

Rail to Digital automated up to autonomous train operation

D16.4 – Hybrid Level 3 Specification

Due date of deliverable: 31/05/2026

Actual submission date: 03/09/2026

Leader/Responsible of this Deliverable: <INDRA>

Reviewed: Y/N

Document status		
Revision	Date	Description
01	12/09/2023	First draft issue
02	18/04/2025	Second draft issue
03	30/05/2025	Third draft issue
04	23/06/2025	Fourth draft issue
05	08/08/2025	Fifth draft issue
06	11/09/2025	Draft ready for review
07	06/02/2026	Version for TMT Review
08	27/03/2026	Version after TMT Review
09	03/09/2026	Version after MCP11

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
	ADIF	Review of the document
	ATSA ALS SE	Review of the document
	AZD	Review of the document
	DLR	Review of the document
	FSI	Main writer of the document
	INDRA	Review of the document
	MM MMSTE AS	Review of the document
	NS	Review of the document
	PRORAIL	Review of the document
	SMO	Review of the document
	TRV	Review of the document

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 deliverable starts from the deliverables of R2DATO WP15 [10][11], addressing the remaining comments and open points in order to have a complete specification of the HL3/HTD Application. There are also further refinements of certain concepts, for example in relation to the management of non-leading engines.

Its content is built on the previous results of WP15 and is completed through a methodological process based on:

- **Comparative analysis of previous specifications** (EUG HTD, X2R5, TSI 2023).
- **Update and review of technical and functional consistency** regarding integrity requirements, train length, and management based on VSS and TTD.
- **Validation through operational scenarios**, evaluating HL3/HTD behaviour under nominal, degraded and ETCS level-transition conditions.
- **Alignment with the architecture proposed in WP19** for train integrity and train length, ensuring systematic compatibility with the rest of the R2DATO ecosystem.

Operational scenarios, developed mainly from the use cases already created in R2DATO WP15, are reported at the end of this document.

Globally the deliverable is deemed to be compliant to R2DATO Grant Agreement, even if the following topics, mentioned in D15.2 for further developments, may need additional work by the specific applications interested in them:

- Accuracy requirements for train lengths;
- Interface with DAC, OTI-I and OTI-L;

What has emerged is that the transition from ETCS L2 to HL3/HTD is relatively simple and this technology can be exploited to achieve capacity improvements and/or cost reductions, for example in the SERA Pre-Phase, as defined in the System Pillar document [12].

Overall, this specification provides a coherent document oriented towards its practical implementation in European railway systems, aligned with the requirements of the R2DATO Grant Agreement and prepared for use by all stakeholders involved in ERJU.

TABLE OF CONTENTS

Acknowledgements	2
Report Contributors	2
Executive Summary	3
Table of Contents	4
List of Figures	6
List of Tables	8
2 Introduction	9
3 Glossary and definitions	9
4 Assumptions	12
5 HL3/HTD Requirements	15
5.1 General Requirements	15
5.1.1 Determination of the connection status of the train	15
5.1.2 Definition of train location	16
5.1.3 Management of the Movement Authority	21
5.1.4 Definition of timers	24
5.1.5 Definition of trackside integrity status	36
5.1.6 Operation of trains treated as integer	37
5.1.7 Operation of trains not treated as integer	38
5.1.8 Entry/exit of a HL3/HTD area	39
5.1.9 State machine for VSS	39
5.2 High Density Application Requirements	50
5.2.1 Areas operated in Supervised Manoeuvre Mode and related state machine	50
5.3 Low Density Application Requirements	64
5.4 Requirements with Operational Impact	65
6 Engineering Rules	66
6.1 Engineering Rules for Main Lines	66
6.1.1 General engineering issues	66
6.1.2 Engineering Rules for Operational procedures	73
6.1.3 Engineering Rules for Degraded scenarios	74
6.2 Engineering Rules for Low Density Lines	75
7 Conclusions	78
8 Detailed Rationales	79
9 Operational Scenarios	88

9.1	Operational Scenario 1: Nominal Start of Mission and Initial Movement with VSS/TTD Transitions	88
9.2	Operational Scenario 2: Degraded SoM with Invalid Position, Connection Loss and Ghost Train Interaction	94
9.3	Operational Scenario 3: Operation in Radio Hole with Timer Management and Level Transition	102
9.4	Operational Scenario 4: Failed Train Recovery with Rescue Locomotive and Joining Operation	110
9.5	Operational Scenario 5: Direction Change Using a Dedicated Siding with Non-Leading Equipment.....	118
9.6	Operational Scenario 6: Exit from Shunting Area, Odometry Failure and RBC Handover 124	
9.7	Operational Scenario 7: Complex Operation: Combined Sweeping, Integrity Loss and TTD/VSS Interactions	131
9.8	Operational Scenario 8: Supervised Manoeuvre with Lost Vehicle States (L/R/LR)	139
10	Traceability with Open Points of D15.1	147
	References	149

LIST OF FIGURES

Figure 1 EUG VSS section state diagram	42
Figure 2 VSS section state diagram for SM.....	61
Figure 3 Unwanted situation – Max Safe Rear End in advance of real train front end.	71
Figure 4 Radio Hole	76
Figure 5 Proposed SoM Area.....	77
Figure 6 Step 1 Shadow Train Timer.....	79
Figure 7 Shadow Train Timer Best Case Situation.....	80
Figure 8 Shadow Train Timer Worst Case Situation.....	80
Figure 9 Start event for base shadow timer.....	82
Figure 10 End Event	82
Figure 11 Interaction between Mute Timer and Wait Integrity Timer	87
Figure 12 Starting Condition Operational Scenario 1	89
Figure 13 Step 3 Operational Scenario 1	89
Figure 14 Step 5 Operational Scenario 1	90
Figure 15 Step 10 Operational Scenario 1	91
Figure 16 Step 12 Operational Scenario 1	92
Figure 17 Step 14 Operational Scenario 1	92
Figure 18 Step 16 Operational Scenario 1	93
Figure 19 Step 17 Operational Scenario 1	93
Figure 20 Step 19 Operational Scenario 1	93
Figure 21 Step 21 Operational Scenario 1	94
Figure 22 Track Layout Operational Scenario 2.....	95
Figure 23 Starting Condition Operational Scenario 2	96
Figure 24 Step 18 Operational Scenario 2	97
Figure 25 Step 19 Operational Scenario 2	97
Figure 26 Step 21 Operational Scenario 2	98
Figure 27 Step 22 Operational Scenario 2	98
Figure 28 Step 23 Operational Scenario 2	98
Figure 29 Step 25 Operational Scenario 2	99
Figure 30 Step 26 Operational Scenario 2	99
Figure 31 Step 29 Operational Scenario 2	100
Figure 32 Step 32 Operational Scenario 2	100
Figure 33 Step 33 Operational Scenario 2	101
Figure 34 Step 35 Operational Scenario 2	101
Figure 35 Layout of SoM and initial Radio Hole Area	103

Figure 36 Starting Condition Operational Scenario 3	103
Figure 37 Step 18 Operational Scenario 3	104
Figure 38 Step 22 Operational Scenario 22	105
Figure 39 Step 23 Operational Scenario 3	106
Figure 40 Step 24 Operational Scenario 3	106
Figure 41 Step 25 Operational Scenario 3	106
Figure 42 Step 27 Operational Scenario 3	107
Figure 43 Step 28 Operational Scenario 3	107
Figure 44 Step 29 Operational Scenario 3	108
Figure 45 Step 31 Operational Scenario 3	108
Figure 46 Step 32 Operational Scenario 3	108
Figure 47 Step 35 Operational Scenario 3	109
Figure 48 Step 37 Operational Scenario 3	109
Figure 49 Step 13 Operational Scenario 4	111
Figure 50 Step 17 Operational Scenario 4	112
Figure 51 Step 21 Operational Scenario 4	112
Figure 52 Step 25 Operational Scenario 4	113
Figure 53 Step 32 Operational Scenario 4	113
Figure 54 Step 48 Operational Scenario 4	115
Figure 55 Step 54 Operational Scenario 4	115
Figure 56 Step 77 Operational Scenario 4	117
Figure 57 Step 85 Operational Scenario 4	118
Figure 58 Initial layout Operational Scenario 5.....	119
Figure 59 Step 16 Operational Scenario 5	121
Figure 60 Step 25 Operational Scenario 5	122
Figure 61 Layout after step 26 Operational Scenario 5	122
Figure 62 Initial situation Operational Scenario 6	125
Figure 63 Step 23 Operational Scenario 6	127
Figure 64 Step 26 Operational Scenario 6	128
Figure 65 Step 30 Operational Scenario 6	128
Figure 66 Step 42 Operational Scenario 6	129
Figure 67 Step 48 Operational Scenario 6	130
Figure 68 Step 4 Operational Scenario 7	132
Figure 69 Step 24 Operational Scenario 7	133
Figure 70 Step 33 Operational Scenario 7	134
Figure 71 Step 42 Operational Scenario 7	135

Figure 72 Step 44 Operational Scenario 7	135
Figure 73 Step 50 Operational Scenario 7	136
Figure 74 Step 73 Operational Scenario 7	138
Figure 75 Step 91 Operational Scenario 7	139
Figure 76 Initial layout Operational Scenario 8.....	140
Figure 77 Starting Condition Operational Scenario 8	140
Figure 78 Step 6 Operational Scenario 8	141
Figure 79 Layout after Step 7 Operational Scenario 8.....	142
Figure 80 Step 10 Operational Scenario 8	142
Figure 81 Layout after Step 34 Operational Scenario 8.....	144
Figure 82 Step 35 Operational Scenario 8	144
Figure 83 Step 55 Operational Scenario 8	145
Figure 84 Step 62 Operational Scenario 6	146

LIST OF TABLES

Table 1 List of Assumptions	14
Table 2 VSS state machine events sequence	40
Table 3 HL3/HTD State Machine	49
Table 4 State Machine for Supervised Manoeuvre Areas.....	60
Table 5 Hazardous Situation	83
Table 6 Example 1	85
Table 7 Example 2	86
Table 8 Example 3	86
Table 9 Position Report Parameters for Step 9	91
Table 6 Solutions of Open Points of D15.1.....	148

2 INTRODUCTION

The present document constitutes the Deliverable D16.4 “Hybrid Level 3 Specification” in the framework of the WP16. This specification uses fixed (pre-configured) virtual blocks for the separation of trains which are able to send train integrity confirmation in the position report, while a limited installation of trackside train detection is used for the separation of trains which are not able to send integrity confirmation, as well as for the handling of degraded situations. The implementation of it is expected to bring capacity or cost reduction benefits, without big modifications to the interlocking principles or operational procedures that are used today for the ETCS Level 2 lines in operation in Europe. It can be used on existing lines, which are already fitted with train detection, to provide a cost-effective way to increase the capacity of the line, specifically in the peak hours. During the off-peak hours, trains which are not able to report confirmed integrity could be scheduled.

Some features, like propagation or shadow train timers, are implemented in order to avoid dangers in degraded situations, e.g. the presence of ghost or shadow trains.

3 GLOSSARY AND DEFINITIONS

In general the abbreviations used in SUBSET 023 are used, below there is a table with some definitions specific for this document and some terms taken from SUBSET 023 and frequently used in this document.

Acronym	Description
Ambiguous (VSS)	The trackside has information from a position report that a train is located on the VSS and the trackside is NOT certain that no other vehicle is located in rear of this train on a VSS on which the first train is located.
Assumed Rear End	equal to the min safe rear end of the train calculated on the basis of the last train length known by the trackside
ATO	Automatic Train Operation
Connected (Train)	The trackside deems connected a train under the conditions described in HL3/HTD_0089. The ETCS-On-Board has the state connected according to the rules of SUBSET-026.
Complete	A train that has just reported “integrity confirmed” Note: This definition is used to avoid confusion with a train deemed as integer by the trackside
CRE	Confirmed Rear End at T equivalent to Min safe rear end at T ₀ (Same definition as in Figure 15 of SUBSET-026-3) Note: This definition is different from the HTD Principles because it takes into account the TSI 2023, anyway it is functionally equivalent, it is expected to stress the importance of the instants T and T ₀
CRE(D)	Confirmed Rear End by Driver. Same meaning as the above abbreviation, but with confirmation by driver.
DAC	Digital Automatic Coupler

Acronym	Description
Disconnected (Train)	The trackside deems connected a train under the conditions described in HL3/HTD_0090. The ETCS-On-Board has the state connected according to the rules of SUBSET-026.
EoM	End of Mission
ERTMS	European Rail Traffic Management System
ERJU	Europe's Rail Joint Undertaking
ETCS	European Train Control System
EUG	ERTMS Users Group
EVC	European Vital Computer
Established rear end	Trackside view of the rear end of a train which is treated as integer.
Free (VSS)	The trackside is certain that no train axle is located on the VSS Note: This definition is slightly different from the definition in the HTD Principles, because in some cases the overhang part of the train can be in a VSS, while no train axle is on the VSS, see for example clause 3.3.2.1.2 of the HTD Principles
FS	Full Supervision
Ghost Train	It is either a physical object that is present on the track and detected by TTD, but that is unknown to the trackside system by means of PTD (no radio communication), or it is a virtual object which seems to occupy the track due to a trackside failure
Halt	Unplanned loss of power of the entire HL3/HTD trackside system
HL3/HTD	ETCS Level 2 with reduced train detection according to the HTD principles Note: This composite name is used in order to provide an easy reference to the Grant Agreement (where HL3 is used) and to the HTD Principles by EUG
In advance of	A term indicating a point beyond a specific location on the track, with respect to a given direction. (Same definition as in SUBSET 023)
In rear of	A term indicating a point on the approach to a specific location on the track, with respect to a given direction. (Same definition that in SUBSET 023)
L2-TTD	ETCS Level 2 with complete train detection (Reference System that it's already in service before the introduction of HL3/HTD or Moving Block)
L3	ETCS Level 3 from previous specification. Similar to L2 with no or reduced train detection and trains with train integrity
LOA	Limit of Authority
LRBG	Last Relevant Balise Group

Acronym	Description
MA	Movement Authority
MSFE	Max Safe Front End
mSFE	Min Safe Front End
Occupied (VSS)	<p>The trackside has information from a position report that an complete train is located on the VSS and the trackside is certain that no other vehicle is located in rear of this train on a VSS on which the first train is located (Note: the definition is slightly different from the one in the HTD Principles [4] because the term 'complete' is used instead of 'integer')</p> <p>For Consists in Supervised Manoeuvre:</p> <p>The trackside has information from a position report that a complete consist is located on the VSS and the trackside is certain that no other vehicle is inside the same VSS on which the first consist is located</p>
ORBG	Other Reference Balise Group
OS	On Sight
OTI-I	Train Integrity Monitoring Device (TIMS in the CCS TSI)
OTI-L	Train Length Determination Device
PTD Information	Information based on Position Reports, Safe Consist Length for Supervised Manoeuvre and Validated Train Data Note: This definition is slightly different from the definition in the HTD Principles, because it takes into account the packets regarding the train lengths
R2DATO	Rail to Digital automated up to autonomous train operation
SERA	Single European Railway Area
Shadow Train	It is a ghost train that is chasing a train operating normally in the HTD area
Shadow Train Risk	<p>Generic term used in order in order to indicate the risk related to:</p> <p>Shadow trains;</p> <p>More trains in a VSS;</p> <p>Lost vehicles maintained at standstill, for example after integrity loss</p>
SH	Shunting
Shutdown	Planned loss of power of the entire HL3/HTD trackside system.
SIL	Safety Integrity Level
SM	Supervised Manoeuvre
SoM	Start of Mission
SvL	Supervised Location

Acronym	Description
TTD	Trackside Train Detection
Unknown (VSS)	The trackside has no information from a position report that a train is located on the VSS, but it is not certain that the VSS is free. (Note: This is a state for the “degraded” operation, for example in case of loss of the communication session)
VSS	Virtual sub-section
X2R5	X2RAIL5

4 ASSUMPTIONS

The following assumptions have been adopted during the WP15 development, some of them need to be checked with the following developments expected to be carried by WP19/WP20 and all the other activities related to Train Integrity and Train Length.

Assumption	Description	Notes
[Pre 1]	In case of unintentional train separation, the two parts of the train shall be brought to a standstill.	This is an assumption that is expected to be valid even today in the current L2-TTD applications around Europe (see bullet 4 of clause 4.2.4.2.1 of TSI LOC&PAS and bullet 2 of clause 4.2.4.3.1 of TSI WAG)
[Pre 2]	P.M. Intentional Deleted	
[Pre 3]	P.M. Intentional Deleted	
[Pre 4]	P.M. Intentional Deleted	
[Pre 5]	It is expected that the OTI-I has a low occurrence of false alarms “Train integrity lost” to build a good trust in this device before to put in service a HL3/HTD line. A first proposal is that 1 out of 100 alarms can be a false alarm. To achieve this, it is recommended that an adequate experimentation or testing campaign is performed	Request for the OTI-I. It is only a first proposal that should be verified when more OTI-I devices will be available.
[Pre 6]	It is expected that the train length provided by the rolling stock according to the requirements 2.6.2.4.2 or 2.6.3.2.1 of SUBSET 034 will become the new train length stored as valid Train Data	This is expected to bring safety benefits in comparison to current operation with train length entered by the driver
[Pre 7]	Faults of the OTI-L that cause the unavailability of the determination of the train length by the device shall be no more frequent than once in a year for any given train	Request for the OTI-L, not applicable if a fixed train length is used

Assumption	Description	Notes
[Pre 8]	It is up to the railway operators (RU & IM) to define appropriate procedures according to their Safety Management System in case of detection of Train Integrity Loss and related alarms.	This is related to the system boundaries, harmonisation of procedures related to train integrity is outside the scope of WP16
[Pre 9]	TTD information is considered as safe, i.e. reporting free only if no train axle is present on the TTD section. .	Identical to clause 3.1.1.5 of the HTD Principles, with the addition of the “axle” to take into account the overhang part of the train (maximum 5 m according to the specification ERA/ERTMS/033281)
[Pre 10]	The Train Length (L_TRAIN) reported in the train data is correct. This means that the Train Length can be used for L_TRAININT calculation and provide it to the L3 Trackside to release track behind the train.	Identical to ASM-Length-1 of X2Rail-5 in deliverable D4.1 Moving Block Specification Part 2 – System Definition
[Pre 11]	The Train Length reported by the train represents the maximal length of the train. This means the length of the train at maximum extension, if the train can stretch and contract. This means without any additional Margin, as this is added by the HL3/HTD Trackside. This means that the Train Length can be used by the HL3/HTD Trackside to release track behind the train, and for splitting and joining	
[Pre 12]	In case of operation in Supervised Manoeuvre in HL3/HTD Area in any case of movement in the direction of the vehicles in front of the engine, taking into account the side of the active cab which defines the front of the engine, it is taken for granted that the Specific Application will take appropriate mitigations to lower the safety impact of a collision of the consist with a lost vehicle, generated by real train integrity loss	Mitigations related to operation in Supervised Manoeuvre Mode
[Pre 13]	The train integrity status provided by OTI-I has three possible values: Confirmed, Unknown and Lost. When the Confirmed value is sent it means that the train length has also been correctly evaluated by OTI-L. Additionally, once OTI-I reports the Lost value, it cannot change again until is performed a system reset. The reset can be obtained by opening the driver desk, or through the reset command available in OTI systems, or it can be sent by the ETCS On-Board when the train is at standstill (See SUBSET 026 § 3.6.5.1.4 a)) and the OTI-I is reporting train integrity lost.	Request for OTI-I and OTI-L

Assumption	Description	Notes
[Pre 14]	Each VSS will be entirely contained in a TTD, with the exception of the case of the radio hole. It is not excluded that a VSS can cover and coincide with a single TTD.	
[Pre 15]	If the specific application wants to use the train lengths and/or safe consist lengths for train length calculations during splitting and joining, it is assumed that a safe way to combine train lengths is established, taking into account also the features of the applicable rolling stock.	This is needed only in case of use of the transitions #11B, #SM24B, #SM26A, #SM27A with joining.
[Pre 16]	The ETCS On-Boards in mode Non Leading, Passive Shunting and Sleeping are expected to be coupled with ETCS On-Boards in other modes. Only in the limited time between train separation and standstill the ETCS On-Boards may maintain these modes without any coupling.	This assumption is made in order to ensure that input signals coming from the rolling stock are not stuck at a permissive value. For the ETCS On-Board part, the assumption is expected to be covered by the prevention of the hazardous events TI-3, TI-7 and TI-8 of SUBSET 091.

Table 1 List of Assumptions

5 HL3/HTD REQUIREMENTS

5.1 GENERAL REQUIREMENTS

5.1.1 Determination of the connection status of the train

HL3/HTD_0089

A train is deemed connected by the HL3/HTD trackside if one of the following conditions occurs:

- The train has a started and not expired radio hole timer;
- At least one ETCS On-Board associated to the train has a started and not expired mute timer

AND

The same ETCS On-Board is not in Non Leading, Sleeping or Passive Shunting Mode.

Rationale:

In comparison to the specification [4], the approach has been generalised in order to manage particular situations, like the application of radio holes and the presence of slave engines. At the reception of the Session established Message (Message 159 of SUBSET 026 part 8), the HL3/HTD is not aware of any train location (established according to §5.1.2) so any ETCS On-Board is expected to be treated as a train. When the mode is reported with the first position report, the specific application may decide to order the disconnection of the slave engines (managing only the leading engines and preventing anyway the starting of the disconnect propagation timer for the slave engines) or to maintain the communication. If the communication is maintained, the specific application may use its own specific way (not defined here) to associate ETCS On-Boards to trains, in particular when the train location, defined in §5.1.2, is available. If a train is composed by slave engines in ETCS and a leading engine without radio connection (for any reason) it will be managed as a ghost train. The trackside has no obligation to make the association of leading engines with slave engines, so it is possible that a trackside treats each ETCS On-Board as a train.

HL3/HTD_0090

When the conditions of the requirement HL3/HTD_0089 are no more true the train is deemed disconnected.

Rationale:

See rationale of HL3/HTD_0089.

5.1.2 Definition of train location

HL3/HTD_0001

The term “train location” defines the trackside view of the stretch of track that is currently occupied by a connected train. The granularity of the train location is one VSS.

Note: It is not necessary that all the connected trains have a train location. Some features, like the mute timer, are managed for the single ETCS On-Board, and in some implementations it is possible that a single train has multiple ETCS On-Boards (one for the leading engine and others for the slave engines). It is possible that other features are monitored, like the number of simultaneous SR authorisations, but this is a choice of the specific application.

Rationale:

This requirement is derived from requirement 3.3.1.1 of EUG HTD Specification. It is a definition to explain how the trackside deals with the train location. One part of the HTD requirement has been deleted, because it was deemed informative and no more valid with the possible use of safe consist length.

HL3/HTD_0002

The train location can only be based on one type of rear end at a time. The established and assumed rear end are mutually exclusive. When the train is not considered integer anymore, the train location is based on the assumed rear end, not anymore on the established rear end.

Rationale:

This requirement is derived from requirement 3.3.1.1.1 of HTD Specification. It is necessary to have only one rear end, otherwise the management of the train location becomes complex.

HL3/HTD_0003

The front and rear end of the train location are considered independently from each other. If information of the front and rear end is received together, i.e. one position report, they are treated as two independent events, and the front end is processed first.

Rationale:

This requirement is derived from requirement 3.3.1.2 of HTD Specification. It is necessary for the order of processing of the state machine.

HL3/HTD_0004

The train location only exists as long as the train is considered as connected to the trackside. As soon as the train is deemed disconnected according to HL3/HTD_0090, the train location is deleted, but a memorised train location is created, in order to be used in the state machine. It is possible that the trackside stores some train data, like the length of the train, for the use of optional transitions.

Rationale:

This requirement is similar to the requirement 3.3.1.3 of HTD Specification. The memorised train location is used in some transitions of the state machine, in particular after re-connection or to propagate the unknown state. Some optional transitions use also the train data, like the length of the train. It is assumed that the mute timer will expire before the occurrence of the conditions defined at the § 3.5.4.2.1 of SUBSET 026.

5.1.2.1 Front end of the train location

HL3/HTD_0005

When the trackside receives the confirmation that the max safe front end of the train has entered a VSS, it considers the train to be located on this VSS and all preceding VSS up to the last VSS currently covered by the train location.

Rationale:

This requirement is similar to requirement 3.3.2.1 of HTD Specification. It is necessary to manage the train location when there is no TTD border available. The requirement HL3/HTD_0007 deals with the situation of a TTD border available.

HL3/HTD_0006

Exception 1: If the max safe front end is on the VSS in advance of the EOA, but the min safe front end is in rear of the EOA, the train location shall not be considered to extend on the VSS in advance of the EOA. The exception is to avoid treating the next VSS in advance of the MA as “occupied”, which would prevent sending a new FS MA over it. The consequence of this exception is that the train may have physically entered the VSS in advance of the EOA, while the state of this VSS is still “free”. This risk can be mitigated with a release speed zero.

For TTD limits this risk does not exist (train in advance of EOA would be detected by TTD).

Rationale:

This requirement is derived from requirement 3.3.2.1.1 of HTD Specification. It has been decided to avoid the possibility of having “occupied” VSS in advance of the MA. Opposing movements on VSS limits are forbidden by the requirement HL3/HTD_0028. There may be some situations, with a

degraded odometry and critical field devices like level crossings, where this behaviour can be dangerous. To avoid this the requirements HL3/HTD_0027 and HL3/HTD_0028 are established.

HL3/HTD_0007

Exception 2: As long as the TTD where the max safe front end is reported is free, or if this TTD becomes free when a preceding train leaves it, the train location shall not be considered to extend on the VSS which are part of this free TTD. This avoids setting a VSS to “occupied” before the train physically entered it and therefore helps when cancelling routes or changing the train orientation.

Rationale:

This requirement is derived from requirement 3.3.2.1.2 of HTD Specification. It is adopted to improve the performances exploiting the TTD borders.

HL3/HTD_0008

Exception 3: When the trackside detects that a TTD inside a radio hole is occupied, it considers the train to be located on this TTD and all preceding VSS up to the last VSS currently covered by the train location if the following conditions occur:

- The radio hole timer is not expired;
- The train has an MA that encompasses the radio hole;

Rationale:

In this way the train can be located inside the radio hole.

HL3/HTD_0009

When the safe consist length is not available, updating the front end of the train position does not depend on the integrity status in the position report.

Rationale:

This requirement is similar to the requirement 3.3.2.2 of HTD Specification. It avoids doubts about the consideration of integrity status, when the safe consist length is not available. Management of integrity for consists in Supervised Manoeuvre is explained in §5.2.1.

HL3/HTD_0010

When the trackside receives information that the max safe front end of the train has moved backwards within the previous confidence interval (this could be due to relocation), a VSS which was

previously part of the train location and which is now in advance of the max safe front end, shall still be considered as part of the train location.

Rationale:

This requirement is derived from requirement 3.3.2.3 of HTD Specification. It is a choice to avoid many state transitions due to relocation.

5.1.2.2 Established rear end of the train location

HL3/HTD_0011

For a train treated as integer the established rear end of the train location is derived from the estimated front end and the confirmed train length of the last position report with “integrity confirmed” as well as from TTD information confirming that the train is not located on a VSS.

Rationale:

This requirement is similar to the requirement 3.3.3.1 of HTD Specification. It defines the concept of established rear for a train treated as integer, integrating the information from position reports and TTDs. The term “safe train length” used in the EUG HTD specification Rev. F, is not used because it is not defined in the latest ERTMS specifications.

HL3/HTD_0012

The established rear end of the train location is never updated by position reports of on-board in the modes Sleeping, Non-Leading and Staff Responsible.

Rationale:

This requirement is similar to the requirement 3.3.3.5 of HTD Specification. There is an extension of the scope of the original requirement 3.3.3.5 to cover all the modes when linking is not usually used.

HL3/HTD_0013

If an update of the established rear end of the train location by TTD information would lead to a train located on no VSS anymore, the train is considered to be located on the first VSS of the following occupied TTD.

Rationale:

This requirement is similar to the requirement 3.3.3.6 of HTD Specification. This is to avoid losing the train location due to delayed position reports.

HL3/HTD_0014

An update of the established rear end of the train shall only take place if the resulting rear end will not be in advance of the train front end.

Rationale:

This requirement is similar to the requirement 3.3.3.6.1 of HTD Specification. This is to avoid an inconsistent location in case the TTD, which was left by the train, has become free, while the next TTD has not yet become occupied (due to delays in the detection).

HL3/HTD_0015

If the established rear end of the train location has moved forward due to a TTD becoming free, and if this TTD becomes occupied again (due to a following train), the confirmed rear end might be reported again on a VSS of this TTD. In that case the established rear end shall only be updated if this newly received confirmed rear end is in rear of the confirmed rear end from the last position report when the concerned TTD was still free.

Rationale:

This requirement is derived from requirement 3.3.3.7 of HTD Specification. In this way the relevant VSS are only updated if a real movement in backwards direction took place.

5.1.2.3 Assumed rear end of the train location**HL3/HTD_0016**

The assumed rear end of the train location is derived from the reported rear end (the train length of the train data and the min safe front end of the last position report) of a train as well as from TTD information confirming that the train is not located on a VSS.

Rationale:

This requirement is derived from requirement 3.3.4.2 of HTD Specification. The use of assumed rear end is a choice for trains not treated as integer.

HL3/HTD_0017

If an update of the assumed rear end of the train location by TTD information would lead to a train located on no VSS anymore, the train is considered to be located on the first VSS of the following occupied TTD.

Rationale:

This requirement is derived from requirement 3.3.4.4 of HTD Specification. This is to avoid losing the train location due to delayed PTD information ("jumping train").

HL3/HTD_0018

An update of the assumed rear end of the train shall only take place if the resulting rear end will not be in advance of the train front end.

Rationale:

This requirement is derived from requirement 3.3.4.4.1 of HTD Specification. This is to avoid an inconsistent location in case the TTD, which was left by the train, has become free, while the next TTD has not yet become occupied (due to delays in the detection).

HL3/HTD_0019

If the assumed rear end of the train location has moved forward due to a TTD becoming free, and if this TTD becomes occupied again (due to a following train), the reported rear end might be again on a VSS of this TTD. In that case the assumed rear end shall only be updated if this new reported rear end is in rear of the reported rear end from the last position report when the concerned TTD was still free.

Rationale:

This requirement is derived from requirement 3.3.4.5 of HTD Specification. In this way the relevant VSS are only updated if a real movement in backwards direction took place.

HL3/HTD_0020

On an ambiguous VSS the assumed rear end is used for the train location.

Rationale:

This requirement is derived from requirement 3.3.4.6 of HTD Specification. This is relevant in particular for sweeping.

5.1.3 Management of the Movement Authority

HL3/HTD_0021

In the context of the HL3/HTD concept (the trackside view), an MA is understood as to cover the track between the rear end of the train location and the SvL or LOA.

This notion of MA remains valid when the train location is deleted. In that case the MA is based on the memorised train location, but it is still considered to exist.

Note: This does not mean that the MA and the memorised train location will exist forever. For each specific train that is deemed disconnected by the trackside the specific application of the trackside may have its own specific conditions to delete the following information:

- the MA that was sent to a train;
- the memorised train location.

Rationale:

This requirement is derived from the clauses 3.1.1.7 and 3.1.1.7.1 of EUG HTD Specification. It is a definition to explain how the trackside deals with MAs. The conditions to delete the MA and the memorised train location are left to the specific application.

HL3/HTD_0022

In case of presence of critical devices like level crossings, each specific application shall evaluate if the behaviour connected to the loss of connection (i.e. possibly a large number of VSSs in “unknown” status) is acceptable or not. If not the impact may be mitigated for example with use of TTDs or by a more complex type of propagation based on speed, as evidenced in the clause 4.2.1.8 of the HTD Principles [4] or using particular rules for the closure of level crossings.

Rationale:

The time of closure of the barriers of a level crossing is considered safety related in some countries. The use of long MAs, in combination with loss of connection and transition #1B, can increase the time of closure of the barriers beyond the limits of the specific application.

HL3/HTD_0023

Each specific application must analyse if the possibility of a TTD always occupied can introduce hazards (e.g. ghost trains are possible and TTD is needed for that hazard). If this is the case, after a timer to be configured by the specific application, the specific application shall cause the transitions #4A, #6A, #9A (e.g. reducing the length of some MAs in order to cause the TTD to become free and cause the transitions #4A, #6A, #9A).

Rationale:

A TTD always occupied can jeopardise the ability of the specific application to detect ghost trains.

HL3/HTD_0024

When sweeping is performed on some VSSs or TTDs involved in the expiration of a propagation timer, the specific application needs to establish if the sweeping operation is acceptable in these particular cases (for example a runaway vehicle can crash with the sweeping train). In case it is acceptable the rules for the sending of the authorisation to the sweeping train need to be established, in particular if an update of the sweeping authorisation after the expiration of the propagation timer is necessary.

Rationale:

When there is an expiration of a propagation timer, it can't be excluded in general that a roll-away vehicle is generated. So the specific application may decide to abort the sweeping and to send the sweeping train far away from the potential roll-away vehicle.

HL3/HTD_0025

Each specific application shall calculate an appropriate safe rear margin to be added at the rear of the CRE according to the rules of the specific application (e.g. value of D_NVROLL, distance between axles and front ends) in order to avoid collisions.

Rationale:

It is important to take into account possible backwards movements and distance between the first/last axle of the train and train front/rear end.

HL3/HTD_0026

The amount of time that the train spends without using linking on-board shall be minimized.

The specific application can decide to ignore position reports in modes where linking is not usually used (e.g. SR Mode).

Rationale:

In some applications the occurrence of a relocation without linking can bring an additional complexity. Once the train has a valid position, it is recommended that the RBC sends an MA with linking, so relocation without linking can be avoided.

HL3/HTD_0027

The HL3/HTD trackside shall react according to the specific application if the reported max safe front end is in advance of the current EoA when the VSS in advance of the EoA is within the same TTD section.

Rationale:

Please see the rationale of the requirement HL3/HTD_0006. If the release speed is 0 or calculated on-board, this situation is expected to be not possible. As an example, if there is a level crossing in advance of the EoA, the specific application may decide that the EoA shall be a TTD border or the release speed shall be zero.

HL3/HTD_0028

Opposing movements on VSS limits shall be avoided, this includes also situations that involve points. This is not applicable if the VSS limit is also a TTD limit.

Rationale:

Please see the rationale of the requirement HL3/HTD_0006 for a global explanation.

5.1.4 Definition of timers**5.1.4.1 Waiting timers****HL3/HTD_0029**

A waiting timer may be configured with or without a stop event. Without a stop event, once started it will always run until it expires and will stay in the "expired" state. It will be reset when the start condition is met again.

Rationale:

This requirement is derived from requirement 3.4.1.1.2 of HTD Specification. It is a choice to define the states of waiting timers.

HL3/HTD_0030

If a start or stop event contains more than one numbered condition (such as a, b, c etc.), these conditions shall be combined with an OR, i.e. any of these conditions will trigger the start/stop event.

Rationale:

This requirement is derived from requirement 3.4.1.1.3 of HTD Specification. It is a choice about the format of the conditions.

HL3/HTD_0031

A “mute timer” is assigned to each ETCS On-Board which has sent the Session established Message (Message 159 of SUBSET 026 part 8).

Note: Conditions to delete the mute timer are left to the specific application.

Rationale:

This requirement is similar to the requirement 3.4.1.2 of HTD Specification. In this way the “mute timer” is managed for all trains that are able to establish a communication session. Trains not able to establish a communication session (not expected to be present) will be managed as ghost trains, the trackside may decide to react in some way to their presence.

HL3/HTD_0032

Start event for “mute timer” of HL3/HTD_0031:

- a) Information different from Message 156 is received from the ETCS On-Board that is in a mode different from Non Leading, Passive Shunting and Sleeping

AND

HL3/HTD Trackside is not certain that the ETCS On-Board is inside a Radio Hole.

Note: The timer is immediately started after the reception of the Session established Message foreseen by HL3/HTD_0031. ETCS On-Boards in Non Leading, Passive Shunting and Sleeping are expected to be connected to other ETCS On-Boards, see assumption [Pre 16].

Rationale:

This requirement is similar to the requirement 3.4.1.2.1 of HTD Specification. It defines the start event for the “mute timer”. A difference is caused by the application of the radio hole scenario and the decision to not manage the timer for slave engines.

HL3/HTD_0033

Stop event for “mute timer” of HL3/HTD_0031:

- a) The trackside receives the Message 156: Termination of a communication session from the ETCS On-Board and the train associated to the ETCS On-Board can be assumed to be stopped.
- b) The Radio Hole timer is started for the train associated to the ETCS On-Board.

Rationale:

If the Termination of the communication session is sent by the ETCS On-Board, there is no need to continue with the progress of the timer. The same is true inside a Radio Hole, where the protection has to be ensured by the Radio Hole timer.

HL3/HTD_0034

A “wait integrity timer” is assigned to each train that has sent integrity confirmation.

Rationale:

In this way the trackside system will monitor the train integrity status of every train able to confirm its integrity, even the ones that have no valid train data but can confirm their integrity (like the ones able to provide safe consist length). Even for trains deemed disconnected the expiration of the wait integrity timer will be maintained.

HL3/HTD_0035

Start event of “wait integrity timer”:

- a) Integrity confirmation is received from the train outside a radio hole

Rationale:

In this way the wait integrity timer is used only for trains able to confirm their integrity. Inside the radio hole the integrity is expected to be managed via the radio hole timer and appropriate rule for the rescue of the train inside the radio hole, if there is an unintentional train separation.

HL3/HTD_0036

Stop events of “wait integrity timer”:

- a) The train reports "integrity lost"
- b) The mute timer of the train expires
- c) The train reports a change of train data train length (with the inclusion of the case of train data to be revalidated as in Standby Mode if the Safe Consist Length is not available)
- d) The Radio Hole timer is started for the train

Rationale:

In the cases a) and c) the integrity is lost, so the train is not treated as integer anymore. In the case b) the management of loss of integrity will be achieved using the disconnect propagation timer.

HL3/HTD_0037

A “shadow train timer” is assigned to each TTD outside an engineered radio hole for each direction and for each connected train on the TTD. When the train is no more in the TTD, the conditions for transition #11A in the VSS adjacent to TTD are checked before deleting the timer.

Rationale:

See detailed rationale considering the global behaviour of the state machine in the § 8.

HL3/HTD_0038

Start event of “shadow train timer”:

a) The complete train in the direction of the shadow train timer reports that its max safe rear end is inside the TTD

Rationale:

See detailed rationale considering the global behaviour of the state machine in the § 8.

HL3/HTD_0039

The value of shadow train timer should be sum of these 2 factors:

- a base timer value determined by the specific application taking into account systematic issues like position report transfer delay and TTD delays;
- the time to cover the distance from the last reported max-safe-rear to the TTD-limit, with a maximum of the position_report_period time (to be on the safe side an acceleration shall be assumed).

Rationale:

See detailed rationale considering the global behaviour of the state machine in the § 8.

HL3/HTD_0040

Stop events of shadow train timer:

a) The train becomes not treated as integer anymore

Rationale:

See detailed rationale considering the global behaviour of the state machine in the § 8.

HL3/HTD_0041 (Optional)

A radio hole timer is assigned to each VSS with an engineered radio hole covered by a MA.

Rationale:

The radio hole timer is used to cope with unexpected events inside the radio hole, like unintended train integrity loss

HL3/HTD_0042 (Optional)

Start event

- a) The max safe front end of the train is reported in advance to the radio hole timer start location

Rationale:

See Radio holes Eng. Rule 2 for a detailed rationale.

