

## X2Rail-2

Project Title:	Enhancing railway signalling systems based on train satellite positioning, on-board safe train integrity, formal methods approach and standard interfaces, enhancing traffic management system functions
Starting date:	01/09/2017
Duration in months:	36
Call (part) identifier:	H2020-S2RJU-CFM-IP2-01-2017
Grant agreement no:	777465

### Deliverable D4.1

## Train Integrity Concept and Functional Requirements Specifications

Due date of deliverable	Month 32
Actual submission date	30-04-2020
Organization name of lead contractor for this deliverable	STS
Dissemination level	PU
Revision	23-06-2020

## Authors

<b>Authors</b>	<b>STS</b> S. Iovino N. Ricevuto M. Dalia T. Marinelli
	<b>AZD</b> P. Gurnik
	<b>CAF</b> Igor Lopez Orbe
	<b>INDRA</b> F. Parilla Ayuso A. Alberdi
	<b>MERMEC</b> F. Inzirillo
	<b>RAILENIUM</b> El Miloudi El Koursi (IFSTTAR-COSYS-ESTAS)
	<b>SBB</b> D. Grabowsky
<b>Contributors</b>	<b>BTSE</b> Thomas Eriksson
	<b>CEIT</b> Adrian Rodriguez Lopez
	<b>NR</b> James Ambrose
	<b>SIEMENS</b> Sven Adomeit
	<b>RAILENIUM</b> Insaf Sassi

## Modification History

Issue Number Date	Section Number	Modification / Description	Author (Company)
0.1 6-Dec-2017	6.2	First draft Product Classes and Target scenarios definition, Context for functional requirement specification	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
0.2 27-Feb-2018	6.2.6, 7	Added scenarios description, Functional Requirement Specification and Preliminary Hazard Analysis	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
0.3 14-Mar-2018	6.3.6.3, 6.2.6.4, 7.1.2, 7.1.6	Third draft Added train coupling and train separation description. Modifications to OTI FSM and OTI SLAVE. Added sequence diagrams for train coupling and train separation scenarios.	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
0.4 15-Mar-2018	6	Fourth draft. Added preliminary results from concept task activities (i.e. market investigation, wireless sensors and transponder technologies analysis, installation analysis, feasibility study about satellite based localization)	S. Iovino (ASTS) P. Gurnik (AZD) I. Lopez Orbe (CAF) F. Parilla Ayuso (INDRA) A. Alberdi (INDRA) F. Inzirillo (MERMEC)
0.5 19-Mar-2018	7.1.3, 7.1.4, 7.1.5	Minor changes to network and communication requirements	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
0.6 27-Mar-2018	6.2.2, 6.2.6.6, 7.1.1.1  6.2.6.5, 7.1.2.1, 7.1.6.1.	Added scenario for on-board equipment with central ETCS.  Added diagnostic scenario.	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
0.7 29-Mar-2018	6.3.1	Added preliminary installation analysis for freight context	D. Grabowski (SBB)

<p>0.8 4-Apr-2018</p>	<p>7.1.2.1 7.1.5.1.1 7.1.5.1.2 7.1.6.1</p> <p>6.2, 6.2.6.6 7.1.2.3</p> <p>7.2</p>	<p>Comments from CEIT</p> <p>Comments from SIE</p> <p>Completed preliminary hazard analysis for Class 1 and Class 2A.</p>	<p>S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)</p>
<p>0.9 14-Apr-2018</p>	<p>7.1.2, 7.1.4, 7.3</p> <p>6.4</p> <p>7.4.1</p>	<p>Diagnostic requirement REQ_7.1.2.1.9. Communication requirements REQ_7.1.4.7, REQ_7.1.4.8. Radio Communication general description.</p> <p>Added analysis about installation context.</p> <p>Added information for energy harvesting from INDRA experience in DEWI project.</p>	<p>S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)</p> <p>F. Parilla Ayuso (INDRA) A. Alberdi (INDRA) T. Marinelli (ASTS)</p> <p>F. Parilla Ayuso (INDRA)</p>

1.0 07 May 2018	6.1	Added contribution about State of Art.	F. Inzirillo (MERMEC) F. Parilla Ayuso (INDRA) A. Alberdi (INDRA)
	6.3	Changes at section 6.3.5. Added new section 6.3.7 with conclusions.	F. Parilla Ayuso (INDRA)
	6.3.2.4.1 and 6.3.2.4.2	Added subsections 6.3.2.4.1 and 6.3.2.4.2	4. I. Lopez Orbe (CAF)
	7.2	Added PHA for product classes 2B-2C	N. Ricevuto (ASTS)
	7.3, 7.4	Contribution to communication requirement and energy harvesting	F. Parilla Ayuso (INDRA) A. Alberdi (INDRA)
1.1 08 May 2018	6.1	Minor updated	F. Inzirillo (MERMEC)
	6.4.4	Added Contribution from RU	F. Inzirillo (MERMEC)
1.2	6.1.4	Section added again and completed	F. Parilla Ayuso (INDRA) A. Alberdi (INDRA)
	6.3.5	Section Reworked Subsection added from WP2 feedback	F. Parilla Ayuso (INDRA) A. Alberdi (INDRA)
	6.3.7	Section reworked to reflect other changes	F. Parilla Ayuso (INDRA) A. Alberdi (INDRA)
1.3 14 May 2018	7.5	Section Reworked	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
1.4 21 May 2018	6.2	Updated product classes table	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
	6.2.6	Added virtual coupling analysis	
	7.1	Updated FSM according to forth F2F meeting	

1.5 22 May 2018	6.4	Feedback from fourth F2F meeting	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
1.5 22 May 2018	6.5	Feasibility study about satellite based localization – major update	P. Gurník (AZD) EL-KOURSI El-Miloudi (RAILENIUM) I. Lopez Orbe (CAF) S. Iovino (ASTS) F. Inzirillo (MERMEC)
1.6 23 May 2018	6.2.5.7, 6.2.5.8  7.1  7.1.7	Added shunting and GNSS scenarios  Updates to support for Decoupling and Shunting scenarios, according to Feedback from fourth F2F meeting  Added example of FSM analysis in relation to virtual coupling assumptions	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
1.7	6.1	Integrate CAF contribution	F. Inzirillo (MERMEC) I. Lopez Orbe (CAF)
1.2 28 May 2018	7.2	Updated Functional Hazard Analysis in relation to updated product classes	N. Ricevuto (ASTS)
1.3 31 May 2018	5, 7.2, 7.5, 8	Added introduction and conclusion, updated PHA and non-functional requirements.	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
1.4 1 June 2018	  8	Comments from INDRA and SBB review sheet  Updated conclusion	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
1.5 4 June 2018	6.2.5.8 6.2.5.10	Updated for comments from Moving Blocks.	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
1.6 4 June 2018	7.1.2	Paragraphs renumbering	S. Iovino (ASTS)
1.7 4 June 2018	6.5	Updated after review comments	P. Gurník (AZD)
1.8 5 June 2018	6.1	Updated after review comments	F. Inzirillo (MM)

1.9 6 June 2018  Full Version for TMT review	6.1  7.4	Updated broken links.  Added functional introduction.	S. Iovino (ASTS)
2.0 6 June 2018  Full Version for TMT review		Added RAILENIUM as contributor for GNSS	S. Iovino (ASTS)
2.1 3 August 2018  Full Version for TMT review	6.4.5, 7.5.5, 7.5.6  6.2, 7.1  7.2  Appendix A-H	Added freight maintenance analysis and RAM requirements.  Updated for comments from Moving Blocks and UEG  Aligned respect to requirement renumbering  Added tables related to hazard analysis	D. Grabowsky (SBB)  S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)  N. Ricevuto (ASTS)  N. Ricevuto (ASTS)
2.2 8 August 2018  Full Version for TMT review	6.2.4.11, 7.1.1, 7.1.5	Updated for ETCS backward compatibility in relation to comments from Moving Blocks	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
2.3 4 September 2018  TMT review	1, 5	Updated in relation to executive summary, deliverable objectives and other editorial comments from TMT review.	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
3.0 13 February 2019	Section 7.1, 7.2, Appendix I	Updated in relation to Railenium/Ifsttar safety analysis	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)

4.0 19 February 2019	Section 7.1	Update in relation to Preliminary report on the OTI FSM formal validation performed by Railenium/Ifsttar.	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
4.1 8-March-2019	Section 7.1, 7.2, Annex I	Update in relation to results of safety analysis presented by Railenium/Ifsttar in Madrid Face2Face meeting.	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
4.2 29-March-2019	Sections 7.1.1.2, 7.1.5, 7.1.5.1, 7.1.5.6, 7.2.9, 7.2.10, Annex D, I	Updated in relation to Railenium/Ifsttar review sheet	S. Iovino (ASTS) N. Ricevuto (ASTS) M. Dalia (ASTS)
4.3 13-May-2019	Section 7.1	Updated in relation to Railenium/Ifsttar review sheet	S. Iovino (STS) N. Ricevuto (STS) M. Dalia (STS)
4.4 31-May-2019	Section 7.1.1.1	Updated mastership state in relation to discussion in Lille F2F meeting.	S. Iovino (STS) N. Ricevuto (STS) M. Dalia (STS)
4.5 05-June-2019	Appendixes	Table format updated.	S. Iovino (STS) N. Ricevuto (STS) M. Dalia (STS)
4.6 20-06-2019	Section 6.5	Updated for comments from TD2.4	P. Gurnik (AZD)
4.7 27-June-2019 Version for TMT/SteCo review	Sections 7.1.3, 7.1.5.4, Annex B	Updated in relation to traceability with test specification.	S. Iovino (STS) N. Ricevuto (STS) M. Dalia (STS)
4.71 13-Nov-2019	Sections 7.3.4, 7.4.	Modification resulted from D4.3 requirements traceability. Optional tag added to some energy harvesting and radio communication requirements already formulated as general guidelines.	S. Iovino (STS) N. Ricevuto (STS) M. Dalia (STS)
4.72 13-Feb-2020	Section 7.5.2	updated REQ. 7.5.2.1 and added REQ. 7.1.1.6.7 and REQ. 7.1.1.6.8 in relation to D4.4/D4.1 requirements traceability	S. Iovino (STS) N. Ricevuto (STS)



4.8 31-Mar-2020	Sections 7.1.7, 8, Appendix J	Added requirements for Product Class 3 and for train length determination.	S. Iovino (STS) N. Ricevuto (STS)
4.9 14-May-2020	Sections 7, 8 Appendix I, J, K, L	Updated for comments from Moving Block and from WP4 internal review	S. Iovino (STS) N. Ricevuto (STS)
5.0 23-June-2020	Section 7.1.7, 8.7.1	Updated in relation to feedback from functional testing traceability and editorial comments from TMT/SteCo review	S. Iovino (STS) N. Ricevuto (STS)

# 1 Executive Summary

---

The Train Integrity is an on-board function responsible for verifying the completeness of the train, while the train is in operation. The research objective consists concretely in monitoring the status of the train's tail to check that last wagon is regularly advancing in a coherent way in relation to the movement of the remaining train. The event of accidental train separation constitutes a serious danger for the next train, being a possible unexpected obstacle on the line, and therefore it need to be promptly reported to the signalling system.

The key issue of Train Integrity is that this function becomes a need for the implementation of more efficient signalling systems based on concepts like Moving Block or Train Position delivered by on-board equipment. Systems based on these concepts deliver very significant advantages in terms of capacity, shorter headways; capital and maintenance cost, removal of track infrastructure for block detection; resiliency, and others such us compatibility among lines, etc.

In particular, the adoption of the moving block concept, as prescribed by ERTMS L3 and CBTC systems, implies that the train integrity monitoring and detection could not be carried out by fixed wayside infrastructures. Conventional train detection systems such as track circuits, axle counters and others, could be used just as a fall back system or to confirm the train position in degraded situations.

In addition to the new functional and performance requirements, the On-board Train Integrity functionality could be the enabler in getting the economic sustainability of new railway lines, especially for freight and low density mixed-traffic lines. In these cases, the OTI functionality allows the elimination of fixed infrastructures along the line, relying on the autonomous position and integrity information with consequent important economic advantages.

In this context deliverable D4.1 is focused on OTI concept definition and functional requirement specification. In particular this document:

- contains the state of art regarding the train integrity function;
- defines target scenarios and product classes for all S2R application domains: Intercity-High Speed, Regional, Urban-Suburban, Freight;
- investigates and analyses the possible use of wireless sensors and/or transponders technologies, including their networking issues and safety aspects;
- analyses possible installation options, related to devices that could be required at train tail, considering operational rules, required components for power supply generation & harvesting and asset management;
- performs a feasibility study concerning the use of GNSS-based solution for train tail localization;
- defines functional and not functional requirements for Train Integrity Management System;
- include a functional hazard analysis.

Note that D4.1 was delivered in M12. This new version includes the review of the hazard analysis, integrates results from OTI Finite State Machine formal validation and includes the train length determination functionality.

## 2 Table of Contents

---

1	EXECUTIVE SUMMARY .....	10
2	TABLE OF CONTENTS.....	11
3	ABBREVIATIONS, ACRONYMS, TERMS .....	23
4	BACKGROUND .....	25
5	OBJECTIVE.....	26
6	CONCEPT.....	28
6.1	STATE OF ART .....	28
6.1.1	Introduction.....	28
6.1.2	DEWI Project .....	29
6.1.3	The DEWI project Demonstrator .....	33
6.1.4	SCOTT Project.....	33
6.1.5	Wireless Sensor Network (WSN).....	35
6.1.6	Network Discovery Techniques.....	37
6.1.7	Train Integrity trough Monitors brake pipe pressure .....	48
6.1.8	Market aspects.....	53
6.1.9	Conclusion .....	53
6.2	PRODUCT CLASSES AND TARGET SCENARIOS .....	54
6.2.1	ETCS Specification Context .....	54
6.2.2	S2R Application Domains .....	55
6.2.3	Product Classes.....	59
6.2.4	Reference Scenarios .....	67
6.2.5	Virtual Coupling assumptions and preliminary analysis.....	79
6.3	INVESTIGATION ON WIRELESS SENSORS AND TRANSPONDER TECHNOLOGIES.....	83
6.3.1	Available terrestrial wireless technologies .....	83
6.3.2	Mobile Cellular Networks .....	97
6.3.3	IoT Wide-Area Networks .....	102
6.3.4	Satellite technologies and services.....	111
6.3.5	Available Wireless Sensors .....	113
6.3.6	Transponder Technologies .....	116
6.3.7	Conclusions.....	119
6.4	INSTALLATION ANALYSIS .....	121
6.4.1	Introduction.....	121
6.4.2	Shunting Process analysis in freight context .....	122
6.4.3	Installation analysis for existing freight rolling stocks .....	124
6.4.4	Wireless Installation .....	129
6.4.5	Maintenance for freight waggons.....	130
6.4.6	Feedback from users .....	130
6.4.7	Conclusion .....	130
6.5	FEASIBILITY STUDY ABOUT SATELLITE BASED LOCALIZATION .....	131
6.5.1	Introduction to the GNSS technology .....	131

6.5.2	GNSS-based OTI function.....	143
6.5.3	Conclusions.....	155
<b>7</b>	<b>DEFINITION OF REQUIREMENTS.....</b>	<b>157</b>
7.1	FUNCTIONAL REQUIREMENTS SPECIFICATION .....	157
7.1.1	OTI Master Functional Module.....	160
7.1.2	Network Functional Module.....	180
7.1.3	On-board Communication Network .....	181
7.1.4	On-board Communication Protocol (OCP).....	182
7.1.5	OTI Slave Functional Module.....	185
7.1.6	Virtual Coupling preliminary analysis.....	197
7.1.7	Product Class 3 .....	202
7.2	FUNCTIONAL HAZARD ANALYSIS .....	214
7.2.1	System Definition .....	214
7.2.2	Functions Identification .....	215
7.2.3	Hazard identification .....	216
7.2.4	Risk evaluation without mitigation .....	218
7.2.5	Mitigations Identification.....	220
7.2.6	Risk evaluation with mitigation.....	220
7.2.7	FMECA Worksheet.....	220
7.2.8	Product Classes Hazard Analysis .....	223
7.2.9	Hazards List .....	237
7.2.10	Mitigation List.....	238
7.2.11	PHA Conclusion .....	244
7.3	RADIO COMMUNICATION REQUIREMENTS SPECIFICATION .....	246
7.3.1	Human Exposure requirements .....	246
7.3.2	Testing Radio requirements .....	247
7.3.3	Frequency selection requirements.....	248
7.3.4	High Level Radio Communication Requirements.....	249
7.4	ENERGY HARVESTING REQUIREMENT SPECIFICATION .....	250
7.5	NON FUNCTIONAL REQUIREMENT SPECIFICATION .....	251
7.5.1	Configuration and Maintenance Requirements .....	251
7.5.2	Mechanical Requirements.....	251
7.5.3	Environment Requirements.....	252
7.5.4	Safety.....	252
7.5.5	Maintenance .....	252
7.5.6	RAM Requirements.....	252
<b>8</b>	<b>TRAIN LENGTH DETERMINATION .....</b>	<b>254</b>
8.1	ANALYSIS OF ERTMS/ETCS SPECIFICATION .....	254
8.1.1	CR 940 .....	254
8.1.2	Subset-026.....	257
8.1.3	Subset-119.....	262
8.1.4	DMI.....	263
8.2	APPROACH DESCRIPTION .....	264

8.3	ASSUMPTIONS .....	265
8.4	REFERENCE SCENARIOS .....	265
8.4.1	Use Case n. 1 .....	267
8.4.2	Use Case n. 2 .....	280
8.4.3	Use Case n. 3 .....	283
8.4.4	Use Case n. 4 .....	292
8.4.5	Use Case n. 5 .....	294
8.4.6	Use Case n. 6 .....	294
8.5	RESULTS OF THE ANALYSED SCENARIOS.....	295
8.6	HAZARD ANALYSIS .....	301
8.7	REQUIREMENTS SPECIFICATION .....	305
8.7.1	Functional Requirements.....	305
8.7.2	Performance Requirements.....	309
8.7.3	Safety Requirements .....	309
9	CONCLUSIONS.....	311
10	REFERENCES.....	312
APPENDIX A	PHA .....	316
APPENDIX B	PRODUCT CLASS FTA .....	317
APPENDIX C	OTI_PHA_PC_1A.....	319
APPENDIX D	OTI_PHA_PC_1A_JOIN .....	340
APPENDIX E	OTI_PHA_PC_1B.....	343
APPENDIX F	OTI_PHA_PC_1B_JOIN.....	364
APPENDIX G	OTI_PHA_PC_2A_2B.....	367
APPENDIX H	TI_PHA_PC_2A_2B_JOINSPLIT.....	390
APPENDIX I	TI_PHA_PC_3A_3B .....	395
APPENDIX J	TI_PHA_PC_3A_3B_JOINSPLIT.....	434
APPENDIX K	HAZARD LOG .....	438
APPENDIX L	HAZARD ANALYSIS FOR OTI-I AND OTI-L SCENARIOS.....	460
L.1	HAZARD ANALYSIS FOR SOM SCENARIO .....	461
L.2	HAZARD ANALYSIS FOR JOINING SCENARIO.....	470
L.3	HAZARD ANALYSIS FOR SPLITTING SCENARIO .....	484
L.4	ANALYSIS OF TRAIN LENGTH PROVIDED TO OTI-I FROM OTI-L AND ERTMS/ETCS ON-BOARD .....	502
L.4.1	Start of Mission .....	502
L.4.2	Joining/Splitting scenario .....	509

## TABLE OF FIGURES:

Figure 6-1: DEWI bubble architecture.....	31
Figure 6-2: DEWI bubbles for train composition and integrity .....	32
Figure 6-3: SIP architecture.....	33
Figure 6-4: Use Case 19 Smart Train Composition Coupling HLA.....	34
Figure 6-5: Wireless Train Topology Detection Topology .....	35
Figure 6-6 - General physical ETB architecture .....	38
Figure 6-7 – TTDB manager interface telegrams.....	44
Figure 6-8 – TCN-URI resolving .....	44
Figure 6-9 – TCN-DNS name space with division into zones (Source IEC 61375-2-3:2015) .....	45
Figure 6-10 – Overview of the TRDP protocol stack (Source: IEC 61375-2-3:2015).....	46
Figure 6-11 – SDTV2 channel.....	47
Figure 6-12 – ETCS regulations context for OTI.....	54
Figure 6-13 – Freight scenario example for train integrity refresh period .....	56
Figure 6-14 – Passenger scenario example for train integrity refresh period .....	57
Figure 6-15 – Example 1 for OTI Product Class 1-A.....	62
Figure 6-16 – Example 2 of OTI Product Class 1-A.....	62
Figure 6-17 – Example of OTI Product Class 1-B.....	63
Figure 6-18 – Example of OTI Product Class 1-B for central ETCS configuration.....	63
Figure 6-19 – Example of OTI Product Class 2-A.....	64
Figure 6-20 – Example of OTI Product Class 2-B.....	65
Figure 6-21 – Example of OTI Product Class 2-B with waggon and cargo diagnosis.....	66
Figure 6-22 - Passengers trains with fixed composition .....	67
Figure 6-23 – Joined passenger trains .....	68
Figure 6-24 – Train joining: first step .....	69
Figure 6-25 – Train joining: second step.....	69
Figure 6-26 – Train joining: third step .....	70
Figure 6-27 – Train splitting: first step.....	71
Figure 6-28 – Train splitting: second step.....	71
Figure 6-29 – Train splitting: third step .....	72
Figure 6-30 - Freight train.....	72

Figure 6-31 – Diagnostic scenario example 1 .....	73
Figure 6-32 – Central ETCS configuration .....	74
Figure 6-33 – Central ETCS configuration vs Cabin Selection.....	74
Figure 6-34 – Train compositions during dynamic splitting .....	80
Figure 6-35 – Central ETCS configuration vs Cabin Selection.....	82
Figure 6-36 – Terrestrial Networks .....	85
Figure 6-37 - Throughput of 802.11p and 802.11b .....	89
Figure 6-38 - End-to-End Delay of 802.11p and 802.11b.....	89
Figure 6-39 - Delivery ratio of 802.11p and 802.11b.....	89
Figure 6-40 - New PC5 interface .....	100
Figure 6-41 - Cellular Vehicle-to-Everything technology [67] .....	101
Figure 6-42 - C-V2X evolution roadmap [67] .....	102
Figure 6-43: IoT Wide Area Networks.....	103
Figure 6-44 – Distance relation to RSSI measurement. The red line represents RSSI measurements, but the blue line the distance between the Coordinator and the WSN node. ..	115
Figure 6-45 – Calculation of Safe Train Length when train integrity was established.....	116
Figure 6-46 - High Level Architecture AIOTI .....	117
Figure 6-47 - STCC GW architecture.....	117
Figure 6-48 - wOBU proposed architecture .....	118
Figure 6-49 – Pressure tube .....	122
Figure 6-50 – Connected pressure tubes .....	123
Figure 6-51 – Holder of the backboard .....	123
Figure 6-52 – Installation context: suitable areas.....	128
Figure 6-53 – Installation context: unsuitable areas.....	128
Figure 6-54 – Wireless Installation: example for avoiding pairing waggon in near train .....	129
Figure 6-55 GNSS Segments .....	131
Figure 6-56 – <i>GNSS interface to OTI device</i> .....	132
Figure 6-57 – <i>Orbits of GNSS systems</i> .....	133
Figure 6-58 – <i>Reflection, Refraction and Obscuration of GNSS signals</i> .....	136
Figure 6-59 – <i>GNSS Dilution of precision in position domain (PDOP)</i> .....	136
Figure 6-60 Signal propagation model.....	144

Figure 6-61 GNSS Positioning Failure Classification .....	145
Figure 6-62 <i>GNSS-related hazards and structure of causes (negative events)</i> .....	148
Figure 6-63 : OTI Master FSM in GNSS scenario.....	151
Figure 6-64 : Loss of coverage in GNSS scenario .....	152
Figure 6-65: Localization error in GNSS scenario.....	153
Figure 7-1 - ETCS regulations context for OTI.....	157
Figure 7-2 - OTI functional module .....	158
Figure 7-3 - OTI Module: FSM High Level .....	159
Figure 7-4 - OTI Master functional module .....	160
Figure 7-5 - OTI Master Module: FSM High Level .....	160
Figure 7-6 – OTI Master Module: Mastership state.....	163
Figure 7-7 – Mastership management – Example 1 .....	164
Figure 7-8 – Mastership management – Example 2 .....	165
Figure 7-9 – Mastership management – Example 3 .....	166
Figure 7-10 – Mastership management – Example 4 .....	167
Figure 7-11 - OTI Master Module: Inauguration State.....	168
Figure 7-12 – Example of Master-Slave inauguration .....	170
Figure 7-13 - OTI Master FSM – MONITORING STATE .....	172
Figure 7-14: Example of transition from Init to Regular before T_OTIM_I expires.....	175
Figure 7-15: Example of transition from Loss to Regular before T_OTIM_R expires .....	175
Figure 7-16 – OTI Master Sequence Diagram: Initialisation.....	176
Figure 7-17 – OTI Master Sequence Diagram: False alarm filtering .....	177
Figure 7-18 – OTI Master Sequence Diagram: Loss and Restore .....	178
Figure 7-19 – Network functional module .....	181
Figure 7-20 – Example of asynchronous Master-Slave communication.....	184
Figure 7-21 – Example of synchronous Master-Slave communication.....	184
Figure 7-22 - OTI Slave functional module .....	185
Figure 7-23 - OTI Slave Module: FSM.....	186
Figure 7-24 – FSM OTI Slave: Inauguration State .....	188
Figure 7-25 - OTI Slave FSM: Monitoring State .....	189
Figure 7-26 – Sequence diagram in Train Joining scenario – Example 1 .....	192



Figure 7-27 – Sequence diagram in Train Splitting scenario – Example 1 .....	193
Figure 7-28 – Example of OTI sequence diagram in Shunting scenario .....	194
Figure 7-29– Sequence diagram in Train Joining scenario – Example 2 .....	195
Figure 7-30 – Sequence diagram in Train Splitting scenario – Example 3 .....	196
Figure 7-31 – Virtual Coupling - OTI Master: FSM0 .....	197
Figure 7-32 – Virtual Coupling - OTI Master: FSM1=FSM2 .....	198
Figure 7-33 – Virtual Coupling - OTI Master: sequence diagram example .....	199
Figure 7-34 – Virtual Coupling - OTI Slave: FSM0 .....	200
Figure 7-35 – Virtual Coupling - OTI Slave: FSM1=FSM2 .....	200
Figure 7-36 – Virtual Coupling - OTI Slave: sequence diagram example .....	201
Figure 7-37: Product Class 3: Distance between wagons .....	202
Figure 7-38: OTI Master Module: FSM High Level for Product Class 3 .....	203
Figure 7-39: OTI Master Module: Mastership state for Product Class 3 .....	205
Figure 7-40: OTI Master Module: Inauguration State for Product Class 3 .....	206
Figure 7-41: Example of train composition .....	206
Figure 7-42: OTI Master FSM – MONITORING STATE for Product Class 3 .....	208
Figure 7-43: OTI Slave Module: FSM for Product Class 3 .....	210
Figure 7-44: FSM OTI Slave: Inauguration State for Product Class 3 .....	212
Figure 7-45: FSM OTI Slave: Monitoring State for Product Class 3 .....	213
Figure 7-46: Logical System Architecture .....	215
Figure 7-47: FMECA Worksheet .....	221
Figure 7-48: Hazard description sheet .....	221
Figure 7-49: Mitigation sheet .....	222
Figure 7-50: Example of Product Class 1-A .....	224
Figure 7-51: Product class 1-A: example of joining scenario .....	225
Figure 7-52: Product class 1-A: example of splitting scenario .....	225
Figure 7-53: Example of Product Class 1-B .....	226
Figure 7-54: OTI modules configuration with two cabins and one ETCS/ERTMS On-board system .....	226
Figure 7-55: Product class 1-B: example of joining scenario .....	227
Figure 7-56: Example of Product Class 2-A .....	228

