Rail to Digital automated up to autonomous train operation

D15.1 – HL3 System Specification with identification of use cases and related engineering rules

Due date of deliverable: 31/08/2024
Actual submission date: 05/12/2024

Leader/Responsible of this Deliverable: Francesco Inzirillo MERMEC

Reviewed: Y/N

Document status		
Revision	Date	Description
00	25/02/2024	First issue
00.01 – 00.22		internal versions preparatory to the drafting of the final version
01	23/07/2024	Final Version provided to TMT
01.01	05/12/2024	Final Version after Maturity Check

Project funded from the European Union's Horizon Europe research and innovation programme		
Dissemination Level		
PU	Public	X
SEN	Sensitive – 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
Manuel Cáceres	ADIF	Reviewer/Contribution chapter 7
Gregorio Velasco	ADIF	Reviewer/Contributor
Alfonso Martínez	ADIF	Reviewer/Contributor
Javier Montes	ADIF	Reviewer/Contributor chapter 7
Staffan Pettersson	ATSA ALS SE	Reviewer of the document
Daniel Kolář	AZD	Reviewer/Contributor of the document
Maria Bermudez	CAF CAFS	Reviewer/Contributor of the document
Oliver Röwer	DLR	Reviewer/Contributor of the document
Dominik Hansen	GTSD	Reviewer/Contributor of the document
Jose Ramón Seco Sáiz	INDRA	Reviewer of the document
Francesco Inzirillo	MM and AS	Main writer
Christian Bagnoli	MMSTE	Reviewer/Contributor of the document
Chantal Schneider	NSR	Reviewer of the document
Martin Nusselder	PRORAIL	Reviewer of the document
Claudio Evangelisti	RFI (FSI Affiliated Entity)	Review and writing of some paragraphs and review the document
Craig McLellan	SMO	Reviewer of the document
Jan Bystrom	TRV	Reviewer of the document

EXECUTIVE SUMMARY

In the last years many initiatives have developed the Hybrid Train Detection concept for ERTMS/ETCS applications. Some projects in different countries are also starting the implementation of this solution probably making different assumptions and using national rules.

This document aims to define a standardised implementation of the Hybrid Train Detection concept and to align it with the Operational view and System Architecture being defined in the System Pillar.

It includes the System Definition (as defined in EN50126) with the identification of System Interfaces and Actors, the System Requirement Specification and the main Use Cases and Engineering Rules. A view on different applications (high speed lines, regional lines, etc.) will be provided to analyse possible different engineering rules for the different use cases.

The starting point for the development of this document is based on the deliverables of Shift2Rail X2Rail-5 Moving Block and the EUG documents on the Hybrid Train Detection concept.

This deliverable contains the activities resulting from both task 15.1 System Definition System Interfaces, Requirements and Use Cases and task 15.3 Engineering Rules. The harmonization of the activities in the two tasks has produced the current document that has in the opinion of the participants within these activities achieved the intended purpose.

Initially, there were problems in receiving the documents from Shift2Rail but it was solved by the JU in the following months.

The activity carried out in WP15 task 15.1 has produced a consistent and exhaustive set of Use Cases that covers all the foreseen operating options of the HL3/HTD system.

Also, the set of specifications and definition of requirements mediated by the reference documents has allowed these to be consolidated and shared by all participants. The requirements that integrated those from the existing documents were defined from the Use Cases produced.

The document also reports the interactions that occurred with the R2DATO WP19 and WP20 for the interaction between the determination of train integrity and train length, which are fundamental for an efficient use of the HL3/HTD system.

The open points that emerged during the work have not all been closed, these will be part of the activities that will be allocated in R2DATO WP16.

Moreover, the document is considered sufficiently advanced to be delivered to the work of WP16.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

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	A train with an established safe radio connection to the trackside and valid train data or a train with an established safe radio connection to the trackside and safe consist length. Note: This is slightly different from the definition in the HTD Principles [8], because it takes into account the possibility of the use of safe consist length.
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 [8] because it takes into account the TSI 2023. Anyway, it is functionally equivalent, it is expected to stress the importance of the instances T and T_0
CRE(D)	Confirmed Rear End by Driver. Same meaning as CRE (see above abbreviation), but with confirmation by driver.
DAC	Digital Automatic Coupling
Established rear end	Trackside view of the rear end of a train which is treated as integer.
EVC	European Vital Computer (ETCS on board)
Free (VSS)	The trackside is certain that no train axle is located on the VSS. Note: This is slightly different from the definition in the HTD Principles [8], 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 [8]
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.
HL3/HTD	ETCS Level 2 with reduced train detection according to the HTD Principles [8] 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 [8] 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 is already in service before the introduction of HL3/HTD or Moving Block)

Acronym	Description
L3	ETCS Level 3 from previous ETCS baselines. Similar to L2 with no or reduced train detection and trains with train integrity.
MA	Movement Authority
MSFE	Max Safe Front End
mSFE	min Safe Front End
Occupied (VSS)	The trackside has information from a position report that a 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 [8] [8] because the term 'complete' is used instead of 'integer'. For Consists in Supervised Manoeuvre: 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 or consist is inside the same VSS on which the first consist is located
OTI-I	Onboard Train Integrity, function for Train Integrity Monitoring (TIMS in the CCS TSI)
OTI-L	Onboard Train Integrity, function for Train Length Determination
PTD Information	Positive Train Detection, 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 [8], because it takes into account the packets regarding the train lengths,
R2DATO	Rail to Digital automated up to Autonomous Train Operation
Shadow Train	A ghost train that is chasing a train operating in the HTD area
Shadow Train Risk	Generic term used in order in order to indicate the risk related to: • Shadow Trains; • More trains in a VSS; • Lost vehicles maintained at standstill, for example after integrity loss
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

Table 1: Abbreviations and Acronyms

1 INTRODUCTION

This document is the deliverable D15.1 of the tasks 15.1 and 15.3 included in WP15 “Hybrid Level 3 Specification” in FP2 R2DATO project.

Background of ERTMS/ETCS Hybrid Train Detection System, hereinafter referred to as HL3/HTD System, is ETCS level 2/3: from the start the ETCS specifications contained a trackside implementation concept where the train separation function (collision avoidance) is based on the position of the train rear end reported by the on-board to the trackside.

In conventional level 2 applications, the "end of authorities" ensuring not overlapping MAs are always the borders of fixed block sections and the MA is extended according to their state (free or occupied) reported by Train Detection Systems. However, if train integrity information is available in the ETCS position report, then it introduces the possibility of placing the end of authorities closer to the tail of the preceding train, and no longer restricted to Train Detection boundaries.

The HL3/HTD system is a Level 2 ERTMS/ETCS application that uses fixed (pre-configured) virtual blocks for the train separation and train integrity confirmation in the position report, together with a limited installation of trackside train detection, to determine the track status. The presence of trackside train detection is used for the separation of trains which are not able to confirm integrity , as well as for the handling of degraded situations.

The hybrid solution proposed with HL3/HTD offers the advantages of a reduction of the trackside life cycle cost, or of improved performance, or a combination of both.

Note: a reference for the train position remains necessary, therefore Eurobalise shall be installed as in existing ETCS level 2 implementations or other references, when available, can be used (for example virtual balises generated by satellite positioning provided it has no impact on the concept).

In HL3/HTD it is easy to achieve very short fixed virtual block sections just by adapting the configuration of the trackside system, without an increase in costs for additional trackside devices, thereby improving the performance at relatively low cost, provided that the trackside subsystem can provide adequate computational power.

The main challenge for HTD deployment is due to the fact that safety still relies on the knowledge by the trackside system that a Virtual Sub-Section (VSS) is really not occupied by a “not connected” train or other obstacles.

While the state “free” of a VSS can easily be determined when it is included in a fixed section reported free by TTD, in case the fixed section is reported occupied by TTD, the state of a VSS included in it must be determined through the positions of train’s front and rear ends reported to trackside and the train integrity is confirmed. If trains not connected are running in the line, hazards arising from their presence must be analysed. This analysis is part of deliverable D15.2, whereas in this document the system definition and the related use cases are provided.

1.1 SCOPE

This document constitutes the Deliverable D15.1 “HL3 System Specification with identification of use cases and related engineering rules” in the framework of the WP15 of FP2 R2DATO.

This document describes the signalling system called “ERTMS/ETCS Hybrid Train Detection System”, hereinafter referred to as HL3/HTD System. This specification is planned to be used in WP16 of R2DATO in order to achieve Technology Readiness Level 6 (TRL6) according to what is established in the R2DATO Grant Agreement.

1.2 PURPOSE

The purpose of this document is to provide a solid basis of description of the ERTMS/ETCS Hybrid Train Detection System Function in terms of System Specification Requirements, Engineering Rules and Use Cases.

In the following table is reported the document structure.

§	Title	Description
1	Introduction	Current chapter document introduction
2	Development Methodology	Describe the activities performed for obtain this document
3	System Definition	Contains the System Definition of the ERTMS/ETCS Hybrid Train Detection System, including the assumptions
4	HL3/HTD System specification	This section describes the operational concept and the principles on which HTD is based.
5	Overview on HL3/HTD Use Cases	This section contains the operational scenarios that can occur during the mission of a train on a line where HTD is implemented, in both normal and degraded conditions
6	Additional HL3/HTD Requirements	Summarises the functional requirements for HTD design arising from the system definition and use cases
7	Engineering Rules	This section summarises the engineering rules to be adopted for HTD installation arising from the system definition and use cases
8	HL3/HTD USE CASES	Contains all the developed Use Cases divided into groups
9	Adapted requirements from EUG specification	Contains all functional requirements applicable to HL3/HTD
10	Exported constraints	Contains all the constraints exported to external actors
11	Conclusions	The results obtained and the conclusions are contained in this chapter.

Table 2: Document Structure

1.3 LIMITATIONS

Detailed operational rules for HL3/HTD are not within the scope of this document.

2 DEVELOPMENT METHODOLOGY

In this section, the methodology on how this deliverable was developed is reported. The methodology section is split into the following sections: i) Deliverable Objectives; ii) Process Overview; iii) Existing and Relevant Documents; iv) Methodology for Deliverable Development.

2.1 DELIVERABLE OBJECTIVES

This deliverable is created on the basis of the guidelines as described in the Grant Agreement. It is linked to the activities performed in the task 15.1 and 15.3. From the GA WP15 has this mandate.

The overall objective of the HL3 Work Package is to align and integrate the Hybrid ERTMS/ETCS Level 3 (HL3) approach into the future Functional Railway System Architecture defined by the System Pillar and to apply the defined principles to different kinds of railways(e.g., it is expected that high density lines will have different needs in comparison to regional low traffic lines). For several Infrastructure Managers, HL3 is perceived as a faster and simpler way to increase capacity at a lower cost, maintaining a highly reliable signalling system, without the complexity of a Full Moving Block architecture. This WP will build on top of previous HL3-related achievement like the EUG (ERTMS Users Group) specs or S2R deliverables, advancing on possible open points and gaps of the specifications that are currently available. In HL3, the track occupancy is primarily defined by a train detection system installed in the track, and the train position reporting information are used to elaborate virtual sections in order to put more trains in a physical section. In Moving Block, the track occupancy is primarily defined from the train position report information and train detection systems installed on the track are optional to manage some specific situation (clearances, degraded modes recovery). Within this Work Package, the objectives are as follows: • Alignment of the HL3 approach with the EU-RAIL System Pillar. • Elaboration of an operational concept for a HL3 system based on the System Pillar operational concept, analysing the application of the HL3 specifications to different networks and kind of lines (e.g., high density lines, regional low traffic lines, etc.). • Definition of HL3 engineering rules applicable to different railway types, considering the different demonstrators to be realized within the EU-RAIL. • Performance of a generic safety analysis for HL3 applications.

Task 15.1: HL3 -System Definition –System Interfaces, Requirements and Use Cases (Leader: MERMEC; Participants: FSI, GTSD CAF, ADIF, INDRA, DLR, NS, PRORAIL, ATSA, SMO, AZD, TRV) (Duration: M1 to M21) The objective of this task is to work collaboratively to derive a System Definition based on the HL3 principles paper and S2R findings related with HL3, which is aligned with the System Pillar Functional Railway System Architecture in regard to interfaces and level of detail. This task also includes to refine the level of detail of the System Pillar requirements to completely cover the HL3 principles. Also, HL3 with Train Integrated Management System (TIMS) safety requirements as included in TSI 2022 and S2R requirement will be considered. Various use cases will be identified and analysed (e.g., high density lines, regional low traffic lines, etc.).

Task 15.3: HL3 - Engineering Rules (Leader: ADIF; Participants: FSI, ADIF, GTSD, ATSA, SMO, AZD) (Duration: M1 to M21) The objective of this task is to work collaboratively to elaborate and define engineering rules for deploying HL3 system defined in tasks 15.2 and 15.3 to main and regional lines.

On the basis of the description that was provided in the GA, the following can be concluded that are prerequisites for the creation of the D15.1:

1. Relevant input from partner projects or other entities (X2Rail-5 Deliverable D4.1 EUG, other FAs and SP) needs to be collected, analysed and if relevant, included in the deliverable. Input from these partner projects has been considered until month 12, December 2023, of the project.
2. Task 15.1 focuses on the following main activities: definition of the specification, requirements and the use cases for HL3.
3. Task 15.3 focuses on the elaboration of the engineering rules.

2.2 PROCESS OVERVIEW

Figure 1 shows the process followed to obtain Deliverable D15.1.

As can be seen from the process shown in Figure 1, the main steps that participated in the achievement of the final document are indicated.

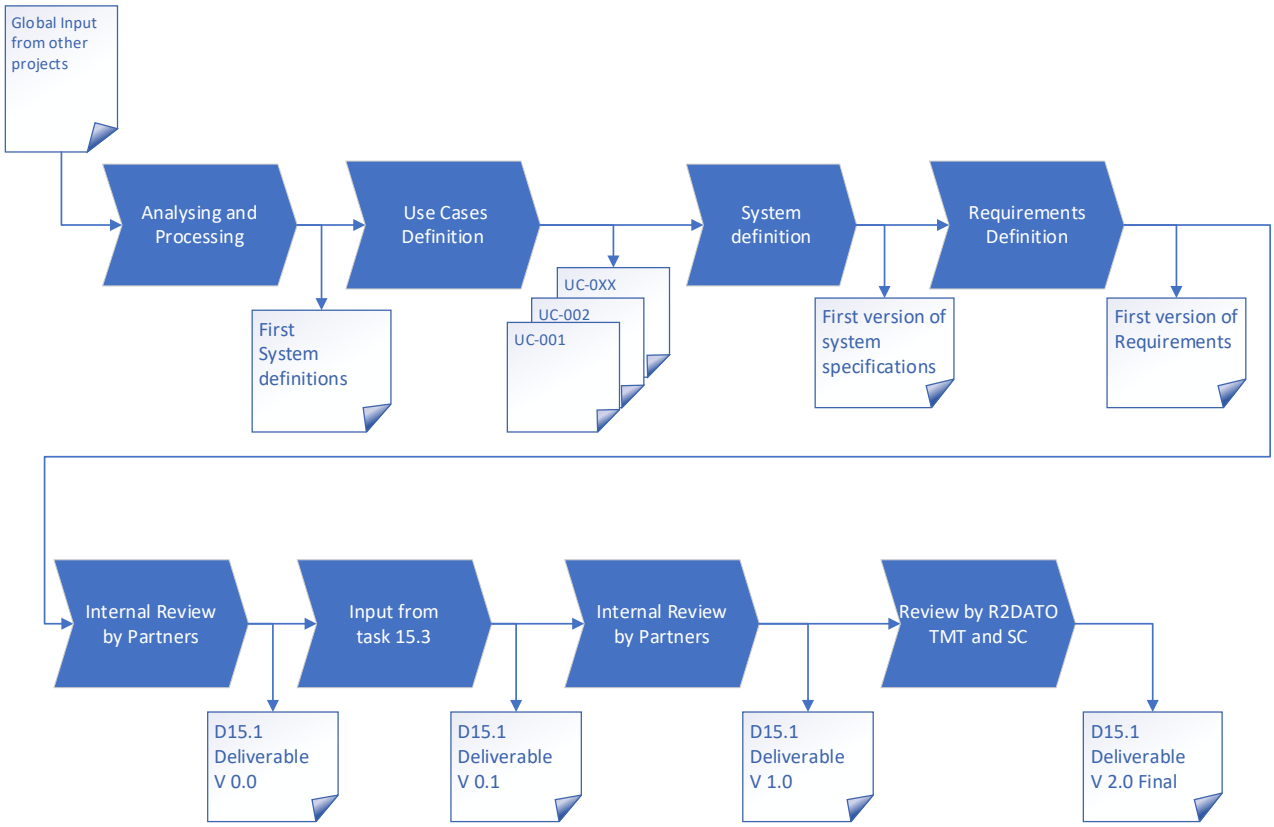

Figure 1: Process Overview

2.3 EXISTING AND RELEVANT DOCUMENTS

As input to Work Package 15, Task 15.1 process, the state of the art was considered and deliverables from past projects or relevant entities were identified and actively requested at Work Package level. For this process, inputs were collected from several relevant projects:

- SUBSET-026-3 (4.0.0). System Requirements Specification Chapter 3 – Principles.
- SUBSET-026-4 (4.0.0). System Requirements Specification. Chapter 4 - Modes and Transitions.
- SUBSET-026-5 (4.0.0). System Requirements Specification. Chapter 5 - Procedures.
- SUBSET-034 (4.0.0) Train Interface FIS
- SUBSET-091 (4.0.0) Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2
- SUBSET-119 (4.0.0) Train Interface FFFIS
- SUBSET-120 (4.0.0) FFFIS TI – Safety-related Requirements
- X2Rail-5 Deliverable D4.1 Moving Block Specification Part 2 – System Definition Rev-09
- X2Rail-5. Deliverable D4.1 Moving Block Specification. Part 3 - System Specification. Rev-23
- X2Rail-5 Deliverable D4.1 Moving Block Specification Part 4 – Operational Rules Rev-15

- X2Rail-5 Deliverable D4.1 Moving Block Specification Part 5 – Engineering Rules rev-16
- EUG ERTMS/ETCS Hybrid Train Detection Ref 16E042 Ver. 1F Date 20 12 2022
- 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
- COMMISSION IMPLEMENTING REGULATION (EU) 2023/1693 of 10 August 2023 amending Implementing Regulation (EU) 2019/773 on the technical specification for interoperability relating to the operation and traffic management subsystem of the rail system within the European Union

These documents are present also in the Reference chapter.

To avoid further delay and ensure a viable result before the deadline M21 of WP15, the work package team started work on the basis of these deliverable and draft documents, establishing the potential gap with the intended WP15 results (remaining open points, etc.).

2.4 METHODOLOGY FOR DELIVERABLE DEVELOPMENT

The work carried out in Task 15.1 involved the study and further study of the results obtained in previous projects.

The reference documents are [4],[5],[6],[7] and [8].

Once the chapters were drafted, the workgroup followed a structured approach from the point of drafting the chapters to finalization of the deliverable with the required consensus and approval.

The following steps illustrate this process:

1. First development stage – responsibility of partner writing the chapters;
2. Review – responsibility of partner reviewing the chapters;
3. Second development stage that include the input from task 15.3 – responsibility of partner writing the chapters;
4. Formal review – responsibility of partner reviewing the document;
5. Third development stage that include the final input from task 15.3 – responsibility of partner writing the document;
6. Finalized (stored in Cooperation Tool the Deliverable document D15.1) – responsibility of partner writing the document;

As can be seen in the process described, there was a good collaboration among the partners for writing and reviewing the chapters before agreeing on the finalized document.

3 SYSTEM DEFINITION

This chapter will provide the general system definition, according to the scope of deliverable D15.1 of R2DATO. It is the prerequisite for the system specification that is in chapter 4.

For reaching the goal the following steps are described for the system definition:

- ✓ System Scope
- ✓ System Objective
- ✓ System Capabilities
- ✓ System Boundaries
- ✓ System Function and Elements
- ✓ Scope of operational requirements influencing the system
- ✓ Assumptions and exiting Safety Measures

3.1 SYSTEM SCOPE

System Version 2.1 is expected to cover all the functionalities of System Version 3.0, except for Supervised Manoeuvre, use of FRMCS, ATO operation and other enhancements.

System Version 2.2 is expected to cover all the functionalities of System Version 3.0, with the exception of Supervised Manoeuvre, use of FRMCS and other enhancements.

The detailed CRs that are excluded by System Versions 2.1 and 2.2 are listed in the Appendix G of the CCS TSI [9].

3.2 SYSTEM OBJECTIVE

The main objectives of the HL3/HTD system are a cost reduction of the trackside implementation and/or an increase of the line capacity. The cost optimization (across the overall system life cycle) is given by the partial removal of trackside train detection equipment, i.e. covering the trackside with the implementation of longer fixed block sections or by a proper use of the ETCS radio hole functionality. Long fixed sections do not decrease the system performance in terms of train spacing, due to the fact that each section is subdivided into short virtual sections.

The reduced number of trackside assets improves indirectly the overall trackside system reliability.

Regarding the increase of the line capacity, when HL3/HTD is integrated in an ETCS level 2 system, the capacity of the line can be increased using short fixed virtual block sections by adapting the configuration of the trackside system after the implementation of the state machines to set the status of the virtual block sections, without an increase in cost for the installation of additional trackside devices.

The HL3/HTD system proposed in this document achieves its objectives with minimum impact on the basic structure and functionality of ETCS and existing interlocking, radio and Traffic Management Systems.

In particular this document is expected to take into account:

- ETCS On-Board Subsystems fully compliant to System Version 2.1, 2,2 or 3.0 according to the COMMISSION IMPLEMENTING REGULATION (EU) 2023/1695 of 10 August 2023;
- ETCS Trackside Subsystems fully compliant to System Version 2.1, 2,2, 2.3 or 3.0 according to the COMMISSION IMPLEMENTING REGULATION (EU) 2023/1695 of 10 August 2023;

It is in principle possible to realise HL3/HTD implementations with lower System Versions or with partial fulfilment, but this possibility is left to the specific applications.

Even if the HL3/HTD does not, in itself, require large modifications, it can make use of additional technologies when available, like ATO, ASTP or FRMCS, without substantial modifications to the behaviour of the system.

Train equipped with OTI-I and OTI-L should be able to run on both HL3/HTD and Moving Block lines. The investment on the train can therefore be used for both concepts.

3.3 SYSTEM CAPABILITIES

The fundamental objectives of the system into which the proposed HL3/HTD will be integrated are to ensure safe train movement and prevent railway accidents, in terms of collisions and derailment, i.e. supervision of train spacing and respect of speed limitations: in this context, the full extent of train protection functionality and performance, as provided by current ETCS implementations, is ensured by HL3/HTD implementation. The objective is to increased line capacity and facilitate the integration/adaptation to the regional lines.

The increased line capacity through additional virtual sections is obtained with the same SIL as the train spacing through fixed block separation.

The remaining train detection equipment installed trackside permits:

1. Safe management of mixed traffic of trains equipped with ETCS suitable for HL3/HTD and trains not equipped with ETCS or able to confirm integrity.
2. Safe and easy management of degraded conditions (e.g., movement of trains affected by loss of on-board train integrity confirmation)

3.4 SYSTEM BOUNDARIES

The main characteristic of the HL3/HTD functional aspect is that it 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 reduced 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 HL3/HTD concept is defined in a generic way, which makes it applicable for all kind of lines, from high-density, high-performance lines to low density lines. To implement the concept, TTD sections (including those containing movable elements) can be divided into several VSS sections.

Note: The introduction of VSS in general does not change the principles of route setting and handling of MAs since VSS are treated in the same way as sections with TTD. Also, the principles for placing marker boards do not need to change compared to sections with TTD. The rulesrelated to the interlocking, the Traffic Management System and the conditions to assign and send an MA by the RBC are not in the scope of this document, and it is planned that the HL3/HTD is “super-imposed” on the existing legacy rules and interfaces. To give an example, it is possible that the RBC today takes as a necessary but not sufficient condition to send an MA in Full Supervision that the status of a TTD is “free”. With the implementation of HL3/HTD the same RBC is expected to use instead as input condition the status “free” of one or more VSSs belonging to the same TTD.

The reference architecture for HL3/HTD is the current architecture defined in the TSI, with the elimination of some ETCS Level 1 features planned to be discontinued in the TSI [9] (Euroloop and Radio Infill), as show in Figure 2.

It is planned that the HL3/HTD software algorithms will be implemented in the trackside, in particular to manage the requirements to set the status of virtual sub-sections. In general, the ETCS On-board is expected to implement the requirements defined in the TSI according to the applicable System Version, with some small clarifications to avoid misunderstandings (to prevent train length overestimation and excessive delay in the sending of some information see section 10.1).

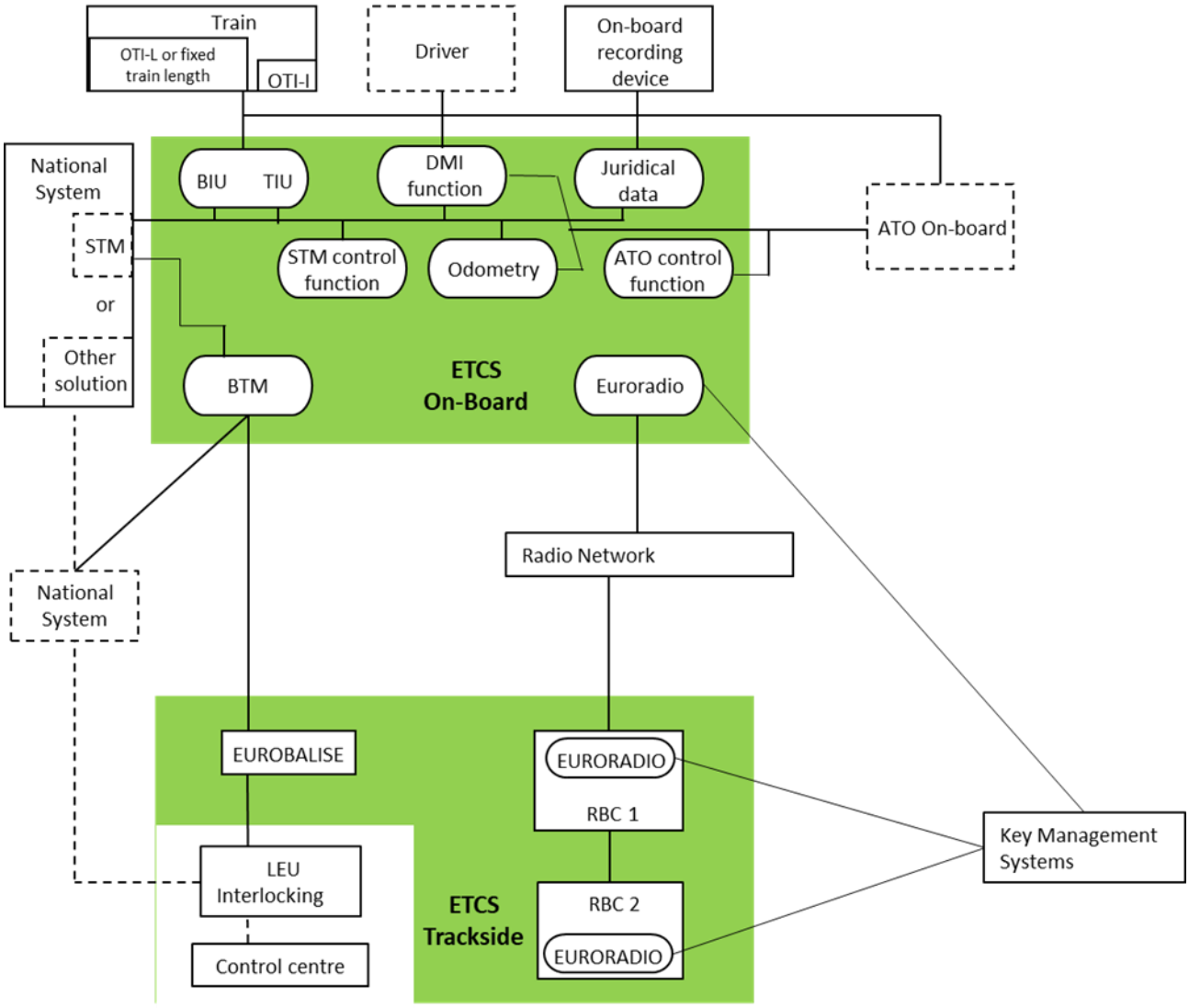

Figure 2: Architecture for HL3/HTD

Regarding the other parts that are outside the green area of Figure 2**,** the following considerations are made:

- In the figure the radio network is generic, it can be GSM-R or FRMCS as in the TSI today, but in general HL3/HTD can be implemented with any radio communication system suitable for ETCS.
- Regarding the key management systems, any system providing an adequate level of cybersecurity can be used;
- Train driver can be present or not, in case of ATO;
- In general, the on-boards without ETCS but with the National System can be managed in HL3/HTD as “ghost trains”. Some use cases are reported in § 8.19. Anyway, these features are subject to specific application analyses, as the behaviour of the National Systems is not harmonised;

- analogy with L2-TTD; in HL3/HTD the trains are generally expected to be equipped at least with OTI-I and OTI-L (providing the information defined in § 2.6.3.2 of SUBSET-034) or OTI-I and OTI-L connected to DAC (providing the information defined in § 2.6.2 of SUBSET-034). Integrated devices providing Train Integrity and Train Length are possible. According to some interpretations of clause 2.6.3.2.1 in SUBSET-034 it is possible to use a preconfigured train length instead of an OTI-L or DAC. These interpretations are accepted in the framework in WP15, anyway some use cases, like splitting, have to be managed procedurally in this case. Trains equipped with ETCS but without OTI-I can be allowed in HL3/HTD, but with a performance degradation for following trains.

A Human Machine Interface of the RBC can be present, it is expected that it will be defined in order to allow easy operation of the line, taking into account its features (for example the dispatcher may be involved in sweeping operation and an adequate display of the information may be needed).

Regarding the details of the interface of the ETCS On-Board with the OTI-I and OTI-L (that are part of R2DATO WP19 and WP20), the following architecture (see Figure 3) has been adopted (OTI-L could be not present if fixed train length is used, DAC is expected to be connected to OTI-I and OTI-L without direct interface to ETCS On-Board).

What is specified in WP19/WP20 provides that OTI-I has the function of recognizing the integrity of the train. This will report three possible values to the EVC: Confirmed, Unknown or Lost. Confirmed will be sent only if there is also the real time computed train length evaluated by OTI-L.

Actually, Diagnostic information from OTI-I and OTI-L is not foreseen in Subset-119. Also, the reset command towards OTI-I and OTI-L is not currently foreseen.

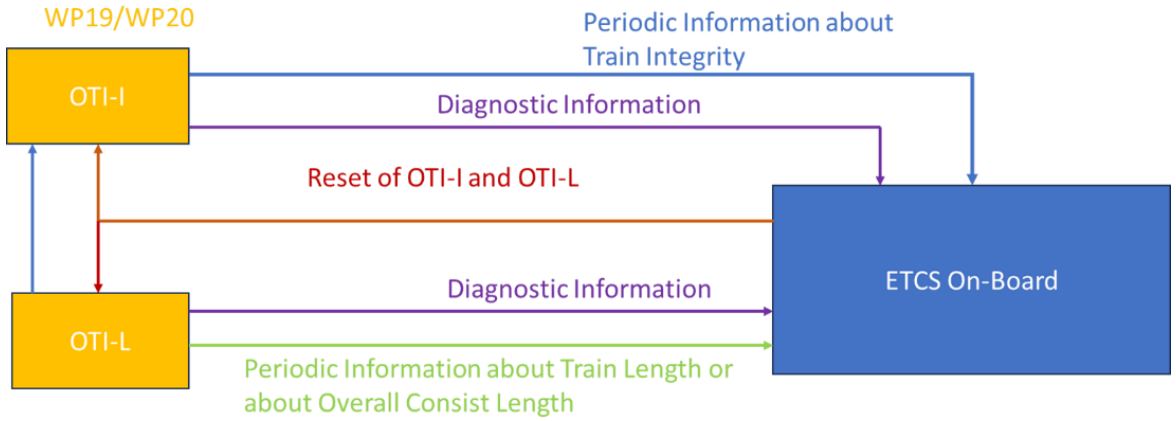

Figure 3: Functional interaction between ETCS OB and OTI-I – OTI-L

What has been created in WP19 and WP20 complies with the diagram shown in Figure 3 and depending on the potential modifications made on the EVC side, information that is not currently described in Subset-119 can also be used.