HL3/HTD_0088 (Optional)

Stop event

- a) The max safe front end of the train is reported in advance to the engineered radio hole.

Rationale:

In this way the radio hole timer is stopped when the mute timer and the wait integrity timer are started again, to avoid a “double” supervision.

HL3/HTD_0043 (Optional)

A train length monitoring timer is assigned to each TTD.

Rationale:

This is required to allow transition #11B. The specific application may decide to apply this requirement only to specific TTDs, where SoM is normal operation.

HL3/HTD_0044 (Optional)

Start event: Requirement HL3/HTD_0076 is applied.

Rationale:

When there is the storing of information according to the requirement HL3/HTD_0076, there is the need to monitor the involved TTD, to ensure that there are no intrusions from other trains.

HL3/HTD_0045 (Optional)

When a VSS with stored data according to the requirements HL3/HTD_0076 and HL3/HTD_0047 becomes free, the train length monitoring timer shall be considered immediately expired and the requirement HL3/HTD_0046 shall be applied.

Rationale:

This is needed to cope with unexpected movements of the train, that has performed End of Mission in the past.

HL3/HTD_0046 (Optional)

When the train length monitoring timer expires, all the information stored according to the requirement HL3/HTD_0076 shall be deleted.

Rationale:

In this way this information is not kept for an unlimited time, avoiding an unlimited time for the monitoring described in the requirement HL3/HTD_0047.

HL3/HTD_0047 (Optional)

After the train length monitoring timer start, if it cannot be excluded that another train has entered in the TTD, the timer shall be considered immediately expired and requirement HL3/HTD_0046 shall be applied

Exception: This is not valid if a train deemed as integer has entered the TTD in the VSS with stored data according to the requirement HL3/HTD_0076 with an MA for joining causing the transition #12B. In this case the storage of the data shall be modified in the following way:

- The combination of the train lengths shall be assigned to the VSS, so when the joined train makes the SoM it is possible to have the transition #11B;
- The 2 NID_ENGINES at the extremities of the joined train shall be assigned to the VSS;

Note: As example the exclusion may be performed, by :

- Detection at the borders of the TTD associated to the VSS;
- Physical independence checking the position of the points;
- Checking that the adjacent TTDs remain free.

Rationale:

During the running of the train length monitoring timer, it should be ensured that the stored data is still valid.

HL3/HTD_0048 (Optional)

When a SoM Position Report is received from a train that is inside a VSS with stored data according to the requirements HL3/HTD_0076 and HL3/HTD_0047, the trackside shall maintain the storage of the data only if the NID_ENGINE is one of the 2 stored ones (the one in the leading cab and the one at the other extremity, if present), otherwise the train length monitoring timer shall be considered expired and the requirement HL3/HTD_0046 shall be applied immediately.

Rationale:

This check of the NID_ENGINE is adopted in order to have additional confidence that no other train has entered in the involved section.

HL3/HTD_0049 (Optional)

When the Validated Train Data or the Safe Consist Length for Supervised Manoeuvre is received from a train that is inside a VSS with stored data according to the requirements HL3/HTD_0076 and HL3/HTD_0047, the trackside shall check if the Validated Train Data corresponds to the stored data according to the requirements HL3/HTD_0076 and HL3/HTD_0047.

If not, the train length monitoring timer shall be considered expired and the requirement HL3/HTD_0046 shall be applied immediately.

Note: To use this requirement, it is fundamental that assumption [Pre 15] is satisfied in some non-harmonised way by the specific application

Rationale:

The check of the train length is fundamental to exclude the possibility of train integrity loss at standstill, in addition to be an additional verification that there is no possibility that another train has entered in the involved TTD.

HL3/HTD_0050 (Optional)

The wait first integrity confirmation timer is assigned to every VSS with stored data according to the requirements HL3/HTD_0076 and HL3/HTD_0047.

Rationale:

This timer is used in order to not wait undefinedly the confirmation of the train integrity once the acknowledgement of the train length has been sent.

HL3/HTD_0051 (Optional)

If the checks described in the requirement HL3/HTD_0049 are positive, when the trackside sends the acknowledgement of the Train Data or of the Safe Consist Length for Supervised Manoeuvre it shall start a wait first integrity confirmation timer.

Rationale:

This timer is used in order to not wait undefinedly the confirmation of the train integrity once the acknowledgement of the train length has been sent.

HL3/HTD_0052 (Optional)

If the wait first integrity confirmation timer expires, the train length monitoring timer shall be considered expired, the requirement HL3/HTD_0046 shall be applied immediately.

Rationale:

This timer is used in order to not wait undefinedly the confirmation of the train integrity once the acknowledgement of the train length has been sent.

HL3/HTD_0053 (Optional)

When transition #11B is performed, the train length monitoring timer and the wait first integrity confirmation timer shall be considered expired, the requirement HL3/HTD_0046 shall be applied immediately.

Rationale:

Once the transition #11B is performed, the stored data can be deleted.

5.1.4.2 Propagation timers**HL3/HTD_0054**

A propagation timer which is stopped after it has expired, is not considered as expired anymore. This to make sure that its expiration is processed only once.

Rationale:

This is a choice that is a trade-off between availability and safety, that ensures that when the propagation timer expires, the state “unknown” will be propagated but only once. This situation is not worse than the current L2-TTD operation, where propagation is not used.

HL3/HTD_0055

If a start or stop event contains more than one numbered condition (a, b, c), these conditions shall be combined with an OR, i.e. any of these conditions will trigger the start/stop event. When a propagation timer is started, it is not restarted if another start condition occurs before it is expired.

Rationale:

This requirement is derived from requirement 3.4.2.1.4 of HTD Specification. It is a choice about the format of the conditions. In general multiple propagation is avoided. This situation is not worse than the current L2-TTD operation, where propagation is not used.

HL3/HTD_0056

A “disconnect propagation timer” is assigned to each VSS.

Rationale:

This requirement is derived from requirement 3.4.2.2 of HTD Specification. In general this choice is a simplification in comparison to assigning a disconnect propagation timer to each NID_ENGINE. This takes into account also the possibility of real train integrity loss of disconnected trains, as example the trains with a single ETCS On-Board in Standby with no radio connection.

HL3/HTD_0057

Start event of “disconnect propagation timer”:

- a) The VSS changes to “unknown” because it is part of the MA of a train deemed disconnected.
- b) A train located on the VSS is deemed disconnected (See §5.1.1) with the exception of trains which have only ETCS On-Boards in modes Non Leading, Passive Shunting and Sleeping.

Rationale:

This requirement is derived from requirement 3.4.2.2.1 of HTD Specification. In general this choice allows the use of propagation to manage trains that become not able to communicate with the trackside. The requirement has become more complex, in order to improve the management of slave engines, in order to avoid to generate propagation in case of disconnection of a slave engine (accidental or ordered by the trackside). This is particularly relevant if the HL3/HTD trackside specific application treat each ETCS On-Board as a train, as there is no obligation to associate slave engines with leading engines.

HL3/HTD_0058

Stop event of “disconnect propagation timer”:

- a) The connection of all trains for which the timer was started, is restored with the same train orientation

- b) The TTD of the VSS becomes “free”
- c) The VSS state machine is fully processed after the timer expired

Rationale:

This requirement is derived from requirement 3.4.2.2.2 of EUG HTD Specification. In general this choice allows to manage the disconnections with the transition #12A.

HL3/HTD_0059

The disconnect propagation timer shall be dimensioned in such a way to ensure that the disconnected train can't move undetected (commanded by the driver or unintentionally) outside the zone of propagation. If the train terminates the communication session after reporting the mode shunting, this timer expires immediately.

Rationale:

This is established to explain the intended use of the disconnect propagation timer. In general the value of the timer can take into account some other conditions, like the number of trains with an assigned mute timer that are moving in SR, such specific implementations are left to the specific application.

HL3/HTD_0060

A “ghost train propagation timer” is assigned to each TTD.

Rationale:

This requirement is derived from requirement 3.4.2.3 of HTD Specification. In general this choice allows the use of propagation to manage trains that are not able to communicate with the trackside.

HL3/HTD_0061

Start events for “ghost train propagation timer”: Transition #1A or #SM1A.

Note: Requirement HL3/HTD_0082 does not cause the start of the ghost propagation timer. It is supposed that after a halt the trains have been stopped in some way and there are no ghost trains that are moving.

Rationale:

This requirement is similar to the requirement 3.4.2.3.1 of HTD Specification. In general this choice allows the use of propagation to manage trains that are not able to communicate with the trackside.

HL3/HTD_0062

Stop event for “ghost train propagation timer”:

- a) The VSS state machine is fully processed after the timer expired

Rationale:

This requirement is similar to the requirement 3.4.2.3.2 of HTD Specification. In general the ghost propagation timer is stopped only after propagation. The propagation is performed only one time.

HL3/HTD_0063

A started ghost train propagation timer is considered immediately expired when the TTD becomes free again. In that case the train must be on one of the neighbouring TTDs, and therefore propagation should start immediately.

Rationale:

This requirement is derived from the requirement 3.4.2.3.3 of HTD Specification. This requirement is intended to follow the movement of a ghost train, in particular in case it enters a TTD where there are also connected trains. In this case the connected train is treated as not integer according to the condition f) of the requirement HL3/HTD_0071.

HL3/HTD_0064

The ghost train propagation timer shall be dimensioned in such a way to ensure that the ghost train can't move undetected (commanded by the driver or unintentionally) outside the zone of propagation.

Rationale:

This is established to explain the intended use of the ghost train propagation timer. In general the value of the timer can take into account some other conditions, like the number of trains with an assigned mute timer that are moving in SR, such specific implementations are left to the specific application.

HL3/HTD_0065

Each specific application shall evaluate if it is necessary to take additional mitigation measures after the expiration of the ghost train propagation timer, for example establishing a zone around the TTD where movement of trains is not allowed.

Rationale:

In case of expiration of the timer, it can't be excluded that the ghost train will move. This can cause collisions with reporting trains.

HL3/HTD_0066

In areas where Supervised Manoeuvre is not used, an “integrity loss propagation timer” is assigned to each VSS.

Rationale:

This requirement is similar to the requirement 3.4.2.4 of HTD Specification. See § 5.2.1 for the management of areas where Supervised Manoeuvre is used.

HL3/HTD_0067

Start event (only applicable for a train on a VSS in state “occupied” or “ambiguous”):

- a) train becomes not treated as integer anymore

Note that the event a) also triggers a transition of the VSS to state “ambiguous”.

Rationale:

This propagation timer is intended to manage the possibility of roll-away vehicles caused by real train integrity loss. It is in general avoided that the integrity loss propagation timer and the disconnect propagation timer are running at the same time, so in general for disconnected trains the situation is managed by the disconnect propagation timer.

HL3/HTD_0068

Stop events:

- a) All trains, for which the timer was started, report confirmed integrity again with unchanged train data train length compared to the last position report based on which the train was still treated as integer before the timer started. This stop condition is valid only for the trains that became treated as not integer because of conditions a), b), c) and g) of the requirement HL3/HTD_0071.
- b) VSS state changes to “occupied” or to “free”
- c) The VSS state machine is fully processed after the timer expired

Rationale:

This requirement is similar to the requirement 3.4.2.4.2 of HTD Specification. This propagation timer is intended to manage the possibility of roll-away vehicles caused by real train integrity loss. To avoid complexity, this timer is also started with 2 trains confirming integrity inside a VSS, even if in this case there is no real train integrity loss. Condition a) is not used where there is no clear identification of the involved trains or if the timer is started because of condition d) of HL3/HTD_0071, to avoid to start and stop immediately the timer.

HL3/HTD_0069

The information obtained using the IntegrityLossPropagationTimer – Eng. Rule 2 shall be used to configure the timers relevant for train integrity loss (e.g. the sum of wait integrity timer, integrity loss propagation timer, mute timer and disconnect propagation timer or the radio hole timer)

Rationale:

In the worst case, described in the §8, there can be a delayed start of the integrity loss propagation timer, so the specific application shall consider this possibility.

5.1.5 Definition of trackside integrity status**HL3/HTD_0070**

The trackside will treat a train as integer if it receives a position report from the train reporting confirmed integrity and there is no shadow train risk

Rationale:

This requirement is derived from the requirement 3.5.1.2 of HTD Specification. The condition about shadow train risk (that according to the definitions is not limited to shadow trains) needs to be checked in order to avoid that a section is set to free

HL3/HTD_0071

The trackside will not treat a train (with the exception of consists in Supervised Manoeuvre Mode) as integer if one of the following events occurs:

- a) the train reports “integrity lost”
- b) PTD with no integrity information is received after the “wait integrity timer” has expired
- c) the train, previously with valid train data, reports changed train data train length
- d) the train is located on at least one VSS where there is also another train located
- e) the VSS in rear of the train location becomes “unknown” due to propagation
- f) a propagation timer of the VSS in rear of the train location expires or a ghost train propagation timer of the TTD in rear expires
- g) the train reports Mode Reversing

Rationale:

This requirement is similar to the requirement 3.5.1.3 of HTD Specification. There are some additional scenarios because:

- In Reversing the train length from the Train Length Determination Device is not used automatically;
- In condition f) the ghost train propagation timer, assigned to the TTD, is taken into account.

See §5.2.1 for what happens in areas where Supervised Manoeuvre is used.

HL3/HTD_0072

When

- A VSS becomes “unknown” due to propagation in rear of a VSS with memorised train location;
- A propagation timer of a VSS expires or a ghost train propagation timer of a TTD expires in rear of a VSS with memorised train location;

The transition #12A shall be inhibited in all the VSSs that are part of the MA based on the memorised train location. The inhibition is removed when the MA is no more valid.

Rationale:

This requirement is intended to mitigate a scenario with ghost trains described in § 4.2 of D15.2 and in Step 33 of Operational Scenario 2.

5.1.6 Operation of trains treated as integer

HL3/HTD_0073

The trackside will release infrastructure based on position reports from a train reporting confirmed integrity. The VSS that the train leaves will become “free” if there is no shadow train risk

Rationale:

This requirement is derived from the requirement 3.6.1.1 of the EUG HTD Specification. This is according to the general concept of using position reports to set sections to free, providing there is insurance that one and only one train is in the section (i.e. no shadow train risk)

HL3/HTD_0074

A train that reports “no integrity information available”, after having reported “confirmed integrity”, is treated as integer as long as none of the events to change the trackside integrity status occurs. This does not mean that the reported rear end is used to update the train location.

Rationale:

This requirement is derived from the requirement 3.6.1.2 of the EUG HTD Specification. This is according to the general concept of using only position reports with integrity confirmed to set sections to free.

HL3/HTD_0075 (Optional)

When there are the transitions #2A, #11A, #12A and the train has entered the VSS with a FS MA, the trackside shall consider the train length of the reporting train available for the following possible storage of data described by requirement HL3/HTD_0076.

Otherwise the train lengths shall be not memorised when there is the transition #7A.

Rationale:

Only if there is assurance that there is no vehicle in front of the reporting train it is possible to use the features described in HL3/HTD_0076, this is ensured by the transition #2A, #11A and #12A with a FS MA

HL3/HTD_0076 (Optional)

When there is the transition #7A, if the train length according to the requirement HL3/HTD_0075 is available and there was only one VSS in the state occupied in the associated TTD and all the other VSSs are free, the HL3/HTD trackside shall memorise the train orientation, the train data and the NID_ENGINE of the trains (The leading one and the one at the other extremity of the train if present) and the VSS where the train can be.

The HL3/HTD trackside shall start the train length monitoring timer of the associated TTD.

Note: This can be used to prevent sweeping and use this information for example for Joining and Start of Mission. The application of this requirement is optional, it is necessary in order to allow the transition #4C and #11B

5.1.7 Operation of trains not treated as integer

HL3/HTD_0077

The trackside will not release infrastructure based on position reports from a train that is not treated as integer. The “ambiguous” VSS that the train leaves, i.e. the assumed rear end of the train is in advance of this VSS, will become “unknown”. These sections will be set to “free” when the whole TTD becomes free. Thus, this corresponds to a system without virtual sub-sectioning.

Rationale:

This requirement is derived from the requirement 3.7.1.1 of the EUG HTD Specification. This is according to the general concept of managing the situation in a way similar to current Level 2 operation when there is no insurance that one and only one train is in the section (i.e. shadow train risk).

5.1.8 Entry/exit of a HL3/HTD area

HL3/HTD_0078

As soon as the train is not located anymore in the HL3/HTD area , it is not taken into account anymore by the HL3/HTD trackside, i.e. location and related “mute timer” and “wait integrity timer” do not exist anymore.

Rationale:

This requirement is derived from the requirement 3.11.1.2 of the EUG HTD Specification. This requirement takes into account trains with train location, the trackside may have its own rules to manage the trains without train location.

5.1.9 State machine for VSS

HL3/HTD_0079

The state machine does not run continuously, but is event driven. VSS states are updated by running the state machine according to a sequence of actions based on the following events:

Event	Sequence of actions
PTD information or Termination of a communication session received	1. Reinststate the train location from the memorised train location (if applicable due to reconnection)
	2. Update the front end of the train location and evaluate the timer start/stop conditions
	3. Update the VSS states (run the state machine)
	4. Update the rear end of the train location and evaluate the timer start/stop conditions
	5. Update the VSS states (run the state machine)

	6. If transition #11B has been performed, update the VSS states (run the state machine)
TTD information (occupied/free)	1. Update the front end of the train location and evaluate the timer start/stop conditions
	2. Update the VSS states (run the state machine)
	3. Update the rear end of the train location and evaluate the timer start/stop conditions
	4. Update the VSS states (run the state machine)
Timer expires	1. Evaluate the timer start/stop conditions
	2. Update the VSS states (run the state machine)
	3. Evaluate the timer start/stop conditions

Table 2 VSS state machine events sequence

Rationale:

This requirement is derived from the requirement 5.1.1.2 of the EUG HTD Specification. There are some modifications to manage the Termination of a communication session and the transition #11B, that is specific of HL3/HTD.

HL3/HTD_0080

When a transition condition contains the state of a VSS on which a train is or was located, it shall use the state after the update of the train location has been processed by the state machine.

Rationale:

This requirement is derived from the requirement 5.1.1.2.2 of the EUG HTD Specification. This is a convention in order to make the state machines more clear.

HL3/HTD_0081

Events are handled in the order of reception as atomic events for all VSS sections, i.e. the sequence related to an event shall be processed completely before the next event is taken into account

Rationale:

This requirement is derived from the requirement 5.1.1.3 of the EUG HTD Specification. This is a requirement for the management of the state machine.

HL3/HTD_0082

At the start-up of the trackside system all VSS are first put in state “unknown” and then the state machine is run once, which will set all VSS on free TTD to “free”. Position reports from trains shall be not considered in this first run.

Rationale:

This requirement is derived from the requirement 5.1.1.4 of the EUG HTD Specification. This is a requirement for the management of the start-up, after a planned shutdown or an unexpected halt.

HL3/HTD_0083

The term “TTD” without a qualifier like “previous” refers to the TTD of the VSS for which the condition is checked (the evaluated VSS).

Rationale:

This requirement is derived from the requirement 5.1.1.5 of the EUG HTD Specification. This is a requirement for the management of the state machine.

HL3/HTD_0084

A timer is only considered as “not expired” if it is running, i.e. was activated by a start event in the context of the concerning train run.

Rationale:

This requirement is derived from the requirement 5.1.1.6 of the EUG HTD Specification. This is a requirement for the management of the state machine, for what regards the timers.

HL3/HTD_0085

Whenever a transition condition refers to a previous TTD or VSS, and in case there is no known previous TTD/VSS (e.g. when entering a HTD area), the condition is not fulfilled.

Rationale:

This requirement is derived from the requirement 5.1.1.7 of the EUG HTD Specification. This is a requirement for the management of the state machine.

HL3/HTD_0086

When the word “train” / “timer” is used more than once in a transition condition, the same train / timer is meant.

Rationale:

This requirement is derived from the requirement 5.1.1.8 of the EUG HTD Specification. This is a requirement for the management of the state machine.

HL3/HTD_0087

The following state machine is used in HL3/HTD applications, with the specific exception described in the requirement for applications that want to use Supervised Manoeuvre.

Note: The state machine is illustrated in the figure, taken from the EUG specification. For readability the states to which the transition condition refers are indicated with F (free), O (occupied), A (ambiguous) and U (unknown). E.g. F>O means transition from “free” to “occupied”.

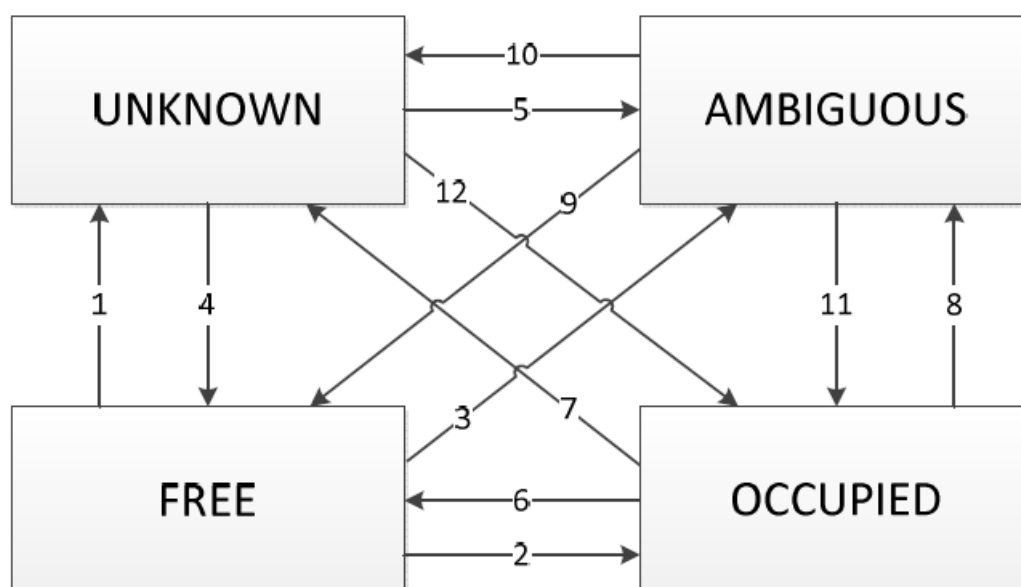


Figure 1 EUG VSS section state diagram

#	Condition	Priority over	Notes
#1A F>U	(TTD becomes occupied) AND ((in each direction no FS MA exists covering the first VSS of this TTD) OR ((the TTD is part of an MA) AND (the train to which the MA was sent could not have reached the TTD in the time between the last position report and the moment the TTD becomes occupied))) AND (no train located on this TTD)		This transition is identical to the one in the HTD Principles, except for some differences in the writing
#1B F>U	(TTD is occupied) AND (the evaluated VSS is part of the MA sent to a train deemed disconnected) AND (the evaluated VSS is located in advance of the VSS of the memorised train location)		This transition is identical to the one in HTD Principles.
#1C F>U	(TTD is occupied) AND (there is(/are) only “free” or “unknown” VSS or none between the evaluated VSS and the VSS for which the “disconnect propagation timer” is expired) AND (the evaluated VSS is located on the same TTD as the VSS for which the timer is expired)		This transition is identical to the one in the HTD Principles

#	Condition	Priority over	Notes
#1D F>U	<p>(TTD is occupied)</p> <p>AND</p> <p>(there is(/are) only “free” or “unknown” VSS on an occupied TTD or none between the evaluated VSS and the VSS for which the “disconnect propagation timer” is expired)</p> <p>AND</p> <p>(the evaluated VSS is not located on the same TTD as the VSS for which the timer is expired)</p> <p>AND</p> <p>(the evaluated VSS is not part of an MA)</p>		This transition is identical to the one in the HTD Principles
#1E F>U	<p>(TTD is occupied)</p> <p>AND</p> <p>(there is(/are) only “free” or “unknown” VSS or none between the evaluated VSS and the VSS for which the “integrity loss propagation timer” is expired)</p> <p>AND</p> <p>(the evaluated VSS is located on the same TTD as the VSS for which the timer is expired)</p>		This transition is identical to the one in the HTD Principles
#1F F>U	<p>(TTD is occupied)</p> <p>AND</p> <p>(there is(/are) only “free” or “unknown” VSS on an occupied TTD or none between the evaluated VSS and the VSS for which the “integrity loss propagation timer” is expired)</p> <p>AND</p> <p>(the evaluated VSS is not located on the same TTD as the VSS for which the timer is expired)</p> <p>AND</p> <p>(the evaluated VSS is not part of an MA)</p>		This transition is identical to the one in the HTD Principles

#	Condition	Priority over	Notes
#1G F>U	(TTD is occupied) AND (there is(/are) only “free” or “unknown” VSS on an occupied TTD or none between the evaluated VSS and the TTD for which the “ghost train propagation timer” is expired) AND (the evaluated VSS is not located on the TTD for which the timer is expired) AND (it cannot be excluded by means of detection at the TTD border that the ghost train has entered the evaluated TTD)		This transition is identical to the one in the HTD Principles
#2A F>O	(TTD is occupied) AND (train is located on the evaluated VSS) AND (VSS where the train was located before it was located on the evaluated VSS, was “occupied”) AND (VSS where the train was located before it was located on the evaluated VSS, is not in advance of the train)	#3	This transition is identical to the one in the HTD Principles
#3A F>A	(TTD is occupied) AND (train is located on the evaluated VSS)		This transition is identical to the one in the HTD Principles [4]
#4A U>F	(TTD is free)		This transition is identical to the one in the HTD Principles [4]

#	Condition	Priority over	Notes
#4B U>F	(train reconnects with the same train orientation) AND (the evaluated VSS is part of the FS MA sent to this train) AND (the evaluated VSS is in advance of the VSS where the reconnected train is located) AND (the MA sent to this train is still valid)	#5, #12	This transition, that is identical to the one in the HTD Principles, is subject to the verification that the reconnected train is identical to the one that lost the connection. In particular it has to have a compatible train length and any fault of the OTI-L has to be known to the RBC.
#4C U>F	(in the same TTD transition #11B has been performed) AND (the VSS has become unknown because of the transition #1C caused by the termination of communication session of the train with NID_ENGINE stored according to requirements HL3/HTD_0076 and HL3/HTD_0048)		This is an additional optional transition in addition to the HTD Principles [4]. This transition is possible if the assumption [Pre 15] is satisfied and if there is a way to confirm the engine that is performing Start of Mission was at an extremity of the train
#4D U>F	(the VSS has become unknown because of the transition #1C caused by the termination of communication session of the train with a NID_ENGINE stored according to requirements HL3/HTD_0076 and HL3/HTD_0048) AND (the train is connected again with the same NID_ENGINE) AND (the evaluated VSS is in advance of the VSS where the train is located)		This is an additional optional transition in addition to the HTD Principles
#5A U>A	(train is located on the evaluated VSS)		This transition is identical to the one in the HTD Principles
#6A O>F	(TTD is free)		This transition is identical to the one in the HTD Principles

#	Condition	Priority over	Notes
#6B O>F	(train has left the evaluated VSS) AND (train treated as integer)		This transition is identical to the one in the HTD Principles
#7A O>U	((mute timer expires) OR (communication session is being terminated) OR (Radio Hole Timer expires)) AND (the evaluated VSS becomes part of the memorised train location)	#8	This transition is identical to the one in the HTD Principles [4] with the addition of the case of the Radio Hole Timer. If the optional functionality of assignment of train length to VSS sections is used, if the conditions described in the requirement HL3/HTD_0076 are satisfied, the HL3/HTD trackside may memorise additional data to attempt transition #11B at a later stage.
#8A O>A	(train is located on the evaluated VSS) AND (train is not treated as integer)		This transition is identical to the one in the HTD Principles
#8B O>A	The ETCS On-Board is reporting Reversing Mode		This additional transition is related to Reversing (It is in general assumed that this type of mode is not used very much)
#9A A>F	(TTD is free)		This transition is identical to the one in the HTD Principles but a small typo has been corrected (U>O instead of A>F)
#10A A>U	(the evaluated VSS is left by all reporting trains, i.e. the assumed rear end of the train as defined in 3.3.4 of HTD Principles [4] is in advance of the evaluated VSS)		This transition is identical to the one in the HTD Principles

#	Condition	Priority over	Notes
#10B A>U	((mute timer expires) OR (communication session is being terminated)) AND (the evaluated VSS becomes part of the memorised train location) AND (no other train is located on the evaluated VSS)		This transition is identical to the one in the HTD Principles
#11A A>O	(TTD in rear is free) AND (train treated as integer) AND (the “shadow train timer” of the TTD in rear for this direction and for this train is not expired) AND (train is located on the evaluated VSS)		This transition is identical to the one in the HTD Principles [4]
#11B A>O	(the wait first integrity confirmation timer is started and is not expired) AND (train is located on the evaluated VSS) AND (train is complete)		This additional optional transition is based on the optional functionality of assignment of train length to VSSs. See use cases related to SoM and EoM. This transition is possible if the assumption [Pre 15] is satisfied and if there is a way to confirm the engine that is performing Start of Mission was at an extremity of the train

#	Condition	Priority over	Notes
#12A U>O	<p>(train reconnects with the same train orientation)</p> <p>AND</p> <p>(VSS where the train was located when the connection was lost, was “occupied”)</p> <p>AND</p> <p>(train treated as integer)</p> <p>AND</p> <p>(In rear of the evaluated VSS and subsequent VSS(s) that had become “unknown” because of the lost connection of this train is a “free” VSS on an “occupied” TTD or a “free” TTD)</p> <p>AND</p> <p>(train is located on the evaluated VSS)</p> <p>AND</p> <p>(the MA sent to this train is still valid)</p>	#5	This transition is slightly different from the one in the HTD Principles [4] because in the fourth condition a “free” TTD is considered. The requirement HL3/HTD_0072 mitigates a possible hazardous scenario with ghost trains described in § 4.2 of D15.2 and in Step 33 of Operational Scenario 2.
#12B U>O	<p>(train is located on the evaluated VSS)</p> <p>AND</p> <p>(VSS where the train was located before it was located on the evaluated VSS, was “occupied”)</p> <p>AND</p> <p>(VSS where the train was located before it was located on the evaluated VSS, is in rear of the train)</p> <p>AND</p> <p>(the train is not re-connecting, i.e. the mute timer was not expired)</p> <p>AND</p> <p>(train treated as integer)</p>	#5	This transition is identical to the one in the HTD Principles [4].

Table 3 HL3/HTD State Machine

5.2 HIGH DENSITY APPLICATION REQUIREMENTS

This section presents the requirements for applications that want to use HL3/HTD to achieve increased performance. These applications are expected to be high density applications, where cost is not a critical point.

APP_0001

If the performance impact of transition #8A caused by the clauses e)/f) of the requirement HL3/HTD_0071 is not acceptable, the specific application shall individuate appropriate mitigations. They can be for example:

- Avoid connection losses;
- Including a TTD section with one VSS section at strategic locations as suggested by clause 4.2.1.7 of the EUG HTD Principles [4];
- Sweeping (in this case the performance impact is expected to be lowered, not eliminated);
- Reset of the ambiguous state caused by the clauses 3.5.1.3 e)/f) when they are not valid anymore, provided that there is no shadow train hazard.

Rationale:

In high density applications propagation can cause some disruptions because it can cause adverse effects on train treated as integer. Anyway it may be needed, because of possible movements of not connected trains, in particular in case of long MAs.

APP_0002

Overall Consist Length used in HL3/HTD Applications shall be SIL4

Rationale:

Using SIL2 overall consist length it is not possible to fulfil the safety requirement EXT_SR07 of SUBSET 091. Moreover, in case of change of direction, the use of a SIL2 overall consist length is problematic if there is a change of the train orientation, in this case the application of clause 4.4.21.1.7 of SUBSET 026 can bring to have a too high failure rate for the base event ODO-4 of SUBSET-091

5.2.1 Areas operated in Supervised Manoeuvre Mode and related state machine

APP_0003

Areas where Supervised Manoeuvre is planned to be used normally are expected to be distant from radio holes and areas with poor radio coverage.

Rationale:

The radio connection is expected to be needed for proper operation in Supervised Manoeuvre. If the radio connection is not available, the mode Shunting should be used.

APP_0004

For the specific case of Supervised Manoeuvre operation, in specific areas of stations where this type of mode is planned to be used, the following state machine is used.

<u>#</u>	<u>Condition</u>	<u>Priority over</u>	<u>Notes</u>
#SM1A F>U	(TTD becomes occupied) AND ((in each direction no MA exists covering the first VSS of this TTD) OR ((the TTD is part of an MA) AND (the train to which the MA was sent could not have reached the TTD in the time between the last position report and the moment the TTD becomes occupied))) AND (no train located on this TTD)		

#	Condition	Priority over	Notes
#SM1B F>U	(TTD is occupied) AND (the evaluated VSS is part of the MA sent to a train for which the mute timer is expired) AND (the evaluated VSS is located in advance of the VSS of the memorised train location)		
#SM1C F>U	(TTD is occupied) AND (there is(/are) only “free” or “unknown” VSS or none between the evaluated VSS and the VSS for which the “disconnect propagation timer” is expired) AND (the evaluated VSS is located on the same TTD as the VSS for which the timer is expired)		In comparison with the standard case, there is no more the check that the VSS is not part of the MA, because in Supervised Manoeuvre a shadow train can appear in front of the consist
#SM1D F>U	Intentionally Deleted		Intentionally Deleted
#SM1E F>U	(TTD is occupied) AND (there is(/are) only “free” or “unknown” VSS or none between the evaluated VSS and the VSS for which the “integrity loss propagation timer” is expired) AND (the evaluated VSS is located on the same TTD as the VSS for which the timer is expired)		In comparison with the standard case, there is no more the check that the VSS is not part of the MA, because in Supervised Manoeuvre a shadow train can appear in front of the consist
#SM1F F>U	Intentionally Deleted		Intentionally Deleted

#	Condition	Priority over	Notes
#SM1G F>U	<p>(TTD is occupied)</p> <p>AND</p> <p>(there is(/are) only “free” or “unknown” VSS on an occupied TTD or none between the evaluated VSS and the TTD for which the “ghost train propagation timer” is expired)</p> <p>AND</p> <p>(the evaluated VSS is not located on the TTD for which the timer is expired)</p> <p>AND</p> <p>(it cannot be excluded by means of detection at the TTD border that the ghost train has entered the evaluated TTD)</p>		
#SM2A F>O	<p>(TTD is occupied)</p> <p>AND</p> <p>(train is located on the evaluated VSS)</p> <p>AND</p> <p>(VSS where the train was located before it was located on the evaluated VSS, was “occupied”)</p>		In comparison with the standard case, there is no more the check about the direction of the movement because the use of safe consist length allows to determine that the consist is integer even in case of reverse movement (that is expected to not be normal operation in Supervised Manoeuvre)
#SM2B F>O	<p>(TTD is occupied)</p> <p>AND</p> <p>(train is located on the evaluated VSS)</p> <p>AND</p> <p>(VSS where the train was located before it was located on the evaluated VSS, was “Lost Vehicle in Front of the Consist”)</p> <p>AND</p> <p>(the train entered the evaluated VSS according to the direction of the SM MA used for sweeping)</p>		This transition takes into account that the consist has been authorised for sweeping using the SM MA. It may be that, after the lost vehicle in front of the consist appears, the SM MA is updated with a reduced speed for sweeping.

#	Condition	Priority over	Notes
#SM3A F>R	(TTD is occupied) AND (train is located on the evaluated VSS) AND (VSS where the train was located before it was located on the evaluated VSS, was “Lost Vehicle in Rear of the Consist”) AND (the train entered the evaluated VSS according to the direction of the SM MA)		
#SM3B F>R	(TTD is occupied) AND (train is located on the evaluated VSS) AND (VSS where the train was located before it was located on the evaluated VSS, was “Lost Vehicle in Rear and in Front of the Consist”) AND (the train entered the evaluated VSS according to the direction of the SM MA used for sweeping)		
#SM4A U>F	(TTD is free)		
#SM5A U>R	(train is located on the evaluated VSS) AND (the train entered the evaluated VSS according to the direction of the SM MA used for sweeping)		If coming from another VSS, it is supposed that the consist has been authorised for sweeping. The case of SoM is excluded. Any lost vehicle in front of the consist is not expected to be “carried” in the next VSS because of sweeping procedures.

#	Condition	Priority over	Notes
#SM6A U>LR	(train is located on the evaluated VSS) AND (the consist is performing SoM)		To be generic, when performing SoM, it is considered that the consist has vehicles both in front and in rear of it
#SM7A O>F	(TTD is free)		This transition is identical to the one in the HTD Principles [4]
#SM7B O>F	(train has left the evaluated VSS) AND (train treated as integer)		This transition is identical to the one in the HTD Principles [4]
#SM8A O>U	((mute timer expires) OR (communication session is being terminated)) AND (the evaluated VSS becomes part of the memorised train location)		This transition is identical to the one in the HTD Principles [4]. In case of Supervised Manoeuvre is implemented, it is expected that the RBC memorises the NID_ENGINES (It can be more than one) and the length of the consist, if the consist entered in the VSS with a FS MA. This transition shall be avoided as much as possible during operation in Supervised Manoeuvre, anyway it is possible that it is performed because of features of the ERTMS specification (as example transition [83] of SUBSET 026 part 5) According to the specific application operational procedures the lost vehicle can be sent to an Area where Shunting Mode is used.
#SM9A O>L	(train is located on the evaluated VSS) AND (train is not treated as integer because there can be a lost vehicle or an active cab in front of the Consist)		

#	Condition	Priority over	Notes
#SM10 A O>R	(train is located on the evaluated VSS) AND (train is not treated as integer because there can be a lost vehicle or an active cab in rear of the Consist)		
#SM11 A L>LR	There can be a lost vehicle or a reporting cab in front of the consists in the evaluated VSS		
#SM12 A R>LR	There can be a lost vehicle or a reporting cab in front of the consists in the evaluated VSS		
#SM13 A O>LR	There can be lost vehicles or reporting cabs in rear and in front of the consists in the evaluated VSS		This transition is expected to be rare; it is possible for example in case of real loss of consist integrity both in front and in rear of the train in same cycle of the state machine
#SM14 A L>R	All the consists present in the evaluated VSS can have lost vehicles or reporting cabs only in rear		This transition is expected to be influenced by the SM MA sent to the consists in the evaluated VSS
#SM15 A R>L	All the consists present in the evaluated VSS can have lost vehicles or reporting cabs only in front		This transition is expected to be influenced by the SM MA sent to the consists in the evaluated VSS
#SM16 A LR>R	All the consists present in the evaluated VSS can have lost vehicles or reporting cabs only in rear		This is expected to be reached with a sweeping until the end of the VSS
#SM17 A LR>L	All the consists present in the evaluated VSS can have lost vehicles or reporting cabs only in front		
#SM18 A L>F	(TTD is free)		

#	Condition	Priority over	Notes
#SM18 B L>F	(the evaluated VSS is left by all reporting trains in the direction of the sweeping MA)		It is assumed that operational procedures for sweeping avoid that a potential lost vehicle in front of the consist is «pushed» without any joining
#SM19 A R>F	(TTD is free)		
#SM20 A LR>F	(TTD is free)		
#SM21 A R>U	(the evaluated VSS is left by all reporting trains in the direction of the MA)		
#SM21 B R>U	((mute timer expires) OR (communication session is being terminated)) AND (the evaluated VSS becomes part of the memorised train location) AND (no other consist is located on the evaluated VSS)		In case of Supervised Manoeuvre is implemented, it is expected that the RBC memorises the NID_ENGINES (It can be more than one) and the length of the consist. This transition shall be avoided as much as possible during operation in Supervised Manoeuvre. According to the specific application operational procedures the lost vehicle can be sent to an Area where Shunting Mode is used.
#SM22 A LR>U	(the evaluated VSS is left by all reporting trains in the direction of the MA)		

#	Condition	Priority over	Notes
#SM22 B LR>U	((mute timer expires) OR (communication session is being terminated)) AND (the evaluated VSS becomes part of the memorised train location) AND (no other consist is located on the evaluated VSS)		This transition is identical to the one in the HTD Principles [4]. In case of Supervised Manoeuvre is implemented, it is expected that the RBC memorises the NID_ENGINES (It can be more than one) and the length of the consist. This transition shall be avoided as much as possible during operation in Supervised Manoeuvre. According to the specific application operational procedures the lost vehicle can be sent to an Area where Shunting Mode is used.
#SM23 A L>U	(the evaluated VSS is left by all reporting trains in the direction opposite to the MA)		
#SM23 B L>U	((mute timer expires) OR (communication session is being terminated)) AND (the evaluated VSS becomes part of the memorised train location) AND (no other consist is located on the evaluated VSS)		This transition is identical to the one in the HTD Principles [4]. In case of Supervised Manoeuvre is implemented, it is expected that the RBC memorises the NID_ENGINES (It can be more than one) and the length of the consist. This transition shall be avoided as much as possible during operation in Supervised Manoeuvre. According to the specific application operational procedures the lost vehicle can be sent to an Area where Shunting Mode is used.