Figure 7-57: OTI Master: Check of train tail movement function .....	228
Figure 7-58: Product Class 2-A: joining between two consists.....	229
Figure 7-59: Product Class 2-A: cars/waggons added into the middle of consist .....	229
Figure 7-60: Product Class 2-A: cars/waggons added at the end of consist .....	230
Figure 7-61: Product Class 2-A: splitting between two consists .....	230
Figure 7-62: Product Class 2-A: cars/waggons detached from the middle of consist .....	231
Figure 7-63: Product Class 2-A: cars/waggons detached from the end of consist.....	231
Figure 7-64: Example of Product Class 3-A.....	232
Figure 7-65: Product Class 3-A: joining between two consists.....	233
Figure 7-66: Product Class 3-A: cars/waggons added into the middle of consist .....	233
Figure 7-67: Product Class 3-A: cars/waggons added at the end of consist .....	234
Figure 7-68: Product Class 3-A: splitting between two consists .....	234
Figure 7-69: Product Class 3-A: cars/waggons detached from the middle of consist .....	235
Figure 7-70: Product Class 3-A: cars/waggons detached from the end of consist.....	235
Figure 7-71: Classes for degree of extend.....	252
Figure 8-1: CR940 - Calculation of Safe Train Length .....	255
Figure 8-2: SUBSET 026 §5.17- Changing Train Data from sources different from the driver..	260
Figure 8-3: Start of Mission diagram.....	262
Figure 8-4: DMI Main window dialogue sequence .....	263
Figure 8-5: Use Case 1 - Example 1 (only Train Length) .....	268
Figure 8-6: Receiving of train length during SoM in S20 state .....	269
Figure 8-7: Use Case 1 - Example 2 (only Train Length) .....	270
Figure 8-8: Receiving of train length during SoM in S21 state .....	271
Figure 8-9: Use Case 1 - Example 3 (only Train Length) .....	272
Figure 8-10: Use Case 1 - Example 4 – First part (only Train Length) .....	274
Figure 8-11: Use Case 1 - Example 4 – Second part (only Train Length) .....	275
Figure 8-12: Use Case 1 - Example 5 (Train Length with ACK and Train Integrity).....	277
Figure 8-13: Use Case 1 - Example 6 (Train Length without ACK and Train Integrity).....	279
Figure 8-14: Use Case 2 - Example 1 (Train Integrity and Train Length) .....	282
Figure 8-15: Use Case 3 - Joining procedure – Step 1 – Nominal scenario .....	283
Figure 8-16: Use Case 3 - Joining procedure – Step 2 – Nominal scenario .....	284

Figure 8-17: Use Case 3 - Example 1 (only Train Length) .....	284
Figure 8-18: Use Case 3 - Joining procedure – Step 1 – Degraded scenario .....	285
Figure 8-19: Use Case 3 - Joining procedure – Step 2 – Degraded scenario .....	285
Figure 8-20: Use Case 3 - Example 2 (only Train Length) .....	286
Figure 8-21: Use Case 3 - Example 3 (Train Length and Train Integrity) .....	288
Figure 8-22: Use Case 3 - Splitting procedure – Step 1 – Nominal scenario.....	289
Figure 8-23: Use Case 3 - Splitting procedure – Step 2 – Nominal scenario.....	289
Figure 8-24: Use Case 3 - Example 4 (Train Length and Train Integrity) .....	291
Figure 8-25: Use Case 4 - Example 1 (Train Integrity and Train Length) .....	293
Figure 8-26: Example of Train Length and Train Integrity reception during SoM.....	296
Figure 8-27: Example of Joining operation .....	297
Figure 8-28: Example of Train Length and Train Integrity reception after joining operation.....	298
Figure 8-29: Example of Splitting operation .....	299
Figure 8-30: Example of Train Length and Train Integrity reception after splitting operation ....	300
Figure 8-31: FSM for train length determination .....	305
Figure 8-32: OTI-L FSM .....	306
Figure 8-33: OTI-L: RUNNING State .....	307
Figure 10-1: Management of Train Length by OTI-I .....	503
Figure 10-2: Management of Train Length by OTI-I – Degraded condition 1 .....	505
Figure 10-3: Management of Train Length by OTI-I – Degraded condition 2 .....	506
Figure 10-4: Management of Train Length by OTI-I – Degraded condition 3 .....	507
Figure 10-5: Management of Train Length by OTI-I – Joining scenario .....	510
Figure 10-6: Management of Train Length by OTI-I – Splitting scenario .....	511

## TABLE OF TABLES:

Table 6-1 - ETB Link Layer requirements .....	39
Table 6-2 – ETB Transport Layer requirements.....	40
Table 6-3 – Specific Requirements in S2R Application Domains relevant for OTI context .....	55
Table 6-4 – Product Classes 1 and 2.....	60
Table 6-5 – Product Classes 3 .....	61

Table 6-6 – 802.11a/b/g/n/ac characteristics .....	87
Table 6-7 – 802.11ah characteristics.....	88
Table 6-8 802.11p characteristics.....	90
Table 6-9 - 802.15.1 Bluetooth characteristics.....	91
Table 6-10 - 802.15.4 ZigBee characteristics .....	92
Table 6-11 - IEEE 802.15.4 6LoWPAN.....	93
Table 6-12 - 802.15.4 Thread characteristics .....	94
Table 6-13 - 802.16 WiMAX characteristics.....	95
Table 6-14 - Z-Wave characteristics .....	96
Table 6-15 – ANT characteristics .....	104
Table 6-16 – NB-IoT .....	105
Table 6-17 – LoRaWAN .....	107
Table 6-18 – SigFox.....	108
Table 6-19 – Symphony Link.....	109
Table 6-20 – EnOcean characteristics.....	111
Table 6-21: Results in Gulbene-Alūksne railway testing .....	114
Table 6-22 - Typical frequencies for transponder systems (SBB Cargo, 2013).....	119
Table 6-23: Railway-related projects dealing with GNSS – related aspects .....	143
Table 7-1: OTI Master Module: FSM High Level Transitions.....	161
Table 7-2: OTI Master module: FSM High Level Transition conditions .....	162
Table 7-3: Priority table of OTI Master Module FSM.....	162
Table 7-4: OTI Master: FSM Transitions.....	173
Table 7-5: OTI Master: FSM Transitions conditions.....	174
Table 7-6: OTI Slave Module: FSM Transitions .....	186
Table 7-7: OTI Slave Module: FSM Transitions conditions .....	187
Table 7-8: Priority table of OTI Slave Module FSM.....	187
Table 7-9: OTI Master Module: FSM High Level Transitions for Product Class 3.....	203
Table 7-10: OTI Master module: FSM High Level Transition conditions for Product Class 3 ...	204
Table 7-11: OTI Master of Product Class 3: Monitoring State Transitions conditions.....	209
Table 7-12: OTI Slave Module: FSM Transitions for Product Class 3 .....	211
Table 7-13: OTI Slave Module: FSM Transitions conditions for Product Class 3 .....	211

Table 7-14: Failure Mode .....	217
Table 7-15: Severity Level (EN 50126).....	218
Table 7-16: Frequency or Probability of Occurrence.....	219
Table 7-17: Risk Categories .....	219
Table 7-18: Risk evaluation and acceptance .....	219
Table 7-19: List of identified hazards .....	238
Table 7-20: List of safety-related mitigations .....	243
Table 7-21: Basic restrictions for electric, magnetic and electromagnetic fields (0-300 GHz) ..	246
Table 7-22: Reference levels for electric, magnetic and electromagnetic fields (0-300 GHz) ...	247
Table 8-1: Transitions between values of the train integrity status information to be reported to the RBC (CR940) .....	256
Table 8-2: Transition conditions for the train integrity status information to be reported to the RBC (CR940) .....	257
Table 8-3: extract of Handling of Accepted and Stored Information in specific Situations table defined in Subset026-3 ([1]) .....	257
Table 8-4: extract of Active Functions table defined in Subset026-4 ([1]) .....	258
<b>Table 8-5:</b> extract of DMI Input table defined in Subset026-4 ([1]).....	259
<b>Table 8-6:</b> extract of “Accepted information depending on the level and transmission media” table defined in Subset026-4 ([1]) .....	259
Table 8-7: extract of “What happens to accepted and stored information when entering a given mode” table defined in Subset026-4 ([1]).....	259
Table 8-8: Extract from Subset-119.....	263
Table 8-9: Uses Cases.....	266
Table 8-10: List of hazards for Train Integrity and Train Length Determination functions.....	302
Table 8-11: List of Mitigations for Train Integrity and Train Length Determination hazards .....	304
Table 8-12: Traceability: Hazards Train Length Determination – Mitigations .....	304
Table 8-13: OTI-L: FSM Transitions .....	306
Table 8-14: OTI-L: FSM Transitions conditions .....	307
Table 8-15: RUNNING State internal transition condition .....	307
Table 10-1: Hazard Module .....	445
Table 10-2: Hazard field description .....	448
Table 10-3: Mitigation list.....	457

Table 10-4: Mitigation field description .....459

### 3 Abbreviations, acronyms, terms

Abbreviation / Acronyms	Description
BeiDou	Chinese Navigation Satellite System
BG	Balise Group
DMI	Driver Machine Interface
DOP	Dilution of Precision
EGNOS	The European Geostationary Navigation Overlay Service (SBAS version)
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
FMECA	Failure Modes, Effects, and Criticality Analysis
FS	Full Supervision mode
FSM	Finite State Machine
GALILEO	European Global Satellite Navigation System
GBAS	Ground-based augmentation system
GLONASS	GLObal NAVigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
INS	Inertial navigation system
Level 3	Application level defined in [1]
LRBG	Last Relevant Balise Group
LS	Limited Supervision mode
MEMS	Microelectromechanical systems
NLOS	Non Line Of Sight
OBU	On-board Unit
OCN	On-board Communication Network
OCP	On-board Communication Protocol
OS	On-sight mode
OTI	On-board Train Integrity
OTI-I	On-board train Integrity providing the Train Integrity status (Train Integrity status functionality)
OTI-L	On-board train Integrity providing the Train Length value (Train Length determination functionality)
OTI-M	OTI Master
OTI-S	OTI Slave
PHA	Preliminary Hazard Analysis
PT	Post Trip mode
PTV	Position Velocity Time
RBC	Radio Block Centre
RV	Reversing mode
SB	Stand-by mode
SBAS	Satellite-based augmentation system
SIS	Signal in Space
SN	National System mode
SoM	Start of Mission
SR	Staff Responsible mode
TI	Train Integrity status

TIN	Technical Informative Note
TIU	Train Interface Unit
TL	Train length value
TR	Trip mode
UN	Unfitted mode
WMC	Wayside Maintenance Centre
WOCN	Wireless On-board Communication Network

For the following terms refer to [76]:

Term	Description
BALISE	A passive transponder mounted on the track which can communicate with a train passing over it
BALISE GROUP	One or more balises which are treated as having the same reference location on the track. The telegrams transmitted by all the balises of a group form a track-to-train message
Cab/Cabin	The space in the power unit or driving unit of the train containing the operating controls and providing shelter and seats for the driver or engine crew
CAB, ACTIVE	The active cab is the cab associated with an ERTMS/ETCS on-board equipment, from which the traction is controlled
Desk	Inside a cab, the set of operating controls, which is dedicated to preferred movements in a given direction (i.e. forward movements, in which visibility from the cab is provided to the driver). Exception: some single cab locomotives are fitted with one single desk, allowing normal movements in both directions
DMI	The interface to enable direct communication between the ERTMS/ETCS on-board equipment and the driver
ERTMS/ETCS On-board	The part (software and/or hardware) of the on-board equipment, which fulfils the ERTMS/ETCS specification
Level 3	A level of ERTMS/ETCS that uses radio to pass movement authorities to the train. Level 3 uses train reported position and integrity to determine if it is safe to issue the movement authority.
MISSION, ETCS	Any train movement started under the supervision of an ERTMS/ETCS on-board equipment in one the following modes: FS, LS, SR, OS, NL, UN, or SN. The ETCS mission is ended when any of the following modes is entered: SB, SH
NON-LEADING MODE	ERTMS/ETCS on-board equipment mode when it is connected to an active cab which is not in the leading engine of the train.



## 4 Background

---

The present document constitutes the first issue of Deliverable D4.1 “Train Integrity Concept and Functional Requirements Specifications” in the framework of the Project titled “Enhancing railway signalling systems based on train satellite positioning, on-board safe train integrity, formal methods approach and standard interfaces, enhancing traffic management system functions” (Project Acronym: X2Rail-2; Grant Agreement No 777465).

## 5 Objective

---

This document is focused on On-board Train Integrity concept and functional requirements.

Concept is intended in terms of state of art, product classes and reference scenarios, investigation on wireless sensors and transponder technologies, installation analysis and feasibility for adopting GNSS.

State of art constitutes the starting point as analysis of existing project related to on-board train integrity topic. Product classes and reference scenarios identifies general guidelines and high level functions as input for subsequent functional requirements specification. Description of existing technologies for wireless communications constitutes a reference background for subsequent candidate technologies selections and product development. Installation analysis provides general guidelines for product definition in freight applications. GNSS feasibility analysis explores satellite based localization technologies in train integrity applications.

Requirements specification is referred at functional level and is supported by a functional hazard analysis, moreover general guidelines are defined in relation to radio communications and energy harvesting.

On-board Train Integrity functional module is defined as external functionality respect to ETCS Core logic specified in Sub026 and CR940. In relation to the four Shift2Rail Application domains (i.e. Intercity-High Speed, Regional, Urban-Suburban, Freight) the following requirements have been identified as relevant for OTI functionality: train composition, head-tail communication, power supply, train tail status and availability of ETCS at train tail. On this bases three OTI product classes have been defined with modular approach respect to costs and functionalities. In general the Train Integrity Monitoring System is composed of a OTI Master module located in front cabin, an OTI Slave module located at train tail and an on-board communication network.

In general the trains with a wired communication network are addressed by OTI Product Class 1, whereas OTI Product Class 2 is defined for trains with wireless communication network. The main difference between the two product classes consists in train integrity criteria that in presence of wired on-board network is based on communication liveness, whereas in presence of wireless on-board network requires verifying train tail coherent movement respect to front cabin. In fact communication between train tail and front cabin could be present also after train splitting with limited distance of separated waggons in presence of wireless on-board network. In Product Class 2 the train length is assumed to be an input to OTI functionality (i.e. train length entered by train driver during data entry procedure). The safe train length determination is addressed by Product Class 3 and requires OTI module installed in each wagon and includes wagon length as configuration parameter.

Functional requirement specification started from defined product classes and analysed relevant operational scenarios (e.g. train joining/splitting, rescue, shunting) thus identifying OTI macro-functionalities (e.g. Mastership phase to identify OTI Master/Slave role, inauguration phase to pair OTI Master with OTI Slave at train tail and monitoring function focused on train integrity criteria). On this bases OTI Master FSM and OTI Slave FSM have been designed.

Note that X2Rail-2 WP4 scope of Work is limited to defining the requirements for On-board Train Integrity functionality. The ETCS rules to manage train integrity information inside Position Report messages, the RBC rules to manage the received train integrity information and train driver or railway operator rules in managing emergency situation for loss of integrity are out of X2Rail-2 WP4 scope of work.

## 6 Concept

---

### 6.1 State of Art

This section contains the state of art regarding the train integrity function developed around the world. In some case there are ongoing studies on systems in operation that have not yet been finalized.

There aren't common specifications for this function in term of performance and safety integrity level. For this reasons an overview of the areas deemed most significant and of what is in operation will be provided.

#### 6.1.1 Introduction

The identification of the integrity of the train has always been a very important function in the railway field, especially in those contexts in which there is no presence of train detection systems installed on the tracks.

This function takes on greater importance when we introduce ETCS level 3 for which Train Integrity SIL4 function is mandatory.

The absence of trackside train detection systems shifts more responsibility for the safe operation of the railway from the infrastructure managers to the railway undertakings. The latter have to make sure by means of vital technical On Board equipment and safe operational procedures that their trains remain complete throughout the whole journey.

Any left alone or lost vehicle would result in a non-detectable obstacle on the track endangering the safe journey of other trains. Like the trackside train detection systems, on-board train integrity monitoring systems need to comply with the highest safety integrity levels.

On high speed trains and lines operated with short headways these systems require high performance in terms of detection of any loss of train integrity or system failure which has to be notified to the trackside control centre within seconds.

The technical solutions for train integrity heavily depend on whether the trains have an overall electrical infrastructure or whether the air brake pipe is the only link between the vehicles besides the mechanical couplings.

Modern passenger trains are equipped with bus systems used for traction and vehicle control functions, traditional mainline trains are using the cable which has cores that can be used to implement a train bus system. On these trains a train integrity system can be implemented with reasonable engineering effort, the main challenge is the high safety requirements of this function compared to the non-vital train control functions. In some countries passenger and freight trains are equipped with automatic couplings or EP brake systems.

The electrical infrastructure of these systems could also be used as the backbone of a train integrity system.

The ultimate challenge for monitoring train integrity is with freight trains that have no electrical infrastructure along the train. This is the field which most of the patent applications on the matter are focusing on. An analysis of these patents shows different solutions which can be classified into two classes for on-board application.

- 1) Systems relying on an end of train device:

- Detection of the train head and tail position by means of satellite positioning systems. The position of the train end device is transmitted by radio to the evaluation unit installed on the leading vehicle. Due to the non-continuous coverage by satellite signals through shading caused by buildings, topography and tunnels a satellite based system needs to be complemented by at least a second, diverse system.
  - Radio devices at head and tail of the train, evaluation of the signal transmission time on the leading car.
  - Detection of brake air pipe pressure reduction on the last vehicle and radio transmission of the status to the evaluation unit on the leading vehicle.
  - Train end device feeding acoustic waves into the brake air pipe which are evaluated on the leading vehicle.
- 2) Systems needing no train end device
- Monitoring of several parameters of the air brake pipe on the leading vehicle like pressure or volumetric air flow.
  - System injecting acoustic signals into the brake air pipe on the leading car and evaluation of the reflections.

What is on the market and will be described in the following paragraphs is a set of existing systems and projects in progress.

Most of the existing systems are used outside Europe for applications on freight trains on very long lines often single track.

In this paragraph there is a description of the different applied technologies, of open points not yet resolved and if available for each application described we will try to provide the economic impact.

### 6.1.2 DEWI Project

The following information on the DEWI project was obtained from the “DEWI - Wirelessly into the Future” [46] Conference paper, the public cited deliverables from the DEWI project [47] and own INDRA expertise as member and leader of Rail domain in the project.

In DEWI the Rail domain developed four different Use Cases:

1. *Train Integrity Detection System*: This system has the clear functionality to ensure the completeness of the train.
2. *Train composition Detection System*: This system shall be able to collect important variables of the train, like the length or the waggon in order to be used by the on-board units.
3. *Smart Integration Platform*: This is a platform able to store and manage the collected data from sensors in order to provide it to train systems.
4. *WSN for freight advanced monitoring and management*: This comprises a system for freight monitoring in goods transport and a system for freight monitoring optimized in underground worksites.

From this Use Cases, three are related to this WP. This three Use Cases developed functional demonstrators up to TRL5:

- *Train Integrity Detection System*: Both, real and laboratory tests were performed. In the laboratory tests, the whole system was tested in a simulated environment on test beds. After the laboratory tests the system was tested, validated and assessed in a real-life

mock-up demonstration on a touristic train. The integrity of a train was controlled by monitoring the completeness of a train composition.

- *Train composition Detection System:* Laboratory tests were carried out over a simulated environment. The Train Integrity demonstrator above supported this Composition Detection System.
- *Smart Integration Platform:* The demonstrator was carried out in laboratory, but the Smart integration Platform was used in the real-world demonstration because it is part of the system developed in the Train Integrity Detection System.

The real life mock-up described in the final DEWI X2Rail-2 WP4 deliverable supposes a real demonstration about the usability of WSN in the Rail framework, where this type of technology has not been used before.

The demonstrator was an added value to the laboratory demonstrators described in the D.400.001 and D.400.002, where the Train integrity and train composition detection systems were designed and developed. This mock-up was done to confirm the results of the laboratory tests but in a real environment. This gave the opportunity to study additional points like the behaviour of the systems in bad weather conditions, real interferences, etc.

Some tests were the same as the laboratory tests to demonstrate that the results were the same. This proved the results on deliverables D401.1.6 for Train integrity static tests, and D4.2.5 for Train Composition static tests.

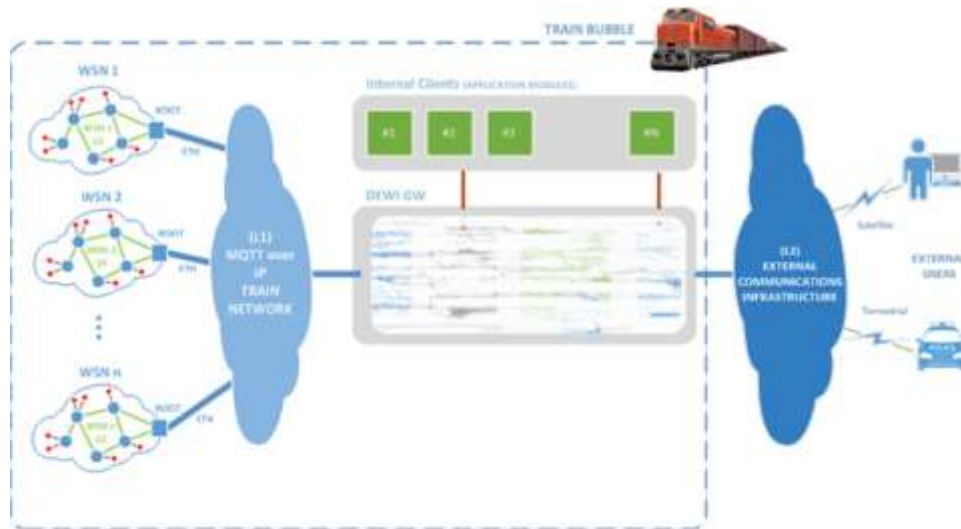
From the dynamic tests, it is possible to conclude that the results were successful. The demonstrator for the dynamic tests were carried out with a touristic train making use of a 750mm narrow gauge train. Located in the Country of Latvia - Vidzeme. The train connects two towns Gulbene and Aluksne (34km) on a daily basis.

In the testing site, a locomotive with two waggons was available for test purposes, taken into consideration that the locomotive was used as a third waggon. This allowed the team to produce the proof-of-concept tests for the project.

The results for Indra, which are in line with most of the partners in the DEWI project proved that this demonstrator provided evidences about the usability of WSN based solutions to sense the train composition and the completeness of the train.

The different tests took into consideration the hard environmental effects which probed the reliability of the adopted solution combining the different and complementary WSN and its efficiency as well as the ease of installation and use.

The DEWI architecture was used as the base for the design of the wireless train integrity control system. This architecture comprises three layers to structure the communications within the system limits as well as with the exterior.

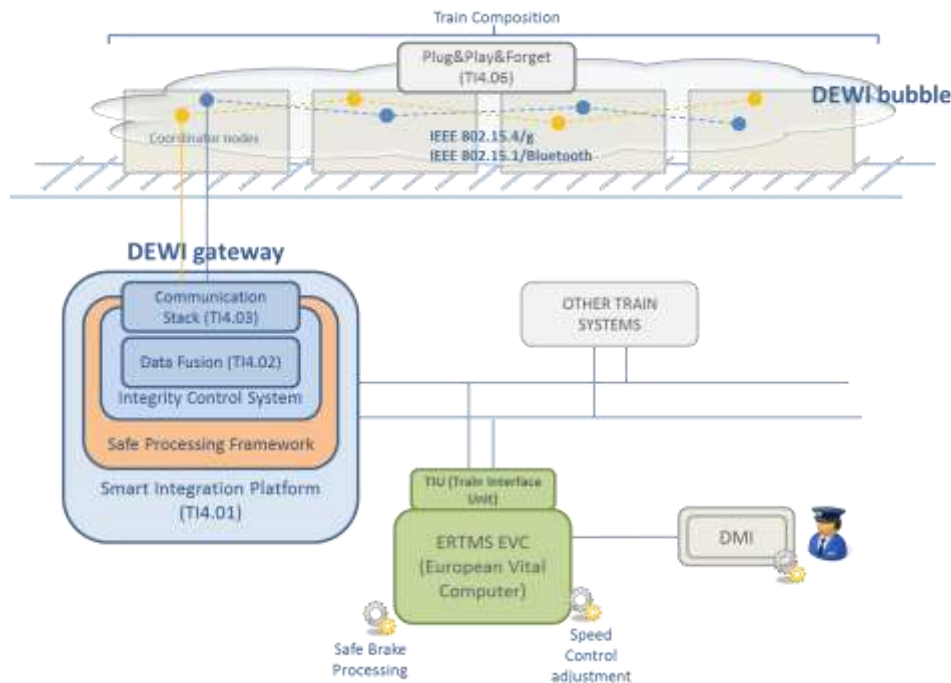


**Figure 6-1: DEWI bubble architecture**

The DEWI architecture consists of two main subsystems the DEWI bubble and the DEWI Gateway:

- DEWI bubble provides services for controlling train completeness by monitoring and controlling network nodes. It should also provide automatically relevant train composition data (length, weight, max load, breaks...).
- DEWI Gateway implements – using the SIP Platform - a safe train integrity control system providing safe interfaces to existing train control systems (e.g. ETCS). This Gateway provides the calculation needed to provide a safe Train Integrity.

On the following figure, the connectivity of the DEWI Gateway is shown in more detail. On the lower right part, the connection with other train systems (EVC, DMI, and RBC) is shown. On the top part of the figure, the DEWI bubble concept is shown applied to the train composition and integrity system.



**Figure 6-2: DEWI bubbles for train composition and integrity**

The DEWI bubble is composed in this case by multiple WSNs. Three different WSNs were tested:

1. WSN1: The train integrity system developed by Adevice consists of a number of wireless sensors deployed in the train and a data concentrator that gather information from every sensor and integrate the processed information into the train management systems. Wireless devices installed on waggons are based on Ultrasound sensors.
2. WSN2: The physical union between the rear node of a waggon and the front node of the next one is detected using reed switches and magnets. While all the waggons are moving together, each magnet is near its associated reed switch. When one waggon separates from another one, the reed switches detect the absence of the magnets and an integrity fault alarm is reported.
3. WSN3: Each waggon of the train is equipped with a WSN node, which measures accelerometer and GPS data. Acceleration and velocity measurements are also sent to the Coordinator (located on the locomotive), which holds the accelerometer and GPS reference measurements against which, the measurements from each node are compared to detect the train integrity

Indra implemented the DEWI Gateway concept for a safe processing of WSN services suitable to be integrated in rail environment, in train control systems and rail safety ambient. This DEWI Gateway was the Task 4.3 of the DEWI project (Smart Integration Platform (SIP)).

As shown on the following picture the SIP has been implemented based on open and standardized platforms, avoiding proprietary environments and solutions based on legacy systems, and providing open interfaces for existing railway systems.



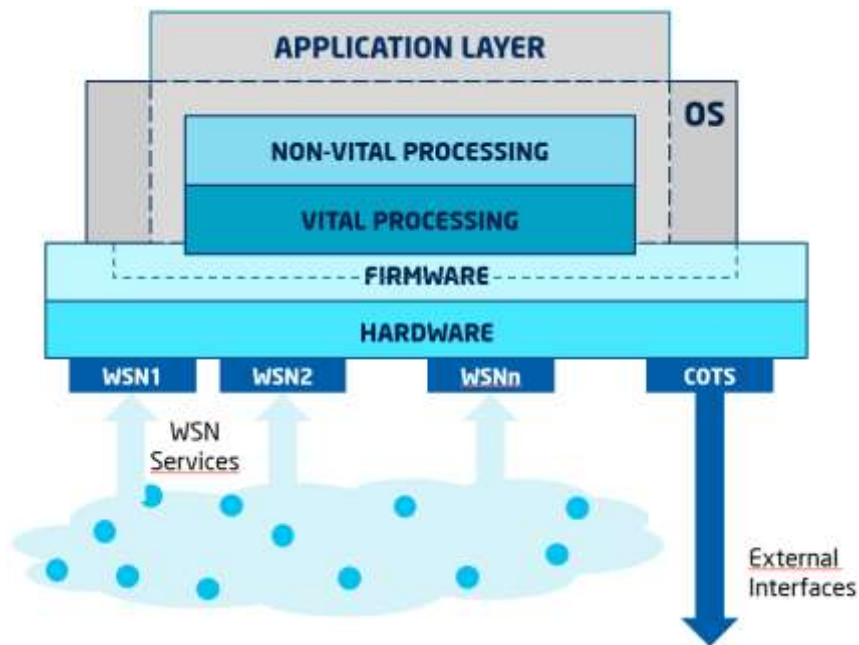


Figure 6-3: SIP architecture

### 6.1.3 The DEWI project Demonstrator

As shown in section 6.3.7, what was developed in the DEWI project had the following characteristics:

- The GW was safe (SIL4). The SIP was certified CENELEC EN50155 as SIL4.
- The WSNs did not need to be safe (SIL2). No certifications were passed.
- The demonstration was 3 days long during 8 hours a day. A total of 24 hours OTI system testing.
- The results proved that no significant alarm was raised during the 24 hours of testing.
- The alarms were raised using a voting system, only when two sensors raise an alarm, the system raises an alarm.

