a *TVPS Occupancy Status* or *TDP Status* message through I_TACS and a *Shunting Permission* ends

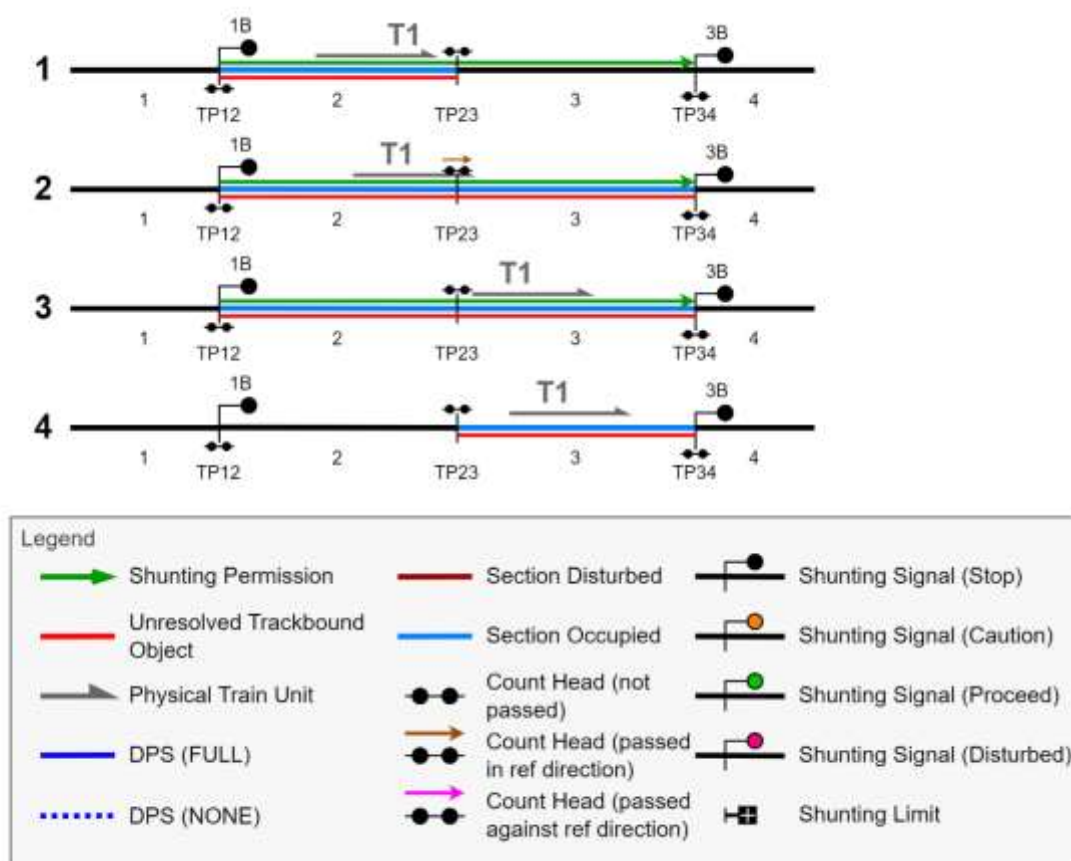
- at a shunting signal where the attribute *automaticallyReleaseLastPartOfShuntingPermission* is set to TRUE
 - OR at a *Shunting Limit*

- OR at a Buffer Stop
- AND a *TVPS Occupancy Status* message with status “TVPS is in state occupied” was received for the last TVP section of this *Shunting Permission*
- AND a *TDP Status* message with status “passed” with a reference direction matching the direction of the *Shunting Permission* was received for the TDP of the last TVP section of this *Shunting Permission*
- AND the last TVP section is not overlapped with a URA having the restriction property *preventAutomaticShuntingRouteRelease*

, MBS shall remove the *Shunting Permission*.

Rationale: Under certain circumstance the rest of a shunting permission shall be automatically removed.