#	Condition	Priority over	Notes
#SM24 A R>O	(TTD in rear is free) AND (train treated as integer) AND (the “shadow train timer” of the TTD in rear for this direction and for this train is not expired) AND (train is located on the evaluated VSS)		
#SM24 B R>O	(train treated as integer) AND (train is located on the evaluated VSS) AND (the combination of the lengths reported in the Safe consist length information for Supervised Manoeuvre corresponds to the expected lengths of the vehicles that can be present in the evaluated VSS)		The detailed features for the last condition are left open to the specific implementation
#SM25 A U>O	(train is located on the evaluated VSS) AND (VSS where the train was located before it was located on the evaluated VSS, was “occupied” or “Lost Vehicle in Front of the Consist”) AND (VSS where the train was located before it was located on the evaluated VSS, is in rear of the train according to the direction of the SM MA used for sweeping) AND (the train is not re-connecting, i.e. the mute timer was not expired) AND (train treated as integer)		

#	Condition	Priority over	Notes
#SM26 A L>O	(train treated as integer) AND (train is located on the evaluated VSS) AND (the combination of the lengths reported in the Safe consist length information for Supervised Manoeuvre corresponds to the expected lengths of the vehicles that can be present in the evaluated VSS)		The detailed features for the last condition are left open to the specific implementation
#SM27 A LR>O	(train treated as integer) AND (train is located on the evaluated VSS) AND (the combination of the lengths reported in the Safe consist length information for Supervised Manoeuvre corresponds to the expected lengths of the vehicles that can be present in the evaluated VSS)		The detailed features for the last condition are left open to the specific implementation

Table 4 State Machine for Supervised Manoeuvre Areas

Rationale:

This state machine has a certain degree of complexity, so in principle it is not the only solution, the specific application may decide for example that after any degrade during Supervised Manoeuvre (that are expected to be rare) the operation will continue in Shunting Mode.

The main assumption of this state machine, see Figure 2 , is that Supervised Manoeuvre can be used for sweeping, even if the cab is not at the front of the consist. If the specific application safety analysis shows that this is not valid, other solutions have to sought (for example use of Shunting Mode).

Additional states are planned to be used for Supervised Manoeuvre operation, in particular the state ambiguous is divided in various states:

- Lost Vehicle in Front of the Consist: L: At least one consist can have a lost vehicle or a reporting cab in front of it according to the direction of the SM MA authority. This state is useful in case the operational rules for sweeping in Supervised Manoeuvre are different to the ones for normal operation in Supervised Manoeuvre;
- Lost Vehicle in Rear of the Consist: R: At least one consist can have a lost vehicle or a reporting cab in rear of it according to the direction of the SM MA authority. This state is similar to the classic “ambiguous” state

- Lost Vehicle in Front and in Rear of the Consist: LR. This state encompasses the 2 previous states.

The additional states in substitution to “ambiguous” are introduced in order to differentiate between a “normal” SM MA (towards a free VSS) and a sweeping SM MA, that can have in principle different speeds. In addition, these states allow to give a direction to the propagation, when there is an integrity loss.

The state “occupied” has a different meaning in the Supervised Manoeuvre area:

The trackside has information from a position report that a complete consist is located on the VSS and the trackside is certain that no other vehicle is inside the same VSS on which the first consist is located.

Transitions F>L and F>LR are not possible because no lost vehicle or reporting cab can be in front of a train that enters a VSS that was free. Transition U>L is not possible because there is no guaranty that the train entering the VSS cannot have a lost vehicle in rear.

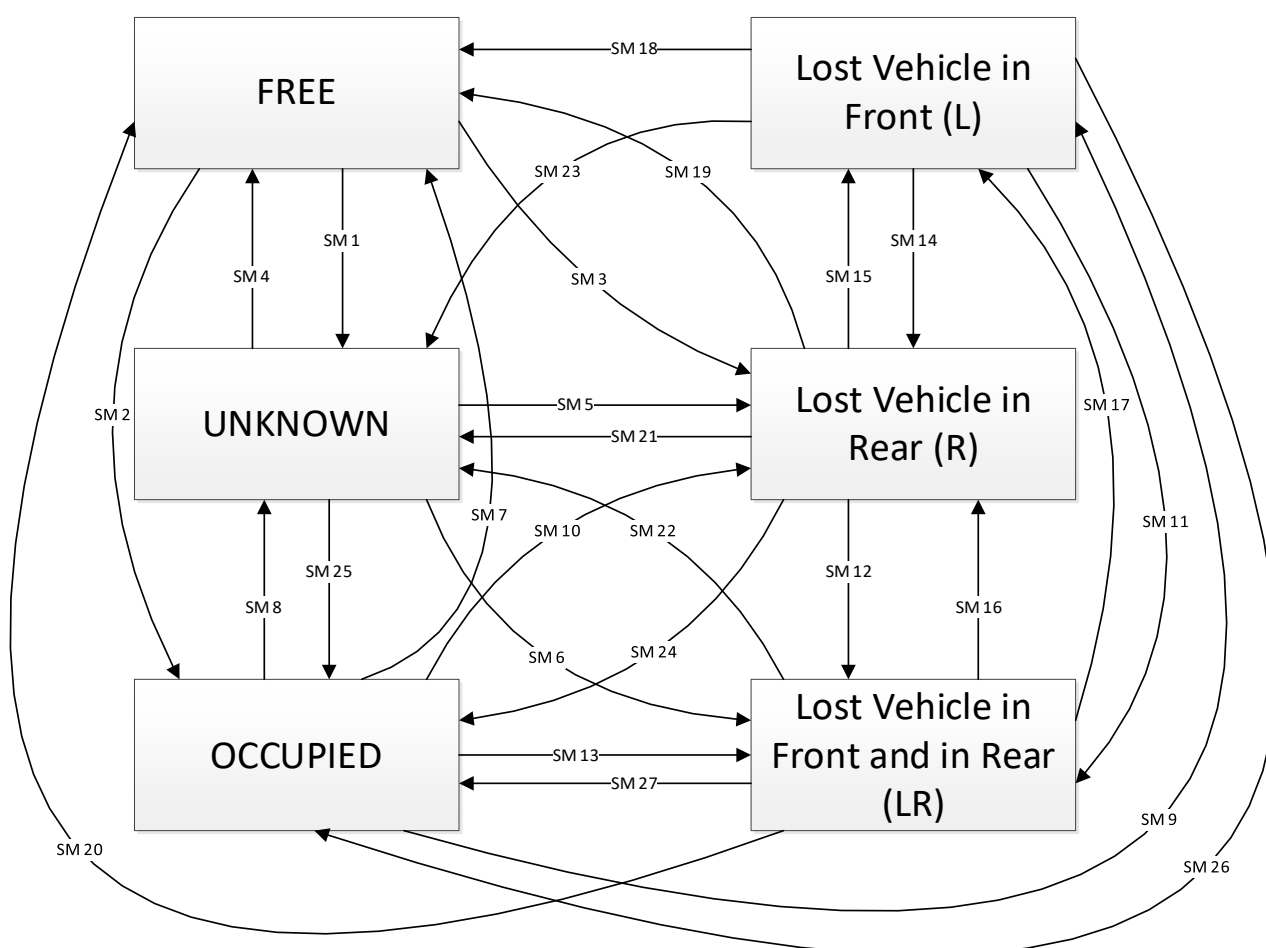


Figure 2 VSS section state diagram for SM

APP_0005

The state machine of the Table 4 is activated, instead of the one defined in Table 3, when a train located in the Supervised Manoeuvre Area has reported a safe consist length in front of the engine

different from zero. When the state machine is activated, the VSS in state “ambiguous” become “Lost Vehicle in Front and in Rear (LR).

Rationale:

In this way it is expected to use the state machine only when Supervised Manoeuvre Movements are needed.

APP_0006

It shall be ensured that the consist in Supervised Manoeuvre will be stopped after a loss of connection (to continue the operation in Shunting with appropriate Operational Procedures). This can be achieved for example:

- With an appropriate value of T_NVCONTACT for Supervised Manoeuvre operation;
- With Section Timers of the SM MA;

Note: It is expected that operation in Supervised Manoeuvre will be normally performed in stations, not in dedicated shunting areas.

Rationale:

The radio connection is expected to be needed for proper operation in Supervised Manoeuvre. If the radio connection is not available, the mode Shunting should be used.

APP_0007

For consists in Supervised Manoeuvre Mode the trackside will not treat a consist as integer with potential vehicle in front of the active cab according to the consist orientation if one of the following events occurs:

- a) the consist reports decreased safe consist length in front of the active cab according to the consist orientation
- b) the consist is located on at least one VSS where there is also another train located in front of the active cab according to the consist orientation
- c) the VSS in advance of the consist location according to the consist orientation becomes “unknown” due to propagation
- d) a propagation timer of the VSS in advance of the consist location according to the consist orientation expires or a ghost train propagation timer in advance of the consist location according to the consist orientation expires.

Rationale:

In Supervised Manoeuvre the lost vehicle can be in front or in rear of the active cab. The information of the safe consist length allows to understand where the lost vehicle can be.

APP_0008

For consists in Supervised Manoeuvre Mode the trackside will not treat a consist as integer with potential vehicle in rear of the active cab according to the consist orientation if one of the following events occurs:

- a) the consist reports decreased safe consist length in rear of the active cab according to the consist orientation
- b) the consist is located on at least one VSS where there is also another train located in rear of the active cab according to the consist orientation
- c) the VSS in rear of the consist location according to the consist orientation becomes “unknown” due to propagation
- d) a propagation timer of the VSS in rear of the consist location according to the consist orientation expires or a ghost train propagation timer in rear of the consist location according to the consist orientation expires.

Rationale:

In Supervised Manoeuvre the lost vehicle can be in front or in rear of the active cab. The information of the safe consist length allows to understand where the lost vehicle can be.

APP_0009

In areas where Supervised Manoeuvre is used, an “integrity loss propagation timer” is assigned to each VSS and for each direction.

Rationale:

The propagation in case of loss of integrity is directional in Supervised Manoeuvre areas, because the lost vehicle can be in front or in rear of the engine.

APP_0010

The direction of the propagation for the integrity loss propagation timer in areas where Supervised Manoeuvre is used is established according to the side, where the lost vehicle can be according to the requirements APP_0007 and APP_0008.

Rationale:

The propagation in case of loss of integrity is directional in Supervised Manoeuvre areas, because the lost vehicle can be in front or in rear of the engine.

5.3 LOW DENSITY APPLICATION REQUIREMENTS

This section presents the requirements for applications that want to use HL3/HTD to achieve cost reduction. These applications are expected to be low density applications, where performance is not a critical point.

APP_0011

In the specific portions of line where there is not an extensive use of TTDs, there shall be at least a VSS free between the EoA of a MA and the train in advance of the EoA.

Rationale:

This is to avoid the negative effects caused by the loss of connection of the train and the conditions e) and f) of the requirement HL3/HTD_0071.

APP_0012

In the specific portions of line where there is not an extensive use of TTDs, the presence of a shadow or ghost trains must be detected at the entrance of the line.

In case a ghost or shadow train is detected, the transitions #11B, #12A shall be inhibited in the whole portion of the line without extensive use of TTD until the presence of the shadow or ghost train is excluded.

Note: Some possibilities are:

- Use 1 or more sections with TTD to detect and possibly block all the “shadow trains”
- Keep track of the total length of the trains that enter the line, taking into account the accuracy requirements for the train lengths established by the specific applications (See §5.3 of D15.2).

Rationale:

In the open line, when probably just a single TTD is used, excluding the presence of shadow and ghost trains can become difficult.

APP_0013

Each specific application shall evaluate the possible impact of the use of the radio hole track condition, considering that in the radio hole it will be not possible to send updated MAs to stop the trains, change the direction, withdraw the MA as in L2-TTD and it will not possible to receive position reports with integrity confirmed etc.. The HL3/HTD trackside offers the following possibilities:

- The use of the radio hole timer to detect the possible anomalies in the radio hole;
- The check of the confirmed rear end at the end of the radio hole, to detect possible integrity loss in the radio hole, using for example the wait integrity timer;
- The possibility to follow the sequence of occupation of the TTDs.

Rationale:

The radio hole can be used to achieve cost reduction in low density applications, trying to minimize the cost for the radio communication network on the open line. Anyway the operational and safety aspects shall be considered.

APP_0014

Each specific application shall define the reaction of the dispatcher/Traffic Management System in case the radio hole timer expires.

Rationale:

When the radio hole timer expires, it is expected that a problem has occurred inside the radio hole. The specific application shall take appropriate not harmonised measures.

5.4 REQUIREMENTS WITH OPERATIONAL IMPACT

OPE_0001

Each specific application shall indicate to the driver the appropriate way to react to the System status message “Train data changed”.

Rationale:

The System status message “Train data changed” can be more frequent in HL3/HTD applications, in particular if splitting and joining are performed. The driver shall be properly trained to understand the meaning of this message and react according to the operational rules of the specific application.

OPE_0002

The operational procedures for sweeping have to be established by the Specific Application, in particular it shall be established:

- What are the conditions to have an acceptable level of confidence that there is no train or set of lost wagons in the “unknown” VSS;
- What are the conditions to send the MA to the sweeping train;
- What has to be done if the sweeping train finds a section that is really occupied by a vehicle.

Rationale:

Sweeping, if adopted by the specific application of HL3/HTD, can be a new type of operation, that shall be properly managed. Even applications that have already sweeping (for example to clear a section with axle counters in ETCS Level 2) may need to define additional procedures.

OPE_0003

The operational procedures for the recovery of a failed train have to be established by the Specific Application.

Rationale:

Procedures for the recovery of a failed train are not harmonised and they shall be defined at National level.

OPE_0004

The specific application needs to train the drivers and the operators for the specific situations that can happen on an HL3/HTD line. In particular it may be possible that the driver of a chasing train will see the rear end signal of the chased train. This situation shall not decrease the trust of the various operators in the system.

Rationale:

It is important, in particular for high density applications, that the operators have a good trust in the technological system. Otherwise some benefits can be jeopardized.

6 ENGINEERING RULES

6.1 ENGINEERING RULES FOR MAIN LINES

6.1.1 General engineering issues

HL3/HTD introduces new functionalities compared to previous ETCS levels such as VSS, the utilization of Train Integrity, Train Length and Timers for managing the occupancy of these VSS. This chapter will establish specific engineering rules for these functionalities.

Train integrity – Eng. Rule 1

Train integrity can be confirmed by the driver, even though it is not recommended except for low-density lines.

It is up to the IM to configure the trackside to accept (train is considered integer) or not confirmation of integrity by the Driver.

Rationale:

Accepting confirmation of Train Integrity by the Driver provides a mechanism for clearing “unknown” track status areas.

Train integrity – Eng. Rule 2

The frequency of integrity reports to ETCS on-board should be defined considering traffic capacity and other operational situations that are reliant on train position reports, being higher than the position report frequency to avoid performance degradation (see also [CR940]).

Rationale:

The frequency of integrity reports to the ETCS on-board is not relevant from a safety perspective as long as the trackside safety system does not move the Confirmed Rear End of the reporting train until train integrity is confirmed or section is released based on TTD information.

Train integrity – Eng. Rule 3

IM shall define whether trackside authorises a MA for trains reporting Loss of integrity or No train integrity information for longer than “Wait Integrity Timer”.

IM may decide to apply this rule only for certain areas.

Rationale:

Authorising it could cause operational difficulties since this may prohibit a failed train from being moved to a siding.

Train integrity – Eng. Rule 4

Reaction when train reports Loss of integrity or it is assumed due to the expiration of the Wait Integrity Timer shall be engineered by the IM.

Rationale:

It may be configured differently depending on if the Loss of Integrity is intentional or not to balance safety and operational efficiency ensuring that emergency actions, like halting the train, are taken judiciously (specifically, this should be avoided in RV mode).

It can be determined if additional information such as the train's speed is used to ascertain whether the loss of integrity is intentional or not (splitting procedure) and generate a different response for each case.

VSS – Eng. Rule 2

The minimum length of the VSS will be limited, among other reasons, by the presence of sequential section release, if this means that jumping trains are not allowed. The sizing of the VSS will also

consider the delays implemented in the sequential change of the occupation of blocks, i.e, the minimum time the system needs to consider the train located in two consecutive VSS at the same time, if any. This criterium does not apply to TTDs with single VSS.

Rationale:

This is established in order to cope with the different implementations of sequential section release.

VSS – Eng. Rule 3

In the places where an acknowledgement window for SH can be programmed, a single VSS in rear of the start location of the shunting profile will cover the associated acknowledgement window in such a way that the EVC can only enter in SH mode with the train located in that VSS.

This rule applies if no other constraint impedes it.

Rationale:

This is proposed to have an optimal management of the entrance in SH mode.

VSS – Eng. Rule 4

If there is no operational need, no marker board should be placed between a marker board with release speed and the start of the release speed monitoring area related to it. Regarding the possible presence of VSS borders within this distance, this can be achieved by accordingly sizing (if feasible) the VSS in rear of the aforementioned stop marker board, if a marker board is required to be installed at the VSS border, or not placing any marker board at the VSS border.

Rationale:

This is proposed to have a reduced use of marker boards.

VSS – Eng. Rule 5

Outside a radio hole, a VSS should not overlap on two adjacent TTDs, i.e. the border points of a TTD are also border points of adjacent VSSs.

Rationale:

This is to avoid unnecessary difficulties in the implementation of HL3/HTD functionality. In case of radio hole, the presence of TTDs can be used to have a mean to detect roll-away vehicles.

MuteTimer – Eng. Rule 1

The mute timer should be shorter than the communication session timer and longer than the time needed for an on-board to recover from a temporary loss of connection. It is recommended the mute timer is comparable to the value given to T_NVCONTACT.

Rationale:

If the timer is too short the track sections in advance of the train will be treated as “unknown” while no risk of real occupation exists. As the movement authority has already been reserved and sent to the train, the marking of these track sections for train movement as “unknown” by the trackside will have no direct performance impact. However, other related timers, e.g., the disconnect propagation timer, could start earlier.

If the timer is too long, it is possible that a train could move undetected (in rear of its former EOA) to other track sections. A possible scenario is that the route over these track sections is revoked and used for another train's movement.

WaitIntegrityTimer – Eng. Rule 1

Recommended is a value comparable to the position report cycle time [T_CYCLOC]. This timer shall be shorter than the mute timer.

Rationale:

If the timer is too short, trains with integrity confirmed which report “no train integrity information available” due to a lower integrity reporting frequency will be treated as integrity lost. Other related timers, e.g., the integrity loss propagation timer, could start earlier. This could also impact performance.

If the timer is too long, it is possible that a train loses its integrity without any system reaction.

The need for a wait integrity timer shorter than the mute timer is described in § 8.

ShadowTrainTimer – Eng. Rule 1

Recommended is a value in range of 5 to 10 seconds.

Rationale:

If the timer is too short, the trackside must assume a shadow train and keep the track section in ambiguous state while there is no risk. A next train must sweep this section or the whole track section must be freed based on TTD information.

If the timer is too long, it is possible that a real shadow train is undetected. This could lead to the risk that, if the next track section is left by the train with integrity confirmed, the track section is wrongfully treated as free, and another train could get an authorisation for this track section.

In the framework of this deliverable only this general recommendation is made, and ultimately it is down to application projects to determine a safe value for their specific application and to build the

safety case according to the features of the specific application, like operational rules, national values, TTD features, permissive reds etc. In particular various examples of sources of shadow trains have already been mentioned in the deliverable [11].

Of course the specific application may even conclude in its safety case that moving shadow trains are not realistic. In the §8 some example calculations are illustrated for the cases where moving shadow trains are deemed possible.

ShadowTrainTimer – Eng. Rule 2

The recommended distance between the last balise group in rear of a TTD border and the TTD border in the HL3/HTD line should not exceed.

$$[(length\ of\ the\ shortest\ train\ in\ the\ line) - 5m - Q_{LOCACC}] \cdot \frac{100}{5}$$

Rationale:

This rule is established taking into account what it is expected according to requirement 5.3.1.1 of SUBSET 041. When the L_DOUBTUNDER exceeds the train length, the shadow train timer will be not be started because the max safe rear end can be in advance of the real front end, so when the TTD gets occupied, the max safe rear end is already in advance of the TTD.

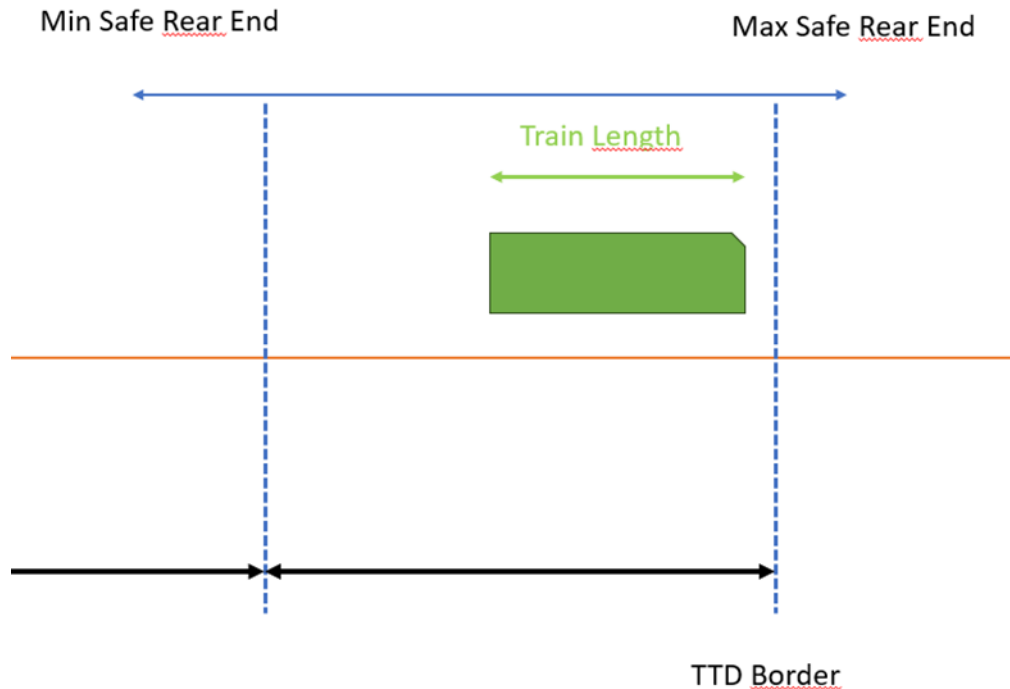


Figure 3 Unwanted situation – Max Safe Rear End in advance of real train front end.

DisconnectPropagationTimer – Eng. Rule 1

Recommended is a value in range of 5 to 15 minutes.

Rationale:

- If the timer is too short, the track sections in advance of the movement authority and in rear of the train will be treated as “unknown” while no risk of real occupation exists. These track sections could be already reserved for other train movements, and this will result in emergency revocation of movement authorities.
- If the timer is too long, it is possible that a train moves undetected (in advance of its former EoA or backwards) to other track sections. The possibility of movements depends for example on the value of M_NVCONTACT (no reaction keeps the MA), when the driver uses the Override EoA procedure or closes/opens the desk and SR is prompted at SoM due to lack of communication session. A possible scenario is that the train moves (forwards or backwards) to a track section which is reserved for another train’s movement.

GhostTrainPropagationTimer – Eng. Rule 1

Recommended is a value considering the expected time a TTD section could be passed by a ghost train, i.e., based on the length of the TTD section and the highest allowed speed.

Rationale:

- If the timer is too short, the trackside must assume a ghost train and set adjacent track sections to “unknown” while there is no risk. A next train must then sweep this section or the whole track section must be freed based on TTD information.
- If the timer is too long, it is possible that a ghost train has moved to another track section undetected. This could lead to the risk that, if the next track section is left by a train with integrity confirmed, the track section is wrongfully treated as free, and another train could get an authorisation for this track section.

IntegrityLossPropagationTimer – Eng. Rule 1

Recommended is a value in range of 5 to 15 minutes.

Rationale:

- If the timer is too short, the track sections in rear of the train will be treated as “unknown” while no risk of real occupation exists. These track sections could be already reserved for other train movements, and this will result in emergency revocation of movement authorities.
- If the timer is too long, it is possible that a piece of train moves undetected to other track sections. A possible scenario is that the train moves to a track section which is reserved for another train's movement.

IntegrityLossPropagationTimer – Eng. Rule 2

To manage appropriately the possibility of unintended train integrity loss, IM shall have the following information for each vehicle expected to be used on the line:

- The time the lost vehicle will be maintained at standstill by the rolling stock;
- The maximum time that the TIMS uses to confirm the integrity and if it is subject to unexpected delays.

It is up to the IM to decide if this information will be extrapolated:

- using access criteria (e.g. no access to trains that maintain lost vehicle at standstill less than a certain time) or
- by building a database of trains that can be present in the line or
- identifying only the worst train, (typically the one that maintain the vehicle at standstill for the lowest amount of time) and configuring the trackside timers.

Rationale:

Unintentional train integrity loss can generate dangerous situations when roll away vehicles are generated. For this reason it is important that appropriate reactions are taken in order to mitigate or prevent this possibility.

6.1.2 Engineering Rules for Operational procedures

Start of Mission Eng. Rule 1

In the VSS where SoM is expected to be executed, the train must be able to determine its position (via balises or ASTP).

If the train needs to move to achieve a valid position, the risk of movement of trains in SR mode shall be considered.

Rationale:

The movement of the train with an unknown position should be normally contained within the VSS where the SoM is executed.

End of Mission Eng. Rule 1

The Infrastructure Manager shall consider the provision of TTD in areas where EoM is likely to occur.

Rationale:

To prevent the propagation of the “unknown” state once the EoM is executed and the disconnect propagation timer expires.

Shunting Eng. Rule 1

The Infrastructure Manager shall define Permanent and Temporary Shunting Areas where operationally required. The borders of a permanent Shunting Area shall coincide with TTD boundaries.

Rationale:

To protect shunting activities from other authorised train movements and to protect authorised train movements from shunting activities.

Level Transition Eng. Rule 1

Detection of trains, even without communication, entering the HL3/HTD area must be ensured. The entry in this area must match the entry in a TTD.

Rationale:

To prevent a train from entering the HL3/HTD area unnoticed and support establishing track status.

Supervised Manoeuvre Mode Eng. Rule 1

Areas where Supervised Manoeuvre is operated shall have a short TTD section in order to avoid propagation from the areas outside.

Rationale:

In order to allow sweeping of the Supervised Manoeuvre Area, it is good to detect if lost vehicles are coming from outside.

Supervised Manoeuvre Mode Eng. Rule 2

The borders of VSSs in Supervised Manoeuvre Area shall be visible to the driver.

Rationale:

This is made to facilitate sweeping.

Splitting & Joining Eng. Rule 1

Intentionally deleted.

Reversing Eng. Rule 1

Intentionally deleted.

6.1.3 Engineering Rules for Degraded scenarios**Unintentional Loss of train integrity Eng. Rule 1**

Railway operators shall define procedures according to their Safety Management System in case of detection of Train Integrity Loss. In this procedure the following aspects must be considered:

- If the MA is modified to allow the train to be taken to a siding or stopping point
Note: This could be prevented by Train integrity – Eng. Rule 3
- If once at the siding or stopping point, Driver can confirm integrity
Note: This could be prevented by Train integrity – Eng. Rule 1

Rationale:

The management of unintentional train integrity loss is currently not harmonized, so the railway operators may have different solutions on the basis of the specific line and the specific train implementation.

Trains without OTI-I Eng. Rule 1

IM shall define in which situations and places is allowed the entry into the HL3/HTD area of trains that are not able to confirm train integrity.

Rationale:

In general this choice can be done according to the needs of the specific application. In some applications all the trains will be allowed, in other cases, in particular if there is a significant reduction of the number of TTDs, the entrance of these trains should be avoided as much as possible.

Trackside system restart after shutdown Eng. Rule 1

In case the trackside system performs a restart, the system must assume a safe state of the trackside, i.e., “unknown”. Methods are needed to resume to a known state.

Rationale:

This is needed in order to ensure the safety. According to the specific operational procedures, sweeping can be used to allow the recovery of the normal operation.

OTI-I Eng. Rule 1

Intentionally deleted.

6.2 ENGINEERING RULES FOR LOW DENSITY LINES

Radio holes Eng. Rule 1

Radio hole area should preferably be included inside the same VSS, except if there are multiple TTDs inside this Radio Hole.

Rationale:

This is to avoid that an authorisation ends inside the Radio Hole. If there are multiple TTDs, then the RBC will need to make sure that the authorisation does not end inside the Radio Hole.

Radio holes Eng. Rule 2

Measures must be implemented to resolve additional connection loss near a Radio Hole, for example:

In the following (adaptation of Figure 16 in 5.18.5 of the SRS), where points D and E indicate the beginning and end of the Radio Hole Area as received from the RBC, it is defined point F, in relation to point D, at the distance the train would cover running at the maximum permitted speed within the time specified for the Mute Timer.

After MaxSFE passes point F, the first Position Report received by HL3/HTD Trackside initiates the Radio Hole Timer with a value: time needed to travel from the reporting position up to the expected place where the first Position Report after the Radio Hole is received plus the time estimated for the train, running from that location.

After MaxSFE is reported beyond point D, HL3/HTD Trackside resets the Radio Hole Timer with a value: time estimated for the train, running from that location.

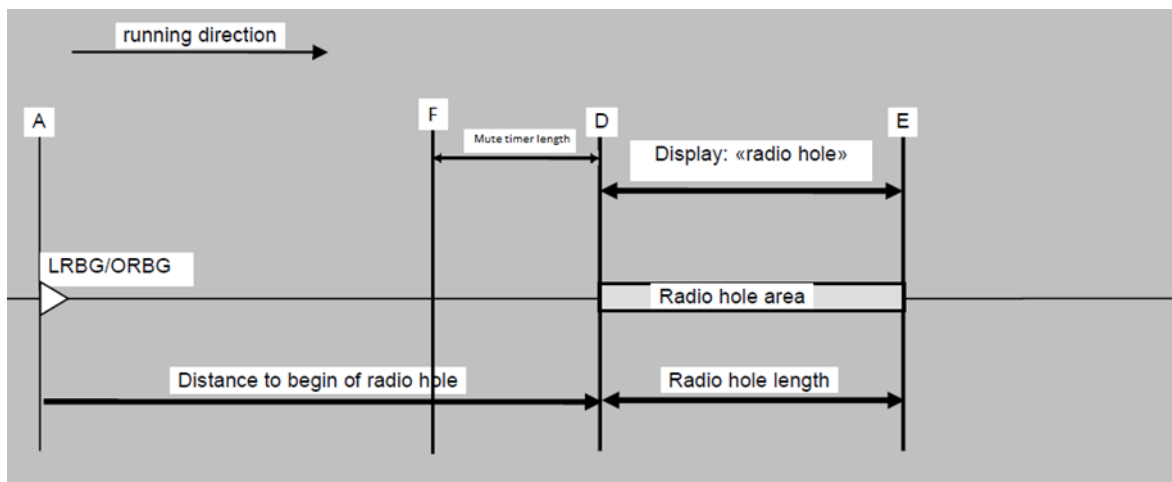


Figure 4 Radio Hole

Rationale:

This allows that the Radio Hole timer is started even if the train does not report the MaxSFE beyond the start of the Radio Hole area due to a connection loss between point F and D. If a connection loss takes place and the train is not able to report the MaxSFE between F and E, the mute timer expires and the Radio Hole timer is not started, so this serves to identify connection loss in the proximity of the Radio Hole area.

VSSs and TTDs Eng. Rule 1

In zones where SoM and splitting/joining are normal operations, the presence of 3 TTDs (coincident with VSS) is proposed (see below).



Figure 5 Proposed SoM Area

Rationale:

TTD2 is expected to be extended enough to manage all the splitting and joining. Balise Groups BG1 and BG2 are intended to be used to allow the train to get a valid position and be able to confirm its integrity, they may be duplicated if deemed necessary. TTD1 and TTD3 have 2 main functions:

- Avoid propagation from the rest of the line to TTD2 and vice versa.
- Allow the triggering of the transition #11A.

In general it is expected that TTD1 and TTD3 will be quite short, in this way they will be normally free, allowing to trigger the transition #12A in case the train has connection problems where it is on the open line (probably composed by a single TTD with a large number of VSSs). To be sure to trigger transition #11A, in particular in case of short values of shadow train timer, various engineering solutions are possible, taking into account that the start condition for the shadow train timer is the reporting of the max safe rear end inside the TTD:

- Limitation of the speed of the trains in TTD1 and TTD3;
- Use of location parameters for the position report parameters (see for example 3.6.5.1.5 b) and c) of SUBSET 026).

7 CONCLUSIONS

HL3/HTD is a solution that can be implemented quickly by reusing the existing infrastructure and with modifications to the on-board system for the introduction of integrity verification and train length calculation.

This should allow to increase the capacity of the lines on the one hand and to simplify the management of the infrastructure on the other, for example on regional lines. All this by having a system on the ground that in case of fault in normal operation allows to have under control the presence of trains on the line. For example, for regional lines it is conceivable to have very long physical sections with many VSSs inside them. On the main lines instead, maintaining the current physical sections would reduce the distance between trains thanks to the introduction of VSSs inside them.

What has emerged is that the transition from ETCS L2 to HL3/HTD is relatively simple. Of course the detailed migration can be more or less complex according to the complexity of the specific applications.

In this specification some features have been tagged as optional, because not all the specific applications may need them. Moreover some features have been developed only for high density or only for low density applications.

In comparison to the starting point of the EUG Specification [4], additional scenarios, as example:

- storage of the train length;
- use of slave engines;
- supervised manoeuvre;

have been considered. Of course, on the basis of the needs of the specific applications, it is possible that additional features are developed, for example the use of axle counters and the association of master and slave engines.

Regarding the following topics, mentioned in D15.2 for further developments, the situation at the date of the emission of this deliverable is the following:

- Accuracy requirements for train lengths: Assumption [Pre 15] has been established, it may be incorporated in the future in some accuracy requirements for train lengths, but at the moment the discussion is not mature enough;
- Interface with DAC, OTI-I and OTI-L: the discussion is not mature enough for a general solution, in particular regarding the DAC. There are a certain number of projects on-going regarding these devices, their results are expected to consolidate further the situation;

In §10 there is a summary of the open points coming from D15.1 and the related solutions. Even with these limitations, this specification is deemed compliant to what it is expected by R2DATO Grant Agreement, considered the budget and time constraints and it is expected to be released publicly for all the following works of the interested stakeholders.

8 DETAILED RATIONALES

Detailed Rationale for the requirements HL3/HTD_0037, HL3/HTD_0038, HL3/HTD_0039 and HL3/HTD_0040. Considerations about the ShadowTrainTimer – Eng. Rule 1

The shadow train timer is intended to be used to detect shadow trains, using TTD limits. This timer is started multiple times when the train is on a TTD that has a certain length, but only the last start of the timer is critical for the detection of shadow trains. In particular, considering a nominal case when the timer is started for the last time in the situation depicted in the figure:

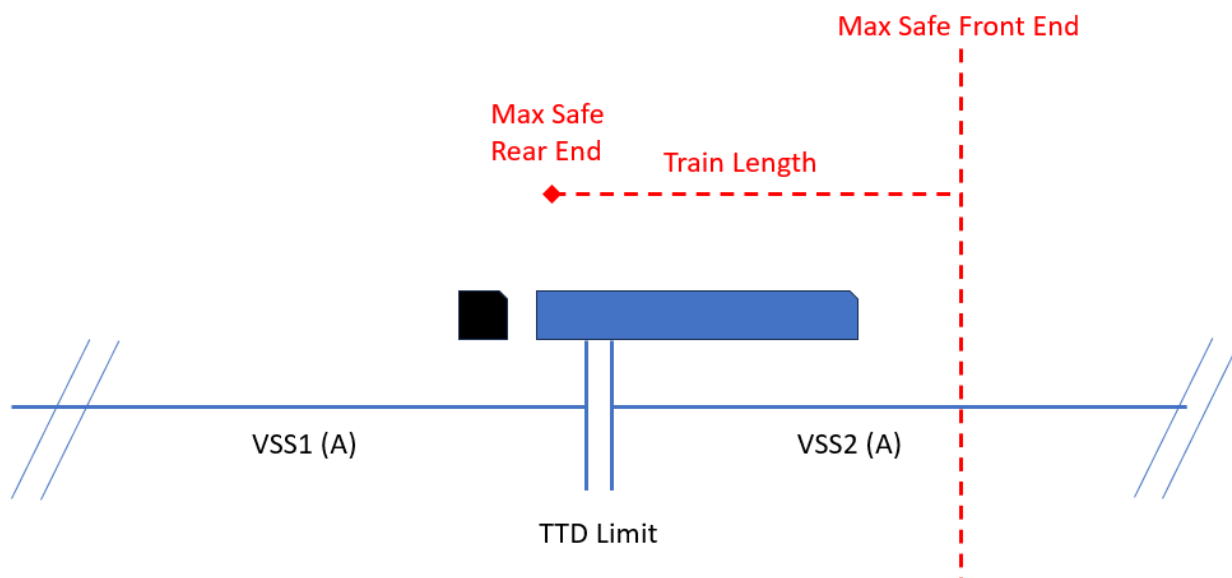


Figure 6 Step 1 Shadow Train Timer

The trackside is able to detect that no shadow train is present if the TTD in rear becomes free with the timer still running, in the situation of the following figure:

If the

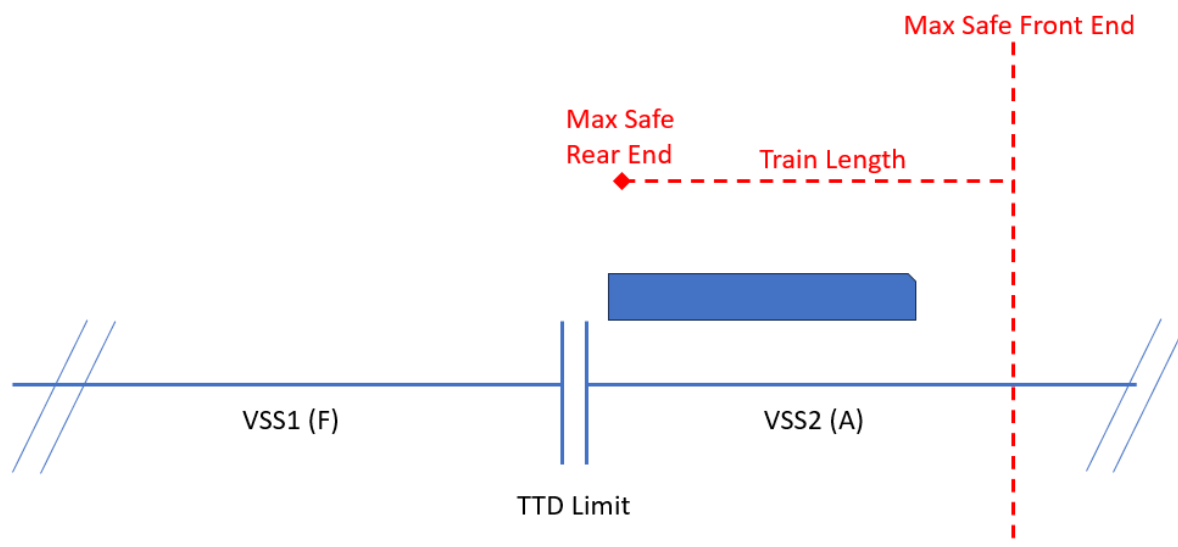


Figure 7 Shadow Train Timer Best Case Situation

If the TTD remains occupied, it can be concluded that a shadow train is present, as depicted in the following picture.