### 6.1.4 SCOTT Project

The following information about the SCOTT project was compiled from the public deliverables published up to this point, as well as INDRA's own expertise as member and main leader of the rail domain use cases developed during the project.

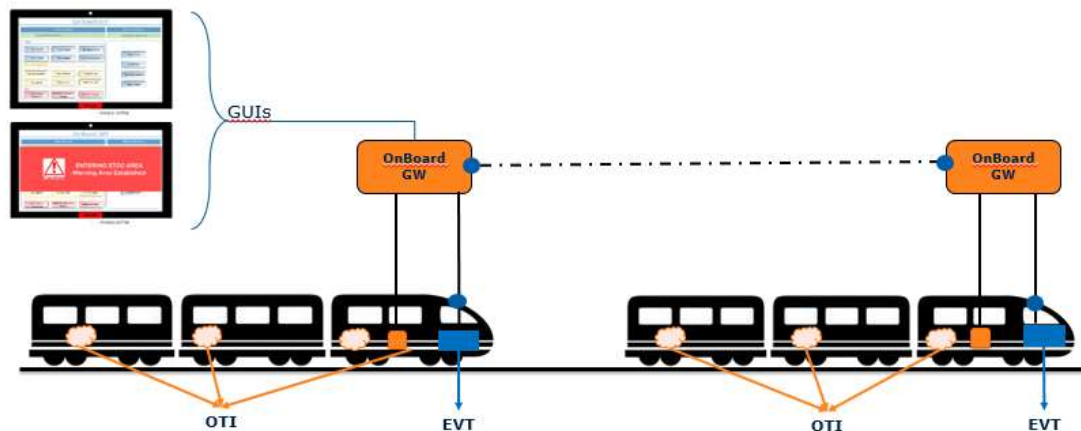
The SCOTT project is a follow-up of the DEWI project. The rail domain within project develops three main use cases:

- **UC18 Autonomous Wireless Network for Logistics and Maintenance:** The main objective of this Work Package is to develop an Autonomous Wireless Communication Network for Rail Logistics and Maintenance –AWN- that will provide all the information from the infrastructure and the train to a centralized system (Cloud, TMS) using wireless technologies that will reduce in both, wire costs and civil works going towards I2I communications.

- **UC19 Smart Train Composition Coupling (STCC):** This system addresses the possibility to achieve a Smart Train Composition Coupling between two or more trains in order to get a unique composition. It would allow the circulation of the trains keeping a shorter distance between them, and as consequence, it would be possible to increase the capacity of the lines.
- **UC20 Trustable Warning System for Critical Areas:** The main innovation consists of a smart sensor system that detects dangerous obstacles on the tracks and replacing wired functionality and adding warning functionality for the train driver

Inside these use cases different developments are envisaged. Major points, as part of the development of Use Cases 19 and 20 further improvements on the TI developed during the DEWI project are planned. This new Train Integrity solution will solve problems that were found during the development of the DEWI project.

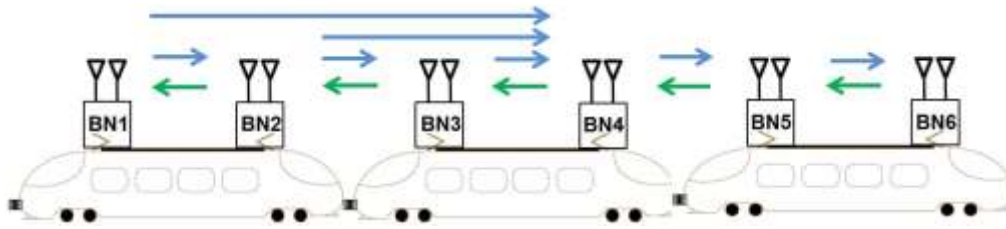
In Figure 6-4, the High-level architecture of the Use Case related to Train Integrity is shown.



**Figure 6-4: Use Case 19 Smart Train Composition Coupling HLA**

The Smart Train Composition Coupling Use Case treats the virtual coupling through local Vehicle to Vehicle (V2V) communications. This enables Virtual Coupling to be performed offline, without connection to the infrastructure. Indeed, it makes on-board Train Integrity detection compulsory for the development of the Use Case.

In the SCOTT project, a complete implementation of the Wireless Train Topology Detection Protocol (WTDP) has been performed. The WTDP is a wireless implementation of the Train Topology Detection Protocol (TTDP).



**Figure 6-5: Wireless Train Topology Detection Topology**

### 6.1.5 Wireless Sensor Network (WSN)

In this section, the different technologies that could be used to measure the status of a train composition connection are exposed. This state of the art is a simple exposition of the different technologies available in the market that can measure this status.

In section 6.3.5 Available Wireless Sensors a detailed description on how these sensors could be used is presented. A more detailed explanation can also be found.

#### 6.1.5.1 Ultra sound sensor

Ultrasound is a feasible, certified and widely tested technology, which can provide robust communications based on low density modulation schemes (2-FSK, 4-FSK). Without the need of a high reception power level the system can reach rates from 1.2 to 9.6 kbps. The former rates could be considered enough to share identification data with low delay values.

In terms of consumption, the ultrasound sensors require low values of current to reach the power budget requirements (order of mA).

#### 6.1.5.2 Reed switches

A candidate, which could be useful to reduce the deployment problems and foster its agile development, is the detection based on reed switches. It is based on reed switches, which requires low power consumption requirements because they are based on the deformation of their metallic filaments under the presence of an electromagnetic field. The sensors are deployed together with magnets, which keep the filaments joined, if the magnet disappears it will mean that the waggons are not coupled any more. In the former case, the integrity alarm will be reported to the network.

#### 6.1.5.3 RSSI based sensitization

The Received Signal Strength Indicator (RSSI) sensitization could be used as a reporter of Train Integrity. The distance among waggons in a composition is fixed so the signal strength should be between constrained values. It may differ as the waggons change their position in curves or during breaking/acceleration actions.

This node will raise a train integrity lost alarm to the coordinator when the RSSI values differ a big amount from the predicted value.

#### 6.1.5.4 **Accelerometer**

The accelerometer provides acceleration data of each waggon. By exchanging this information among waggons, the system could check the train integrity. The speed information from the different waggons shall not differ much.

An alarm on a loss of Train Integrity will be raised when the information from the different accelerometers installed in the composition differ above a certain threshold.

#### 6.1.5.5 **GNSS**

The GNSS systems could provide a complementary source of data for the position and speed of the waggons with a reasonable accuracy. This node will transmit the information on the location and speed to the coordinator where it will be compared among waggons to determine the integrity.

#### 6.1.5.6 **RADAR Detection And Ranging (RADAR)**

The RADAR can calculate the relative position and speed of an object with respect to the sensor. The RADAR uses radio waves to calculate these parameters of a target. The RADAR sensor can provide an accurate measurement of the distance between the waggons in a composition.

This system has been proven in military appliances since II world war. This system has been widely studied and a minimum distance of 0.05m detection was proven as part of the “Automotive radar sensor for ultra-short range applications” [51] study in an ITS context.

#### 6.1.5.7 **Light Detection And Ranging (LIDAR)**

The LIDAR is an evolution of the RADAR making use of pulsed light. The LIDAR systems can find the relative distance and speed between the sensor and the target object. This could be used to measure the distance between waggons and the shape, differentiating the waggons by shape, for example.

The LIDAR systems commonly use pulsed light emitting systems and a camera for capturing. With these two subsystems a 3D scan of near objects can be performed. This system is highly affected by the environmental conditions.

The use of LiDAR has been studied in the United States for the diagnosis of the rural side tracks. [52]

#### 6.1.5.8 **LAser Detection And Ranging (LADAR)**

The LADAR is an evolution of the LIDAR making use of laser subsystems. The LADAR systems can find the relative distance and speed between the sensor and the target object. This could be used to measure the distance between waggons and the shape, differentiating the waggons by shape, for example.

The LADAR systems commonly use pulsed laser emitting systems and laser receivers for capturing. With these two subsystems a 3D scan of near objects can be performed. This system is highly affected by the environmental conditions.

In this study, a LADAR system has been used to extract the railroad centerlines “Automatic Extraction of Railroad Centerlines from Mobile Laser Scanning Data” [53].

#### **6.1.5.9 Radio-Frequency Identification (RFID)**

A RFID system could provide train integrity through train composition. By checking and transmitting the composition and integrity through active RFID links the system could add a solution to the train integrity paradigm.

RFID tags have been used by railways for many years, RFID has proven its worth in inventory management. Yet this technology is underutilized for enhancing railway operations and health monitoring due to the limitations of passive RFID technology. Active RFID provides enhanced capabilities with the potential to improve railway operations. [55] GS1/EPCglobal as a standard defines data format, capture and query interfaces for RFID tags EPC Gen 2 UHF (ISO 18000-63) [54].

#### **6.1.6 Network Discovery Techniques**

The Train Control and Monitoring System (TCMS) is a distributed control system which comprises computer devices and software, human-machine interfaces, digital and analogue input/output (I/O) capability and the data networks to connect all these together in a secure and fault-resistant manner. TCMS provides a set of functions for train control. One of these functions is the Train Network Discovery which is a result of the Train Inauguration Process. Depending on the train-level network used the inauguration process is different, therefore in the next subsection a brief summary of the standardized networks is provided. After, the inauguration process used in each network type will be explained. Finally, the ongoing work for providing a new standard which will include a safe train topology to be used by safety-related applications will be introduced.

##### **6.1.6.1 TCMS Networks**

###### **6.1.6.1.1 Wire Train Bus (WTB) – legacy**

Wire Train Bus (WTB) is a serial data communication which features Real-Time Protocols, which offer two communication services: process variables, in a form of a distributed real-time database periodically refreshed through broadcasting; and message transmitted on demand. These messages may be unicast or multicast.

WTB in the TCN offers a common Network Management, which allows debugging, commissioning and maintenance over the network.

As a physical medium, WTB relies on twisted wire pair bus which works at 1Mbps and ensures an end-to-end propagation delay not higher than 60,0µs between any two nodes.

In WTB nodes are inserted in a trunk cable and connected to two bus sections with the exception of nodes located in the ends of the bus which shall electrically terminate the bus. These two cable sections attached to a node shall be named `Direction_1` and `Direction_2`.

Where orientation of the nodes is critical to the left-right recognition, e.g. for Doors control, the following conventions shall be observed:

- a) one end of the consist is identified as Extremity 1, the other as Extremity 2;
- b) if Direction\_1 points north, the side of the consist that points west is named side A, the side which points east is named side B;
- c) a node uses the same conventions for A and B as the consist it is located in.

The link layer of WTB uses an 8-bit identifier both for the source and destination Device\_Address.

From this address pool, addresses from 64 to 126 and from 128 to 254 are reserved for future use. Additionally, address 255 ('1111 1111'B) shall be the broadcast address, to which all nodes listen. An unnamed node shall respond to address 127 ('01111111'B) over both its channels.

The Frame\_Data format is compliant with the HDLC format defined by IEC 13239.

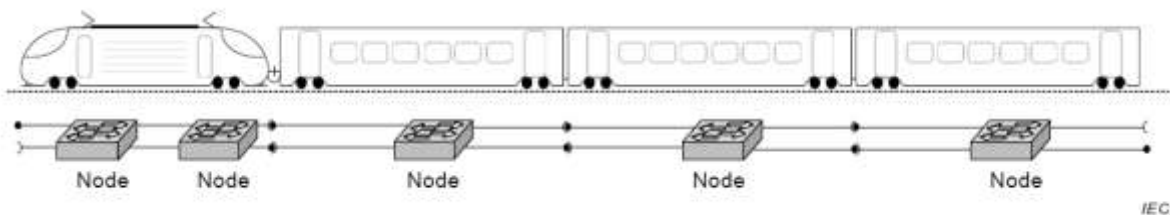
The bus segment is controlled by one master node, which transmits at its own pace on the bus. This master request information to slaves, which only transmit when are requested by the master.

WTB distinguishes three data types

- Process Data: used to update the distributed Process data base.
- Message Data: used for message transfer.
- Supervisory Data: used for bus supervision and inauguration

#### 6.1.6.1.2 Ethernet Train Backbone (ETB)

The norm IEC 61375-2-5 defines the Ethernet Train Backbone used to communicate different type of consists coupled in the same train composition. This norm uses the OSI protocol stack layers as a reference and makes a bottom-up explanation from physical layer to application layer.



**Figure 6-6 - General physical ETB architecture**

The general physical architecture of the ETB network is depicted in Figure 6-6. The general requirements for the ETB physical layer architecture are the following:

- As a switched technology is used, nodes shall provide a data transmission medium to each of their direct neighbour nodes, if present. Each ETBN has at least one ETB forward port and one ETB backward port statically defined.
- When optional redundancy is required, data transmission medium shall be at least doubled.
- Even without redundancy requirement, the link between 2 ETBNs shall be doubled using normal switch ports when Consist reversing capability is required.
- A bypass relay function shall bridge a node if the node is powerless or not operating.

At Link layer, ETB must fulfil the requirements summarized in Table 6-1 - ETB Link Layer requirements

From this set of requirements it must be highlighted that ETB implements L2 QoS as well as VLANs, therefore traffics from different services can be treated differently, providing to each one the needed network requirements and priority. It is also worth noting that ETB uses Link Layer Discovery Protocol (LLDP) as a basis for the Train Topology Discovery.

Requirements	Description
Frame Relaying (IEEE 802.1D)	Frame reception, Frame transmission, Forwarding process which comprises: Queuing, QoS Priority mapping, FCS calculation, etc.
Frame Filtering (IEEE 802.1D)	Learning process, Filtering data base (Mac addresses, ports, VLAN association), static/dynamic entries
Frame Queuing (IEEE 802.1D)	Multiple traffic classes (TC) for relaying frames; assign ingress frames a defined priority.
Frame tagging/untagging (IEEE 802.3 and IEEE 802.1Q)	Ethernet frames can be tagged during switch port ingress. The tag can then remain within the frame or can be removed during port egress.
VLAN Services (IEEE 802.1Q)	Helps subdividing the physical LAN in different virtual LANs.
LLDP protocol Link Layer Discovery Protocol (IEEE 802.1AB)	Used by Train Topology Discovery Protocol between trains.
Management and Remote Management (IEEE 802.1D)	Configuration of the switch, Fault management (detection / diagnostic / correction), Performance management (statistics, bandwidth measurement capability). Only supported on managed ND.

**Table 6-1 - ETB Link Layer requirements**

Regarding the Network Layer requirements, ETB uses IPv4 protocol (defined in the IETF RFC 791) for its addressing. It is also established as mandatory for each End Device to have a unique hostname in the same consist statically defined. The IPv4 addressing must be in the range

10.128/9 and it is dynamically defined as a result of the inauguration process. Each consist applies the network mask 255.255.255.192.0, i.e. each consist has 14 bits for host identification. The following bit set defines the IPv4 addressing use in TCMS:

**00001010.1bbxssss.sshhhhhh.hhhhhhhh/18**

The first 9 bits (10.128.x.x/9) are fixed. The 'b' bits identify the backbone ID and are used to separate the addressing used for different domains, i.e. '0' is used for the applications of the TCMS domain and '1' is used for applications of the OTMS domain. The 'x' bit is a reserved bit and it shall be set to 0. The 's' bit set defines the subnet ID and it is calculated during the Train Inauguration. One subnet ID corresponds to one consist and it is represented as a 6-bits unsigned integer.

Apart from the unicast IP addressing, the following multicast addresses are used:

- Train level: 239.192.0.0/14
- Consist level: 239.255.0.0/16

It is worth noting that the address 239.192.0.0 can be listened by all nodes of all consist of the train.

Table 6-2 summarizes transport layer requirements for a device connected to the train backbone subnet.

Requirements	Description
ICMP Internet Control Message Protocol (IETF RFC 792)	
IGMP v2 Internet Group Management Protocol (IETF RFC 2236)	End Devices shall support IPv4 multicast.
UDP User Datagram Protocol (IETF RFC 768)	
TCP Transmission Control Protocol (IETF RFC 793)	

**Table 6-2 – ETB Transport Layer requirements**

### 6.1.6.2 Train Inauguration Processes

#### 6.1.6.2.1 WTB

The inauguration process in WTB, defined in IEC 61375-2-1, consists on allocating each node a unique address. In order to do so the nodes are ranked in strong nodes, weak node or slave node. A strong node is promoted by the application to become the master. Equally, a strong node may be demoted to weak node by the application. If it was strong master, it will signal its demoting to all nodes and it will remain in control of the bus as weak master until a strong node is appointed. A weak node is a node which the application allows to become master when no strong node is



present. In a composition in which there is no strong node, a contention resolution which treats all nodes equally ensures that one and only one of the weak nodes becomes weak master and all other nodes become Slaves. Finally, a slave node is a node which the application does not allow to become master at any time.

Once the Mastership is defined, the inauguration procedure allocates addresses following the next criteria:

1. nodes in Direction\_1 from the master are sequentially numbered in descending order, starting with 63, the last named node being the bottom node;
2. nodes in Direction\_2 from the master are sequentially numbered in ascending order starting with 02, the last named node being the top node.

Additionally, a procedure to detect other compositions is also defined in IEC 61375-2-1. Within this procedure, the end-nodes detect the presence of an additional node connected to their open end, and they report their own presence to an additional node. The end-node reports in each subsequent Presence Response the presence of another node, the strength of the remote composition and the local decision to yield or insist in case of identical strengths.

#### 6.1.6.2.2 *ETB*

The Train Inauguration is the process consisting in configuring the train network. This process defines an identification number for each CN subnet ("Subnet Id") and each ETBN ("ETBN Id"). As seen in previous sections, these values shall be used to build train IP mapping, train routing definition, NAT rules and ED naming among others.

To determine these values, two types of topology are built by TTDP:

- **Physical Topology:** An ordered and oriented list of ETBNs is calculated, creating the Connectivity Table.
- **Logical Topology:** An ordered and oriented list of train subnets is calculated, creating the Train Network Directory.

According to the IEC 61375-2-5 norm, the Train Inauguration procedure shall respect the following rules:

- The train ETBN ending node inside the Consist with the lowest Consist UUID<sup>1</sup> is defined as the train ETBN top node.
- If train is composed of a unique Consist, ETBN top node is statically defined.
- ETBN top node takes the "ETBN Id" equal to 1.
- Subsequent ETBNs in the ETB reference direction 2 are numbered in ascending order starting with 2, the last numbered ETBN being the ETB bottom node.

---

<sup>1</sup> The Consist UUID is used to uniquely identify a consist in the world. To do so, a 128-bits identifier is used.

- The ETB reference direction always points in the direction of the ETBN top node.

The ETBNs are discovered by other ETBNs by sending periodically multicast Layer 2 frames. These frames are named TTDP TOPOLOGY frames.

ETB lines statuses are sent in TTDP TOPOLOGY frame and shared between all ETBN. Each ETBN computes these statuses for its own lines according to TTDP HELLO frames.

The TTDP HELLO timing is divided in two; Slow sending and Fast sending. The Slow sending has a period of 100ms and a timeout of 1.3\*period, this is 130ms. The Fast sending reduces its period to 15ms and its timeout to 45ms. The detection time of a topology change is determined by these sending times:

$$\text{Detection time} = \text{Slow timeout} + \text{Fast timeout} = 175 \text{ ms.}$$

### 6.1.6.3 Safe Train Inauguration Process

#### 6.1.6.3.1 WTB

The inauguration process in WTB, defined in IEC 61375-2-1, consists on allocating each node a unique address. In order to do so the nodes are ranked in strong nodes, weak node or slave node. A strong node is promoted by the application to become the master. Equally, a strong node may be demoted to weak node by the application. If it was strong master, it will signal its demoting to all nodes and it will remain in control of the bus as weak master until a strong node is appointed. A weak node is a node which the application allows to become master when no strong node is present. In a composition in which there is no strong node, a contention resolution which treats all nodes equally ensures that one and only one of the weak nodes becomes weak master and all other nodes become Slaves. Finally, a slave node is a node which the application does not allow to become master at any time.

Once the Mastership is defined, the inauguration procedure allocates addresses following the next criteria:

1. nodes in Direction\_1 from the master are sequentially numbered in descending order, starting with 63, the last named node being the bottom node;
2. nodes in Direction\_2 from the master are sequentially numbered in ascending order starting with 02, the last named node being the top node.

Additionally, a procedure to detect other compositions is also defined in IEC 61375-2-1. Within this procedure, the end-nodes detect the presence of an additional node connected to their open end, and they report their own presence to an additional node. The end-node reports in each subsequent Presence Response the presence of another node, the strength of the remote composition and the local decision to yield or insist in case of identical strengths.

#### 6.1.6.3.2 ETB

The Train Inauguration is the process consisting in configuring the train network. This process defines an identification number for each CN subnet ("Subnet Id") and each ETBN ("ETBN Id").

As seen in previous sections, these values shall be used to build train IP mapping, train routing definition, NAT rules and ED naming among others.

To determine these values, two types of topology are built by TTDP:

- **Physical Topology:** An ordered and oriented list of ETBNs is calculated, creating the Connectivity Table.
- **Logical Topology:** An ordered and oriented list of train subnets is calculated, creating the Train Network Directory.

According to the IEC 61375-2-5 norm, the Train Inauguration procedure shall respect the following rules:

- The train ETBN ending node inside the Consist with the lowest Consist UUID<sup>2</sup> is defined as the train ETBN top node.
- If train is composed of a unique Consist, ETBN top node is statically defined.
- ETBN top node takes the “ETBN Id” equal to 1.
- Subsequent ETBNs in the ETB reference direction 2 are numbered in ascending order starting with 2, the last numbered ETBN being the ETB bottom node.
- The ETB reference direction always points in the direction of the ETBN top node.

The ETBNs are discovered by other ETBNs by sending periodically multicast Layer 2 frames. These frames are named TTDP TOPOLOGY frames.

ETB lines statuses are sent in TTDP TOPOLOGY frame and shared between all ETBN. Each ETBN computes these statuses for its own lines according to TTDP HELLO frames.

The TTDP HELLO timing is divided in two; Slow sending and Fast sending. The Slow sending has a period of 100ms and a timeout of 1.3\*period, this is 130ms. The Fast sending reduces its period to 15ms and its timeout to 45ms. The detection time of a topology change is determined by these sending times:

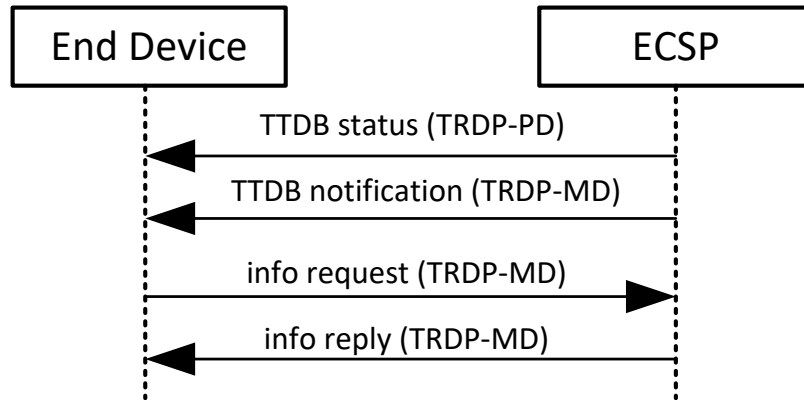
$$\text{Detection time} = \text{Slow timeout} + \text{Fast timeout} = 175 \text{ ms.}$$

#### 6.1.6.4 Functions to Request Topology

To retrieve information about the train topology, there is a defined TTDB manager interface which specifies a set of telegrams over Train Real-time Data Protocol (TRDP). A TRDP-PD telegram is used to inform about the actual operational train directory status, a notification message is sent after each change of the operational train directory. In addition, a set of TRDP-MD telegrams can be used to retrieve data from the TTDB as it is shown in Figure 6-7.

---

<sup>2</sup> The Consist UUID is used to uniquely identify a consist in the world. To do so, a 128-bits identifier is used.

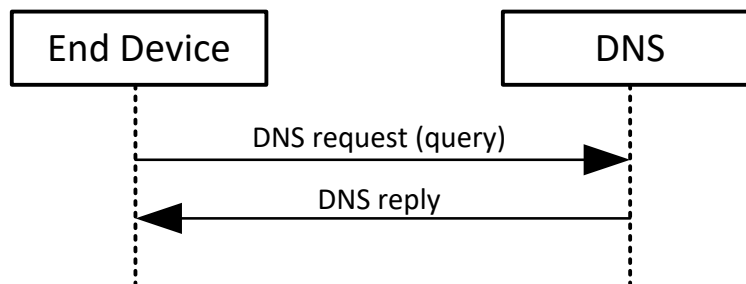


**Figure 6-7 – TTDB manager interface telegrams**

The TTDB status is periodically sent to all devices of the consist with a cycle time  $(1,0 \pm 0,1)s$  and a timeout of 5,0s, the TTDB notification is sent to all devices of the consist after each TCN inauguration. By contrary, info request/reply is exchange by demand of the device. In the following subsections the protocols needed to carry out these requests are explained.

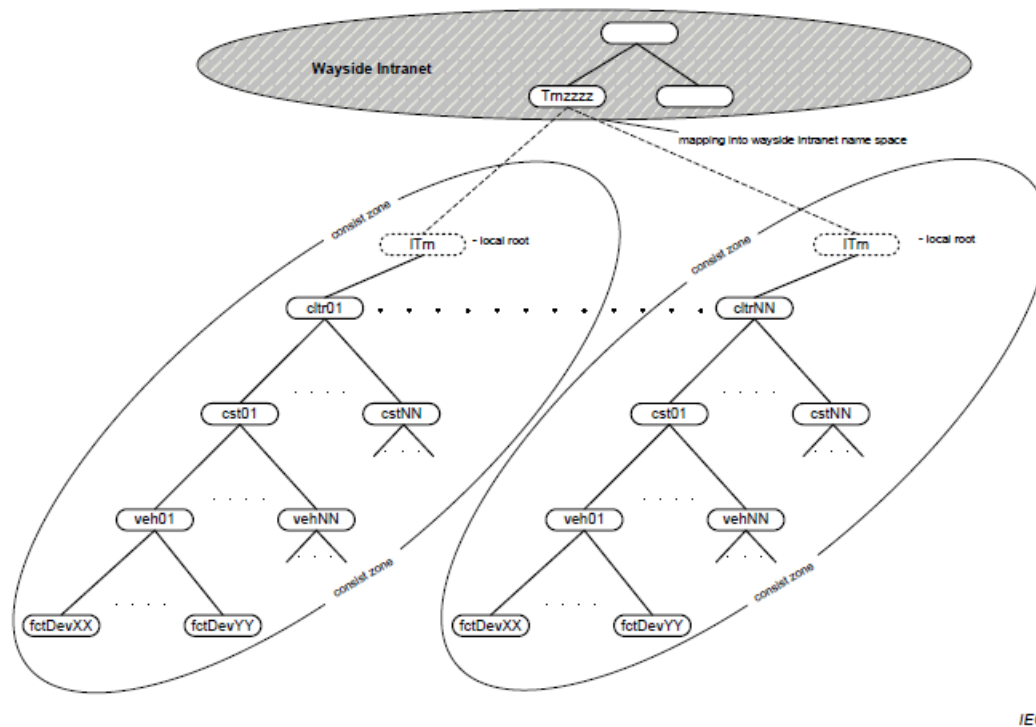
#### 6.1.6.4.1 TCN-DNS

TCN-DNS is a modified interface that can be used in more efficient way in railway domain when multiple TCN-URIs need to be resolved. TCN-URI address resolution is requested by sending a DNS resolving request message as depicted in Figure 6-8. The TCN-DNS will resolve the TCN-URIs contained within the DNS resolving request message and will return a list with related IP addresses.