In this interface periodic information is received by EVC from OTI-I and from OTI-L. Information from OTI-L will have the same SIL level, if, for any reasons, the SIL is different from SIL4, the ETCS On-Board will have to make additional verification to fulfil the requirements for sending confirmed train length, which will be part of the on board specific implementation. The SIL level of the information provided by the OTI-I is SIL2 and for OTI-L is SIL4.

3.5 SYSTEM FUNCTIONS AND ELEMENTS

This paragraph defines the list of functions implemented in the HL3/HTD system, dividing between functions already implemented in L2-TTD that are expected to remain unmodified in comparison to what is already in operation and functions that are expected to be modified or introduced in HL3/HTD.

Functions taken from L2-TTD:

- Management of communications with on-boards
- Movement Authority management (including mode profiles OS/LS)
- Management of Most Restrictive Speed Profile
- Points management
- Level Crossing management.

Functions modified or new for HL3/HTD:

- ✓ Train occupation management (include a record of connected trains) (Modified to take into account VSSs, see § 4.1.1)
- ✓ Track status management (Modified to take into account VSSs)
- ✓ Movement Authority management for authorisation into occupied TTD sections

Regarding the Route Management, given the fact this function is currently not harmonised in Europe, the number of modifications (if any) has to be established by the specific application. In general it is expected that the rules to lock points will not change, whereas the state of occupancy of a route can be impacted or not.

3.6 SCOPE OF OPERATIONAL REQUIREMENTS INFLUENCING THE SYSTEM

In the appendix A of the Regulation [10] (TSI OPE) there are 2 rules that have a specific impact on the HL3/HTD system, regarding:

- ❖ Change of train data by ETCS external sources, as the one foreseen for the train length by the assumption [Pre 6]
- ❖ Managing a TIMS failure (in HL3/HTD the TIMS is called OTI-I)

Regarding the change of train data by ETCS external sources, the rule is here reported for clarity:

"6.4.3. Change of train data by ETCS external sources When the following text message is displayed on the DMI:

"Train data changed"

a) if the change of train data leads to an application of the brake

When at a standstill, the driver shall:

(i) acknowledge the brake application;

(ii) modify and/or validate the train data if requested by the on-board system;

(iii) take into account the modified train data.

In ETCS level 1, and in ETCS level 2 if no new MA is received, the signaller shall authorise the driver to pass the EOA (rule "Authorising the passing of an EOA" – section 6.39).

b) in all other cases

The driver shall take into account the modified train data."

The text message displayed to the driver and the eventual braking can be used for the non-harmonised procedures for Train Integrity Loss, but this procedure is outside the scope of the current specification according to the assumption [Pre 8]. This text message will not be displayed in case the specific application uses a fixed train length instead of an OTI-L device.

Regarding the management of the OTI-I (TIMS) failure, it is in principle applicable the rule defined in the clause 6.56 of the Appendix A [10], here reported:

"When the train preparer / driver of a train scheduled to run or running in an ETCS level 2 area where train integrity has to be confirmed becomes aware that the TIMS has failed, he/she shall apply rule 15 of Appendix B2. "

In HL3/HTD, the most probable interpretation of the term "the TIMS has failed" is the following one:

"A permanent failure of the OTI-I or OTI-L or of the DAC has been reported to the train preparer/driver".

Rule 15 of Appendix B2 is here reported for clarity:

15. FAILURE OF ON-BOARD EQUIPMENT

The railway undertaking shall determine the cases in which a failure of an on-board equipment affects the running of the train. The railway undertaking shall give the necessary information to the driver and/or train crew of what action to take in the case of on-board failures that affect the running of the train. If the driver becomes aware of a failure of any on-board equipment that affects the running of the train, the driver shall:

- Inform the signaller of the situation and the restrictions on the train should the train be allowed to continue its mission,
- The driver shall not commence or recommence the mission until permission to do so has been granted by the signaller,
- If the signaller gives permission for the train to start or continue its mission then the driver shall proceed in accordance with the restrictions placed upon the train,
- If the signaller does not give permission for the train to commence or recommence its mission, then the driver shall follow the instructions given by the signaller.

In general, it is recommended that in HL3/HTD, considering what it is written in the Grant Agreement (see below extract), some sort of degraded operation is allowed for trains not able to confirm their integrity or their length, without involving the driver and the dispatcher. Even with this recommendation, it is crucial, to achieve the goals of performance or cost reduction of HL3/HTD, that the OTI-I, OTI-L and DAC (if installed) have good performance, with minimal occurrence of failures.

With the introduction of HL3/HTD there is the possibility that sweeping is used, even if this operation is in principle possible also in L2-TTD. For this operation it is expected that the specific applications establish operational rules according to the safety principles applicable in each country.

Regarding the new mode Automatic Driving and Supervised Manoeuvre, introduced by the COMMISSION IMPLEMENTING REGULATION (EU) 2023/1695 of 10 August 2023, it is expected that the specific application establishes operational rules according to the safety principles applicable in each country. In particular in Supervised Manoeuvre, it has to take into account that real train integrity loss can generate lost vehicle in advance and in rear of an active cab, or even in the middle between 2 active cabs present in the same Virtual Sub-Section.

It must be noted that in the context of HL3/HTD the transition to Standby or No Power from other modes brings some operational disadvantages, if the safe consist length information is not available, because according to the current specifications the train data have to be re-validated. For this reason, it can be recommended to avoid that transition operationally as much as possible in the context of HL3/HTD, taking into account that ETCS standstill supervision (safety function) would not be active if the desk is left open (This may be mitigated with a parking brake of the train).This is of course not possible for example in case of change of direction and it may be against some goals of a specific application, like the reduction of energy consumption. So, at the end the operational rules for this matter are left to the specific application.

Regarding the following assumption, that is present in UNISIG SUBSET 120 Issue 4.0.0

2.1.7.3.2.5 In addition it is assumed that operational rules for the driver prevent to start the mission with inappropriate train length.

No operational rules for the driver are proposed in this document because the assumption is deemed invalid, as one of the goals of the use of the OTI-L and DAC is to avoid exporting this responsibility to the driver.

In some applications of HL3/HTD it is possible that the driver can see the rear end signal of a chased train (see Figure 4 for example, in some countries such taillights have been abandoned)

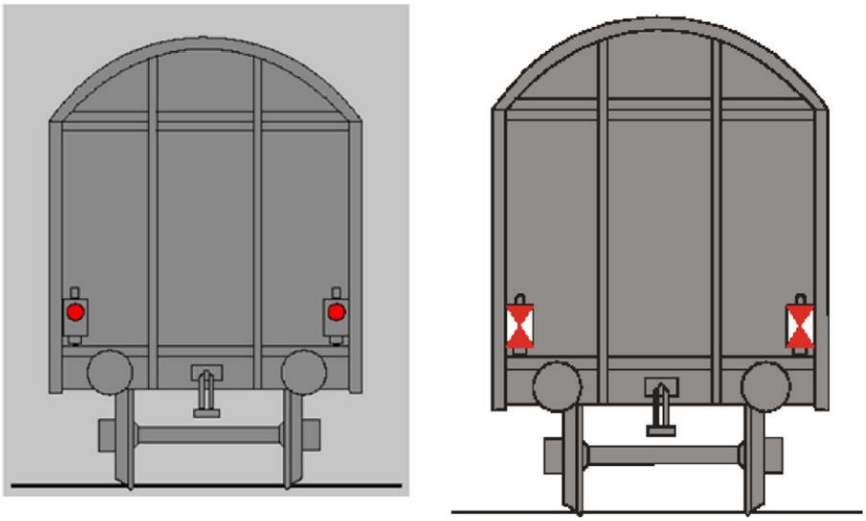

Figure 4: Example of End of Train signals.

This situation is quite rare in the current Level 2 applications, so it seems necessary that the driver is properly trained.

3.7 ASSUMPTIONS AND EXISTING SAFETY MEASURES

The assumptions applied are reported in the following table.

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 testing campaign is performed	Request for the OTI-I
[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 a year for any given train	Request for the OTI-L, not applicable if a fixed train length is used
[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. (ERA is involved in the harmonization of some procedures)	This is related to the system boundaries, harmonisation of procedures related to train integrity is outside the scope of WP15
[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 [8], 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 Trackside to release track behind the train.	From ASM-Length-1 of X2Rail-5 in deliverable D4.1 Moving Block Specification Part 2 – System Definition

Assumption	Description	Notes
[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	From X2Rail-5 in deliverable D4.1 Moving Block Specification Part 2 – System Definition
[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 connected 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 having performed a system reset. The reset can be obtained by opening or closing the driver desk, or through the reset command available in OTI systems.	Request for OTI-I and OTI-L
[Pre 14]	Each VSS will be entirely contained in a TTD. 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 or to exclude the shadow train risk at Start of Mission 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, #12C, #SM24B, #SM26A, #SM27A with joining

Table 3: Assumptions for HL3/HTD

4 HL3/HTD SYSTEM SPECIFICATION

As a direct consequence of what is described in the previous chapter 3, all the main points for the system specification are specified.

This is expressed in the following subsections:

- Main Concepts and Definitions
- Track Status Depending on The Reported Train Integrity
- Track Status in Case Of Disconnected Trains
- VSS State Machine

4.1 MAIN CONCEPTS AND DEFINITIONS

The track of a railway trackside system where HL3/HTD is implemented is divided into sections (TTDs), for which the state of free/occupied is determined, defined by a conventional trackside train detection system (e.g. track-circuits or axle-counters).

Each TTD may (in the configuration data base of ETCS trackside) be considered as split into virtual sub-sections (VSS) (see Figure 5) for which the trackside will be able to determine occupation status. This will be achieved merging reported train locations (max safe front and confirmed rear end position, reported by an integer train, i.e. a train for which proof of integrity exists on-board) and TTD information (that usually the RBC receives in real time from interlocking system - anyway these physical architecture and implementation aspects are not constraining HL3/HTD functions and are therefore not further analysed in this document).

In principle, the splitting of a TTD into more VSSs does not require neither physical actions nor installations trackside: it is entirely made through configuration of the application data of the RBC.

Note: installation of marker boards is an implementation issue for any specific application of HL3/HTD and is not further analysed in this document. Any difference with respect to placing marker boards in current level 2 ETCS applications is not expected.

Note: existing interlocking manage routes using information from train detection systems, i.e. states of TTDs. The possibility for the RBC to inform the interlocking about the state of VSSs and the corresponding balance between installation costs and operational advantages can be considered in the design of a specific application of HL3/HTD but it is not further analysed in this document.

A trackside HTD area will be entirely covered with VSSs and VSSs will not overlap each other

An example of possible combination of TTDs and VSSs is shown in Figure 5 below.

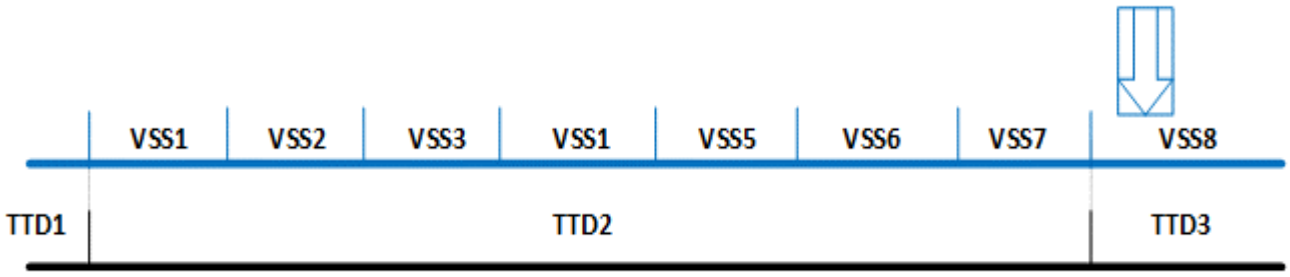

Figure 5: TTD divided into multiple VSS

In different implementations:

- few TTDs are used, track occupancy is mainly based on the train position reports; for example, TTDs are installed only around points areas, level crossings, the remaining piece of track is managed by a single long TTD;
- more TTDs can be used on existing lines already fitted to support also the migration phase when not all the on-boards will be equipped with OTI-I.

The TTDs in any kind of implementation support the HL3/HTD system to detect train movements and to improve recovery from degraded conditions.

The End of Authority can only be assigned at discrete predefined locations, e.g. the separation between TTDs and/or VSSs is based on the status of VSSs.

The state of a VSS is determined, according to the principles shown above, by the merging of information on the state of TTD in which it is contained and the information about the position of front and rear end of the trains. The merging functionality is described in detail in the following sections; a preliminary general description of operations is given in Figure 6.

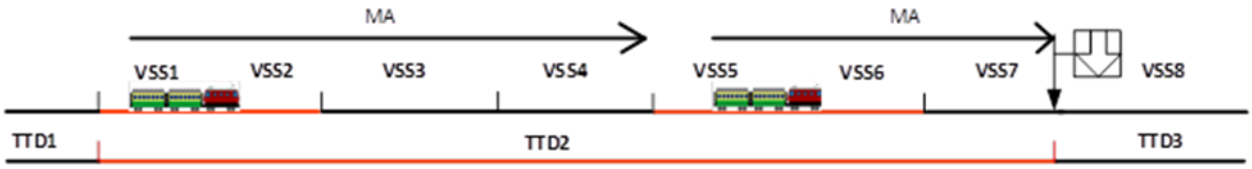

Figure 6: Occupancy of TTDs and VSSs

With reference to Figure 6 the train on the left is a chasing train, i.e. the train that is following another train at a “short” distance (“short” is relative and depends on the trackside configuration, VSS length, speed, etc.), the train on the right is the chased train, i.e. the train in advance of a chasing train, running in the same direction.

In Figure 6 is assumed that the chased train is equipped with an ETCS version that supports reporting the confirmed rear end position: this information allows the RBC to understand that, while TTD2 is reported as “occupied” by the train detection system, the safe rear end of the chased train is confirmed to be in VSS5. If the RBC has also the proof that no other train or obstacle is between the confirmed rear end of the chased train and the front end of the chasing train, the RBC is able to extend a MA in FS mode up to the border between VSS4 and VSS5.

If the chased train is not able to report a confirmed safe rear end position, the RBC will consider the whole TTD2 occupied by the chased train (i.e. it will consider all VSSs inside it in a “not free” state - see below a more precise description of VSS states).

4.1.1 Train status

The train status, in regard of the status of the capability of communicating with trackside and on the capability of safe train integrity reporting, is fundamental for the trackside function of determining the status of VSSs in the supervised area.

Note: the state of trains considered here is a “trackside view”, based on information available trackside and can be different from an “on-board view”.

In this document the following definitions apply:

- A **connected** train is a train for which an established safe radio connection with the trackside exists, and which has reported valid Train Data or Safe Consist Length to trackside and for which trackside has confirmation of active ETCS on-boards (i.e. the mute timer or radio hole timer have not expired).
- A **not connected** train is a train without an established safe radio connection to the trackside, or a train with an established safe radio connection, but without validated Train Data, or without Safe Consist Length e.g. during SoM or a train with an established radio connection but unable to send messages to RBC (i.e. the mute timer or radio hole timer have expired);
- A **complete train** is a train that has just reported "integrity confirmed".
- A **train treated as integer**: a train that is complete and for which no shadow train risk exists.
- A **non-integer** train is a train for which at least one of the conditions of non-integrity are reached (for example it has reported a new train length or there is another train inside its VSS, see below for detailed conditions).

To understand the definitions above, the following matters need to be considered:

- As far as radio connection is concerned, it must be noted that both on-board and trackside ETCS equipment will continuously be informed on the existence of a safe connection (managed by the safety layer on top of the transport connection of EURORADIO protocols). Anyway, it cannot be excluded that, even when EURORADIO reports such safe connection as "active", the ETCS functions of an on-board equipment are no more able to communicate updated train position information. For safety reason it is therefore necessary that the trackside receives messages from the ETCS on-board with a period that can be tailored according to the specific application needs. See "mute timer" below.
- Similar considerations apply for train integrity: it must be periodically reported to trackside, and for optimal engineering the periodicity of the position reports should be comparable to the frequency of the confirmation of the train integrity by OTI-L. The trackside is responsible to decide about integrity of train according to position report information and the delay to consider missing information as loss of train integrity. See "wait integrity timer" below.
- In addition, the trackside will treat a train as not integer if there is shadow train risk (see chapter 4.1.5)

Summarizing, the concept of "integrity confirmed information" in the definitions above means that usually the trackside will not treat a train as integer if one of the following events occurs (list 1):

a) the train reports "integrity lost".
b) Position Report with no integrity information is received after the "wait integrity timer" has expired.
c) the train reports changed train data with a new 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 (see [8] for the concept of propagation).
f) the delay for the propagation of the "unknown" state of the VSS in rear of the train location expires (see [8] for the concept of propagation).

In the specific context of areas operated in Supervised Manoeuvre Mode the trackside will not treat a train as integer in the following 2 conditions:

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:

- the consist reports decreased safe consist length in front of the active cab according to the consist orientation

- 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
- the VSS in advance of the consist location according to the consist orientation becomes “unknown” due to propagation
- a propagation timer of the VSS in advance of the consist location according to the consist orientation expires

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:

- the consist reports decreased safe consist length in rear of the active cab according to the consist orientation
- 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
- the VSS in rear of the consist location according to the consist orientation becomes “unknown” due to propagation
- a propagation timer of the VSS in rear of the consist location according to the consist orientation expires

To allow trackside to manage changes in connection state of a train, a “mute timer” is established trackside for each connected train:

1. Start event: Information is received from the train.
2. Stop event: The train is disconnected and can be assumed to have stopped.

The trackside considers the communication lost with the train after expiration of the mute timer.

To allow trackside to manage changes in integrity state of a train, a “wait integrity timer” is established trackside for each connected train:

1. Start event: Integrity confirmation is received from the train
2. Stop events:
   a) the train reports "integrity lost", OR
   b) the mute timer of the train expires, OR
   c) the train reports a change of train data with a new train length.

The trackside considers the train “not integer” after expiration of the wait integrity timer.

See chapter 4.2 for the requirements related to the treatment of integer and not integer trains.

As soon as the “mute timer” expires, the VSS section on which the train is located is considered as “unknown”.

When the train is considered disconnected from the trackside because the mute timer expires, the VSS sections part of the MA and on an occupied TTD, up to the first VSS which is “occupied” or "ambiguous" (both states due to another train), are set immediately to “unknown”.

Because the train can still move after the mute timer expires, the VSS on a TTD section that becomes occupied within the MA are also immediately set to “unknown”.

This is done because the train can occupy all VSS which are part of its MA.

When a train reconnects with the same train orientation after the “mute timer” has expired, the VSS sections set “unknown” when the “mute timer” expired can be restored based on the following conditions:

- The VSS sections where the train is located will become “occupied” if the train reports “integrity confirmed”, no change of train data train length was reported since the previous position report and there is no shadow train risk. If these conditions are not fulfilled, these VSS sections will become “ambiguous”.

- The VSS sections in advance of the train covered by the original MA will become “free” if the original MA is still valid on-board or can be re-issued to the train. If this condition is not fulfilled, these VSS sections will remain “unknown”.
- The VSS sections in rear of the train location become “free” if the train reports “integrity confirmed”, no change of train data train length was reported since the previous position report and there is no risk that another train had entered these sections. If these conditions are not fulfilled, these VSS sections will remain “unknown”.

Note: VSS sections in state “unknown” in rear of the train would of course also become “free” if the TTD is released.

4.1.2 Number of TTD

The number of TTD may be tailored to the needs in different implementations, considering the following considerations:

- If few TTDs are used, track occupancy is mainly based on the train position reports; for example specific TTDs can be installed only around points areas, level crossings, while the remaining parts of the line can be managed by long TTDs. This approach, which minimises the trackside costs, is efficient where the majority of trains are equipped with ETCS version that supports reporting train integrity confirmation; in this case close spacing can be achieved relying on position reports. It is an approach that may be suitable for lines with limited traffic;
- In high density nodes a larger number of TTDs can be used This approach does not permit immediate cost reductions, but supports the migration phase, where a significant amount of trains are not equipped with an ETCS version that supports reporting train integrity information.

The TTDs in any kind of implementation support the HL3/HTD system to detect train movements, to improve recovery from degraded conditions and to minimise the effect of the odometry in critical points.

4.1.3 VSS states

Besides the two states (free, occupied) which at least exist for a TTD (depending on the implementation there may be other logical states, which are however outside the scope of this document), two additional states are needed for a VSS to cover all operational situations:

- State "unknown" when there is no certainty if the VSS is “free” or not.
- State "ambiguous" when the VSS is known to be occupied by a (connected) train, but when it is unsure whether another (not connected) vehicle is located in rear of this train on the VSS on which the rear end of the connected train is located.

A VSS can therefore have four different states:

- **Free**: The trackside is certain that no train/axle is located on the VSS
- **Occupied**: The trackside has information from a position report that an integer 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 train is located
- **Unknown**: 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.
- **Ambiguous**: 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 train is located

The state of a VSS is derived from TTD occupancy information and train position reports, according to the concepts in sections 4.1.1, 4.1.4, 4.2 and 4.3, and will be considered for mitigation of hazards as specified in chapter 4.1.5 of this document.

For areas operated in Supervised Manoeuvre (limited areas in stations that can be operated in this mode in order to enhance the management of manoeuvres) the state ambiguous is substituted by the following 3 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 Authorisation This state is useful in case the operational rules for sweeping are different to the one for 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 Authorisation. 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 Authorisation (towards a free VSS) and a sweeping SM Authorisation, that can have in principle different speeds because the "normal" SM Authorisation is towards a free VSS whereas the sweeping SM Authorisation can be towards an Unknown VSS.

The separate state machine is expected to be activated when a consist is in SB mode reporting the safe consist length in the area of the station aimed at Supervised Manoeuvre operation. It shall be a consist equipped with an ETCS on-board with system version 3.0.

4.1.4 Train location

This represents the trackside view of the track currently occupied by a train, i.e. the view of the stretch of track that is currently occupied by a connected train. More precisely, the trackside view of train location can be represented as the list of VSSs on which the train is present according to the train reports (from Confirmed Rear End to Max safe front end).

The granularity of the train location is one VSS.

In the case of connected train with confirmed integrity, the list of VSSs corresponding to the trackside view of its location starts with the VSS where the front end is located and ends with the VSS where rear end is located.

For connected trains with no confirmed integrity, the trackside view of train location extends to including VSSs up to the assumed rear end. The assumed rear end will be anyway not used to clear VSSs in rear because of lack of integrity confirmation.

HL3/HTD trackside cannot have a train location of not connected trains; their possible presence and movement on the concerned lines will be managed in terms of mitigation of hazards (see chapter 4.1.5).

See chapter 4.1.1 for the principles of management of connection state and integrity state of trains.

See the state machine in chapter 4.4 for a detailed description of the management of state of VSSs in relation to state and location of trains and states of TTDs.

For every connected train the HL3/HTD system dynamically maintains a record of the train location.

The train location can be updated trackside as long as the train is connected to the trackside. As soon as the train is considered "disconnected" (see chapter 4.1.1) , the train location is stored as "memorised train location", still valid for use by trackside functions.

The train location is determined by the trackside merging information of the train position report together with the status of the TTD(s) on which the train is located.

Train position report includes:

- Estimated front end
- Confidence interval (Max Safe front end / Min safe front end)
- Confirmed train length (L_TRAININT), that can be used to deduce the position of the confirmed rear end of the train (see below the picture taken from SUBSET-026 part 3)

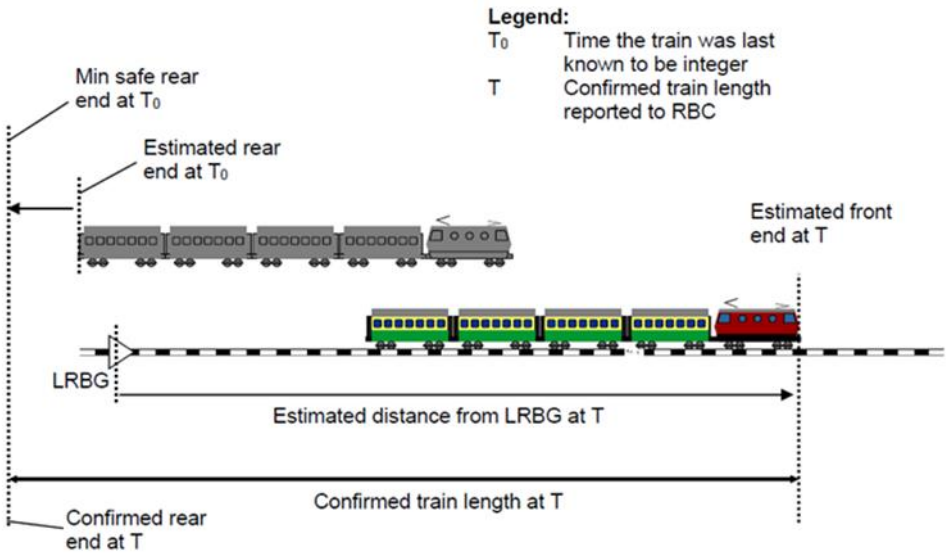

Figure 7: Calculation of Confirmed Train Length when train integrity is reported to the RBC (from SUBSET-026)

As far as front-end information is concerned, when the trackside receives the confirmation that the max safe front end of the train has entered a VSS (through position reports), 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, with the following exceptions:

- **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 is not 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 or by forbidding opposing movements on VSS limits. For TTD limits this risk does not exist (train in advance of EOA would be detected by TTD)
- **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 is not 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

Outside Supervised Manoeuvre Mode, updating the front end of the train position does not depend on the integrity status in the position report. In Supervised Manoeuvre Mode instead there is the need to consider always the value of the length of the consist in front of the active cab.

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, is still considered as part of the train location, i.e. it will still be considered occupied.

Note: In this way the relevant VSSs are only updated if a real movement in backwards direction took place.

As far as rear end information is concerned, the trackside elaboration determines the following items of the train location:

- **Established rear end**: Trackside view of the rear end of a complete train.

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. See Figure 8 below.

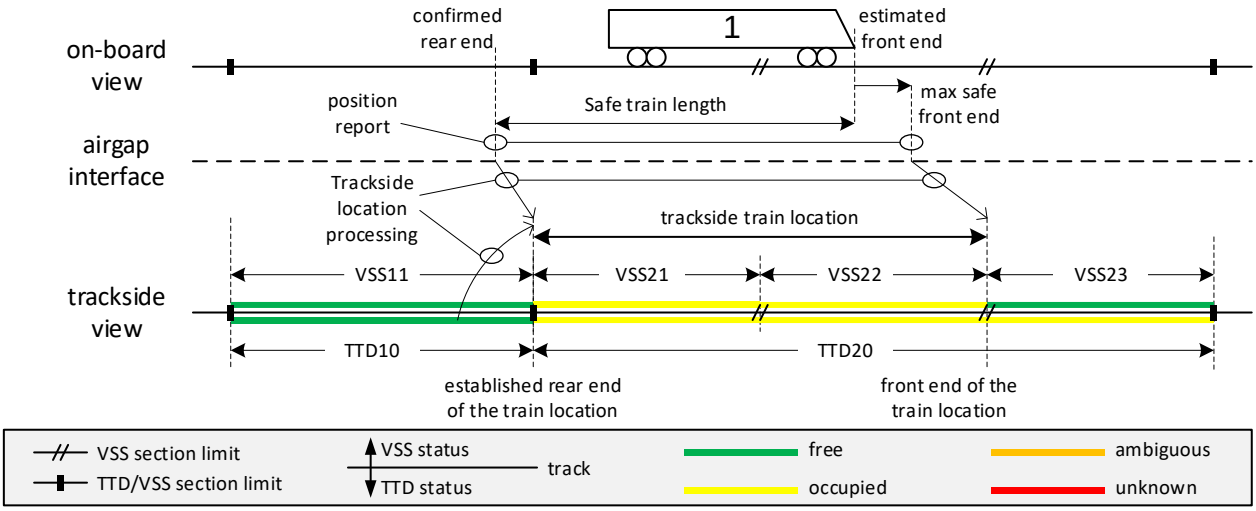

Figure 8: Definition of train rear end for a complete train.

Note: a complete train is not located anymore on a VSS and all preceding VSS (i.e. the established rear end of the train location is moved) when the trackside receives the confirmation that the rear end of the train has left a VSS

Note: It is up to the specific trackside implementation whether an integrity confirmation by driver is taken into account for updating the established rear end of the train location or not. The arguments to take driver confirmation into account or not, are outside the scope of this document.

The established rear end of the train location is never updated by position reports with the integrity status “Train integrity Lost” or “No train integrity information”.

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

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. This is to avoid losing the train location due to delayed information from position reports (“jumping train”).

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

If the established rear end of the train location has moved forward due 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 is only 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.

Note: In this way the relevant VSS are only updated if a real movement in backwards direction took place

- **Assumed rear end:** Trackside view of the rear end of a non-integer train**.**

The assumed rear end of the train location is derived from the train length in 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.

Note: since there is no positive confirmation of its location, the position of the rear end of the train location can only be assumed. See picture below:

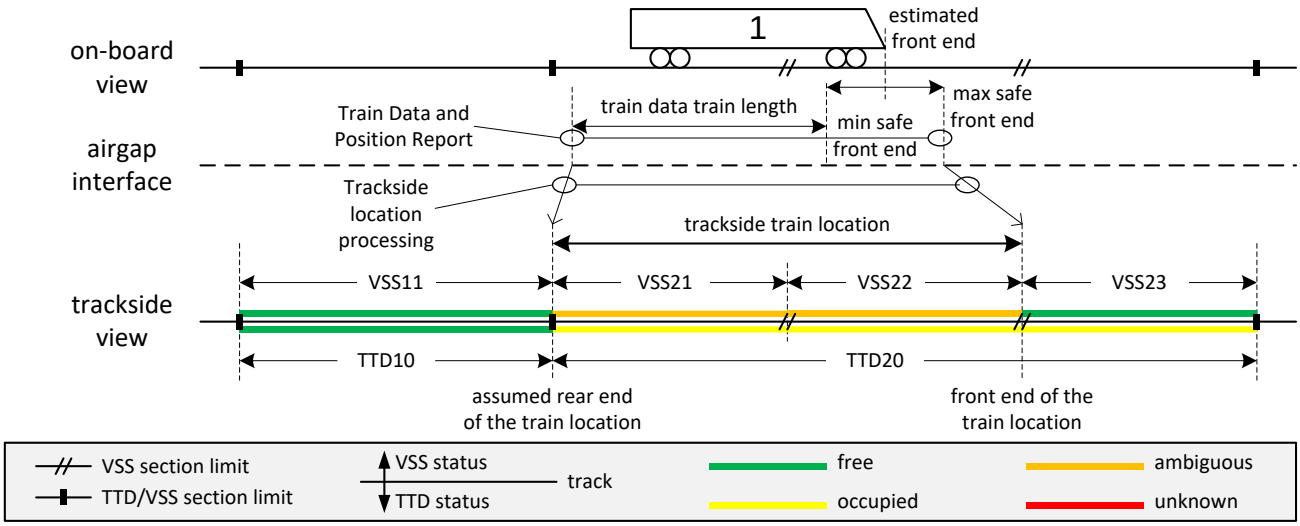

Figure 9: Definition of train rear end for no integer train.

The train unable to confirm its integrity is not located anymore on a VSS and all preceding VSS (i.e. the assumed rear end of the train location is moved) when the trackside receives by position reports the information that the assumed rear end of the train has left a VSS. Since the assumed rear end of the train location is only "assumed" it can never be used to clear a VSS in rear. Therefore, the VSS that was left by the assumed rear end of the train is not set to "free", but to “unknown”. See state machine in chapter 4.4 for an exhaustive analysis of VSS state changes.

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. This is to avoid losing the train location due to delayed PTD information (“jumping train”).

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

If the assumed rear end of the train location has moved forward due 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 is only 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.

Note: In this way the relevant VSS are only updated if a real movement in backwards direction took place

A VSS where the assumed rear end of a train is located will be in state “Ambiguous”.

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 (see following section 4.2), the train location is based on the assumed rear end, not anymore on the established rear end.