Guidance:



REQ-USP-4

After receiving a *TVPS Occupancy Status* or *TDP Status* message through I_TACS but before applying SysF “Set Shunting Signal to Stop” and

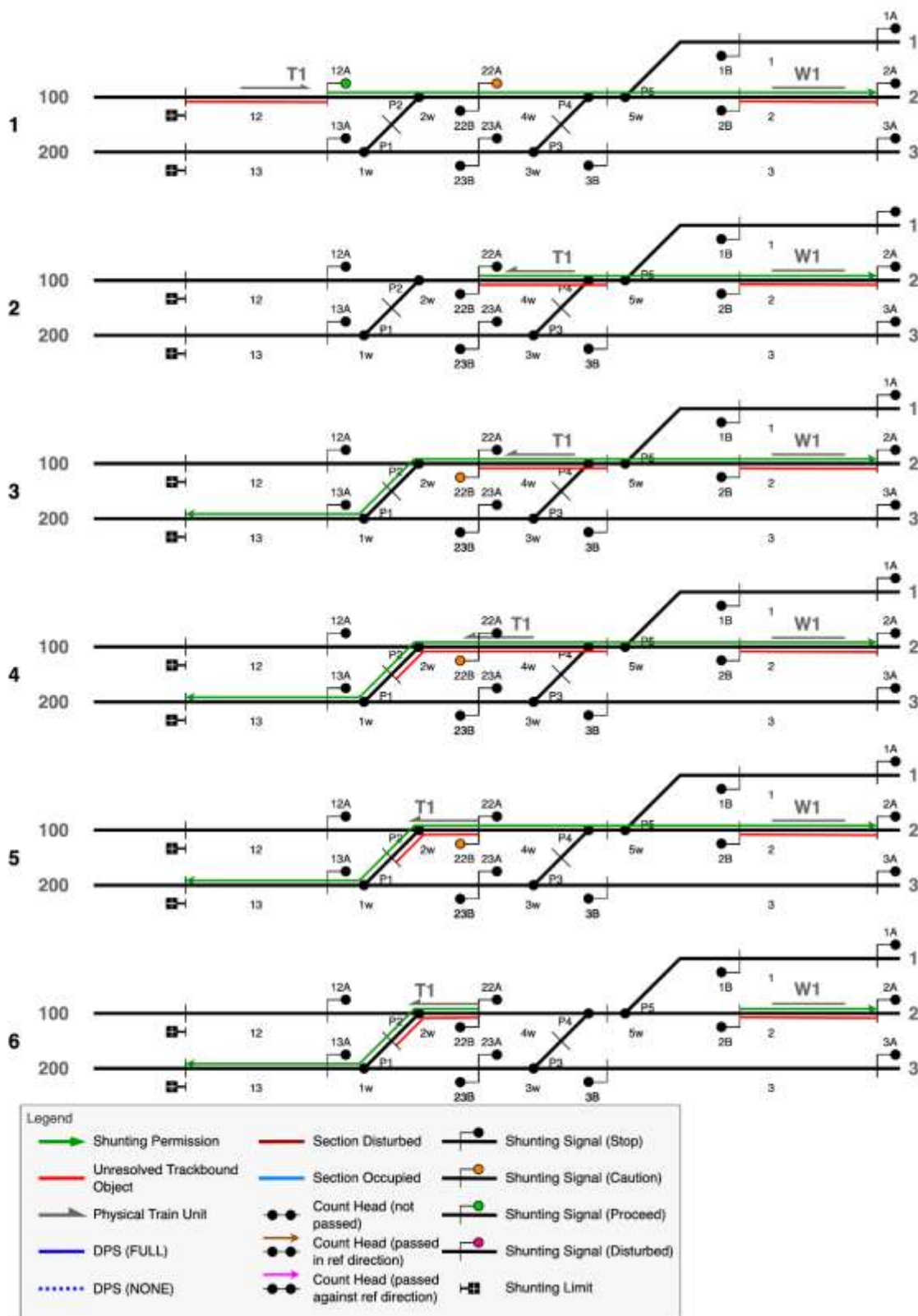
- a *Shunting Permission 1* starts at a shunting signal and is in the same direction as that shunting signal

- AND the rear end of another *Shunting Permission 2* is in the same place into the opposite direction
- AND the shunting signal at the start of *Shunting Permission 1* is showing a signal aspect that is not equal to stop
- AND a *TVPS Occupancy Status* message with status “TVPS is in state occupied” was received followed by a *TVPS Occupancy Status* message with status “TVPS is in state free” for the rearmost TVP section of *Shunting Permission 2*
- AND a *TVPS Occupancy Status* message with status “TVPS is in state occupied” was received for the rearmost TVP section of *Shunting Permission 1*
- AND a *TDP Status* message with status “passed” with a reference direction matching the direction of the *Shunting Permission 1* was received for the TDP at the *Shunting Signal*
- AND a *TDP Status* message with status “not passed” was received for the TDP at the *Shunting Permission*
- AND the rearmost TVP section of *Shunting Permission 1* and *Shunting Permission 2* is not overlapping a URA with the restriction property *preventAutomaticShuntingRouteRelease*