**Figure 6-8 – TCN-URI resolving**

The host part of a TCN-URI is defined in accordance to the hierarchical structure illustrated in Figure 6-9, as a string of the following form: fctdevLabel.vehLabel.cstLabel.cltrnLabel.trnLabel.

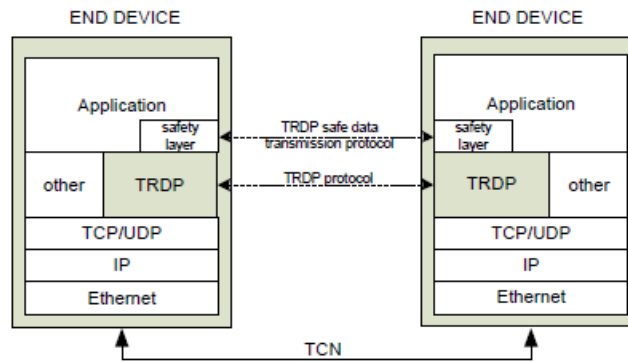


**Figure 6-9 – TCN-DNS name space with division into zones (Source IEC 61375-2-3:2015)**

The DNS query (DNS resolving request message) with the TCN-URI string will be complemented with the related IP address by the DNS server (resolver) in the reply (DNS resolving reply message), providing the demanded IP address to the End-device.

#### 6.1.6.4.2 TRDP

The Train Real-time Data Protocol (TRDP) is used to exchange TCN data over ETB. TRDP differentiates two types of data, Process Data (TRDP-PD) and Message Data (TRDP-MD). TRDP layer works on top of transport layer (see Figure 6-10), being able to work with UDP and TCP. Additionally, a safety layer can be added to the TRDP payload to provide safe end-to-end data transmission. This safety layer will be further explained in section 6.1.6.4.3.



**Figure 6-10 – Overview of the TRDP protocol stack (Source: IEC 61375-2-3:2015)**

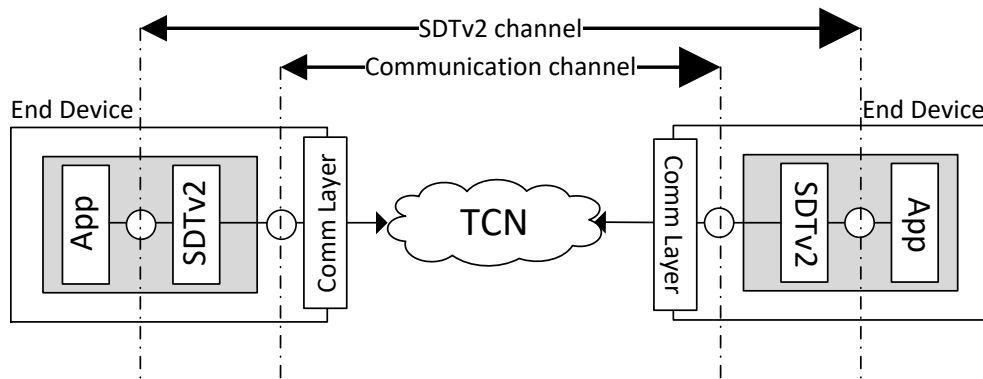
The TRDP-PD defines the exchange of PD-PDUs for the transfer of process data. PD-PDUs can be cyclically transmitted or by request. Moreover, the communication can be from a publisher and one or many subscribers using a connectionless and unconfirmed TRDP service.

The TRDP-MD defines the message data exchange between a caller and one or many repliers over a confirmed TRDP service. The maximum length of a telegram is limited to 64 kBytes. The source is sending a request message and the replier(s) sends back a reply message. The source then shall quit reception of the reply by sending a confirmation if required by the replier.

#### 6.1.6.4.3 SDTv2

Safe Data Transmission (SDTv2) provides a SIL2 safe communication path between a source of safety related data (SDSRC) and one or several destinations of those data (SDSINK). This data transmission is done over a SDTv2 channel which starts and ends in safe applications of the safe end devices, including the TCN network which is considered non-trustable medium from the safety point of view, this is a back channel model is used. Figure 6-11 illustrates how the boundaries of this safe channel.

The SDTv2 protocol layer provides two interfaces: the communication channel interface and the SDTv2 application interface. The first one is defined by the underlying communication technology, i.e. TRDP, whereas the second one is product specific and it is the place where safety related process data are put to or get from the application.



**Figure 6-11 – SDTv2 channel**

SDTv2 protocol fulfils the following requirements directly extracted from the standard IEC 61375-2-3:

- a) Safety communication and standard (regular) communication shall be independent. However, standard devices and safety devices shall be able to use the same communication channel.
- b) Safety communication shall be suitable for Safety Integrity Level SIL2 for continuous mode of operation (see IEC 61508-1).
- c) Safety communication shall use a single-channel communication system. Redundancy may only be used optionally for increased availability.
- d) Implementation of the safe transmission protocol shall be restricted to the communication end devices.
- e) Due to the dynamic nature of train compositions with a varying number of consists, a 1:n communication relationship between the safe data source and safe data sinks has to be supported.
- f) The transmission duration times shall be monitored.
- g) Environmental conditions shall be according to general railway requirements, mainly IEC 60571, if there are no particular product standards.
- h) Transmission equipment such as controllers, ASICs, Ethernet switch cores, cables, couplers, etc., shall remain unmodified (black channel). The safety functions shall be above OSI layer 7 (i.e. profile, no standard protocol changes or enhancements).
- i) The safety communication shall not reduce the permitted number of devices.
- j) The safety communication shall support data exchange over the ETB in dynamically changing train compositions.

The following safety measures are implemented in this protocol in order to overcome possible transmission errors:

- Sequence Counter
- Sink-time supervision
- Safety Code
- Guard time

- Source Identifier(SID)
- Latency Monitoring
- Channel Monitoring

Note that the for the safety code a cyclic redundancy code of 32 bit defined in IEC 61784-3-3 is used.

#### **6.1.6.5 Safe Train Inauguration Process**

The Next Generation of TCMS aims to remove Safety Train Lines in its path to reduce costs. With the suppression of this safety mechanism SIL4 functionalities must be supported by the NG-TCN. Two functionalities affected by this evolution are Doors functions and Brake functions. This last subsystem is also migrating from a combination of different brakes (e.g. pneumatic, electronic, etc.) to a single electronic brake system that should be able to support SIL4 level.

The reason why Train Integrity function should take this evolution into account is twofold. On the one hand, until now, in many trains the Train Integrity was ensured by the pressure level of the pipe which connects all pneumatic brakes along a consist. This is, when the train completeness was somehow broken the pipe used to loss its pressure and therefore, pneumatic brakes were actioned stopping the train. This approach will not be valid in the future if a single electronic brake system is deployed. On the other hand, the evolution of NG-TCN to allow SIL4 applications provides a communication channel to communicate safely the OTI devices within the train. Moreover, if Safe Train Inauguration function is present in the train's TCMS, then the TCMS itself could become a source of integrity checker as it periodically checks and detects the train topology which implicitly detects the train incompleteness. In order to use the Safe Train Inauguration function as a source of train completeness the detection times explained in section 6.1.6.3.2 should be compliant with the Train integrity requirements and adapted if needed.

#### **6.1.6.6 SIL4 Safe Data Transmission (SDTv4)**

As explained in section 6.1.6.4.3 the current SDTv2 provides SIL2 communications using a black channel model. The extension of this safety layer to allow SIL4 is foreseen, as the result of the calculation made of the Tolerable Hazard Rate (THR) according to IEC61784-3, shows that the length of the safety code is not enough to achieve this level. Therefore, in close future a modification of this protocol is expected which could produce one of these two options:

1. Use smaller telegrams and reuse the existing polynomial for the safety code. In this case the 24 Bytes in sum with a maximum of 8 Byte safety relevant application Data.
2. Use larger telegrams and incorporate a second 32Bit CRC additional to the existing CRC polynomial so that 1500 Byte in sum with a maximum of 1440 Byte relevant application Data can be used.

#### **6.1.7 Train Integrity trough Monitors brake pipe pressure**

This function has been developed and applied mainly on freight trains. This type of application is mainly in US Canada Australia and South Africa. It has been designed to comply with the type of



brake control unit applied in these countries. It also uses air pressure to power the EOT system located at the end of the train.

An improvement in an End-of-Train (EOT) monitor system allows the continuity of the brake pipe of a train to be verified. Obstructions in the brake-pipe, such as, for example, closed angle cocks, kinks, blockages, or breaks, adversely affect brake safety. A pressure sensor is installed in the Locomotive Cab Unit (LCU) to sense brake application.

If the brake pipe is intact, a brake application initiated from the locomotive should correspondingly result in a drop in pressure at the EOT unit.

The time require for the drop to propagate through the train is a function of train length. If a pressure drop is not sensed at the EOT unit within a predetermined period of time, it is assumed to be due to either a corrupted brake pipe or a communications failure between the LCU and EOT unit. A Microprocessor in the LCU initiates a communications check by interrogating the EOT unit from the LCU. If no reply is received, an alarm sounds warning the engineer of a communications failure. If, on the other hand, the LCU receives a reply from the EOT to the interrogation, a brake pipe continuity alarm is sounded warning the engineer of a brake fault condition.

Monitoring the condition of the brake pipe pressure has the advantage of not having to add equipment along the train; for long train composition the time to recognize a problem can be long. When the trains are very long, longer than 2 kilometers, the times are more than 14 seconds.

The Train Integrity function would have to discriminate between the train braking or loss of integrity occurring.

The systems on the market at present are not SIL4 certified.

#### **6.1.7.1 Brake Pipe Description**

Even the most modern, purely air brake systems rely on the transmission of an air signal along the brake pipe. This is initiated from the front of the train and has to be sent to all vehicles along the train.

There will always be a time lapse (called the propagation rate) between the reaction of the leading vehicle and the reaction of one at the rear. This time lapse is a considerable restraint on operation. It causes the braking of vehicles to happen at different times along the train so that while some cars are slowing down, others are still trying to push, unbraked, from the rear.

When releasing, the front of the train is pulling the rear, which is still braking, and causes stress to the couplers.

There are many types of e-p brake systems use today and most of them were developed as an "add-on" to the original air brake system and, as a result, incorporated some common principles in their design as follows:

- The e-p brake does not compromise the fail-safe or "vital" features of the air brake
- The air brake normally remains in the "Release" position, even while the e-p brake is in "Application" and the same brake cylinders are used.
- E-P brakes are invariably used on multiple unit passenger trains.

#### 6.1.7.2 Systems relying on an end of train device

Currently the systems for monitoring the pressure in piping have been developed mainly for the US market. These system provide the status of the train integrity.

As an example, the characteristics of existing systems for some suppliers are reported. This is applied mainly to freight trains.

The system architecture is comprised of a Head of Train Unit, located in the locomotive and an End of Train, located on the last car. The End of Train is connected to the Head of Train via a unique RF Radio link.

##### 6.1.7.2.1 **DAIKEN SYSTEM**

An improvement in an End-of-Train (EOT) monitor system allows the continuity of the brake pipe of a train to be verified. Obstructions in the brake-pipe, such as, for example, closed angle cocks, kinks, blockages, or breaks, adversely affect brake safety. A pressure sensor is installed in the Locomotive Cab Unit (LCU) to sense brake application. If the brake pipe is intact, a brake application initiated from the locomotive should correspondingly result in a drop in pressure at the EOT unit.

The time require for the drop to propagate through the train is a function of train length.

If a pressure drop is not sensed at the EOT unit within a predetermined period of time, it is assumed to be due to either a corrupted brake pipe or a communications failure between the LCU and EOT unit. A Microprocessor in the LCU initiates a communications check by interrogating the EOT unit from the LCU. If no reply is received, an alarm sounds warning the engineer of a communications failure. If, on the other hand, the LCU receives a reply from the EOT to the interrogation, a brake pipe continuity alarm is sounded warning the engineer of a brake fault condition.

The EOT device provides the operator with essential functionalities for safe train operation:

- Monitors and reports the brake pipe pressure
- Monitors the integrity of the train composition
- Provides a backup emergency braking device

The EOT communicates via radio UHF two way communications with any CDU that uses the AAR (American Association of Railroads) protocol for EOT System.

##### Salient Features

- Daiken GEP provides power and recharges the battery of the rear unit.
- Motion Sensor, informs when the last car is in movement or stopped.
- Inclination sensor allows the EOT's shut down when it is left in a horizontal position, preventing the unnecessary wear of the battery when the equipment is not under use.
- High performance and shock resistant antenna with special cover to prevent bad usage.
- Clamp system versatile for fitting into several types of couplings.
- Steel case with stands the most adverse conditions of use. As operational bumps, is resistant to harsh weather, and has anti-corrosive treatment.
- The electronic modules and pneumatic actuation system have a dampening system to lessen the bumps caused by the vibration.
- Sealed Lead Acid battery power the unit when the brake pipe pressure is bellow 60psig.
- Transport brace and handle ergonomically designed for easier handling.

Daiken GEP: Derives a small amount of air of the brake pipe pressure to generate electricity for feeding the electronic board and charging the battery.

- Generates electric power for the electronic circuits and charges the battery
- Eliminates stops due to batteries recharge, allowing longer trips
- Increases the efficiency on train composition
- Eliminates the reposition of batteries and chargers and the operational procedures for recharges
- Eliminates delays due to dead batteries

#### 6.1.7.2.2 **WABTEC SYSTEM**

The Wabtec End of Train telemetry system performs three major functions: monitoring many essential last car conditions, providing rear of train emergency braking capability, and providing a high visibility marker for night time use.

The system is comprised of a Head of Train Unit, located in the locomotive and an End of Train, located on the last car.

The End of Train sends the Head of Train the following Information (via a unique RF Radio link):

- Last Car Brake Pipe Pressure
- Motion Status
- Marker Light Status (On or Off )
- Battery Life
- RF Communication Status
- Emergency Valve Status

The Head of Train relays this information the operator of the train. It also allows the operator to check communication status and initiate emergency braking.

Self-contained unit that is located on the control stand in the locomotive cab.

#### 6.1.7.2.3 **INTELETRACK SYSTEM**

One Touch fixed Mount Cab Unit. It is an end-of-train monitor system. The system measures the air-brake pressure or vacuum at the end of the train and transmits the information to the driver in the cab via a radio link.

This new version of the telemeter is designed according to AAR S-5701 specifications. A complete telemeter system consists of a cab unit mounted or stowed in the cab of a train where the crew operates and a rear unit mounted with a clamp on the last waggon of the train. The system is designed to be a simple, rugged and reliable system. Maintenance is done through changing the modules.

EOT Remote Head is a visual extension of the AAR Cab Unit. Its application is aimed at scenarios where the Cab Unit is mounted away from the loco driver's visual equipment, such as a closed mounting rack. In this case the Remote Head will provide the MMI (Man Machine Interface) interface to the Cab Unit and will have the same feel, functionality and information as the Cab Unit. It connects directly to the Cab Unit via a cross-over Ethernet cable or through a hub with a straight Ethernet cable. It will accept partial as well as full DGI (Differential Graphic Information) packets as per TFR specification document BBF0334 which implies it will be compatible to all equipment adhering to that specification including other equipment supporting TCS (Train Communication System).

GPS3 Rear Unit is an end-of-train monitor system. The system measures the air-brake pressure or vacuum at the end of the train and transmits the information to the driver in the cab via a radio link. This new version of the telemeter is designed according to AAR S-5701 specifications. A

complete telemeter system consists of a cab unit mounted or stowed in the cab of a train where the crew operates and a rear unit mounted with a clamp on the last waggon of the train.

#### **6.1.7.2.4 NIKSAR SYSTEM**

The End-of-Train Telemetry System consists of an instrumentation and telemetry unit (SBU/EOT) mounted on the rear coupler and is connected to the air braking system of the last train car. It communicates via built-in UHF radio modems with a Communications Display Unit (CDU) or Locomotive Cab Unit (LCU) mounted in the Cabin.

The SBU/EOT, when operating in conjunction with the CDU/LCU, provides the locomotive driver with information about the conditions at the rear of the train that are important to the operation of the train, as:

- Brake pressure
- Status of the data link
- Car motion
- Communications link tests
- Emergency activation of the braking system, and
- Battery status of the SBU/EOT

#### **6.1.7.2.5 SIEMENS SYSTEM**

End of Train Device feature an air generator to keep the battery charged, a GPS receiver, and an integrated event recorder.

A single pushbutton is used to arm the unit, disable the air generator, and display EOT status. The integrated GPS receiver determines location, motion and speed. This information is stored in the integrated event recorder, along with elapsed time of operation and EOT communication status.

The event recorder stores approximately the last 23,000 events in memory. The cell modem equipped, remote tracking EOT allows the EOT to report its position on a periodic (and over-the-air adjustable) basis. The EOT will also report its position any time it receives an emergency braking command from the HOT.

Features:

- High strength, space age polymer enclosure
- Enclosed antennas & AEI tag
- Low-profile, pivot-pin clamp assembly
- Battery charging air generator
- External battery charging port
- Internal event recorder
- Ultra-high intensity single LED high visibility marker
- GPS receiver
- 8 character display
- Single push-button operation
- Cellular Data Service with Over-the-Air upgrades
- 8Watt narrow-band radio
- Expansion slot for an Optional 3rd wireless device (WiFi, Zigbee, etc.)
- "Hands-off" (Closed Box) Radio Calibration/Alignment
- Socketed modem, GPS, wireless modules (easy upgrade path)
- Future support of various battery chemistries

### **6.1.8 Market aspects**

The train integrity function is mandatory for ETCS Level 3 systems. Regardless of this in the world, there are currently applications that do not have the same system level requirements for ETCS Level 3 application implement train integrity control.

These were developed mainly for the freight train market, when these are very long and a broken train not properly managed could block the line for long periods.

These are usually not associated with a degree of SIL in terms of system level, most often they are single-track lines with very mild train timing.

As it is structured the ETCS signaling system and for the needs of the scheduling of the trains, what is now in service is not applicable for ETCS purpose.

It becomes difficult to compare what is required on the European market from what is required by other markets.

### **6.1.9 Conclusion**

From the analysis carried out, it emerges that the applications of the integrity of the train in operation concern freight trains for very long lines often with single track.

The solutions adopted up to now for freight trains have a system at the top and one at the end of the train.

This is because there are difficulties in having power systems present on freight cars. In fact these systems either have rechargeable batteries or are powered by the pressure of the train brake pipe.

For applications for passenger trains there are studies in progress but these require response times in the recognition of the state of the integrity of the train that are compatible with the management of the scheduling of the trains adopted.

Encouraging projects using wireless networks have been made and are ongoing. There are some aspects concerning safety that need to be deepened.

The availability values currently required by early studies concerning ETCS level 3 should be guaranteed.

Regardless of the technology adopted preliminary values predict an availability of at least  $10^{-6}/h$  for the OTI device.

The more in-depth analysis of these issues will be addressed in further step of the project.

## 6.2 Product Classes and Target Scenarios

This sections contains the description of OTI product classes respect to the four S2R application domains: Intercity-High Speed, Regional, Urban-Suburban, Freight.

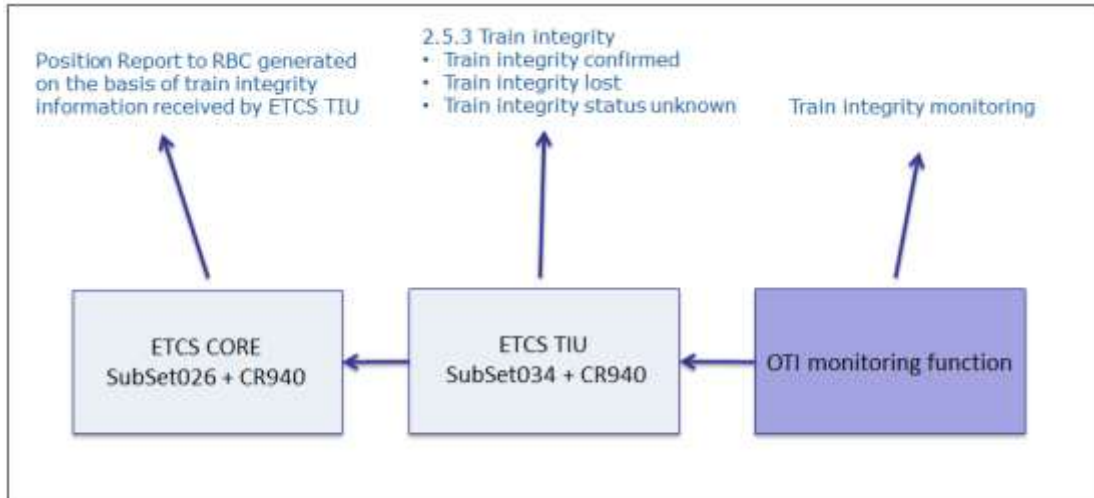
The approach to define product classes consisted in identifying for each application domain the specific requirements relevant for OTI context and then defining classes of solutions that meet identified requirements. On this bases several on-board configuration are identified and described for each product class.

Finally, relevant reference scenarios are identified and analysed to identify main functionality related to on-board train integrity.

### 6.2.1 ETCS Specification Context

Relevant information in defining OTI product classes is the ETCS regulation context, depicted in Figure 6-12 and described at section 7.1.

ETCS CORE functionalities are specified in SUBSET 026 [1] and CR940 [3] that essentially describes how to manage and deliver train integrity information to RBC by means of Position Reports messages. Train integrity information is acquired by means of ETCS TIU, according to SUBSET 034 [2] and CR940 [3], and can have three possible values: (i) confirmed, (ii) lost or (iii) unknown. Finally the OTI Monitoring function is focused on train integrity monitoring.



**Figure 6-12 – ETCS regulations context for OTI**

OTI monitoring function interfaces with the ETCS associated with the active cabin to confirm that the train from that active cabin to the physical rear end of the train is integral.

## 6.2.2 S2R Application Domains

Table 6-3 contains, for the four S2R application domains, the requirements relevant for OTI context and related values. Head-Tail communication refers to availability of wired or wireless on-board networks. Moreover power supply and odometry information can be available or not at train tail. Finally, train composition and ETCS equipment at train tail are relevant in OTI context.

OTI Relevant Requirements	Intercity-High Speed	Regional	Urban-Suburban	Freight
Head-Tail Communication	WIRED	WIRED	WIRED	WIRED / WIRELESS
Power supply	YES	YES	YES	YES / NO
Train composition	SINGLE / MULTIPLE	SINGLE / MULTIPLE	SINGLE / MULTIPLE	SINGLE / MULTIPLE / MIXED
Tail status (i.e. localisation, kinematic data)	None	None	None	None / Satellite based / IMU
Availability of ETCS at train tail.	YES / NO	YES / NO	YES / NO	YES / NO

**Table 6-3 – Specific Requirements in S2R Application Domains relevant for OTI context**

For passenger trains the costs for installing extra cabling through multiple coaches can be relevant and some passenger trains has not fixed formation, therefore existing electrical connections is also one possible option related to WIRED communication.

Note that MIXED train, composed of passengers and freight waggons, and Service and Maintenance Vehicles are considered as part of freight application domain.

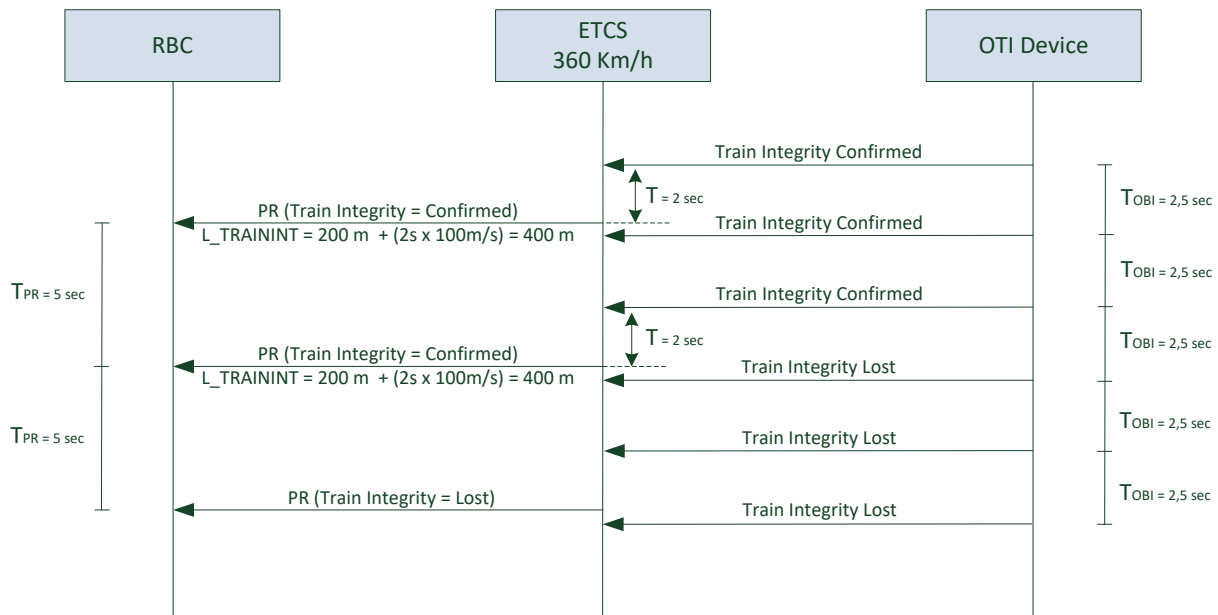
Headway was also initially considered in the analysis and finally not included in Table 6-3 because it was found non relevant in the OTI context. In fact the Headway has values in a range from few minutes in Urban-Suburban applications to hours in low traffic lines. Position Report has value in a range from few seconds to half a minute. However mixed traffic (i.e. passengers and freight) is often present in a railway network. Instead the period of Position Report message is more relevant then headway in defining *freshness* of train integrity information.

In general train integrity information freshness is relevant to ensure that track section behind the train becomes available as soon as possible for the following train thus increasing the line capacity respect to traditional solutions based on track circuits or axle counters.





Figure 6-14 depicts a passenger scenario example with Position Report period of 5 seconds and train integrity refresh period of 2.5 seconds for a train running at 360 Km/h (i.e.  $\approx 100$  m/sec) and train length of 200m. In the considered example train confirmation arrives 2 seconds before sending to RBC the PR and the result is that calculated train length is 400 meters respect to nominal train length of 200 meters. Therefore in considered example a space of 200 meters is considered as unavailable for the following train. Note that safety margin was not considered in the considered example, therefore the space not available is longer than 200 meters.



**Figure 6-14 – Passenger scenario example for train integrity refresh period**

Note that considered values for Position Reports are just examples to evaluate the relation with train integrity monitoring period. No assumption is done in relation to typical PR values in passenger or freight application domains.

Reducing train integrity refresh is therefore a benefit for line capacity, however the appropriate value have to keep into account latency time of wireless on-board communication network and power limitation in case of energy harvesting power supply applied to on-board wireless communication network.

Independently from CR940 [3] possible evolutions, the proposed examples shows that train integrity information monitoring period could be around 1 sec. Smaller values could imply relevant constraints for wireless networks in freight scenarios powered with energy harvesting sources. The assignment of the monitoring period shall be performed in subsequent phase of the project, as part of candidate technologies selection task in D4.2 [7].

In general a train mission in ETCS L3 shall be possible with train at stand still, powered OTI system and confirmed train integrity. For this reason an energy harvesting source need to provide energy both with train at stand-still and when the train is running.

Relevant decision driver for product classes definition is also the “*migration strategy*” for existing trains. In relation to CAPEX and OPEX, OTI functionality implementation allows removing expensive train integrity trackside infrastructures (e.g. track circuits, axle counters). In relation to capacity, on-board train integrity is an enabler for moving blocks that ensure a higher performances respect to traditional track circuits.

To facilitate the migration to OTI equipped trains two specific solutions have been identified during the analysis: (i) designing OTI module applicable also to non ETCS applications and (ii) supporting optional diagnostic functionalities (e.g. waggon diagnosis, cargo monitoring).