4.1.5 Main hazards of the HL3/HTD system

The HL3/HTD concept relies on the information both from the TTDs and from the position reports to know at all times the position of the trains that are in operation in the line and their integrity. When the integrity of the train is confirmed and there is no shadow train risk, the information from the position reports can be used to set a Virtual Sub Section to free in alternative to the information from the corresponding TTD. In some situations, there can be some lack of information that can be summarized in the following way:

- Unintentional train integrity loss;

Not without trackside train detection, the HL3/HTD concept relies on the condition that the trackside always knows the position and integrity status of each train or vehicle that is present in the area under its control. The problem is that in practice this condition cannot always be fulfilled. when there is no connection, a train is not visible anymore for the trackside, e.g. the on-board enters shunting mode, is switched off intentionally (NP mode) or loses the radio connection. Even if the trackside remembers the last reported position of the train and the area in which the train was authorised to move, there is no guarantee that the train will stay within this area. There could be reasons to move the train under the supervision of operational procedures. The train could also move without any authorisation. Without trackside train detection, there is no way for the trackside to know the location of such a train in a sufficiently reliable way.

In case of switching on/off the trackside system (intentional restart or due to crash) it would have no knowledge at all of the trains in its area. Recovering from this situation would be cumbersome (sweeping of the whole trackside system area) and could require a long time.

- For all these considerations the risk of not known / not detected vehicles has to be considered by the HL3/HTD system. These vehicles are defined as:
    - **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;
    - **shadow train**: it is a ghost train that is chasing a train operating normally in the HL3/HTD area;

Due to the un-synchronicity of the train position report and the TTD status a weird operational effect can be presented to the signaller interface, known as:

- **jumping train**: A train which does not report its position on every block, due to the discrete intervals in which position reports are sent and/or time delays in the trackside train detection.

More details on the safety analysis are present in the dedicated deliverable D15.2.

4.2 TRACK STATUS DEPENDING ON THE REPORTED TRAIN INTEGRITY

The status of the VSS affects the train separation function and the train movement authorisation. In order to provide this functionality in a safe way, the trackside system determines the status of the virtual sub-sections (VSS) based on the information received from the trains about their position and integrity. The trackside will consider a train as integer as long as the train is reporting confirmed integrity and there is no shadow train risk (including the event of reporting “no integrity information available” after having reported “confirmed integrity”), and none of the events reported in 4.1.1 (list 1).

Based on the status of the train integrity reported to the trackside system, the track status will be determined in the following manner:

- **Integrity confirmed**: If a train fulfils the conditions for being treated as integer by the trackside, the trackside system sets the VSS where the train is located to "occupied" if it was previously free. The trackside system also uses the confirmed train length and the estimated front end of the train to calculate the established rear end of the train location (and TTD status when entering in the following TTD) and update it, considering the conditions of update the established rear end dealing with "jumping train" and delays in the TTD. The VSS in rear of the established rear end are set to "free" if they were previously "occupied".
- **Integrity lost**: If a train reports its position with train integrity lost, the trackside system does not treat the train as integer and sets the VSS where the train is located to "ambiguous". The trackside system starts an integrity loss propagation timer for the VSS where the train has reported the train integrity lost. The trackside system also uses the train data train length and the minimum safe front end of the train to calculate the assumed rear end of the train location. The VSS in rear of the initial assumed rear end is set to "unknown" when the integrity loss propagation timer expires and the TTD keeps being occupied, not being that VSS part of an MA of another train or in "occupied" or "ambiguous" states. When the train leaves the current "ambiguous" VSS with the assumed rear end, the status of that VSS is set to "unknown".
- **No integrity information**: If a train reports its position without integrity information after having reported confirmed integrity, the trackside system keeps treating the train as integer while none of the events to change the trackside integrity status occurs. As such, the VSS statuses are set as in the case with integrity confirmed, with the particularity that the established rear end is not updated with the reported rear end. If a condition to consider the train as not integer takes place, the trackside does not treat the train as integer and the VSS statuses are set as in the case with integrity lost.

4.3 TRACK STATUS IN CASE OF DISCONNECTED TRAINS

A train is considered disconnected from the trackside when there is no established safe radio connection, e.g. after an End of Mission or communication failure takes place, or with an established safe radio connection but without valid train data, e.g. Start of Mission, and when the dedicated timer to supervise the train connection with the trackside expires (mute timer or the radio hole timer).

When a train is considered disconnected from the trackside, the VSS sections on which the train is located, or which are part of its MA (in case an MA has been sent previously to the train) are set to "unknown" to indicate that a not-connected vehicle can be present on these VSS. The state "unknown" is propagated (by means of a disconnection propagation timer) to adjacent VSS until a free TTD or a VSS with a connected train is reached.

The TTD occupancy information is used to detect ghost trains and shadow trains, which are potential hazards for the train separation function.

When a train reconnects to the trackside after a disconnection, the track status can be recovered by using PTD information from the reconnecting train or from a sweeping train. The VSS sections occupied by the reconnecting train or by a sweeping train are set to "occupied" or "free" depending on the integrity status of the train. The reconnection can be:

- **In Start of Mission:** After the train reports valid train data and valid position with train integrity, the status of VSS occupied by the train is changed from "unknown" to "ambiguous". The status of VSS occupied by the train can change to "occupied" when there is no shadow train risk.

- **Reconnection after mute timer expiration:** If the train reconnects with the same train orientation and length, the VSS sections set “unknown” can be restored to the following VSS status based on the following conditions:
    - “Occupied”: In the VSS sections where the train is located if the train reports integrity confirmed, and no change of train data train length was reported since the previous position report and there is no shadow train risk.
    - “Ambiguous”: In the VSS sections where the train is located if the conditions for “occupied” above are not fulfilled.
    - “Free”: In the VSS sections in advance of the train covered by the original MA if the original MA is still valid on-board or can be re-issued to the train. In the VSS sections in rear of the train location if the train reports “integrity confirmed”, no change of train data train length was reported since the previous position report and there is no risk that another train had entered these sections, and regardless of this, if the TTD covering those sections is released.

The VSS sections referenced in the “free” conditions above will remain in “unknown” status if those conditions are not fulfilled.

In case a sweeping procedure based on an integer train is used to clear the “unknown” sections, when the train enters in a VSS with “unknown” status with an authorisation, the VSS becomes “occupied” if there is no shadow train risk and becomes “free” when that integer train exits that VSS in the same direction as when it entered. In the event of a failure in the TTD that makes its status as permanently occupied, some mitigations shall be put in force due to the fact that all the VSS become free after sweeping.

4.4 VSS State Machine

In this session there are two paragraphs, one for the state machine for online operations and one specifically for Supervised Manoeuvre.

4.4.1 VSS State Machine

The state machine of each VSS shown in Figure 10 is coming from [8].

The transitions to identify the VSS states are shown in the following Table 4. Each transition is identified with a code which is then used in the document. The sub-conditions (e.g. #1A, #1B) are always combined with a logical OR to give the result for the main condition, e.g. #4 = #4A OR #4B. Compared to document [8], some clarifications and additions have been made, these are indicated in the collum Notes.

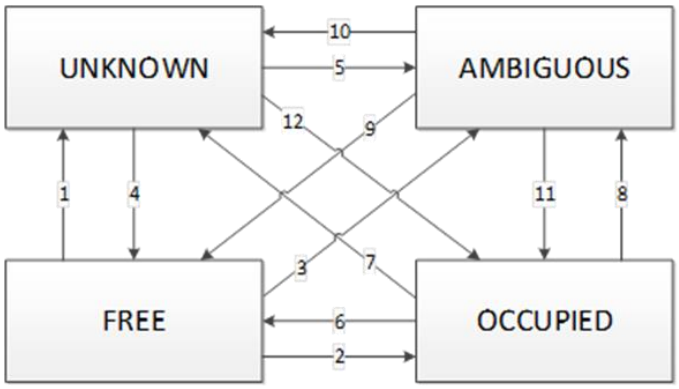

Figure 10: VSS section state diagram.

IN THE FOLLOWING TABLE

A= AMBIGUOUS

F = FREE

O = OCCUPIED
U = UNKNOWN

#	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 [8], 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 for which the mute timer or the Radio Hole Timer is expired) 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 [8] with the addition of the case of the Radio Hole Timer (see related use cases in § 8.8).
#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 [8]
#1D 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 VSS for which the “disconnect propagation timer” is expired) AND (the evaluated VSS is not located on the same TTD as the VSS for which the timer is expired) AND (the evaluated VSS is not part of an MA)		This transition is identical to the one in the HTD Principles [8]

#	Condition	Priority over	Notes
#1E 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)		This transition is identical to the one in the HTD Principles [8]
#1F 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 VSS for which the “integrity loss propagation timer” is expired) AND (the evaluated VSS is not located on the same TTD as the VSS for which the timer is expired) AND (the evaluated VSS is not part of an MA)		This transition is identical to the one in the HTD Principles [8]
#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 [8]
#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 [8]
#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 [8]

#	Condition	Priority over	Notes
#4A U>F	(TTD is free)		This transition is identical to the one in the HTD Principles [8]
#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 [8], 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 ADD_0009 and ADD_0024)		This is an additional optional transition in addition to the HTD Principles [8]. 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 ADD_0009 and ADD_0024) 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 [8]
#5A U>A	(train is located on the evaluated VSS)		This transition is identical to the one in the HTD Principles [8].
#6A O>F	(TTD is free)		This transition is identical to the one in the HTD Principles [8]
#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 [8]

#	Condition	Priority over	Notes
#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 [8] with the addition of the case of the Radio Hole Timer (see related use cases in § 8.8). If the optional functionality of assignment of train length to VSS sections is used, if the conditions described in the requirement ADD_0009 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 [8]
#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 [8] 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 [8] is in advance of the evaluated VSS)		This transition is identical to the one in the HTD Principles [8]
#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 [8]
#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 [8]

#	Condition	Priority over	Notes
#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
#12A U>O	(train reconnects with the same train orientation) AND (VSS where the train was located when the connection was lost, was “occupied”) AND (train treated as integer) AND (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) AND (train is located on the evaluated VSS) AND (the MA sent to this train is still valid)	#5	This transition is slightly different from the one in the HTD Principles [8] because in the fourth condition a “free” TTD is considered. The requirement ADD_0019 mitigates a possible hazardous scenario with ghost trains, see D15.2 for more details
#12B 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”) AND (VSS where the train was located before it was located on the evaluated VSS, is in rear of the train) AND (the train is not re-connecting, i.e. the mute timer was not expired) AND (train treated as integer)	#5	This transition is identical to the one in the HTD Principles [8].

Table 4: Transition between states for VSS sections

4.4.2 VSS state machine for Supervised Manoeuvre

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 proposed, it is expected to be activated when the first train reports Supervised Manoeuvre Mode in those areas. It 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 11, 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.

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.

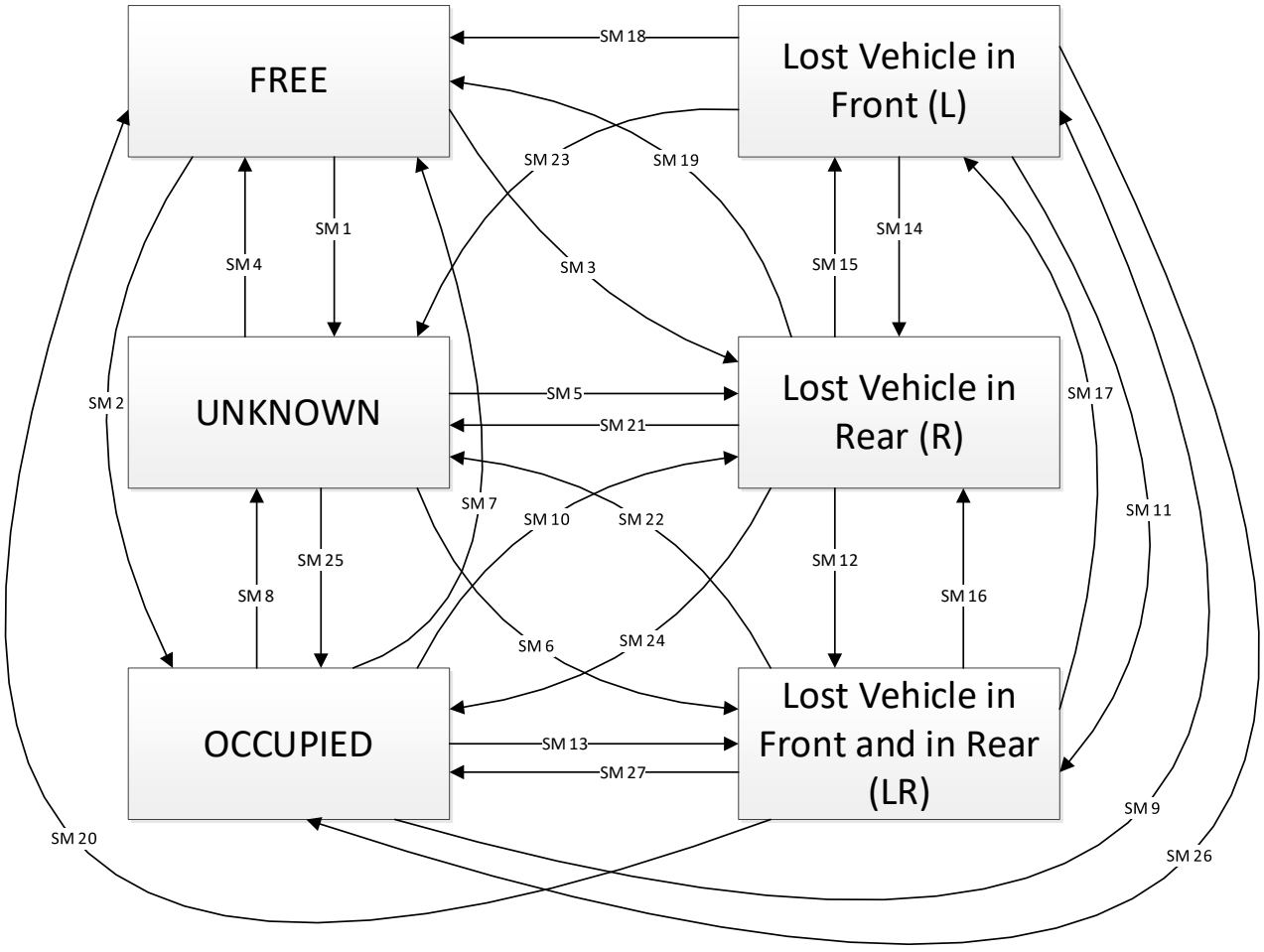

Figure 11: VSS section state diagram for SM

The state machine will be thoroughly reviewed in the specific applications that want to use this mode, some details, like the way to combine the lengths for the transitions #SM24B, #SM26A and #SM27A, are intentionally left open.

IN THE FOLLOWING TABLE

F = FREE
L = LOST VEHICLE IN FRONT
LR = LOST VEHICLE IN FRONT AND IN REAR
O = OCCUPIED
R = LOST VEHICLE IN REAR
U = UNKNOWN

#	Condition	Priority over	Notes
#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)		
#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)		

#	Condition	Priority over	Notes
#SM1D 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 VSS for which the “disconnect propagation timer” is expired) AND (the evaluated VSS is not 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
#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)		
#SM1F 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 VSS for which the “integrity loss propagation timer” is expired) AND (the evaluated VSS is not 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
#SM1G 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)		

#	Condition	Priority over	Notes
#SM2A 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”)		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	(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 Front of the Consist”) AND (the train entered the evaluated VSS according to the direction of the SM MA used for sweeping)		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.
#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)		

#	Condition	Priority over	Notes
#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.
#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 [8]
#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 [8]
#SM8A O>U	((mute timer expires) OR (communication session is being terminated)) AND (the evaluated VSS becomes part of the memorised train location)	#8	This transition is identical to the one in the HTD Principles [8]. 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.
#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)		
#SM10A 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)		
#SM11A L>LR	There can be a lost vehicle or a reporting cab in front of the consists in the evaluated VSS		
#SM12A R>LR	There can be a lost vehicle or a reporting cab in front of the consists in the evaluated VSS		

#	Condition	Priority over	Notes
#SM13AO>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
#SM14AL>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
#SM15AR>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
#SM16ALR>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
#SM17ALR>L	All the consists present in the evaluated VSS can have lost vehicles or reporting cabs only in front		
#SM18AL>F	(TTD is free)		
#SM18BL>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
#SM19AR>F	(TTD is free)		
#SM20ALR>F	(TTD is free)		
#SM21AR>U	(the evaluated VSS is left by all reporting trains in the direction of the MA)		
#SM21BR>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.
#SM22ALR>U	(the evaluated VSS is left by all reporting trains in the direction of the MA)		

#	Condition	Priority over	Notes
#SM22B 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 [8]. 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.
#SM23A L>U	(the evaluated VSS is left by all reporting trains in the direction opposite to the MA)		
#SM23B 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 [8]. 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.
#SM24A 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)		
#SM24B 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

#	Condition	Priority over	Notes
#SM25A 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)		
#SM26A 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
#SM27A 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 5: State Machine for Supervision Manoeuvre

5 OVERVIEW ON HL3/HTD USE CASES

This chapter reports an overview of the use cases. All the use cases produced are reported in the chapter 8.

This chapter is organized as follows, an introductory part where all the possible families of use cases described in the document are listed and the description of the prototype to be adopted for each use case and a paragraph which contains a subparagraph for each group of use cases. In this way reading and possible research of topics of interest should be facilitated.

5.1 GENERAL ASPECTS

The use case groups present in the table are the use case group developed in this document.

# UC group	Use Cases Group
1.	End of Mission / Start of Mission
2.	Handover
3.	Joining
4.	Level Transitions
5.	Loss of Communications
6.	Loss of Integrity
7.	Movement in Staff Responsible
8.	Radio Holes
9.	Release of Points
10.	Reversing
11.	Shunting
12.	Splitting
13.	Sweeping
14.	Trackside Initialisation
15.	Use of Reserved
16.	Interaction between HL3/HTD and ATO
17.	Use of Train Position Parameters to manage particular situations
18.	Supervised Manoeuvre
19.	Coexistence of HL3/HTD and NTC

Table 6: List of Use Cases

Each use case is described according to the following format, **USE CASE Prototype:**

Use Case Group	Note: Recommendation to have in advance numbered list of all UC groups to be defined. See Table 6 above
Use Case	Note: Name should refer to the main goal of the UC.
UC ID	UC_XX_YY Note: ID of each UC should be unique. (XX=number of UC group, YY=number of specific UC) Example: UC_01_04 (01 = ”End of mission/Start of mission”, 04 = ”Check Status”) Note: Numbering of UC groups (XX) is defined in advance. Numbering of aspecific UC (YY) is in charge of the partner responsible for the specific UC.
Main actor	The actor that initiates the Use Case
Other actors	List of all actors that play any role during UC scenario in any event of the UC. Note: Recommendation to have in advance list of all possible actors to be used (e.g. EVC, dispatcher, RBC, etc.).
Main goal	Description of the UC main goal – what operational scenario (concept) is provided. Note: It is not easy to define all possible operational scenarios, but at least for those which are already defined there should exist some relationship between them to help a reader better understand the operational context.
Assumptions	List of indicated generic assumptions which are needed for performing the UC in an intended way (e.g. some system or interface is not available yet).
Precondition	Defines all conditions that have to be fulfilled before the UC is started. Example: “specific system is switched on, specific environment condition is available”.
Flow of events	Numbered sequence of UC scenario events (step by step from the start of the UC to its successful end) – “what shall happen to fulfil UC goal”. Note: Proposal: In first stage to write UC’s in “sunny day” way – it means that the goal of the UC will be achieved successfully without any disruption. Note: Alternative scenarios (e.g. some event is not executed properly) could be managed in later stages as an extension. Note: Recommendation to describe all events on the same level of detail. Proposal: Not to be too much specific. Operational scenario should be described, not a technical solution (system here is more like a black box which performs some action and interacts with other systems or operational environment). Example of the event sequence: First (initial) event (Main actor initiates something) Second event XY event … Final event (after the last event is done, the main goal of the UC is successfully fulfilled) Note: Proposal: Number of events should not exceed approximately 10 events.

Postcondition	Defines all conditions that must be fulfilled when the UC is successfully completed or the condition where we go in failed case.
Safety relation	Defines, if any event in the use case has any relation to safety and a function performed by an actor is supposed to be safety relevant.
Open topics / consideration	Whatever you find interesting to note which has already not been written above.

Table 7: Use Case prototype

5.2 DESCRIPTION OF THE HL3/HTD USE CASES

This paragraph lists all the use cases developed and for each of these there is a brief description. All use cases are reported in the chapter 8.

UC Group	End of Mission / Start of Mission	
UC ID	**Use Case**	**Main goal**
UC_01_01	End of Mission with train integrity confirmed after standstill	Describes what happens to the track status at End of Mission when Train Integrity has been confirmed after the train has reached standstill..
UC_01_02	End of Mission without train integrity confirmed after standstill	Describes what happens to the track status at End of Mission when Train Integrity has NOT been confirmed after the train has reached standstill.
UC_01_03	Start of Mission with valid position - Trackside provides a FS MA.	Describes the steps taken and the changes to the track status during the Start of Mission procedure when the position of the train is still known by the ETCS On-board and the HL3/HTD Trackside is able to recover the Unknown area created at End of Mission
UC_01_04	Start of Mission with invalid position	Describes the steps taken during the Start of Mission procedure when the position of the train is invalid
UC_01_05	Start of Mission with unknown position	Describes the steps taken during the Start of Mission procedure when the position of the train is unknown.
UC_01_06	EoM-SoM Train receives FS MA after SoM and frees VSSs	Train receives FS MA after SoM and Train frees VSSs after SoM
UC_01_07	Start of Mission with valid position – exclusion of the presence of shadow trains	Describes the steps taken and the changes to the track status during the Start of Mission procedure when the position of the train is valid and there is no shadow train risk

Table 8: UC for End of Mission / Start of Mission

UC Group	Handover	
UC ID	**Use Case**	**Main goal**
UC_02_01	Nominal Handover without interface for communication of the state of the VSSs	HL3/HTD Trackside authorises a train running in FS, reporting frequently its position with Train Integrity confirmed, to travel towards a Handover border. Train is able to handle two communication sessions. When the MA reaches the Handover border, Handing Over RBC starts Handover and Accepting RBC sends information to the Handing Over RBC for the train to go beyond the Handover border. Handing Over RBC sends an MA beyond the Handover border. Train passes the Handover border and Accepting RBC takes over the responsibility of the train. Handing Over RBC orders the train to terminate communication session after receiving a position report with the CRE beyond the Handover border.
UC_02_02	Loss of Connection between Handing Over RBC and Accepting RBC	HL3/HTD Trackside authorises a train running in FS, reporting frequently its position with Train Integrity confirmed, to travel towards a Handover border. Train is able to handle two communication sessions. When the MA reaches the Handover border, Handing Over RBC starts Handover and Accepting RBC sends information to the Handing Over RBC for the train to go beyond the Handover border. Handing Over RBC sends an MA beyond the Handover border. There is a loss of connection between the 2 RBCs and there is a shortening of the movement authority to the Handover border.
UC_02_03	Handover with only one communication session	HL3/HTD Trackside authorises a train running in FS, reporting frequently its position with Train Integrity confirmed, to travel towards a Handover border. Train is able to handle one communication session. When the MA reaches the Handover border, Handing Over RBC starts Handover and Accepting RBC sends information to the Handing Over RBC for the train to go beyond the Handover border. Handing Over RBC sends an MA beyond the Handover border. Train passes the Handover border and Accepting RBC takes over the responsibility of the train. Handing Over RBC orders the train to terminate communication session after receiving a position report with the CRE beyond the Handover border.
UC_02_04	Train Integrity Loss during Handover	HL3/HTD Trackside authorises a train running in FS, reporting frequently its position with Train Integrity confirmed, to travel towards a Handover border. Train is able to handle two communication sessions. When the MA reaches the Handover border, Handing Over RBC starts Handover and Accepting RBC sends information to the Handing Over RBC for the train to go beyond the Handover border. Handing Over RBC sends an MA beyond the Handover border. Train reports having lost its integrity the Handover is cancelled and the situation is managed by operational procedures for train integrity loss.

Table 9: UC for Handover

UC Group	Joining	
UC ID	**Use Case**	**Main goal**
UC_03_01	Train Joint another one	Two trains to be joining and new train ready to start.

Table 10: UC for Joining

UC Group	Level Transitions	
UC ID	**Use Case**	**Main goal**
UC_04_01	Leaving HL3/HTD Area	Level transition from HL3/HTD to another Level.
UC_04_02	Entering HL3/HTD Area	Level transition to HL3/HTD from another Level.

Table 11: UC for Level Transitions

UC Group	Loss of Communications	
UC ID	**Use Case**	**Main goal**
UC_05_01	Loss of Communication without re-connection	Train is at standstill and located in the area of the last granted MA. The VSSs of the TTDs where train could be located are set to Unknown to protect the train against movements of other trains in FS (safe situation).

Table 12: UC for Loss of Communications

UC Group	Loss of Integrity	
UC ID	**Use Case**	**Main goal**
UC_06_01	Loss of Train Integrity during Normal Movement	Recovering Normal Movement of train after loss of train Integrity during Normal Movement
UC_06_02	EoM after Loss of Train Integrity	Manage the EoM of train after loss of Train Integrity
UC_06_03	Train does not confirm Integrity – Wait Integrity timer expires	Manage the expiration of Integrity wait timer without Integrity confirmation from train.

Table 13: UC for Loss of Integrity

UC Group	**Movement in** Staff Responsible	
UC ID	**Use Case**	**Main goal**
UC_07_01	Movement in Staff Responsible with SR authorisation	Staff Responsible (SR) mode is the primary means of moving communicating trains without a Train Location or communicating trains with Train Location when, for some reason, it is not possible to issue an MA.

Table 14: UC for

Movement in Staff Responsible

UC Group	Radio Holes	
UC ID	**Use Case**	**Main goal**
UC_08_01	Train passes through Radio Hole within expected time	Normal Movement through Radio Hole without an impact on following trains
UC_08_02	Train passes through Radio Hole longer than expected time	Radio Hole timer expires and the VSS status is changed accordingly

Table 15: UC for Radio Holes

UC Group	Release of Points	
UC ID	**Use Case**	**Main goal**
UC_09_01	Release of points without dedicated TTDs	The train overpass a point area, using the Confirmed Rear End to set the VSS, where the point is located, to free.
UC_09_02	Release of points without dedicated TTDs (Loss of connection)	The train overpass a point area, using the Confirmed Rear End to set the VSS, where the point is located, to free.
UC_09_03	Release of points with dedicated TTDs	The train overpass a point area, using the Confirmed Rear End to set the VSS, where the point is located, to free.

Table 16: UC for Release of Points

UC Group	Reversing	
UC ID	**Use Case**	**Main goal**
UC_10_01	Reversing in HL3/HTD Area	The train performs Reversing in order to escape a danger situation

Table 17: UC for Reversing

UC Group	Shunting	
UC ID	**Use Case**	**Main goal**
UC_11_01	Train enters an active Shunting Area and changes to SH mode	HL3/HTD Trackside authorises a train to enter an active Shunting Area in OS mode. When the train is located inside the active Shunting Area, Driver selects Shunting and HL3/HTD Trackside sends SH authorisation to the train. Train changes to SH mode and ends its mission.
UC_11_02	Temporary Shunting Area activated	HL3/HTD Trackside authorises a train to enter a temporary Shunting Area in OS mode. When the train is located inside the active Shunting Area, Train changes to SH mode and ends its mission.

UC_11_03	Train leaves an active Shunting Area with MA	A train is at standstill at a location close to the border of an active Shunting Area, following completion of movements in SH mode. The Driver performs SoM and the train receives an MA to leave the active Shunting Area.
UC_11_04	Temporary Shunting Area deactivated	Performs the shunting and deactivates the temporary Shunting Area

Table 18: UC for Shunting

UC Group	**Splitting**	
UC ID	**Use Case**	**Main goal**
UC_12_01	Splitting of a train with integrity confirmed Alternative 1	A train splits and there are two resulting trains. “Train 2” resulting from splitting remains not connected to trackside “Train 1” can start a new mission
UC_12_02	Splitting of a train with integrity confirmed Alternative 2	A train splits and there are two resulting trains. Boths Trains resulting from splitting can start a new mission

Table 19: UC for Splitting

UC Group	Sweeping	
UC ID	**Use Case**	**Main goal**
UC_13_01	Nominal Sweeping	HL3/HTD Trackside authorises a train to enter a VSS section in “unknown” status in order to bring this section to the state “occupied” and resume the normal operation of HL3/HTD Specific Application.
UC_13_02	Sweeping with MA and expiration of the disconnect/integrity loss propagation timer	HL3/HTD Trackside authorises a train to enter a VSS section in “unknown” status in order to bring this section to the state “occupied” and resume the normal operation of HL3/HTD Specific Application. With MA and expiration of the disconnect/integrity loss propagation timer
UC_13_03	Sweeping with SR Authorisation and expiration of the disconnect/integrity loss propagation timer	HL3/HTD Trackside authorises a train to enter a VSS section in “unknown” status in order to bring this section to the state “occupied” and resume the normal operation of HL3/HTD Specific Application
UC_13_04	Sweeping with expiration of the ghost train propagation timer and detection at the TTD border	HL3/HTD Trackside authorises a train to enter a VSS section in “unknown” status in order to bring this section to the state “occupied” and resume the normal operation of HL3/HTD Specific Application. With expiration of the ghost train propagation timer and detection at the TTD border.
UC_13_05	Sweeping with expiration of the ghost train propagation timer and no detection at the TTD border	HL3/HTD Trackside authorises a train to enter a VSS section in “unknown” status in order to bring this section to the state “occupied” and resume the normal operation of HL3/HTD Specific Application. With expiration of the ghost train propagation timer and no detection at the TTD border.

Table 20: UC for

Sweeping

UC Group	Trackside Initialisation	
UC ID	Use Case	Main goal
UC_14_01	Initialisation with Track Circuits TTDs	After a shutdown the HL3/HTD shall resume normal operation

Table 21:UC for Trackside Initialisation

UC Group	Interaction between HL3/HTD and ATO	
UC ID	Use Case	Main goal
UC_16_01	Use of ATO to set a TTD to free	Setting a TTD to free for the particular uses connected to HL3/HTD (for example to trigger the transition #11A or to check if a TTD is not failed i.e. it is not able anymore to make the transition from occupied to free)

Table 22: UC for Interaction between HL3/HTD and ATO

UC Group	Use of Train Position Parameters to manage particular situations	
UC ID	Use Case	Main goal
UC_17_01	Selection of the appropriate position report parameters according to the length of the train reported as train data	On the basis of the information reported by the train, in particular the train length, it is possible to select the adequate position report parameters in order to maximize the performance
UC_17_02	Selection of the appropriate position report parameters to facilitate the transition from ambiguous to occupied	If a VSS is in the ambiguous state, the position report parameters may be dynamically changed by the HL3/HTD Trackside in order to facilitate the transition to occupied when the train overpasses the TTD boundary

Table 23: UC for Use of Train Position Parameters to manage particular situations

UC Group	Supervised Manoeuvre	
UC ID	Use Case	Main goal
UC_18_01	Joining in Supervised Manoeuvre	Joining is performed in Supervised Manoeuvre without loss of the connection
UC_18_02	Start of Mission in Supervised Manoeuvre	Start of Mission is performed and the VSS can be set to occupied after a sweeping procedure

Table 24: UC for Supervised Manoeuvre

UC Group	Coexistence of HL3/HTD and NTC	
UC ID	Use Case	Main goal

UC_19_01	Ghost train propagation timer generated by LNTC train	Allowing the circulation of LNTC trains in HL3/HTD area

Table 25: UC for Coexistence of HL3/HTD and NTC

6 ADDITIONAL HL3/HTD REQUIREMENTS

This chapter contains the reference additional functional requirements, in comparison to the ones already defined in the HTD Specification (see § 9). The requirements contained in this chapter are the result of the work done in previous projects together with the consolidation activities of the same.