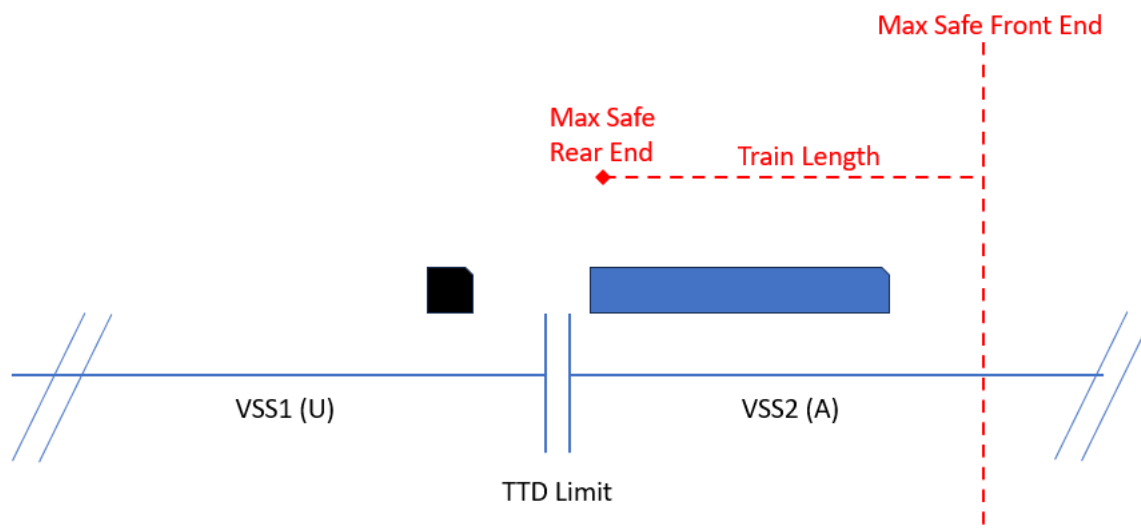


Figure 8 Shadow Train Timer Worst Case Situation

The figures above depict nominal cases, of course the specific application of the shadow train timer shall consider the specific constraints of the application, in particular:

- The delay in the transition from occupied to free of the TTD;
- The possibility of the over-estimation of the train length;
- The minimal length of shadow trains that are considered possible in the specific application;

If one of the events described by the requirement HL3/HTD_0071 happens, the timer is stopped, because there is no guarantee that the first train is integer, and a shadow train can't be excluded.

The shadow train timer is composed of 2 main factors, as described in the requirement HL3/HTD_0039:

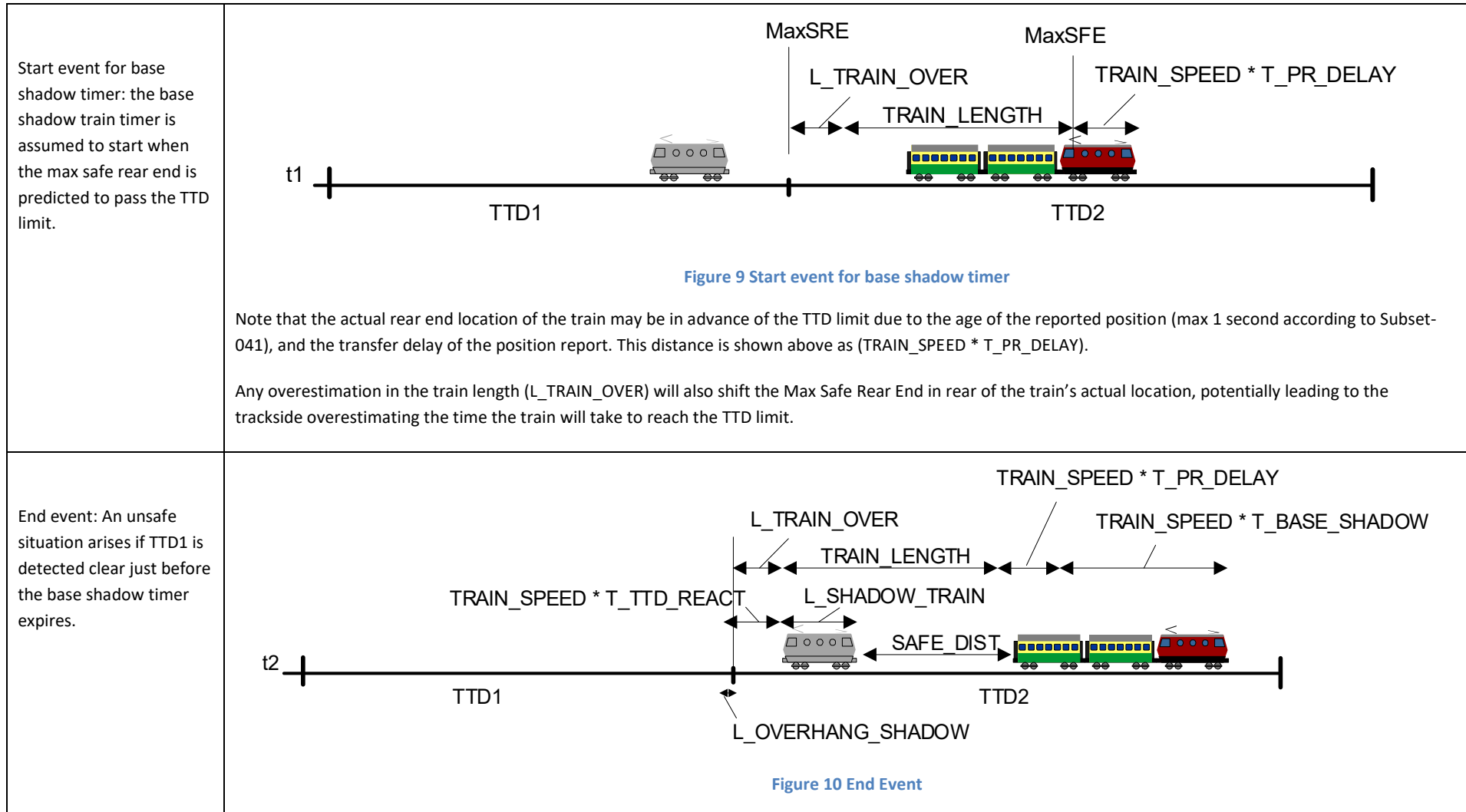
- *“a base timer value determined by the specific application taking into account systematic issues like position report transfer delay and TTD delays;*
- *the time to cover the distance from the last reported max-safe-rear to the TTD-limit, with a maximum of the position_report_period time (to be on the safe side an acceleration shall be assumed).”*

It can be inferred from this description that, in order to remove the shadow train risk (i.e. to determine that there is no shadow train closely following the communicating train), the TTD must clear within a certain time (i.e. the base shadow timer) of the max safe rear end of the train passing the TTD boundary. The purpose of the second bullet is because the trackside is expected to predict when the event of the max safe rear end passing the TTD limit will take place, taking into account the reported speed and position of the train.

Clearly, both the base timer value and the additional time based on the reported speed and position will affect the safety of the shadow train function. For example, if the trackside overestimates the time it will take for the max safe rear end of the train to reach the TTD limit, then this can interfere with the ability to detect a shadow train. Similarly, systematic errors and delays, which should be taken into account in the base timer value, can also interfere with the ability to safely detect a shadow train.

Given that the trackside's prediction of when the max safe rear end will reach the TTD limit will vary greatly depending on the reported speed and position of the train, this paragraph analyses only the systematic errors and delays that affect the base value of the shadow train timer and the safety of the shadow train function, leaving to the specific applications the random factors, that are strongly dependent on that context.

The following table illustrates the hazardous situation that may lead to the erroneous removal of the shadow train risk (please note that the figure does not show the actual proportion between the trains).



--	--

Table 5 Hazardous Situation

Regarding the figures above:

- $\text{TRAIN_SPEED} * \text{T_BASE_SHADOW}$ is the distance covered by both trains during the base shadow train timer, assuming both trains travel at a constant speed.
- $\text{TRAIN_SPEED} * \text{T_PR_DELAY}$ is the distance that the train may be ahead of its reported position, due to the age of the position estimation and radio transfer delay.
- TRAIN_LENGTH is the actual length of the communicating train.
- L_TRAIN_OVER is the amount by which the train length is overestimated in train data.
- L_SHADOW_TRAIN is the length of the shadow train.
- L_OVERHANG_SHADOW is the distance between the last axle of the shadow train and the rear end of the shadow train.
- $\text{TRAIN_SPEED} * \text{T_TTD_REACT}$ is the distance travelled during the time taken for the TTD to clear behind the shadow train. The faster the TTD reaction time, the higher the likelihood that a shadow train may go undetected.
- SAFE_DIST is the distance within which a shadow train would have to follow the preceding train to be undetected.

As illustrated above, an unsafe situation arises at t_2 if the last wheel of the shadow train is detected clear of the TTD1 and the shadow train timer has not yet expired. Therefore, an unsafe situation arises if the shadow train follows the preceding train within a distance of:

$$\text{SAFE DIST} = (\text{TRAIN_SPEED} * \text{T_BASE_SHADOW}) + (\text{TRAIN_SPEED} * \text{T_PR_DELAY}) + \text{L_TRAIN_OVER} + \text{L_OVERHANG_SHADOW} + \text{L_TTD_UNCERTAINTY} - \text{L_SHADOW_TRAIN} - (\text{TRAIN_SPEED} * \text{T_TTD_REACT})$$

The factor L_TTD_UNCERTAINTY is the location accuracy of the TTD limit, not shown in the picture for easiness. If the axle counter head or track circuit joint is installed in rear of its nominal location, then this can also lead to the value of the timer being overestimated by trackside, with the shadow train clearing the TTD quicker than expected.

The following table provides an example of how closely the shadow train must follow the communicating train in order to go undetected, for a train speed of 30km/h and a base shadow timers from 1 to 10 seconds, with fast TTD reaction time.

Note: the actual speed can be a little bit higher or lower than the expected speed in SR mode.

Total PR delay (s)	2.50	2.50	2.50	2.50	2.50	2.50	2.50	2.50	2.50	2.50
train speed (km/h)	30	30	30	30	30	30	30	30	30	30
train length overestimation (m)	3	3	3	3	3	3	3	3	3	3
max overhang of shadow train (rear end to last axle) (m)	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2
min TTD reaction time	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
min length of shadow train (m)	12	12	12	12	12	12	12	12	12	12

Base shadow train timer value (s)	1	2	3	4	5	6	7	8	9	10
Location accuracy of the TTD limit	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
A shadow train may be undetected if it follows the preceding train within this distance. (m)	20.40	28.73	37.07	45.40	53.73	62.07	70.40	78.73	87.07	95.40

Table 6 Example 1

If we assume that the shadow train is being driven by a driver, and we consider a service brake deceleration rate of around 0.7 m/s/s, the braking distance required would be approximately 50m. If we also factor in driver reaction time of around 2 seconds, as well as brake reaction time of around 3 seconds, then the total braking distance required from a speed of 30 Km/h would be around 90m. Therefore, even with a shadow train timer of up to 10 seconds, it can be seen that at a speed of 30 kph the shadow train would have to be driven dangerously close the train in front in order for the shadow train to go undetected.

Of course, the shadow train could also be an uncontrolled vehicle, in which case any assumptions about how closely that may be driven to the train ahead become invalid, which may justify using lower base timer values.

The following table provide an example of how closely the shadow train must follow the communicating train in order to go undetected, for a train speed of 40km/h and a base shadow timers from 1 to 10 seconds, with parameters deemed typical in WP16:

- 1,5 of train length overestimation (almost 0 for single rolling stock units, more for longer trains);
- 1,5 seconds of TTD reaction time;
- 40 km/h as typical speed in SR for the shadow train;
- Length of the shadow train of 12 m;

Total PR delay (s)	2.50	2.50	2.50	2.50	2.50	2.50	2.50	2.50	2.50	2.50
train speed (km/h)	40	40	40	40	40	40	40	40	40	40
train length overestimation (m)	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5	1,5
max overhang of shadow train (rear end to last axle) (m)	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2
min TTD reaction time	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5
min length of shadow train (m)	12	12	12	12	12	12	12	12	12	12
Base shadow train timer value (s)	1	2	3	4	5	6	7	8	9	10
Location accuracy of the TTD limit	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2

A shadow train may be undetected if it follows the preceding train within this distance. (m)	16.12	27.23	38.34	49.46	60.57	71.68	82.79	93.90	105.01	116.12
--	-------	-------	-------	-------	-------	-------	-------	-------	--------	--------

Table 7 Example 2

Given the fact that the total braking distance required from a speed of 40 Km/h would be around 145m, even in this case the values recommended in **ShadowTrainTimer – Eng. Rule 1** seem feasible.

The following table provide an example of how closely the shadow train must follow the communicating train in order to go undetected, with the typical parameters of the previous example but with a big train length overestimation (50 m) and an high speed context (5 m overhang).

Total PR delay (s)	2.50	2.50	2.50	2.50	2.50	2.50	2.50	2.50	2.50	2.50
train speed (km/h)	40	40	40	40	40	40	40	40	40	40
train length overestimation (m)	50	50	50	50	50	50	50	50	50	50
max overhang of shadow train (rear end to last axle) (m)	5	5	5	5	5	5	5	5	5	5
min TTD reaction time	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5
min length of shadow train (m)	12	12	12	12	12	12	12	12	12	12
Base shadow train timer value (s)	1	2	3	4	5	6	7	8	9	10
Location accuracy of the TTD limit	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
A shadow train may be undetected if it follows the preceding train within this distance. (m)	65.42	76.53	87.64	98.76	109.87	120.98	132.09	143.20	154.31	165.42

Table 8 Example 3

In this case base shadow train timer values of less than 8 seconds seem advisable but the evaluation if such big overestimation is realistic is left to the specific application.

Detailed Rationale for the requirement HL3/HTD_0069 and WaitIntegrityTimer – Eng. Rule 1

There can be some critical cases, where the protection given by the wait integrity timer is jeopardized, if the wait integrity timer is not shorter than the mute timer, as established in the engineering rule WaitIntegrityTimer – Eng. Rule 1. Please see the following figure.

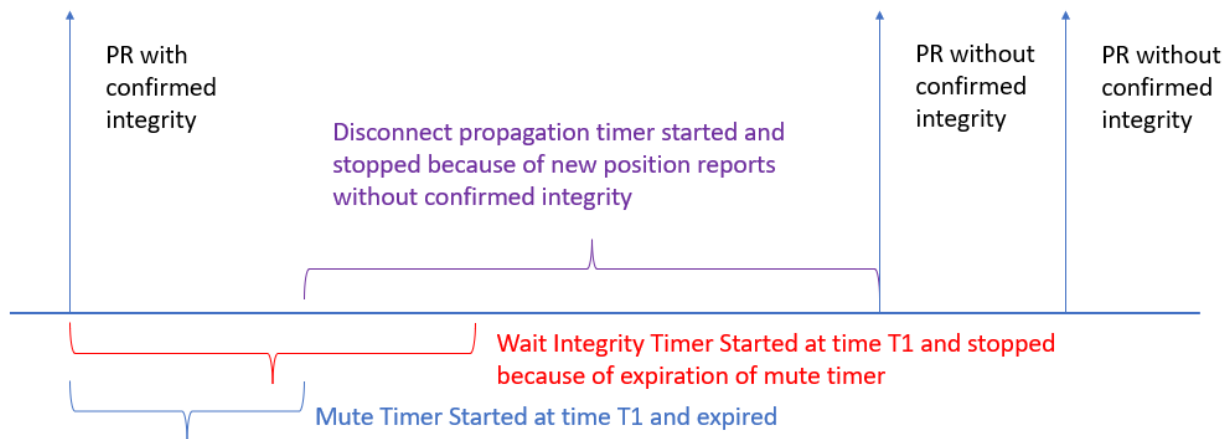


Figure 11 Interaction between Mute Timer and Wait Integrity Timer

If, after the start of the wait integrity timer, the mute timer expires, the wait integrity timer is stopped and the disconnect propagation timer is started. Anyway, once a new position report without confirmed integrity is received by the trackside, the disconnect propagation timer is stopped and the wait integrity timer will be not started anymore until there is a new confirmation of the integrity. To avoid this, the wait integrity timer shall be shorter than the mute timer, as established by the engineering rule. In this way, when the PR without confirmed integrity is received, the wait integrity timer is already expired and the condition b) of the requirement HL3/HTD_0071 is applicable. The integrity loss propagation timer is then started. In this theoretical worst case scenario, the reaction to train integrity loss may be delayed, the specific application needs to consider this when establishing the value of the timers.

9 OPERATIONAL SCENARIOS

In the following paragraphs there is a description of various operational scenarios, that are possible on a line that uses a HL3/HTD Specification. In the figures there is the following simbology:

- VSSs can be ambiguous (orange), free (green), occupied (yellow) and unknown (red);
- TTDs can be free (green) or occupied (yellow)
- Trains can be disconnected (red), connected (green) or complete (blue)

Other symbols can be used in specific scenarios.

9.1 OPERATIONAL SCENARIO 1: NOMINAL START OF MISSION AND INITIAL MOVEMENT WITH VSS/TTD TRANSITIONS

Introduction	This operational scenario shows a nominal situation where there is a SoM without the use of the optional requirements to maintain the state occupied after End of Mission and Start of Mission. There is normal transition to occupied using a free TTD in rear and transition #11A. A particular engineering of position report parameters is used, to try to facilitate transition #11A and minimize the number of position report sent by the train. This type of engineering is anyway not mandatory, it is just an example
Assumptions	<ul style="list-style-type: none"> • The HL3/HTD Trackside can trust the information received from the On-board about the train integrity status (Q_INTEGRITY) and the confirmed train length (L_TRAININT).
Preconditions	<ul style="list-style-type: none"> • There is a train parked in a station with all desks closed. The ETCS On-board is in SB mode with no communication session but registered to a radio network. There is a part of track in the station with some VSSs with status "Unknown". • The trackside has no stored data about this train, so there is no memorised train location nor any stored NID_ENGINE or train length. • All the propagation timers, eventually started in the past, have expired. • Starting conditions is depicted in the Figure 12. • The train does not provide the safe consist length information • Valid train data are not stored on-board
Notes	<p>This use case takes origin from the use cases UC_01_07, UC_17_01 and UC_17_02 from deliverable D15.1.</p> <p>All the timers, once started, do not expire if not explicitly mentioned.</p> <p>All the MAs are sent together with the needed information, hence applicable mode profile if applicable, linking if applicable, all the applicable profiles.</p>
Legenda	<p>In the figures the following simbology is used:</p> <p>VSSs can be ambiguous (orange colour), free (green colour), occupied (yellow colour) and unknown (red colour)</p> <p>TTD can be free (green colour) or occupied (yellow colour)</p> <p>Disconnected trains are red, connected trains are green, complete trains are blue</p>

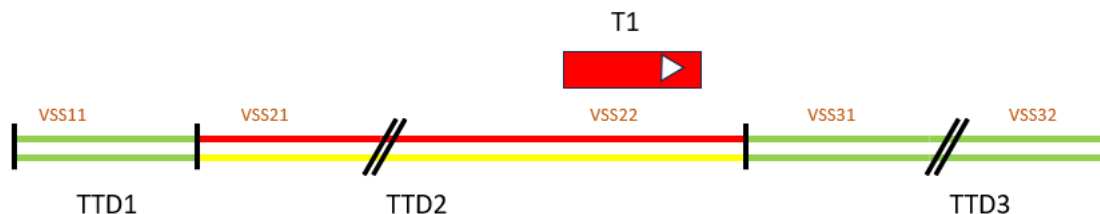


Figure 12 Starting Condition Operational Scenario 1

- 1) ETCS On-board initiates the Start of Mission procedure; the stored position and level are still valid. The Driver is requested to revalidate or change the Driver ID and is offered to revalidate or change Train Running Number.
- 2) ETCS On-board opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159)
- 3) The mute timer for train T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the requirement HL3/HTD_0089.

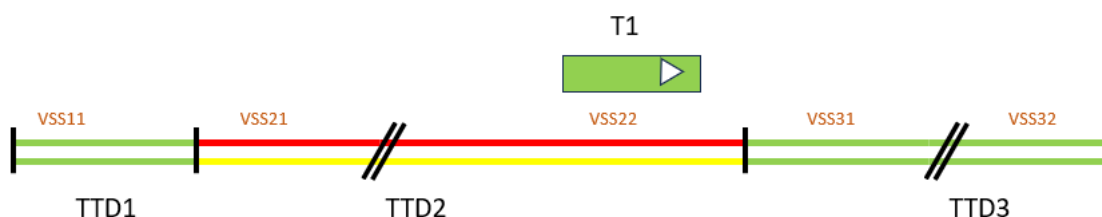


Figure 13 Step 3 Operational Scenario 1

- 4) The session is established. After the successful establishment of the communication, the train sends the SoM Position Report according to the state A33 of § 5.4.3.2 of SUBSET 026 .
- 5) The front end of train T1 is now located in VSS22 that becomes ambiguous (transition #5A). 2 shadow train timers for train T1 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

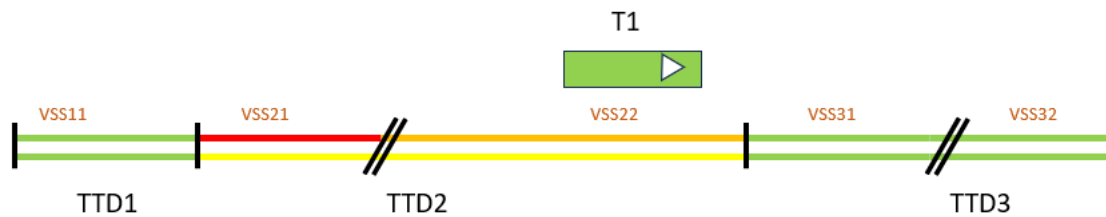


Figure 14 Step 5 Operational Scenario 1

6) Driver enters or (re-) validates the Train Data. The Train Length may be provided by OTI-L, by the driver or it can be a fixed pre-configured value. This value shall be able anyway to fulfil the safety requirements, otherwise the ETCS On-Board will never confirm its integrity.

7) ETCS On-board sends the Validated Train Data to the HL3/HTD Trackside, including a position report with no train integrity information.

8) HL3/HTD Trackside acknowledges having received Validated Train Data. HL3/HTD Trackside uses received Train Length info to locate the assumed rear end. The integrity loss propagation timer is not started because the condition c) of HL3/HTD_0071 is applicable only to trains that have previously a valid train length.

The trackside sends to the train the position report parameters periodic in time in order to allow the sending of the first position report with integrity confirmed in the following step. (Note: In this scenario in the step 9) different parameters will be sent on the basis of the sent MA. This functionality is anyway optional, the trackside is free to maintain the train position parameters sent at this step, if it is desired). MA request parameters are sent according to the rules of the specific application.

9) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I).

10) No update of the state of the VSSs is made by the HL3/HTD trackside, because there are not the conditions identified in other requirements to set the VSS to occupied (for example there is no assigned train length). The train is now complete according to the HL3/HTD trackside. The wait integrity timer is assigned according to the requirement HL3/HTD_0034 and immediately started according to the requirement HL3/HTD_0035.

The max safe rear end of the train is in VSS22 and the direction of the train is towards VSS31, so the shadow timer towards VSS31 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

(Note: It is in principle possible that the max safe rear end is already in TTD3. In that case the shadow train timers of TTD2 will be not started, to try to avoid this behaviour engineering rule ShadowTrainTimer – Eng. Rule 2 has been established)

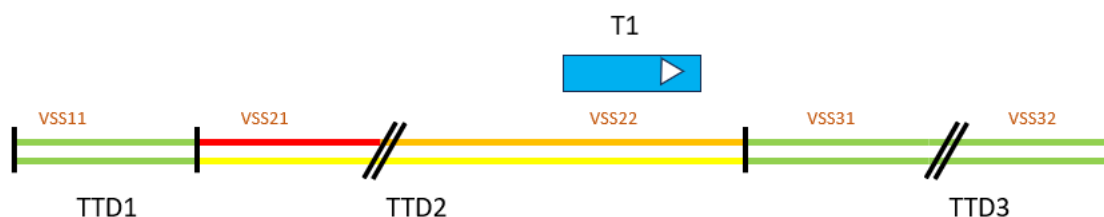


Figure 15 Step 10 Operational Scenario 1

- 11) The driver selects “Start” and the Train sends a MA Request according to the requirement 3.8.2.1.1 of SUBSET 026.
- 12) Trackside sends an MA that crosses the TTD2 border until the end of TTD3, this may contain an OS mode profile according to the specific rules for TAF used in each country. The trackside sends with the MA the following position report parameters:

Variable	Length	Value
NID_PACKET	8	58
Q_DIR	2	Nominal
L_PACKET	13	Calculated Length
Q_SCALE	2	According to the specific application
T_CYCLOC	8	According to the specific application
D_CYCLOC	15	According to the specific application
M_LOC	3	According to the specific application
N_ITER	5	4
D_LOC(1)	15	Value in order to trigger the sending of the position report when the max safe front end of T1 reaches VSS31
Q_LGTLOC(1)	1	1 (Max safe front end)
D_LOC(2)	15	Value in order to trigger the sending of the position report just before the max safe rear end of T1 leaves TTD3
Q_LGTLOC(2)	1	1 (Max safe front end)
D_LOC(3)	15	Value in order to trigger the sending of the position report when the max safe front end of T1 reaches VSS32
Q_LGTLOC(3)	1	1 (Max safe front end)
D_LOC(4)	15	Value in order to trigger the sending of the position report with confirmed integrity immediately after the confirmed rear end leaves VSS31
Q_LGTLOC(4)	1	0 (Min safe rear end)

Table 9 Position Report Parameters for Step 9

In the following figure the position report locations are depicted with lightning figures, blue when the max safe front end is involved, red when the min safe front end is involved. The lightning figures of the position reports are deleted once the position report is sent.

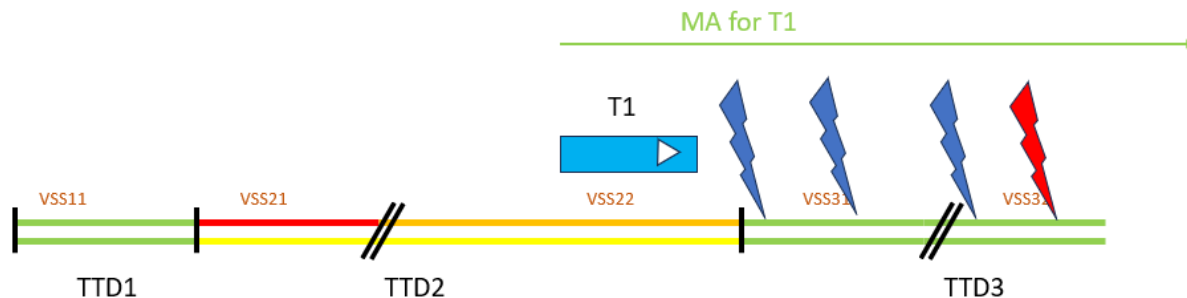


Figure 16 Step 12 Operational Scenario 1

13) The train T1 starts moving. When the train T1 reaches with the max safe front end the location D_LOC(1), it sends a position report to the HL3/HTD trackside

14) According to the requirement HL3/HTD_0006 there is no update of the state of the VSS when the trackside receives the position report. When TTD3 gets occupied, the train location is updated by the HL3/HTD trackside according to the requirement HL3/HTD_0005 and VSS31 becomes ambiguous according to the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD3, according to the requirement HL3/HTD_0037.

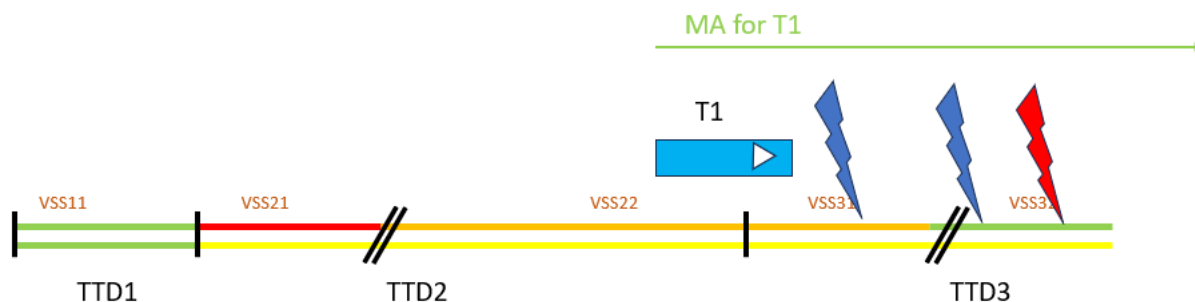


Figure 17 Step 14 Operational Scenario 1

15) When the train T1 reaches with the max safe front end the location D_LOC(2), the train T1 sends a position report with integrity confirmed, with the max safe rear end of the train still in the TTD2.

16) Following the reception of the position report of step 15 the shadow train timer is re-started for train T1 on TTD2 for the last time.

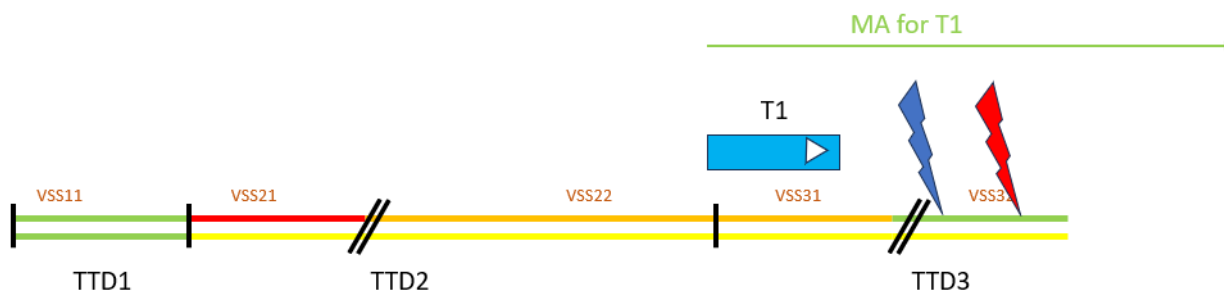


Figure 18 Step 16 Operational Scenario 1

17) When the TTD2 becomes free, all the VSSs in the TTD2 are set to free (transition #9A for VSS22, transition #4A for VSS21). VSS31 becomes occupied (transition #11A) because the shadow train timer of train T1 related to TTD2 is not expired when TTD2 becomes free. Once the transition #11A is performed, the shadow train timers related to TTD2 are deleted according to HL3/HTD_0037.

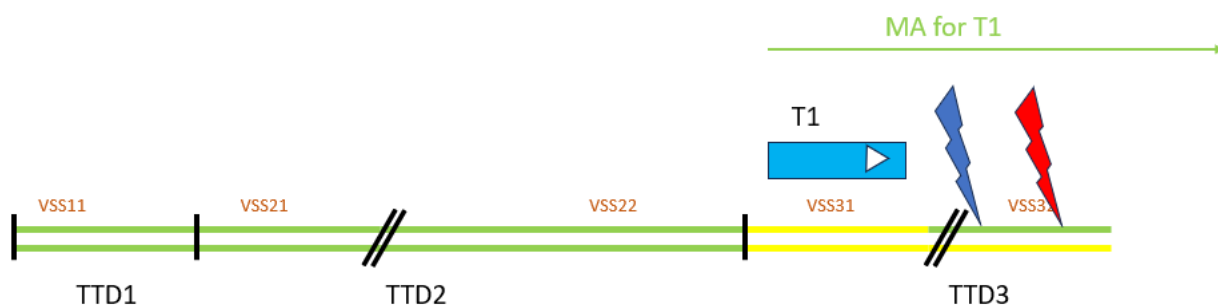


Figure 19 Step 17 Operational Scenario 1

18) When the train T1 reaches with the max safe front end the location D_LOC(3), the train T1 sends a position report with integrity confirmed, with the max safe rear end of the train inside VSS32.

19) VSS32 becomes occupied according to the requirement HL3/HTD_0005 and the transition #2A. The shadow train timer of TTD3 in direction of VSS32 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

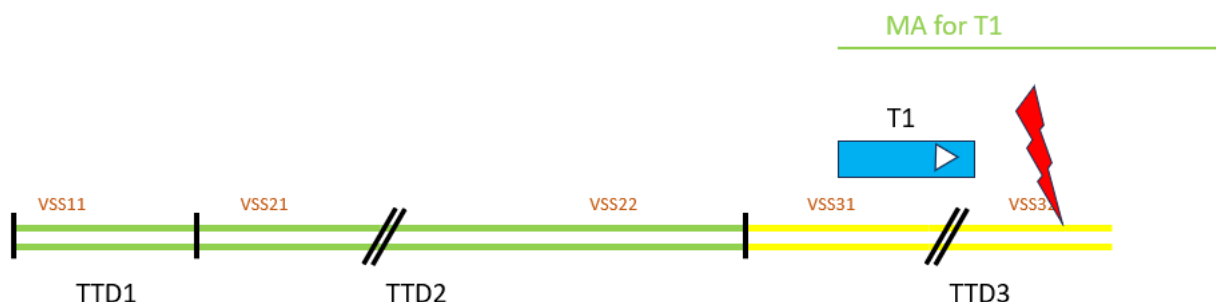


Figure 20 Step 19 Operational Scenario 1

20) When the train T1 reaches with the min safe front end the location D_LOC(4), the train T1 sends a position report with integrity confirmed, with the confirmed rear end of the train outside VSS31 (This is expected to be achieved by appropriate engineering of distance D_LOC(4) if the time needed by the OTI-I to confirm the integrity is known at least approximately by the Infrastructure Manager).

21) VSS31 becomes free according to the transition #2A.

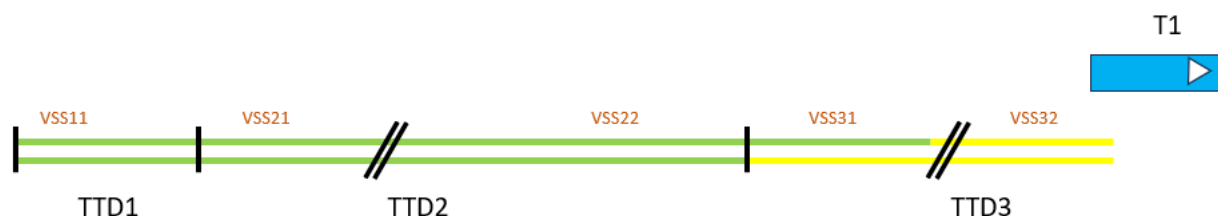


Figure 21 Step 21 Operational Scenario 1

9.2 OPERATIONAL SCENARIO 2: DEGRADED SoM WITH INVALID POSITION, CONNECTION LOSS AND GHOST TRAIN INTERACTION

Introduction	This operational scenario shows a degraded situation where there is a SoM with invalid position. The train is authorised to move via an SR authorisation. The train is located after the detection of a balise group and there is normal transition to occupied using a free TTD in rear and transition #11A. When the train is in the open line there is a loss of connection and the first train is stopped (e.g. because of T_NVCONTACT reaction). A lost vehicle starts to move and is detected as a ghost train. The vehicle enters in the section where there is the first train. The first train recovers the connection and proceeds, without setting the VSS in rear to free.
Assumptions	<ul style="list-style-type: none"> •The HL3/HTD Trackside can trust the information received from the On-board about the train integrity status (Q_INTEGRITY) and the confirmed train length (L_TRAININT). • With the opening of the desk there is a reset of the train integrity according to the assumption [Pre 13].