Therefore compatibility with non ETCS systems and support for waggons and cargo monitoring ensure a higher attractiveness for operators.

The benefit for infrastructure managers in having OTI equipped trains consists in enabling ETCS L3 thus increasing line capacity, therefore a possible strategy to support the migration could be to assign lower fees for OTI equipped trains.

In conclusion the migration strategy analysis is considered at product level in terms of: (i) defining the interface between OTI module and ETCS in a general way thus being applicable also to non ETCS systems, (ii) defining an interface between OTI module and diagnostic sensors.

Guidelines for defining above interfaces are reported at section 6.2.4.11 as interfaces overview. Detailed interface specification is reported in [7].

Train composition is a topic applicable to all application domains in different ways in terms of frequency and operational procedures.

As examples high speed trains could travel coupled in high traffic periods, whereas freight trains are frequently recomposed in the freight yards depending on the type of goods to be transported. Therefore train composition procedure need to be analysed keeping into account operators need to avoid or limit “training of operators” and “maintenance effort” and general acceptability by operators. According to operators/infrastructure managers’ experience, the migration to new technology often fails in case of complex operational/maintenance procedures.

As example in freight application two opposite configuration can be considered:

- OTI module manually fixed at train tail or manually configured by freight yard personnel
- OTI module installed in all waggons to provide additional functionalities (e.g. train composition determination, safe train length determination, cargo/waggon diagnosis)

In first case only one OTI device per train is sufficient, whereas in second case one OTI device per waggon is installed. First solution requires limited investment costs, however involves manual procedures. Second solution requires higher investments and support automatic configuration procedures (i.e. train composition determination, safe train length determination).

Availability of ETCS at train tail was also considered to include the option of implementing OTI module as a SW module inside on-board safe platform, intended as an external module hosted inside the same platform and independent from ETCS core logic and operation modes. Therefore intended as SW module interfaces with ETCS TIU as reported above in Figure 6-12.

### 6.2.3 Product Classes

On the basis of performed analysis, the criteria identified to define OTI product classes includes communication type (i.e. wired or wireless), availability of power supply and odometry at train tail, presence of ETCS equipment at train tail and implemented functionalities (i.e. train integrity monitoring, train composition determination, safe train length determination, cargo/waggon diagnosis).

In general trains with wired communication network are addressed with Product Class 1 and trains with wireless communication network are addressed with Product Class 2. The difference consists in integrity criteria that in wired on-board network is based on communication liveness, whereas in wireless on-board network requires verifying train tail coherent movement respect to front cabin. In fact communication between train tail and front cabin could be present also after train splitting with limited distance of separated waggons in presence of wireless on-board network.

Note that in Product Class 2 the train length is assumed to be an input to OTI (i.e. train length entered by train driver during data entry procedure). The safe train length determination is addressed with optional Product Class 3 with OTI module installed in each waggon and including waggon length as configuration parameter. In this case the train integrity criteria includes status of separation sensors present in each waggon.

Note that loss of integrity detection with train at stand-still in case of wireless communication can be partially addressed by optional Product Class 3 by using separation sensors for each waggon.

In Product Class 1 the difference between A and B consists in availability of ETCS at train tail. Whereas in Product Class 2 and 3 the difference between A and B consists in availability of energy harvesting source. Note that the table includes for each class also the list of implemented functionalities.

Exceptions respect to defined product classes:

- MIXED train with passengers and freight waggons are included in Product Class 2 for Freight and requires a MIXED network (i.e. wired and wireless communication).
- New generation trains for passengers applications with wireless consist-to-consist communication are included in Product Classes 2 and 3.

PRODUCT CLASS ID		SPECIFIC REQUIREMENTS		INTERCITY HIGH-SPEED	REGIONAL	URBAN SUB-URBAN	FREIGHT
1	A	COMMUNICATION	WIRED	X	X	X	X
		ETCS AT TRAIN TAIL	YES				
		TAIL ODO/POSITION SENSORS	NO				
		ENERGY HARVESTING	NO				
		FUNCTIONALITY	TRAIN INTEGRITY MONITORING				
	B	COMMUNICATION	WIRED	X	X	X	X
		ETCS AT TRAIN TAIL	NO				
		TAIL ODO/POSITION SENSORS	NO				
		ENERGY HARVESTING	NO				
		FUNCTIONALITY	TRAIN INTEGRITY MONITORING				
2	A	COMMUNICATION	WIRELESS				X
		ETCS AT TRAIN TAIL	NO				
		TAIL ODO/POSITION SENSORS	YES				
		ENERGY HARVESTING	NO				
		FUNCTIONALITY	TRAIN INTEGRITY MONITORING CARGO/WAGGON DIAGNOSIS				
	B	COMMUNICATION	WIRELESS				X
		ETCS AT TRAIN TAIL	NO				
		TAIL ODO/POSITION SENSORS	YES				
		ENERGY HARVESTING	YES				
		FUNCTIONALITY	TRAIN INTEGRITY MONITORING CARGO/WAGGON DIAGNOSIS				

**Table 6-4 – Product Classes 1 and 2**

PRODUCT CLASS ID		SPECIFIC REQUIREMENTS		INTERCITY HIGH-SPEED	REGIONAL	URBAN SUB-URBAN	FREIGHT
3	A	COMMUNICATION	WIRELESS				X
		ETCS AT TRAIN TAIL	NO				
		TAIL ODO/POSITION SENSORS	YES				
		ENERGY HARVESTING	NO				
		FUNCTIONALITY	TRAIN INTEGRITY MONITORING TRAIN COMPOSITION DETERMINATION SAFE TRAIN LENGTH DETERMINATION CARGO/WAGGON DIAGNOSIS				
	B	COMMUNICATION	WIRELESS				X
		ETCS AT TRAIN TAIL	NO				
		TAIL ODO/POSITION SENSORS	YES				
		ENERGY HARVESTING	YES				
		FUNCTIONALITY	TRAIN INTEGRITY MONITORING TRAIN COMPOSITION DETERMINATION SAFE TRAIN LENGTH DETERMINATION CARGO/WAGGON DIAGNOSIS				

**Table 6-5 – Product Classes 3**

The following paragraphs includes examples for on-board configuration in different product classes. A complete system architecture definition and interfaces specification is reported in D4.2.

On the basis of defined Product Classes 1 and 2 the on-board train integrity monitoring function is organized in three functional blocks:

- (i) Master module in front cabin,
- (ii) communication network, and
- (iii) Slave module at train tail.

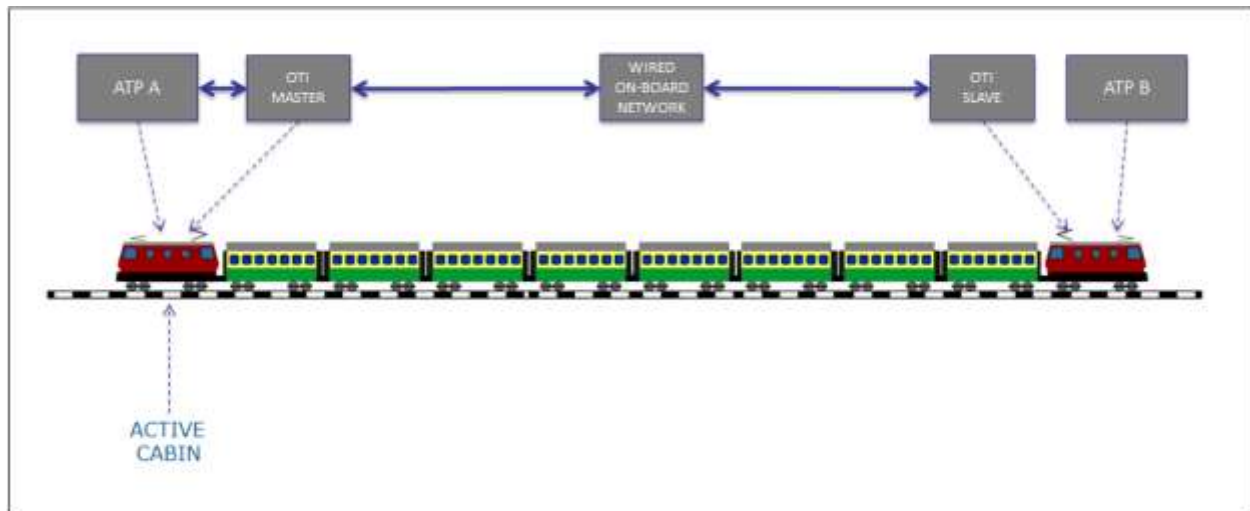
OTI Slave module acquires the status of train tail and provide collected information to OTI Master module over on-board communication network. OTI Master module checks coherence of train tail status and finally provides train integrity information to ETCS. Product Class 3 requires OTI Slave device installed in each waggon.

#### 6.2.3.1 Product Class 1

Figure 6-15 depicts a product class 1 example for a train with fixed composition and wired on-board network. Considered example adopts external devices as OTI MASTER and OTI SLAVE modules.

The benefit for this solution consists in applicability to ETCS or non ETCS equipped trains.

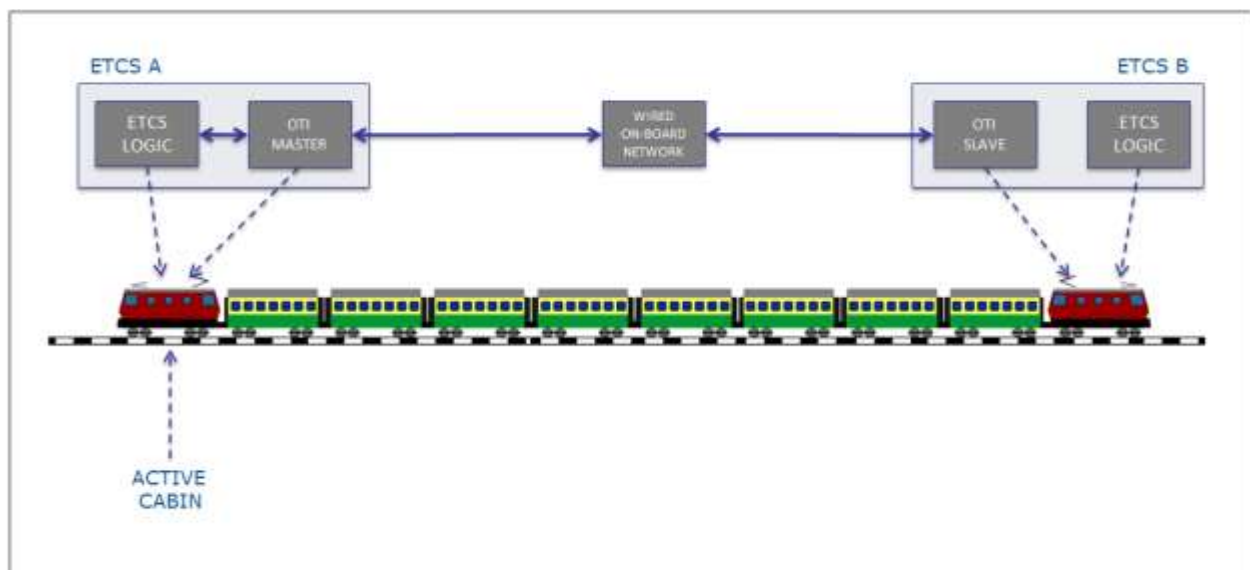
The cost is related to activities for OTI device installation in each train cabin and interfaces wiring towards ATP and on-board network.



**Figure 6-15 – Example 1 for OTI Product Class 1-A**

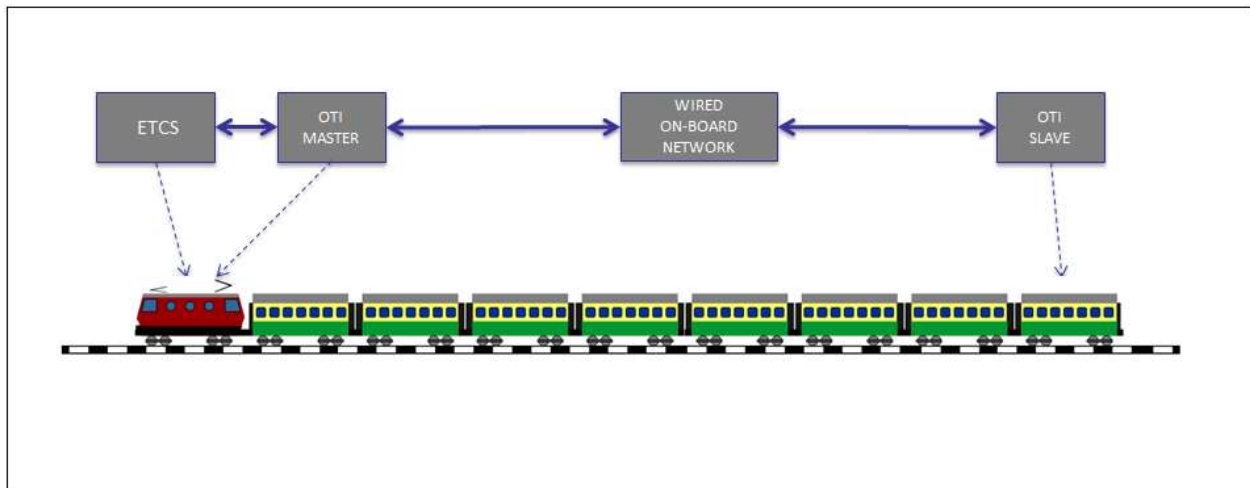
Figure 6-16 depicts a Product Class 1 example for train with fixed composition and wired on-board network. Considered example includes OTI MASTER and OTI SLAVE module implementation inside the ETCS equipment, separately from ETCS logic functionalities.

The benefit for this solution consists in small impact at installation level limited to SW upgrade for OTI Module.



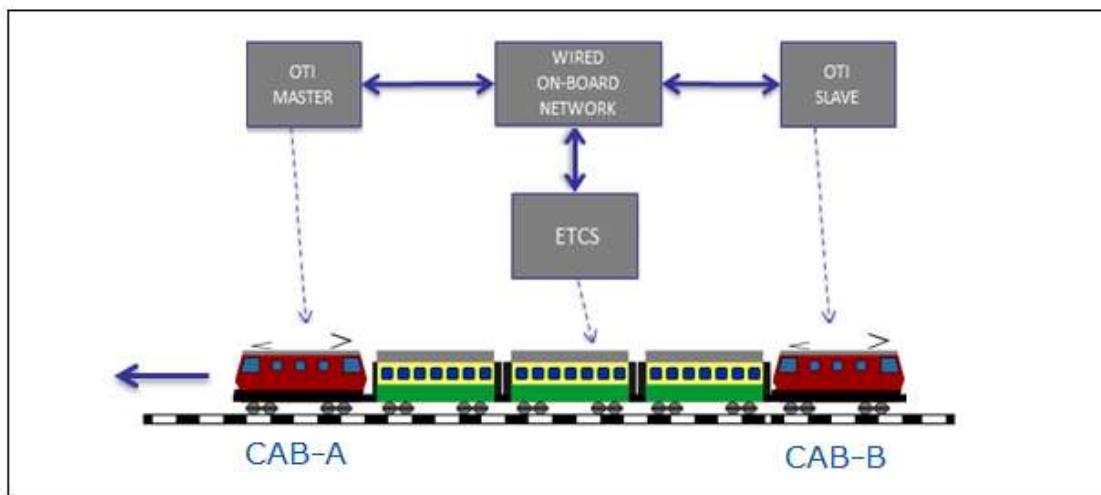
**Figure 6-16 – Example 2 of OTI Product Class 1-A**

Figure 6-17 depicts a Product Class 1-B example for a train with ETCS equipment available only at one side and wired on-board network. In this case the installation impact consists in installing OTI device at train tail, connecting ETCS to on-board network and SW upgrade for OTI module in front cabin.



**Figure 6-17 – Example of OTI Product Class 1-B**

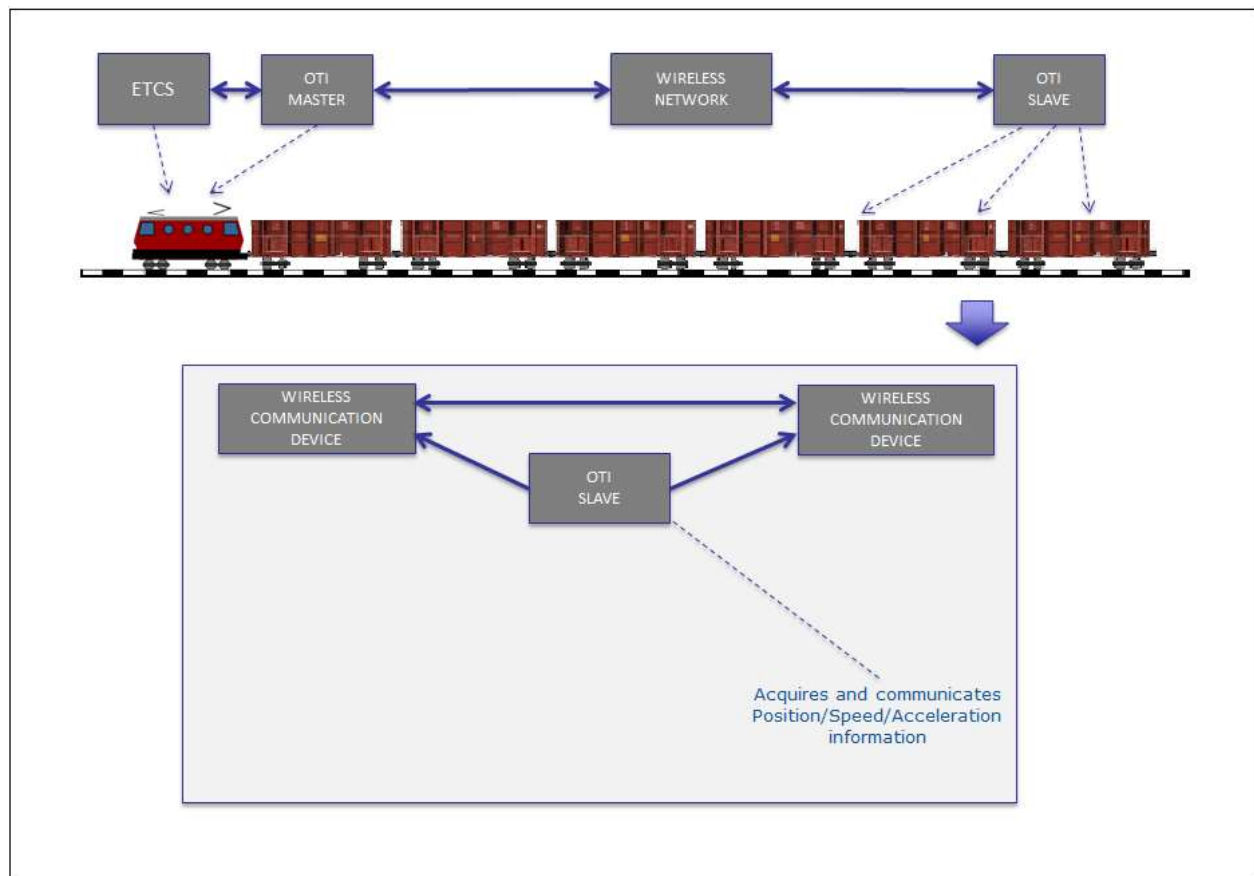
Figure 6-18 depicts a second Product Class 1-B example for a train with ETCS equipment in central configuration and wired on-board network.



**Figure 6-18 – Example of OTI Product Class 1-B for central ETCS configuration**

#### 6.2.3.2 Product Class 2

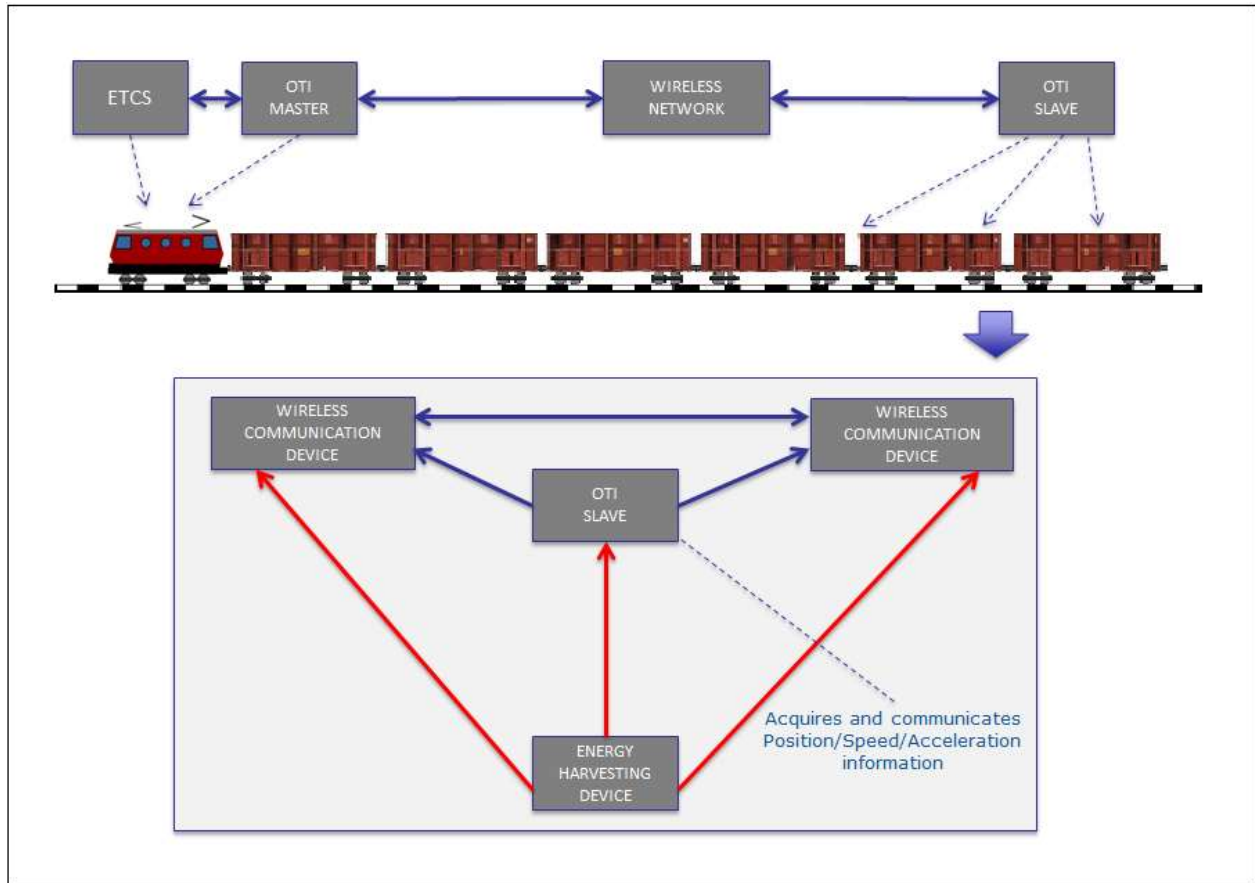
Figure 6-19 depicts a Product Class 2-A example for a train with ETCS equipment available only at one side, wireless on-board network and power supply available.



**Figure 6-19 – Example of OTI Product Class 2-A**

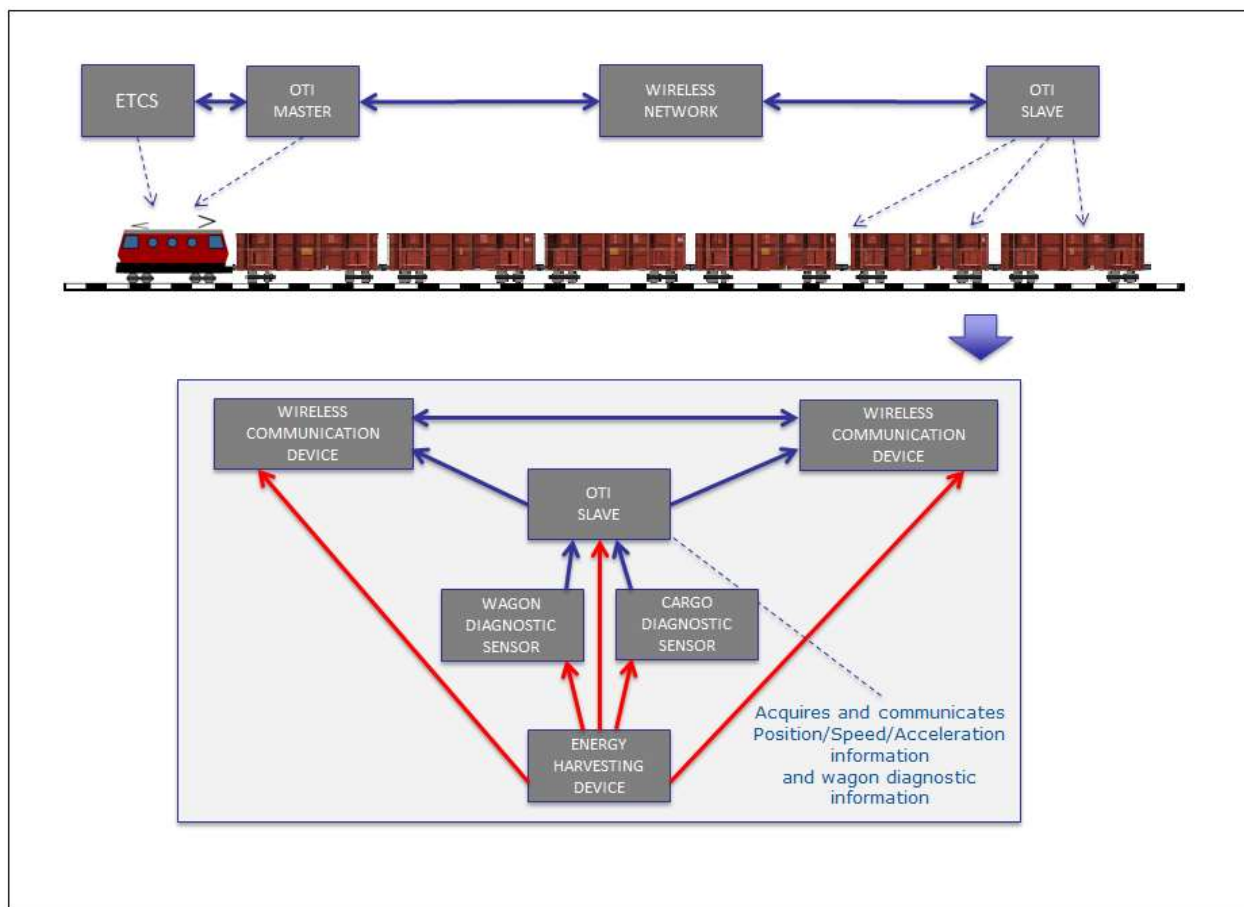


Figure 6-20 depicts a Product Class 2-B example for a train with ETCS equipment available only at one side, wireless on-board network and energy harvesting as power supply.



**Figure 6-20 – Example of OTI Product Class 2-B**

Figure 6-21 depicts a Product Class 2-B example for a train with ETCS equipment available only at one side, wireless on-board network and energy harvesting as power supply. In this case also waggon and cargo monitoring sensors are present.



**Figure 6-21 – Example of OTI Product Class 2-B with wagon and cargo diagnosis**

In general Product Class 2 OTI requires device installed at train tail. Optionally also other waggons can be equipped with OTI device to offer more flexibility in train composition phase and to provide wagon/cargo diagnostic functionalities.

### 6.2.3.3 Product Class 3

Optional class 3 refers to an on-board configuration with all waggons equipped with OTI module to support the optional functionality of: (i) determining train length and (ii) detecting loss of integrity with train at stand-still by separation sensors installed in all wagon.

## 6.2.4 Reference Scenarios

This sections contains identification and analysis of reference scenarios with the aim of identifying high-level functionalities to be analysed and described in more details at section 7.