6.1 GENERAL REQUIREMENTS

General Requirements	
IND	**Description**
ADD_0001	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.
ADD_0002	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 5.2.1.8 of the HTD Principles [8] or using particular rules for the closure of level crossings.
ADD_0003	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).
ADD_0004	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.
ADD_0005	A "wait integrity timer" is assigned to each train with an established safe radio connection
ADD_0006	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 and integrity loss propagation timer or the sum of mute timer and disconnect propagation timer or the radio hole timer)
ADD_0007	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.

General Requirements	
IND	**Description**
ADD_0008	Each specific application shall indicate to the driver the appropriate way to react to the System status message “Train data changed”.
ADD_0009	When there is the transition #7A, if the train length according to the requirement ADD_0021 is available and there was only one VSS in the state occupied in the associated TTD, 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
ADD_0010	Each specific application shall calculate an appropriate safe rear margin to be added at the rear of the CRE according to their rules (e.g. value of D_NVROLL, distance between axles and front ends) in order to avoid collisions.
ADD_0011	When a train reports Reversing Mode, the VSSs where the train is located are set to ambiguous and the train is not treated as integer anymore by trackside.
ADD_0012	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
ADD_0013	The operational procedures for the recovery of a failed train have to be established by the Specific Application
ADD_0014	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)
ADD_0015	The HL3/HTD shall not send a FS MA with an EoA that is in rear of the max safe front end of the train
ADD_0016	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

General Requirements	
IND	**Description**
ADD_0017	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.
ADD_0018	When a VSS becomes free, the train length monitoring timer shall be considered immediately expired and the requirement ADD_0022 shall be applied
ADD_0019	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.
ADD_0020	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.
ADD_0021	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 ADD_0009. 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 ADD_0009, this is ensured by the transition #2A, #11A and #12A with a FS MA.
ADD_0022	When the train length monitoring timer expires, all the information stored according to the requirement ADD_0009 shall be deleted.

General Requirements	
IND	**Description**
ADD_0023	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 ADD_0022 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 ADD_0009 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;
ADD_0024	When a SoM Position Report is received from a train that is inside a VSS with stored data according to the requirements ADD_0009 and ADD_0023, 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 ADD_0022 shall be applied immediately.
ADD_0025	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 ADD_0009 and ADD_0023, the trackside shall check if the Validated Train Data corresponds to the stored data according to the requirements ADD_0009 and ADD_0023. If not, the train length monitoring timer shall be considered expired and the requirement ADD_0022 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
ADD_0026	If the checks described in the requirement ADD_0025 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
ADD_0027	The wait first integrity confirmation timer is assigned to every VSS with stored data according to the requirements ADD_0009 and ADD_0023.
ADD_0028	If the wait first integrity confirmation timer expires, the train length monitoring timer shall be considered expired, the requirement ADD_0022 shall be applied immediately.

General Requirements	
IND	**Description**
ADD_0029	When transition #11B is performed, the train length monitoring timer and the wait first integrity confirmation timer shall be considered expired, the requirement ADD_0022 shall be applied immediately.

Table 26: General Requirements

6.2 HIGH DENSITY APPLICATION REQUIREMENTS

High Density Application Requirements	
IND	**Description**
HDA_0001	If the performance impact of transition #8A caused by the clauses e)/f) of the requirement HTD_46 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 HTD Principles [8]; • 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.
HDA_0002	Areas where Supervised Manoeuvre is planned to be used normally are expected to be distant from radio holes and areas with poor radio coverage.
HDA_0003	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.
HDA_0004	Overall Consist Length used in HL3/HTD Applications shall be SIL4

High Density Application Requirements	
IND	**Description**
HDA_0005	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
HDA_0006	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
HDA_0007	In areas where Supervised Manoeuvre is used, an "integrity loss propagation timer" is assigned to each VSS and for each direction.
HDA_0008	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 HDA_0005 and HDA_0006

Table 27: High Density Application Requirements

6.3 REGIONAL APPLICATION REQUIREMENTS

Regional Application Requirements: Applications with reduced use of TTDs	
IND	**Description**
REG_0001	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.

Regional Application Requirements: Applications with reduced use of TTDs	
IND	**Description**
REG_0002	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 and #12C 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);

Table 28: Regional Application Requirements: Applications with reduced use of TTDs

Regional Application Requirements: Applications with radio holes	
IND	**Description**
REG_1001	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 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
REG_1002	Each specific application shall define the reaction of the dispatcher/Traffic Management System in case the radio hole timer expires.

Table 29: Regional Application Requirements: Applications with radio holes

7 ENGINEERING RULES

This chapter reports the activities developed into the task 15.3 of FP2-R2DATO WP15:

From the GA: "*The objective of this task is to work collaboratively to elaborate and define engineering rules for deploying HL3 system defined in tasks 15.2 and 15.3 to main and regional lines.*"

Therefore, this section contains the engineering rules of the HL3/HTD for main and regional lines identify during the task activities. Moreover, covers the specific engineering rules for HL3/HTD.

The engineering rules shared with previous ETCS levels are beyond the scope of this activities.

The section is composed by two main paragraphs:

- Engineering Rules for Main Line
- Engineering Rules for Regional Lines

7.1 ENGINEERING RULES FOR MAIN LINES

7.1.1 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.

7.1.1.1 Train Integrity Eng Rules

7.1.1.1.1 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.

7.1.1.1.2 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

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

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

7.1.1.1.4 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.

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.

7.1.1.2 VSS Eng Rules

7.1.1.2.1 VSS – Eng. Rule 1

The trackside will consider the train to be located on a VSS when entering it upon receiving the confirmation (through position report) that the maximum safe front end of the train has entered the VSS, including all preceding VSS up to the last VSS currently covered by the train location, only if the TTD/s covering all those VSS is/are not free. In the case of a VSS in advance of the EoA, the trackside will consider the train located in that VSS if the minimum safe front end of the train is confirmed to have entered that VSS.

7.1.1.2.2 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.

7.1.1.2.3 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.

7.1.1.2.4 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.

7.1.1.2.5 VSS – Eng. Rule 5

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: To avoid unnecessary difficulties in the implementation of HL3/HTD functionality.

7.1.1.3 Timers Eng Rules

7.1.1.3.1 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.

- 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.

7.1.1.3.2 WaitIntegrityTimer - Eng. Rule 1:

Recommended is a value comparable to the position report cycle time [T_CYCLOC].

- 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.

7.1.1.3.3 ShadowTrainTimer - Eng. Rule 1:

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

If the timer is too short, the trackside must assume a shadow train and keep the track section occupied 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.

7.1.1.3.4 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 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.

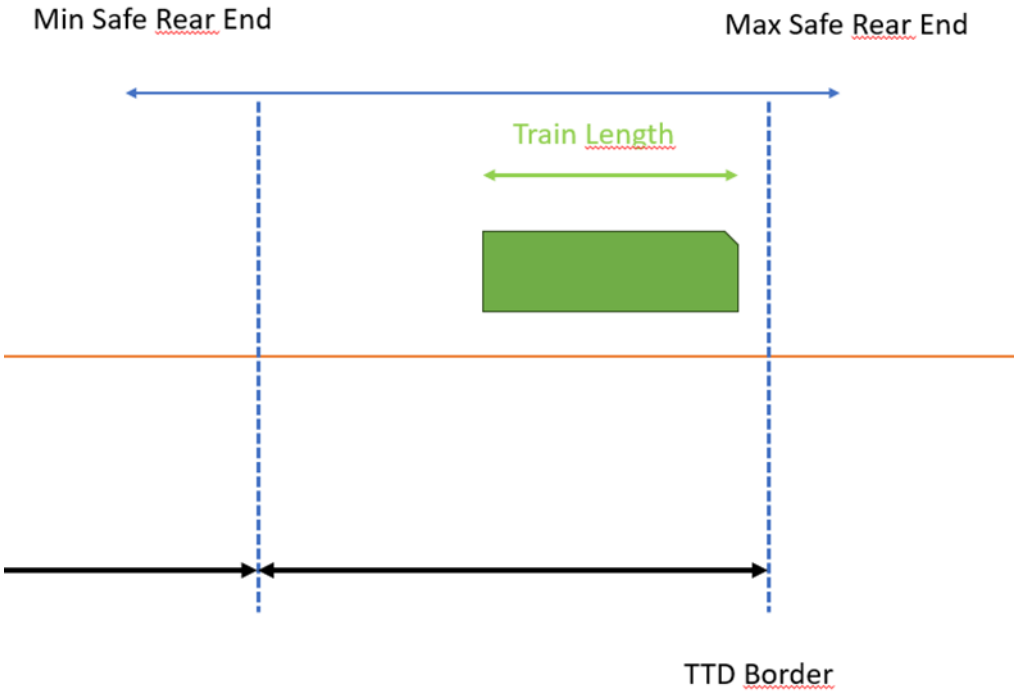

Figure 12: Unwanted situation - Max Safe Rear End in advance of real train front end.

7.1.1.3.5 DisconnectPropagationTimer - Eng. Rule 1:

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

- 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 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.

7.1.1.3.6 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 in modes SR or SH.

- 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 the train with integrity confirmed, the

track section is wrongfully treated as free, and another train could get an authorisation for this track section.

7.1.1.3.7 IntegrityLossPropagationTimer - Eng. Rule 1:

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

- 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.

7.1.1.3.8 IntegrityLossPropagationTimer - Eng. Rule 2:

To define the timer value, IM shall have the following information for each vehicle expected to be used on the line:

- The amount of 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 train with the worst bi r, (typically the one that maintain the vehicle at standstill for the lowest amount of time) and configuring the trackside timers.

7.1.2 Engineering Rules for Operational procedures

This subchapter contains the engineering rules that must be considered for nominal operations in an HL3/HTD trackside area.

7.1.2.1.1 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 must be contained within the VSS where the SoM is executed.

7.1.2.1.2 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.

7.1.2.1.3 Splitting & Joining Eng. Rule 1:

Dedicated TTDs composed of a single VSS, dimensioned in such a way that they are able to contain all the planned trains for joining/splitting, can be considered.

Rationale: As additional measures to safely localise a disconnected train or wagon and detecting an unintentional movement when occurs out of this dedicated area.

7.1.2.1.4 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.

7.1.2.1.5 Reversing Eng. Rule 1:

The area where trains are allowed to perform reversing movement (furthest location that the rear of a train can reach) shall be a single VSS.

Rationale: To limit the area where the rear end of the train can be positioned after reversing and thus avoid collisions with other trains.

7.1.2.1.6 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.

7.1.2.1.7 Supervised Manoeuvre Mode Eng. Rule 1:

Areas where Supervised Manoeuvre is operated shall have a short TTD section (as the one defined at the border), 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.

7.1.2.1.8 Supervised Manoeuvre Mode Eng. Rule 2:

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

Rationale: This is made to facilitate sweeping.

7.1.3 Engineering Rules for Degraded scenarios

This subchapter contains the engineering rules that must be considered for degraded scenarios in an HL3/HTD trackside area.

7.1.3.1.1 OTI-I failure Eng. Rule 1:

The IM will determine whether to accept integrity confirmation from the Driver following a failure in the OTI-I.

7.1.3.1.2 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
- If once at the siding or stopping point, Driver can confirm integrity.

7.1.3.1.3 Trains without OTI-I Eng. Rule 1:

IM shall define in which situations and places is allowed the entry into the HL3/HTD area to trains that do not report TI information.

7.1.3.1.4 Radio holes Eng. Rule 1:

Radio hole area should always be included inside the same VSS.

Rationale: To prevent the EoA to be within the Radio Hole.

7.1.3.1.5 Radio holes Eng. Rule 2:

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

In the following Figure 13 (adaptation of Figure 16 in 5.18.5 of the SRS [8]), 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.

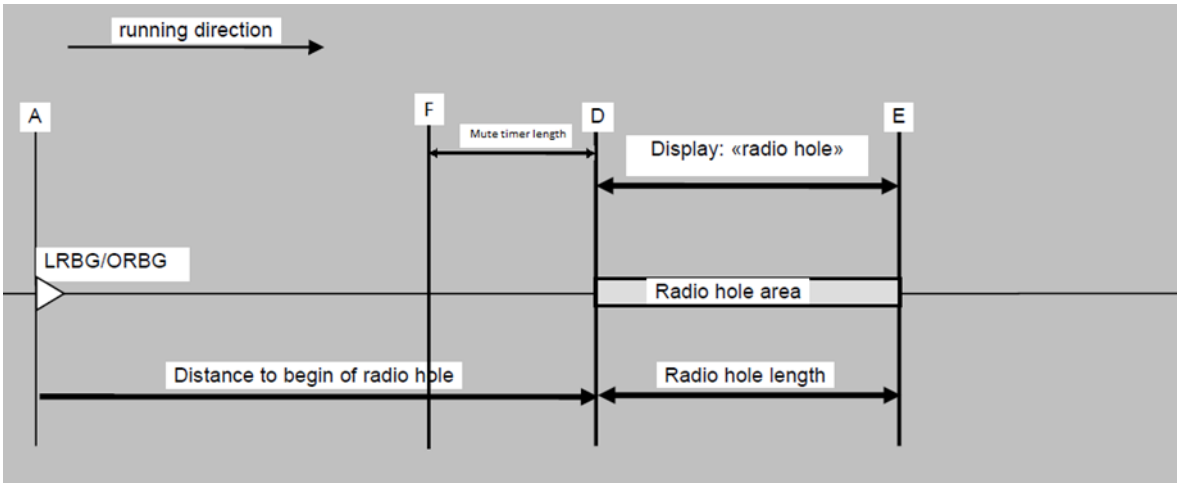

Figure 13:Radio Hole

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.

7.1.3.1.6 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. Trains that are reporting their position could be used for that. In these cases, all occupied TTD sections should be swept (OS or SR) by communicating trains that have confirmed their integrity to resume safely.

7.2 ENGINEERING RULES FOR REGIONAL LINES

On regional lines, in addition to less traffic, it is expected a significant reduction of TCO (OPEX and CAPEX), which means a reduction in the trackside equipment. That is, fewer balises, fewer TTDs, and less radio equipment along the track, which can increase the presence of radio holes and the risk of loss of communications on regional lines.

7.2.1 General engineering issues

7.2.1.1.1 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 Figure 14 below)

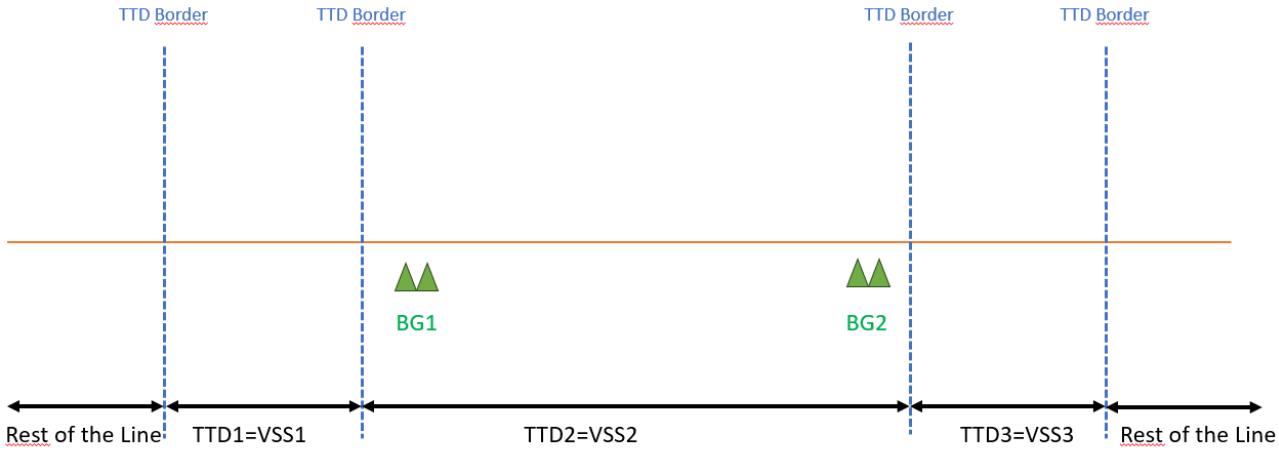

Figure 14: Three TTDs and VSSs are coincident

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 functions:

- Avoid propagation from the rest of the line to TTD2 and viceversa;
- Allow the triggering of the transition #11A;

In general it is expected that TTD1 and TTD3 will be quite short. 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 train in TTD1 and TTD3;

- Increase of the frequency of the position reports inside 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)

8 HL3/HTD USE CASES

This session reports all the Use Cases developed divided by use case group as reported in Table 6.

8.1 END OF MISSION / START OF MISSION

8.1.1 UC_01_01

Use Case Group	SoM EoM
Use Case	End of Mission with train integrity confirmed after standstill
UC ID	UC_01_01
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside
Main goal	Describes what happens to the track status at End of Mission when Train Integrity has been confirmed after the train has reached standstill.
Assumptions	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).
Precondition	• Train stopped in a station (at standstill). The ETCS On-board has reported a position with integrity confirmed after reaching standstill, so the CRE is at the min safe rear end. Driver closes the desk. • The state of all VSSs covered by the train location is Occupied • The state of the VSSs in rear and in front of the train are Free • There are free TTDs adjacent to the TTD where the train is located
Flow of events	1. ETCS on board changes to SB mode and reports EoM with no integrity info. 2. The HL3/HTD Trackside orders to terminate the communication session, 3. ETCS on board terminates communication session with HL3/HTD Trackside. 4. The HL3/HTD Trackside updates VSS states previously occupied by train to “unknown” state (transition #7A) and starts a disconnect propagation timer for each VSS of memorised train location. According to the requirement ADD_0009 the train data may be memorised. 5. On trackside, the disconnect propagation timers expire and the VSS in rear and beyond the memorised train location on the same TTD are changed from Free to Unknown (transition #1C).
Postcondition	ETCS on board in SB after EoM and no longer communicating with HL3/HTD Trackside.
Safety relation	
Open topics / consideration	

8.1.2 UC_01_02

Use Case Group	SoM EoM
Use Case	End of Mission without train integrity confirmed after standstill

UC ID	**UC_01_02**
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside
Main goal	Describes what happens to the track status at End of Mission when Train Integrity has NOT been confirmed after the train has reached standstill.
Assumptions	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).
Precondition	Train stopped in a station (at standstill). The ETCS On-board has not reported a position with integrity confirmed after reaching standstill, so the CRE is at some location in rear of the actual rear end of the train, being further away than if integrity had been confirmed. Driver closes the desk.
Flow of events	1. ETCS on board changes to SB mode and reports EoM with no integrity info in same location. 2. The HL3/HTD Trackside orders to terminate the communication session. 3. ETCS on board terminates communication session with HL3/HTD Trackside. 4. The HL3/HTD Trackside updates VSS states previously occupied by train to “unknown” state (transition #7A) . The disconnect propagation timer is started. According to the requirement ADD_0009 the train data may be memorised.
Postcondition	ETCS on board in SB after EoM and no longer communicating with HL3/HTD Trackside. For system types using TTD, the area can be cleared.
Safety relation	
Open topics / consideration	

8.1.3 UC_01_03

Use Case Group	SoM EoM
Use Case	Start of Mission with valid position - Trackside provides a FS MA.
UC ID	**UC_01_03**
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside
Main goal	Describes the steps taken and the changes to the track status during the Start of Mission procedure when the position of the train is still known by the ETCS On-board and the HL3/HTD Trackside is able to recover the Unknown area created at End of Mission
Assumptions	-- 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 ETCS On-Board is not able to provide the Safe Consist Length information
Precondition	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 VSS with status “Unknown” corresponding to the location of the train after it performed End of Mission. The disconnect propagation timer of the VSS

	is expired. A desk is opened.-- The HL3/HTD trackside has memorised the train length according to the requirement ADD_0009, so it has verified that there is no other train except the one that performed EoM. The train length monitoring timer is not expired. There are no Valid Train Data.
Flow of events	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 and reports a valid position (with no train integrity information) in SB mode. 3. HL3/HTD Trackside receives the Start of Mission Position Report, evaluates the reported position and the NID_ENGINE in the Start of Mission Position Report. The VSS remain unknown because the train is not deemed connected, it has no valid train data. The check of the NID_ENGINE according to the requirement ADD_0024 is positive. 4. Driver validates the Train Data. 5. ETCS On-board sends the Validated Train Data to the HL3/HTD Trackside, including a position report with no train integrity information. Transition #5A is made on the VSS, because now the train is deemed connected. Transition #4D is performed and the VSSs in front of the engine, that became unknown only because of the expiration of the disconnect propagation timer, become free. 6. HL3/HTD Trackside checks the Validated Train Data according to the requirement ADD_0025. 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 started because the train becomes not treated as integer (condition c) of HTD_46) 7. ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I). 8. HL3/HTD Trackside determines the Confirmed Rear End, and updates the VSS corresponding to the Train Location from ambiguous to occupied (transition #11B). The integrity loss propagation timer is stopped because of condition b) of requirement HTD_44. HL3/HTD Trackside determines the other VSSs in rear of the CRE of the train in the TTD where there was transition #11B are free, because they were unknown only because of the disconnect propagation timer (transition #4C). The train length monitoring timer and the wait first integrity confirmation timer are stopped according to the requirement ADD_0029. 9. Train sends a MA Request. 10. Trackside provides an FS MA to the train as there are some free VSSs in front of the train location and there is no other vehicle inside the same VSS because of the conditions checked with the requirement ADD_0009. (Note: TAF procedure may be applied but is not strictly needed because there is assurance that there is no other vehicle) 11. Train receives FS MA, starts moving and regularly reports its new position with integrity confirmed. 12. Trackside receives TPR with integrity confirmed. Trackside computes the new train location and changes the VSS in front of the train to from Free to Occupied (transition #2A), and the VSS of the old train location which are no longer part of the new train location from Occupied to Free (transition #6B).
Postcondition	Train is moving in FS after SoM and has freed the location where EoM was performed.
Safety relation	

Open topics / consideration	This requires some additional functionality in comparison to the EUG specification [8]

8.1.4 UC_01_04

Use Case Group	SoM EoM
Use Case	Start of Mission with invalid position
UC ID	**UC_01_04**
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside
Main goal	Describes the steps taken during the Start of Mission procedure when the position of the train is invalid
Assumptions	•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).
Precondition	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 VSS status Unknown corresponding to the location of the train after it performed End of Mission. A desk is opened.
Flow of events	1. ETCS On-board 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. 2. ETCS On-board opens a communication session with the HL3/HTD Trackside and reports invalid position (with no train integrity information) in SB mode. 3. HL3/HTD Trackside receives the Start of Mission Position Report, accepts the train, independent of the reported position. There is no change to VSS states. ETCS On-Board deletes the train position information. 4. 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). . 5. ETCS On-board sends the Validated Train Data to the HL3/HTD Trackside, including a position report with position unknown and no train integrity information. 6. HL3/HTD Trackside acknowledges having received Validated Train Data. The reported position is still unknown. 7. ETCS On-board enables the START button on the DMI. 8. The ETCS On-board is in SB mode and communicating with the HL3/HTD Trackside; the Unknown VSS states remains after Start of Mission. From here, the train can be given an SR authorisation.
Postcondition	Train is ready to depart in SR when authorised to do so.
Safety relation	
Open topics / consideration	

8.1.5 UC_01_05

Use Case Group	SoM EoM
Use Case	Start of Mission with unknown position
UC ID	**UC_01_05**
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside
Main goal	Describes the steps taken during the Start of Mission procedure when the position of the train is unknown.
Assumptions	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).
Precondition	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 VSS status Unknown corresponding to the location of the train after it performed End of Mission. A desk is opened.
Flow of events	1. ETCS On-board 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. 2. ETCS On-board opens a communication session with the HL3/HTD Trackside and reports position referred to an unknown LRBG (with no train integrity information) in SB mode. 3. L3 Trackside receives the Start of Mission Position Report, accepts the train, evaluates the reported position. L3 Trackside is not able to establish a valid location for the train with the reported position, but the communication session is kept. 4. 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). . 5. ETCS On-board sends the Validated Train Data to the HL3/HTD Trackside, including a position report with position unknown and no train integrity information. 6. HL3/HTD Trackside acknowledges having received Validated Train Data. The reported position is still unknown. 7. ETCS On-board enables the START button on the DMI. 8. The ETCS On-board is in SB mode and communicating with the HL3/HTD Trackside; the Unknown VSS states remains after Start of Mission. From here, the train can be given an SR authorisation.
Postcondition	Train is ready to depart in SR when authorised to do so.
Safety relation	
Open topics / consideration	

8.1.6 UC_01_06

Use Case Group	EoM-SoM
Use Case	EoM-SoM Train receives FS MA after SoM and frees VSSs

UC ID	UC_01_06
Main actor	HL3/HTD Trackside
Other actors	ETCS On-board, Driver, Train
Main goal	Train receives FS MA after SoM Train frees VSSs after SoM
Assumptions	There are no other trains in the area where the Train performs EoM and SoM There are no expiring timers of other trains affecting the states of area where the considered train is located.
Precondition	The train is at standstill (speed zero) Conditions described in requirement ADD_0021 are satisfied The state of the VSS covered by the train location is Occupied The state of the VSSs in rear and in front of the train are Free

Flow of events	1. The Driver closes the cab. 2. The Train terminates the communication session with trackside. 3. Trackside changes the VSS covered by train location to unknown (transition #7A) and starts the related disconnect propagation timer. Trackside stores train related information like train location, integrity status and train length according to ADD_0009 and starts the train length monitoring timer of the associated TTD. 4. The disconnect propagation timers expire and the VSS in rear and beyond the memorised train location on the same TTD are changed from Free to Unknown (transition #1C). -- time passes without expiration of the train length monitoring timer-- 5. 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. 6. ETCS On-board opens a communication session with the HL3/HTD Trackside and reports a valid position (with no train integrity information) in SB mode. 7. 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 ADD_0024 is positive, so the trackside maintains the storage of the data according to the requirements ADD_0009 and ADD_0023. 8. Driver validates the Train Data. 9. Train sends Validated Train Data (VTD) 10. Trackside determines that the train has not moved since EoM (e.g. based on cold movement detector; a margin for small roll movements might be used) and determines an unambiguous Front End position of the train. The FE is within the stored train location and trackside changes the VSS of the FE to Ambiguous (Transition #5A). The states of the VSS in front of the FE are changed from Unknown to Free as trackside is sure that the disconnect propagation timer is the only reason why they are Unknown (transition #4D). 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 ADD_0025. 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 started because the train becomes not treated as integer, applying condition c) of HTD_46 11. ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I). 12. Trackside receives TPR with integrity confirmed, determines the Confirmed Rear End and changes all VSSs of the train location from Ambiguous to Occupied (transition #11B). The integrity loss propagation timer is stopped because of condition b) of requirement HTD_44. HL3/HTD Trackside determines the other VSSs in rear of the CRE of the train in the TTD where there was transition #11B are free, because they were unknown only because of the disconnect propagation timer (transition #4C). The train length monitoring timer and the wait first integrity confirmation timer are stopped according to the requirement ADD_0029. 13. Train sends a MA Request.

	14. 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 TTD where the train is. 15. Train receives FS MA, starts moving and regularly reports its new position with integrity confirmed. 16. Trackside receives TPR with integrity confirmed. Trackside computes the new train location and changes the VSS in front of the train to from Free to Occupied (transition #2A), and the VSS of the old train location which are no longer part of the new train location from Occupied to Free (transition #6B).
Postcondition	Train is moving in FS after SoM and has freed the location where EoM was performed.
Safety relation	
Open topics / consideration	This requires some additional functionality in comparison to the EUG specification [8]

8.1.7 UC_01_07

Use Case Group	SoM EoM
Use Case	Start of Mission with valid position – exclusion of the presence of shadow trains
UC ID	UC_01_07
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside
Main goal	Describes the steps taken and the changes to the track status during the Start of Mission procedure when the position of the train is valid
Assumptions	•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). •There are no other trains in the area where the Train performs EoM and SoM
Precondition	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 VSS status “Unknown” corresponding to the location of the train after it performed End of Mission.

Flow of events	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 and reports a valid position (with no train integrity information) in SB mode. 3. HL3/HTD Trackside receives the Start of Mission Position Report, evaluates the reported position. As no updated train length info is received, HL3/HTD Trackside do not update states of VSS, which will remain unknown. 4. 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. 5. ETCS On-board sends the Validated Train Data to the HL3/HTD Trackside, including a position report with no train integrity information. 6. HL3/HTD Trackside acknowledges having received Validated Train Data. HL3/HTD Trackside uses received Train Length info to update state of VSS. HL3/HTD trackside checks that the train is located in the same area previously set as “unknown”. The HL3/HTD Trackside updates VSS to state “Ambiguous” (Transition #5A). The integrity loss propagation timer is started because the train becomes not treated as integer, applying condition c) of HTD_46 7. ETCS On-board sends a position report with train integrity confirmed by external device (OTI-I). No update of the state of the VSSs is made, because there are not the conditions described in the use cases 01_03 and 01_06 or the optional transitions #4C, #4D and #11B are not used 8. Train sends a MA Request. 9. Trackside receives an MA that crosses the TTD border. The procedure for TAF applicable in each country is followed. 10. The train starts moving, setting to unknown the VSSs in rear of the assumed rear end of the train (transition #10A) and setting the VSS where the train is located to ambiguous (transition #3A); 11. When the train leaves the TTD where it performed SoM, all the VSSs in the left TTD are set to free (transition #9A). Depending of the operational conditions (speed, value of the shadow train timer, etc.) transition #11A may be triggered and the VSSs where the train is located can become occupied.
Postcondition	The VSSs where the train is located are now occupied
Safety relation	Yes
Open topics / consideration	Specific SoM/Splitting/Joining Areas may be defined in order to: • Allow easy transition #11A (in particular in applications with short values of shadow train timer); • Avoid propagation of unknown state from the VSSs external to SoM Area; • Avoid operational impact of the ambiguous state in applications that don’t use a large number of TTDs

8.2 HANDOVER

8.2.1 UC_02_01

Use Case Group	Handover
Use Case	Nominal Handover without interface for communication of the state of the VSSs
UC ID	**UC_02_01**
Main actor	Dispatcher/Traffic Management System
Other actors	Train ETCS On-board Handing Over RBC Accepting RBC
Main goal	HL3/HTD Trackside authorises a train running in FS, reporting frequently its position with Train Integrity confirmed, to travel towards a Handover border. Train is able to handle two communication sessions. When the MA reaches the Handover border, Handing Over RBC starts Handover and Accepting RBC sends information to the Handing Over RBC for the train to go beyond the Handover border. Handing Over RBC sends an MA beyond the Handover border. Train passes the Handover border and Accepting RBC takes over the responsibility of the train. Handing Over RBC orders the train to terminate communication session after receiving a position report with the CRE beyond the Handover border.
Assumptions	• The Accepting and Handing Over RBC are managed by the same Dispatcher; • TTD borders coincide with the Handover Border; • 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 and release the VSSs in the handing over area (i.e. in rear of the border); • Train is able to handle two communication sessions;
Precondition	• A train is running in FS in the direction of the Handover border, reporting frequently with Train Integrity confirmed.