, MBS shall remove *Shunting Permission 2* up to a section that is occupied by a UTO or the whole *Shunting Permission* if there is no overlap between *Shunting Permission 2* and a UTO,

Rationale: When a shunting movement is turning and the secured path on the first movement is not carried out completely, the first movement can be removed as long as there is no other chance of a moving

Guidance:



DPS and Flank Protection not shown for clarity reasons.

6.43 SYSF AUTHORISE SHUNTING SIGNAL STOP DEMAND

6.43.1 Overview

This function is responsible to assess the safety of a demand to set a shunting signal to stop.

The Shunting Signal Stop Demand message shall contain the following information:

- *Shunting Signal Identifier*

6.43.2 Inputs

- Shunting Signal Stop Demand message according to I_OP

6.43.3 Outputs

- Message “demand granted” according to I_OP
- Message “demand rejected” according to I_OP

6.43.4 Functional requirements

REQ-ESTOP-1

The MBS shall perform a series of checks given by the following ordered list when it receives an *Shunting Signal Stop Demand* message from OP:

1. REQ-GENERAL_SYNTAX
2. REQ-GENERAL_EXISTANCE

Rationale: The request to set a shunting signal to stop shall be safeguarded.

Guidance: None

REQ-ESTOP-2

If none of the checks fails, MBS shall send a *Demand Granted* reply.

Rationale: OP shall be informed about the successful check of the demand.

Guidance: None

REQ-ESTOP-3

If one of the checks fails, MBS shall send a *Demand Rejected* reply.

Rationale: OP shall be informed about the unsuccessful check of the demand.

Guidance: None

6.44 SYSF SUPERVISE SHUNTING PERMISSION

6.44.1 Overview

This function supervises the *Shunting Permissions* and reacts to a violation of safety checks

6.44.2 Inputs

- Domain Object State

6.44.3 Outputs

- Domain Object State

6.44.4 Functional requirements

REQ-SUPERVISE_SP-1

When MBS detects that one of the checks contained in chapter 'DPS related safety checks' is violated for a granted *Shunting Permission*, then MBS shall set the target aspect of

- the shunting signal related to this *Shunting Permission* AND
- each shunting signal related to a consecutive connected *Shunting Permission* in rear of this *Shunting Permission*
- to stop.

Rationale: A shunting signal shall show a stop aspect if there is a violation of related *Shunting Permission*. Additionally, also the shunting signals of the consecutively connected *Shunting Permissions* in rear have to be set to 'Stop' to react in a safe manner.

Guidance: None

REQ-SUPERVISE_SP-2

When MBS detects that one of the checks not contained in chapter 'DPS related safety checks' is violated for a granted *Shunting Permission*, then MBS shall set the target aspect of

- the shunting signal related to this *Shunting Permission* AND
- each shunting signal related to a consecutive connected *Shunting Permission* in rear of this *Shunting Permission*
- to stop.

Rationale: A shunting signal shall show a stop aspect if there is a violation of related *Shunting Permission*. Additionally, also the shunting signals of the consecutively

connected *Shunting Permissions* in rear have to be set to 'Stop' to react in a safe manner.

Guidance: None

6.45 SysF SET SHUNTING SIGNAL TO STOP

6.45.1 Overview

This function sets a shunting signal to the stop aspect.

6.45.2 Inputs

- Domain Object State
- Successful request in SysF Authorise Set Shunting Signal to Stop

6.45.3 Outputs

See I_TACS

6.45.4 Functional requirements

REQ-SIG_STOP-1

After an *Shunting Signal Stop Demand* has been authorised, MBS shall send an *Indicate Signal Aspect* message with a stop signal aspect through I_TACS.

Rationale: After the demand has been authorised, the trackside asset is to be updated.