High level functionalities reported in this section are expressed with the following notation:

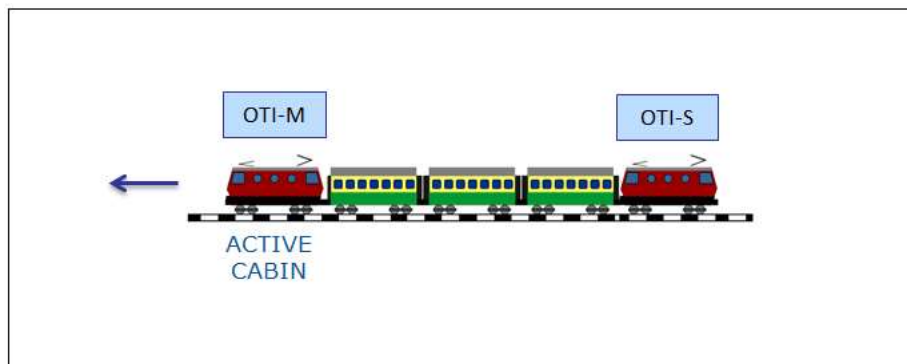
- High Level Functionality
  - General high level requirements #1
  - General high level requirements #2
  - .....
  - General high level requirements #N

Actors considered in selected scenarios are reported in the following:

- ETCS
- Train Driver
- Operation Personnel
- Maintenance Personnel
- Wayside Diagnostic Centre

### 6.2.4.1 Passenger train with fixed composition

Scenario depicted in Figure 6-22 refers to a passenger train with fixed composition related to Product Class 1. ETCS equipment is present in both cabin and OTI module is installed in both cabins.



**Figure 6-22 - Passengers trains with fixed composition**

Functional Requirements related to considered scenario refer to Mastership management to identify OTI Master and OTI Slave module. In this case OTI module in front cabin behaves as OTI Master, whereas the OTI module at train tail behave as OTI Slave. Mastership management is based on active cabin information. Subsequently OTI Slave provides its status to OTI Master that checks train integrity and informs ETCS.

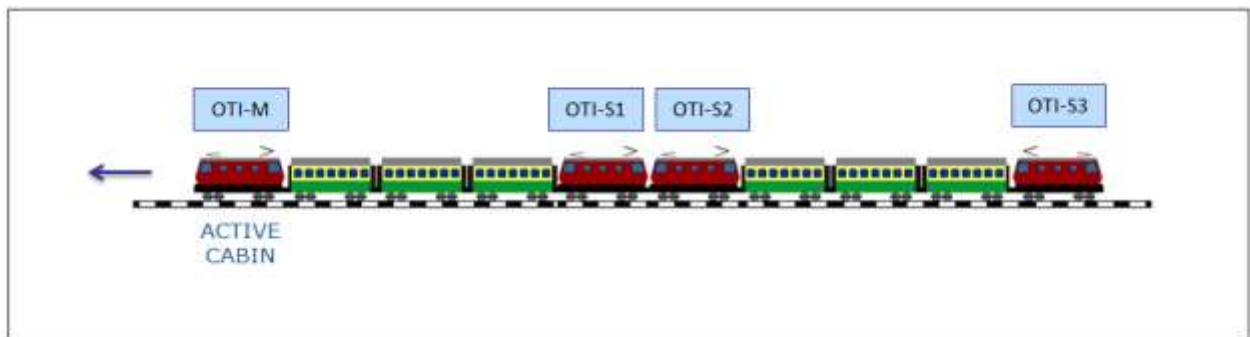
In conclusion the requirements identified in considered scenarios includes:

- Functional Requirement (Mastership)

- OTI in active cabin behave as OTI Master
- Functional Requirement (OTI Slave Status)
  - OTI Slave provides its status to OTI Master
- Functional Requirements (Train Integrity)
  - OTI Master check status of OTI Slave to evaluate train integrity status
  - OTI Master inform ETCS about train integrity status

#### 6.2.4.2 Joined passenger trains

Scenario depicted in Figure 6-23 refers to two joined passenger trains related to Product Class 1. ETCS equipment is present in both cabins on each train and OTI module is installed in both cabins of each train.



**Figure 6-23 – Joined passenger trains**

Several OTI Slave modules are present in the coupled trains and the functional requirements related to considered scenario refers to identifying present OTI Slaves and localizing OTI Slave at train tail. Finally pairing process is used to establish a communication between OTI Master and OTI Slave at train tail.

Localisation procedure is described in more details at sections 7.1.1.2 and 7.1.5.1.

Note that this document is focused on functional requirements specification. Technological solutions, including TAIL/NON TAIL determination, shall be addressed at design phase.

In conclusion the additional requirements identified in considered scenarios includes:

- Functional Requirement s (localisation, identification and pairing)
  - Defining OTI Slave localisation procedure (e.g. Manual, semi-automatic, automatic)
  - Ensuring procedures that OTI Slave represents indeed train tail (e.g. Manual, semi-automatic, automatic)
  - OTI Slave in intermediate waggons/cabins behave as OTI Slave NON TAIL
  - OTI Slave at train tail behaves as OTI Slave TAIL
  - OTI Master pairs only with OTI Slave TAIL for train integrity monitoring

#### 6.2.4.3 Train joining

Train joining scenario considered in the following refers to three steps relevant for OTI module Mastership management and train tail identification.

Scenario depicted in Figure 6-24 refers to train joining phase for two passenger trains. In this case OTI module is present at front active cabin as master (OTI-M), an OTI Slave is also present at train tail (OTI-S1). The assumption is that OTI Slave shall identify its position in the train (i.e. at train TAIL or in an intermediate waggon).

Therefore in Step 1:

- OTI-M communicates with OTI-S1 located in train TAIL.
- OTI-M provides to ETCS the value “confirmed”.

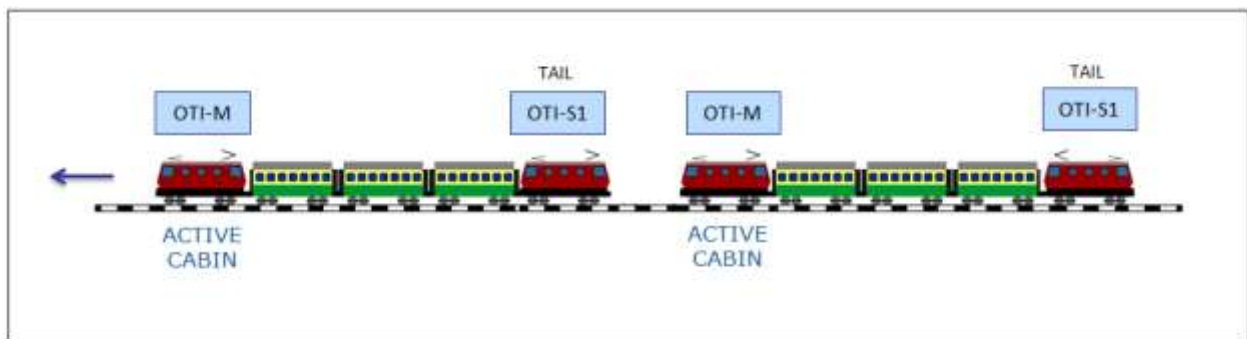


Figure 6-24 – Train joining: first step

Figure 6-28 depicts second step with two just joined trains:

- OTI-S1 becomes a NON TAIL node and therefore the pairing with OTI-M is lost
- OTI-M provides to ETCS the sequence: “lost” , “unknown”

The OTI-M of the second train becomes a slave after the cabin is deactivated. The OTIs of the second train are renumbered.

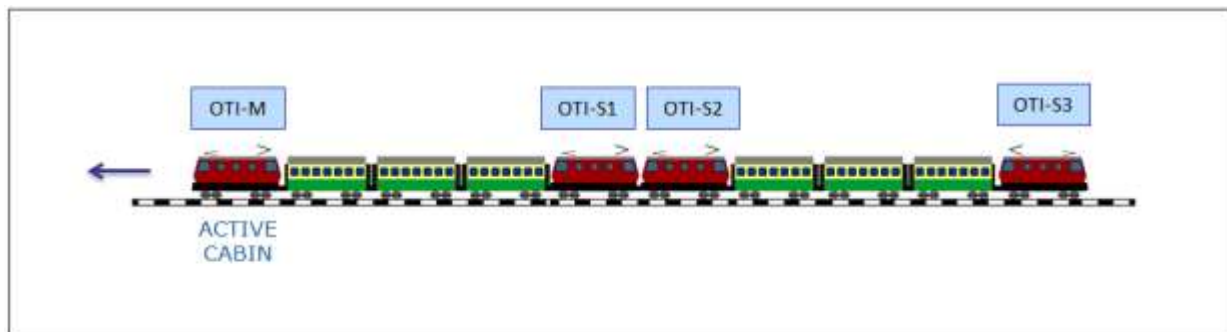
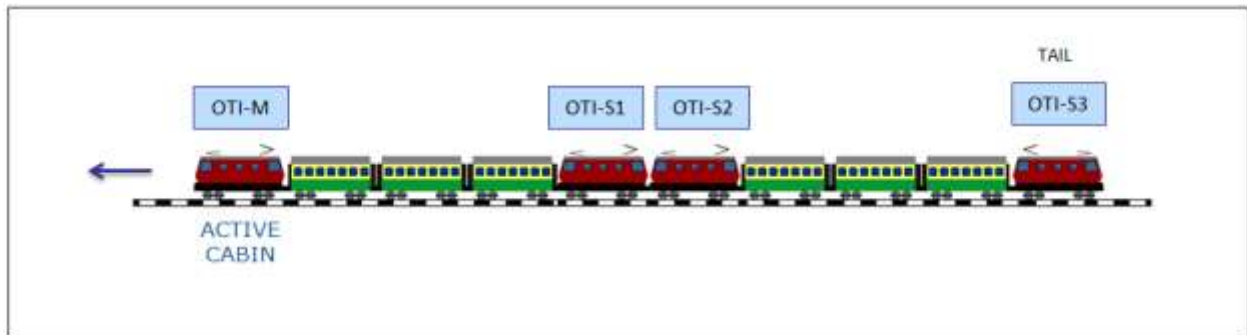


Figure 6-25 – Train joining: second step

In Figure 6-26, related to third step, the train on the left identifies its train tail and is ready to provide again train integrity confirmation:

- OTI-S3 at train tail becomes TAIL node
- OTI-M pairs with OTI-S3 at train tail
- OTI-M provides to ETCS the value “confirmed”.

Note that new train length is considered in joined train.



**Figure 6-26 – Train joining: third step**

- Functional Requirements (train joining)
  - Identify OTI Slave role change (from TAIL to NON TAIL)
  - Restart OTI Slaves identification and pairing procedure with OTI Master
  - OTI Master pairs with new OTI Slave TAIL for train integrity monitoring
  - OTI Master shall reset on ETCS command
  - OTI Master shall re-start on ETCS command

#### 6.2.4.4 Rescue Scenario

Rescue scenario is a general train joining scenario with two trains that could have different OTI product classes. In the following “first train” is the rescuing train and “second train” is the rescued train.

In case of Product Class 1 OTI system in first train (e.g. passenger train with wired communication and ETCS at train tail) and Product Class 2 OTI system in second train (wireless communication and OTI Slave device at train tail) the OTI reconfiguration process shall set an overall Product Class 2 with OTI Master in active cabin paired with OTI Slave at train tail by means of a mixed on-board communication network. Same OTI reconfiguration happens in the opposite situation (i.e. Product Class 2 for first train and Product Class 1 for second train).

In case of Product Class 3 OTI system connected to a Product Class 1 or 2 OTI system, the OTI reconfiguration process shall determine in general an OTI Product Class 2 as a result

#### 6.2.4.5 Train splitting

Train splitting scenario considered in the following refers to three steps relevant for OTI module Mastership management and train tail identification.

Scenario depicted in Figure 6-27 refers to train splitting phase for a passenger train composed of two joined trains. In this case OTI module is present at front active cabin as master (OTI-M), an OTI Slave is also present at train tail (OTI-S3). Other intermediate OTI Slave modules (OTI-S1 and OTI-S2), does not contribute to determine train integrity status (OTI-S1 and OTI-S2). The assumption is that OTI Slave shall identify its position in the train (i.e. at train tail or in an intermediate waggon).

Therefore in first Step:

- OTI-M communicates with OTI-S3 located in train TAIL
- OTI-M provides to ETCS the value “confirmed”

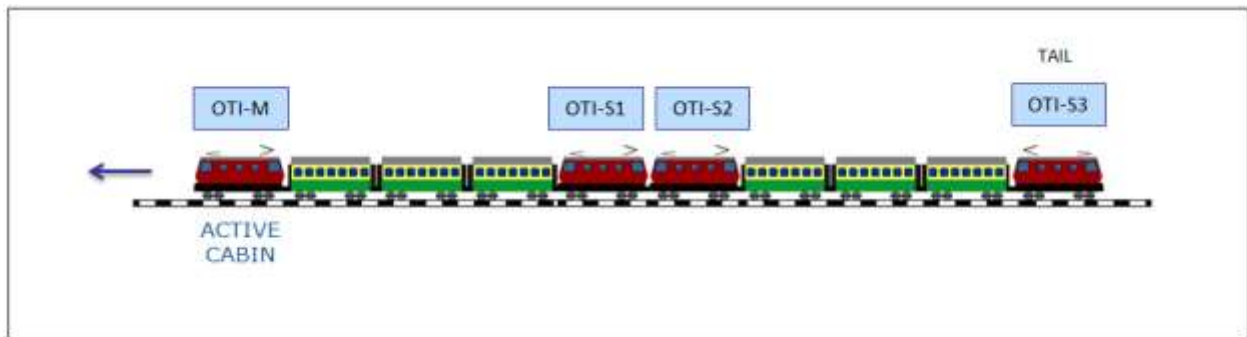


Figure 6-27 – Train splitting: first step

Figure 6-28 depicts second step with two just split trains:

- OTI-S3 becomes and NON TAIL node.
- OTI-M provides to ETCS the sequence: “lost” , “unknown”

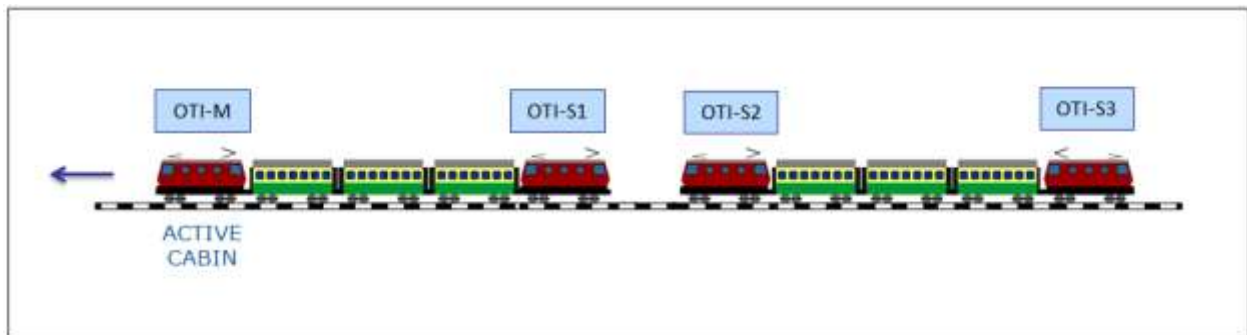
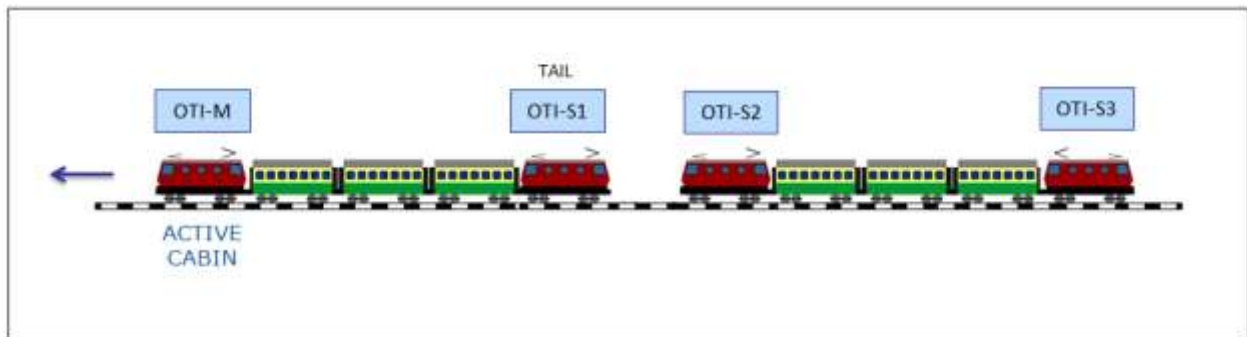


Figure 6-28 – Train splitting: second step

In Figure 6-29, related to third step, the train on the left identify its train tail and is ready to provide again train integrity confirmation:

- OTI-S1 becomes a TAIL node
- OTI-M pairs with OTI-S1 at train tail
- OTI-M provides to ETCS the value “confirmed”.

Note that new train length is considered in split train.



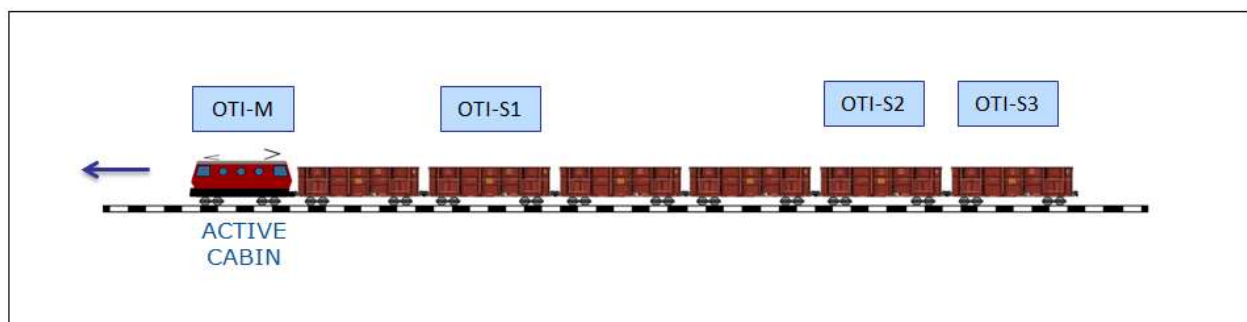
**Figure 6-29 – Train splitting: third step**

Finally, in the second train, OTI-S2 becomes an OTI Master.

- Functional Requirements (train splitting)
  - Identify OTI Slave role change (from TAIL to NON TAIL and vice versa)
  - Restart OTI Slaves identification and pairing procedure with OTI Master
  - OTI Master pairs with new OTI Slave TAIL for train integrity monitoring
  - OTI Master shall reset on ETCS command
  - OTI Master shall re-start on ETCS command

#### 6.2.4.6 Freight train

Scenario depicted in Figure 6-30 refers to freight train related to product class 2. ETCS equipment and OTI-M are present in front cabin on several OTI-S modules are installed in some waggons.

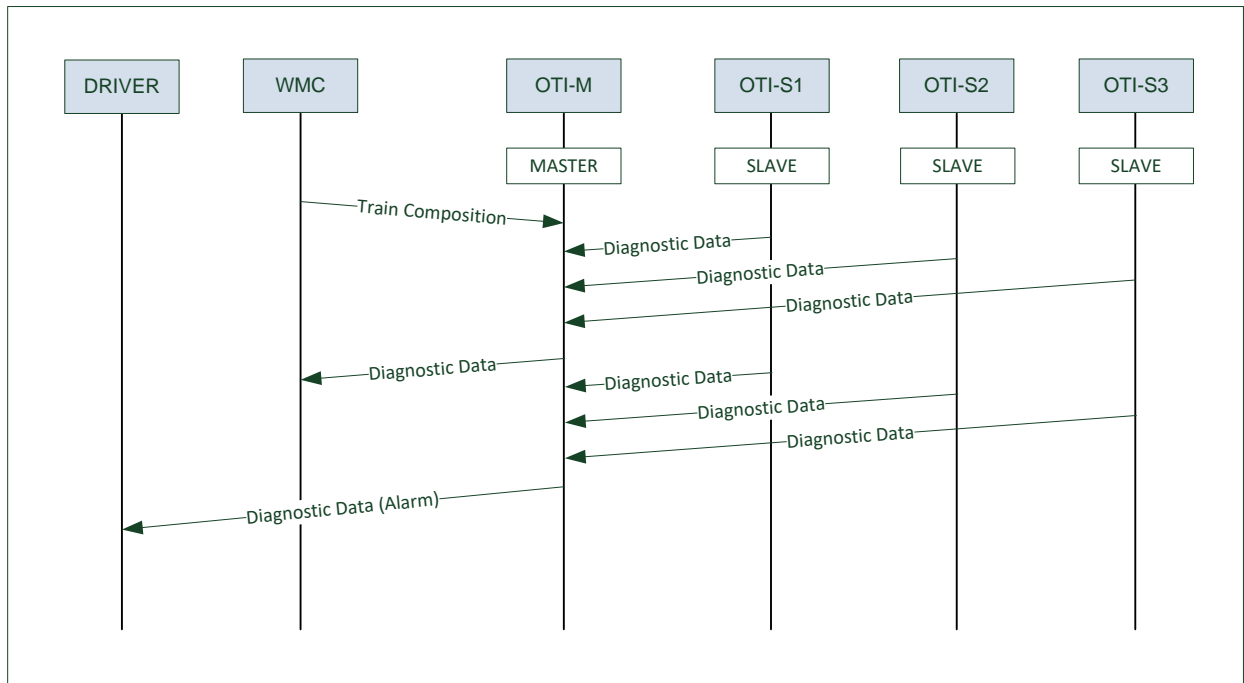


**Figure 6-30 - Freight train**



Considered scenario includes, as functional requirements, the Mastership management and OTI Slaves identification, localisation and pairing. Additional functionalities refers to waggon/cargo diagnosis provided all OTI Slave modules. Diagnostic information can be provided by each OTI Slave directly to Wayside Maintenance Centre (WMC) or provided to OTI Master that collect diagnostic data in relation to train composition and provide them to WMC. Warning to Train Driver is also considered to provide alarms about waggon/cargo status.

Figure 6-31 depicts an example of a diagnostic scenario with the OTI Master collecting cargo/waggon diagnostic data from OTI Slaves and subsequent data forwarding from OTI-M to the WMC and to the Driver.



**Figure 6-31 – Diagnostic scenario example 1**

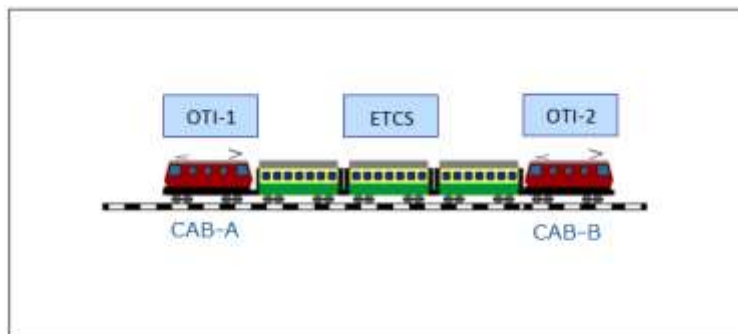
In conclusion the requirements identified in considered scenarios includes:

- (OPTIONAL) Diagnostic Requirements (waggon/cargo diagnosis)
  - OTI modules and wireless network nodes discover train composition for diagnostic purposes
  - All OTI Slave collect waggon/diagnostic data
  - All OTI Slave provides waggon/diagnostic data to
    - Wayside Maintenance Centre
      - Direct communication with wayside maintenance centre
      - Communication with OTI Master that collects diagnostic data and forward them to wayside centre
    - Train Driver

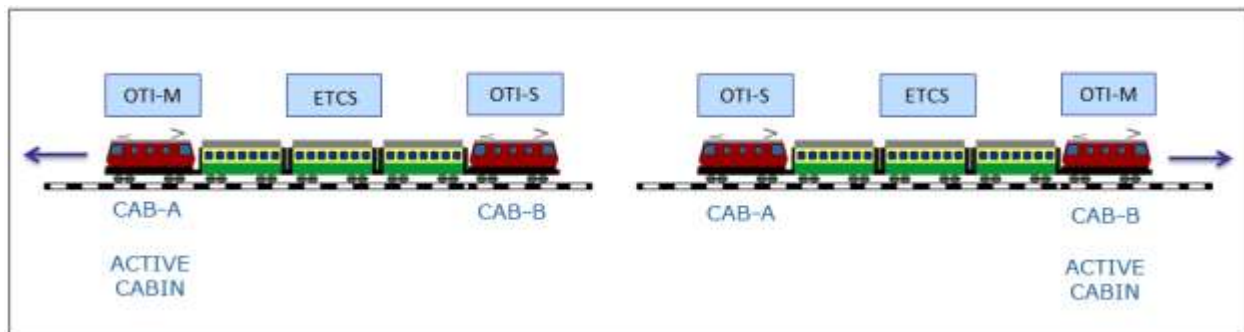
- Communication with OTI Master that collects diagnostic data and Inform train driver thus allowing him to intervene appropriately (e.g. Reducing the speed and braking the train in a safe location).
- Non-Functional Requirements (configuration and maintenance)
  - OTI modules configuration shall be performed by local maintenance personnel or by remote maintenance centre
  - OTI module SW upgrade shall be performed by local maintenance personnel or by remote maintenance centre

#### 6.2.4.7 Scenario with central ETCS configuration

This scenario refers to trains equipped with a central ETCS configuration, as depicted in Figure 6-32 and in Figure 6-33. In this scenario ETCS shall communicate with OTI module in Cabin A or Cabin B, depending on the active cabin.



**Figure 6-32 – Central ETCS configuration**



**Figure 6-33 – Central ETCS configuration vs Cabin Selection**

In this case ETCS need a logical communication channel with both OTI modules that shall acquire Master or Slave role depending on active cabin. More specifically ETCS need to know in advance the ID of the two connected OTI modules thus properly assigning the Master role and thus properly receiving train integrity messaged only from OTI Master.

The results of the analysis of present scenario is that in central ETCS configuration the communication protocol have to include identification of OTI module in each message.

Detailed Mastership sequence diagrams are reported at Figure 7-7 and Figure 7-8.

- Communication Requirements (OTI modules identification)
  - Each OTI module shall have a unique identifier
  - OTI unique identifier shall be included in each message
  - ETCS shall check the identifier of paired OTI Master module

#### 6.2.4.8 Shunting Scenario

During shunting phases, train composition is changed and one or several waggons are coupled/decoupled to/from the train and OTI module should avoid performing train integrity monitoring. As example the OTI slave at train tail changes while adding waggons at the end. Or more than one tail could be present with locomotive in intermediate position during train composition.

For these reasons "start" and "reset" commands from ETCS need to be taken into account in defining the functional requirements.

- Functional Requirements (Shunting)
  - OTI shall start on ETCS command
  - OTI shall reset on ETCS command

Note that shunting scenario could be referred to train composition phase or not. In first case the OTI functionality need to be suspended and then restarted after completing the train composition process. In second case the OTI functionality need to be kept active. The reset and start commands have been added to provide more flexibility to on-board equipment and to the operator.

#### 6.2.4.9 Moving Blocks Scenario

On-board train integrity functionality is relevant to implement moving blocks and to reach high performances and high capacity levels. For this reason OTI shall provide periodically the train integrity information to ETCS.

Moreover, before ending the mission, ETCS need updated train integrity status. Periodic status reporting could be not sufficient in case of long reporting period. Therefore a "Status Request" command from ETCS is introduced.

Note that if the period is short enough (1s as described above) then there is no need for an additional ETCS functionality "Status Request".

- Functional Requirements (Moving Blocks)
  - OTI shall provide periodic train integrity status to ETCS
  - OTI shall provide updated train integrity status on "Status Request" ETCS command

In general changing the train composition implies a reconfiguration process for OTI system. Using train cabin disable and re-enable as trigger events implies performances limitations due to the need for ETCS to re-establish the connection with RBC. This situation causes delays in case the train composition is changed in intermediate stops of a journey (e.g. removing or adding passenger waggons). For this reason alternative trigger event have been considered for OTI system reconfiguration as described at section 6.2.4.8.

Another relevant remark related to Moving Blocks assumptions refers to take into account ETCS backward compatibility (i.e. BL3 R2 [1] and CR940 [3]). This topic is addressed in further details in D4.2 [7] in relation to interface specification.