Flow of events	1. Dispatcher or Traffic Management System requests route extension for the train beyond the Handover border. 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. The train moves towards the border. Accepting RBC receives information from Handing Over RBC that Handover process has started and sends acknowledgement to the Handing Over RBC. Handing Over RBC sends a request for Route Related Information and Accepting RBC sends Route Related Information to Handing Over RBC. 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; 2. Handing Over RBC sends to the ETCS On-board the RBC Transition Order to establish a communication session with the Accepting RBC. ETCS On-board establishes communication with Accepting RBC and starts sending position reports to the Accepting RBC; 3. 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). The Handing Over RBC does not send anymore route related information to the ETCS On-board (req. 3.15.1.2.8 of SUBSET 026). The Handing Over RBC sends the Announcement Message to the Accepting RBC. 4. The train passes the border, the ETCS On-board reads the border balise group with an order to execute the RBC transition immediately and sends a position report to both the Handing Over and Accepting RBCs. Handing Over RBC receives the position report. Accepting RBC receives the position report. The TTD in advance of the border becomes occupied, 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), the VSS section in advance to the border is set to ambiguous (Transition #3A). This is consistent with the fact that some conditions to treat the train as integer (see HTD_46) will not be sent through the RBC-RBC interface) 5. The train proceeds in the accepting area, the ETCS On-board sends position reports with Train Integrity confirmed to the Handing Over RBC. When the Handing Over RBC determines that the train is completely in the accepting area, i.e. the last TTD in rear of the border becomes free, it orders to the ETCS On-board to terminate the communication session. The ETCS On-board terminates the communication session with the Handing Over RBC; *Note: The ambiguous state with the related possible shadow train will be solved in the accepting RBC area.*
Postcondition	The use case is successfully completed if it is possible to terminate the communication session with the Handing Over RBC when the train is in the accepting RBC area. The use case fails in case it is not possible to establish that the train has reached the Accepting RBC Area. (There is no safety issue, only an operational one)
Safety relation	All Events are safety relevant.
Open topics / consideration	

8.2.2 UC_02_02

Use Case Group	Handover
Use Case	Loss of Connection between Handing Over RBC and Accepting RBC
UC ID	**UC_02_02**
Main actor	Dispatcher/Traffic Management System
Other actors	Train ETCS On-board Handing Over RBC Accepting RBC
Main goal	HL3/HTD Trackside authorises a train running in FS, reporting frequently its position with Train Integrity confirmed, to travel towards a Handover border. Train is able to handle two communication sessions. When the MA reaches the Handover border, Handing Over RBC starts Handover and Accepting RBC sends information to the Handing Over RBC for the train to go beyond the Handover border. Handing Over RBC sends an MA beyond the Handover border. There is a loss of connection between the 2 RBCs and there is a shortening of the movement authority to the Handover border.
Assumptions	The Accepting and Handing Over RBC are managed by the same Dispatcher; TTD borders coincide with the Handover Border; 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 is able to handle two communication sessions;
Precondition	A train is running in FS in the direction of the Handover border, reporting frequently with Train Integrity confirmed.
Flow of events	1. Dispatcher or Traffic Management System requests route extension for the train beyond the Handover border. 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. The train moves towards the border. Accepting RBC receives information from Handing Over RBC that Handover process has started and sends acknowledgement to the Handing Over RBC. Handing Over RBC sends a request for Route Related Information and Accepting RBC sends Route Related Information to Handing Over RBC. 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; 2. Handing Over RBC sends to the ETCS On-board the RBC Transition Order to establish a communication session with the Accepting RBC. ETCS On-board establishes communication with Accepting RBC and starts sending position reports to the Accepting RBC; 3. Handing Over RBC detects loss of connection with the Accepting RBC. The MA is shortened to the Handover border. Note: Cancellation information to the Accepting RBC is avoided in order to maintain the communication session between the ETCS On-board and the Accepting RBC; 4. According to the specific application procedures, Dispatcher/Traffic Management System authorises the driver to enter the Accepting Area, the driver selects Override to pass the Handover border, ETCS On-board changes to SR mode and informs both the Handing Over and the Accepting RBCs of the new mode. The train moves towards the border.

	5. 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). The Handing Over RBC does not send anymore route related information to the ETCS On-board (req. 3.15.1.2.8 of SUBSET 026). 6. The train passes the border, the ETCS On-board reads the border balise group with an order to execute the RBC transition immediately and sends a position report to both the Handing Over and Accepting RBCs. Handing Over RBC receives the position report and informs the Accepting RBC that the train has reached the location corresponding to the border. Accepting RBC receives the position report. The TTD in advance of the border becomes occupied, taking into account that it is not foreseen to have a communication between the 2 RBCs about the status of the VSS sections, the VSS section in advance to the border is set to ambiguous (Transition #3A). This is consistent with the fact that some conditions to treat the train as integer (see HTD_46) will not be sent through the RBC-RBC interface 7. The train proceeds in the accepting area, the ETCS On-board sends position reports with Train Integrity confirmed to the Handing Over RBC. When the Handing Over RBC determines that the train is completely in the accepting area, i.e. the last TTD in rear of the border becomes free; it orders to the ETCS On-board to terminate the communication session. The ETCS On-board terminates the communication session with the Handing Over RBC; *Note: The ambiguous state with the related possible shadow train will be solved in the accepting RBC area*
Postcondition	The use case is successfully completed if it is possible to terminate the communication session with the Handing Over RBC when the train is in the accepting RBC area. The use case fails in case it is not possible to establish that the train has reached the Accepting RBC Area. (There is no safety issue, only an operational one)
Safety relation	All Events are safety relevant
Open topics / consideration	

8.2.3 UC_02_03

Use Case Group	Handover
Use Case	Handover with only one communication session
UC ID	**UC_02_03**
Main actor	Dispatcher/Traffic Management System
Other actors	Train ETCS On-board Handing Over RBC Accepting RBC

Main goal	HL3/HTD Trackside authorises a train running in FS, reporting frequently its position with Train Integrity confirmed, to travel towards a Handover border. Train is able to handle one communication session. When the MA reaches the Handover border, Handing Over RBC starts Handover and Accepting RBC sends information to the Handing Over RBC for the train to go beyond the Handover border. Handing Over RBC sends an MA beyond the Handover border. Train passes the Handover border and Accepting RBC takes over the responsibility of the train. Handing Over RBC orders the train to terminate communication session after receiving a position report with the CRE beyond the Handover border.
Assumptions	The Accepting and Handing Over RBC are managed by the same Dispatcher; TTD borders coincide with the Handover Border; 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;
Precondition	A train is running in FS in the direction of the Handover border, reporting frequently with Train Integrity confirmed.

Flow of events	1. Dispatcher or Traffic Management System requests route extension for the train beyond the Handover border. 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. The train moves towards the border. Accepting RBC receives information from Handing Over RBC that Handover process has started and sends acknowledgement to the Handing Over RBC. Handing Over RBC sends a request for Route Related Information and Accepting RBC sends Route Related Information to Handing Over RBC. 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; 2. Handing Over RBC sends to the ETCS On-board the RBC Transition Order; 3. When the train with its max safe front end reaches the border, the ETCS On-board sends a position report to the Handing Over RBC (req. 5.15.3.2.3.1 of SUBSET 026). The Handing Over RBC sends the Announcement Message to the Accepting RBC (req. 5.15.3.2.3.2 of SUBSET 026). 4. The train passes the border, the ETCS On-board reads the border balise group with an order to execute the RBC transition immediately. The TTD in advance of the border becomes occupied, the ETCS On-board is not connected with the Accepting RBC so the VSS in advance to the border is set to unknown (Transition #1A). To avoid that a restrictive reaction is adopted, the Accepting RBC shall not trigger a restrictive reaction because of this unknown VSS. 5. When the min safe rear end of the train passes the location of the border, the ETCS On-board shall send the position report to the "Handing Over" RBC. The Handing Over RBC shall send a session termination order to the ETCS On-board and the ETCS On-board shall terminate the session with the Handing Over RBC and open the session with the accepting RBC. Once the communication with the Accepting RBC is established the VSS section in advance of the border will be set to ambiguous (Transition #5A) Note: delaying the session termination order by the Handing Over RBC it is possible to have an additional transition #6B for the liberation of the last VSS in rear of the border. Anyway the cost will be to delay the session establishment with the accepting RBC; The last VSS in rear of the border becomes free when the last TTD in rear of the border becomes free (transition #6A)
Postcondition	The use case is successfully completed if it is possible to free the last VSS in rear of the border. The use case fails in case it is not possible to free the last VSS in rear of the border
Safety relation	All Events are safety relevant
Open topics / consideration	The way to avoid restrictive reactions in case of occupation of the first TTD in advance of the Handover Border is left to the specific applications. In principle it is possible to have a special "unknown" state that does not prevent the issue of a FS MA over it, if the Announcement Message has already been received by the Accepting RBC.

8.2.4 UC_02_04

Use Case Group	Handover
Use Case	Train Integrity Loss during Handover

UC ID	**UC_02_04**
Main actor	Dispatcher/Traffic Management System
Other actors	Train ETCS On-board Handing Over RBC Accepting RBC
Main goal	HL3/HTD Trackside authorises a train running in FS, reporting frequently its position with Train Integrity confirmed, to travel towards a Handover border. Train is able to handle two communication sessions. When the MA reaches the Handover border, Handing Over RBC starts Handover and Accepting RBC sends information to the Handing Over RBC for the train to go beyond the Handover border. Handing Over RBC sends an MA beyond the Handover border. Train reports having lost its integrity the Handover is cancelled and the situation is managed by operational procedures for train integrity loss.
Assumptions	The Accepting and Handing Over RBC are managed by the same Dispatcher; TTD borders coincide with the Handover Border; 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 is able to handle two communication sessions;
Precondition	A train is running in FS in the direction of the Handover border, reporting frequently with Train Integrity confirmed.

Flow of events	1. Dispatcher or Traffic Management System requests route extension for the train beyond the Handover border. 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. The train moves towards the border. Accepting RBC receives information from Handing Over RBC that Handover process has started and sends acknowledgement to the Handing Over RBC. Handing Over RBC sends a request for Route Related Information and Accepting RBC sends Route Related Information to Handing Over RBC. 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; 2. Handing Over RBC sends to the ETCS On-board the RBC Transition Order to establish a communication session with the Accepting RBC. ETCS On-board establishes communication with Accepting RBC and starts sending position reports to the Accepting RBC; 3. The ETCS On-board gives to the trackside the information of integrity lost (by a position report with Q_INTEGRITY=3, by a changed train length or by expiration of the wait integrity timer). The train is expected to brake because of rolling stock requirements for broken trains. The last VSS in rear of the border becomes ambiguous according to transition #8A 4. two sub-steps are possible: a. If the train is stopped before the maximum safe front end reached the border, the Handing Over RBC shall send cancellation information to the Accepting RBC if the MA is revoked. The Accepting RBC disconnects the train according to requirement 3.15.1.4.4 of SUBSET 026. Note: This allows to free the communication network, taking into account the fact that the non-harmonised procedures for recovering from train integrity loss can take some time, b. If the train is not stopped before the maximum safe front end reached the border, 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). The Handing Over RBC does not send anymore route related information to the ETCS On-board (req. 3.15.1.2.8 of SUBSET 026). 5. If train occupies the first TTD in advance of the border, the first VSS in advance of the border is set to ambiguous according to transition #3A. The Handing Over RBC disconnects the train. Note: This allows to free the communication network, taking into account the fact that the non-harmonised procedures for recovering from train integrity loss can take some time Non harmonised procedures for recovering from train integrity loss are applied.
Postcondition	Defines all conditions that must be fulfilled when the UC is successfully completed or the condition where we go in failed case. The use case is successfully completed if it is possible to use the non-harmonised procedures for the train integrity loss (in the Handing Over or in the Accepting RBC areas) The use case fails in case the information about train integrity loss is lost.
Safety relation	All Events are safety relevant
Open topics / consideration	

8.3 JOINING

The use case foreseen the joining of two trains in the following environment showed in Figure 15, where Train 2 will have to join Train 1 in a station to then continue the service as a single Train.

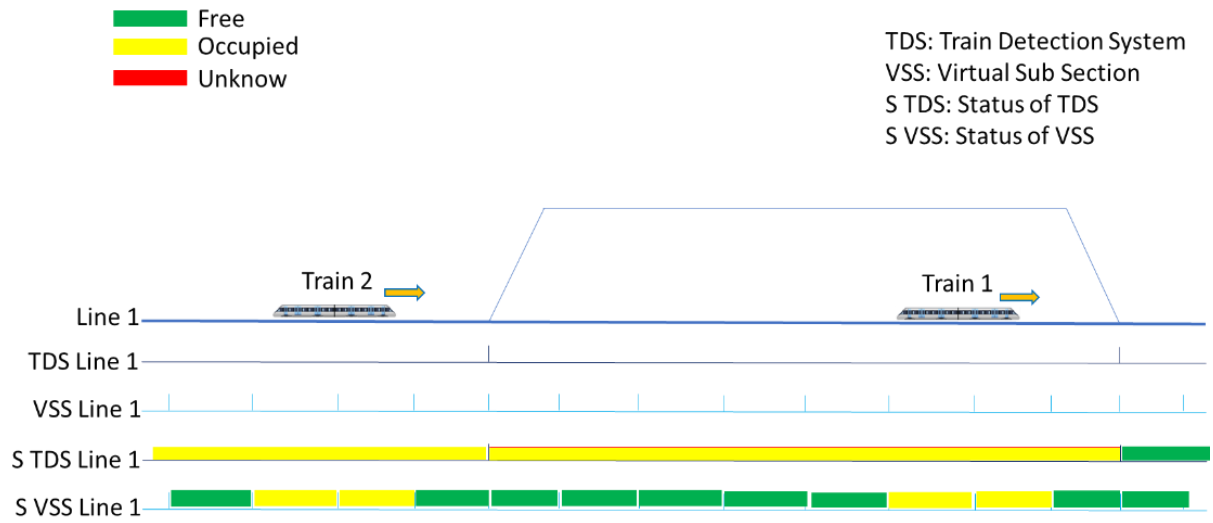

Figure 15: Started condition for Joining Scenario

The final expected condition is shown in Figure 16.

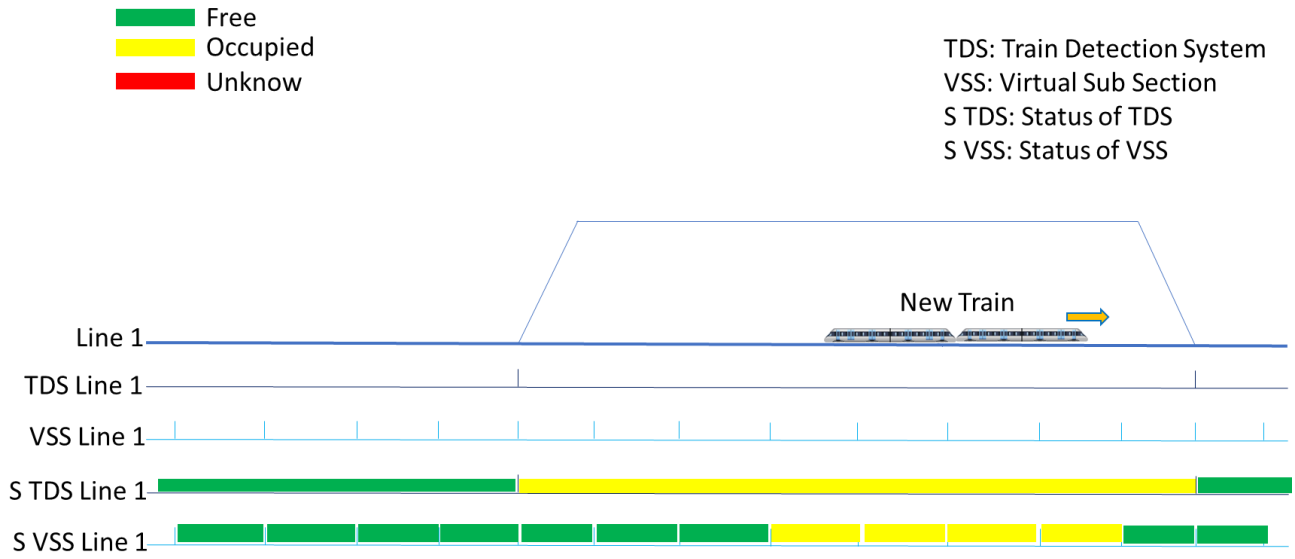

Figure 16: Final condition for Joining Scenario

The Train OTI-I is the on-board system able to detect the Train Integrity Status

The Train OTI-L is the on-board system able to calculate the train length.

8.3.1 UC_03_01

Use Case Group	Train Joining
Use Case	Train Joint another one
UC ID	**UC_03_01**
Main actor	Train 1
Other actors	Train 2 ETCS On-board RBC
Main goal	Two trains to be joining and new train ready to start.
Assumptions	Trains are standstill. Joining Train approaches in the same direction. The two trains have no faults. The Cab Activation, transition from NP a SB, provide the OTI-I and OTI-L reset.
Precondition	The two trains are in FS and communicating with the RBC Trackside
Flow of events	1. Train 1 has performed EoM on VSS 22 (see Figure 17) 2. Train 2 is approaching on VSS 12 3. Train 2 is authorised according to trackside rules (e.g. OS mode or SR) and moves to VSS 21 which becomes "occupied". VSS 12 becomes "free" This cover the sweeping authorization. 4. Train 2 moves to VSS 22, which becomes “occupied”. VSS 21 becomes "free". Note: If train 1 was a connected train, VSS 22 would have been "ambiguous" already. As soon as the front end of train 2 is reported on VSS 22, train 2 would not be treated as integer anymore and VSS 21 would become "ambiguous". When the assumed rear end has moved to VSS 22, VSS 21 becomes "unknown". 5. Train 2 joins Train 1 and performs EoM. VSS 22 becomes "unknown" The disconnect propagation timer related to VSS 22 is started. 6. Trainset 1-2 performs the Cab Activation (OTI-I/L reset), The train Integrity and train length information are provided to the EVC. Later on the Start of Mission procedure is performed with the validation of the data, the session with the trackside is established. The cab of train 1 is the driving cab and the corresponding ETCS will send updated length and integrity information and will receive the authorisation to move; the cab of train 2 will be in SL or NL mode. Trainset 1-2 is not yet treated as integer (shadow train risk). VSS 22 becomes “ambiguous” (#5A). The established session does not stop the disconnect propagation timer of VSS 22, because it is a different train (ETCS on-board) that is connected. 7. Trainset 1-2 moves to VSS 23 which becomes "ambiguous" (#5A). VSS 22 becomes "unknown" (#10A) 8. Trainset 1-2 moves to VSS 31 which becomes "occupied" if there isn’t any risk of shadow train, and all VSS on TTD 20 become "free".
Postcondition	The two trains are joining.
Safety relation	The Joining is safety relevant.

Open topics / consideration	The RBC could check that the new length is the sum of the two trains length. Anyway, in order to perform this operation it is necessary that assumption [Pre 15] is satisfied

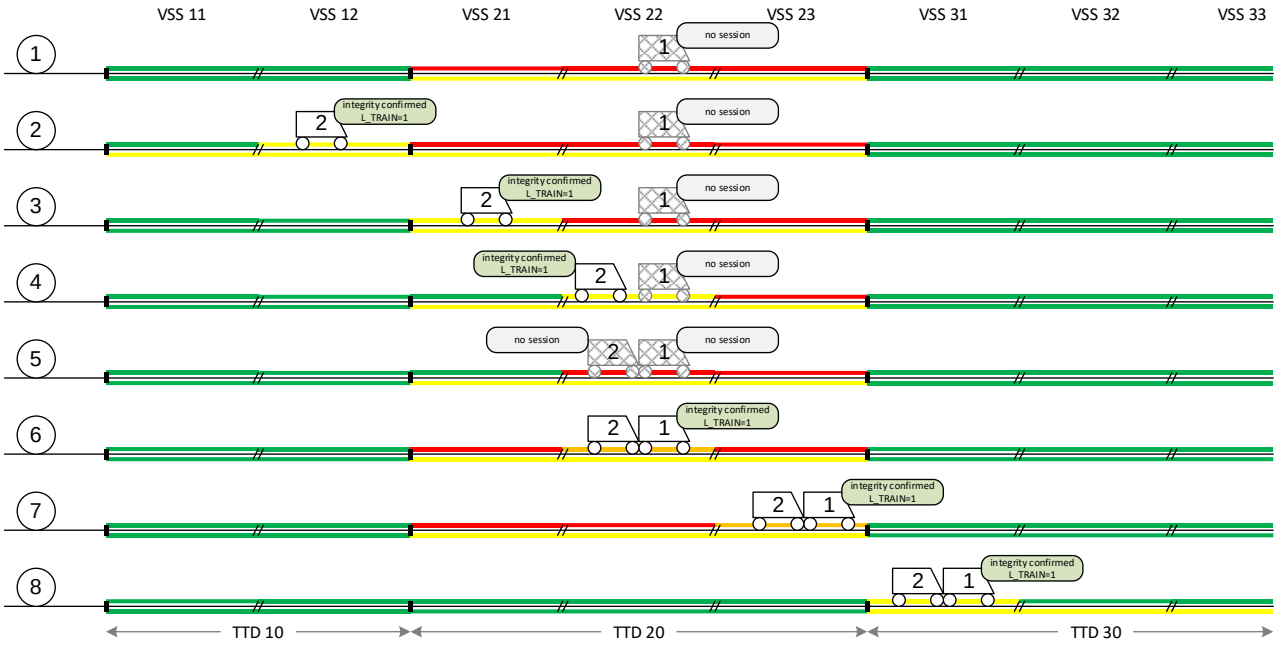

Figure 17: Joining step description.

To ensure that the train integrity and train length are reported correctly a reset of the systems that evaluate train integrity and train length is required.

This can take place by closing and opening the Cabin Desk or by resetting the dedicated modules. However, a SoM, or at least a new train data entry, is necessary because of a new train length. For this reason, the simplest solution seems to be to do an EoM and immediately after a SoM.

The scenario described above can actually be used in case the direction of the New Train changes.

The SoM will have to be done in the new cab of Train 1.

An attempt has been made to standardize the procedures as much as possible so as to have one that is always applicable.

Before starting to move the new Train, an activation of the Cabin Desk with consequent SoM must always be made.

This simplifies the scenario and always has the same behaviour of the systems involved.

Any specific application where this operational scenario will be implemented is responsible to evaluate and define the maximum latency to receive the expected information and the reaction to activate in case of excessive delays:

- Confirmation of successful coupling between trains.
- Confirmation of the measurement of the new train length.
- Confirmation of Train Integrity.

8.4.1 UC_04_01

Use Case Group	Level transitions
Use Case	Leaving HL3/HTD Area
UC ID	**UC_04_01**
Main actor	HL3/HTD Trackside
Other actors	ETCS On-board, driver, Train TIMS
Main goal	ID of the UC main goal: G_UC_04_01 Level transition from HL3/HTD to another Level.
Assumptions	1.- Train fitted with OTI-I. 2.- Not fallback situations. 3.- Unique Level transition (1, no more). 4.-The level transition order is immediate, not conditional. 5.- The level transition is not started by the driver. 6.- TTD borders coincide with the Level Transition Border
Precondition	1.- Neither Shunting Mode nor passive shunting, nor reversing mode, nor sleeping mode, nor NL (Non Leading) Mode, nor SB (Stand By). 2.- Not Start of Mission. 3.- L2 is configured in ETCS On-board and at least one Mobile Terminal is available on-board, i.e. the ETCS On-board has detected at least one Mobile Terminal in working condition, independently whether it is registered to a network or not.
Flow of events	1. Level transition announcement in the DMI. 2. ETCS On-board receives MA and track description into the new area or target speed at the level transition border 3. Driver acknowledges level transition (if L0/NTC) when the max safe front end of the train has passed a trackside defined location in rear of the level transition border. 4. The train reports position in such a way that the last VSSs in the HL3/HTD area become occupied (transition #2A). 5. HL3/HTD Trackside orders level transition. 6. ETCS On-board reports new level to HL3/HTD Trackside. 7. The last TTD in the HL3/HTD area becomes free, and therefore the last VSSs in the HL3/HTD area becomes free as well (transition#6A). The established rear end of the train is set to the Level transition border 8. When the train has passed the level transition border with its min safe rear end, i.e. when the whole train has left the HL3/HTD area, the ETCS On-board equipment of the leading engine sends a position report to the HL3/HTD Trackside. 9. ETCS On-board confirms integrity. 10. HL3/HTD Trackside receives a position report which allows the HL3/HTD Trackside to determine that the CRE is beyond the border for trains leaving the HL3/HTD Area. (in case of step 7 does not occur) 11. The HL3/HTD Trackside orders the train to terminate the communication session (leading and non-leading engines).

	12. The ETCS On-board equipment terminates the communication session. 13. HL3/HTD trackside no longer takes the train into consideration. All of its associated timers are discarded. 14. The level transition has finished.
Postcondition	ETCS On-board applies MA and track description for the new level.
Safety relation	The function Level Transition is safety relevant as part of ERTMS/ETCS system.
Open topics / consideration	What happens in case the HL3/HTD trackside doesn`t receive train integrity confirmation.

8.4.2 UC_04_02

Use Case Group	Level transitions
Use Case	Entering HL3/HTD Area
UC ID	**UC_04_02**
Main actor	HL3/HTD Trackside
Other actors	ETCS On-board, driver, OTI-I
Main goal	ID of the UC main goal: G_UC_04_02 Level transition to HL3/HTD from another Level.
Assumptions	1.- The L2 is supported by the ETCS On-board. 2.- Train fitted with OTI-I. 3.-The level transition order is immediate, not conditional. 4.- The level transition is not started by the driver. 5.- Not fallback situations. 6.- Unique Level transition (1, no more). 7.- No communication failures. 8.- TTD borders coincide with the Level Transition Border
Precondition	1.- Not Start of Mission. 2.- Neither Shunting Mode nor passive shunting, nor reversing mode, nor sleeping mode, nor NL (Non Leading) Mode, nor SB (Stand By). 3.- L2 is configured in ETCS On-board and at least one Mobile Terminal is available on-board, i.e. the ETCS On-board has detected at least one Mobile Terminal in working condition, independently whether it is registered to a network or not.

Flow of events	1. Level transition announcement in the DMI. 2. An order to connect to the HL3/HTD Trackside with a given id and telephone number is given via balise group in rear of the border location and ETCS On-board establishes Communication session with the HL3/HTD Trackside if not established before. 3. When the ERTMS/ETCS communication session is open, Train Data are sent to the HL3/HTD Trackside (which acknowledges the data). 4. ETCS On-board reports integrity confirmation. 5. Level 2 MA and track description information is received from the HL3/HTD trackside before the level transition border. 6. The ETCS On-board/driver is responsible for entering the level 2 HTD area at a speed not exceeding the speed limits of the previous level (1&2/NTC/0) 7. When the level transition location is passed with the estimated front end, a position report, including the new ETCS On-board level, is sent to the HL3/HTD Trackside. 8. The ETCS On-board equipment switchs to L2. 9. The train enters the HL3/HTD area and the first TTD in the HL3/HTD area becomes occupied 10. Mute Timer, Wait Integrity Timer and Shadow Train Timer assigned to the train and starts 11. The train reports position with integrity information in the HL3/HTD area and the first VSSs of the HL3/HTD area become ambiguous (#3A)
Postcondition	ETC On-board applies MA and track description for the HL3/HTD area.
Safety relation	The function Level Transition is safety relevant as part of ERTMS/ETCS system.

Open topics / consideration	What happens if the train cannot report integrity. The Infrastructure Manager shall configure the HL3/HTD Trackside options for authorising a train without integrity confirmed to move within or enter a HL3/HTD area. The Infrastructure Manager may conclude that, at certain locations, it is acceptable for trains to proceed into a HL3/HTD area with no fitted OTI-I or with a faulty OTI-I, or that they must be diverted, or the service terminated. The Infrastructure Manager may provide announcement signs for HL3/HTD areas to supplement the Driver's knowledge of the route or the announcement on the DMI may be considered sufficient. When OTI-I is not working or the train is not reporting train integrity confirmed and the HL3/HTD trackside is engineered not to authorise such trains to enter, the Dispatcher shall apply non-harmonised rules whether to authorise a train to enter a HL3/HTD area. In those circumstances when the system will not issue an MA into a HL3/HTD area because a train has not reported train integrity confirmed, the Dispatcher will need to authorise the Driver to use the Override procedure. Once the train enters the HL3/HTD area, it will be managed in accordance with loss of train integrity. How to allow the change of the first VSSs from ambiguous to occupied when the train is fully inside the HL3/HTD area The HL3/HTD area may not have information about the other level area. In order to change the concerned VSSs from ambiguous to occupied, the HL3/HTD trackside should have information of the last TTD in the other level area, if any, and it shall be able to define a shadow train timer for that TTD, in order to fulfil the #11A condition from the VSS state machine

8.5 LOSS OF COMMUNICATIONS

8.5.1 UC_05_01

Use Case Group	Loss of Communications
Use Case	Loss of Communication without re-connection
UC ID	**UC_05_01**
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside Dispatcher/Traffic Management System
Main goal	Train is at standstill and located in the area of the last granted MA. The VSSs of the TTDs where train could be located are set to Unknown to protect the train against movements of other trains in FS (safe situation).
Assumptions	A FS MA is not granted over Unknown VSSs. M_NVCONTACT is service break or emergency brake SR movements initiated by the driver are excluded
Precondition	Train is located on VSSs which are Occupied Train has a Movement Authority (FS or OS) over Free VSS in front of the train The mute timer of the train is started The train no longer sends train position reports The train is not in an RBC Handover Area

Flow of events	1. The mute timer expires. Trackside stores the memorised train location. The VSSs of the memorised train location become Unknown (transition #7A). The VSSs in advance of the memorised train location on occupied TTD and part of the MA become Unknown (transition #1B), too. The disconnect propagation timer for each VSS of the MA is started (for VSSs which became Unknown; 3.4.2.2.1 of HTD Principles [8]). 2. The train does not re-connect and the disconnect propagation timers expire. VSSs which are Free and adjacent to the MA area and on the same TTD become Unknown due to the propagation (#1C). 3. After T_NVCONTACT, the train starts to brake due to the configured reaction (i.e. service brake or emergency brake) and is finally at standstill. 4. After 5 minutes, the communication session is terminated by the train and by trackside.
Postcondition	Train is at standstill and located in the area of the last granted MA. VSSs of the TTDs where train could be located are set to Unknown.
Safety relation	It is safety related that the VSSs in unknown state cover the real position of the train. Under the specific application rules this state of the VSS can be used to perform non-harmonised safety related tasks, for example to decide if it is acceptable to open the barriers of a level crossing after a certain time.
Open topics / consideration	Correct configuration of the disconnect propagation timer is needed according to the rules of the specific application

8.6 LOSS OF INTEGRITY

8.6.1 UC_06_01

Use Case Group	Loss of Integrity
Use Case	Loss of Train Integrity during Normal Movement
UC ID	**UC_06_01**
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside
Main goal	ID of the UC main goal: G_UC_06_01 Recovering Normal Movement of train after loss of train Integrity during Normal Movement
Assumptions	• 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). • It is assumed that HL3/HTD Trackside is configured to keep on sending MAs to the trains.
Precondition	Train running in Normal Movement

Flow of events	1. Train running in Normal Movement. The HL3/HTD Trackside updates the Train Location with position reports. 2. Train reports loss of integrity (PR with "Train integrity lost"). The HL3/HTD Trackside updates the Front of the Train Location but does not update the CRE and changes the VSSs associated with the train to Ambiguous (transition #8A). Optionally, the Driver might be made aware of loss of train integrity. 3. Train continues moving. The ETCS On-board continues sending position reports without integrity confirmed. The HL3/HTD Trackside updates the Max Safe Front End and the VSSs are updated. 4. Train starts again to confirm train integrity, the VSSs left by train changes to Unknown (#10A) and these VSS becomes free when the TTD becomes free (#4A)
Postcondition	Train running in Normal Movement
Safety relation	
Open topics / consideration	Note that if the train reports "No train integrity information" for some time but without the Wait Integrity timer expiring, there is no reaction from the HL3/HTD Trackside.