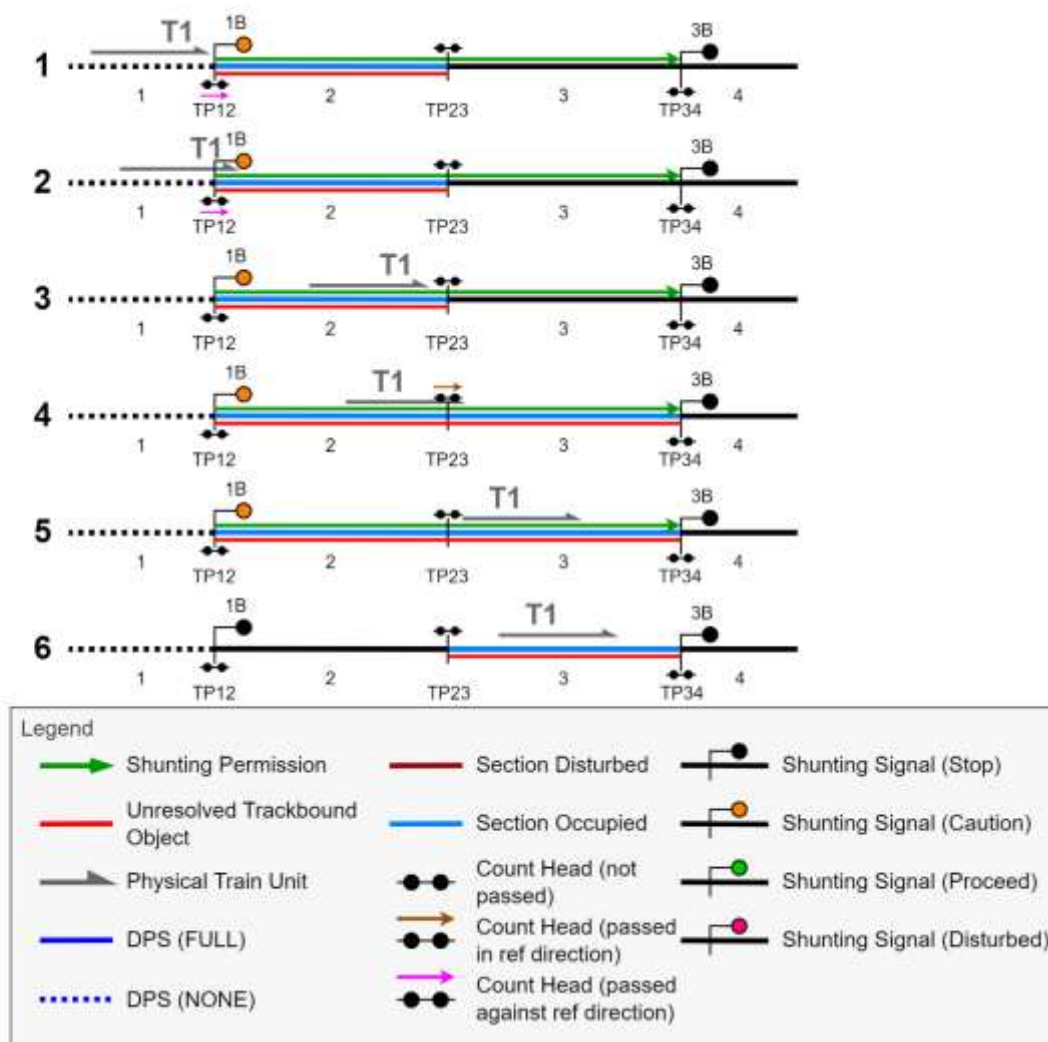
Guidance: None

REQ-SIG_STOP-2

MBS shall send an *Indicate Signal Aspect* message with a stop signal aspect through I_TACS if the target state of the shunting signal is not equal to a stop aspect and no *Shunting Permission* starts at the shunting signal.

Rationale: A signal shall show a stop aspect if no shunting permission is covering the path behind the signal.

Guidance:



Note: section 1 is not supervised in the figure.