Preconditions	<ul style="list-style-type: none"> There is 1 train parked in a station with all desks closed. The ETCS On-board is in SB mode with no communication session but registered to a radio network. There is a part of track in the station with some VSSs with status “Unknown”. There is also a lost vehicle T2 in the TTD2. The trackside has no stored data about the trains, so there is no memorised train location nor any stored NID_ENGINE or train length. All the propagation timers, eventually started in the past, have expired. Starting conditions are depicted in the Figure 22 and Figure 23 Note: The initial situation may be caused by unintentional train integrity loss at standstill. The train does not provide the safe consist length information. Valid train data are not stored on-board. The trackside is engineered according to VSSs and TTDs Eng. Rule 1, in order to satisfy the requirement APP_0012 for low density lines. M_NVCONTACT is service brake or emergency brake. The switches adjacent to TTD2 are set for the diverted route, as depicted in Figure 22.
Notes	<p>This use case takes origin from the use cases UC_01_04, UC_05_01, UC_07_01 and UC_09_03 from deliverable D15.1 and from the hazardous scenario described in the figures from 1 to 6 of the deliverable D15.2.</p> <p>All the timers, once started, do not expire if not explicitly mentioned.</p> <p>All the MAs are sent together with the needed information, hence applicable mode profile if applicable, linking if applicable, all the applicable profiles.</p>
Legenda	<p>In the figures the following simbology is used:</p> <p>VSSs can be ambiguous (orange colour), free (green colour), occupied (yellow colour) and unknown (red colour)</p> <p>TTD can be free (green colour) or occupied (yellow colour)</p> <p>Disconnected trains are red, connected trains are green, complete trains are blue</p> <p>The name TTDXX is used for a TTD that is not crossed by the trains and the vehicles during their movement.</p> <p>Balise Groups are depicted as a couple of triangles.</p>



Figure 22 Track Layout Operational Scenario 2

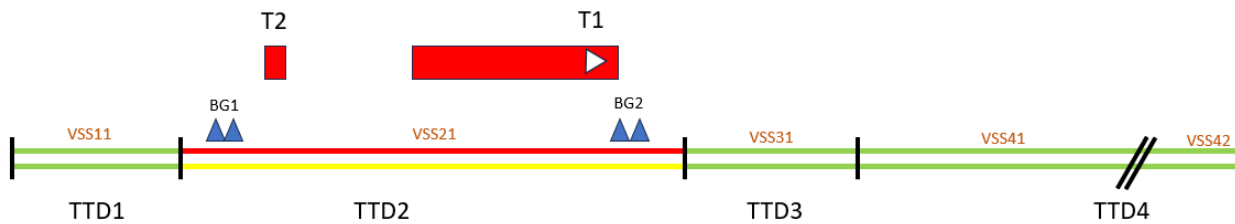


Figure 23 Starting Condition Operational Scenario 2

- 1) The driver opens the desk of train T1.
- 2) ETCS On-board of train T1 initiates the Start of Mission procedure; the stored position and level are invalid. The Driver is requested to revalidate or change the Driver ID and is offered to revalidate or change Train Running Number. ETCS On-board requests driver to enter level.
- 3) The driver enter level 2 in the ETCS On-board.
- 4) ETCS On-board of train T1 opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159).
- 5) The mute timer for train T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the requirement HL3/HTD_0089.
- 6) The train T1 sends the SoM Position Report according to the state A34 of § 5.4.3.2 of SUBSET 026. The position report contains invalid position (with no train integrity information) in SB mode.
- 7) HL3/HTD Trackside receives the Start of Mission Position Report, it does not validate the position in the state D33 of § 5.4.3.2 of SUBSET 026 but it accepts the train according to the state A23 of § 5.4.3.2 of SUBSET 026. There is no change to VSS states.
- 8) ETCS On-Board deletes the train position information after receiving the train accepted message, according to the state A24 of § 5.4.3.2 of SUBSET 026 .
- 9) Driver enters or (re-) validates the Train Data, including the Train Length (following a safe process or alternatively the Train Length is provided safely by OTI-L).
- 10) ETCS On-board sends the Validated Train Data to the HL3/HTD Trackside, including a position report with no train integrity information and position unknown.
- 11) HL3/HTD Trackside acknowledges having received Validated Train Data. The integrity loss propagation timer is not started because the condition c) of HL3/HTD_0071 is applicable only to trains that have previously a valid train length.
- 12) The HL3/HTD Trackside sends to the train the position report parameters periodic in time and at every LRBG compliant balise group. MA request parameters are sent according to the rules of the specific application.
- 13) The dispatcher may provide an estimated train position to the HL3/HTD Trackside.
- 14) The driver selects “start” and the train sends an MA Request.
- 15) The HL3/HTD Trackside authorises the train for movement in SR with an SR distance and optionally a list of balises that can be passed (based on the estimated train position provided by the dispatcher if applicable) in such a way that allows the train to get a valid position in a safe way. The SR distance may be conditioned to the number of the connected trains that are moving on the line in SR or to the size of the occupied TTDs in the line;
- 16) The train moves in SR.
- 17) The ETCS On-board reads a balise group, gets an unambiguous valid position and reports it to the HL3/HTD Trackside. The train integrity is still not confirmed because of the condition “(the train position was valid and was referred to an LRBG at the time the train was last known to be integer)” in condition [2] of Table 2b of SUBSET 026. It is supposed that the position report triggered by the passage of the LRBG

compliant balise group happens before the second confirmation of the train integrity by the OTI-I. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

18) The HL3/HTD Trackside receives the position report. The max safe front end of the train is located in VSS31 but the TTD3 is still free, so there is no update of the status of VSS31 according to the requirement HL3/HTD_0007. The assumed rear end is located in the VSS21, that becomes ambiguous according to the transition #5A.

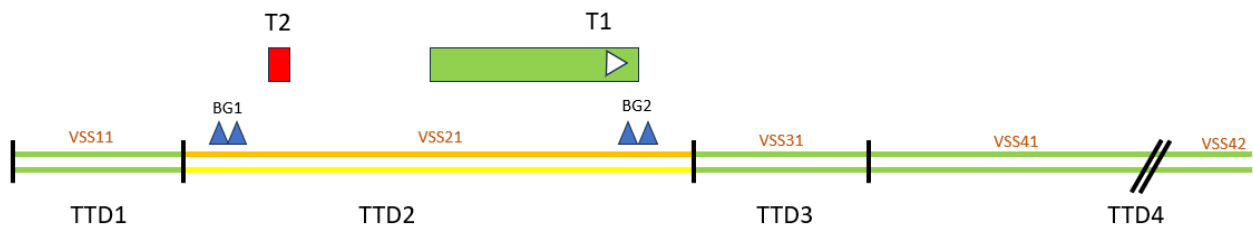


Figure 24 Step 18 Operational Scenario 2

19) The HL3/HTD Trackside sends an MA that crosses TTD2 and TTD3 borders until the end of VSS42, this may contain an OS mode profile according to the specific rules for TAF used in each country. The part of the MA that covers VSS41 and VSS42 has no mode profile.

Note: It is supposed that the HL3/HTD is able to react to the first position report before the train sets TTD3 to occupied.

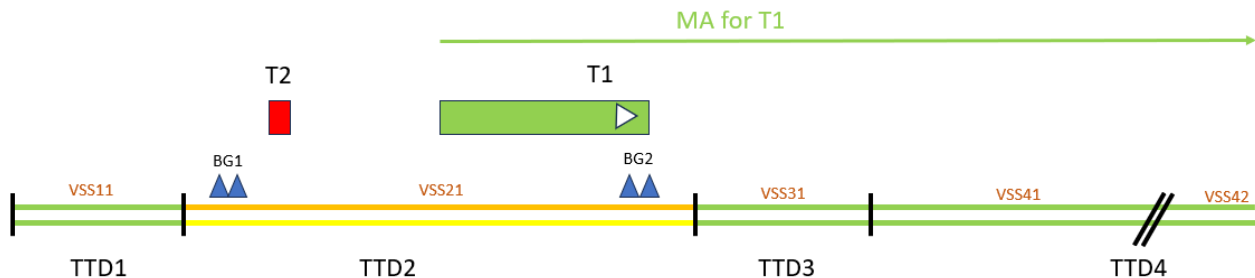


Figure 25 Step 19 Operational Scenario 2

20) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I).

21) The train is now complete according to the HL3/HTD trackside. The wait integrity timer is assigned according to the requirement HL3/HTD_0034 and immediately started according to the requirement HL3/HTD_0035. The max safe rear end of the train is in VSS21 and the direction of the train is towards VSS31, so the shadow timer towards VSS31 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

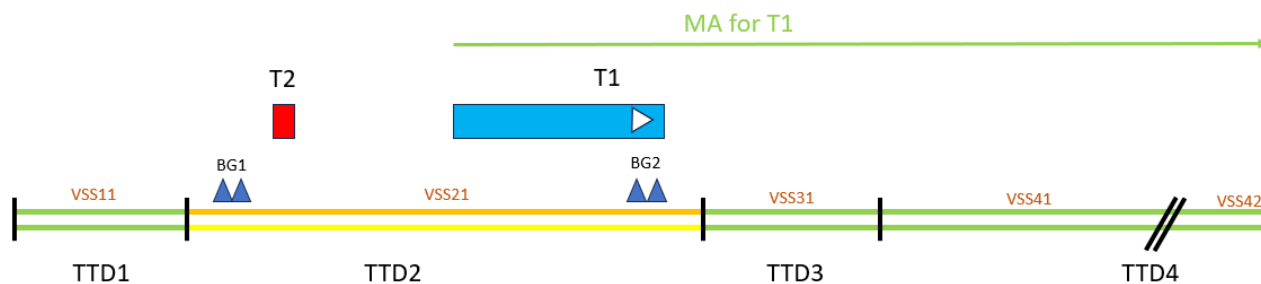


Figure 26 Step 21 Operational Scenario 2

22) TTD3 becomes occupied. VSS31 becomes ambiguous according to the requirement HL3/HTD_0007 and the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD3 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

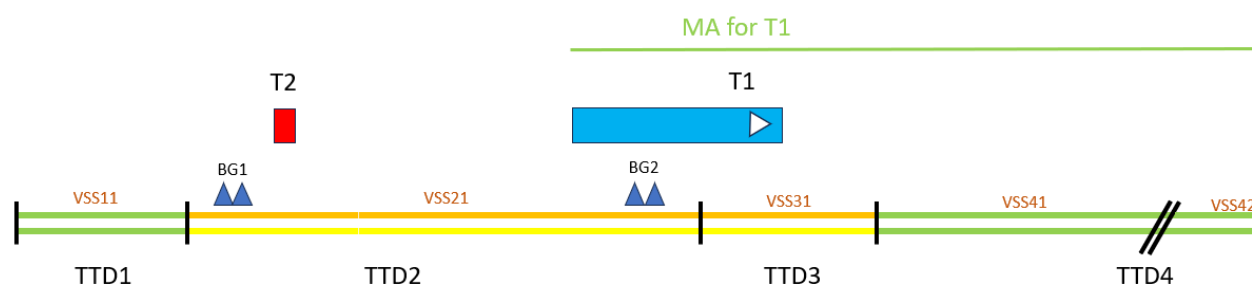


Figure 27 Step 22 Operational Scenario 2

23) TTD4 becomes occupied. VSS41 becomes ambiguous according to the requirement HL3/HTD_0007 and the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD4 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

Note: TTD3 is expected to be quite short

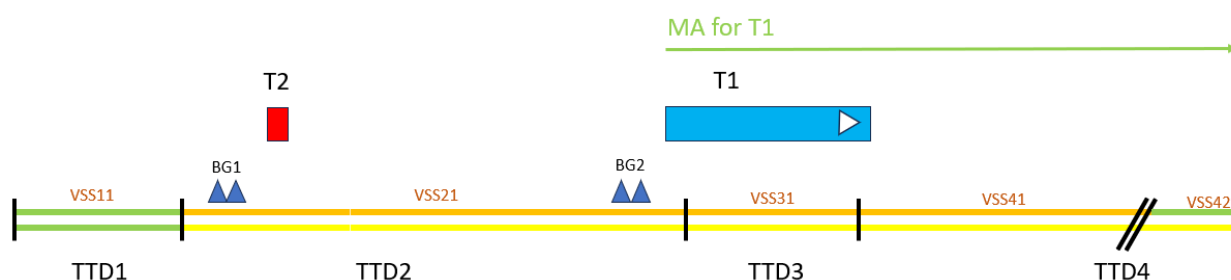


Figure 28 Step 23 Operational Scenario 2

24) ETCS On-board of Train T1 sends a position report with the min safe rear end in advance of the VSS21/VSS31 border.

25) VSS21 becomes unknown because it has been left by all the reporting trains and transition #10A is performed. The shadow train timers related to TTD2 are deleted according to HL3/HTD_0037. The max safe rear end of the train is in VSS31 and the direction of the train is towards VSS41, so the shadow timer

towards VSS41 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

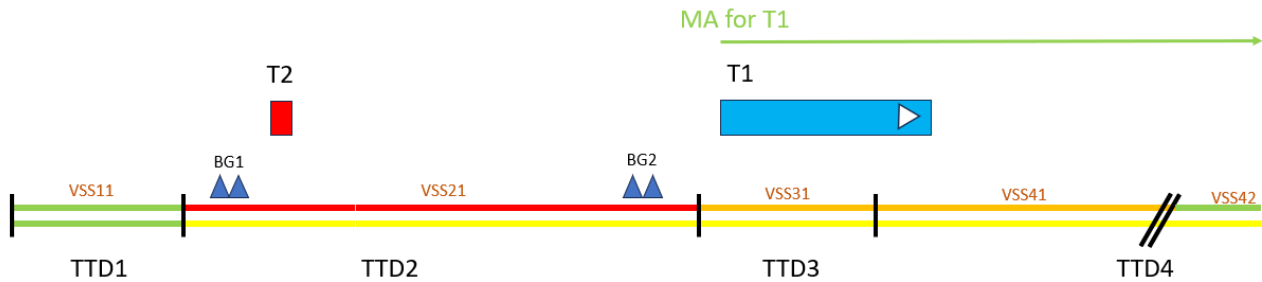


Figure 29 Step 25 Operational Scenario 2

26) When the TTD3 becomes free, VSS31 is set to free (transition #4A for VSS31). VSS41 becomes occupied (transition #11A) because the shadow train timer of train T1 related to TTD3 is not expired when TTD3 becomes free. Once the transition #11A is performed, the shadow train timers related to TTD3 are deleted according to HL3/HTD_0037.

Note: At the moment of this step the shadow train timer of train T1 related to TTD4 is already started, but it is not relevant.

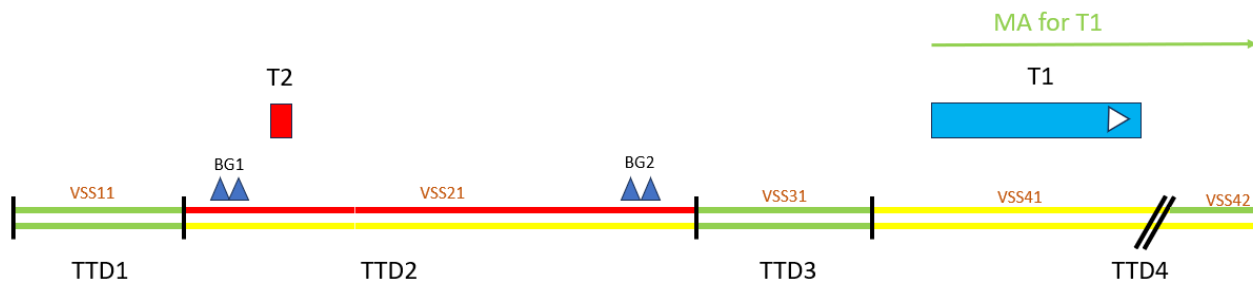


Figure 30 Step 26 Operational Scenario 2

27) The ETCS On-board of train T1 stops sending radio messages.

28) The wait integrity timer for train T1 expires. There is no update of the state of the VSSs, because condition b) of the requirement HL3/HTD_0071 is not fulfilled.

Note: According to WaitIntegrityTimer – Eng. Rule 1 the wait integrity timer is always shorter than the mute timer.

29) The mute timer for train T1 expires. HL3/HTD Trackside deems disconnected the train and stores the memorised train location. VSS41 become unknown (transition #7A). VSS42 becomes unknown (transition #1B). The disconnect propagation timers of VSS41 and VSS42 are started according to the requirement HL3/HTD_0057. The shadow train timers of TTD4 are no more assigned according to the requirement HL3/HTD_0037.

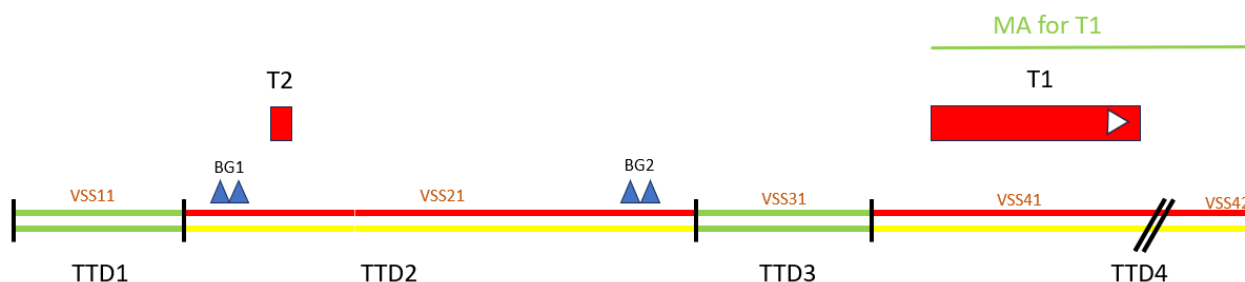


Figure 31 Step 29 Operational Scenario 2

30) The disconnect propagation timers expire. According to the condition c) of the requirement HL3/HTD_0054 the timers are stopped after the full processing of the state machine and then they are not considered expired anymore according to the requirement HL3/HTD_0054. There is no update of the state of the VSSs because TTD3 is free.

Note: It is supposed that the trackside maintains the MA even after the expiration of the disconnect propagation timer. This is compliant to the requirement HL3/HTD_0021, but a specific application may have a different choice.

31) The lost vehicle T2 starts moving.

Note: If T2 is the result of unintentional train integrity loss of T1, it may be that the movement is caused by the decrease of the pressure of the brake cylinder.

32) TTD3 gets occupied and VSS31 becomes unknown because of transition #1A. The ghost train propagation timer of TTD3 starts to the requirement HL3/HTD_0061.

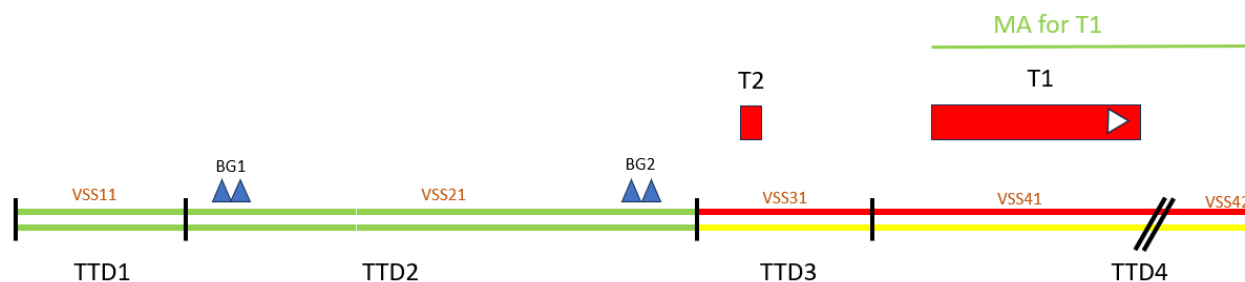


Figure 32 Step 32 Operational Scenario 2

33) TTD3 becomes free. According to the requirement HL3/HTD_0063 the ghost train propagation timer expires immediately and then it is stopped according to the requirement HL3/HTD_0062. According to the requirement HL3/HTD_0072 the transition #12A is inhibited in VSS41 and VSS42.

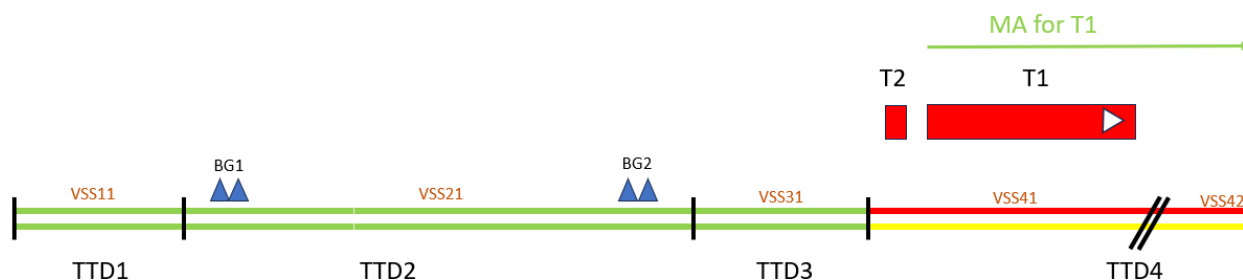


Figure 33 Step 33 Operational Scenario 2

34) Train T1 reconnects with the same train orientation, sending a position report with integrity confirmed.

35) HL3/HTD Trackside deems connected train T1 and VSS41 becomes ambiguous (transition #5A), because transition #12A has been inhibited in step 33. The mute timer and wait integrity timer for train T1 are re-started according to the requirements HL3/HTD_0032 and HL3/HTD_0035. VSS42 becomes free according to the transition #4B. The shadow train timers of TTD4 are assigned according to the requirement HL3/HTD_0037 and the shadow train timer of TTD4 towards the right is started according to the requirement HL3/HTD_0038 .

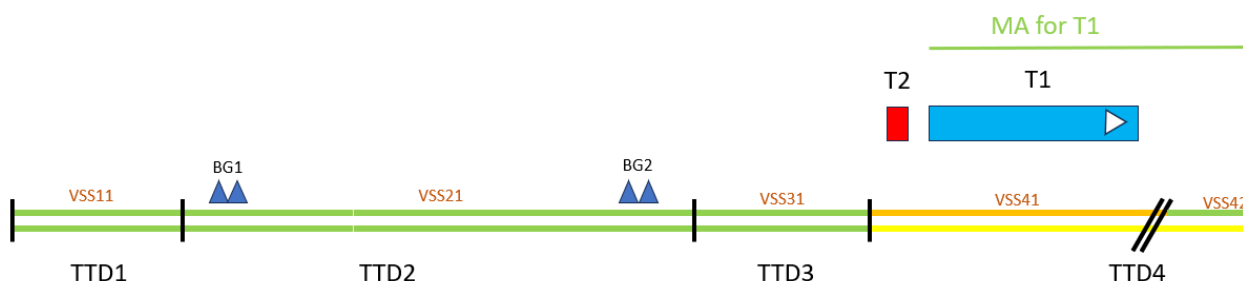


Figure 34 Step 35 Operational Scenario 2

9.3 OPERATIONAL SCENARIO 3: OPERATION IN RADIO HOLE WITH TIMER MANAGEMENT AND LEVEL TRANSITION

Introduction	This operational scenario shows a degraded situation where there is a SoM with unknown position. The train is authorised to move via an SR authorisation. The train is located after the detection of a balise group and there is normal transition to occupied using a free TTD in rear and transition #11A. The train receives an MA to enter a radio hole, that is used in the specific application to achieve cost reduction. The train comes out from the radio hole and makes the transition to another ETCS Level.
Assumptions	<ul style="list-style-type: none"> • The HL3/HTD Trackside can trust the information received from the On-board about the train integrity status (Q_INTEGRITY) and the confirmed train length (L_TRAININT).
Preconditions	<ul style="list-style-type: none"> • There is 1 train parked in a station with all desks closed. The ETCS On-board is in SB mode with no communication session but registered to a radio network. There is a part of track in the station with some VSSs with status “Unknown”. • The trackside has no stored data about the trains, so there is no memorised train location nor any stored NID_ENGINE or train length. • All the propagation timers, eventually started in the past, have expired. • Starting conditions are depicted in the Figure 35 and Figure 36. • The train does not provide the safe consist length information. • Valid train data are not stored on-board. • The trackside is engineered according to VSSs and TTDs Eng. Rule 1, in order to satisfy the requirement APP_0012 for low density lines. • M_NVCONTACT is service brake or emergency brake. • The switches adjacent to TTD2 are set for the diverted route, as depicted in Figure 35. • An appropriate Radio Hole timer is set in the HL3/HTD Trackside for the expected duration of travel through the Radio Hole. • Radio Hole is covered by a single VSS (named VSSRH) and the borders of the track condition Radio Hole coincide with TTD boundaries. In the Radio Hole there are the TTDs from TTD5 to TTD26. • Radio Hole timer start location is engineered in rear of the Radio Hole according to Radio holes Eng. Rule 2
Notes	<p>This use case takes origin from the use cases UC_01_05, UC_04_01, UC_07_01, UC_08_01 and UC_09_03 from deliverable D15.1.</p> <p>All the timers, once started, do not expire if not explicitly mentioned.</p> <p>All the MAs are sent together with the needed information, hence applicable mode profile if applicable, linking if applicable, all the applicable profiles.</p>

Legenda	<p>In the figures the following simbology is used:</p> <p>VSSs can be ambiguous (orange colour), free (green colour), occupied (yellow colour) and unknown (red colour)</p> <p>TTD can be free (green colour) or occupied (yellow colour)</p> <p>Disconnected trains are red, connected trains are green, complete trains are blue</p> <p>The name TTDXX is used for a TTD that is not crossed by the trains and the vehicles during their movement.</p> <p>Balise Groups are depicted as a couple of triangles.</p> <p>When, inside the Radio Hole, the borders of the TTDs does not coincide with borders of VSS, only the border of the TTD is depicted</p>
---------	--

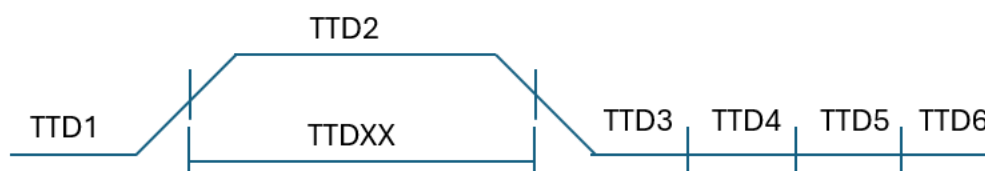


Figure 35 Layout of SoM and initial Radio Hole Area

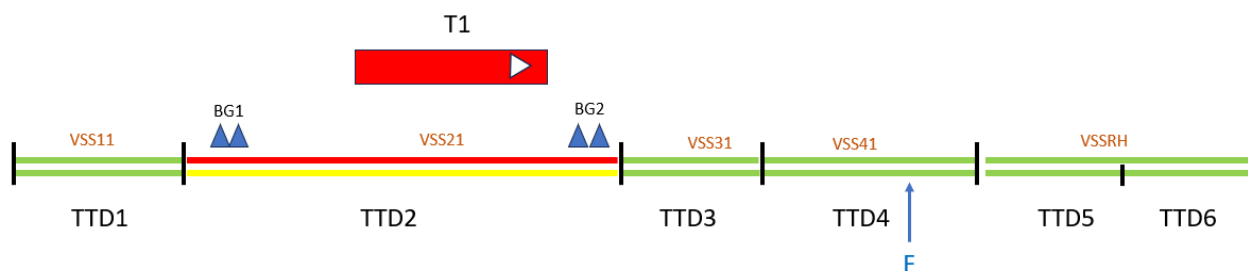


Figure 36 Starting Condition Operational Scenario 3

- 1) The driver opens the desk of train T1.
- 2) ETCS On-board of train T1 initiates the Start of Mission procedure; the stored position and level are unknown. The Driver is requested to revalidate or change the Driver ID and is offered to revalidate or change Train Running Number. ETCS On-board requests driver to enter level.
- 3) The driver enter level 2 in the ETCS On-board.
- 4) ETCS On-board of train T1 opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159).
- 5) The mute timer for train T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the requirement HL3/HTD_0089.
- 6) The train T1 sends the SoM Position Report according to the state A34 of § 5.4.3.2 of SUBSET 026. The position report contains unknown position (with no train integrity information) in SB mode.

- 7) HL3/HTD Trackside receives the Start of Mission Position Report, the position can't be validated according to the state D33 of § 5.4.3.2 of SUBSET 026 but the HL3/HTD Trackside accepts the train according to the state A23 of § 5.4.3.2 of SUBSET 026. There is no change to VSS states.
- 8) ETCS On-Board deletes the train position information after receiving the train accepted message, according to the state A24 of § 5.4.3.2 of SUBSET 026 .
- 9) Driver enters or (re-) validates the Train Data, including the Train Length (following a safe process or alternatively the Train Length is provided safely by OTI-L).
- 10) ETCS On-board sends the Validated Train Data to the HL3/HTD Trackside, including a position report with no train integrity information and position unknown.
- 11) HL3/HTD Trackside acknowledges having received Validated Train Data. The integrity loss propagation timer is not started because the condition c) of HL3/HTD_0071 is applicable only to trains that have previously a valid train length.
- 12) The HL3/HTD Trackside sends to the train the position report parameters periodic in time and at every LRBG compliant balise group. MA request parameters are sent according to the rules of the specific application.
- 13) The dispatcher may provide an estimated train position to the HL3/HTD Trackside.
- 14) The driver selects "start" and the train sends an MA Request.
- 15) The HL3/HTD Trackside authorises the train for movement in SR with an SR distance and optionally a list of balises that can be passed (based on the estimated train position provided by the dispatcher if applicable) in such a way that allows the train to get a valid position in a safe way. The SR distance may be conditioned to the number of the connected trains that are moving on the line in SR or to the size of the occupied TTDs in the line;
- 16) The train moves in SR.
- 17) The ETCS On-board reads a balise group, gets an unambiguous valid position and reports it to the HL3/HTD Trackside. The train integrity is still not confirmed because of the condition "(the train position was valid and was referred to an LRBG at the time the train was last known to be integer)" in condition [2] of Table 2b of SUBSET 026. It is supposed that the position report triggered by the passage of the LRBG compliant balise group happens before the second confirmation of the train integrity by the OTI-I. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 18) The HL3/HTD Trackside receives the position report. The max safe front end of the train is located in VSS31 but the TTD3 is still free, so there is no update of the status of VSS31 according to the requirement HL3/HTD_0007. The assumed rear end is located in the VSS21, that becomes ambiguous according to the transition #5A. The shadow train timer of TTD2 towards the right is started according to the requirement HL3/HTD_0038.

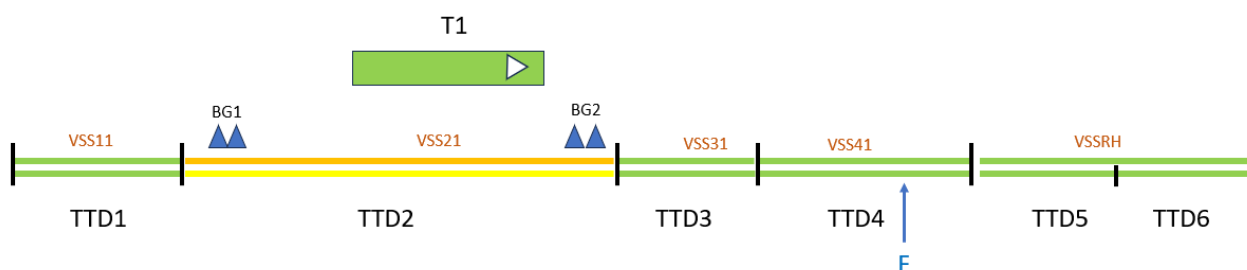


Figure 37 Step 18 Operational Scenario 3

19) The HL3/HTD Trackside sends an MA that covers the whole radio hole (VSSRH), this may contain an OS mode profile according to the specific rules for TAF used in each country. The part of the MA that covers VSS41 and VSSRH has no mode profile. The radio hole timer is assigned to VSSRH according to the requirement HL3/HTD_0041.

Note: It is supposed that the HL3/HTD is able to react to the first position report before the train sets TTD3 to occupied.

20) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I).

21) The train is now complete according to the HL3/HTD trackside. The wait integrity timer is assigned according to the requirement HL3/HTD_0034 and immediately started according to the requirement HL3/HTD_0035. The max safe rear end of the train is in VSS21 and the direction of the train is towards VSS31, so the shadow timer towards VSS31 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

22) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I).

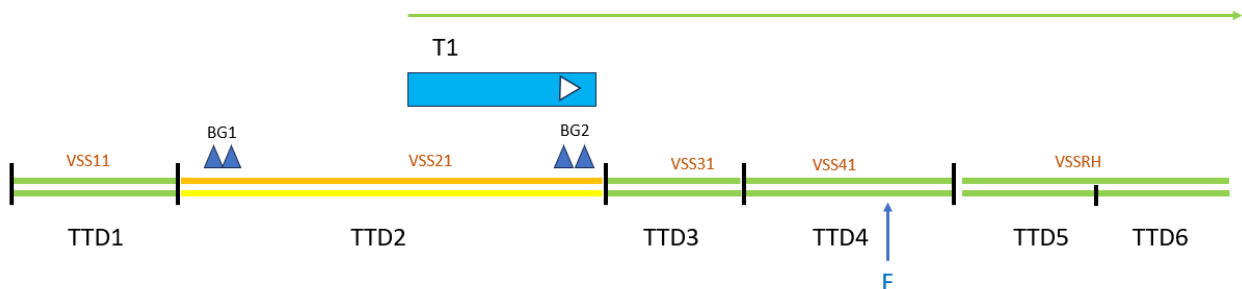


Figure 38 Step 22 Operational Scenario 22

22) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS31.

23) TTD3 becomes occupied. VSS31 becomes ambiguous according to the requirement HL3/HTD_0007 and the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD3 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

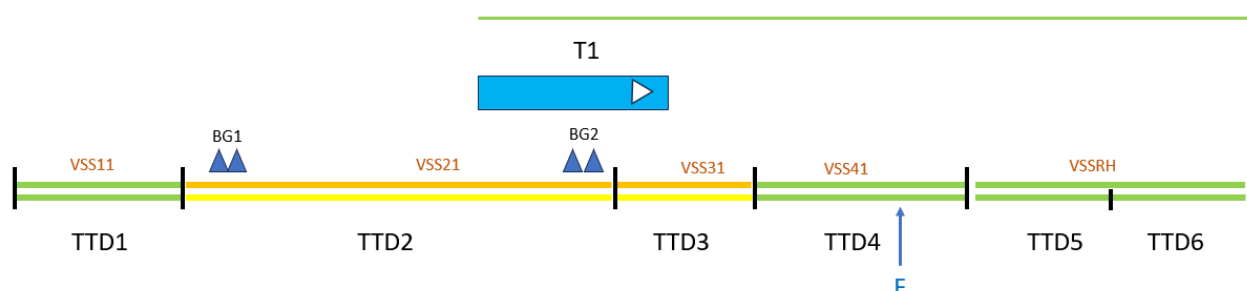


Figure 39 Step 23 Operational Scenario 3

24) TTD4 becomes occupied. VSS41 becomes ambiguous according to the requirement HL3/HTD_0007 and the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD4 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

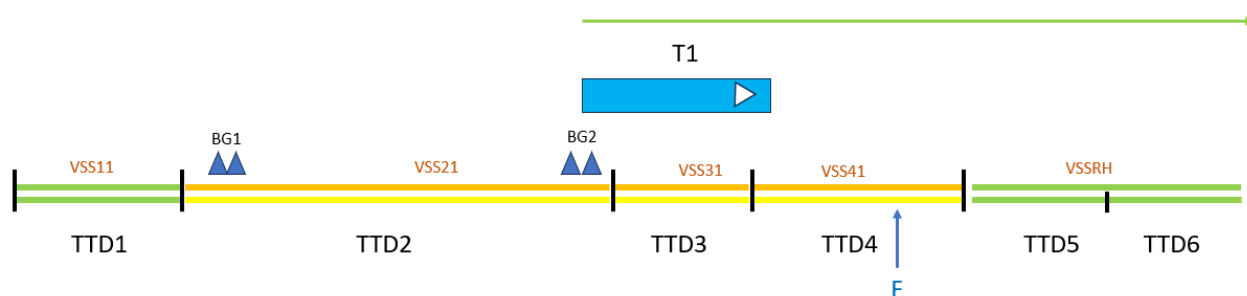


Figure 40 Step 24 Operational Scenario 3

25) When the TTD2 becomes free, VSS21 is set to free (transition #9A for VSS21). VSS31 becomes occupied (transition #11A) because the shadow train timer of train T1 related to TTD2 is not expired when TTD2 becomes free. Once the transition #11A is performed, the shadow train timers related to TTD2 are deleted according to HL3/HTD_0037.

Note: At the moment of this step the shadow train timer of train T1 related to TTD3 is already started, but it is not relevant.

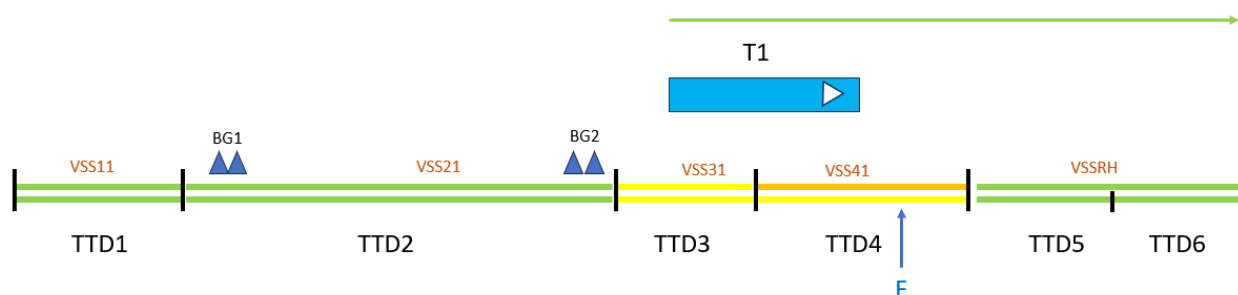


Figure 41 Step 25 Operational Scenario 3

- 25) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end in advance of the radio hole timer start location (F in the picture).
- 26) The HL3/HTD Trackside receives the position report, and the Radio Hole Timer is started according to the requirement HL3/HTD_0042. The Mute timer is stopped according to the requirement HL3/HTD_0033. The Wait Integrity timer is stopped according to the requirement HL3/HTD_0036.
- 27) The ETCS On-board determines its max safe front end inside the engineered radio hole and stops the supervision of the loss of safe radio connection according to the clause 3.12.1.3 of SUBSET 026.

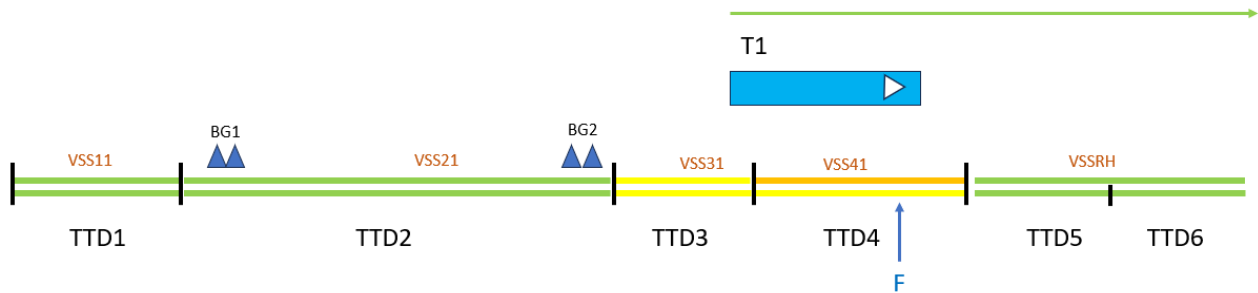


Figure 42 Step 27 Operational Scenario 3

- 28) When the TTD3 becomes free, VSS31 is set to free (transition #6A for VSS31). VSS41 becomes occupied (transition #11A) because the shadow train timer of train T1 related to TTD3 is not expired when TTD3 becomes free. Once the transition #11A is performed, the shadow train timers related to TTD3 are deleted according to HL3/HTD_0037.

Note: At the moment of this step the shadow train timer of train T1 related to TTD4 is already started, but it is not relevant.

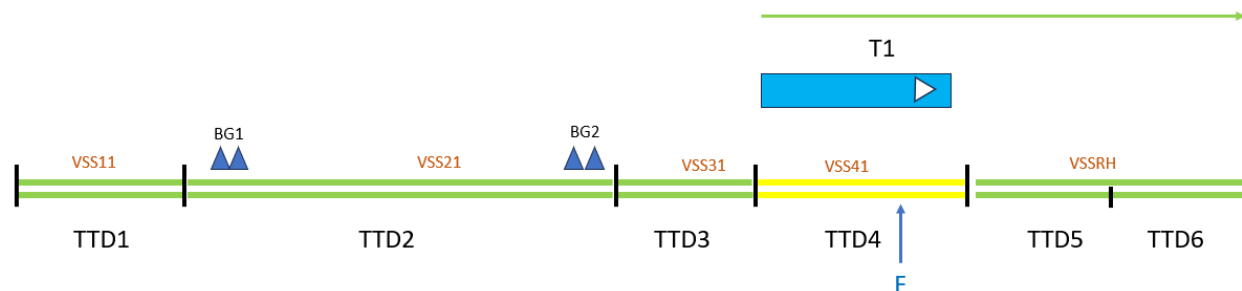


Figure 43 Step 28 Operational Scenario 3

- 29) When the TTD5 becomes occupied, VSSRH is set to occupied (transition #2A for VSSRH), because the train is located in that TTD according to the requirement HL3/HTD_0008.