8.6.2 UC_06_02

Use Case Group	Loss of Integrity
Use Case	EoM after Loss of Train Integrity
UC ID	**UC_06_02**
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside
Main goal	ID of the UC main goal: G_UC_06_02 Manage the EoM of train after loss of Train Integrity
Assumptions	The HL3/HTD Trackside can trust the information received from the On-board about the train integrity status (Q_LENGTH) and the safe train length (L_TRAININT). It is assumed that HL3/HTD Trackside is configured to keep on sending MAs to the trains.
Precondition	Train running in Normal Movement

Flow of events	1. Train running in Normal Movement. The HL3/HTD Trackside updates the Train Location with position reports. 2. Train reports loss of integrity (PR with “Train integrity lost”). The HL3/HTD Trackside updates the Front of the Train Location but does not update the CRE and set the VSSs to ambiguous (transition #8A). Optionally, the Driver might be made aware of loss of train integrity. 3. Train continues moving. The ETCS On-board continues sending position reports without integrity confirmed. The HL3/HTD Trackside updates the Max Safe Front End. 4. The train continues moving and stops near the EoA. The ETCS On-board sends a position report with train integrity lost. The HL3/HTD Trackside updates the Max Safe Front End. 5. The train performs EoM. a) The Driver closes the desk and ETCS On-board terminates the communication session with the HL3/HTD Trackside.
Postcondition	The ETCS On-board is in SB mode and no longer communicates with the HL3/HTD Trackside.
Safety relation	
Open topics / consideration	

8.6.3 UC_06_03

Use Case Group	Loss of Integrity
Use Case	Train does not confirm Integrity – Wait Integrity timer expires
UC ID	UC_06_03
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside
Main goal	Manage the expiration of Integrity wait timer without Integrity confirmation from train.
Assumptions	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). It is assumed that HL3/HTD Trackside is configured to keep on sending MAs to the trains.
Precondition	Train running in Normal Movement

Flow of events	1. Train running in Normal Movement. The HL3/HTD Trackside updates the Train Location with position reports. 2. Train reports “No train integrity information” while moving. The HL3/HTD Trackside updates the front of the Train Location. The rear of the train remains at the same location. 3. The train reports “No train integrity information” for longer than the wait integrity timer. The HL3/HTD Trackside considers the train integrity as lost. HL3/HTD changes the VSSs where the train is located to ambiguous (transition #8A). 4. The train continues moving and stops near the EoA. The HL3/HTD Trackside updates the Front of the Train Location. The rear of the train remains at the same location. 5. The train reports train integrity confirmed. When the conditions for the transition #11A are satisfied, the ambiguous state will be cleared
Postcondition	Train running in Normal Movement
Safety relation	
Open topics / consideration	

8.7 MOVEMENT IN STAFF RESPONSIBLE

8.7.1 UC_07_01

Use Case Group	Movement in Staff Responsible
Use Case	Movement in Staff Responsible with SR authorisation Note: there is another UC for Override scenarios
UC ID	UC_07_01
Main actor	Driver
Other actors	EVC, HL3/HTD Trackside, Dispatcher
Main goal	Staff Responsible (SR) mode is the primary means of moving communicating trains without a Train Location or communicating trains with Train Location when, for some reason, it is not possible to issue an MA. When in SR mode the ERTMS/ETCS on-board equipment shall supervise train movements against: • a ceiling speed: the staff responsible mode speed limit • a given distance: the staff responsible mode distance • a list of expected balise groups if this list has been sent by the RBC • balise groups giving the order ‘stop if in SR’ running in the direction opposite to the train orientation (reverse movement protection)

Assumptions	• Train keeps an open communication session with RBC. • The ERTMS/ETCS on-board shall determine the start location of the SR distance. • Since the gradient is unknown, the supervision of the braking curves in Staff Responsible mode does not ensure that the train will not pass the given distance. • When entering SR mode, the value applicable for SR mode speed limit and the value applicable for SR distance shall be the corresponding National/Default values. Exception for SR. distance: SR mode is authorised by RBC giving an SR distance. • The ERTMS/ETCS on-board equipment shall give the possibility to the driver to modify the value of the SR mode speed limit and of the given distance. This shall be possible only at standstill. • If a train movement is detected while the driver is entering the SR speed/distance limits, the ERTMS/ETCS on-board equipment shall trigger the brake command. • The driver shall have the possibility to request a new distance to run in Staff Responsible, by selecting "Start". This triggers an MA request. • If the train is in SR and receives a new distance to run in SR mode from the RBC, the stored list of expected balise groups, if any, shall be deleted or shall be replaced by the list of expected balise groups sent together with the distance to run in SR. If receiving a "track ahead free" request from the RBC, the ERTMS/ETCS on-board equipment requests the driver to enter the "track ahead free" information.
Precondition	Driver is executing a SoM or Train Trip procedure. Two possible scenarios: a) Train has a connection to the HL3/HTD Trackside but cannot be located due to invalid or unknown position. OR Train has a connection to the HL3/HTD Trackside and can be located, but it is not possible to issue an MA.

Flow of events	**Scenario 1** - Train has a connection to the HL3/HTD Trackside but cannot be located due to invalid or unknown position: 1. The VSS in the TTD where the train is located are in “unknown” status 2. The dispatcher may provide an estimated train position to the HL3/HTD Trackside. 3. The driver selects "start". 4. The HL3/HTD Trackside authorises the train for movement in SR with an SR distance and a list of balises that can be passed (based on the estimated train position provided by the dispatcher) engineered in such a way that allows the train to get valid location in a safe way. 5. The train moves in SR. 6. The train gets an unambiguous valid location and reports it to the RBC together with the train integrity information. 7. The VSS status under the train changes to “ambiguous” (transition #5A) 8. The VSS status when the train leaves the VSS with its confirmed rear end changes to “unknown” if the TTD remains occupied (transition #10A) **Scenario 2** - Train has a connection to the HL3/HTD Trackside and has reported an unambiguous valid location together with the train integrity information, but it is not possible to issue an MA: 1. The VSS status under the train is “ambiguous”. 2. The driver selects "start". 3. The HL3/HTD Trackside calculates the SR distance and a list of balises that can be passed, engineered in such a way that allows the train to move in SR in a safe way. 4. The HL3/HTD Trackside authorises the train for movement in SR. 5. The train moves in SR. 6. The VSS status when the train leaves the VSS with its confirmed rear end changes to “unknown” if the TTD remains occupied (#10A)
Postcondition	The driver is fully responsible for the train driving while in SR mode. The ERTMS/ETCS on-board equipment supervises a ceiling speed, a SR distance if finite and, if available, a list of balises.
Safety relation	The function of Movement in SR is safety relevant as part of ERTMS/ETCS system
Open topics / consideration	Extend the concept of balise groups sent by RBC in SR authorisation to take full advantage of the Digital Map. In the future, any designated point of the track on the map could be used as a reference 1D positioning.

8.8 RADIO HOLES

8.8.1 UC_08_01

Use Case Group	Radio Holes
Use Case	Train passes through Radio Hole within expected time
UC ID	**UC_08_01**
Main actor	ETCS On-board

Other actors	HL3/HTD Trackside
Main goal	Normal Movement through Radio Hole without an impact on following trains
Assumptions	• Radio Hole is pre-defined (Permanent or Temporary) • 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 and the borders of the Radio Hole coincide with TTD boundaries • Radio Hole timer start location is engineered in rear of the Radio Hole beginning by the distance depending on the length of the Mute timer
Precondition	Train running in Normal Movement (in FS or OS mode)
Flow of events	1. The HL3/HTD Trackside extends an MA for the train through the whole Radio Hole and sends track condition “radio hole” information to the ETCS On-board. 2. Train reports MaxSFE having passed the start location of the Radio Hole timer. The HL3/HTD Trackside updates the Front of the Train Location and starts the Radio Hole timer, stops supervising the Mute timer, the Wait Integrity timer and the ETCS session timer. 3. First TTD inside the Radio Hole becomes occupied. The status of the VSS inside the Radio Hole is changed to occupied (#2A). 4. Train continues moving but the ETCS On-board does not send position reports. 5. Train has passed the end location of the Radio Hole and re-establishes a communication session before the Radio Hole timer expires. 6. The ETCS On-board sends a position report with the train integrity confirmed. The HL3/HTD Trackside updates the Train Location of the train, updates the VSS status, stops the Radio Hole timer and starts supervising the Mute Timer, the Wait Integrity timer and the ETCS session timer.
Postcondition	Train running in Normal Movement. The VSS status inside the Radio Hole is free, unknown or occupied depending on the Train Location.
Safety relation	
Open topics / consideration	Preconfigured Temporary Radio Hole could be activated over more than one VSS, but it does not bring any operational benefits as an MA for a following train cannot end inside a Radio Hole (HL3/HTD trackside can only adjust a Train Location based on TTD occupancy).

8.8.2 UC_08_02

Use Case Group	Radio Holes
Use Case	Train passes through Radio Hole longer than expected time
UC ID	**UC_08_02**
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside
Main goal	Radio Hole timer expires and the VSS status is changed accordingly
Assumptions	• Radio Hole is pre-defined (Permanent or Temporary)

	• 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 and that the borders of the Radio Hole coincide with TTD boundaries. • Radio Hole timer start location is engineered in rear of the Radio Hole beginning by the distance depending on the length of the Mute timer
Precondition	Train running in Normal Movement (in FS or OS mode)
Flow of events	1. The HL3/HTD Trackside extends an MA for the train through the whole Radio Hole and sends the track condition "radio hole" information to the ETCS On-board. 2. Train reports MaxSFE having passed the start location of the Radio Hole timer. The HL3/HTD Trackside updates the Front of the Train Location and starts the Radio Hole timer, stops supervising the Mute timer, the Wait Integrity timer and the ETCS session timer. 3. First TTD inside the Radio Hole becomes occupied. The VSS status inside the Radio Hole is changed to occupied (#2A). 4. Train continues moving but the ETCS On-board does not send position reports. 5. Radio Hole timer expires and the HL3/HTD Trackside changes the status of the VSS inside the Radio Hole to unknown and extend "unknown" to the end of the last occupied TTD section within the MA and alerts the Dispatcher. 6. The non-communicating train continues moving and occupies next TTD, the HL3/HTD Trackside changes the status of all VSS within the TTD to unknown. 7. Train has passed the end location of the Radio Hole and re-establishes a communication session. 8. The ETCS On-board sends a position report with the train integrity confirmed. The HL3/HTD Trackside updates the Train Location of the train, updates the VSS status and starts supervising the Mute timer, the Wait Integrity timer and the ETCS session timer.
Postcondition	Train running in Normal Movement. The VSS status inside the Radio Hole is free, unknown or occupied depending on the Train Location.
Safety relation	
Open topics / consideration	Preconfigured Temporary Radio Hole could be activated over more than one VSS, but it does not bring any operational benefits as an MA for a following train cannot end inside a Radio Hole (HL3/HTD trackside can only adjust a Train Location based on TTD occupancy).

8.9 RELEASE OF POINTS

8.9.1 UC_09_01

Use Case Group	Release of points
Use Case	Release of points without dedicated TTDs
UC ID	**UC_09_01**
Main actor	Dispatcher/Traffic Management System

Other actors	Train ETCS On-board HL3/HTD Trackside
Main goal	The train overpass a point area, using the Confirmed Rear End to set the VSS, where the point is located, to free
Assumptions	• In this use case TTDs are not used to set the VSS that contains the point to free • The train is localised, and an MA can be assigned to it, with the packet 5 for linking (this is to avoid the condition of recalibration with unlinked balise groups) • The train has a short length (no more than 400 m) with good odometry
Precondition	
Flow of events	1. The Dispatcher/Traffic Management System sets the route to overpass the VSS where the point is located. The MA in FS is sent by the HL3/HTD Trackside to the ETCS On-board. The MA covers VSS1, VSS2, VSS3 and beyond (See Figure 18 below), the direction is from left to right; 2. The train proceeds setting the VSS in rear of the point area (VSS1 in Figure 18 below) to “occupied”. According to HTD_6 the VSS1 is set occupied with the max safe front end; 3. The train proceeds setting the VSS in the point area (VSS2 in Figure 18 below) to “occupied”. According to HTD_6 the VSS2 is set occupied with the max safe front end; 4. The train proceeds setting the VSS in rear of the point area (VSS1 in Figure 18 below) to “free”. This is achieved with the transition #6B; 5. The train proceeds setting the VSS in advance of the point area (VSS3 in Figure 18 below) to “occupied”. According to HTD_6 the VSS3 is set occupied with the max safe front end; 6. The train proceeds setting the VSS in the point area (VSS2 in Figure 18 below) to “free”. This is achieved with the transition #6B;
Postcondition	The Use case is successful if the HL3/HTD Trackside is able to determine that the VSS where the points are located is free. This condition (VSS of the point free) can be used as a condition for the movement of the point
Safety relation	All Events are safety relevant

Open topics / consideration	In general the odometric error can have a big impact in this kind of scenario when the TTDs are not used. To try to avoid an increased time of occupation of the point are it seems advisable that recalibration balise groups are placed to minimise the odometric error, in the following locations: • A certain distance in rear of the border between VSS1 and VSS2, in order to avoid the occupation of VSS2 when the real front end is far from the border; • A certain distance in advance of the border between VSS2 and VSS3, in order to anticipate as much as possible the liberation of the VSS2. This distance should be the medium distance between the rear end of the train and the eurobalise antenna, calculated on the basis of the trains that are usually present on the line (see Figure 19 to set VSS3 to free); Similar engineering is expected to be possible in case of use of ASTP (Absolute Safe Train Positioning). (NOTE: The critical case of loss of connection or similar degraded situations will be matter of the following use case)

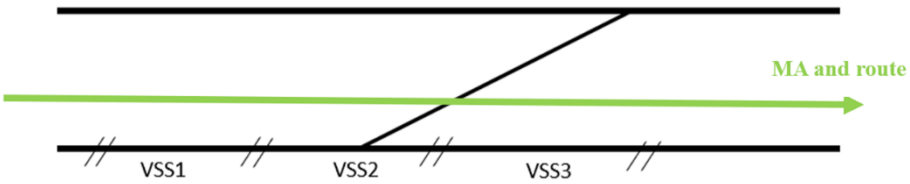

Figure 18: VSS positioning

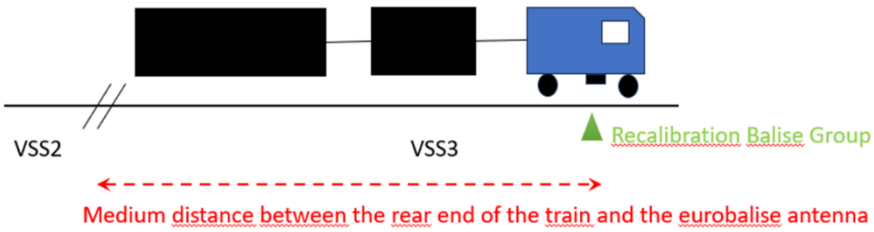

Figure 19: Recalibration Balise Group

8.9.2 UC_09_02

Use Case Group	Release of points
Use Case	Release of points without dedicated TTDs (Loss of connection)
UC ID	**UC_09_02**
Main actor	Dispatcher/Traffic Management System
Other actors	Train ETCS On-board HL3/HTD Trackside

Main goal	The train overpass a point area, using the Confirmed Rear End to set the VSS, where the point is located, to free
Assumptions	• In this use case TTDs are not used to set the VSS that contains the point to free • The train is localised and an MA can be assigned to it, with the packet 5 for linking (this is to avoid the condition of recalibration with unlinked balise groups)
Precondition	
Flow of events	1. The Dispatcher/Traffic Management System sets the route to overpass the VSS where the point is located. The MA in FS is sent by the HL3/HTD Trackside to the ETCS On-board. The MA covers VSS1, VSS2, VSS3 and beyond (See Figure 20), the direction is from left to right; 2. The train proceeds setting the VSS in rear of the point area (VSS1 in the figure below) to "occupied". According to to HTD_6 the VSS1 is set occupied with the max safe front end; 3. There is a loss of connection with the train. According to the transition #1B all the VSSs the MA (taking into account that there is no separate TTD for the area of the point) are set to unknown; 4. The VSSs will be set to free only when the corresponding TTD will be set to free (Transition #4A) or with sweeping of the following train. This is likely to be achieved when the train will be moved by non-harmonised operational procedures
Postcondition	The Use case is successful if the HL3/HTD Trackside is able to determine that the VSS where the points are located is free. This condition (VSS of the point free) can be used as a condition for the movement of the point.
Safety relation	All Events are safety relevant.
Open topics / consideration	This is the critical scenario in case there is no separate TTD for the area where the point is located. The point area can remain blocked for a long time, if the occupation of the VSSs blocks the movement of the points (common engineering across Europe, even if not harmonised). To mitigate the impact, a more complex of propagation may be used according to clause 5.2.1.8 of the HTD Guideline. Another solution is the use of dedicated TTDs for the point areas (see the following use case)

8.9.3 UC_09_03

Use Case Group	Release of points
Use Case	Release of points with dedicated TTDs
UC ID	**UC_09_03**
Main actor	Dispatcher/Traffic Management System
Other actors	Train ETCS On-board HL3/HTD Trackside
Main goal	The train overpass a point area, using the Confirmed Rear End to set the VSS, where the point is located, to free

Assumptions	• In this use case TTDs are used to set the VSS the contains the point to free • The train is localised and an MA in Full Supervision can be assigned to it
Precondition	
Flow of events	1. The Dispatcher/Traffic Management System sets the route to overpass the VSS where the point is located. The MA in FS is sent by the HL3/HTD Trackside to the ETCS On-board. The MA covers VSS1, VSS2, VSS3 and beyond (See Figure 20 below), the direction is from left to right; 2. The train proceeds setting the VSS in rear of the point area (VSS1 in Figure 20 below) to “occupied”. According to the HTD_6 the VSS1 is set occupied with the max safe front end; 3. The train proceeds setting the VSS in the point area (VSS2 in Figure 20 below) to “occupied”. This is done when the TTD that covers VSS2 is occupied, according to the transition #2A; 4. The train proceeds setting the VSS in rear of the point area (VSS1 in Figure 20 below) to “free” because the TTD that contains VSS1 becomes free. This is achieved with the transition #6A; 5. The train proceeds setting the VSS in advance of the point area (VSS3 in Figure 20 below) to “occupied”. This is done when the TTD that contains VSS3 is occupied, according to the transition #2A; 6. The train proceeds setting the VSS in the point area (VSS2 inFigure 20 below) to “free”. This is achieved with the transition #6A;
Postcondition	The Use case is successful if the HL3/HTD Trackside is able to determine that the VSS where the points are located is free. This condition (VSS of the point free) can be used as a condition for the movement of the point
Safety relation	All Events are safety relevant
Open topics / consideration	In the steps 4 and 6 it is assumed that the liberation of the TTD is faster than the reporting of the confirmed rear end in advance of the related TTD. This is expected to be true quite often, but if it is not verified (for example because of delays in the interface RBC-Interlocking, transition #6B will be used instead. In this second case the odometric error may become relevant as in use case UC_09_03

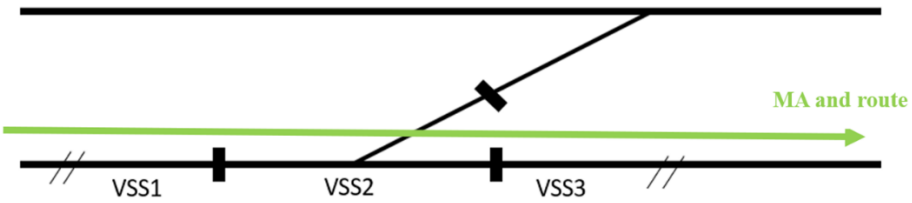

Figure 20: Release of points with dedicated TTD

8.10 REVERSING

8.10.1 UC_10_01

Use Case Group	Reversing
Use Case	Reversing in HL3/HTD Area
UC ID	**UC_10_01**
Main actor	Dispatcher/Traffic Management System
Other actors	Train ETCS On-board HL3/HTD Trackside Driver
Main goal	The train performs Reversing in order to escape a danger situation
Assumptions	Reversing operation is not normal operation on the line, it is used only to escape from a danger situation
Precondition	
Flow of events	1. The train is in a reversing area; 2. The driver puts the direction controller in reverse position and acknowledges the transition to Reversing Mode; 3. The HL3/HTD Trackside receives the position report of the train in reversing, considers the train as not integer anymore according to the condition g) of HTD_46 and sets the VSSs where the train is located to ambiguous according to the transition #8A. Train Integrity Loss Propagation Timer is started. The HL3/HTD Trackside sends a maximum distance to run in reverse movement; 4. The train moves in reverse direction
Postcondition	The Use case is successful if the ETCS on board is able to perform reversing to escape the danger situation.
Safety relation	All Events are safety relevant
Open topics / consideration	

8.11 SHUNTING

8.11.1 UC_11_01

Use Case Group	Shunting
Use Case	Train enters an active Shunting Area and changes to SH mode
UC ID	**UC_11_01**
Main actor	Dispatcher/Traffic Management System

Other actors	Train ETCS On-board HL3/HTD Trackside Driver
Main goal	HL3/HTD Trackside authorises a train to enter an active Shunting Area in OS mode. When the train is located inside the active Shunting Area, Driver selects Shunting and HL3/HTD Trackside sends SH authorisation to the train. Train changes to SH mode and ends its mission.
Assumptions	• In the nominal case, the HL3/HTD Trackside does not authorise a train to change to SH mode while its location is not fully inside a Shunting Area, regardless of whether the Shunting Area is active or not; • The boundaries of a Shunting Area are marked at the trackside somehow, e.g. by a marker board, based on how the Shunting Area is engineered; • The borders of a Shunting Area coincide with TTD boundaries;
Precondition	Train is on the approach to an active Shunting Area. The last TTD in rear of the Shunting Area is occupied. The corresponding VSS is in the state occupied.
Flow of events	1. Dispatcher or Traffic Management System requests a path for the train to enter the Shunting Area. The HL3/HTD Trackside sends a MA to enter the shunting area in On Sight. The train moves. 2. When one of the following events happens: a. the last TTD in rear of the shunting area becomes free; b. The ETCS On-board reports its Confirmed Rear End inside the Shunting Area The VSS in rear of the shunting area becomes free because of transitions #6A or #6B . The HL3/HTD Trackside deems that the train entered the shunting area and can send optionally a text message to the driver to indicate the possibility to select Shunting. 3. The train stops and the ETCS On-board reports standstill to the RBC. The Driver selects Shunting, the ETCS On-board sends a request for Shunting to the HL3 Trackside, the HL3/HTD Trackside replies with the authorisation for shunting; 4. The ETCS On-board changes to SH mode, reports the change of mode to the HL3 Trackside and performed End of Mission. Disconnect propagation timer is started according to the configuration of the Specific Application. 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.
Postcondition	The Use case is successful if the ETCS on board changes to Shunting Mode. The use case fails in case it is not possible to establish that the train is completely inside the shunting area, this is the case when both these events are fulfilled: • The last TTD in rear of the shunting area remains occupied; • The ETCS On-board is not able to send the Confirmed Rear End inside the shunting area; In this case it is not possible to authorise shunting with normal procedures

Safety relation	All Events are safety relevant
Open topics / consideration	Some specific applications may deem useful to keep track of the total length of the trains present in the shunting area. This is possible only if the shunting area is completely in HL3/HTD area and there are no ghost or shadow trains and there is a way to satisfy assumption [Pre 15]

8.11.2 UC_11_02

Use Case Group	Shunting
Use Case	Temporary Shunting Area activated
UC ID	**UC_11_02**
Main actor	Dispatcher/Traffic Management System
Other actors	Train ETCS On-board HL3 Trackside Driver
Main goal	HL3/HTD Trackside authorises a train to enter a temporary Shunting Area in OS mode. When the train is located inside the active Shunting Area, Train changes to SH mode and ends its mission.
Assumptions	• In the nominal case, the HL3/HTD Trackside does not authorise a train to change to SH mode while its location is not fully inside a Shunting Area, regardless of whether the Shunting Area is active or not; • Adequate mitigations have been taken in order to avoid that a roll away vehicle escaping the temporary shunting area impacts with a train, for example derailing points or no extension of the MA of the train in the proximity of the shunting area
Precondition	A train has occupied a VSS section where there is the possibility to activate a temporary shunting area. The status of the VSSs inside the zone is occupied
Flow of events	1. The Dispatcher or the Traffic Management System informs the driver that a temporary shunting area will be activated (probably with the information regarding what the driver has to do, this information may be with a text message or by a phone call or by other means, it is a matter of the specific application). The Dispatcher or the Traffic Management System activates the shunting area. The HL3 Trackside performs successfully the checks according to the specific application and activates the area; 2. The HL3/HTD Trackside performs successfully the checks according to the specific application and activates the area and sends an MA with a Shunting Mode Profile for the current location of the train; 3. ETCS On-board changes to SH mode, reports the change of mode to the HL3/HTD Trackside and performs End of Mission. The driver is requested to acknowledge the mode change to SH and does that. There is the start of a disconnect propagation timer according to the configuration of the specific application. Optionally the HL3/HTD Trackside can add the length of the train to the total length of trains present in the Shunting Area. The VSSs where the train is located becomes unknown (transition #7A)

Postcondition	The use case has success if the train is able to enter the Temporary Shunting Area. The use case fails in case the checks defined by the specific application for the temporary shunting area are not fulfilled
Safety relation	All Events are safety relevant
Open topics / consideration	The activation of a shunting area to reconnect a lost vehicle after train integrity loss may be interesting in some low traffic applications. Anyway, adequate mitigations have to be taken in that case.

8.11.3 UC_11_03

Use Case Group	Shunting
Use Case	Train leaves an active Shunting Area with MA
UC ID	**UC_11_03**
Main actor	Driver
Other actors	• Dispatcher/Traffic Management System • ETCS On-board • HL3/HTD Trackside • Train
Main goal	A train is at standstill at a location close to the border of an active Shunting Area, following completion of movements in SH mode. The Driver performs SoM and the train receives an MA to leave the active Shunting Area.
Assumptions	• After Shunting operation, a train is close to the border of the Shunting Area, beyond possible points, so that no obstruction can be present between the train and the boundary of the Shunting Area; when approaching the boundary of the Shunting Area the train has passed over balises while shunting, enabling it to provide a position which is unambiguous to the HL3/HTD Trackside; • A Shunting Area is protected; possible means of preventing trains operating in SH mode from leaving a designated Shunting Area include derailing points, balises with "Danger for Shunting information" and a list of balise group(s) the train can pass over in SH mode. • Appropriate mitigations, like the use of TTDs, are taken in order to avoid that a shadow vehicle can be in rear of the reporting train
Precondition	A train has finished shunting and it is localised inside the shunting area, close to the border, with a valid position

Flow of events	1. Driver selects “exit Shunting” and performs SoM 2. ETCS On-board sends a SoM position report with the train data 3. HL3/HTD Trackside acknowledges the train data 4. Dispatcher/Traffic Management System authorises the movement of the train. 5. HL3/HTD Trackside checks the condition to assign an MA and sends a MA with an OS mode profile to exit the shunting area 6. ETCS On-board receives the MA and requests the Driver to acknowledge the mode change to OS; after receiving the Driver’s acknowledgment, ETCS On-board changes to OS mode 7. When the ETCS On-board reports its max front end outside the Shunting Area, the VSS where the train is located become ambiguous (transition #3A)
Postcondition	The Use Case is successfully completed if the trains moves outside the Shunting Area with a MA. The use case fails in case it is possible to send a MA to the train
Safety relation	All Events are safety relevant
Open topics / consideration	

8.11.4 UC_11_04

Use Case Group	Shunting
Use Case	Temporary Shunting Area deactivated
UC ID	**UC_11_04**
Main actor	Driver
Other actors	Dispatcher/Traffic Management System ETCS On-board HL3/HTD Trackside Train
Main goal	Performs the shunting and deactivates the temporary Shunting Area
Assumptions	
Precondition	The last train in the shunting area has finished shunting. The Dispatcher/Traffic Management System has been informed by specific application operational procedures.

Flow of events	1. Driver selects “exit Shunting” and performs SoM 2. ETCS On-board sends a SoM position report with a valid position and sends the train data; 3. Dispatcher requests to HL3/HTD Trackside a route for the train; 4. HL3 Trackside checks the condition to assign an MA and sends a MA with an OS mode profile to exit the shunting area 5. ETCS On-board receives the MA and requests the Driver to acknowledge the mode change to OS; after receiving the Driver’s acknowledgment, ETCS On-board changes to OS mode 6. When the ETCS On-board reports its max front end outside the Shunting Area, the VSS section where it is located becomes ambiguous (transition #3A) . 7. The Dispatcher/Traffic Management System deactivates the Shunting Area after the specific application verifications. 8. The VSSs that were in the Shunting Area are set to free by the HL3/HTD Trackside
Postcondition	The Use Case is successfully completed if the Temporary Shunting Area is deactivated. The use case fails in case it is not possible to deactivate the Shunting Area
Safety relation	All Events are safety relevant
Open topics / consideration	

8.12 SPLITTING

This use case refers to splitting of a train whose integrity is confirmed on-board. The train to be split is a composition of two trainsets, each with driving cab. Two possible alternatives are described.

Alternative 1

The following use case refers to the case where “train 2” resulting from splitting remains not connected to trackside.

8.12.1 UC_12_01

Use Case Group	Splitting
Use Case	Splitting of a train with integrity confirmed Alternative 1
UC ID	**UC_12_01**
Main actor	HL3/HTD Trackside
Other actors	ETCS On-board, driver, OTI-I OTI-L
Main goal	A train splits and there are two resulting trains. “Train 2” resulting from splitting remains not connected to trackside “Train 1” can start a new mission

Assumptions	• A train to be split. • Train is at standstill. • The train has no faults. • The Cab Activation, transition from NP to SB, provide the OTI-I and OTI-L reset.
Precondition	The train (cab of trainset 1) is in FS and communicating with the HL3/HTD Trackside - the cab of trainset 2 is in NL or SL mode
Flow of events	1. Trainset 1-2 has entered from the left side with an FS MA until end of VSS 12 (see Figure 21) and occupies VSS 12. It has stopped. 2. Train 1 and 2 are split. Train 1 remains connected with the trackside and reports train integrity lost. The cab of train 2 is closed, the mode change to SB is reported to trackside and train 2 remains disconnected and starts the train integrity evaluation by OTI-I. On the train 1 the Cab Activation is performed. FS –> NP and NP –> SB transition, the OTI-I starts the train integrity evaluation. On the train 1 the SoM is performed. Except for the reporting of the mode change, train 2 is not connected to the trackside. Until the newly reported train data train length of train 1 is acknowledged by the trackside, train 1 can only send "no info" for the integrity status . Due to the reported change of train data train length, train 1 is not treated as integer anymore (train1 is also in a VSS where disconnected train 2 is) and as a consequence VSS 12 becomes “ambiguous” (#8A). The moment of change of train data train length is the start of a timer for integrity loss related to VSS12. 3. Train 1 receives an MA (with optionally for VSS 12 an OS mode profile) until end of VSS 33, starts to run again, passes the TTD section border, and reports its position on VSS 21, which becomes “ambiguous” (#3A). VSS 12 becomes "unknown" (#10A). 4. Train 1 moves on to VSS 22, which becomes “ambiguous” (#3A). VSS 21 becomes "unknown" (#10A) 5. Train 1 moves on to VSS 23, which becomes “ambiguous” (#3A). VSS 22 becomes "unknown" (#10A). At the expiration of the integrity loss propagation timer, configured according to the safety analysis for trackside, after VSS12 has been declared “ambiguous”, all VSS in TTD 10 become “unknown” (#1E) 6. Train 1 moves to VSS 31, with the physical rear still in VSS 23. VSS 31 becomes “ambiguous” (#3A) and VSS 23 remains "ambiguous" 7. When Train 1 has physically left VSS 23, TTD 20 becomes “free”. As a consequence, VSS 21, 22 and 23 (all VSS sections in TTD 20) go to “free” (#4A for VSS 21, 22 and #9A for VSS 23). Because TTD 20 is free, the established rear end of the train location of train 1 is moved to the border between TTD 20 and TTD 30. Train 1 is now located on VSS 31 and, if the time elapsed between the moment the TTD has become free and the moment the trackside processes this information is sufficiently short, the trackside can consider that no vehicle may be located between TTD border and rear end of the train 1. The trackside considers therefore train 1 as integer and not followed by any ghost train. (transition #11A) 8. Train 1 reports its position, including the confirmed rear end, inside VSS 31. This has no further effect.
Postcondition	The train is split. Train 1 moves normally and train 2 can perform SoM
Safety relation	The splitting is safety relevant.