REQ-SIG_STOP-3

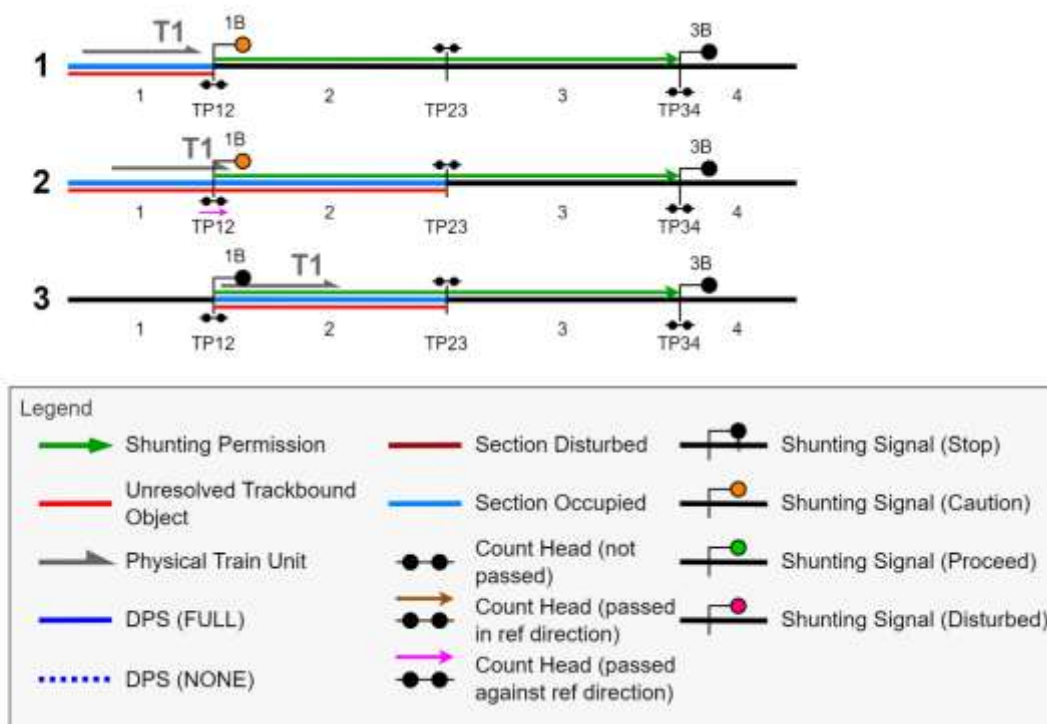
After receiving a *TVPS Occupancy Status* or *TDP Status* message through I_TACS and

- a *TVPS Occupancy Status* message with status “TVPS is in state occupied” was received followed by a *TVPS Occupancy Status* message with status “TVPS is in state free” for the section in rear of the shunting signal
- AND a *TDP Status* message with status “passed” with a reference direction matching the direction of the shunting signal was received for the TDP at the shunting signal location

, MBS shall send an *Indicate Signal Aspect* message with a stop signal aspect through I_TACS

Rationale: After the shunting unit has passed the shunting signal, it shall be set to stop as soon the shunting unit has fully passed the signal.

Guidance:



Note: last wheel replacement is systematically applied to always allow propelling movement in SH (driver will still see the signal at Proceed or Caution in this case).

Remaining risk: another SH train could follow the first one and still see the SH signal showing Proceed or Caution.

REQ-SIG_STOP-4

MBS shall set the state of a shunting signal to settable if the indicated signal aspect is stop and no *Shunting Permission* starts at the shunting signal.

Rationale: After the shunting permission is removed, the signal can be cleared again.

Guidance: None

6.46 SysF AUTHORISE REVOKE SP DEMAND

6.46.1 Overview

This function is responsible to assess the safety of a request to revoke a *Shunting Permission*.

The purpose of this revocation is either:

- to remove the permission before a train has passed the signal, or
- to remove the Shunting Permission when the shunting movement has been completed.

The Revoke SP Demand message shall contain the following information:

- *Shunting Permission Identifier*

6.46.2 Inputs

- Revoke SP Demand message according to I_OP

6.46.3 Outputs

- Message “Demand Granted” according to I_OP
- Message “Demand Rejected” according to I_OP

6.46.4 Functional requirements

REQ-ARSP-1

The MBS shall perform a series of checks given by the following ordered list when it receives an *Revoke SP Demand* message from OP:

1. REQ-GENERAL_SYNTAX
2. REQ-GENERAL_EXISTANCE
3. REQ-RSP-SC_SIG_STOP

Rationale: The request to set a shunting signal to stop shall be safeguarded.

Guidance: None

REQ-ARSP-2

If none of the checks fails, MBS shall send a *Demand Granted* reply.

Rationale: OP shall be informed about the successful check of the demand.

Guidance: None

REQ-ARSP-3

If one of the checks fails, MBS shall send a *Demand Rejected* reply.

Rationale: OP shall be informed about the unsuccessful check of the demand.