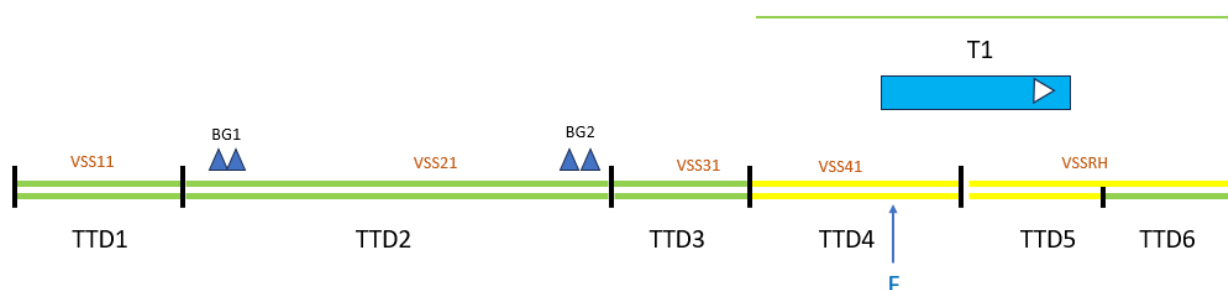


Figure 44 Step 29 Operational Scenario 3

- 30) When the TTD6 becomes occupied, VSSRH is set to occupied (transition #2A for VSSRH), because the train is located in that TTD according to the requirement HL3/HTD_0008.
- 31) When the TTD4 becomes free, VSS41 is set to free according to the transition #6A.

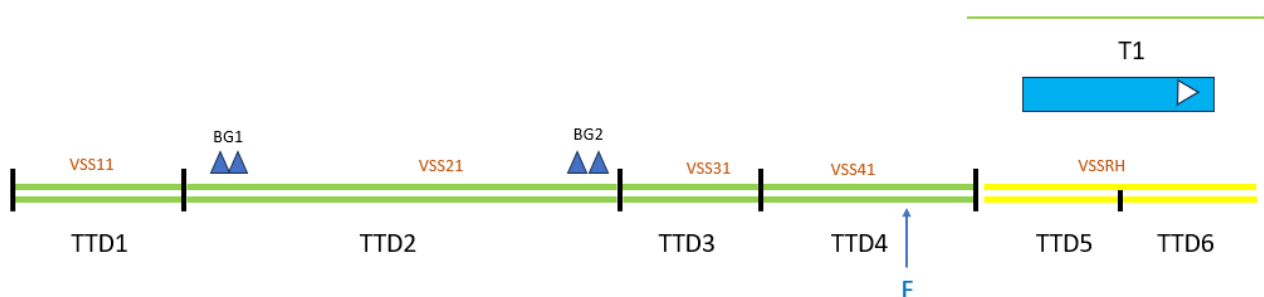


Figure 45 Step 31 Operational Scenario 3

- 32) The scenario continues with steps similar to 29/30/31 until the train approaches the end of the engineered radio hole (see figure below).

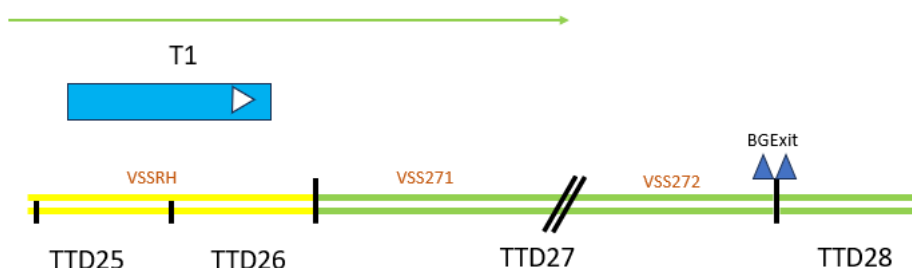


Figure 46 Step 32 Operational Scenario 3

- 33) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end in advance of the engineered radio hole.
- 34) The HL3/HTD Trackside receives the position report, and the Radio Hole Timer is stopped according to the requirement HL3/HTD_0088. The Mute timer is started according to the requirement HL3/HTD_0032. The Wait Integrity timer is started according to the requirement HL3/HTD_0035.
- 35) TTD27 gets occupied. VSS271 becomes occupied according to the transition #6A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD27 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

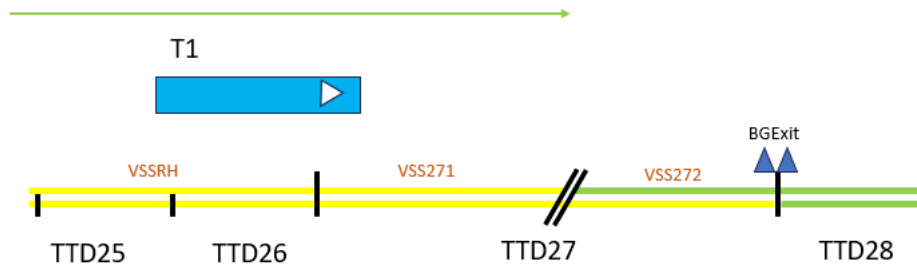


Figure 47 Step 35 Operational Scenario 3

36) The HL3/HTD Trackside sends an updated MA, with a level transition announcement to L1/L0/LNTC that targets a point in advance of the BGExit, in order to compensate the odometric error and to avoid that the transition is made in rear of the exit border.

Note: the information needed for the operation of the train in the L1/L0/LNTC area is not described in the scenario.

37) TTD25 and then TTD26 become free. VSSRH becomes free according to the transition #6B. The MA does not cover anymore the radio hole area and the radio hole timer is no more assigned according to the requirement HL3/HTD_0041.

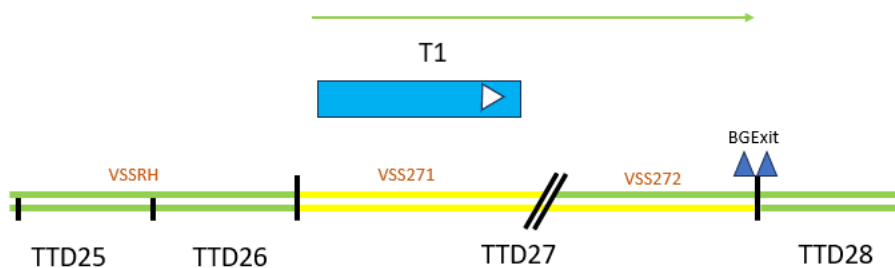


Figure 48 Step 37 Operational Scenario 3

38) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end in VSS272. The max safe rear end of the train is in VSS271 and the direction of the train is towards VSS272, so the shadow timer towards VSS272 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

39) VSS272 becomes occupied according to transition #2A.

40) ETCS On-board receives the telegram of BGExit and performs the level transition.

41) TTD27 becomes free and VSS272 becomes free according to transition #6A.

Note: At this step TTD28 should be already occupied, anyway it is not compulsory that that the HL3/HTD trackside receives this information.

42) When the train has passed the level transition border with its min safe rear end, the ETCS On-board sends a position report to the HL3/HTD Trackside according to the requirements 5.10.3.3.3, 5.10.3.6.2 and

5.10.3.10.3 of SUBSET 026. The shadow train timers related to TTD27 are deleted according to HL3/HTD_0037.

43) The HL3/HTD Trackside orders the train to terminate the communication session.

Note: Different choices can be done according to the requirements 5.10.3.3.4, 5.10.3.6.3 and 5.10.3.10.4 of SUBSET 026.

44) The ETCS On-board terminates the communication session.

45) The train is deemed disconnected by the HL3/HTD trackside and the wait integrity timer is deleted according to the requirement HL3/HTD_0034.

46) The HL3/HTD Trackside deletes the mute timer, the MA and the memorised train location according to its specific rules.

9.4 OPERATIONAL SCENARIO 4: FAILED TRAIN RECOVERY WITH RESCUE LOCOMOTIVE AND JOINING OPERATION

Introduction	This operational scenario shows a situation when there is a train that enters an HL3/HTD line. The train proceeds for a certain number of VSSs, then it is stopped (for example because of a traction problem). The train is unable to proceed and a rescue locomotive is sent to recover the train. The rescue locomotive enters in the line, makes the joining with the train, changes the direction and exits the line.
Assumptions	<ul style="list-style-type: none"> • The HL3/HTD Trackside can trust the information received from the On-board about the train integrity status (Q_INTEGRITY) and the confirmed train length (L_TRAININT).
Preconditions	<ul style="list-style-type: none"> • At the start of the scenario there is no train in the involved part of the track. • The trains don't provide the safe consist length information. • The trackside orders the disconnection of the sleeping engines • TTD2 is large enough to contain the whole train T1, but not the joined trains T1+T2.
Notes	<p>This use case takes origin from the use cases UC_03_01, UC_04_01, UC_04_02, UC_05_01 and UC_13_01 from deliverable D15.1.</p> <p>All the timers, once started, do not expire if not explicitly mentioned.</p> <p>All the MAs are sent together with the needed information, hence applicable mode profile if applicable, linking if applicable, all the applicable profiles.</p>
Legenda	<p>In the figures the following simbology is used:</p> <p>VSSs can be ambiguous (orange colour), free (green colour), occupied (yellow colour) and unknown (red colour)</p> <p>TTD can be free (green colour) or occupied (yellow colour)</p> <p>Disconnected trains are red, connected trains are green, complete trains are blue</p>

1) The train T1 outside the HL3/HTD area receives a telegram from a balise group with a level transition announcement to L2.

2) The train T1 outside the HL3/HTD area receives a telegram from a balise group with an order to connect to the HL3/HTD Trackside.

- 3) ETCS On-board of train T1 opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159) with a position report with no integrity information according the requirement 3.6.5.1.4 h) of SUBSET 026 in mode different from Non Leading, Passive Shunting and Sleeping.
- 4) The mute timer for train T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the requirement HL3/HTD_0089.
- 5) The train T1 sends the Train Data to the HL3/HTD Trackside.
- 6) HL3/HTD Trackside acknowledges having received Validated Train Data. The integrity loss propagation timer is not started because the condition c) of HL3/HTD_0071 is applicable only to trains that have previously a valid train length.
- 7) The HL3/HTD Trackside sends to the train the position report parameters periodic in time and at every LRBG compliant balise group. MA request parameters are sent according to the rules of the specific application. The HL3/HTD Trackside sends an MA that allows the entering in the HL3/HTD line.
- 8) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I).
- 9) The train is now complete according to the HL3/HTD trackside. The wait integrity timer is assigned according to the requirement HL3/HTD_0034 and immediately started according to the requirement HL3/HTD_0035. The max safe rear end of the train is still outside the HL3/HTD area.
- 10) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS11.
- 11) ETCS On-board receives the telegram of BGEntry and performs the level transition.
- 12) TTD1 becomes occupied. VSS11 becomes ambiguous according to the requirement HL3/HTD_0007 and the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD1 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 13) ETCS On-board reports the new level to the HL3/HTD Trackside with the max safe front end inside VSS11.

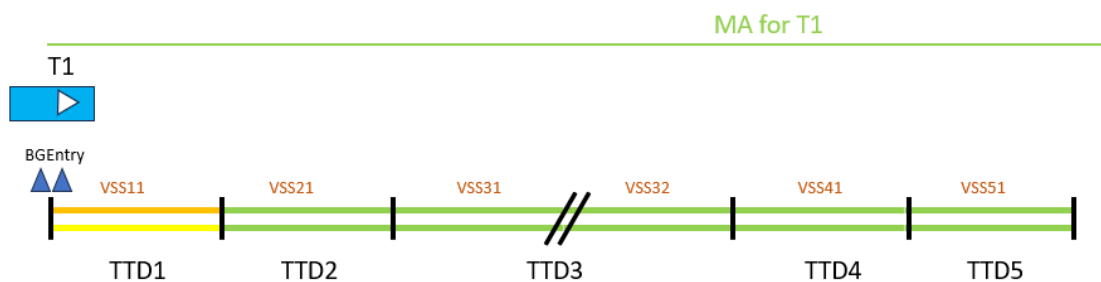


Figure 49 Step 13 Operational Scenario 4

- 14) The train T1 sends a position report with integrity confirmed, with the max safe rear end of the train inside TTD1. The shadow train timer of TTD1 in direction of VSS21 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.
- 15) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS21.
- 16) TTD2 becomes occupied. VSS21 becomes ambiguous according to the requirement HL3/HTD_0007 and the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 17) When the TTD1 becomes free, VSS11 is set to free (transition #9A). VSS21 becomes occupied (transition #11A) because the shadow train timer of train T1 related to TTD1 is not expired when TTD1

becomes free. Once the transition #11A is performed, the shadow train timers related to TTD1 are deleted according to HL3/HTD_0037.

Note: At the moment of this step the shadow train timer of train T1 related to TTD2 is already started, but it is not relevant.

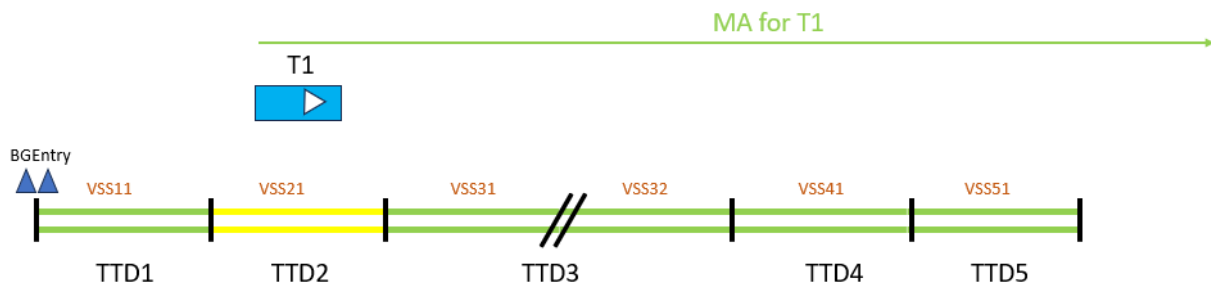


Figure 50 Step 17 Operational Scenario 4

18) TTD3 becomes occupied. No transition is performed, because no train is located on VSS31 according to the requirement HL3/HTD_0005. Also transition #1A is not applicable, because there is an MA on the TTD3.

Note: Taking into account the position report frequency and the odometric error of the trains that are in operation today, it is in general expected that the position report with the max safe front end inside the TTD will normally happen before the TTD occupation. This step is related to a not nominal situation.

19) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS31.

20) According to the requirements HL3/HTD_0005 and HL3/HTD_0007 the train has the front end located inside VSS31 and VSS31 becomes occupied according to the requirement the transition #2A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD3 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

21) When the TTD2 becomes free, VSS21 is set to free (transition #6A). The shadow train timers related to TTD2 are deleted according to HL3/HTD_0037.

Note: The shadow train timer related to TTD3 is already started but it is not relevant for the scenario.

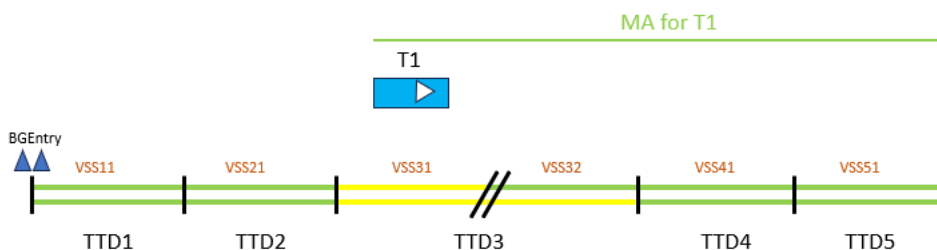


Figure 51 Step 21 Operational Scenario 4

22) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS32.

- 23) According to the requirement HL3/HTD_0005 the train has the front end located inside VSS32 and VSS32 becomes occupied according to the transition #2A.
- 24) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I) with the confirmed rear end inside VSS32.
- 25) VSS31 is set to free (transition #6B).

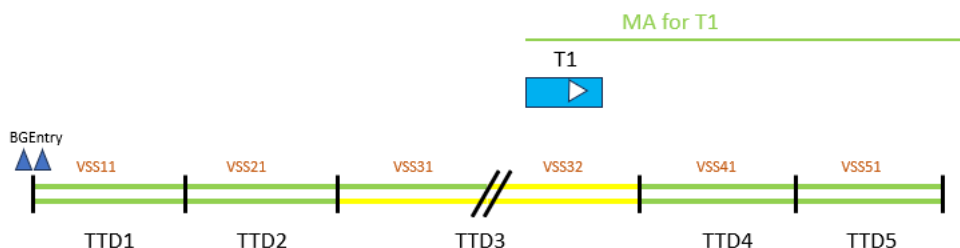


Figure 52 Step 25 Operational Scenario 4

- 26) Train T1 has a problem, it is unable to proceed and it loses the radio connection with the HL3/HTD trackside.
- 27) The wait integrity timer for train T1 expires. There is no update of the state of the VSSs, because condition b) of the requirement HL3/HTD_0071 is not fulfilled.
Note: According to WaitIntegrityTimer – Eng. Rule 1 the wait integrity timer is always shorter than the mute timer.
- 28) The mute timer for train T1 expires. HL3/HTD Trackside deems disconnected the train and stores the memorised train location. VSS32 become unknown (transition #7A). The disconnect propagation timer of VSS32 is started according to the requirement HL3/HTD_0057. The shadow train timers of TTD3 are no more assigned according to the requirement HL3/HTD_0037.
- 29) After some communication between the train driver and the dispatcher according to national procedures, a rescue train is sent by the dispatcher to bring the train T1 outside the HL3/HTD line. This train T2 has 2 ETCS on-boards, the first one (ETCS1_T2) associated to the leading engine and the one on the rear of the consist, that is in Sleeping Mode (ETCS2_T2).
- 30) The disconnect propagation timer of VSS32 expires. VSS31 becomes unknown (transition #1C)
- 31) The HL3/HTD Trackside deletes the mute timer, the MA and the memorised train location for the train T1 according to its specific rules.
- 32) Train T1 makes End of Mission, with the transition to No Power.

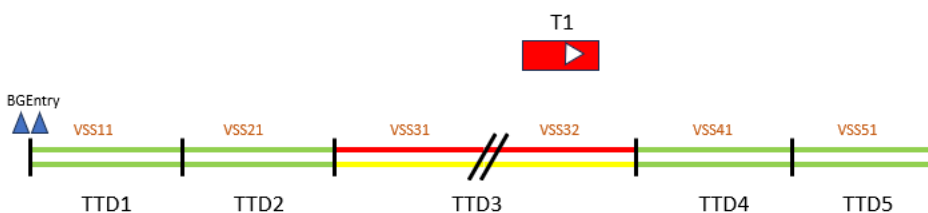


Figure 53 Step 32 Operational Scenario 4

- 33) ETCS1_T2 outside the HL3/HTD area receives a telegram from a balise group with a level transition announcement to L2.

- 34) ETCS2_T2 outside the HL3/HTD area receives a telegram from a balise group with a level transition announcement to L2.
- 35) ETCS1_T2 outside the HL3/HTD area receives a telegram from a balise group with an order to connect to the HL3/HTD Trackside.
- 36) ETCS2_T2 outside the HL3/HTD area receives a telegram from a balise group with an order to connect to the HL3/HTD Trackside. The variable Q_SLEEPSESSION is set to 1.
- Note: This is a choice for simplicity, to try to avoid to manage connected sleeping equipment. Different choices are possible and they will be described in some of the following scenarios.
- 37) ETCS1_T2 opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159) with a position report with no integrity information according the requirement 3.6.5.1.4 h) of SUBSET 026 in mode different from Non Leading, Passive Shunting and Sleeping.
- 38) The mute timer for ETCS1_T2 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the requirement HL3/HTD_0089.
- 39) ETCS1_T2 sends the Train Data to the HL3/HTD Trackside.
- 40) HL3/HTD Trackside acknowledges having received Validated Train Data. The integrity loss propagation timer is not started because the condition c) of HL3/HTD_0071 is applicable only to trains that have previously a valid train length.
- 41) The HL3/HTD Trackside sends to the train the position report parameters periodic in time and at every LRBG compliant balise group. MA request parameters are sent according to the rules of the specific application. The HL3/HTD Trackside sends an MA that allows the entering in the HL3/HTD line and covers with an OS profile the zone where train T1 can be located. The train driver is already instructed to do sweeping by the dispatcher where necessary (this last item depends on the national implementation of sweeping, it may be that some implementations consider sufficient the OS profile).
- 42) ETCS1_T2 sends a position report with train integrity confirmed by external device (OTI-I).
- 43) ETCS1_T2 is now complete according to the HL3/HTD trackside. The wait integrity timer is assigned according to the requirement HL3/HTD_0034 and immediately started according to the requirement HL3/HTD_0035. The max safe rear end of the train is still outside the HL3/HTD area.
- 44) ETCS1_T2 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS11.
- 45) ETCS1_T2 receives the telegram of BGEntry and performs the level transition.
- 46) TTD1 becomes occupied.
- 47) ETCS1_T2 reports the new level to the HL3/HTD Trackside with the max safe front end inside VSS11. VSS11 becomes ambiguous according to the requirement HL3/HTD_0007 and the transition #3A. 2 shadow train timers for train T2 (one for each direction) are assigned to TTD1 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 48) ETCS2_T2 receives the telegram of BGEntry and performs the level transition. It reports its position to the HL3/HTD trackside according to requirement 3.6.5.1.4 j) of SUBSET 026.

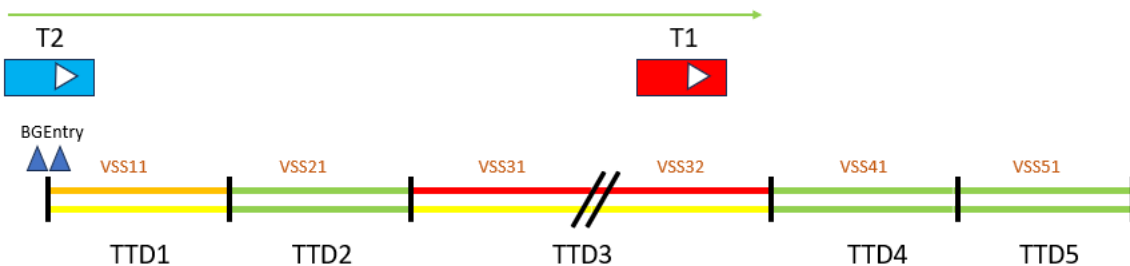


Figure 54 Step 48 Operational Scenario 4

49) ETCS1_T2 sends a position report with integrity confirmed, with the max safe rear end of the train inside TTD1. The shadow train timer of TTD1 in direction of VSS21 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

50) ETCS1_T2 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS21.

51) TTD2 becomes occupied. VSS21 becomes ambiguous according to the requirement HL3/HTD_0007 and the transition #3A. 2 shadow train timers for train T2 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

52) When the TTD1 becomes free, VSS11 is set to free (transition #9A). VSS21 becomes occupied (transition #11A) because the shadow train timer of rescue train T2 related to TTD1 is not expired when TTD1 becomes free. Once the transition #11A is performed, the shadow train timers related to TTD1 are deleted according to HL3/HTD_0037.

Note: At the moment of this step the shadow train timer of train T2 related to TTD2 is already started, but it is not relevant.

53) ETCS1_T2 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS31.

54) VSS31 becomes occupied (transition #12B). 2 shadow train timers for train T2 (one for each direction) are assigned to TTD3 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

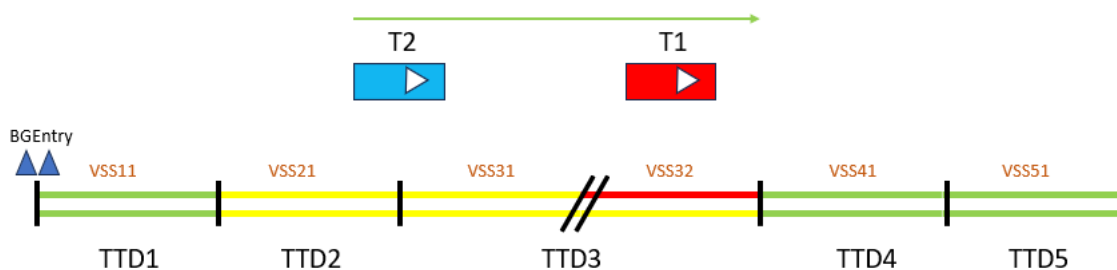


Figure 55 Step 54 Operational Scenario 4

55) TTD2 becomes free. The shadow train timers related to TTD1 are deleted according to HL3/HTD_0037.

- 56) ETCS1_T2 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS32.
- 57) VSS32 becomes occupied (transition #12B).
- 58) Train T2 joins train T1 and performs EoM (transition to No Power). Termination of the communication session is reported.
- 59) The Train T2+T1 changes its orientation.
- 60) HL3/HTD Trackside deems disconnected the train T2 and stores the memorised train location. VSS31 and VSS32 become unknown (transition #7A). The disconnect propagation timers of VSS31 and VSS32 are started according to the requirement HL3/HTD_0057. The shadow train timers of TTD3 are no more assigned according to the requirement HL3/HTD_0037.
- 61) The disconnect propagation timers of VSS31 and VSS32 expire. This has no consequences because TTD2 and TTD4 are free. Once expired the timers are stopped according to the condition c) of the requirement HL3/HTD_0058.
- 61) The HL3/HTD Trackside deletes the mute timer, the MA and the memorised train location according to its specific rules.
- 62) The Train T2+T1 performs Cab Activation (OTI-I/L reset) and the desk is opened in direction towards VSS11. The Train Integrity and Train Length information are provided to the EVC. ETCS_T2 goes in Standby Mode. The stored position and level are still valid.
- 63) ETCS2_T2 establishes a communication session according to the requirement 3.5.3.4 c) of SUBSET 026. Mode Standby is reported to the ETCS trackside.
- 64) ETCS1_T2 establishes a communication session according to the requirement 3.5.3.4 c) of SUBSET 026. Mode Sleeping is reported to the ETCS trackside.
- 65) The mute timers are assigned to ETCS1_T2 and ETCS2_T2 according to HL3/HTD_0031 and the mute timer of ETCS2_T2 is started according to HL3/HTD_0032. The Train T2+T1 is deemed connected according to the requirement HL3/HTD_0089. The HL3/HTD trackside orders the termination of the communication session to ETCS1_T2 and ETCS2_T2.
Note: This is done because the HL3/HTD trackside does not manage the connection of sleeping units in this scenario and the association to the leading engine and the state S0 of the requirement 5.4.3.2 of SUBSET 026 requires the absence of established communication session.
- 66) ETCS1_T2 and ETCS2_T2 performs the steps to terminate the communication session.
- 67) The mute timer for ETCS2_T2 is stopped according to HL3/HTD_0033. The Train T2+T1 is deemed disconnected according to HL3/HTD_0090. The disconnect propagation timer is started for ETCS2_T2 according to HL3/HTD_0057.
- 68) ETCS2_T2 initiates the Start of Mission procedure. The Driver is requested to revalidate or change the Driver ID and is offered to revalidate or change Train Running Number.
- 69) ETCS2_T2 opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159).
- 70) The disconnect propagation timer for ETCS2_T2 is stopped according to HL3/HTD_0058.
- 71) After the successful establishment of the communication, the train sends the SoM Position Report according to the state A33 of § 5.4.3.2 of SUBSET 026 .
- 72) The mute timer for ETCS2_T2 is started according to requirement HL3/HTD_0032. The train T2+T1 is now connected according to the requirement HL3/HTD_0089. The front end of Train T2+T1 is now located in VSS31 that becomes ambiguous (transition #5A). 2 shadow train timers for train T2+T1 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 73) Driver enters or (re-) validates the Train Data. The Train Length may be provided by OTI-L or by the driver. This value shall be able anyway to fulfil the safety requirements, otherwise the ETCS On-Board will never confirm its integrity.
- 74) ETCS2_T2 sends the Validated Train Data to the HL3/HTD Trackside.

75) HL3/HTD Trackside acknowledges having received Validated Train Data. HL3/HTD Trackside uses received Train Length info to locate the assumed rear end. VSS32 becomes ambiguous (transition #5A). The integrity loss propagation timer is not started because the condition c) of HL3/HTD_0071 is applicable only to trains that have previously a valid train length.

The HL3/HTD Trackside sends to the train the position report parameters periodic in time and at every LRBG compliant balise group. MA request parameters are sent according to the rules of the specific application.

76) ETCS2_T2 sends a position report with train integrity confirmed by external device (OTI-I).

77) No update of the state of the VSSs is made by the HL3/HTD trackside, because there are not the conditions identified in other requirements to set the VSS to occupied (for example there is no assigned train length). The train is now complete according to the HL3/HTD trackside. The wait integrity timer is assigned according to the requirement HL3/HTD_0034 and immediately started according to the requirement HL3/HTD_0035.

The max safe rear end of the train is in VSS32 and the direction of the train is towards VSS11, so the shadow train timer towards VSS11 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

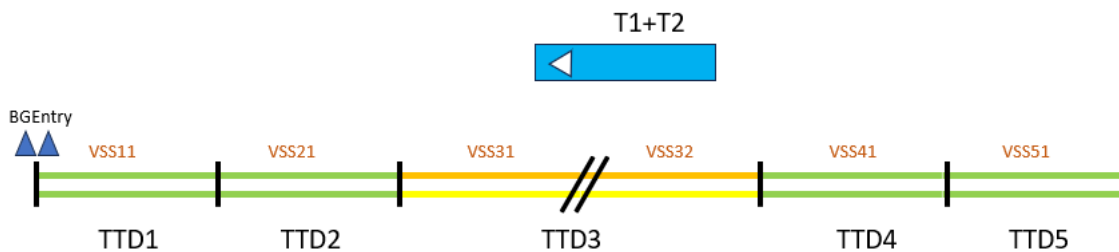


Figure 56 Step 77 Operational Scenario 4

78) The HL3/HTD Trackside sends a MA, with a level transition announcement to L1/L0/LNTC that targets a point in advance of the BGEntry, in order to compensate the odometric error and to avoid that the transition is made in rear of the exit border.

Note: the information needed for the operation of the train in the L1/L0/LNTC area is not described in the scenario.

79) ETCS2_T2 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end in VSS21.

80) TTD2 becomes occupied. VSS21 becomes ambiguous according to the requirement HL3/HTD_0007 and the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

81) ETCS2_T2 sends a position report with train integrity confirmed by external device (OTI-I) with the min safe front end in VSS31. VSS32 becomes unknown (transition #10A).

82) ETCS2_T2 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end in VSS11 and the max safe rear end is in VSS21.

83) The shadow train timer of TTD2 towards VSS11 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

84) TTD1 becomes occupied. VSS11 becomes ambiguous according to the requirement HL3/HTD_0007 and the transition #3A. 1 shadow train timer for train T1 is assigned to TTD1 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

Note: The shadow train timer towards the exit of the line is not assigned, because it is anyway not used.

85) When the TTD3 becomes free, all the VSSs in the TTD3 are set to free (transition #9A for VSS31, transition #4A for VSS32). VSS21 becomes occupied (transition #11A) because the shadow train timer of

train T1 related to TTD3 is not expired when TTD3 becomes free. Once the transition #11A is performed, the shadow train timers related to TTD3 are deleted according to HL3/HTD_0037.

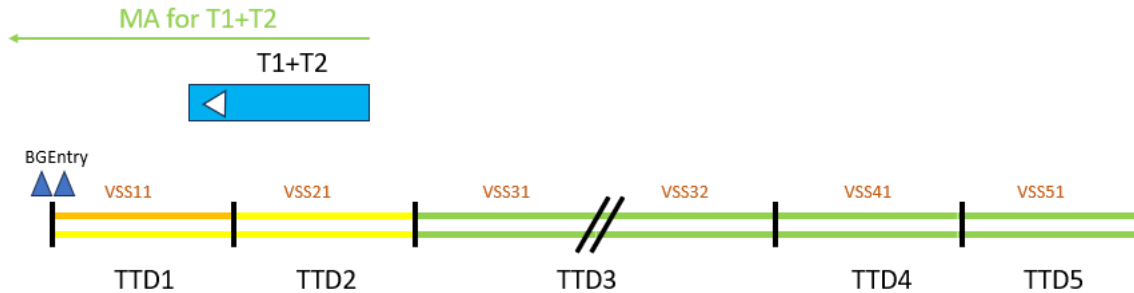


Figure 57 Step 85 Operational Scenario 4

- 86) ETCS2_T2 receives the telegram of BGEEntry and performs the level transition.
 - 87) ETCS1_T2 receives the telegram of BGEEntry and performs the level transition.
 - 88) ETCS2_T2 sends a position report with the new level to the HL3/HTD trackside, according to the requirement 3.6.5.1.4 g) of SUBSET 026.
 - 89) TTD2 becomes free and VSS21 becomes free according to transition #6A. VSS11 becomes occupied (transition #11A) because the shadow train timer of train T1 related to TTD2 is not expired when TTD2 becomes free. Once the transition #11A is performed, the shadow train timers related to TTD2 are deleted according to HL3/HTD_0037.
 - 90) TTD1 becomes free and VSS11 becomes free according to transition #6A.
 - 91) When the train has passed the level transition border with its min safe rear end, ETCS2_T2 sends a position report to the HL3/HTD Trackside according to the requirements 5.10.3.3.3, 5.10.3.6.2 and 5.10.3.10.3 of SUBSET 026. The shadow train timer related to TTD1 is deleted according to HL3/HTD_0037.
 - 92) The HL3/HTD Trackside orders the train to terminate the communication session.
- Note: Different choices can be done by according to the requirements 5.10.3.3.4, 5.10.3.6.3 and 5.10.3.10.4 of SUBSET 026.
- 93) ETCS2_T2 terminates the communication session.
 - 94) The train T1+T2 is deemed disconnected by the HL3/HTD trackside and the wait integrity timer is deleted according to the requirement HL3/HTD_0034.
 - 95) The HL3/HTD Trackside deletes the mute timer, the MA and the memorised train location according to its specific rules.

9.5 OPERATIONAL SCENARIO 5: DIRECTION CHANGE USING A DEDICATED SIDING WITH NON-LEADING EQUIPMENT

Introduction	This operational scenario shows a situation when there is a train that enters an HL3/HTD line. This train has 2 ETCS On-Boards, 1 is in mode Non Leading. The train enters in the line, changes the direction in a dedicated siding (to allow a fast change of direction) and exits the line.
--------------	---

Assumptions	<ul style="list-style-type: none"> • The HL3/HTD Trackside can trust the information received from the On-board about the train integrity status (Q_INTEGRITY) and the confirmed train length (L_TRAININT).
Preconditions	<ul style="list-style-type: none"> • At the start of the scenario there is no train in the involved part of the track. • The trains don't provide the safe consist length information. • The trackside doesn't order the disconnection of the slave engines • Conditions described in requirement HL3/HTD_0075 are satisfied • The train T2 has 2 ETCS on-boards, the first one (ETCS1_T1) associated to the leading engine at the start of the scenario and the one on the rear of the consist, that is in Non Leading Mode (ETCS2_T1) and it is associated to the slave engine at the start of the scenario. • The HL3/HTD trackside has its own rules to associate the leading engine and the slave engine at the other extremity of the train . The detailed behaviour is left to the specific application. • TTD2 is large enough to contain the whole train T1. • The initial layout of the track is illustrated in the Figure 58.
Notes	<p>This use case takes origin from the use cases UC_01_06, UC_04_01 and UC_04_02 from deliverable D15.1.</p> <p>All the timers, once started, do not expire if not explicitly mentioned.</p> <p>All the MAs are sent together with the needed information, hence applicable mode profile if applicable, linking if applicable, all the applicable profiles.</p>
Legenda	<p>In the figures the following symbology is used:</p> <p>VSSs can be ambiguous (orange colour), free (green colour), occupied (yellow colour) and unknown (red colour)</p> <p>TTD can be free (green colour) or occupied (yellow colour)</p> <p>Disconnected trains are red, connected trains are green, complete trains are blue</p>

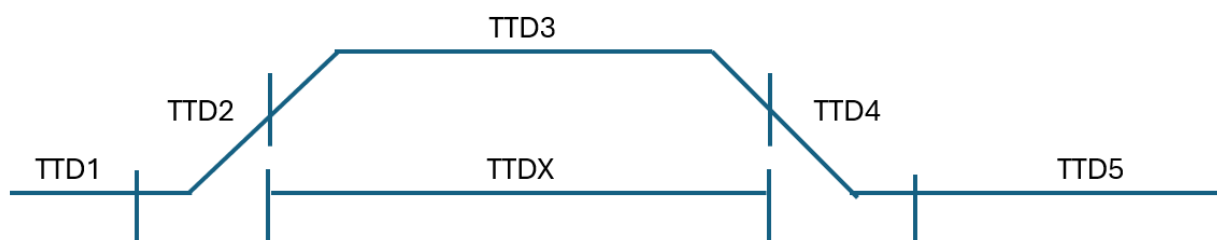


Figure 58 Initial layout Operational Scenario 5

- 1) ETCS1_T1 outside the HL3/HTD area receives a telegram from a balise group with a level transition announcement to L2.
- 2) ETCS2_T2 outside the HL3/HTD area receives a telegram from a balise group with a level transition announcement to L2.

- 3) ETCS1_T1 outside the HL3/HTD area receives a telegram from a balise group with an order to connect to the HL3/HTD Trackside.
- 4) ETCS2_T1 outside the HL3/HTD area receives a telegram from a balise group with an order to connect to the HL3/HTD Trackside.
- 5) ETCS1_T1 opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159) with a position report with no integrity information according the requirement 3.6.5.1.4 h) of SUBSET 026.
- 6) ETCS2_T1 opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159) with a position report with no integrity information according the requirement 3.6.5.1.4 h) of SUBSET 026.
- 7) The mute timer for ETCS1_T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the requirement HL3/HTD_0089.
- 8) The mute timer for ETCS2_T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032.
- 8) ETCS1_T1 sends the Train Data to the HL3/HTD Trackside.
Note: ETCS2_T1 will not send the Train Data according to the requirements 5.10.3.1.3, 5.10.3.2.2 and 5.10.3.7.2 of SUBSET 026.
- 9) HL3/HTD Trackside acknowledges having received Validated Train Data. The integrity loss propagation timer is not started because the condition c) of HL3/HTD_0071 is applicable only to trains that have previously a valid train length.
- 10) The HL3/HTD Trackside sends to ETCS1_T1 and ETCS2_T1 the position report parameters periodic in time and at every LRBG compliant balise group. MA request parameters are sent according to the rules of the specific application. The HL3/HTD Trackside sends an MA that allows the entering in the HL3/HTD line and it is extended until the end of TTD3.
Note: For the sake of simplicity MA request parameters are sent also to the ETCS On-Board in Non Leading, it will use them after the change of direction.
- 11) ETCS1_T1 sends a position report with train integrity confirmed by external device (OTI-I).
- 12) ETCS1_T1 is now complete according to the HL3/HTD trackside. The wait integrity timer is assigned according to the requirement HL3/HTD_0034 and immediately started according to the requirement HL3/HTD_0035. The max safe rear end of the train is still outside the HL3/HTD area.
- 13) ETCS1_T1 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS11.
- 14) ETCS1_T1 receives the telegram of BGEntry and performs the level transition.
- 15) TTD1 becomes occupied.
- 16) ETCS1_T1 reports the new level to the HL3/HTD Trackside with the max safe front end inside VSS11. VSS11 becomes ambiguous according to the requirement HL3/HTD_0007 and the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD1 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

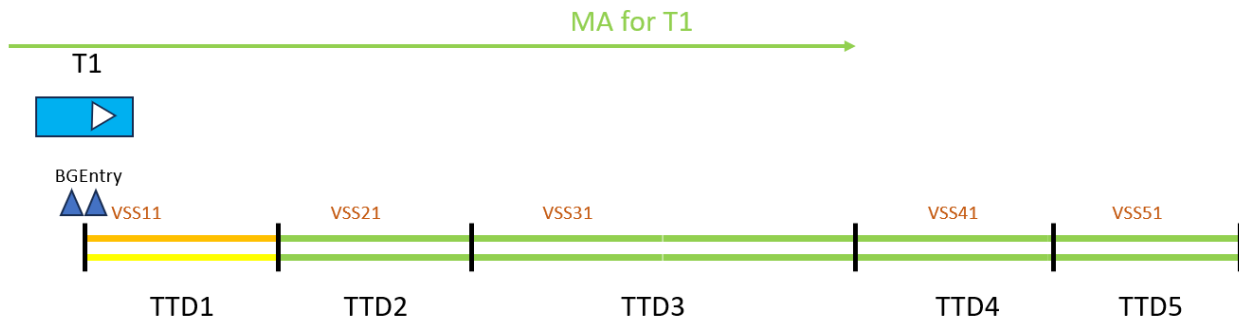


Figure 59 Step 16 Operational Scenario 5

- 17) ETCS2_T1 receives the telegram of BGEntry and performs the level transition. A position report may be sent to the HL3/HTD trackside according to the position report parameters received at step 10.
- 18) ETCS1_T1 sends a position report with integrity confirmed, with the max safe rear end of the train inside TTD1. The shadow train timer of TTD1 in direction of VSS21 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.
- 19) ETCS1_T1 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS21.
- 20) TTD2 becomes occupied. VSS21 becomes ambiguous according to the requirement HL3/HTD_0007 and the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 21) When the TTD1 becomes free, VSS11 is set to free (transition #9A). VSS21 becomes occupied (transition #11A) because the shadow train timer of train T1 related to TTD1 is not expired when TTD1 becomes free. Once the transition #11A is performed, the shadow train timers related to TTD1 are deleted according to HL3/HTD_0037.
Note: At the moment of this step the shadow train timer of train T1 related to TTD2 is already started, but it is not relevant.
- 22) ETCS1_T1 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS31.
- 23) VSS31 becomes occupied (transition #2A). 2 shadow train timers for train T1 (one for each direction) are assigned to TTD3 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037. The conditions foreseen by the requirement HL3/HTD_0075 are available.
- 24) TTD2 becomes free. The shadow train timers related to TTD1 are deleted according to HL3/HTD_0037.
- 25) ETCS1_T1 sends a position report with train integrity confirmed by external device (OTI-I) according to the requirement 3.6.5.1.4 a) of SUBSET 026, because the train T1 has reached standstill.