Open topics / consideration	

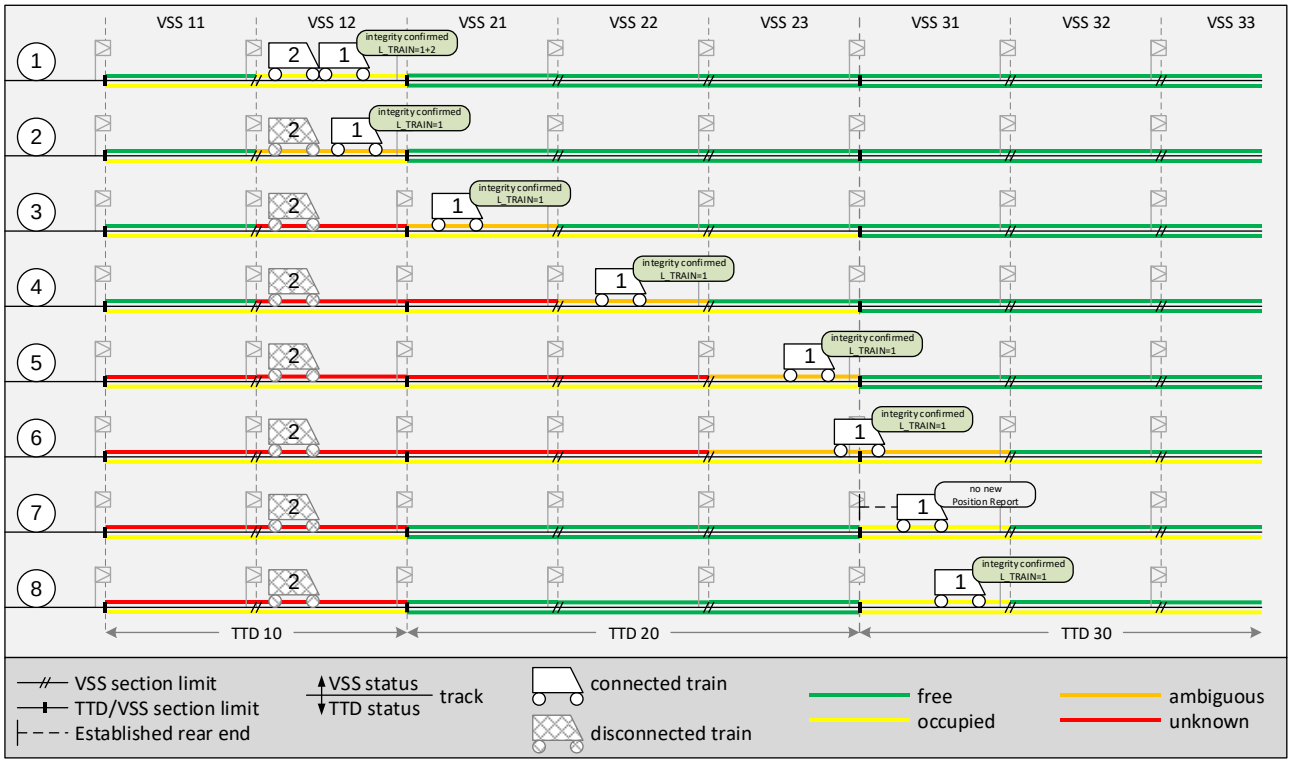

Figure 21: Splitting steps description.

Alternative 2

In this use case Train 2, after splitting, performs SoM and reports its length.

The trackside waits for the SoM of trains 2 and checks that the sum of the reported lengths of train 1 and train 2 is equal to the length of the initial train. This could permit the trackside to consider train 1 integer with no possible ghost train following it. Assumption [Pre 15] shall be satisfied to allow this use case and there shall be an association between the 2 splitted trains in order to make the operations on the train lengths.

8.12.2 UC_12_02

Use Case Group	Splitting
Use Case	Splitting of a train with integrity confirmed Alternative 2
UC ID	**UC_12_02**
Main actor	L2 + HTD Trackside
Other actors	ETCS On-board, driver, OTI-I OTI-L
Main goal	A train splits and there are two resulting trains. Boths Trains resulting from splitting can start a new mission

Assumptions	• A train to be split. • Train is at standstill. • The train has no faults • The Cab Activation, transition from NP a SB, provide the OTI-I and OTI-L reset. • After splitting the trackside waits the SoM of both trains for a defined timer. To be configured in the trackside specific application.
Precondition	The train (cab of trainset 1) is in FS and communicating with the L2 + HL3/HTD Trackside - the cab of trainset 2 is in NL or SL mode
Flow of events	1. Trainset 1-2 has entered from the left side with an FS MA until end of VSS 12 and occupies VSS 12. It has stopped. The TTD in advance to train 1 and in the rear of train 2 are free. 2. Train 1 and 2 are split. Train 1 remains connected with the trackside and reports train integrity lost. The moment of report of train integrity lost is the start of a timer for integrity loss related to VSS12. The cab of train 2 is closed, the mode change to SB is reported to trackside and train 2 remains disconnected and starts the train integrity evaluation by OTI-I. On the train 1 the Cab Activation is performed. FS –> NP and NP –> SB transition, the OTI-I starts the train integrity evaluation. On the train 1 the SoM is performed. Except for the reporting of the mode change, train 2 is not connected to the trackside. Until the newly reported train data train length of train 1 is acknowledged by the trackside, train 1 can only send "no info" for the integrity status (see CR940). Due to the reported change of train data train length, train 1 is not treated as integer anymore (train1 is also in a VSS where disconnected train 2 is) and as a consequence VSS 12 becomes “ambiguous” (#8A). 3. Train 2 performs the SB –> NP and NP –> SB transitions (it is doing the Cab Activation) the OTI-I starts the train integrity evaluation. Train 2 performs SoM and reports its length this ensures that no movement inserting vehicles in the rear, in advance or in between train 1 and train 2 has occurred. Until the newly reported train data train length of train 2 is acknowledged by the trackside, train 2 can only send "no info" for the integrity status. 4. The RBC has the train length of both trains. It can check that the sum of the two values is the same of the previous train set (Train 1 + train 2). . If the check is positive and the TTD in advance and in the rear do not have changed state from the step 1, the trackside can consider train 1 and train 2 integer. The timer related to the delay for integrity loss may be stopped and train 1 may receive a MA according to the “normal” SoM use case.
Postcondition	The original train is split. The two trains (Train 1 and Train 2) can move normally
Safety relation	The splitting is safety relevant.
Open topics / consideration	This requires some additional functionality in comparison to the EUG specification [8]

8.13 SWEEPING

The sweeping mechanism allows clearing VSS with state "unknown" without waiting until the TTD becomes free.

8.13.1 UC_13_01

Use Case Group	Sweeping
Use Case	Nominal Sweeping
UC ID	**UC_13_01**
Main actor	Dispatcher/Traffic Management System
Other actors	Driver ETCS On-board HL3/HTD Trackside Train
Main goal	HL3/HTD Trackside authorises a train to enter a VSS section in “unknown” status to bring this section to the state “occupied” and resume the normal operation of HL3/HTD Specific Application.
Assumptions	•
Precondition	At least a VSS section has the status “unknown”. The train is in FS and communicating with the HL3/HTD Trackside. There is no storage of the data according to the requirements ADD_0009 and ADD_0023, otherwise sweeping gives no added benefit, it is more a joining scenario.
Flow of events	1. Dispatcher/Traffic Management System authorises a train to sweep the unknown VSS; 2. The driver of the train and the ETCS On-board get some sort of authorisation (it may be an MA or a SR Authorisation with a written order etc.) to enter the unknown VSS 3. The train proceeds and enter the “Unknown” VSS section; 4. The transition #12B is performed and the VSS becomes occupied. The disconnect propagation timer related to the VSS is stopped. 5. The train proceeds, setting the left VSS to free according to transition #6B
Postcondition	The Use Case is successfully completed if the VSS that was in state unknown is set to free
Safety relation	All Events are safety relevant.
Open topics / consideration	

8.13.2 UC_13_02

Use Case Group	Sweeping
Use Case	Sweeping with MA and expiration of the disconnect/integrity loss propagation timer
UC ID	**UC_13_02**
Main actor	Dispatcher/Traffic Management System

Other actors	Driver ETCS On-board HL3/HTD Trackside Train
Main goal	HL3/HTD Trackside authorises a train to enter a VSS section in “unknown” status in order to bring this section to the state “occupied” and resume the normal operation of HL3/HTD Specific Application. With MA and expiration of the disconnect/integrity loss propagation timer
Assumptions	• There is no real train in the “Unknown” VSS section
Precondition	At least a VSS section has the status “unknown”. There is no storage of the data according to the requirements ADD_0009 and ADD_0023, otherwise sweeping gives no added benefit, it is more a joining scenario.
Flow of events	1. Dispatcher/Traffic Management System authorises a train to sweep the unknown VSS; 2. The driver of the train and the ETCS On-board gets an MA to enter the unknown VSS 3. While the train proceeds, a disconnect or integrity loss propagation timer expires. According to transition #1C all the VSS in the same TTD of the unknown VSS become unknown. The VSSs in the other TTDs that are part of the MA are not affected according to transition #1D 4. Dispatcher/Traffic Management System authorises the train to sweep the other unknown VSSs that are generated by the propagation timer; 5. The train proceeds and enter the first unknown VSS; 6. The transition #12B is performed and the VSS becomes occupied. The disconnect propagation timer related to the VSS is stopped; 7. The train proceeds, setting to the following VSS to occupied according to transition #12B. The disconnect propagation timer related to the VSS is stopped; 8. The train proceeds, setting the left VSS to free according to transition #6B
Postcondition	The Use Case is successfully completed if the VSS that was in state unknown is set to free
Safety relation	All Events are safety relevant
Open topics / consideration	

8.13.3 UC_13_03

Use Case Group	Sweeping
Use Case	Sweeping with SR Authorisation and expiration of the disconnect/integrity loss propagation timer
UC ID	**UC_13_03**
Main actor	Dispatcher/Traffic Management System
Other actors	Driver ETCS On-board HL3/HTD Trackside Train

Main goal	HL3/HTD Trackside authorises a train to enter a VSS section in “unknown” status in order to bring this section to the state “occupied” and resume the normal operation of HL3/HTD Specific Application. With SR Authorisation and expiration of the disconnect/integrity loss propagation timer .
Assumptions	• There is no real train in the “Unknown” VSS section
Precondition	At least a VSS section has the status “unknown”. There is no storage of the data according to the requirements ADD_0009 and ADD_0023, otherwise sweeping gives no added benefit, it is more a joining scenario.
Flow of events	1. Dispatcher/Traffic Management System authorises a train to sweep the unknown VSS; 2. The driver of the train and the ETCS On-board gets a SR Authorisation to enter the unknown VSS; 3. While the train proceeds, a disconnect or integrity loss propagation timer expires. According to transition #1C all the VSS in the same TTD of the unknown VSS become unknown. The VSSs in the other TTDs are affected according to transition #1D 4. Dispatcher/Traffic Management System authorises the train to sweep the other unknown VSSs that are generated by the propagation timer; 5. The train proceeds and enter the first unknown VSS; 6. The transition #12B is performed and the VSS becomes occupied. The disconnect propagation timer related to the VSS is stopped; 7. The train proceeds, setting to the following VSS to occupied according to transition #12B . The disconnect propagation timer related to the VSS is stopped; 8. The train proceeds, setting the left VSS to free according to transition #6B ; 9. Steps from 11 to 13 are repeated until the liberation of all the unknown VSSs
Postcondition	The Use Case is successfully completed if the VSS that was in state unknown is set to free
Safety relation	All Events are safety relevant
Open topics / consideration	

8.13.4 UC_13_04

Use Case Group	Sweeping
Use Case	Sweeping with expiration of the ghost train propagation timer and detection at the TTD border
UC ID	**UC_13_04**
Main actor	Dispatcher/Traffic Management System
Other actors	Driver ETCS On-board HL3/HTD Trackside Train
Main goal	HL3/HTD Trackside authorises a train to enter a VSS section in “unknown” status in order to bring this section to the state “occupied” and resume the

	normal operation of HL3/HTD Specific Application. With expiration of the ghost train propagation timer and detection at the TTD border.
Assumptions	• There is no real train in the unknown VSSs
Precondition	A TTD has become occupied, and a ghost train has been determined according to the transition #1A
Flow of events	1. Dispatcher/Traffic Management System authorises a train to sweep the unknown VSS; 2. The driver of the train and the ETCS On-board get some sort of authorisation (it may be an MA or a SR Authorisation with a written order etc.) to enter the unknown VSSs in the TTD where the ghost train was determined 3. While the train proceeds, the ghost train propagation timer expires and it is stopped according to the requirements HTD_33 and HTD_40 but detection at the TTD border excludes the passage of a vehicle. According to transition #1G no propagation occur 4. The train proceeds and enter the first unknown VSS; 5. The transition #12B is performed and the VSS becomes occupied; 6. The train proceeds, setting to the following VSS to occupied according to transition #12B ; 7. The train proceeds, setting the left VSS to free according to transition #6B ; 8. Steps from 6 to 8 are repeated until the liberation of all the unknown VSSs
Postcondition	The Use Case is successfully completed if the VSSs that were in state unknown are set to free
Safety relation	All Events are safety relevant
Open topics / consideration	

8.13.5 UC_13_05

Use Case Group	Sweeping
Use Case	Sweeping with expiration of the ghost train propagation timer and no detection at the TTD border
UC ID	**UC_13_05**
Main actor	Dispatcher/Traffic Management System
Other actors	Driver ETCS On-board HL3/HTD Trackside Train
Main goal	HL3/HTD Trackside authorises a train to enter a VSS section in “unknown” status in order to bring this section to the state “occupied” and resume the normal operation of HL3/HTD Specific Application. With expiration of the ghost train propagation timer and no detection at the TTD border.
Assumptions	• There is no real train in the unknown VSSs

Precondition	A TTD has become occupied, and a ghost train has been determined according to the transition #1A The sweeping train is in the adjacent TTD
Flow of events	1. Dispatcher/Traffic Management System authorises a train to sweep the unknown VSS; 2. The driver of the train and the ETCS On-board get some sort of authorisation (it may be an MA or a SR Authorisation with a written order etc.) to enter the unknown VSSs in the TTD where the ghost train was determined 3. While the train proceeds, the ghost train propagation timer expires and it is stopped according to the requirements HTD_33 and HTD_40. According to transition #1G propagation occurs and all the VSS in advance of the sweeping train are set to unknown; 4. The driver of the train and the ETCS On-board get some sort of authorisation (it may be an MA or a SR Authorisation with a written order etc.) to enter the unknown VSSs in advance of the train 5. The train proceeds and enter the first unknown VSS; 6. The transition #12B is performed and the VSS becomes occupied.; 7. The train proceeds, setting to the following VSS to occupied according to transition #12B; 8. The train proceeds, setting the left VSS to free according to transition #6B ; 9. Steps from 6 to 8 are repeated until the liberation of all the unknown VSSs
Postcondition	The Use Case is successfully completed if the VSSs that were in state unknown are set to free
Safety relation	All Events are safety relevant
Open topics / consideration	If the ghost train propagation timer expires when the sweeping train is still far away from the unknown VSSs, it is possible that the propagation will not occur. In this case

8.14 TRACKSIDE INITIALISATION

8.14.1 UC_14_01

Use Case Group	Trackside Initialisation
Use Case	Initialisation with Track Circuits TTDs
UC ID	**UC_14_01**
Main actor	Maintainer/Dispatcher
Other actors	Driver ETCS On-board HL3/HTD Trackside Train
Main goal	After a shutdown the HL3/HTD shall resume normal operation

Assumptions	• After the shutdown all the trains that were circulating on the line were stopped, for example because of the expiration of the T_NVCONTACT. Even ghost trains are stopped in some way; • Track Circuits are used on the line; • The Initial State of all the VSSs is "unknown" according to the requirement 5.1.1.4 of the HTD Principles [8];
Precondition	Shutdown is an unexpected event. In case the line goes in shutdown when it is not used, it is assumed that no trains are present on the line
Flow of events	1. The maintainer or dispatcher switches on the HL3/HTD Trackside. The status of the occupied track circuits is received by the RBC. All the VSSs in the occupied TTDs remain unknown and the ghost train propagation timer is started, the others are set to free according to the transition #4A; 2. The trains on the line connect with the RBC. All the sections where a front end of a train is located are set to ambiguous according to the transition #5A ; 3. Non harmonised operation procedures need to apply, in order to resume normal operation. Probably trains need to be moved in order to set the VSSs to free, when there is a TTD border it is in principle possible to trigger transition #11A and set the relevant VSS to occupied
Postcondition	Recovery of normal operation, with all the VSSs in state "occupied" or "free"
Safety relation	All Events are safety relevant
Open topics / consideration	In case of use of axle counters on the line, it is assumed that there are technological features (storage of the state of the section) to use the same scenario

8.15 USE OF RESERVED

P.M. The use of Reserved was not deemed useful in the context of HL3/HTD

8.16 INTERACTION BETWEEN HL3/HTD AND ATO

8.16.1 UC_16_01

Use Case Group	Interaction between HL3 and ATO
Use Case	Use of ATO to set a TTD to free
UC ID	**UC_16_01**
Main actor	HL3/HTD Trackside
Other actors	Traffic Management System (in this case it is not feasible to have a manual dispatcher) ATO-Trackside ATO-On-board ETCS-On-Board Train
Main goal	Setting a TTD to free for the particular uses connected to HL3/HTD (for example to trigger the transition #11A or to check if a TTD is not failed i.e. it is not able anymore to make the transition from occupied to free)

Assumptions	
Precondition	In 3 subsequent TTDs with various VSSs in each TTDs, there are various trains with ATO. There is the need to set the intermediate TTD (TTD2 in the following) to free. The trains are proceeding in the direction from TTD1 to TTD3
Flow of events	1. The HL3/HTD Trackside determines that there is a need to set TTD2 to free; 2. ATO-Trackside sends appropriate journey profiles to: • accelerate the trains in TTD2 towards TTD3 in order to set TTD2 to free; • Stopping all the trains in TTD1 in order to avoid that they occupy TTD2; 3. Once all the trains are outside TTD2, it is possible to verify if it is able to be free
Postcondition	Set a TTD to free or verification that the TTD is failed and needs maintenance
Safety relation	All Events are safety relevant
Open topics / consideration	If the journey profile is normally set in order to optimize energy consumption

8.17 USE OF TRAIN POSITION PARAMETERS TO MANAGE PARTICULAR SITUATIONS

8.17.1 UC_17_01

Use Case Group	Use of Train Position Parameters to manage particular situations
Use Case	Selection of the appropriate position report parameters according to the length of the train reported as train data
UC ID	**UC_17_01**
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside Traffic Management System (for this use case it is not practical that the dispatcher has to do something manually) ETCS On-board
Main goal	On the basis of the information reported by the train, in particular the train length, it is possible to select the adequate position report parameters in order to maximize the performance
Assumptions	The HL3/HTD Trackside knows the cycle time of the OTI-I, i.e. the interval of time that the OTI-I needs to determine a new train integrity
Precondition	
Flow of events	1. The HL3/HTD Trackside sends the Position Report Parameters to set free a VSS using the information of each position report (See example); 2. With each new MA sent by the HL3 Trackside to the ETCS On-Board new position report parameters are sent

Postcondition	The Use case is successful if the information provided by the ETCS On-board allows an optimal management of the information of the position reports, with less unnecessary position reports in comparison to the periodic reporting. The use case fails in case it is not possible to use the information for the optimal management.
Safety relation	There is no relation with safety
Open topics / consideration	Of course, this type of engineering is expected to be more complex than simply sending standard position report parameters at the start of mission. It may be good to improve performances.

Example:

Position Report Parameters Used

Description	This packet is intended to give parameters telling when and how often the position has to be reported.		
Transmitted by	RBC		
Content	Variable	Length	Value
	NID_PACKET	8	58
	Q_DIR	2	Nominal
	L_PACKET	13	Calculated Length
	Q_SCALE	2	1 (1 m scale)
	T_CYCLOC	8	255 (Infinite)
	D_CYCLOC	15	32767 (The train has not to report cyclically its position)
	M_LOC	3	001 (Every LRBG compliant balise group)
	N_ITER	5	4
	D_LOC(1)	15	200
	Q_LGTLOC(1)	1	1 (Max safe front end)
	D_LOC(2)	15	100
	Q_LGTLOC(2)	1	0 (Min safe rear end)
	D_LOC(3)	15	200
	Q_LGTLOC(3)	1	1 (Max safe front end)
	D_LOC(4)	15	100
	Q_LGTLOC(4)	1	0 (Min safe rear end)

Table 30: Position Report structure

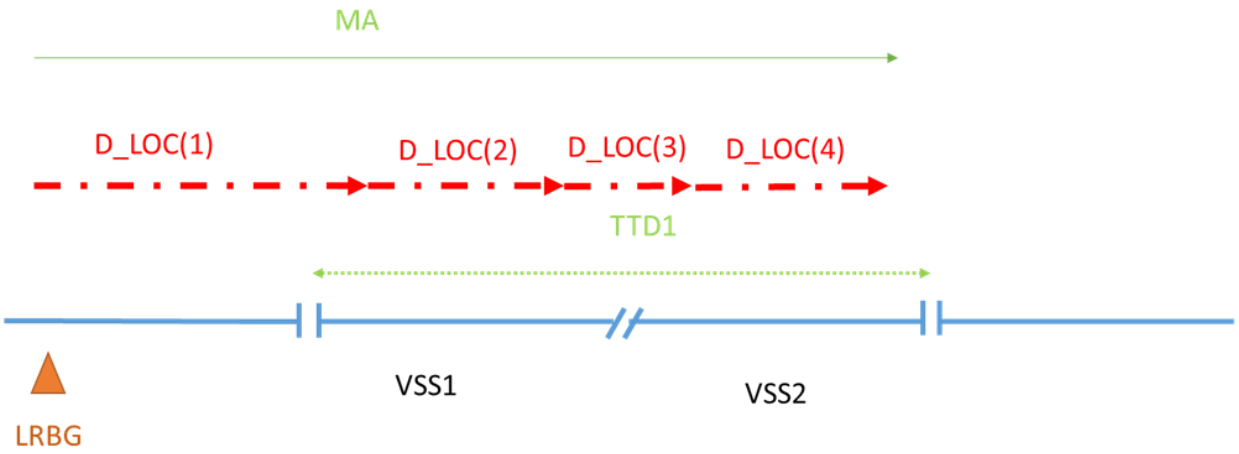

Figure 22: Example for Position Report

Assumption: TIMS cycle time: 5 s

Regarding D_LOC(1), VSS1 is expected to become occupied (only if VSS0 is occupied) when TTD1 becomes occupied according to the requirement HTD_8. With D_LOC(2) it is expected to trigger transition #6B and set VSS0 to free. With D_LOC(3) it is expected to trigger the transition #2A and set VSS2 to occupied. With D_LOC(4) it is expected to trigger transition #6B and set VSS1 to free. See Figure 22.

8.17.2 UC_17_02

Use Case Group	Use of Train Position Parameters to facilitate the transition from ambiguous to occupied.
Use Case	Selection of the appropriate position report parameters to facilitate the transition from ambiguous to occupied.
UC ID	**UC_17_02**
Main actor	HL3/HTD Trackside
Other actors	HL3/HTD Trackside Dispatcher / Traffic Management System ETCS On-board
Main goal	If a VSS is in the ambiguous state, the position report parameters may be dynamically changed by the HL3/HTD Trackside in order to facilitate the transition to occupied when the train overpasses the TTD boundary
Assumptions	• The communication network (not modified by HL3/HTD) is able to sustain the increase of the frequency of the position reports
Precondition	The VSS where the train is located is in the ambiguous state. The train located in the VSS is sending position reports with Q_INTEGRITY=1 (Integrity Confirmed by External Source) and it is approaching the TTD boundary.
Flow of events	1. The HL3/HTD Trackside sends the updated position report parameters to the ETCS on-board in order to facilitate the transition #11A (for example the frequency of the position reports may pass from 7 seconds to 1 second);

	2. The train proceeds setting a new VSS to ambiguous, overpassing the TTD boundary; 3. The train proceeds setting the TTD in rear to free before the latest expiration of the shadow train timer, allowing the transition #11A for the new VSS. The new VSS passes to state occupied. 4. The HL3/HTD Trackside sends the updated position report parameters to resume the normal operation
Postcondition	The Use case is successful if the next VSS can be set to occupied, exploiting the transition #11A
Safety relation	There is no relation with safety
Open topics / consideration	This use case is useful only if the shadow train timer is present and has a value different from infinite

8.18 SUPERVISED MANOEUVRE

8.18.1 UC_18_01

Use Case Group	Supervised Manoeuvre
Use Case	Joining in Supervised Manoeuvre
UC ID	UC_18_01
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside Driver or external safety system for the reset of the train integrity
Main goal	Joining is performed in Supervised Manoeuvre without loss of the connection
Assumptions	• Sweeping in Supervised Manoeuvre is allowed; • Operational procedures for sweeping avoid that a potential lost vehicle in front of the consist is «pushed» without any joining
Precondition	C1, C2 and C3 are consists with an established radio connection and safe consist length information for Supervised Manoeuvre acknowledged by the RBC. They are all in Standby with a train orientation according to the triangle (see Figure 23). The RBC has memory of the sum of all the train lengths that can be present in the area (non-harmonised feature). The integrity loss propagation timer of VSS2 has expired, causing VSS1 to become «Lost Vehicle in Front of the Consist" (#SM9A) and VSS3 to become unknown (#SM1F).
Flow of events	1- C1 receives a sweeping SM MA to enter VSS2. VSS2 becomes LR because of transition #SM11A (for example C2 has C1 in front and C3 in rear). When C1 reports its confirmed rear end outside VSS1, VSS1 becomes free because of transition #SM18B (Figure 24); 2- C1 performs joining with C2 (C1 in grey is the active cab). When the joining is performed successfully, the consist C1+C2 reports loss of integrity and an updated safe consist length. Reset of the train integrity is ordered and the consist C1+C2 confirms the train integrity again with confirmed train length. Taking into account the information sent via the safe consist lengths, the trackside can't exclude the shadow train risk, so the #SM27A is not performed.

	VSS2 stays in LR because C3 is in front of C1+C2 and C1+C2 is in rear of C3 (see Figure 25); 3- C1+C2 performs joining with C3 (C1 in grey is the active cab). When the joining is performed successfully, the consist C1+C2+C3 reports loss of integrity and an updated safe consist length. Reset of the train integrity is ordered and the consist C1+C2+C3 confirms the train integrity again with confirmed train length. Taking into account the information sent via the safe consist lengths and the non harmonised features to exclude the presence of other vehicles entering the area, the trackside is sure that the joining was successful and there is no shadow train risk, so the transition #SM27A is performed, VSS2 becomes occupied (see Figure 26)
Postcondition	The Use case is successful if after joining the VSS is in state occupied The use case fails in case it is not possible to exclude the presence of shadow trains and VSS2 remains LR
Safety relation	Yes
Open topics / consideration	This use case exploits the possibility that the RBC memorizes the length of the trains in the VSSs

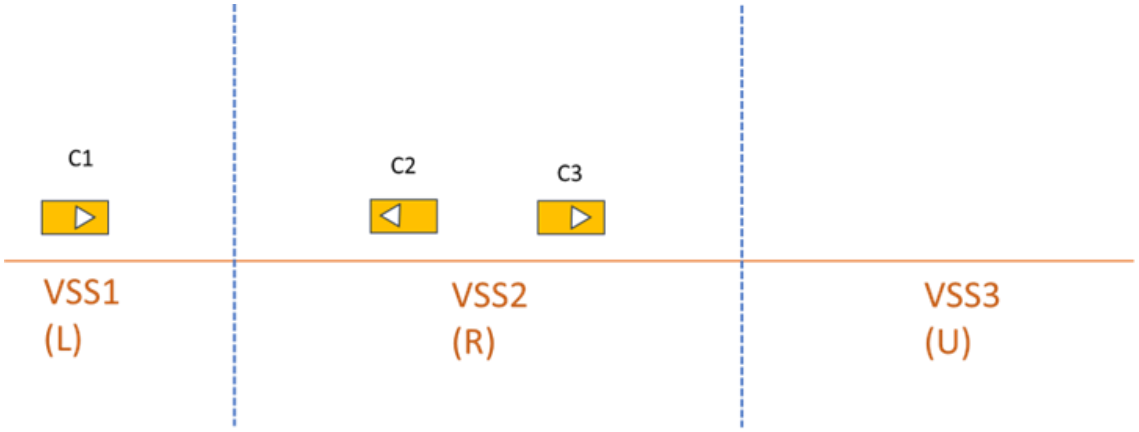

Figure 23: Precondition for Joining in SM

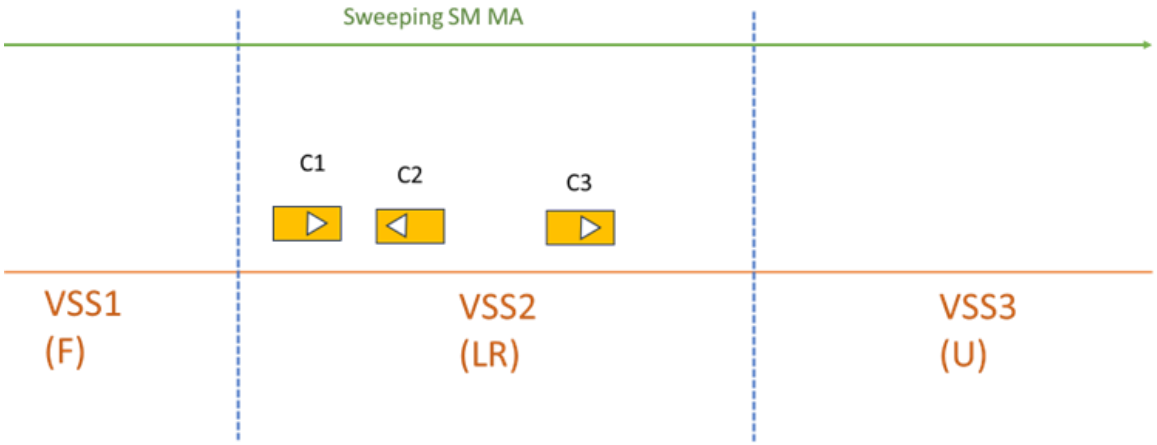

Figure 24: Joining in SM Step 1

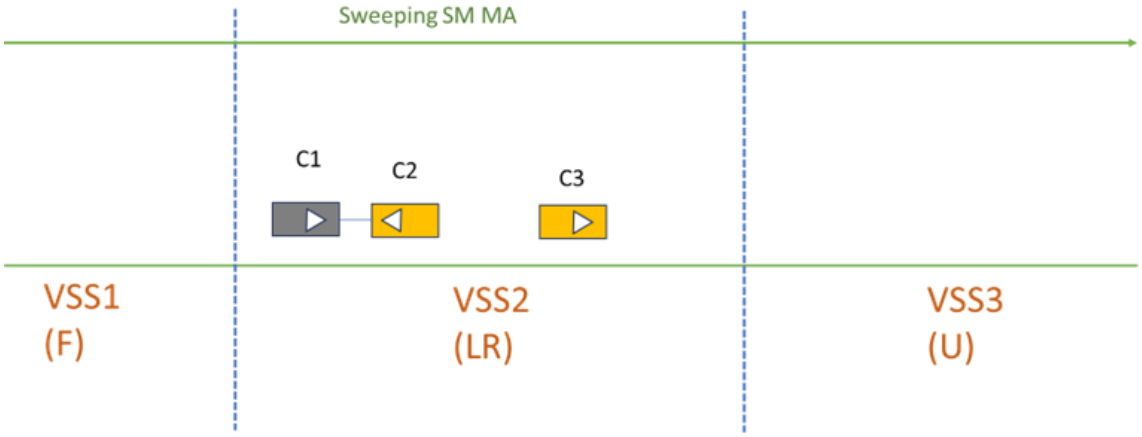

Figure 25: Joining in SM Step 2

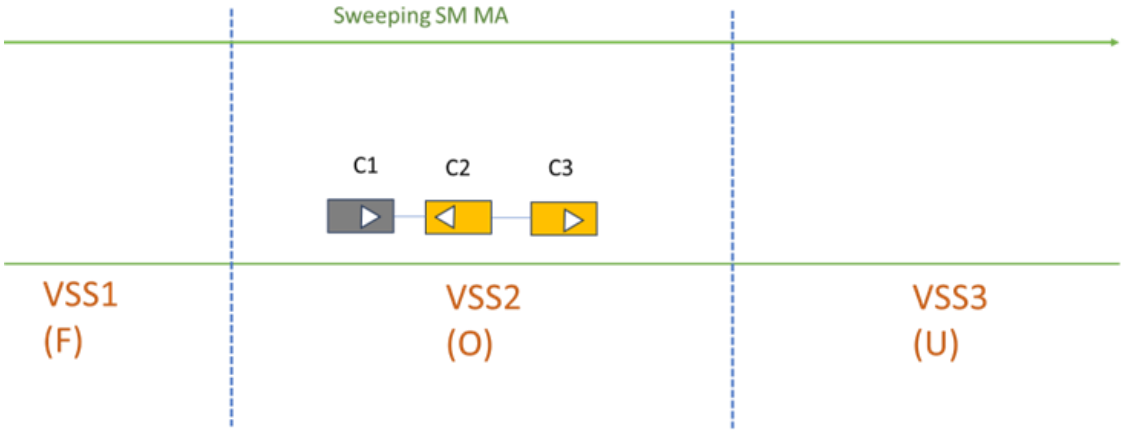

Figure 26: Joining in SM Step 3

8.18.2 UC_18_02

Use Case Group	Supervised Manoeuvre
Use Case	Start of Mission in Supervised Manoeuvre
UC ID	UC_18_02
Main actor	ETCS On-board
Other actors	HL3/HTD Trackside
Main goal	Start of Mission is performed and the VSS can be set to occupied after a sweeping procedure
Assumptions	• Sweeping in Supervised Manoeuvre is allowed; • Operational procedures for sweeping avoid that a potential lost vehicle in front of the consist is «pushed» without any joining
Precondition	Consist C1 is in mode SB in VSS2, in a TTD with 3 VSSs. Adjacent TTDs are free.
Flow of events	1- C1 performs SoM in SM in VSS2. The trackside is not sure where the lost vehicles, if present, are located and what are their length. Transition #SM6A is performed (see Figure 27);