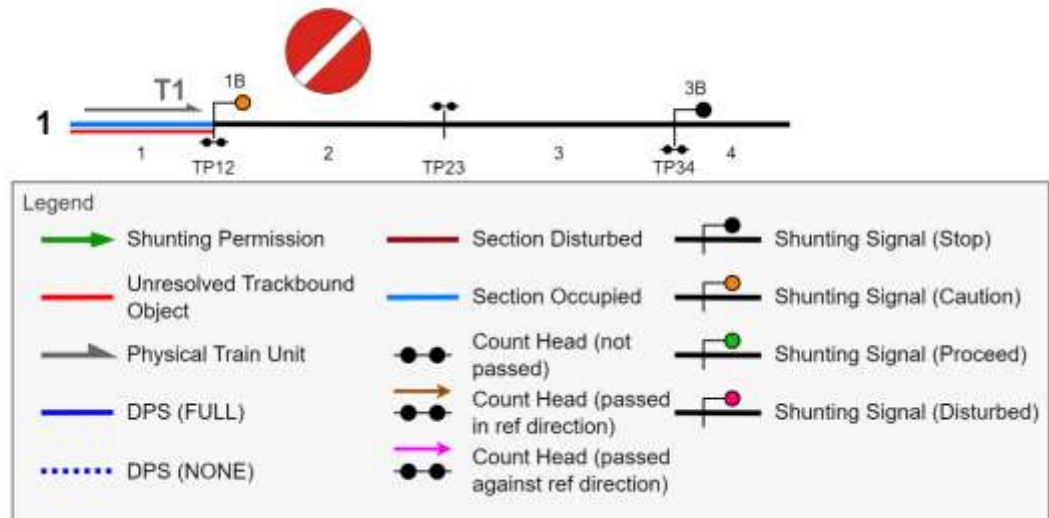
Guidance: None

REQ-ARSP-SC_SIG_STOP

The MBS shall check that the Shunting Permission that is to be removed does not start at a shunting signal whose current state is not equal to stop and if the check fails, the MBS shall send an "SIGNAL_NOT_STOP" reject code.

Rationale: A shunting signal has to be set to stop before the *Shunting Permission* is removed.

Guidance:



Operational Rules: None

6.47 SysF REVOKE SHUNTING PERMISSION

6.47.1 Overview

This function revokes a *Shunting Permission* after the demand has been authorised.

6.47.2 Inputs

- Successful request in SysF Authorise Revoke SP Demand

6.47.3 Outputs

None (but see SysF Report MBS Operational State)

6.47.4 Functional requirements

REQ-RSP-1

After a *Revoke SP Demand* has been authorised, MBS shall delete the *Shunting Permission* from its *Operational State*.

Rationale: After the demand has been authorised, the *Shunting Permission* can be removed.

Guidance: 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.

7.1.3 Physical level

Not applicable, as the hardware definition of MBS is out 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

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

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

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

REQ-0026

The application layer of the I_TACS interface shall be compliant with /SCI-TDS/ for Train Detection System.

Rationale: None

Guidance: None

7.1.6 Input Application Layer Messages

- EULYNX telegrams from TACS Point:
 - Msg_Point_Position : Message “Point Position”
 - Msg_Movement_Failed : Message “Movement Failed” (note: this message is not used by MBS)
 - Msg_Ability_To_Move_Point : Message “Ability To Move Point” (note: this message is not used by MBS)
- EULYNX telegrams from TACS Train Detection System:
 - Msg_TVPS_Occupancy_Status : Message “TVPS_Occupancy_Status”
 - Msg_TDP_Status : Message “TDP_Status”
- EULYNX telegrams from TACS Shunting Signal:
 - Msg_SIG_INDICATED_SIGNAL_ASPECT : Message “Indicated Signal Aspect”

7.1.7 Output Application Layer Messages

- EULYNX telegrams to TACS Point:
 - Cd_Move_point : Command “Move Point”
- EULYNX telegrams to TTD system
 - Cd_DRFC: Command to “Disable the restriction to force section status to clear”
 - Cd_FC (FC-C): Command to “Force section status to clear, conditional”
 - Cd_FC (FC-P-A): Command to “Force section status to clear, preparatory, with acknowledgement”
- EULYNX telegrams from TACS Shunting Signal:

7.1.8 Cd_INDICATE_SIGNAL_ASPECT : Message “Indicate Signal Aspect” 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.