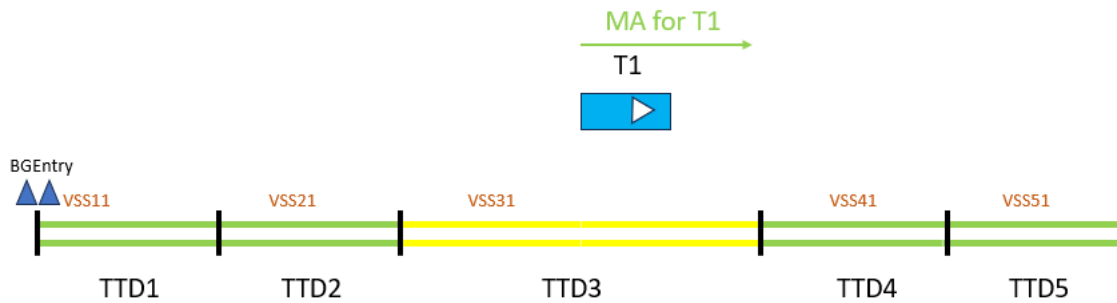


Figure 60 Step 25 Operational Scenario 5

26) The MA may be revoked according to the specific application rules. The switches adjacent to TTD3 are moved to achieve physical independence according to the requirement HL3/HTD_0047 .

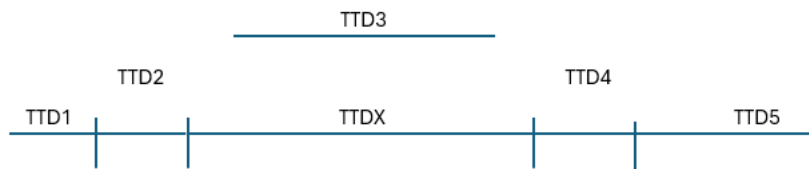


Figure 61 Layout after step 26 Operational Scenario 5

27) The Driver of ETCS1_T1 selects “Non Leading”.

Note: Some coordination is expected in this scenario, to avoid that the driver selects this before the movement of the switches.

28) ETCS1_T1 reports mode Non Leading to HL3/HTD Trackside.

29) Once the non leading input signal is not received any more, ETCS2_T1 switches to Stand-By mode.

30) ETCS2_T1 reports the end of mission to the HL3/HTD trackside via the message “End of Mission” according to the requirement 5.5.3.1.3 of SUBSET 026.

31) HL3/HTD requests to ETCS2_T1 to terminate the communication session according to the requirement 5.5.3.1.4 of SUBSET 026.

32) ETCS2_T1 terminates the communication session.

33) Train T1 is deemed disconnected according to the requirement HL3/HTD_0090. VSS31 becomes unknown according to transition #7A and the disconnect propagation timer related to VSS31 is started (Even if the expiration of this timer has no practical effect, because there is physical independence). Trackside stores train related information like train location, integrity status and train length according to HL3/HTD_0076 and starts the train length monitoring timer of TTD3.

34) The person that was previously in the cab of ETCS2_T1 becomes the driver of the train.

35) ETCS2_T1 initiates the Start of Mission procedure; the stored position and level are still valid. The Driver is requested to revalidate or change the Driver ID and is offered to revalidate or change Train Running Number.

36) ETCS2_T1 opens a communication session with the HL3/HTD Trackside.

After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159).

- 37) The mute timer for train T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the HL3/HTD Trackside because of the requirement HL3/HTD_0089.
- 38) ETCS2_T1 sends the Start of Mission Position Report without Validated Train Data, with valid position (with no train integrity information) in SB mode.
- 39) HL3/HTD Trackside receives the Start of Mission Position Report without Validated Train Data, evaluates the reported position and the NID_ENGINE in the Start of Mission Position Report. The check of the NID_ENGINE according to the requirement HL3/HTD_0048 is positive, so the trackside maintains the storage of the data according to the requirements HL3/HTD_0076 and HL3/HTD_0047.
- 40) VSS31 becomes ambiguous (Transition #5A).
- 41) Driver validates the Train Data.
- 42) ETCS2_T1 sends Validated Train Data.
- 43) Trackside uses the reported train length to compute Assumed Rear End of the train. HL3/HTD Trackside checks the Validated Train Data according to the requirement HL3/HTD_0049. The check is positive. HL3/HTD Trackside acknowledges having received Validated Train Data. The wait first integrity confirmation timer is started. The integrity loss propagation timer is not started because the condition c) of HL3/HTD_0071 is applicable only to trains that have previously a valid train length.
- 44) ETCS2_T1 sends a position report with train integrity confirmed by external device (OTI-I).
- 45) Trackside receives a position report with integrity confirmed, determines the Confirmed Rear End and changes VSS31 from Ambiguous to Occupied (transition #11B). The train length monitoring timer and the wait first integrity confirmation timer are stopped according to the requirement HL3/HTD_0053. The train is now complete according to the HL3/HTD trackside. The wait integrity timer is assigned according to the requirement HL3/HTD_0034 and immediately started according to the requirement HL3/HTD_0035. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD3 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037. The shadow train timer of TTD3 towards VSS21 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.
- 46) The switches are moved in order to return to the situation described by the Figure 58.
- 47) The HL3/HTD Trackside sends to ETCS2_T1 the position report parameters periodic in time and at every LRBG compliant balise group. MA request parameters are sent according to the rules of the specific application. The HL3/HTD Trackside sends an MA that allows the entering in the HL3/HTD line and it is extended until the end of TTD3. The HL3/HTD Trackside sends to ETCS2_T1 the position report parameters according to the rules of the specific application.
- 47) ETCS2_T1 sends a MA Request.
- 48) Trackside provides an FS MA to the train as there are some free VSSs in front of the train location and there is assurance that no other vehicle has entered in the TTD3. With the MA there is a level transition announcement to L1/L0/LNTC that targets a point in advance of the BGEntry, in order to compensate the odometric error and to avoid that the transition is made in rear of the exit border.
- Note: the information needed for the operation of the train in the L1/L0/LNTC area is not described in the scenario. The position report parameters and the MA request parameters are maintained unchanged.
- 49) ETCS2_T1 receives FS MA, starts moving and regularly reports its new position with integrity confirmed.
- 50) ETCS2_T1 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end in VSS21.
- 51) TTD2 becomes occupied. VSS21 becomes occupied according to the requirement HL3/HTD_0007 and the transition #2A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 52) ETCS2_T1 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe rear end in VSS21.
- 53) The shadow train timer of TTD2 towards VSS11 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

54) ETCS2_T1 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end in VSS11.

55) TTD1 becomes occupied. VSS11 becomes occupied according to the requirement HL3/HTD_0007 and the transition #2A. 1 shadow train timer for train T1 is assigned to TTD1 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

Note: The shadow train timer towards the exit of the line is not assigned, because it is anyway not used.

56) ETCS2_T1 receives the telegram of BGEntry and performs the level transition.

57) ETCS1_T1 receives the telegram of BGEntry and performs the level transition.

58) ETCS2_T1 sends a position report with the new level to the HL3/HTD trackside, according to the requirement 3.6.5.1.4 g) of SUBSET 026.

59) ETCS1_T1 sends a position report with the new level to the HL3/HTD trackside, according to the requirement 3.6.5.1.4 g) of SUBSET 026.

60) TTD1 becomes free and VSS11 becomes free according to transition #6A. The shadow train timer related to TTD1 is deleted according to HL3/HTD_0037.

61) When the train has passed the level transition border with its min safe rear end, ETCS2_T1 sends a position report to the HL3/HTD Trackside according to the requirements 5.10.3.3.3, 5.10.3.6.2 and 5.10.3.10.3 of SUBSET 026.

62) HL3/HTD Trackside orders to ETCS2_T1 and ETCS1_T1 to terminate the communication session.

Note: Different choices can be done by according to the requirements 5.10.3.3.4, 5.10.3.6.3 and 5.10.3.10.4 of SUBSET 026.

63) ETCS2_T1 and ETCS1_T1 terminate the communication session.

64) The train T1 is deemed disconnected by the HL3/HTD trackside and the wait integrity timer is deleted according to the requirement HL3/HTD_0034.

65) The HL3/HTD Trackside deletes the mute timer, the MA and the memorised train location according to its specific rules.

9.6 OPERATIONAL SCENARIO 6: EXIT FROM SHUNTING AREA, ODOMETRY FAILURE AND RBC HANDOVER

Introduction	This operational scenario shows a situation when there is a train that exits from a permanent shunting area, has a sudden malfunctioning of the odometry, performs RBC Handover, and then enters in another shunting area.
Assumptions	<ul style="list-style-type: none"> •The HL3/HTD Trackside can trust the information received from the On-board about the train integrity status (Q_INTEGRITY) and the confirmed train length (L_TRAININT). •The Accepting and Handing Over RBC are managed by the same Dispatcher •Regarding balise engineering the Handing Over should have knowledge of balises in the Accepting RBC area to evaluate position reports to update the CRE of a train •Train T1 is able to handle two communication sessions.

Preconditions	<ul style="list-style-type: none"> When approaching the boundary of the permanent shunting area in Shunting Mode the train has passed over balises while shunting, enabling it to provide a position which is unambiguous to the HL3/HTD Trackside; The permanent shunting areas are protected: possible means of preventing trains operating in SH mode from leaving a designated Shunting Area include derailling points, balises with "Danger for Shunting information" and a list of balise group(s) the train can pass over in SH mode; The borders of the permanent shunting areas coincide with TTD boundaries; The trains don't provide the safe consist length information.
Notes	<p>This use case takes origin from the use cases UC_02_01, UC_11_01 and UC_11_03 from deliverable D15.1.</p> <p>All the timers, once started, do not expire if not explicitly mentioned.</p> <p>All the MAs are sent together with the needed information, hence applicable mode profile if applicable, linking if applicable, all the applicable profiles.</p>
Legenda	<p>In the figures the following symbology is used:</p> <p>VSSs can be ambiguous (orange colour), free (green colour), occupied (yellow colour) and unknown (red colour)</p> <p>TTD can be free (green colour) or occupied (yellow colour)</p> <p>Disconnected trains are red, connected trains are green, complete trains are blue</p>

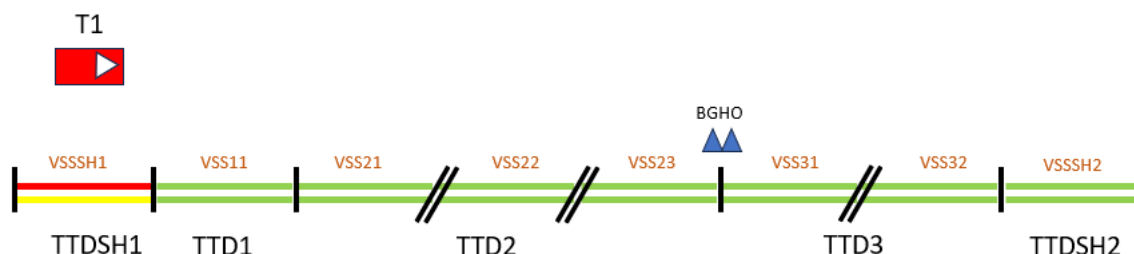


Figure 62 Initial situation Operational Scenario 6

- 1) Driver of train T1 selects "exit Shunting"
- 2) ETCS On-Board performs the transition from Shunting to Standby, establishes the communication session with the trackside according to the requirement 3.5.3.4 c) of SUBSET 026. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159).
- 3) The mute timer for train T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the requirement HL3/HTD_0089.
- 4) The session is established. After the successful establishment of the communication, the train sends the Position Report to report the new mode according to the requirement 3.6.5.1.4 b) of SUBSET 026.
- 5) The front end of train T1 is now located in VSSSH1 that becomes ambiguous (transition #5A). 2 shadow train timers for train T1 (one for each direction) are assigned to TTDSH1 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

6) HL3/HTD Trackside orders the disconnection of the train.

Note: this is done in order because the state S0 of the requirement 5.4.3.2 of SUBSET 026 requires the absence of established communication session.

7) ETCS On-Board sens the Message 156: Termination of a communication session to the HL3/HTD trackside.

8) The mute timer for train T1 is stopped according to HL3/HTD_0033. The Train T1 is deemed disconnected according to HL3/HTD_0090. VSSSH1 becomes unknown (transition #10B) The disconnect propagation timer is started for Train T1 according to HL3/HTD_0057. The shadow train timers related to TTDSH1 are deleted according to HL3/HTD_0037.

9) ETCS On-board initiates the Start of Mission procedure; the stored position and level are still valid. The Driver is requested to revalidate or change the Driver ID and is offered to revalidate or change Train Running Number.

10) ETCS On-board opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159)

11) The mute timer for train T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the requirement HL3/HTD_0089.

12) The session is established. After the successful establishment of the communication, the ETCS On-board sends the SoM Position Report according to the state A33 of § 5.4.3.2 of SUBSET 026.

13) The front end of train T1 is now located in VSSSH1 that becomes ambiguous (transition #5A). 2 shadow train timers for train T1 (one for each direction) are assigned to TTDSH1 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

14) Driver enters the Train Data. The Train Length may be provided by OTI-L, by the driver or it can be a fixed pre-configured value. This value shall be able anyway to fulfil the safety requirements, otherwise the ETCS On-Board will never confirm its integrity.

15) ETCS On-board sends the Validated Train Data to the HL3/HTD Trackside, including a position report with no train integrity information.

16) HL3/HTD Trackside acknowledges having received Validated Train Data. HL3/HTD Trackside uses received Train Length info to locate the assumed rear end . The integrity loss propagation timer is not started because the condition c) of HL3/HTD_0071 is applicable only to trains that have previously a valid train length.

The trackside sends to the train the position report parameters periodic in time in order to allow the sending of the first position report with integrity confirmed in the following step. MA request parameters are sent according to the rules of the specific application.

17) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I).

18) No update of the state of the VSSs is made by the HL3/HTD trackside, because there are not the conditions identified in other requirements to set the VSS to occupied. The train is now complete according to the HL3/HTD trackside. The wait integrity timer is assigned according to the requirement HL3/HTD_0034 and immediately started according to the requirement HL3/HTD_0035.

The max safe rear end of the train is in VSSSH1 and the direction of the train is towards VSS11, so the shadow timer towards VSS11 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

(Note: It is in principle possible that the max safe rear end is already in TTD1. In that case the shadow train timers of TTD2 will be not started, to try to avoid this behaviour engineering rule ShadowTrainTimer – Eng. Rule 2 has been established).

19) The driver selects “Start” and the Train sends a MA Request according to the requirement 3.8.2.1.1 b) of SUBSET 026.

20) HL3/HTD Trackside checks the condition to assign an MA and sends a MA with an OS mode profile to exit the shunting area. The OS profile covers the whole VSSSH1. The EoA of the MA is between VSS21 and VSS22. There is a release speed fixed by the trackside (This is relevant for the following events).

- 21) ETCS On-board receives the MA and requests the OS acknowledgement to the driver according to requirement 5.9.5.1 of SUBSET 026.
- 22) The driver acknowledges the OS mode.
- 23) ETCS On-board makes the transition to OS mode according to requirement 5.9.5.2 of SUBSET 026.

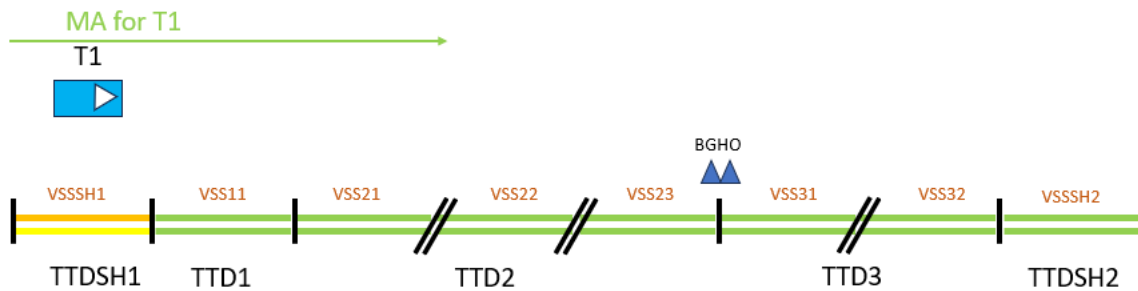


Figure 63 Step 23 Operational Scenario 6

- 24) The train T1 starts moving. When its min safe front end is outside the mode profile OS, it makes the transition to FS mode according to transition [75] of § 4.6.3 of SUBSET 026, and it sends a position report with the max safe front end inside VSS11.
- 25) According to the requirement HL3/HTD_0006 there is no update of the state of the VSS when the trackside receives the position report. When TTD1 gets occupied, the train location is updated by the HL3/HTD trackside according to the requirement HL3/HTD_0005 and VSS11 becomes ambiguous according to the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD1, according to the requirement HL3/HTD_0037.
- 26) When the TTDSH1 becomes free, VSSSH1 is set to free (transition #9A for VSS2SH1). VSS11 becomes occupied (transition #11A) because the shadow train timer of train T1 related to TTDSH1 is not expired when TTDSH1 becomes free. Once the transition #11A is performed, the shadow train timers related to TTD2 are deleted according to HL3/HTD_0037. If the HL3/HTD trackside has a specific implementation to record train lengths present in shunting area, the length of train T1 can be subtracted from the total of the lengths present in the shunting area.

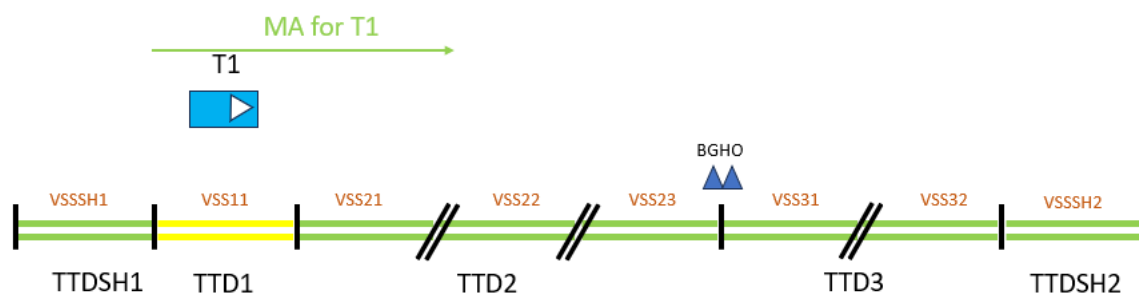


Figure 64 Step 26 Operational Scenario 6

27) ETCS On-board sends a position report with the max safe front end inside VSS23 (for example because of a sudden malfunctioning of the odometry). In this specific case there is no reaction, because there are no opposing movements according to the requirement HL3/HTD_0028 and according to the requirement HL3/HTD_0027 the trackside has established that the situation is not dangerous. There is no update of the state of the VSSs, according to the requirements HL3/HTD_0006 and HL3/HTD_0007.

28) When TTD2 gets occupied, the train location is updated by the HL3/HTD trackside according to the requirement HL3/HTD_0007 and VSS21 become occupied according to the transition #2A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD2, according to the requirement HL3/HTD_0037.

29) Dispatcher or Traffic Management System requests route extension for the train beyond the Handover border.

30) Handing Over RBC sends a MA up to the border to the ETCS On-board and starts the Handover process with Accepting RBC, sending Pre-Announcement Message. As a consequence of this step, the train location is updated by the HL3/HTD trackside according to the requirement HL3/HTD_0007 and VSS22 and VSS23 become occupied according to the transition #2A (These VSSs are now in rear of the EoA).

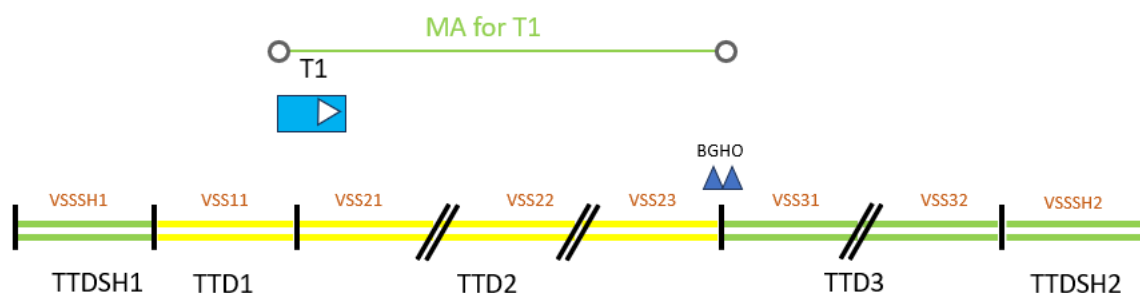


Figure 65 Step 30 Operational Scenario 6

31) Accepting RBC receives the Pre-Announcement and sends acknowledgement to the Handing Over RBC.

32) Handing Over RBC sends a request for Route Related Information.

33) Accepting RBC sends Route Related Information to Handing Over RBC.

34) Handing Over RBC extends the MA for the ETCS On-board beyond the border location according to the Route Related Information sent by the Accepting RBC up to the end of VSS32 and it sends to the ETCS On-

board the RBC Transition Order to establish a communication session with the Accepting RBC. The variable D_RBCTR is over-estimated in order to compensate the odometric error.

35) The max safe front end of the ETCS On-Board passes the RBC Handover Border.

36) The ETCS On-Board sends to the Handing Over RBC and to the Accepting RBC position reports with the max safe front end inside VSS31 in advance of the RBC Handover Border and the confirmed rear end inside VSS22. The on-board considers the Accepting RBC the supervising one, and it is able to accept only a disconnection order from the Handing Over RBC (req. 3.15.1.3.5 of SUBSET 026).

37) As soon as the Handing Over RBC receives from the ETCS On-board a position report and detects that the maximum safe front end of the train has passed the border, it shall send the Announcement Message to the Accepting RBC (req. 5.15.2.2.4.2 of SUBSET 026). VSS21 becomes free according to the transition #6B.

38) As soon as the Accepting RBC receives from the ETCS On-board a position report and detects that the maximum safe front end of the train has passed the border, it shall inform the Handing Over RBC that it has taken over the responsibility (req. 3.15.1.4.2 of SUBSET 026).

39) The train passes the border with the real front-end, the ETCS On-board reads the border balise group with an order to execute the RBC transition immediately.

40) TTD3 becomes occupied. VSS31 is set to ambiguous (Transition #3A) as the train is now located in VSS31 according to the requirement HL3/HTD_0007 and taking into account that it is not foreseen to have a communication between the 2 RBCs about the status of the VSS sections (implementation choice because currently there is not an interoperable interface to exchange the state of the VSSs). 2 shadow train timers for train T1 (one for each direction) are assigned to TTD3, according to the requirement HL3/HTD_0037.

41) TTD2 become free. VSS22 and VSS23 become free (Transition #6A). Handing Over RBC determines that the train is completely in the accepting area and orders to the ETCS On-board to terminate the communication session. The shadow train timers related to TTD2 are deleted according to HL3/HTD_0037.

42) The ETCS On-board terminates the communication session with the Handing Over RBC.

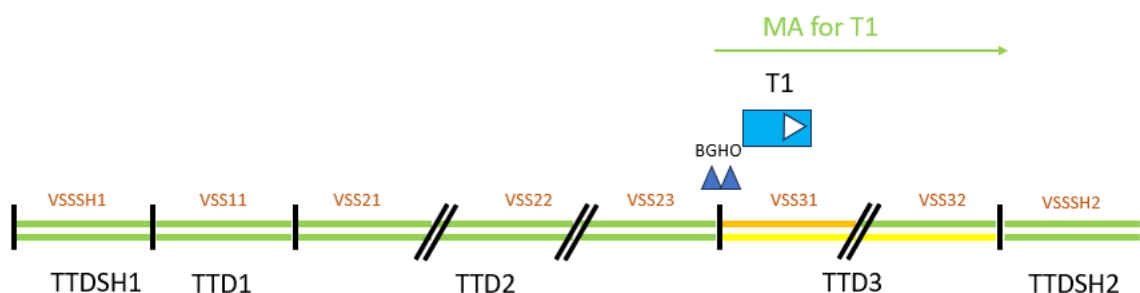


Figure 66 Step 42 Operational Scenario 6

43) Dispatcher or Traffic Management System requests a path for the train to enter the Shunting Area.

44) The HL3/HTD Trackside sends a MA to enter the shunting area. Because the TTDSH2 is free, this MA is in FS with an EoA at the end of TTDSH2. (This can be considered a rare situation in a shunting area).

45) The train T1 sends a position report with integrity confirmed, with the max safe front end of the train in VSS32.

46) VSS32 becomes ambiguous (#3A).

47) The train T1 sends a position report with integrity confirmed, with the min safe rear end of the train in VSS32.

48) VSS31 becomes unknown (#10A).

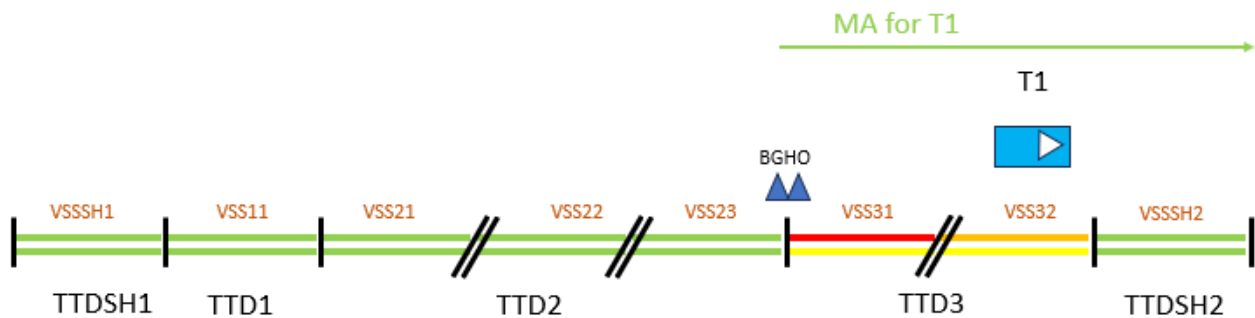


Figure 67 Step 48 Operational Scenario 6

49) The train T1 sends a position report with integrity confirmed, with the max safe front end of the train in VSSSH2.

50) According to the requirement HL3/HTD_0007 there is no update of the state of the VSS when the trackside receives the position report.

49) When TTDSH2 gets occupied, the train location is updated by the HL3/HTD trackside according to the requirement HL3/HTD_0005 and VSS31 becomes ambiguous according to the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD3, according to the requirement HL3/HTD_0037

50) When the TTD3 becomes free, all the VSSs in the TTD3 are set to free (transition #9A for VSS22, transition #4A for VSS21). VSS31 becomes occupied (transition #11A) because the shadow train timer of train T1 related to TTD3 is not expired when TTD3 becomes free. Once the transition #11A is performed, the shadow train timers related to TTD3 are deleted according to HL3/HTD_0037.

51) The train stops and the ETCS On-board reports standstill to the HL3/HTD trackside.

52) The Driver selects Shunting.

53) The ETCS On-board sends a request for Shunting to the HL3/HTD Trackside with a position report with integrity confirmed.

54) The HL3/HTD Trackside replies with the authorisation for shunting (optionally with a list of balise groups for SH area, which the train can pass when the ERTMS/ETCS onboard equipment is in shunting mode).

55) ETCS On-Board makes the transition to mode Shunting and sends the End of Mission message to the HL3/HTD Trackside, reporting the mode Shunting, according to the requirement 5.5.3.1.3 of SUBSET 026.

56) The HL3/HTD Trackside requests the termination of the communication session according to the requirement 5.5.3.1.4 of SUBSET 026.

57) The ETCS On-Board terminates the communication session.

58) The mute timer is stopped according to the requirement HL3/HTD_0033. The HL3/HTD Trackside deems the train disconnected according to the requirement HL3/HTD_0090. The disconnect propagation timer of VSSSH1 expires immediately according to the requirement HL3/HTD_0059. The HL3/HTD Trackside deletes the MA according its specific rules. Optionally the HL3/HTD Trackside can add the length of the train to the total length of trains present in the Shunting Area, provided that a (non harmonised) solution to monitor lengths in the Shunting Area is implemented

9.7 OPERATIONAL SCENARIO 7: COMPLEX OPERATION: COMBINED SWEEPING, INTEGRITY LOSS AND TTD/VSS INTERACTIONS

Introduction	This operational scenario shows a situation when the system is restarted after an halt. Once it is determined that there is only one train in the line, this train proceeds and there is an unintended train separation in advance of a level crossing. A temporary shunting area is established in order to allow to the driver to re-connect the lost part of the train (This is of course a particular choice of the specific application) and continue its mission, before there are adverse consequences on the level crossing with raised barriers. The train enters in a tunnel, there is another emergency situation and the train makes the transition to Reversing.
Assumptions	<ul style="list-style-type: none"> • The HL3/HTD Trackside can trust the information received from the On-board about the train integrity status (Q_INTEGRITY) and the confirmed train length (L_TRAININT).
Preconditions	<ul style="list-style-type: none"> • At the start of the scenario the train T1 is in Standby inside VSS11. After the unexpected halt of the HL3/HTD, the train has been stopped. • The trains don't provide the safe consist length information. • The interlocking remains active during the halt of the HL3/HTD trackside. If also the interlocking is affected by the halt, it may be that the level crossings barriers are closed at the start of the scenario, this can cause some differences, but more on procedural aspects.
Notes	<p>This use case takes origin from the use cases UC_01_07, UC_06_01, UC_06_02, UC_11_02, UC_11_04 and UC_14_01 from deliverable D15.1.</p> <p>All the timers, once started, do not expire if not explicitly mentioned.</p> <p>All the MAs are sent together with the needed information, hence applicable mode profile if applicable, linking if applicable, all the applicable profiles.</p>
Legenda	<p>In the figures the following simbology is used:</p> <p>VSSs can be ambiguous (orange colour), free (green colour), occupied (yellow colour) and unknown (red colour)</p> <p>TTD can be free (green colour) or occupied (yellow colour)</p> <p>Disconnected trains are red, connected trains are green, complete trains are blue.</p> <p>The barriers of the level crossing are illustrated with a vertical rectangle when raised, with an horizontal rectangle when closed. Tunnel is illustrated with a text box.</p>

- 1) The maintainer or dispatcher switches on the HL3/HTD Trackside.
- 2) The HL3/HTD Trackside sets all the VSSs to unknown according to the requirement HL3/HTD_0082.
- 3) The HL3/HTD Trackside performs the first run of the state machine. All the VSSs on free TTD are set to "free" according to the requirement HL3/HTD_0082.
- 4) ETCS On-board initiates the Start of Mission procedure; the stored position and level are still valid. The Driver is requested to revalidate or change the Driver ID and is offered to revalidate or change Train Running Number.

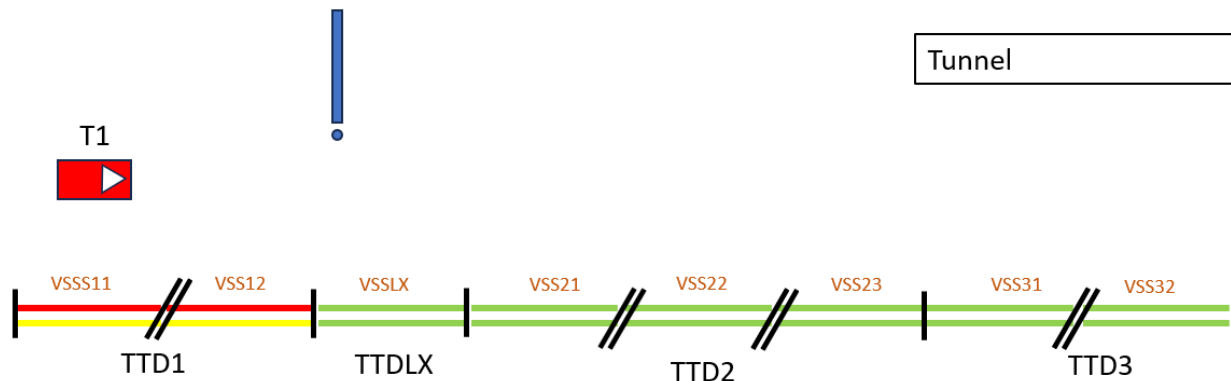


Figure 68 Step 4 Operational Scenario 7

- 5) ETCS On-board opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159).
- 6) The mute timer for train T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the requirement HL3/HTD_0089.
- 7) The session is established. After the successful establishment of the communication, the train sends the SoM Position Report according to the state A33 of § 5.4.3.2 of SUBSET 026.
- 8) The front end of train T1 is now located in VSS11 that becomes ambiguous (transition #5A). 2 shadow train timers for train T1 (one for each direction) are assigned to TTD1 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 9) Driver enters or (re-) validates the Train Data. The Train Length may be provided by OTI-L, by the driver or it can be a fixed pre-configured value. This value shall be able anyway to fulfil the safety requirements, otherwise the ETCS On-Board will never confirm its integrity.
- 10) ETCS On-board sends the Validated Train Data to the HL3/HTD Trackside, including a position report with no train integrity information.
- 11) HL3/HTD Trackside acknowledges having received Validated Train Data. HL3/HTD Trackside uses received Train Length info to locate the assumed rear end . The integrity loss propagation timer is not started because the condition c) of HL3/HTD_0071 is applicable only to trains that have previously a valid train length.
The trackside sends to the train the position report parameters periodic in time in order to allow the sending of the first position report with integrity confirmed in the following step. MA request parameters are sent according to the rules of the specific application.
- 12) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I).
- 13) The train is now complete according to the HL3/HTD trackside. The wait integrity timer is assigned according to the requirement HL3/HTD_0034 and immediately started according to the requirement HL3/HTD_0035.

The max safe rear end of the train is in VSS11 and the direction of the train is towards VSSLX, so the shadow timer towards VSSLX is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

(Note: It is in principle possible that the max safe rear end is already in TTDLX. In that case the shadow train timers of TTD1 will be not started, to try to avoid this behaviour engineering rule ShadowTrainTimer – Eng. Rule 2 has been established)

14) The driver selects “Start” and the Train sends a MA Request according to the requirement 3.8.2.1.1 of SUBSET 026.

15) The interlocking, informed by the HL3/HTD trackside lowers the barriers of the level crossing.

16) Trackside sends an MA in OS mode with an EoA at the end of VSS12 (In this case OS is used because VSS12 is unknown). The specific rules for TAF used in each country are followed.

17) ETCS On-board receives the MA and requests the OS acknowledgement to the driver according to requirement 5.9.5.1 of SUBSET 026.

18) The driver acknowledges the OS mode.

19) ETCS On-board makes the transition to OS mode according to requirement 5.9.5.2 of SUBSET 026.

20) The train T1 starts moving.

21) ETCS On-Board sends a position report with the max safe front end inside VSS12.

22) The train location is updated by the HL3/HTD trackside according to the requirement HL3/HTD_0005 and VSS12 becomes ambiguous according to the transition #3A. The HL3/HTD trackside informs the interlocking that the train is approaching the LX and that the barriers need to be lowered.

23) The interlocking lowers the barriers of the level crossing , receives the control of lowered barriers and informs the HL3/HTD trackside.

24) HL3/HTD Trackside sends an MA until the end of VSS32. Reversing area information and Reversing supervision information are sent together with the MA to allow reversing in the tunnel. The OS Mode profile covers until the end of VSS12.

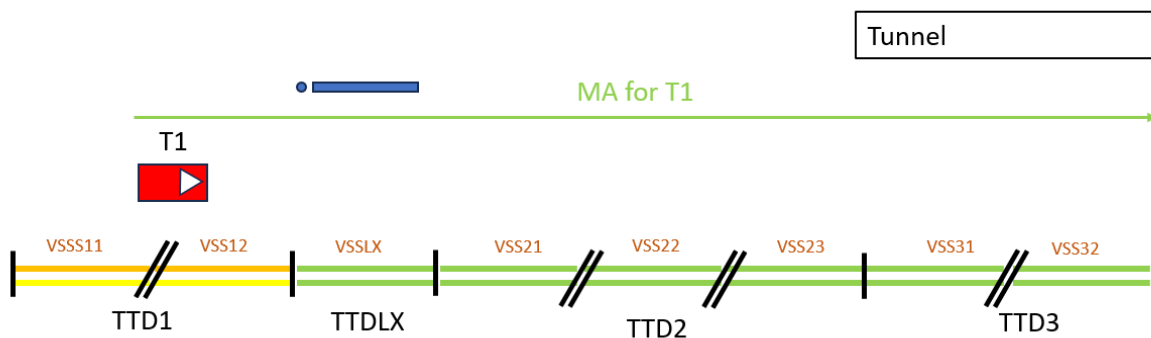


Figure 69 Step 24 Operational Scenario 7

25) ETCS On-Board sends a position report with integrity confirmed with max safe front end inside VSSLX and assumed rear end inside VSS12.

26) According to the requirement HL3/HTD_0007 there is no update of the state of the VSSLX when the trackside receives the position report. VSS11 becomes unknown (transition #10A).

27) TTDLX becomes occupied. The front end of train T1 is now located in VSSLX that becomes ambiguous (transition #3A). 2 shadow train timers for train T1 (one for each direction) are assigned to TTDLX by the HL3/HTD trackside, according to the requirement HL3/HTD_0037

28) When the TTD1 becomes free, all the VSSs in the TTD1 are set to free (transition #9A for VSS12, transition #4A for VSS11). VSSLX becomes occupied (transition #11A) because the shadow train timer of

train T1 related to TTD1 is not expired when TTD1 becomes free. Once the transition #11A is performed, the shadow train timers related to TTD1 are deleted according to HL3/HTD_0037.