#### 6.2.4.10 GNSS Scenario

Train integrity monitoring, based on position derived by GNSS, requires receiving train length as input from ETCS.

- Functional Requirements (GNSS)
  - OTI shall receive train length from ETCS

#### 6.2.4.11 Conclusions

The aim of this section is to list the high-level functional requirements and functional interfaces identified in above analysed scenarios as general guidelines for subsequent functional requirements specification reported at section 7.

High level functionalities reported in this section are expressed with the following notation:

- High Level Functionality
  - General high level requirements #1
  - General high level requirements #2
  - ...
  - General high level requirements #N
- Functional Requirements (Mastership)
  - OTI in active cabin behaves as OTI Master
  - OTI at train tail behaves as OTI Slave TAIL
  - OTI at intermediate train waggons/cabins behave as OTI Slave NON TAIL
- Functional Requirements (OTI Slave Status)
  - OTI Slave provides its status to OTI Master
- Functional Requirements (Train Integrity)
  - OTI Master checks status of OTI Slave TAIL to evaluate train integrity status
  - OTI Master informs ETCS about train integrity status

- Functional Requirements (localisation, identification and pairing)
  - Defining OTI Slave localisation procedure (e.g. Manual, semi-automatic, automatic)
  - Ensuring procedures that OTI Slave represents indeed train tail (e.g. Manual, semi-automatic, automatic)
  - OTI Slave in intermediate waggons/cabins behaves as OTI Slave NON TAIL
  - OTI Slave at train tail behaves as OTI Slave TAIL
  - OTI Master pairs only with OTI Slave TAIL for train integrity monitoring
- Functional Requirements (train joining)
  - Identify OTI Slave role change (from TAIL to NON TAIL)
  - Restart OTI Slaves identification and pairing procedure with OTI Master
  - OTI Master pairs with new OTI Slave TAIL for train integrity monitoring
  - OTI Master shall reset on ETCS command
  - OTI Master shall re-start on ETCS command
- Functional Requirements (train splitting)
  - Identify OTI Slave role change (from TAIL to NON TAIL and vice versa)
  - Restart OTI Slaves identification and pairing procedure with OTI Master
  - OTI Master pairs with new OTI Slave TAIL for train integrity monitoring
  - OTI Master shall reset on ETCS command
  - OTI Master shall re-start on ETCS command
- Functional Requirements (Shunting)
  - OTI shall start on ETCS command
  - OTI shall reset on ETCS command
- Functional Requirements (Moving Blocks)
  - OTI shall provide periodic train integrity status to ETCS
  - OTI shall provide updated train integrity status on "Status Request" ETCS command
- Functional Requirements (GNSS)
  - OTI shall receive train length from ETCS
- (OPTIONAL) Diagnostic Requirements (waggon/cargo diagnosis)
  - OTI modules and wireless network nodes discover train composition for diagnostic purposes
  - All OTI Slave collect waggon/diagnostic data
  - All OTI Slave provides waggon/diagnostic data to
    - Wayside Maintenance Centre
      - Direct communication with wayside maintenance centre
      - Communication with OTI Master that collects diagnostic data and forward them to wayside centre
    - Train Driver

- Communication with OTI Master that collects diagnostic data and Inform train driver thus allowing him to intervene appropriately (e.g. Reducing the speed and braking the train in a safe location).
- Communication Requirements (OTI modules identification)
  - Each OTI module shall have a unique identifier
  - OTI unique identifier shall be included in each message
  - ETCS shall check the identifier of paired OTI Master module
- Non-Functional Requirements (configuration and maintenance)
  - OTI modules configuration shall be performed by local maintenance personnel or by remote maintenance centre
  - OTI module SW upgrade shall be performed by local maintenance personnel or by remote maintenance centre
- OTI Master Interfaces
  - ETCS (train integrity)
  - Active OTI Slave at train tail (train integrity)
  - Non Active OTI Slaves (waggon/cargo diagnosis)
  - Wayside Maintenance Centre (waggon/cargo diagnosis)
  - Train Driver (waggon/cargo alarms)
- OTI Slave Interfaces
  - OTI Master (train integrity)
  - Odometry (train integrity)
  - Wireless sensors (communication, train composition determination)
  - Waggon/cargo diagnostic sensors (waggon/cargo diagnosis)
  - Wayside Maintenance Centre (waggon/cargo diagnosis)

Note that status of train integrity is provided by OTI Master to ETCS. Providing this information also to train driver by means of ETCS DMI is an interesting hypothesis. However this option would require changes at ETCS Core and DMI functional requirements specifications.

Note that according to SUBSET 034 [2] and CR940 [3], the interface between TIMS and ETCS is implicitly unidirectional and includes three possible values as train integrity status from TIMS to ETCS:

- Train integrity confirmed
- Train integrity lost
- Train integrity status unknown

The analysis of reference scenarios reported in previous section remarked the need of the following additional data exchange between OTI and ETCS:

#### 1. Active Cabin

2. Start/Reset commands
3. Train Length
4. Train integrity status on ETCS request

Active cabin information is used in OTI Mastership phase to define OTI module role (i.e. Master in Active Cabin and Slave in Non-Active Cabin). This information can be acquired from ETCS with Start/Stop commands or directly from TIU rolling stock as cabin status.

Start/Reset commands allow managing train joining/splitting phase in operation without closing and re-opening the desk. The result is to avoid ETCS-RBC re-connection thus guaranteeing better performances.

Train Length is an input from ETCS to OTI in Product Class 2 with train tail GNSS based localization. This information is also useful as trigger for OTI reconfiguration after completing the train composition.

OTI device provides periodically the train integrity status to ETCS. The optional command of providing train integrity status on ETCS request is related to End Of Mission scenario with long train integrity monitoring period (e.g. 30 sec). This command allows updating train integrity status on ETCS request before closing the desk.

In conclusion limiting the ETCS-OTI interface to the three values currently quoted inside CR940 implies the following limitations:

- Limited performances in train joining/splitting phase
- Not suitable to support GNSS train tail localization in OTI Product Class 2

For generality OTI functional requirements specification is organized to acquire active cabin information as cabin status from rolling stock or as start/reset commands and train length from ETCS.

## **6.2.5 Virtual Coupling assumptions and preliminary analysis**

This section contains assumptions and preliminary analysis in relation to virtual coupling scenario.

Considering Virtual Coupling concept in terms of trains running simultaneously and virtually coupled to the train in front and communicating and matching their speed to maintain safe splitting. In this scenario the trains are considered as part of a single train.

In this context, to be explored in details in Virtual Coupling TD2.8, the assumption is that monitoring the train integrity of each train is sufficient to support Virtual Coupling.

The preliminary analysis reported in this section refers to supporting dynamic joining/splitting in relation to wireless consist to consist communication with the following assumptions:

- On-board wireless backbone is available as un-trustable communication medium
- Automatic mechanical coupler is available
- Each train-set is equipped with a complete ETCS equipment including OTI functionality

- ETCS need to know train composition (e.g. provided by train Driver or RBC) and train length variation after joining/splitting procedures

In this context the feasibility for OTI function to support dynamic joining and splitting is analysed.

Note that in the following ETCS1 is used to refer to ETCS installed in train 1 and ETCS2 is used to refer to ETCS installed in train 2.

#### 6.2.5.1 Splitting scenario

Figure below depicted a train that is split intentionally. Case A refers to a train made up of two joined train-sets with an OTI master in active cabin (M1), OTI slave modules in intermediate waggons (S1, S2) behave as NON TAIL and an OTI Slave behaving as TAIL in last waggon (S3-T). Case B refers to two split train-sets with independent ETCS and related OTI Master and Slave modules (i.e. M1 and S1-T for first train; M2 and S3-T for second train).

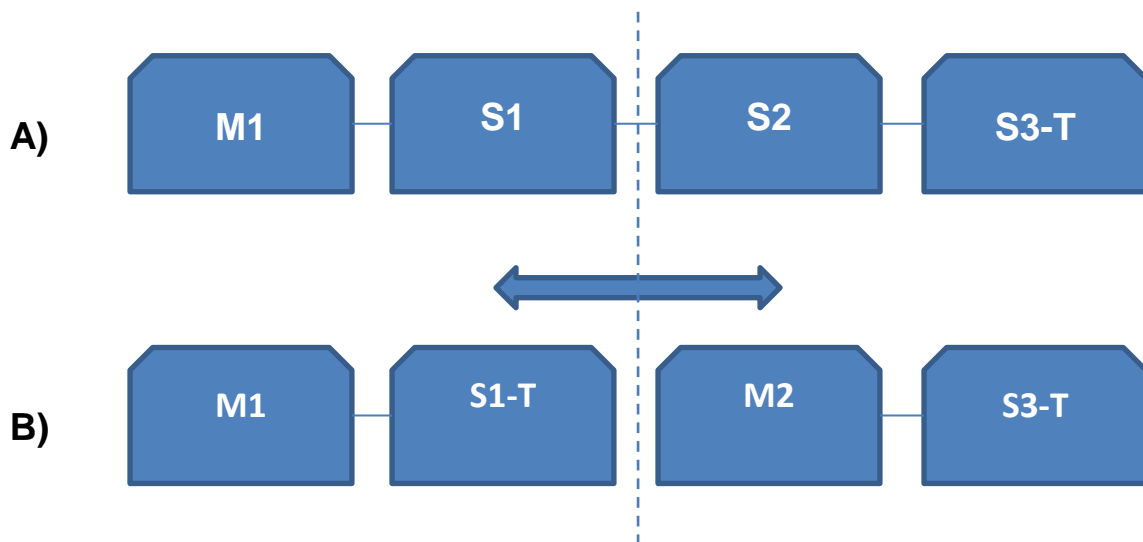


Figure 6-34 – Train compositions during dynamic splitting

#### 6.2.5.2 Static Splitting

In static splitting the assumption is that the train is at stand-still in a freight yard or in shunting area. In this case the following event sequence occurs:

1. M1 is paired with S3-T (Train Integrity information is "CONFIRMED")
2. M1 detects that train integrity lost (Train Integrity information is "LOST") due to the splitting
3. M1 restarts FSM (Train Integrity information is "UNKNOWN")
4. M1 pairs with S1-T (Train Integrity information is "CONFIRMED")



The event that triggers the OTI Master FSM is a loss of pairing with OTI Slave TAIL.

#### 6.2.5.3 Dynamic Splitting

In dynamic splitting the assumption is that the train is in operation and is “running”.

This scenario is considered as preliminary analysis to support future Virtual Coupling functionality that shall be analysed and defined in TD2.8 in terms of functionalities and related hazards.

In the following S1-T refers to an OTI Slave with TAIL role and S3-NT refers to an OTI Slave with NON TAIL role.

The following event sequence occurs:

1. M1 is paired with S3-T (Train Integrity information is “CONFIRMED”) after start command from ETCS
2. M1 pairs with S1 Non Tail and maintains the monitoring of S3-T (Train Integrity information is “CONFIRMED” with S3-T and “UNKNOWN” with S1-NT).

In this case the trigger event is that ETCS1 sends to M1 a pairing command with S1.

3. M1 check the status of train integrity with S3-T and S1-NT (Train Integrity information is “CONFIRMED” with S3-T and “CONFIRMED” with S1-NT).
4. S2 becomes Master M2 (Train Integrity information is “UNKNOWN”).

In this case the trigger event is that ETCS2 sends master command to S2.

5. M2 pairs with S3-T (Train Integrity information is “CONFIRMED”)

M1 closes the pairing with S3-T and maintains train integrity monitoring with S1-NT (Train Integrity information is “CONFIRMED” with S1-NT and “UNKNOWN” with S3-T).

In this case the trigger event is that ETCS2 confirms to ETCS1 that train integrity is “CONFIRMED”.

Subsequent step consists in physical splitting of the two trains sets that becomes autonomous and independent with OTI S1 transition from Non Tail to Tail.

In considered scenario, the assumption is that train length variation after train splitting is already known by ETCS that therefore uses new train length after the splitting. In general the focus of the analysis refers to OTI FSM and related predispositions to support dynamic splitting. Possible changes to ETCS Core need to be further analysed after that TD2.8 has provided a full analysis for Virtual Coupling topic.

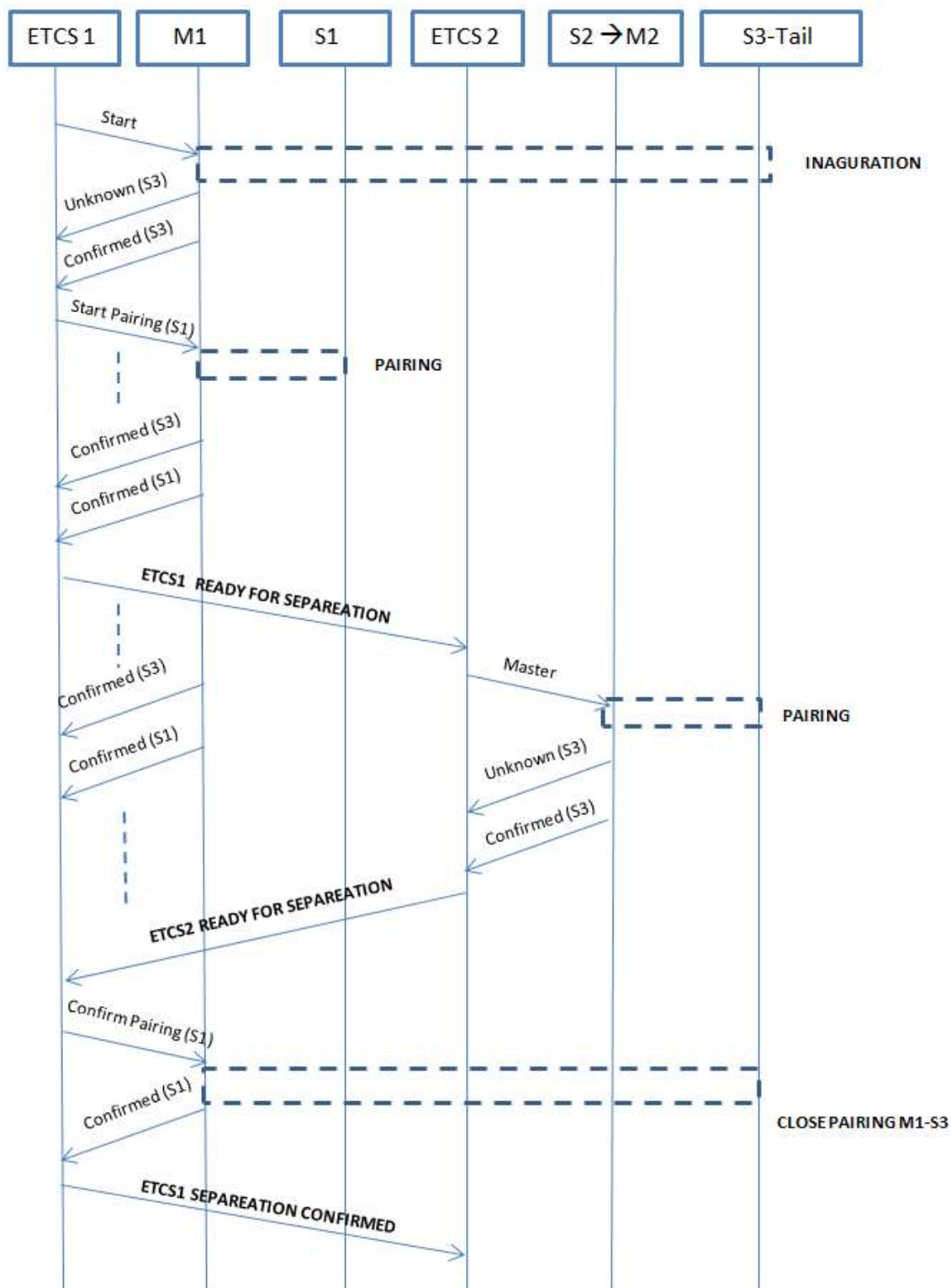


Figure 6-35 – Central ETCS configuration vs Cabin Selection

Above reported analysis, remarks that the following ETCS pre-requirements are necessary to support dynamic splitting:

- ETCS knows Train Composition and Train Length
- ETCS manages splitting process by interacting with other ETCS
- ETCS generates pairing commands to OTI Master

And the following macro-functionalities are required at OTI module level:

- OTI Master manages pairing commands and double pairings
- OTI Slave accepts double pairing commands

#### **6.2.5.4 Conclusion**

Defined OTI-M and OTI-S FSMs and related requirements are suitable to be applied to wireless consist to consist context providing a wireless on-board communication backbone.

Possible predisposition for supporting dynamic joining consists essentially in: (i) introducing in OTI-M FSM the capability to manage pairing commands from ETCS and (ii) introducing in OTI-S FSM the capability to manage multiple pairings.

Most relevant impact for supporting dynamic joining/splitting procedures consists in modifications to ETCS core.

On the basis of identified assumptions, the result of preliminary analysis remarks that availability of full requirements specification from TD2.8 is mandatory to identify the expected functionalities from TD2.5.

Under identified assumption and on the basis of analysed splitting scenario, introducing the support for Virtual Coupling functionality impacts at functional level and not at architectural level.

In conclusion a complete analysis and requirements specification for Virtual Coupling is part of TD2.8 and is out of TD2.5 scope of work.

### **6.3 Investigation on wireless sensors and transponder technologies**

This investigation was performed using the “Technologies Evaluation for Freight Train’s Wireless Backbone” [50] paper as basis of the wireless technologies analysis [68]. The Wireless Sensor Analysis was performed basing it in the DEWI Deliverables [46] [47] and own INDRA expertise.

#### **6.3.1 Available terrestrial wireless technologies**

In the following paragraphs, the main features used for describing for differentiating wireless technologies are described in detail. After these, the different technologies have been described according to the features previously described. Only those, which could suffice to the expected

requirements, are characterized in higher detail. Technologies like IRDA, RFID or UWB are shown only in the graph for reference.

#### 6.3.1.1 **Communications protocols**

The ISO/OSI layered communication protocol model defines seven protocol layers. But often different specifications providers/owners, like standards bodies (ISO, ITU, ETSI, IEEE, IEC), develop only a subset of these layers:

- physical layer (PHY)
- link layer – often mentioned as media access control (MAC) layer

Many wireless technologies are then often developed by industrial consortia, and add only some necessary higher communication layers, like:

- network layer
- application layer

More sophisticated protocol stacks might use other layers of the ISO/OSI layered model adding more layers between the network and application layer:

- transport layer
- session layer
- presentation layer

But mostly the functions of these latter layers are embedded in fewer layers which are then named according the rules of the specification owners.

When analysing the technologies that suit the Train Integrity case we will focus on the first layers up to the application layer maximum.

#### 6.3.1.2 **Communications application areas**

In order to do a valuable analysis it is useful to understand what are the application areas, what are the Use cases.

The main application areas for data transmission are:

- office and home networking
- metropolitan networking
- country-wide and international networking
- industrial control networking
- monitoring and measurement data acquisition

- Intelligent Transportation Systems – ITS
- Internet of Things – IoT

The Use Cases more related with this project will be the last four, or better a combination of them. The use of the network for industrial control systems (it is a Safety system), the acquisition and monitoring of data (the integrity of the train), Intelligent Transportation Systems (For future use in ERTMS level 3), and Internet of Things for the need of new network topologies and systems.

### 6.3.1.3 Data rate and ranges of wireless technologies

The next figure shows the range of the wireless technologies in relation to the available data rates. Based on this figure the most appropriate technologies are then described in more detail. Those technologies which provide sufficient range and fulfil high train speed requirements will be considered. These requirements are:

- 350km/h maximum speed
- 27.5m maximum waggon length.

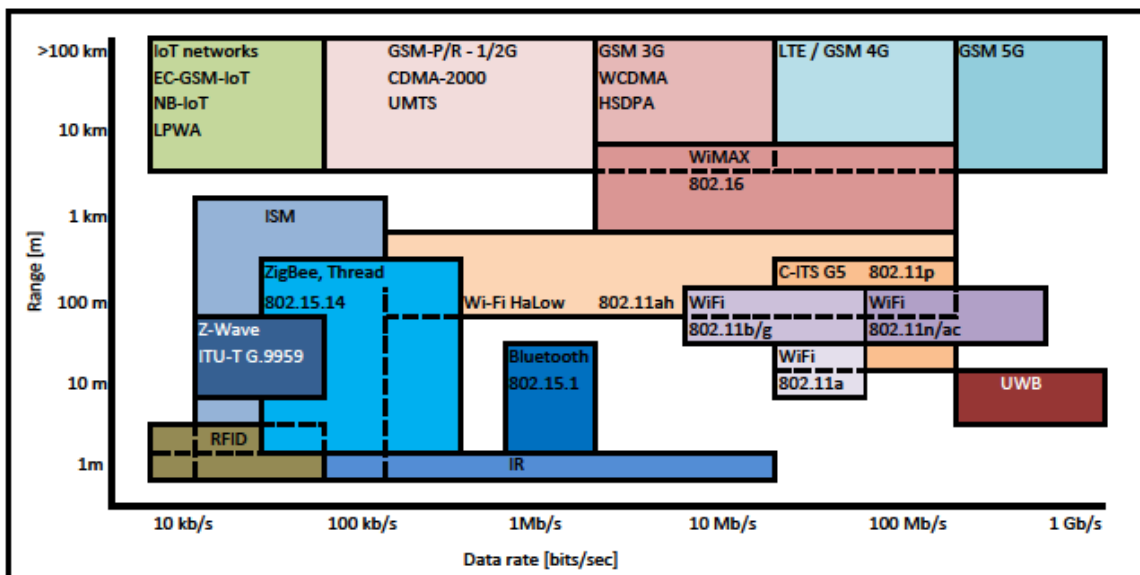


Figure 6-36 – Terrestrial Networks

### 6.3.1.4 IEEE 802.11 family

#### 6.3.1.4.1 IEEE 802.11a/b/g/n/ac (WiFi)

The WiFi standard is widely used public standard designed to enable predominantly office and home networking. It is focused to ensure high bandwidth, high data rate transmissions for the transport of long frames of data packets and files.

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands. They are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802).

Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones, and Bluetooth devices. 802.11b and 802.11g control their interference and susceptibility to interference by using direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM) signalling methods, respectively. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz Industrial, Scientific and Medical (ISM) frequency band offering only three non-overlapping channels, where other adjacent channels overlap. Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment. 802.11n can use either the 2.4 GHz or the 5 GHz band; 802.11ac uses only the 5 GHz band. It is worth noting that in 802.11 family all users of the same network do share the same medium and no scheduled-MAC is performed, which usually generates collisions in dense networks, which produce unpredictable latencies.

Features	Description
Points	Static
Nodes	Static
Type	Master/Client – Point to multipoint
Data rate	11 – 1000 Mbit/s
Average throughput	5 – 600 Mbit/s
Range	10 m – 250 m (usually up to 50 m; upper part of the range only with adequate antenna and higher transmit power)
Frequency	2,4 / 3,7 / 5,0 GHz
Spectrum use	public
MIMO	In n, ac

<b>Point to point</b>	In 5 GHZ band
<b>Point to multipoint</b>	Usually 2,4 GHz
<b>Latency</b>	1-10 ms

**Table 6-6 – 802.11a/b/g/n/ac characteristics**

#### 6.3.1.4.2 Standard 802.11ah (HaLow)

IEEE 802.11ah is a wireless networking protocol that is an amendment of the IEEE 802.11-2007 wireless networking standard. It uses sub-1 GHz license-exempt bands to provide extended range Wi-Fi networks, compared to conventional Wi-Fi networks operating in the 2.4 GHz and 5 GHz bands.

A benefit of 802.11ah is its extended range, making it useful for rural communications and offloading cell phone tower traffic [13]. Compared to cell phone networks it is more suitable for relatively static networks without real-time switching the connections among end client devices.

It uses the 802.11a/g specification down sampled to provide 26 channels, each of them able to provide 100 kbit/s throughput. It can cover a one-kilometer radius. [12] It aims at providing connectivity to thousands of devices under an access point.

Data rates up to 234 Mbit/s are achieved only with the maximum of four spatial streams using one 16 MHz-wide channel. Various modulation schemes and coding rates are defined by the standard and are represented by a Modulation and Coding Scheme (MCS) index value.

Power saving stations are divided into two classes: TIM stations and non-TIM stations. TIM stations periodically receive information about buffered traffic for them from the access point in so-called TIM information element, hence the name. Non-TIM stations use the new Target Wake Time mechanism which allows to reduce signalling overhead [13].

Security is comparable to 802.11a/b/g/n standards.

<b>Features</b>	<b>Description</b>
<b>Points</b>	Static or slow moving
<b>Nodes</b>	Static
<b>Type</b>	Master/Client – Point to multipoint
<b>Data rate</b>	0,65 – 234 Mbit/s

<b>Average throughput</b>	0,1 – 100 Mbit/s
<b>Range</b>	100 m – 1000 m
<b>Frequency</b>	ISM band (868 MHz Europe, 908/916 MHz USA)
<b>Spectrum use</b>	public
<b>MIMO</b>	n.a.
<b>Point to point</b>	yes
<b>Point to multipoint</b>	yes
<b>Latency</b>	? ms

**Table 6-7 – 802.11ah characteristics**

#### 6.3.1.4.3 *Standard 802.11p (ETSI ITS-G5)*

IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments. The IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE) is a higher layer standard based on the IEEE 802.11p. The WAVE standards define an architecture and a complementary, standardized set of services and interfaces that collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications [14].

In Europe, 802.11p was used as a basis for the ITS-G5 standard, supporting the GeoNetworking protocol for vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication [15]. ITS G5 and GeoNetworking is being standardized by the European Telecommunications Standards Institute group for Intelligent Transport Systems.

Comparing the performance of 802.11p and 802.11b [16] for different environments (highway, rural, and urban area), 802.11p shows better benefits than 802.11b in terms of throughput, delay, and delivery ratio. Main results [16] for highway environment are shown as an example:



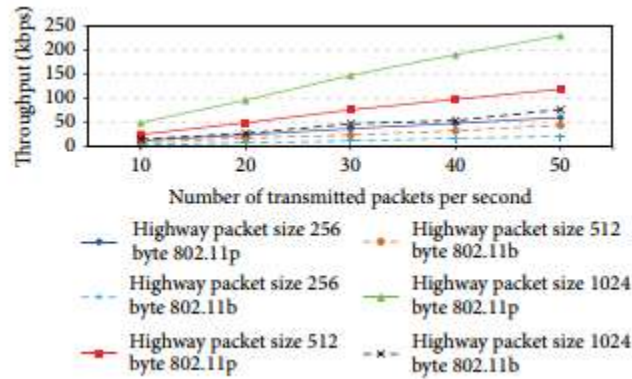


Figure 6-37 - Throughput of 802.11p and 802.11b

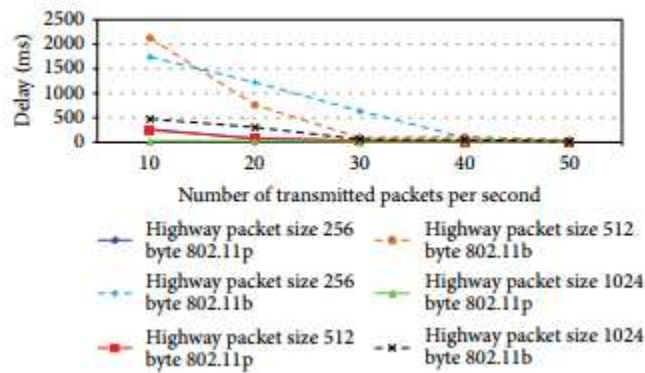


Figure 6-38 - End-to-End Delay of 802.11p and 802.11b

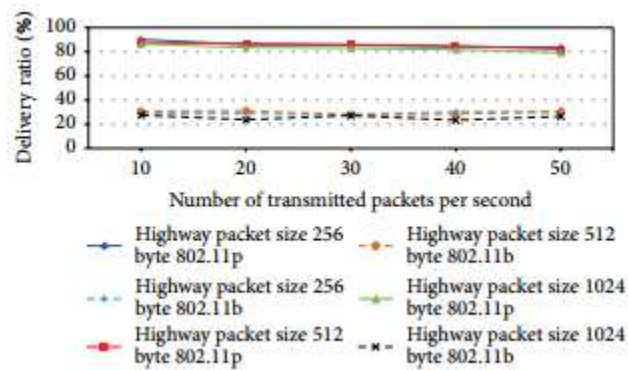


Figure 6-39 - Delivery ratio of 802.11p and 802.11b

Main features of 801.11p are shown in the following table:

Features	Description
----------	-------------

<b>Points</b>	moving (150 km/h or more)
<b>Nodes</b>	Static/moving
<b>Type</b>	Master/Client – Point to multipoint
<b>Data rate</b>	6 – 108 Mbit/s
<b>Average throughput</b>	>1 Mbit/s
<b>Range</b>	50 m – 300 m
<b>Frequency</b>	5,850 – 5,925 GHz
<b>Spectrum use</b>	unlicensed
<b>MIMO</b>	n.a.
<b>Point to point</b>	In 5 GHz band
<b>Point to multipoint</b>	Usually 2,4 GHz
<b>Latency</b>	40 - 200 ms

**Table 6-8 802.11p characteristics**

#### 6.3.1.5 IEEE 802.15.1 (Bluetooth)

The principle application is in the area of low-power communications over short distances, mainly in one room. However, for advanced versions, higher range up to 100 m is described. [17]

Typical data rate is 700 kbit/s. Bluetooth operates at frequencies between 2402 and 2480 MHz, or 2400 and 2483.5 MHz including guard bands 2 MHz wide at the bottom end and 3.5 MHz wide at the top. Bluetooth uses a radio technology called frequency-hopping spread spectrum. Bluetooth divides transmitted data into packets, and transmits each packet on one of 79 designated Bluetooth channels. Each channel has a bandwidth of 1 MHz. It usually performs 800 hops per second, with Adaptive Frequency-Hopping (AFH) enabled. [18]

This protocol is starting to become less secure, multiple attack vectors have been found (hydra, blueBorne ...). This proves dangerous since it is not an open standard and provides most of its security through obscurity.