7.2.2 Overview

In the current version of the specifications, only the application layer messages are listed.

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

- This request triggers a TA command to a TACS

MP Request

- This request defines the start and end for a Movement Permission.

Cooperative Shortening Request

- This request triggers a Request to Shorten MA message to the OBU

Create URA Request

- This request creates a Usage Restriction Area

Shunting Request Confirmed

- This message indicates that a previous Shunting Confirmation Request has been confirmed by OP or PE for a train.

Shunting Request Rejected

- This message indicates that a previous Shunting Confirmation Request has been rejected by OP or PE for a train.

Shunting Permission Request

- This request defines the start and end for a Shunting Permission

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)

Cooperative MP Request Granted

Cooperative MP Request Rejected

MBS Operational State Report (Object Id, reported state)

Shunting Confirmation Request

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.

7.3.2 Overview

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).

7.3.3 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

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

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 Permissions* and if there is no conflict, establishes a *Usage Restriction Area* to keep the updated area free of future *Movement Permissions* 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 Assets*)
- 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

- Parameter: header
- Parameter: 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

7.5.1 Role of the external interface

The interface I_OP allows the operator to manage and monitor train movements and Trackside Assets. In particular, the interface I_OP is used to:

- Manage Usage Restriction Areas (URAs)
- Issuing requests to stop trains (at a certain location)
- Request an assumed Train Position for a train indicated with unknown or ambiguous position
- Request the deletion of an assumed Train Position for a specific train
- Request SR Authorisation for a train indicated with an assumed position
- Confirming or rejecting a shunting confirmation request
- Request a *Shunting Permission*
- Set a shunting signal to stop

MBS provides the MBS Operational Status to the OP via the interface I_OP.

7.5.2 Overview

In the current version of the specifications, only the application layer messages are listed.

7.5.3 Physical level

Not applicable

7.5.4 Protocol level

Out of scope for this Release

7.5.5 Application level

Out of scope for this Release

7.5.6 Input Application Layer Messages

Request for an assumed Train Position

- This request defines the assumed position for a train with unknown or ambiguous position and the position is given together with a direction, an (optional) offset from its reference and whether the front of the associated train is in the same direction as the referenced position.

Request for deletion of an assumed Train Position

- This request deletes the assumed position for the train identified in the message.

MP Request for SR Authorisation

- This request defines the start and end for a Movement Permission in SR mode.

Stop Train Request

- This request may optionally contain a stop location at which the train has to be stopped.
- In case no stop location is contained this request indicates to unconditionally stop the train.

Release Stop Train Request

- This request is used to release a previously issued Stop Train Request and thus allowing MBS to issue authorisations to this train again.

Create URA Request

- This request creates a Usage Restriction Area

Create URA Demand

- This demand creates a Usage Restriction Area

Delete URA Request

- This request deletes a Usage Restriction Area

Reset_TTD_Section

- This request is up to prepare the release (send Cd_DRFC, if necessary) and triggers the release command towards TTD system (send Cd_FC (FC-C)).

Sweeping_TTD_Section

- This request triggers the release command towards TTD system (send Cd_FC (FC-P-A)).

Sweeping_TTD_Section (Acknowledgement)

- This request triggers the acknowledgement command towards TTD system (send Cd_FC (Acknowledgement after FC-P-A command)).

Shunting Request Confirmed

- This message indicates that a previous Shunting Confirmation Request has been confirmed by OP or PE for a train.

Shunting Request Rejected

- This message indicates that a previous Shunting Confirmation Request has been rejected by OP or PE for a train.

Shunting Permission Request

- This request defines the start and end for a Shunting Permission

Shunting Signal Stop Demand

- This demand requires a SH Signal to indicate a stop aspect

7.5.7 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)

This message indicates that a previous request has been rejected by MBS.

Demand Granted (request id)

This message indicates that a demand has been successfully granted by MBS and is now being processed.

Demand Rejected (request id, reason)

This message indicates that a previous demand has been rejected by MBS.

MBS Operational State Report (Object Id, reported state)

This message reports the state of an given object.

Shunting Confirmation Request

This message requests the PE or OP to confirm a Request for Shunting Message received from a train to allow the mode change to SH.