29) ETCS On-Board sends a position report with integrity confirmed with max safe front end inside VSS21.

30) According to the requirement HL3/HTD_0007 there is no update of the state of the VSS21 when the trackside receives the position report.

31) TTD2 becomes occupied. The front end of train T1 is now located in VSS21 that becomes occupied (transition #2A). 2 shadow train timers for train T1 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

32) When the TTDLX becomes free, VSSLX becomes free (transition #6A). The shadow train timers related to TTDLX are deleted according to HL3/HTD_0037. HL3/HTD trackside informs the interlocking that the barriers can be raised.

33) The interlocking raises the level crossing barriers.

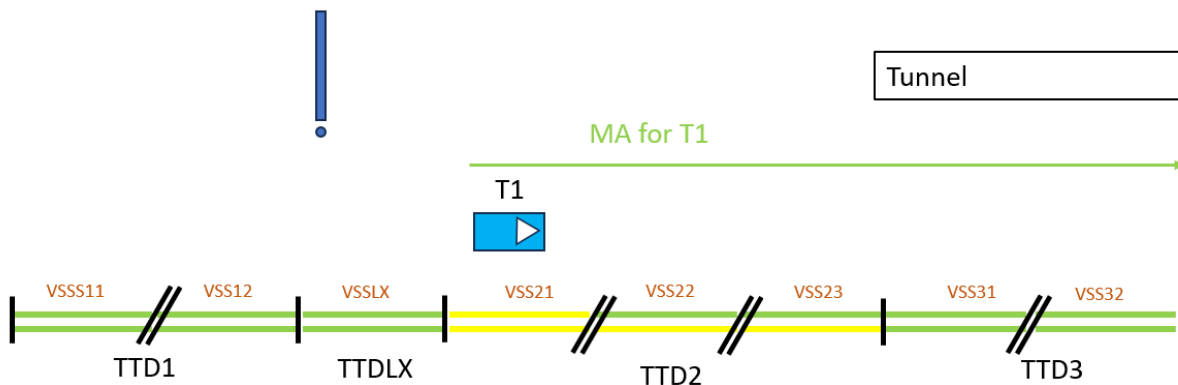


Figure 70 Step 33 Operational Scenario 7

34) ETCS On-Board sends a position report with integrity confirmed with max safe front end inside VSS21.

35) The front end of train T1 is now located in VSS22 that becomes occupied (transition #2A).

36) ETCS On-Board sends a position report with integrity confirmed with confirmed rear end inside VSS22.

37) VSS21 becomes free (transition #6B)

38) The train T1 is subject to unintended train separation. According to the assumption [Pre 1] both parts of the train T1 starts to brake.

39) ETCS On-Board sends a position report with Integrity Lost. Optionally, the Driver might be made aware of loss of train integrity. The Driver is informed of the changed train length, as foreseen by the ID A1 of the clause 5.17.2.2 of SUBSET 026. New train data are sent according to ID A7 of the clause 5.17.2.2 of SUBSET 026.

40) The Driver notices the loss of integrity and prepares to apply the specific application procedures according to the assumption [Pre 8] .

41) The train is no more treated as integer by the HL3/HTD Trackside according to the requirement HL3/HTD_0071 and VSS 22 becomes ambiguous (Transition #8A). The HL3/HTD Trackside informs the interlocking to lower the barriers (This is of course a specific application choice, it may be that the slope of the line brings the lost part of the train towards the LX). The integrity loss propagation timer of VSS22 is started. Optionally, the Dispatcher might be made aware of loss of train integrity.

42) The interlocking lowers the level crossing barriers.

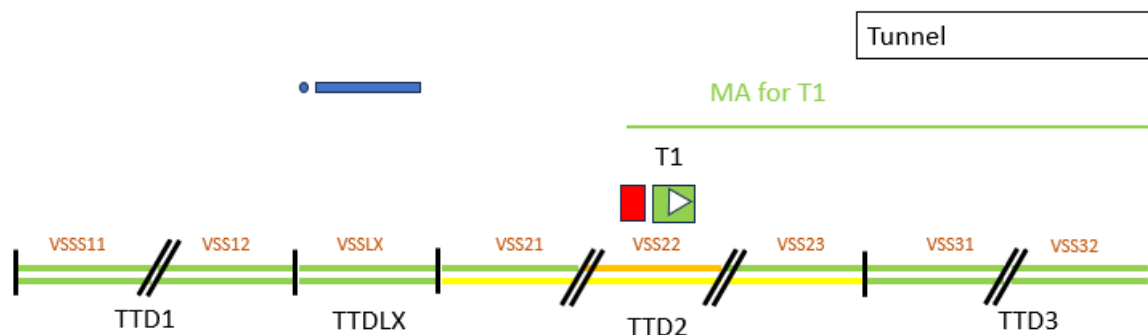


Figure 71 Step 42 Operational Scenario 7

- 43) After some time, given the fact that TTDLX has remained free after the train integrity loss, the HL3/HTD Trackside is confident that the lost part of the train is not in the LX Area and it informs the interlocking to raise the barriers (This is of course a specific application choice according to [Pre 8]).
- 44) The interlocking raises the level crossing barriers.

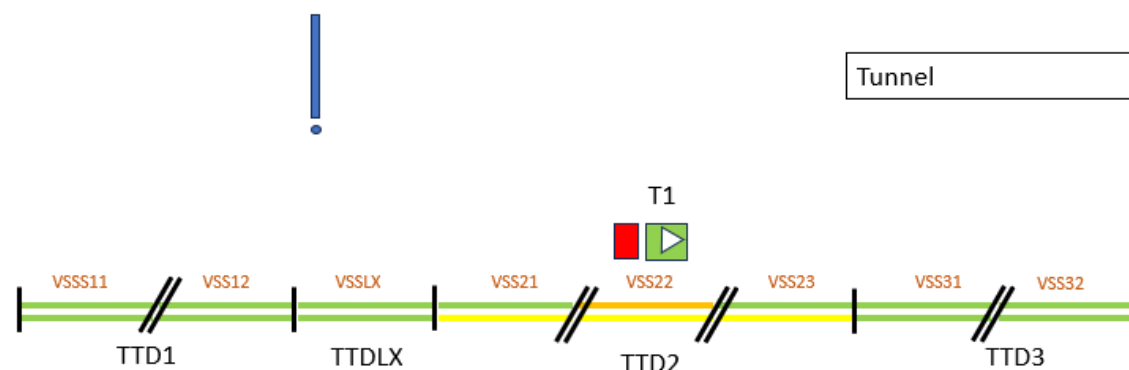


Figure 72 Step 44 Operational Scenario 7

- 45) The Dispatcher, informed by the HL3/HTD Trackside or by the Driver of the real train integrity loss, decides to establish a temporary shunting area from VSS21 to VSS23 to allow the Driver and maybe additional personnel present in the place to pick up the lost part of the train before the integrity loss propagation timer of VSS22 expires and the lost part of the train may move towards the level crossing (This is of course a specific application choice according to [Pre 8]).
- 46) The HL3/HTD Trackside sends an MA with a Shunting Mode Profile for the current location of the train.
- 47) ETCS On-Board requests the acknowledgment of the Shunting Mode to the Driver and makes the transition to mode Shunting according to the requirement 5.7.2.3 of SUBSET 026. The ETCS On-Board sends the End of Mission message to the HL3/HTD Trackside, reporting the mode Shunting, according to the requirements 5.5.3.1.3 and 5.7.1.5 of SUBSET 026.

48) The HL3/HTD Trackside requests the termination of the communication session according to the requirement 5.5.3.1.4 of SUBSET 026.

49) The ETCS On-Board terminates the communication session.

50) The mute timer is stopped according to the requirement HL3/HTD_0033. The HL3/HTD Trackside deems the train disconnected according to the requirement HL3/HTD_0090. The disconnect propagation timer of VSS22 expires immediately according to the requirement HL3/HTD_0059. The HL3/HTD Trackside deletes the MA according its specific rules.

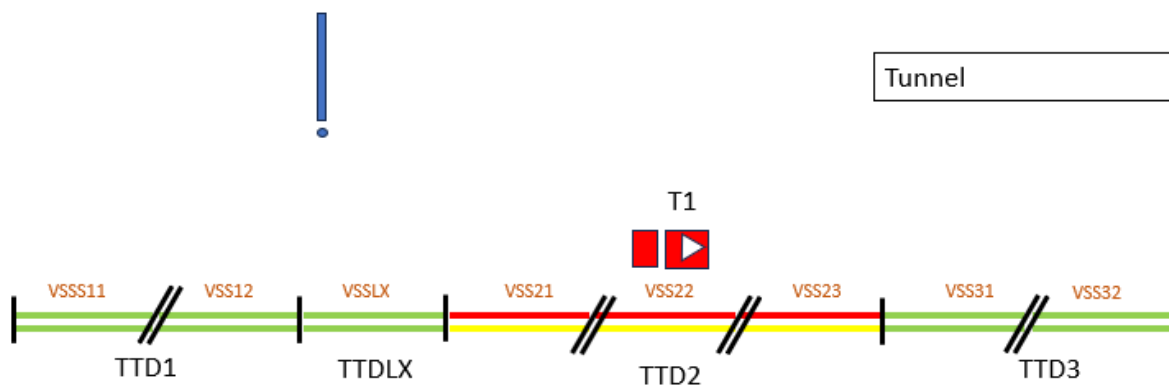


Figure 73 Step 50 Operational Scenario 7

51) After picking up the lost part of the train (maybe with the help of other personnel) the Driver selects “exit Shunting”.

52) ETCS On-Board performs the transition from Shunting to Standby, establishes the communication session with the trackside according to the requirement 3.5.3.4 c) of SUBSET 026. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159).

53) The mute timer for train T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the requirement HL3/HTD_0089.

54) The session is established. After the successful establishment of the communication, the train sends the Position Report to report the new mode according to the requirement 3.6.5.1.4 b) of SUBSET 026.

55) The front end of train T1 is now located in VSS22 that becomes ambiguous (transition #5A). 2 shadow train timers for train T1 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

56) HL3/HTD Trackside orders the disconnection of the train.

Note: this is done in order because the state S0 of the requirement 5.4.3.2 of SUBSET 026 requires the absence of established communication session.

57) ETCS On-Board sens the Message 156: Termination of a communication session to the HL3/HTD trackside.

58) The mute timer for train T1 is stopped according to HL3/HTD_0033. The Train T1 is deemed disconnected according to HL3/HTD_0090. VSS22 becomes unknown (transition #10B). The disconnect propagation timer is started for Train T1 according to HL3/HTD_0057. The shadow train timers related to TTDSH1 are deleted according to HL3/HTD_0037.

59) ETCS On-board initiates the Start of Mission procedure; the stored position and level are still valid. The Driver is requested to revalidate or change the Driver ID and is offered to revalidate or change Train Running Number.

60) ETCS On-board opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159)

61) The mute timer for train T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the requirement HL3/HTD_0089.

62) The session is established. After the successful establishment of the communication, the ETCS On-board sends the SoM Position Report according to the state A33 of § 5.4.3.2 of SUBSET 026.

63) The front end of train T1 is now located in VSS22 that becomes ambiguous (transition #5A). 2 shadow train timers for train T1 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

64) Driver enters the Train Data. The Train Length may be provided by OTI-L, by the driver or it can be a fixed pre-configured value. This value shall be able anyway to fulfil the safety requirements, otherwise the ETCS On-Board will never confirm its integrity.

65) ETCS On-board sends the Validated Train Data to the HL3/HTD Trackside, including a position report with no train integrity information.

66) HL3/HTD Trackside acknowledges having received Validated Train Data. HL3/HTD Trackside uses received Train Length info to locate the assumed rear end . The integrity loss propagation timer is not started because the condition c) of HL3/HTD_0071 is applicable only to trains that have previously a valid train length.

The trackside sends to the train the position report parameters periodic in time in order to allow the sending of the first position report with integrity confirmed in the following step. MA request parameters are sent according to the rules of the specific application.

67) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I).

68) No update of the state of the VSSs is made by the HL3/HTD trackside, because there are not the conditions identified in other requirements to set the VSS to occupied. The train is now complete according to the HL3/HTD trackside. The wait integrity timer is assigned according to the requirement HL3/HTD_0034 and immediately started according to the requirement HL3/HTD_0035.

The max safe rear end of the train is in VSS22 and the direction of the train is towards VSS31, so the shadow timer towards VSS31 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.

69) The driver selects “Start” and the Train sends a MA Request according to the requirement 3.8.2.1.1 b) of SUBSET 026.

70) HL3/HTD Trackside checks the condition to assign an MA and sends a MA with an OS mode profile until the end of VSS23 to exit the shunting area. Reversing area information and Reversing supervision information are sent together with the MA to allow reversing in the tunnel.

71) ETCS On-board receives the MA and requests the OS acknowledgement to the driver according to requirement 5.9.5.1 of SUBSET 026.

72) The driver acknowledges the OS mode.

73) ETCS On-board makes the transition to OS mode according to requirement 5.9.5.2 of SUBSET 026 and reports the new mode.

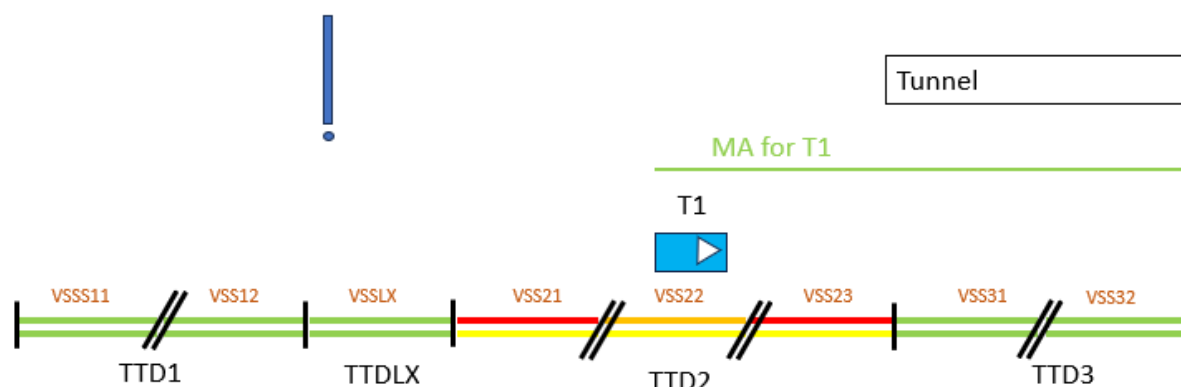


Figure 74 Step 73 Operational Scenario 7

- 74) The train sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS23.
- 75) According to the requirements HL3/HTD_0005 the train has the front end located inside VSS23 and VSS23 becomes ambiguous according to the requirement the transition #3A.
- 76) The train sends a position report with train integrity confirmed by external device (OTI-I) with the min safe rear end inside VSS23.
- 77) VSS22 becomes unknown according to the transition #10A.
- 78) The train sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS31.
- 79) According to the requirement HL3/HTD_0007 VSS31 does not change state because TTD3 is still free.
- 80) TTD3 becomes occupied.
- 81) According to the requirements HL3/HTD_0005 and HL3/HTD_0007 the train has the front end located inside VSS31 and VSS31 becomes ambiguous according to the requirement the transition #3A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD3 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 82) TTD2 becomes free.
- 83) All the VSSs in the TTD2 are set to free (transition #9A for VSS23, transition #4A for VSS21 and VSS22). VSS31 becomes occupied (transition #11A) because the shadow train timer of train T1 related to TTD2 is not expired when TTD2 becomes free. Once the transition #11A is performed, the shadow train timers related to TTD2 are deleted according to HL3/HTD_0037.
- 84) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS32.
- 85) According to the requirement HL3/HTD_0005 the train has the front end located inside VSS32 and VSS32 becomes occupied according to the transition #2A.
- 86) ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I) with the confirmed rear end inside VSS32.
- 87) VSS31 is set to free (transition #6B).
- 88) An emergency situation is detected in the tunnel.
- 89) The dispatcher instructs the driver to stop the train and do a reverse movement.
- 90) ETCS On-board makes the transition to RV mode and reports the new mode.
- 91) The train is no more treated as integer by the HL3/HTD Trackside according to the requirement HL3/HTD_0071 and VSS32 becomes ambiguous (Transition #8A). The integrity loss propagation timer is started.

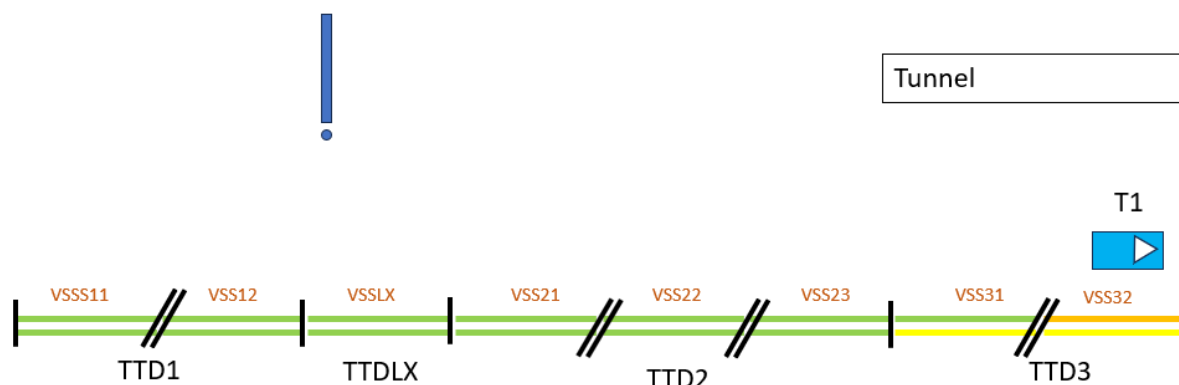


Figure 75 Step 91 Operational Scenario 7

9.8 OPERATIONAL SCENARIO 8: SUPERVISED MANOEUVRE WITH LOST VEHICLE STATES (L/R/LR)

Introduction	This operational scenario shows a situation when the train proceeds to a siding, where splitting is performed. The first part of the splitted train proceeds, while a manoeuvre locomotive picks up the other part of the original train and takes it away in Supervised Manoeuvre Mode.
Assumptions	<ul style="list-style-type: none"> The HL3/HTD Trackside can trust the information received from the On-board about the train integrity status (Q_INTEGRITY) and the confirmed train length (L_TRAININT).
Preconditions	<ul style="list-style-type: none"> At the start of the scenario the train T1 is in Full Supervision inside VSS11. The Manoeuvre Locomotive is in Full Supervision inside VSSSM. The Manoeuvre Locomotive provides the safe consist length information (ETCS On-Board with System Version 3.0). TTD2 is large enough to contain the whole train T1. The initial layout and the start position of the train and the manoeuvre locomotive is illustrated in Figure 76 and Figure 77. The derailler is set to avoid the passage of vehicles between VSSSM and VSS31, the route is set from TTD1 towards TTD3. Position report parameters and MA request parameters have already been sent to T1 and ML1. The mute timers and wait integrity timers for timers and ML1 are already assigned and started. TTD3 is composed of 2 VSSs, VSSSM and VSS31. Initially the derailler is set to avoid the passage of vehicles, so ML1 is not shown in figure. HL3/HTD Trackside can use the area covered by TTD3 as Supervised Manoeuvre Area.

Notes	<p>This use case takes origin from the use cases UC_12_01, UC_13_01 and UC_18_01 from deliverable D15.1.</p> <p>All the timers, once started, do not expire if not explicitly mentioned.</p> <p>All the MAs are sent together with the needed information, hence applicable mode profile if applicable, linking if applicable, all the applicable profiles.</p>
Legenda	<p>In the figures the following simbology is used:</p> <p>VSSs can be ambiguous (orange colour), free (green colour), occupied (yellow colour), unknown (red colour), LR (violet colour) and R (blue colour).</p> <p>TTD can be free (green colour) or occupied (yellow colour)</p> <p>Disconnected trains are red, connected trains are green, complete trains are blue.</p>

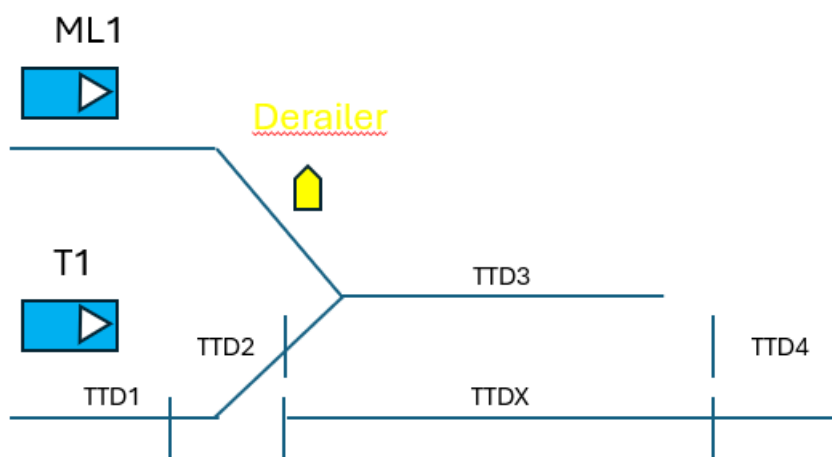


Figure 76 Initial layout Operational Scenario 8

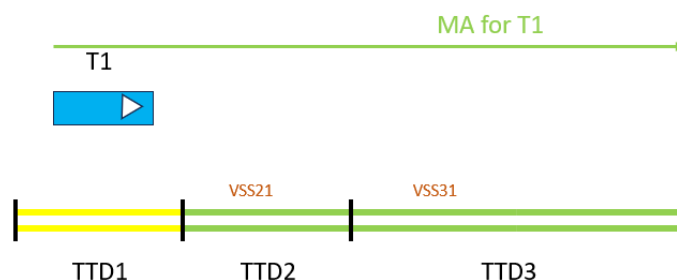


Figure 77 Starting Condition Operational Scenario 8

- 1) T1 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS21.
- 2) TTD2 becomes occupied. VSS21 becomes occupied according to the requirement HL3/HTD_0007 and the transition #2A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD2 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 3) When the TTD1 becomes free, VSS11 is set to free (transition #6A). The shadow train timers related to TTD1 are deleted according to HL3/HTD_0037.
- 4) T1 sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS31.
- 5) TTD3 becomes occupied. VSS31 becomes occupied according to the requirement HL3/HTD_0007 and the transition #2A. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD3 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 6) When the TTD2 becomes free, VSS21 is set to free (transition #6A). The shadow train timers related to TTD2 are deleted according to HL3/HTD_0037.

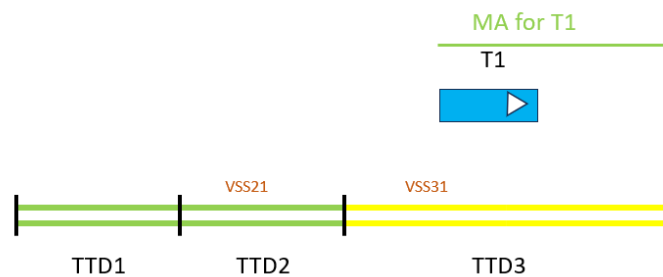


Figure 78 Step 6 Operational Scenario 8

- 7) The switches adjacent to TTD3 are moved to achieve physical independence. The derailler blocks still the passage between VSSSM and VSS31.
Note: This step is made in preparation of the following splitting to avoid propagation outside the siding. The specific application may decide that it is not needed.

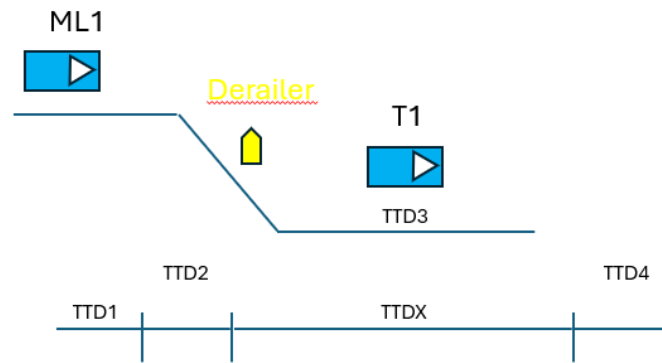


Figure 79 Layout after Step 7 Operational Scenario 8

- 8) The train T1 is split in 2 parts, the first part with ETCS On-Board is still named train T1 whereas the other one (without ETCS On-Board) is named train T2.
- 9) ETCS On-Board sends a position report with Integrity Lost.
- 10) The train is no more treated as integer by the HL3/HTD Trackside according to the requirement HL3/HTD_0071 and VSS 22 becomes ambiguous (Transition #8A). The integrity loss propagation timer of VSS31 is started.

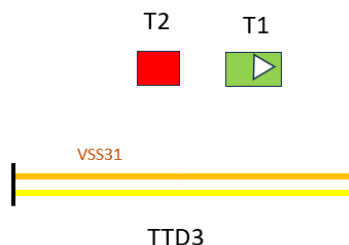


Figure 80 Step 10 Operational Scenario 8

- 11) The Driver of train T1 performs EoM (transition to No Power) and then switches back on the ETCS On-Board (transition to Standby)
- Note: This step is made to re-start the integrity evaluation for train T1.
- 12) Train T1 switches to Standby Mode and establishes a communication session according to the requirement 3.5.3.4 c) of SUBSET 026. Mode Standby is reported to the ETCS trackside.
- 13) The mute timer is assigned to train T1 according to HL3/HTD_0031 and started according to HL3/HTD_0032. The Train T1 is deemed connected according to the requirement HL3/HTD_0089. The HL3/HTD trackside orders the termination of the communication session to train T1.
- Note: This is done because the state S0 of the requirement 5.4.3.2 of SUBSET 026 requires the absence of established communication session.
- 14) Train T1 terminates the communication session according to the requirement 5.5.3.1.4 of SUBSET 026.
- 15) Train T1 is deemed disconnected according to the requirement HL3/HTD_0090. VSS31 becomes unknown according to transition #10B and the disconnect propagation timer related to VSS31 is started. The shadow train timers related to TTD1 are deleted according to HL3/HTD_0037.

- 16) Train T1 initiates the Start of Mission procedure; the stored position and level are still valid. The Driver is requested to revalidate or change the Driver ID and is offered to revalidate or change Train Running Number.
- 17) Train T1 opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159)
- 18) The mute timer for train T1 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. The train is now connected according to the requirement HL3/HTD_0089.
- 19) The session is established. After the successful establishment of the communication, the train sends the SoM Position Report according to the state A33 of § 5.4.3.2 of SUBSET 026 .
- 20) The front end of train T1 is now located in VSS31 that becomes ambiguous (transition #5A). 2 shadow train timers for train T1 (one for each direction) are assigned to TTD3 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 21) Driver enters or (re-) validates the Train Data. The Train Length may be provided by OTI-L, by the driver or it can be a fixed pre-configured value. This value shall be able anyway to fulfil the safety requirements, otherwise the ETCS On-Board will never confirm its integrity.
- 22) ETCS On-board sends the Validated Train Data to the HL3/HTD Trackside, including a position report with no train integrity information.
- 23) HL3/HTD Trackside acknowledges having received Validated Train Data. HL3/HTD Trackside uses received Train Length info to locate the assumed rear end.
The trackside sends to the train the position report parameters and the MA request parameters according to the rules of the specific application.
- 24) Train T1 sends a position report with train integrity confirmed by external device (OTI-I).
- 25) The train is now complete according to the HL3/HTD trackside. The wait integrity timer is assigned according to the requirement HL3/HTD_0034 and immediately started according to the requirement HL3/HTD_0035.
The max safe rear end of the train is in VSS31 and the direction of the train is towards VSS41, so the shadow timer towards VSS31 is started according to the requirement HL3/HTD_0038. The timer is continuously reset by the position reports.
- 26) The driver selects “Start” and the Train sends a MA Request according to the requirement 3.8.2.1.1 of SUBSET 026.
- 27) The interlocking sets the route from TTD3 towards TTD4.
- 28) Trackside sends an MA that crosses the TTD3 border until the end of TTD4, this may contain an OS mode profile according to the specific rules for TAF used in each country.
- 29) The train T1 sends a position report to the HL3/HTD trackside with the max safe front end inside VSS41. 2 shadow train timers for train T1 (one for each direction) are assigned to TTD4 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.
- 30) TTD4 becomes occupied. VSS41 becomes ambiguous according to the transition #3A.
- 31) The train T1 sends a position report to the HL3/HTD trackside with the min safe front end inside VSS41.
- 32) VSS31 becomes unknown (#10A). 2 shadow train timers for train T1 (one for each direction), assigned to TTD3 by the HL3/HTD trackside, are deleted according to the requirement HL3/HTD_0037.
- 33) HL3/HTD Trackside establishes the area of TTD3 as area where Supervised Manoeuvre is possible.
- 34) The interlocking sets the status of the derailer between VSSSM and VSS31 in order to allow the passage of trains.

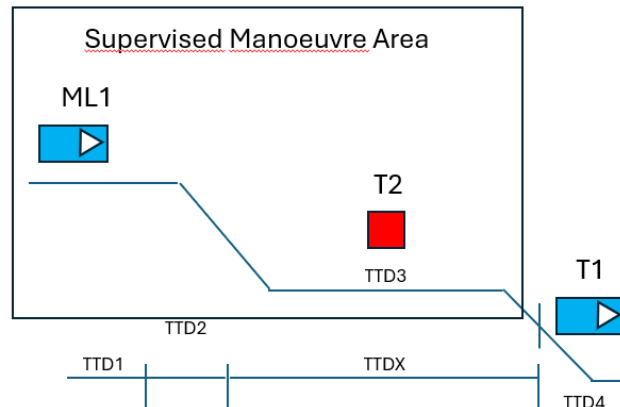


Figure 81 Layout after Step 34 Operational Scenario 8

35) The HL3/HTD trackside sends an MA to ML1 with EoA at the border between TTD3 and TTD4. The OS profile covers the entire length of the MA.

36) ML1 receives the MA and requests the OS acknowledgement to the driver according to requirement 5.9.5.1 of SUBSET 026.

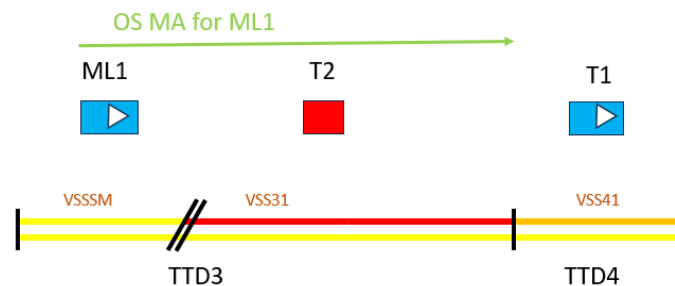


Figure 82 Step 35 Operational Scenario 8

37) The driver acknowledges the OS mode.

38) ETCS On-board makes the transition to OS mode according to requirement 5.9.5.2 of SUBSET 026 and reports the new mode.

39) The train sends a position report with train integrity confirmed by external device (OTI-I) with the max safe front end inside VSS31.

40) According to the requirements HL3/HTD_0005 the train has the front end located inside VSS31 and VSS31 becomes occupied according to the requirement the transition #12B.

41) ML1 performs the joining with T2.

42) The safe consist length in front of the engine of ML1 becomes different from 0.

Note: the resulting consist will be indicated as ML1+T2 in the following steps.

43) ML1+T2 makes the transition to Standby according to the transition [83] of part 4 of SUBSET 026 and sends the safe consist length information for Supervised Manoeuvre to the HL3/HTD trackside according to the requirement 3.18.3.10 of SUBSET 026. End of Mission is reported to the HL3/HTD Trackside according to the requirement 5.5.3.1.3 of part 5 of SUBSET 026.

44) HL3/HTD Trackside changes state machine for the Supervised Manoeuvre Area according to the requirement APP_0005 and sends the acknowledgement to the safe consist length for Supervised Manoeuvre and requests the termination of the communication session according to the requirement 5.5.3.1.4 of part 5 of SUBSET 026.

45) ML1+T2 terminates the communication session.

46) ML1+T2 is deemed disconnected by the HL3/HTD trackside according to the requirement HL3/HTD_0090. VSS31 becomes unknown (#SM8A). The disconnect propagation timer is started according to the requirement HL3/HTD_0057.

Note: In this case there is no storing of the safe consist length, this is a specific application choice.

47) ML1+T2 initiates the Start of Mission procedure; the stored position and level are still valid. The Driver is requested to revalidate or change the Driver ID and is offered to revalidate or change Train Running Number.

48) ML1+T2 opens a communication session with the HL3/HTD Trackside. After the steps foreseen by SUBSET 026, the ETCS On-board send the Session established Message (Message 159).

49) The mute timer for ML1+T2 is assigned by the trackside according to the requirement HL3/HTD_0031 and started according to requirement HL3/HTD_0032. ML1+T2 is now connected according to the requirement HL3/HTD_0089.

50) The session is established. After the successful establishment of the communication, the train sends the SoM Position Report with integrity confirmed according to the state A33 of § 5.4.3.2 of SUBSET 026.

Note: According to the requirement 4.4.7.1.6 b) of part 4 of SUBSET 026 the availability of safe consist length allows to confirm the train integrity in Standby.

51) ML1+T2 is deemed complete by the HL3/HTD Trackside. The front end of ML1+T2 is now located in VSS31 that becomes LR (transition #SM6A). 2 shadow train timers for ML1+T2 (one for each direction) are assigned to TTD3 by the HL3/HTD trackside, according to the requirement HL3/HTD_0037.

52) The driver of ML1+T2 selects Supervised Manoeuvre.

53) ML1+T2 sends the Supervised Manoeuvre Request message to the HL3/HTD trackside, with the position report with integrity confirmed and the safe consist length for Supervised Manoeuvre.

54) HL3/HTD sends an SM authorisation to ML1+T2 until the end of VSSSM.

55) ML1+T2 changes to SM Mode. According to the clause 4.4.21.1.7 of SUBSET 026 part 4 the train fronts are re-evaluated taking into account the direction of Supervised Manoeuvre MA. The train orientation is now determined by the direction of SM MA.

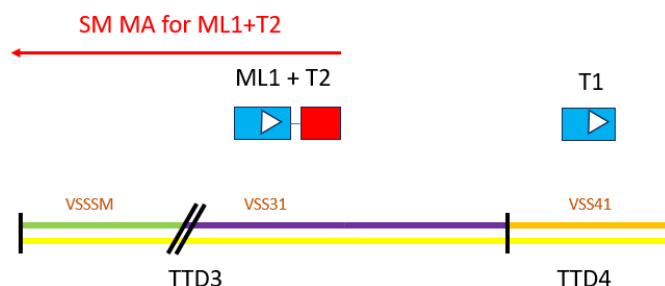


Figure 83 Step 55 Operational Scenario 8

56) ML1+T2 starts to move according to the specific procedures for Supervised Manoeuvre applicable in each country. The driver may have the collaboration of other personnel, taking into account that the active cab is in the opposite direction of the movement and there is the theoretical possibility of a vehicle in the direction of the movement.

- 57) ML1+T2 sends a position report with a max and min safe front end that excludes the possibility of a vehicle inside VSS31 between ML1+T2 and the end of VSS31.
- 58) VSS31 becomes R (#SM16A)
- 59) ML1+T2 report its max safe front end inside VSSSM.
- 60) VSSSM becomes R (#SM3A).
- 61) ML1+T2 report its confirmed rear end inside VSSSM.
- 62) VSS31 becomes unknown (#SM21A).

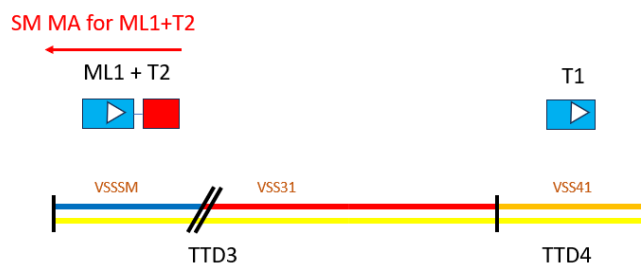


Figure 84 Step 62 Operational Scenario 6

10 TRACEABILITY WITH OPEN POINTS OF D15.1

In the following table there is a summary of the open points coming from D15.1 and how they have been addressed. The text of the document containing the open point is in the deliverable D15.1.

ID	Description	Solution in this Deliverable
OP1	About the event d) it must be clarified why the integrity is considered lost.	For the sake of simplicity the integrity is considered lost even in that case (2 or more trains in the same VSS), but there is a small modification to HL3/HTD_0068 to avoid an instantaneous start and stop of the integrity loss propagation timer.
OP2	About the Stop event: it must be clarified in which way the train can be assumed to have stopped.	A new definition of connected has been introduced, with the related requirements HL3/HTD_0089 and HL3/HTD_0090.
OP3	An agreement has to be found about how to consider the status of the VSS in relation on the TTD.	There was a typo in D15.1, no impact on this document.
OP4	It must be clarified if is it possible to consider the train disconnected if valid train data are not received.	A new definition of connected has been introduced, with the related requirements HL3/HTD_0089 and HL3/HTD_0090.
OP5	The task has to find an agreement about the Ambiguous status of the VSS.	Regarding the transition #12A, slightly modified with the condition of a “free” TTD, the requirement HL3/HTD_0072 mitigates a possible hazardous scenario with ghost trains, see D15.2 for more details.
OP6	In the UC UC_03_01 Train Joint another one, in the event #5 how to deal with the potential expiry of the timer after EoM of Train 1 (step 1). This could cause a restriction of MA for approaching Train 2.	The deliverable is remained generic, each partner can decide in its own application how to use propagation taking into account the applicable conditions. The restriction of the MA can be good for some applications, bad for others.
OP7	In the UC UC_13_02 Sweeping, in the event #3 This may cause a restriction of MA for the sweeping train because free VSSs in front of the train will change to unknown. The task has to find an agreed position.	The deliverable is remained generic, each partner can decide in its own application how to use propagation taking into account the applicable conditions. The restriction of the MA can be good for some applications, bad for others.

OP8	In the UC UC_14_01 Trackside Initialisation #1 Must be clarified which is the trigger condition for starting the timer.	The timer is not started anymore with the new update of the requirement HL3/HTD_0082. See also the note in the requirement HL3/HTD_0061.
-----	--	--

Table 10 Solutions of Open Points of D15.1

REFERENCES

- [1] COMMISSION IMPLEMENTING REGULATION (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009
- [2] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment
- [3] COMMISSION IMPLEMENTING REGULATION (EU) 2023/1695 of 10 August 2023 on the technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union and repealing Regulation (EU) 2016/919
- [4] ERTMS/ETCS Hybrid Train Detection, 16E042, Rev. 1F
- [5] Deliverable D4.1 Moving Block Specification Part 6 – Safety Analysis, X2R5-T4_2-D-SMD-006-10, 21-Dec-2022
- [6] 80. ERTMS/ETCS Hybrid Train Detection Engineering, 21E087 Version 3
- [7] R2D-WP19-D-MER-001-01, D19.1 – Train Integrity and Train Length Architecture & Functional Requirements
- [8] ERA/ERTMS/033281 Version 5.0, Interfaces between Control-Command and Signalling Trackside and other Subsystems
- [9] ERA_ERTMS_015560 Version 4.0.0, ETCS Driver Machine Interface
- [10] R2D-T15_1-D- MER-001-01 Rev. 01.01, D15-1 – HL3 System Specification with identification of use cases and related engineering rules
- [11] FP2-T15_2-A-FSI-012-08, D15.2 – HL3 Safety Analysis
- [12] SPT2-TrafficCS Traffic CS System Concept (rev. 523263)