	2- C1 receives a Sweeping SM MA towards the border between VSS2 and VSS3. When the border of VSS2 is reached there can't be no more a vehicle in front of C1, so transition #SM16A is performed, VSS2 becomes R (see Figure 28); 3- When C1 enters VSS3, transition #SM5A is performed and VSS3 becomes R. VSS2 is left by C1 and makes the transition VSS2 makes the transition #SM21A becoming U (see Figure 29) 4- C1 reaches the end of VSS3, there is a request of an updated Supervised Manoeuvre MA and tha MA is received in the opposite direction in order to continue sweeping. There can be more vehicles in rear of C1 (the adjacent TTDs are free) so transition #SM15A is performed (see Figure 30) 5- When C1 leaves VSS3,transition #SM18B is performed and VSS3 becomes free.VSS2 becomes occupied according to transition #SM25A (see Figure 31
Postcondition	The Use case is successful if VSS2 can be set in the state occupied Otherwise it fails
Safety relation	Yes
Open topics / consideration	This use case does not exploit the possibility that the RBC memorizes the length of the trains in the VSSs

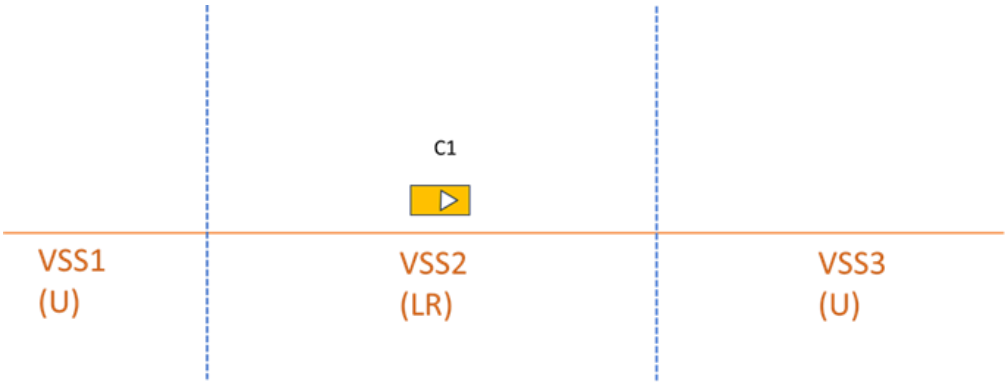

Figure 27: SoM in SM Step 1

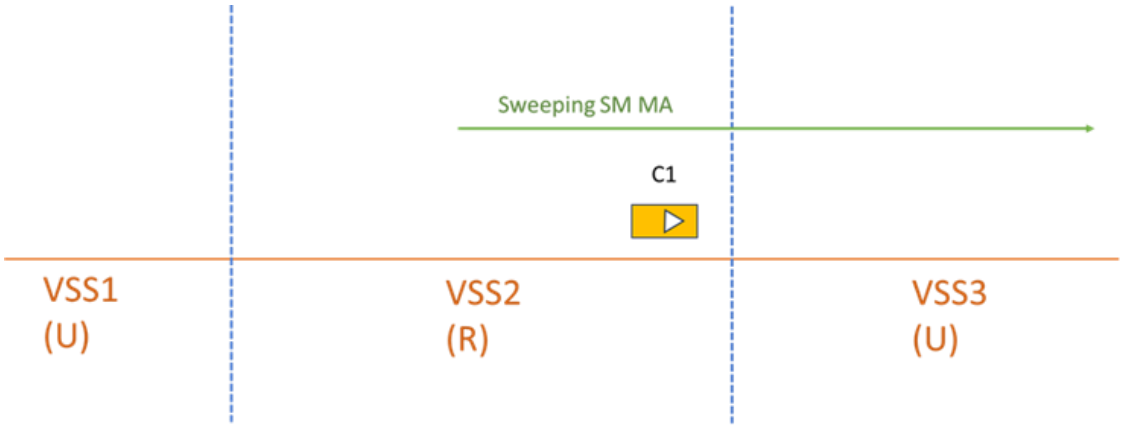

Figure 28: SoM in SM Step 2

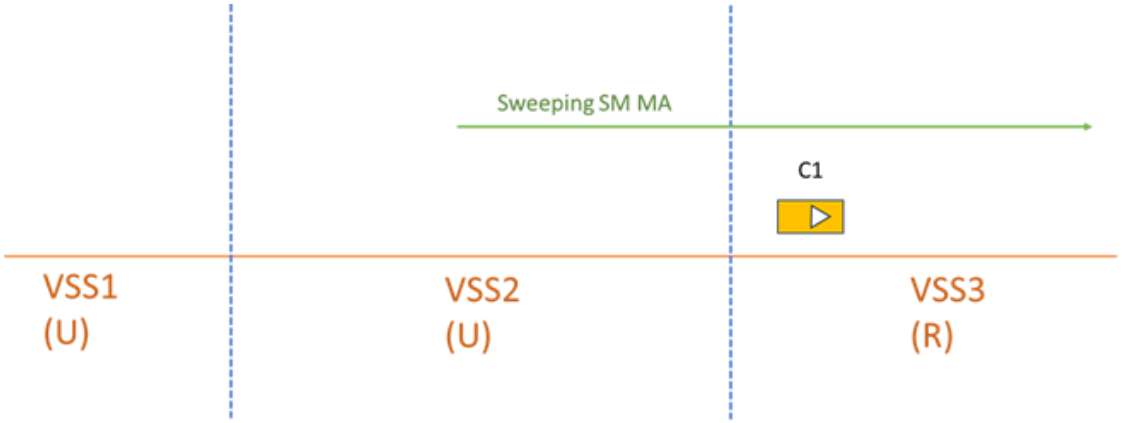

Figure 29: SoM in SM Step 3

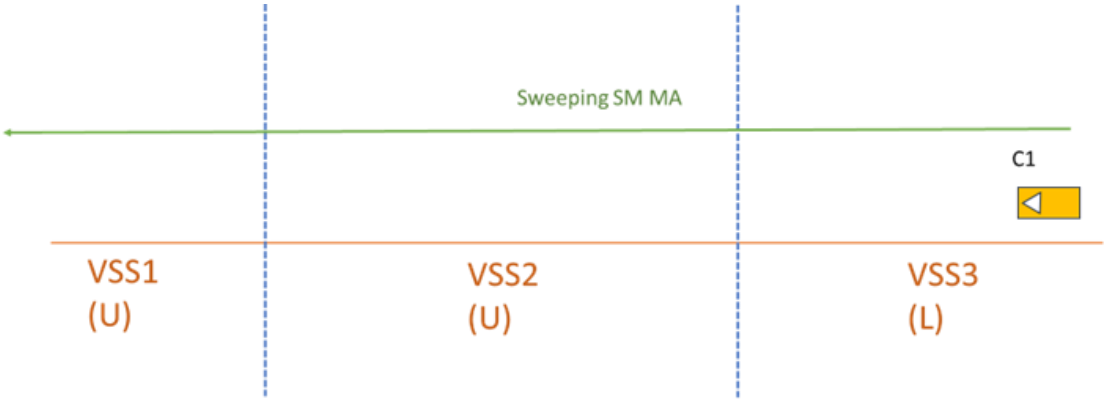

Figure 30: SoM in SM Step 4

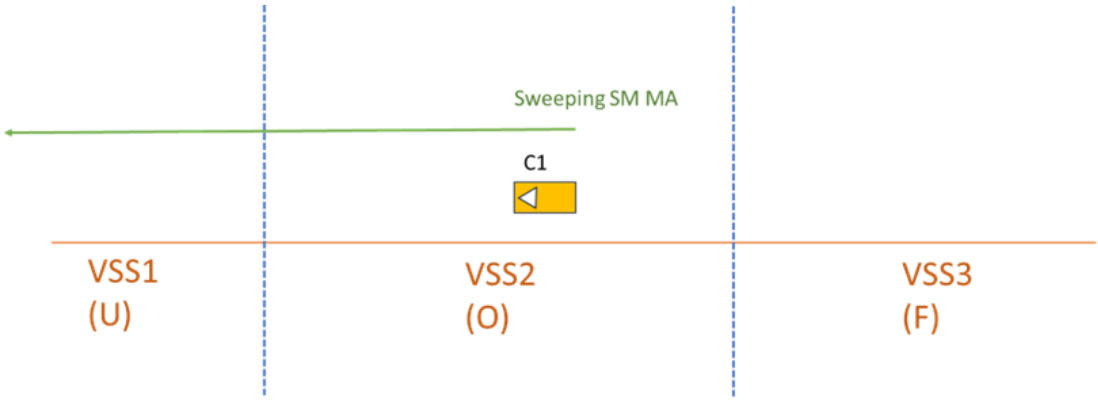

Figure 31: SoM in SM Step 5

8.19 COEXISTENCE OF HL3/HTD AND NTC

8.19.1 UC_19_01

Use Case Group	Use of HL3/HTD and NTC

Use Case	Ghost train propagation timer generated by LNTC train
UC ID	UC_19_01
Main actor	NTC Train
Other actors	HL3/HTD Trackside ETCS On-board
Main goal	Allowing the circulation of LNTC trains in HL3/HTD area
Assumptions	• An LNTC train enters the line according to the aspect of a luminous signal
Precondition	
Flow of events	1. The NTC train enters in the line. All the VSSs in the TTD become “unknown” according to transition #1A. The ghost train propagation timer for TTD1 is started; 2. The NTC train proceeds until the next TTD (authorized by luminous signal). When TTD2 becomes occupied the ghost train propagation timer of TTD2 is started (See Figure 32 Effect of LNTC Train); 3. The NTC train sets TTD1 to free. All the VSSs in that TTD are set to free according to transition #4A; 4. An HL3 ready train is authorized in the line, setting VSS1 to Ambiguous according to the transition #3A 5. When the ghost train propagation timer of train T1 expires, transition #1G is expected to occur in VSS2 and VSS3, with possible impact on the MA of train T1 (See Figure 33 Final Effect of LNTC Train)
Postcondition	
Safety relation	Yes
Open topics / consideration	To avoid the problems various solutions can be found for example: 1) detection at the TTD border 2) Operational rules to avoid that NTC trains go in the opposite direction of ETCS ones

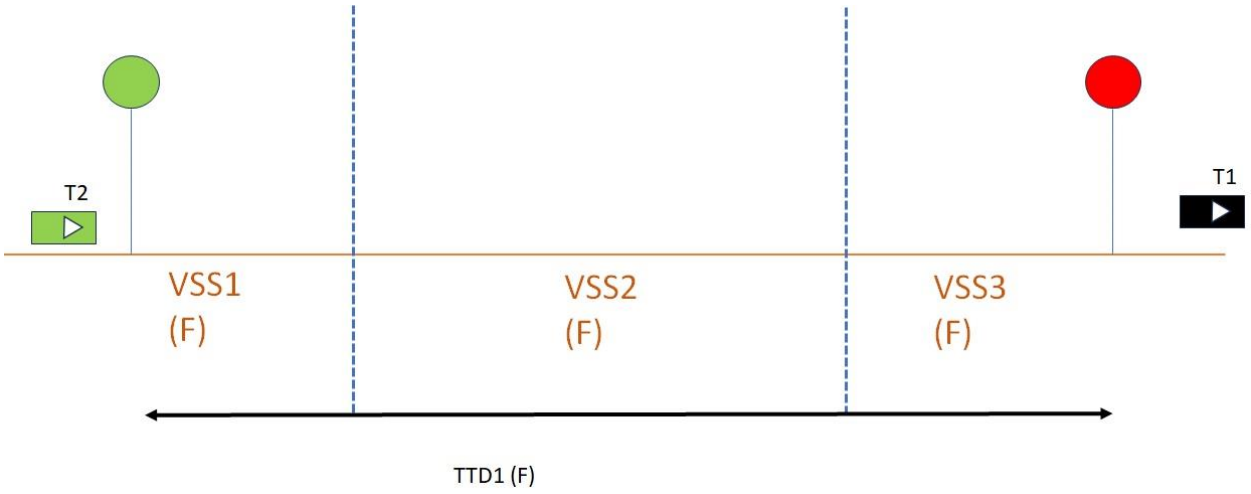

Figure 32: Start of Ghost Train Propagation Timer in TTD2

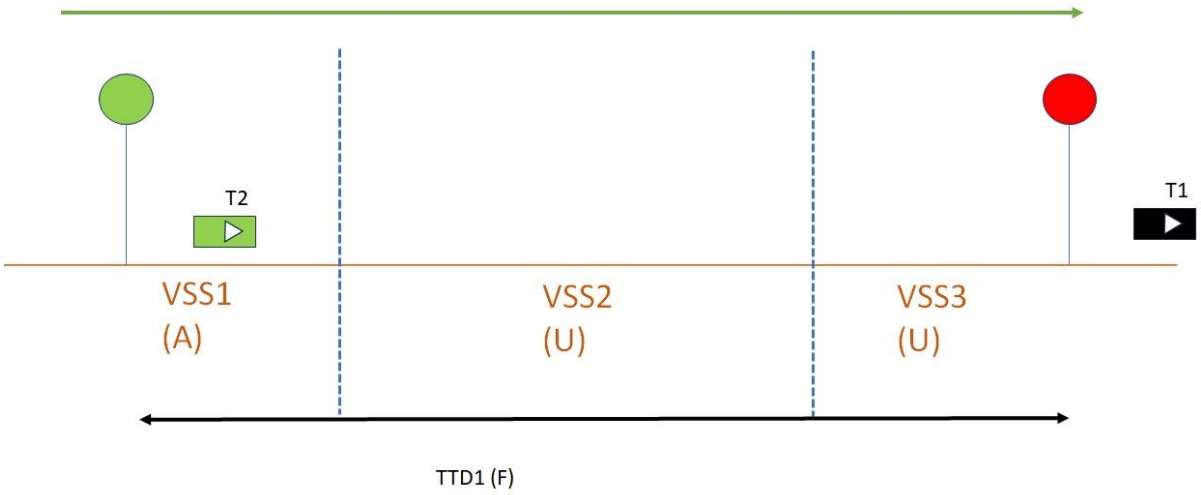

Figure 33: Effect of LNTC Train Final Situation

8.19.2 UC_19_02

Use Case Group	Use of HL3/HTD and NTC
Use Case	Wrong management of the SPAD of LNTC train
UC ID	UC_19_02
Main actor	NTC Train
Other actors	HL3/HTD Trackside ETCS On-board
Main goal	Evidencing the problems of SPAD of LNTC Train
Assumptions	• An LNTC train enters the line according to the aspect of a luminous signal
Precondition	An HL3 Ready train is in VSS2 of the line. VSS2 has the state occupied.
Flow of events	1. A LNTC Train T2 performs SPAD but the VSS1 remains free because TTD1 is already occupied by HL3 ready train T1. (See Figure 34)
Postcondition	
Safety relation	Yes
Open topics / consideration	SPAD of LNTC train shall not be of course normal operation. This use case evidences an additional problem of the use of HL3/HTD in this context, that can be solved for example with a SPAD alarm

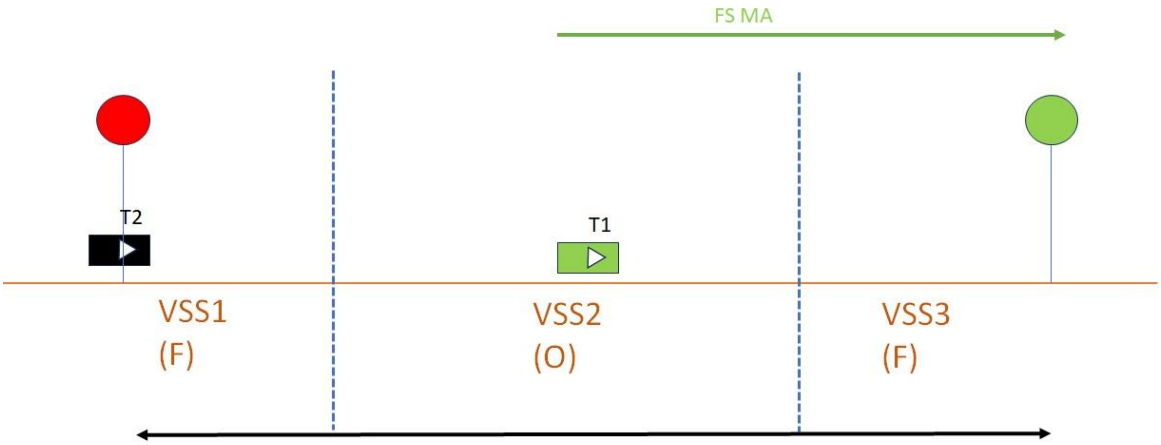

Figure 34: SPAD of LNTC Train

9 ADAPTED REQUIREMENTS FROM EUG SPECIFICATION

In this chapter are reported all the requirements valid for the HL3/HTD solutions that are coming from [8], in some cases with some adaptations (for example because of the possibility of the use of Safe Consist Length). Notes, explanatory texts, all the requirements satisfied with the use of the State Machines and references to the specification [8] are not reported explicitly, there is only the applicable clause of the specification [8] and the classification in the note. For all the requirement is indicate the traceability with the requirement written in the document [8].

ID	traceability [8]	Requirement	Note
HTD_1	3.1.1.7	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.	Like requirement 3.1.1.7 in [8], with the use of the term HL3/HTD
HTD_2	3.3.1.1	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.	Similar to 3.3.1.1 in [8], but with one part deleted because of the possible use of safe consist length
HTD_3	3.3.1.1.1	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.	
HTD_4	3.3.1.2	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.	
HTD_5	3.3.1.3	The train location only exists as long as the train is considered as connected to the trackside. As soon as the mute timer expires, the train location is deleted, but as memorised train location still valid for use in the state machine. It is possible that the trackside stores some train data, like the train data, for the use of optional transitions	Similar to 3.3.1.3 in [8], with the optional possibility to store some train data

ID	traceability [8]	Requirement	Note
HTD_6	3.3.2.1	When the trackside receives the confirmation that the max safe front end of the train has entered a VSS (through position reports), 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.	
HTD_7	3.3.2.1.1	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 or by forbidding opposing movements on VSS limits. For TTD limits this risk does not exist (train in advance of EOA would be detected by TTD).	
HTD_8	3.3.2.1.2	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.	
HTD_9	3.3.2.2	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.	Similar to 3.3.2.2 in [8], but with the consideration of the safe consist length
HTD_10	3.3.2.3	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.	

ID	traceability [8]	Requirement	Note
HTD_11	3.3.3.1	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	Similar to 3.3.3.1 in [8], but with the consideration of the train treated as integer and the confirmed train length
HTD_12	3.3.3.5	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.	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
HTD_13	3.3.3.6	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. This is to avoid losing the train location due to delayed PTD information (“jumping train”).	
HTD_14	3.3.3.6.1	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. 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).	
HTD_15	3.3.3.7	If the established rear end of the train location has moved forward due 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.	

ID	traceability [8]	Requirement	Note
HTD_16	3.3.4.2	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.	
HTD_17	3.3.4.4	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. This is to avoid losing the train location due to delayed PTD information (“jumping train”).	
HTD_18	3.3.4.4.1	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. 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).	
HTD_19	3.3.4.5	If the assumed rear end of the train location has moved forward due 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.	
HTD_20	3.3.4.6	On an ambiguous VSS the assumed rear end is used for the train location. This to prevent that for a complete train the L_TRAININT is used for the shadow train timer when leaving the TTD AND to prevent a ‘train length’ change if temporarily reporting “no integrity info”.	Identical to the original requirement with the term “complete” instead of integer
HTD_21	3.4.1.1.2	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.	

ID	traceability [8]	Requirement	Note
HTD_22	3.4.1.1.3	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.	
HTD_23	3.4.1.2	A “mute timer” is assigned to each train with active radio connection.	Similar to 3.4.1.2 in [8], but with an extension to trains without valid train data (like the ones in Supervised Manoeuvre Mode)
HTD_24	3.4.1.2.1	Start event for “mute timer” of HTD_23: a) Information is received from the train.	
HTD_25	3.4.1.2.2	Stop event for “mute timer” of HTD_23: a) The train is disconnected and can be assumed to be stopped.	
HTD_26	3.4.1.3		Replaced by ADD_0005
HTD_27	3.4.1.3.1	Start event: a) Integrity confirmation is received from the train	
HTD_28	3.4.1.3.2	Stop events: 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)	Similar to 3.4.1.3.2 in [8] with the inclusion of the case of train data to be revalidated in Standby
HTD_29	3.4.1.5	A “shadow train timer” is assigned to each TTD for each direction and for each connected train on the TTD	

ID	traceability [8]	Requirement	Note
HTD_30	3.4.1.5.1	Start event of “shadow train timer”: a) The complete train reports that its max safe rear end is inside the TTD	Similar to 3.4.1.5.1 in [8], with the use of the term “complete” instead of “integer” to reduce the confusion with the term “train deemed as integer”
HTD_31	3.4.1.5.2	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).	Similar to 3.4.1.5.2 in [8] with a different text
HTD_32	3.4.1.5.3	Stop events of shadow train timer: a) The train becomes not treated as integer anymore	
HTD_33	3.4.2.1.3	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.	
HTD_34	3.4.2.1.4	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.	
HTD_35	3.4.2.2	A “disconnect propagation timer” is assigned to each VSS.	

ID	traceability [8]	Requirement	Note
HTD_36	3.4.2.2.1	Start event of “disconnect propagation timer”: a) The VSS changes to "unknown" because it is part of the MA of a train for which the “mute timer” has expired. b) A train located on the VSS reports termination of communication session. c)The mute timer expires for a train, located on the VSS, without an MA.	
HTD_37	3.4.2.2.2	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	
HTD_38	3.4.2.3	A “ghost train propagation timer” is assigned to each TTD.	
HTD_39	3.4.2.3.1	Start events for “ghost train propagation timer”: Transition #1A or #SM1A is performed	Similar to 3.4.2.3.1 in [8], with direct reference to the transitions in the state machine
HTD_40	3.4.2.3.2	Stop event for “ghost train propagation timer”: a) The VSS state machine is fully processed after the timer expired	
HTD_41	3.4.2.3.3	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.	
HTD_42	3.4.2.4	In areas where Supervised Manoeuvre is not used, an “integrity loss propagation timer” is assigned to each VSS.	Similar to 3.4.2.4 in [8] but with the consideration of the areas with Supervised Manoeuvre Mode

ID	traceability [8]	Requirement	Note
HTD_43	3.4.2.4.1	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 this event also triggers a transition of the VSS to state "ambiguous".	
HTD_44	3.4.2.4.2	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 b) VSS state changes to “occupied” or to “free” c)The VSS state machine is fully processed after the timer expired	
HTD_45	3.5.1.2	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	
HTD_46	3.5.1.3	The trackside will not treat a train 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 reports changed 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 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 ETCS On-Board reports Mode Reversing	Similar to 3.5.1.3 in [8] with some additions related to reversing Mode, a scenario related the reconnection of a train with a ghost train in rear and not valid train data in Standby Mode

ID	traceability [8]	Requirement	Note
HTD_47	3.6.1.1	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	
HTD_48	3.6.1.2	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.	
HTD_49	3.7.1.1	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.	
HTD_50	3.11.1.2	As soon as the train is not located anymore 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	
	4		The chapter 4 in [8] is Covered by D15.2

<table>
<tr>
<td>HTD_51</td>
<td>5.1.1.2</td>
<td>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:
<table>
<tr><th>Event</th><th>Sequence of actions</th></tr>
<tr><td rowspan="6">PTD information or communication termination order received</td><td>1. Reinstate the train location from the memorised train location (if applicable due to reconnection)</td></tr>
<tr><td>2. Update the front end of the train location and evaluate the timer start/stop conditions</td></tr>
<tr><td>3. Update the VSS states (run the state machine)</td></tr>
<tr><td>4. Update the rear end of the train location and evaluate the timer start/stop conditions</td></tr>
<tr><td>5. Update the VSS states (run the state machine)</td></tr>
<tr><td>6. If transition #11B has been performed, update the VSS states (run the state machine)</td></tr>
<tr><td rowspan="3">TTD information (occupied/free)</td><td>1. Update the front end of the train location and evaluate the timer start/stop conditions</td></tr>
<tr><td>2. Update the VSS states (run the state machine)</td></tr>
<tr><td>3. Update the rear end of the train location and</td></tr>
</table>
</td>
<td>Modification of the requirement because of optional transition #4C</td>
</tr>
</table>

ID	traceability [8]	Requirement		Note
			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	
HTD_52	5.1.1.2.2	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.		
HTD_53	5.1.1.3	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.		
HTD_54	5.1.1.4	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".		
HTD_55	5.1.1.5	The term “TTD” without a qualifier like “previous” refers to the TTD of the VSS for which the condition is checked (the evaluated VSS).		
HTD_56	5.1.1.6	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.		
HTD_57	5.1.1.7	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.		

ID	traceability [8]	Requirement	Note
HTD_58	5.1.1.8	When the word "train" / "timer" is used more than once in a transition condition, the same train / timer is meant.	

10 EXPORTED CONSTRAINTS

10.1 EXPORTED TO ETCS ON BOARD

According to the current determinations in R2DATO, ETCS On-Board is not in the scope of the project. So, in this chapter there are some exported constraints for the ETCS On-Board, to be considered by the System Pillar.

10.1.1.1.1 EXT_TO_EVC_001

Description	**Age of train data for sending to trackside**
Start Event	not applicable
Stop Event	not applicable
Value	The train data sent to RBC by the ETCS On-Board shall be estimated less than a configurable time before the beginning of sending of the corresponding message 129.
Notes	This is to avoid an excessive delay in case of Intentional Train Integrity Loss. More information is present in Deliverable D15.2

10.1.1.1.2 EXT_TO_EVC_002

Description	**Age of Safe Consist Length for sending to trackside**
Start Event	not applicable
Stop Event	not applicable
Value	The Safe Consist for Supervised Manoeuvre sent to RBC shall be estimated less than a configurable time before the beginning of sending of the corresponding message.
Notes	This is to avoid an excessive delay in case of Intentional Train Integrity Loss (for trains that have the Safe Consist Length) or operation in Supervised Manoeuvre. More information is present in Deliverable D15.2

11 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 sessions with many VSSs inside them. On the main lines instead, maintaining the current physical sessions 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.

The work done in Task 15.1 and Task 15.3 for the consolidation is reported in this document which contains the HL3/HTD system specification, HL3/HTD use cases and engineering rules for main and regional lines.

This result was considered satisfactory by the participants of R2DATO WP15.

Starting from what was achieved in the past in other contexts and projects, the specification activity was contextualized and the open points that were present were filled. The work led to a stable version of the specifications in which the missing requirements were added and traceability with the previously created requirements was maintained.

This has also been done for the engineering rules which, using document 8 as a reference, have been added and improved.

What is reported will become a stable base on which to build the demonstrators that will be realized in R2DATO WP16.

From the feedback of the WP16 activities it will be possible to confirm the choices made and otherwise adjust the requirements.

Moreover, during the task 15.1 meetings, several discussion points emerged which did produce very proactive discussions.

Some of these points have not yet been fully resolved.

These will be taken care of during the activities of R2DATO WP16 in which an update of the current document will be produced.

The following Table 31 reports these open points.

ID Open Point	Text of the document containing the open point	Description of the open point
OP1	Summarizing, the concept of "integrity confirmed information" in the definitions above means that usually the trackside will not treat a train as integer if one of the following events occurs (list 1): a) the train reports "integrity lost". b) Position Report with no integrity information is received after the "wait integrity timer" has expired. c) the train reports changed train data with a new 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 (see [8] for the concept of propagation). f) the delay for the propagation of the "unknown" state of the VSS in rear of the train location expires (see [8] for the concept of propagation).	About the event d) must be clarify why the integrity is considered lost.
OP2	To allow trackside to manage changes in connection state of a train, a "mute timer" is established trackside for each connected train: 1. Start event: Information is received from the train. 2. Stop event: The train is disconnected and can be assumed to have stopped.	About the Stop event: must be clarify in which way the train can be assumed to have stopped
OP3	**Integrity confirmed**: If a train fulfils the conditions for being treated as integer by the trackside, the trackside system sets the VSS where the train is located to "occupied" if it was previously free	Must find an agreement about how to consider the status of the VSS in relation on the TTD
OP4	A train is considered disconnected from the trackside when there is no established safe radio connection, e.g. after an End of Mission or communication failure takes place, or with an established safe radio connection but without valid train data, e.g. Start of Mission, and when the dedicated timer to supervise the train connection with the trackside expires (mute timer or the radio hole timer).	Must be clarify if is it possible to consider the train disconnected if valid train data are not received.

ID Open Point	Text of the document containing the open point	Description of the open point
OP5	• **Reconnection after mute timer expiration:** If the train reconnects with the same train orientation and length, the VSS sections set "unknown" can be restored to the following VSS status based on the following conditions: ○ "Occupied": In the VSS sections where the train is located if the train reports integrity confirmed, and no change of train data train length was reported since the previous position report and there is no shadow train risk. ○ "Ambiguous": In the VSS sections where the train is located if the conditions for "occupied" above are not fulfilled. ○ "Free": In the VSS sections in advance of the train covered by the original MA if the original MA is still valid on-board or can be re-issued to the train. In the VSS sections in rear of the train location if the train reports "integrity confirmed", no change of train data train length was reported since the previous position report and there is no risk that another train had entered these sections, and regardless of this, if the TTD covering those sections is released.	The task has to find an agreement about the Ambiguous status of the VSS
OP6	5. Train 2 joins Train 1 and performs EoM. VSS 22 becomes "unknown" The disconnect propagation timer related to VSS 22 is started.	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.
OP7	While the train proceeds, a disconnect or integrity loss propagation timer expires. According to transition #1C all the VSS in the same TTD of the unknown VSS become unknown.	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 agree position.

ID Open Point	Text of the document containing the open point	Description of the open point
OP8	1. The maintainer or dispatcher switches on the HL3/HTD Trackside. The status of the occupied track circuits is received by the RBC. All the VSSs in the occupied TTDs remain unknown and the ghost train propagation timer is started, the others are set to free according to the transition #4A;	In the UC UC_14_01 Trackside Initialisation #1 Must be clarify which is the trigger condition for starting the timer.

Table 31: Open points to be discuss in the WP16

REFERENCES

[1] SUBSET-026-3 (4.0.0). System Requirements Specification Chapter 3 – Principles.
[2] SUBSET-026-4 (4.0.0). System Requirements Specification. Chapter 4 - Modes and Transitions.

[3] SUBSET-026-5 (4.0.0). System Requirements Specification. Chapter 5 - Procedures.

[4] X2Rail-5 Deliverable D4.1 Moving Block Specification Part 2 – System Definition Rev-09

[5] X2Rail-5. Deliverable D4.1 Moving Block Specification. Part 3 - System Specification. Rev-23

[6] X2Rail-5 Deliverable D4.1 Moving Block Specification Part 4 – Operational Rules Rev-15

[7] X2Rail-5 Deliverable D4.1 Moving Block Specification Part 5 – Engineering Rules rev-16

[8] EUG ERTMS/ETCS Hybrid Train Detection Ref 16E042 Ver. 1F Date 20 12 2022

[9] 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

[10] COMMISSION IMPLEMENTING REGULATION (EU) 2023/1693 of 10 August 2023 amending Implementing Regulation (EU) 2019/773 on the technical specification for interoperability relating to the operation and traffic management subsystem of the rail system within the European Union