7.5.8 Implicit choices and justification

Not applicable

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

/BalnCon/	Basic interoperability constituents in the Control-Command and Signalling Trackside Subsystem Table 5.2 in Legal framework of /CCSTSI/
/SysDef/	R2DATO D14.4 – 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
/IF_CCS_OTHSUB/	ERTMS/ETCS UNIT Interfaces between Control-Command and Signalling Trackside and other Subsystems Version 5.0 https://www.era.europa.eu/system/files/2023-09/index077 - _ERA_ERTMS_033281_v5.pdf
/OPETSI/	Operation and Traffic Management TSI Commission Implementing Regulation (EU) 2019/773 of 16 May 2019 Commission Implementing Regulation (EU) 2023/1693 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?d ocumentIds=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/baseline-set-4-release-2/

/SD1DM/	SPT2-Transversal Systems 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, <i>Risk Path</i>)
/SempR2/	SEMP Annex R2 - Requirements patterns syntax
/SempR3/	SEMP Annex R3 - Rules for writing textual requirements

ANNEX 1: TEMPLATES

SysC: System Capability Template

Table 24 - 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)	<ul style="list-style-type: none"> - <Precondition1> - <Precondition...> - <Precondition n> <p>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)</p>
Postcondition(s) (Success)	<ul style="list-style-type: none"> - <Postcondition 1> - <Postcondition...> - <Postcondition n> <p>Note: Only show postconditions which are visible for external actors</p>
Postcondition(s) (Failure)	<ul style="list-style-type: none"> - <Postcondition 1> - <Postcondition...> - <Postcondition n> <p>Note: Only show postconditions which are visible for external actors</p>
Involved actor(s)	<ul style="list-style-type: none"> - <Actor 1> - <Actor...> - <Actor n>
Trigger(s)	<ul style="list-style-type: none"> - <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”

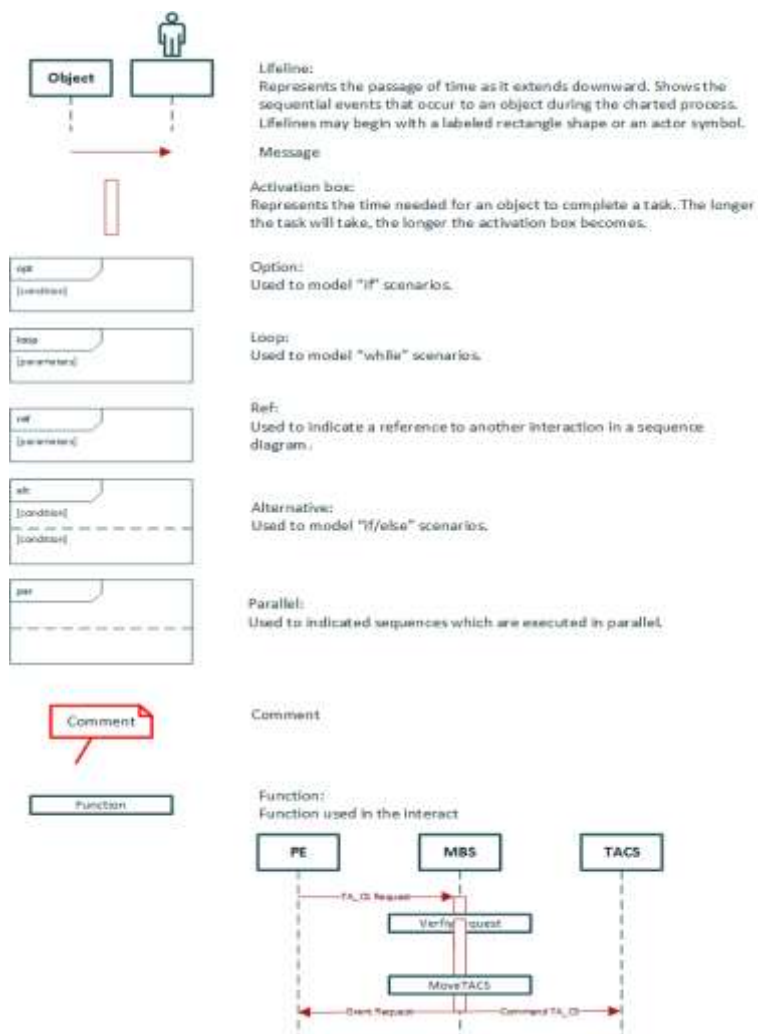


Figure 72 - Scenario: Template Scenario