Supports stars type of network: point-to-point, point-to-multipoint.

Features	Description
Points	Static or slow moving
Nodes	Static
Type	Master/Client – Point to multipoint
Data rate	typ. 1 (up to 10) Mbit/s
Average throughput	typ. 0,1 – 0,5 (up to 5) Mbit/s
Range	10 m – 100 m (usually up to 10 m; upper part of the range only with adequate antenna and higher transmit power)
Frequency	2,4 GHz ISM band
Spectrum use	public
MIMO	n.a.
Latency	10 ms

**Table 6-9 - 802.15.1 Bluetooth characteristics**

#### 6.3.1.6 IEEE 802.15.4 family

##### 6.3.1.6.1 ZigBee

Zigbee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection.

The 802.15.4 standard defines

- physical layer
- media access control (MAC) layer

This standard specifies operation in the unlicensed 2.4 to 2.4835 GHz [19], and 868 to 868.6 MHz (Europe) ISM bands. Sixteen channels are allocated in the 2.4 GHz band, with each channel spaced 5 MHz apart, though using only 2 MHz of bandwidth. The radios use direct-sequence spread spectrum coding, which is managed by the digital stream into the modulator.

The transmission is secured with symmetrical 128 bit AES cryptographic protocol which is fully sufficient for most types of time limited transmission sessions. IEEE 802.15.4 nodes can operate in either secure mode or non-secure mode.

Multi-hop transmission is available hence different types of networks can be set up: star, tree and mesh. Hundreds of devices can be connected to one master through the network.

Features	Description
Points	Static or slow moving
Nodes	Static
Type	Master/Client – Point to multipoint
Data rate	20/40 kbit/s for ISM band, 250 kbit/s for 2,4 GHz band
Average throughput	1 – 50 kbit/s
Range	100 m – 1000 m (usually up to 300 m; upper part of the range only with adequate antenna and higher transmit power)
Frequency	2,4 GHz band, ISM band (868 MHz Europe, 908/916 MHz USA)
Spectrum use	public
MIMO	n.a.
Latency	10 ms

**Table 6-10 - 802.15.4 ZigBee characteristics**

#### 6.3.1.6.2 6LoWPAN

6LoWPAN is an acronym of IPv6 over Low Power Wireless Personal Area Networks. The 6LoWPAN group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks. IPv4 and IPv6 are the work horses for data delivery for local-area networks, metropolitan area networks, and wide-area networks such as the Internet. Likewise, IEEE 802.15.4 devices provide sensing communication-

ability in the wireless domain. The base specification developed by the 6LoWPAN IETF group is RFC 4944.

IEEE 802.15.4 nodes can operate in either secure mode or non-secure mode. Two security modes are defined in the specification in order to achieve different security objectives: Access Control List (ACL) and Secure mode. [20]

Features	Description
Points	Static or slow moving
Nodes	Static
Type	Star – Cluster Tree – Point to multipoint
Data rate	250 kbps (2.4 GHz) 40 kbps (915 MHz) 20 kbps (868 MHz)
Average throughput	1 – 50 kbit/s
Range	1 m – +75 m
Frequency	2,4 GHz band, ISM band (868 MHz Europe, 908/916 MHz USA)
Spectrum use	public
MIMO	n.a.
Latency	? ms

**Table 6-11 - IEEE 802.15.4 6LoWPAN**

#### 6.3.1.6.3 Thread

Thread uses 6LoWPAN, which in turn uses the IEEE 802.15.4 wireless protocol with mesh communication, as does ZigBee and other systems. Thread however is IP-addressable, with cloud access and AES encryption. It currently supports up to 250 devices in one local network mesh. [21]

Unlike other proprietary networks, 6LoWPAN, like any network with edge routers, does not maintain any application layer state because such networks forward datagrams at the network

layer. This means that 6LoWPAN remains unaware of application protocols and changes [22]. This lowers the processing power burden on edge routers. It also means that Thread does not need to maintain an application layer.

Thread promises a high level of security. Only devices that are specifically authenticated can join the network. All communications through the network are secured with a network key. [23]

Features	Description
Points	Static or slow moving
Nodes	Static
Type	Master/Client – Point to multipoint
Data rate	250 kbit/s for 2,4 GHz band
Average throughput	1 – 50 kbit/s
Range	10 m – 100 m (usually up to 30 m)
Frequency	2,4 GHz band, ISM band (868 MHz Europe, 908/916 MHz USA)
Spectrum use	public
MIMO	n.a.
Latency	100 ms

**Table 6-12 - 802.15.4 Thread characteristics**

#### 6.3.1.7 IEEE 802.16 (WiMAX)

WiMAX standard has been defined and developed in 2003 as an IEEE 802.16a standard. It is defined for long ranges of 10 km and above, predominantly at LOS (Line-of-sight). The main focus is on high data rate and high ranges.

Modulation type SOFDM (used in 802.16e-2005) and OFDM256 (802.16d) are not compatible thus equipment will have to be replaced if an operator is to move to the later standard (e.g., Fixed WiMAX to Mobile WiMAX).

An advantage of WiMAX is that enables communication over a maximum distance of 50 km compared to 100 m for WiFi. Naturally, the longer the distance, the slower the data rate. [24]

Security of the transmission is provided by AES 128/256 bit symmetrical keys. Additionally, it is recreated at intervals for optimal security. The 802.16e-2005 amendment specifies Privacy and Key Management Protocol Version 2 as the key management implementation [25].

Standard authentication protocol is employed - user and device authentication for WiMAX consists of certificate support using Internet Engineering Task Force (IETF) Extensible Authentication Protocol (EAP).

Features	Description
Points	Static or moving
Nodes	Static or moving (up to 120 km/h)
Type	Master/Client – Point to multipoint
Data rate	6 – 376 Mbit/s
Average throughput	1 – 50 kbit/s
Range	1000 m – 50 km (with decreasing available data rate; high rates only with MIMO)
Frequency	2,4 GHz ISM, 2,5-2,7 GHz licensed, 3,5 GHz lic., 5,8 GHz unlic., 10,5 GHz lic.
Spectrum use	public/licensed
MIMO	up to 4x4
Latency	50 ms

**Table 6-13 - 802.16 WiMAX characteristics**

#### 6.3.1.8 Z-Wave

Z-Wave is a wireless communications protocol used primarily for home automation. It is a mesh network using low-energy radio waves to communicate from appliance to appliance [26], allowing for wireless control of residential appliances and other devices, such as lighting control, security systems, thermostats, windows, locks, swimming pools and garage door openers. The Z-Wave standard is defined for short ranges around 100 m.

Typical data rate is 9, 6, 40 and 100 kbit/s. But this is highly different from the useful data rate (throughput) as it is expected that the nodes use the data transmission only at a fraction of the working time. Z-Wave works in the ISM band of 868 MHz (Europe), 915 MHz (US).

The transmission is secured with symmetrical 128 bit AES [27] cryptographic protocol which is fully sufficient for most types of time limited transmission sessions except full-time 24/7.

Up to 232 devices can be connected to the master node through the network. Each node may act as a repeater in the mesh network. Multi-hop transmission is available hence different types of networks can be set up: star, tree and mesh.

The Z-Wave protocol is freely available. Even open-source software implementations are publicly available.

Features	Description
Points	Static or slow moving
Nodes	Static
Type	Master/Client – Point to multipoint
Data rate	9,6/40/100 kbit/s
Average throughput	0,1 – 1 kbit/s
Range	20 m – 150 m (typically up to 100 m;)
Frequency	ISM band (868 MHz Europe, 908/916 MHz USA)
Spectrum use	public
MIMO	n.a.
Latency	typ. 200 ms (increases with nr. of hops/retransmissions)

**Table 6-14 - Z-Wave characteristics**

#### 6.3.1.9 TETRA

Terrestrial Trunked Radio (TETRA), is a European standard for a trunked radio system, is a professional mobile radio and two-way transceiver specification. TETRA was designed for use by government agencies, emergency services, for public safety networks, rail transport staff for train radios, transport services and the military. [39]



The TETRA standard [40] provides mobile stations with the means to support circuit mode calls and short data via the Circuit Mode Control Entity, and Internet Protocol (IP) packet data via the Subnetwork Dependent Convergence Protocol layer and the Multimedia Exchange layer.

TETRA uses Time Division Multiple Access (TDMA) with four user channels on one radio carrier and 25 kHz spacing between carriers [41]. Release 2 of the standard includes the TETRA Enhanced Data Service, which provides wideband data capabilities in the order of 30 to 260 kbit/s. TETRA supports point-to-point and point-to-multipoint communications both through the TETRA infrastructure.

TETRA standards presents the following benefits [42] to solve conventional problems:

- Automatic cell handover takes away the need for manual channel selection.
- Call requests are handled on the control channel for immediate call processing.
- Equal grade of service for all radio users on the system is ensured by automatic and dynamic assignment of a small number of communication channels.
- The dynamic and random allocation of channels solve lack of privacy issues.
- The much lower frequency used gives longer range, which in turn permits very high levels of geographic coverage with a smaller number of transmitters.
- TETRA also provides a point-to-point function that traditional analogue emergency services radio systems did not provide.

### **6.3.2 Mobile Cellular Networks**

The mobile Cellular Networks will be interesting for more advanced faces of the project. When the complete integrity and composition information should leave the train composition. As means of generating a connection with on ground premises.

This part has been taken and adapted from the different webpages of the entities generating the standards mentioned. In the following paragraphs, the Mobile Cellular Networks are characterized with emphasis on data transmission over voice transmission.

#### **6.3.2.1 Global System for Mobile Communications Railway**

GSM-R, Global System for Mobile Communications – Railway or GSM-Railway is an international wireless communications standard for railway communication and applications. The formal description states:

*“GSM-R stands for Global System for Mobile Communication for Railways and is based on the commercial system GSM. GSM is the most advanced and frequently used mobile telecommunication system in the world. GSM is standardized by ETSI, the European Telecom Standards Institute and well supported by the GSM Association Group, the association of the GSM suppliers.”*[48]

The frequency band allocated for GSM-R is limited to 4MHz. This means that 19 frequencies are available in most countries, providing a limited number of circuit switched traffic channels for voice or data transmission. The GSM-R system makes use of two different modulation techniques GPRS and EDGE. At the beginning only GPRS was used and it produced problems with the

bandwidth per channel (200kHz). With the introduction of EDGE, which is compatible with GPRS, the problem was solved.

The GSM-R system was not designed to give access to high bandwidth applications. It is a protocol designed and specified with the signalling and small data amounts in mind.

UIC decided in 2012 to set up the Future Rail Mobile Communications System (FRMCS) project to prepare the necessary steps towards the introduction of a successor or GSM-R. These first steps started with evaluation of the actual situation, included several studies on Users' needs and ended with the delivery of a first set of "User Requirements Specification" [49].

#### **6.3.2.2 Evolved High Speed Packet Access (HSPA, HSPA+)**

Evolved High Speed Packet Access, or HSPA+, or HSPA(Plus), or HSPAP is a technical standard for wireless, broadband telecommunication. It is the second phase of HSPA which has been introduced in 3GPP release 7 and being further improved in later 3GPP releases. HSPA+ can achieve data rates of up to 42.2 Mbit/s.

Further releases of the standard have introduced dual carrier operation, i.e. the simultaneous use of two 5 MHz carriers. The technology also delivers significant battery life improvements and dramatically quicker wake-from-idle time, delivering a true always-on connection.

HSPA+ is an evolution of HSPA that upgrades the existing 3G network and provides a method for telecom operators to migrate towards 4G speeds that are more comparable to the initially available speeds of newer LTE networks without deploying a new radio interface. HSPA+ should not be confused with LTE though, which uses an air interface based on Orthogonal frequency-division multiple access modulation and multiple access.

Advanced HSPA+ is a further evolution of HSPA+ and provides data rates up to 84.4 and 168 Megabits per second (Mbit/s) to the mobile device (downlink) and 22 Mbit/s from the mobile device (uplink) under ideal signal conditions. Technically these are achieved through the use of a multiple-antenna technique known as MIMO (for "multiple-input and multiple-output") and higher order modulation (64QAM) or combining multiple cells into one with a technique known as Dual-Cell HSDPA.

#### **6.3.2.3 High Speed Downlink Packet Access (HSDPA)**

High Speed Downlink Packet Access (HSDPA) is an enhanced 3G (third-generation) mobile communications protocol in the High-Speed Packet Access (HSPA) family, also dubbed 3.5G, 3G+, or Turbo 3G, which allows networks based on Universal Mobile Telecommunications System (UMTS) to have higher data speeds and capacity.

HSDPA has been introduced with 3GPP Release 5, which also accompanies an improvement on the uplink providing a new bearer of 384 kbit/s. The previous maximum bearer was 128 kbit/s. As well as improving data rates, HSDPA also decreases latency and so the round trip time for applications. HSPA+ introduced in 3GPP Release 7 further increases data rates by adding 64QAM modulation, MIMO and Dual-Cell HSDPA operation, i.e. two 5 MHz carriers are used

simultaneously. Even higher speeds of up to 337.5 Mbit/s are possible with Release 11 of the 3GPP standards.

The first phase of HSDPA has been specified in the 3GPP release 5. Phase one introduces new basic functions and is aimed to achieve peak data rates of 14.0 Mbit/s with significantly reduced latency. The improvement in speed and latency reduces the cost per bit and enhances support for high-performance packet data applications.

HSDPA is based on shared channel transmission and its key features are shared channel and multi-code transmission, higher-order modulation, short transmission time interval (TTI), fast link adaptation and scheduling along with fast hybrid automatic repeat request (HARQ).

Further new features are the High Speed Downlink Shared Channels (HS-DSCH), the adaptive modulation QPSK and 16QAM and the High Speed Medium Access protocol (MAC-hs) in base station.

The upgrade to HSDPA is often just a software update for WCDMA networks. In general voice calls are usually prioritized over data transfer.

#### **6.3.2.4 Long-Term Evolution (LTE)**

Long-Term Evolution (LTE) is a standard for high-speed wireless communication for mobile phones and data terminals, based on the GSM/EDGE and UMTS/HSPA technologies. It increases the capacity and speed using a different radio interface together with core network improvements. The standard is developed by the 3GPP (3rd Generation Partnership Project) and is specified in its Release 8 document series, with minor enhancements described in Release 9. LTE is the upgrade path for carriers with both GSM/UMTS networks and CDMA2000 networks. The different LTE frequencies and bands used in different countries mean that only multi-band phones are able to use LTE in all countries where it is supported [43].

LTE is commonly marketed as 4G LTE, but it does not meet the technical criteria of a 4G wireless service, as specified in the 3GPP Release 8 and 9 document series, for LTE Advanced. The requirements were originally set forth by the ITU-R organization in the IMT Advanced specification. However, due to marketing pressures and the significant advancements that WiMAX, Evolved High Speed Packet Access and LTE bring to the original 3G technologies, ITU later decided that LTE together with the aforementioned technologies can be called 4G technologies. The LTE Advanced standard formally satisfies the ITU-R requirements to be considered IMT-Advanced. To differentiate LTE Advanced and WiMAX-Advanced from current 4G technologies, ITU has defined them as "True 4G" [44].

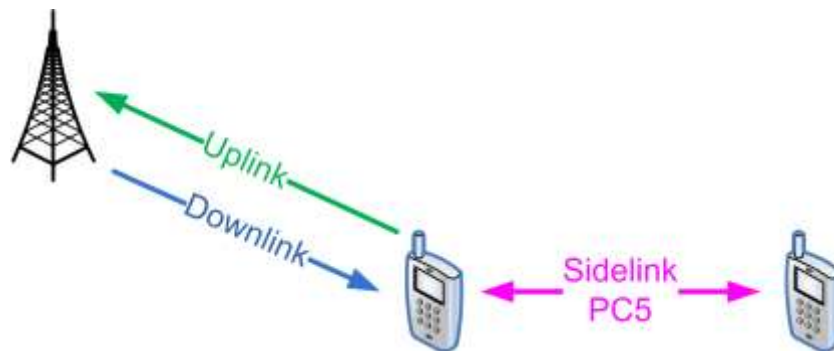
LTE offers throughput rates beyond 100 Mb/s and short latency of around 20 ms. To support this complex functionality, more intelligence must be built into the eNodeB than in its predecessor (3G NodeB). LTE applies the double concept of user-plane (user applications) and control-plane (network control traffic).

Following ITU, the peak data target of LTE is 15 b/s per Hz for downlink and 6,75 b/s per Hz for uplink. This can be realized with a deployment in 20 MHz bandwidth, and MIMO (8 x 8 in downlink, 4 x 4 in uplink).

Under simulation, an average cell throughput of roughly 3 b/s per Hz for downlink (4 x 2) and 2 b/s per Hz for uplink (1 x 4) has been obtained. These figures are almost the same with FDD and TDD modes, in a Rural Macro-cellular deployment supporting high speed [45].

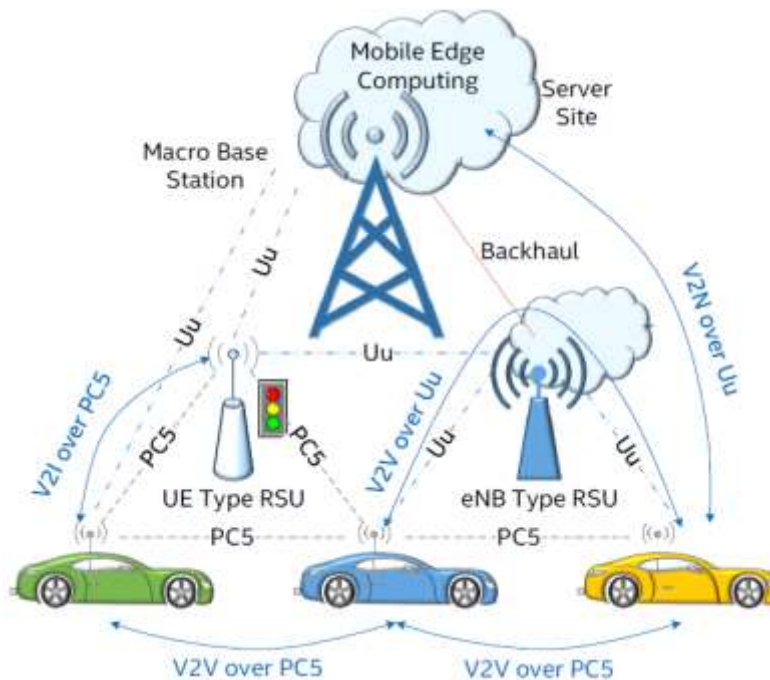
#### 6.3.2.4.1 *LTE-based direct device-to-device communications*

Cellular communications are traditionally based on the communication between the eNodeB and the User Equipment (UE). This communication is carried out over the Uu radio interface. The eNodeB communicates with the UE via the Uplink (UL) and Downlink (DL), for both, control signalling and data. Since the 3GPP release 12 a new radio interface is available in LTE, the Sidelink (SL) or PC5 interface (see Figure 6-40).



**Figure 6-40 - New PC5 interface**

This interface allows the direct communication between two UEs. Resources assigned to the SL are taken from the UL, i.e. from the subframes on the UL frequency in FDD or from the subframes assigned to UL in TDD. There are two reasons for this selection: First, the UL subframes are usually less occupied than those on the DL. In release 12, the PC5 interface was proposed for public safety, but the possibility to use this new interface was extended in release 14 in order to provide direct cellular vehicle-to-vehicle (C-V2V) for automation industry. This specification has been adopted also by ETSI TS 122 185 v14.3.0 within the vehicle-to-everything (V2X) communication framework based on cellular technology which is depicted in Figure 6-41.



Currently, the C-V2V covers basic communications between cars but it is foreseen to evolve this communications to act as a carrier for more demanding applications related to autonomous car driving. The current supported traffic type is a periodic (with a frequency of 100ms) traffic of 4x190bytes packets followed by 1x300 bytes. The minimal required latency, i.e. for pre-crash sensing communications is about 20ms. It is stated that the 3GPP system shall be capable of transferring messages between UEs supporting V2V application, while the maximum relative velocity of the UEs is 500 km/h, regardless of whether the UE(s) are served or not served by E-UTRAN supporting V2X communication. Additionally, according to the ETSI document for UE supporting V2X application with limited resources (e.g., battery), the impact on its resources (e.g., battery consumption) due to message transfer should be minimized.

Comparing to the IEEE 802.11p presented in section 6.3.1.4.3 the V2V based on cellular technology provides better radio resource management [44], which results in higher availability and reliability as each UE has an allocated resource pool and does not compete for the channel producing constant collisions in busy environments. This resource management can be done in two resource allocation modes:

- Mode 3: eNodeB-controlled mode. The eNB schedules vehicle transmission on sidelink resources.
- Mode 4: UE-autonomous mode. The UE selects resource for transmission in pre-configured sidelink resource pool(s) using sensing and resource selection procedure.

The C-V2V communication specification is expected to be evolved in the upcoming 3GPP release 16 and will be also included in the new radio access technology to be adopted by 5G. Figure 6-42 summarizes the C-V2X evolution roadmap.

Q3' 15	Q4' 15	Q1' 16	Q2' 16	Q3' 16	Q4' 16	Q1' 17	Q2' 17	Q3' 17	Q4' 17	Q1' 18	Q2' 18	Q3' 18	Q4' 18	Q1' 19	Q2' 19	Q3' 19	Q4' 19
C-V2X Phase 1 LTE R13 Study Item				Study of radio-layer design components, to enhance LTE technology for efficient support of day one V2X services													
Focus on sidelink work		C-V2X Phase 1 LTE R14 Work Item		The 1 <sup>st</sup> generation of C-V2X system. Sensing and resource selection procedures. Sidelink physical structure and resource allocation. Sidelink synchronization													
Focus on the enhancements			C-V2X Phase 1 LTE R14 Work Item			The 1 <sup>st</sup> generation of C-V2X system. Enhancements of the air-interface targeting V2X use cases. Partial sensing and support of pedestrian UEs.											
Evolution of LTE-V2X technology to further improve its performance and enable additional use cases						C-V2X Phase 2: LTE R15 Work Item						Support of up to 8 sidelink CCs; 64QAM; Transmit diversity; Latency reduction					
Study of design principles to support evolved V2X (eV2X) use cases is expected in 2018/2019 focusing on NR radio access technology followed by design normative work												C-V2X Phase 3 (eV2X Use Cases) NR/LTE V2X Study Item					

**Figure 6-42 - C-V2X evolution roadmap [67]**

In the C-V2V phase 2 a latency reduction is targeted to values lower than 20ms. Additionally, a sidelink relaying feature is expected to be included allowing higher communication range.

#### 6.3.2.4.2 Frequency bands

The LTE standard covers a range of many different bands, each of which is designated by both a frequency and a band number.

- in Europe 700, 800, 900, 1800, 2600 MHz (bands 3, 7, 20) are used;
- In North America, 700, 750, 800, 850, 1900, 1700/2100 (AWS), 2300 (WCS) 2500 and 2600 MHz (Rogers Communications, Bell Canada) are used (bands 2, 4, 5, 7, 12, 13, 17, 25, 26, 30, 41);
- 2500 MHz in South America;
- 800, 1800 and 2600 MHz in Asia (bands 1, 3, 5, 7, 8, 11, 13, 40)
- 1800 MHz and 2300 MHz in Australia and New Zealand (bands 3, 40).

### 6.3.3 IoT Wide-Area Networks

Internet-of-Things (IoT) WANs are a specific branch of WANs, usually called LPWANs – Low-Power WANs, which are focused on providing services to thousands up to millions of low-power devices in order to ensure their data connection to monitoring and control centres. The specificity of those networks lie in the characteristics that the data primarily travel wirelessly from the “Thing” over the internet via IP protocol to a centrally located devices (monitoring servers or controllers). Therefore, typically the uplink transfer is the major direction of data transport and downlink bandwidth is either limited or even impossible.

This is in high contrast to other internet and data/voice transmission technologies which provide either balanced/symmetrical bandwidth or higher bandwidth in the downlink direction.

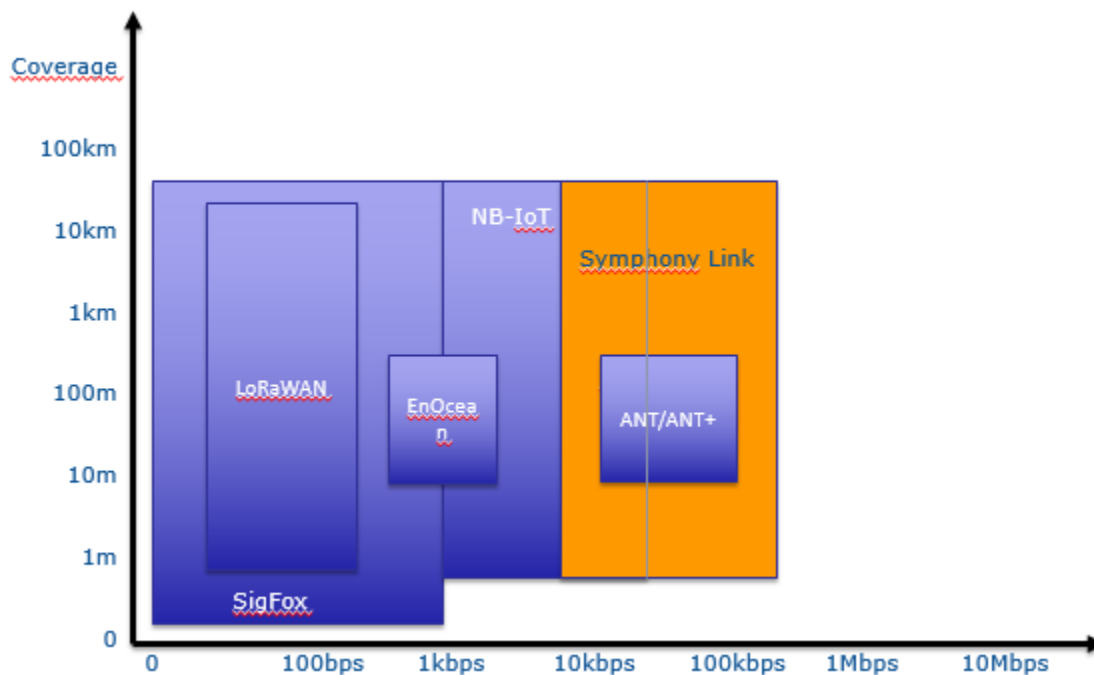


Figure 6-43: IoT Wide Area Networks

#### 6.3.3.1 ANT/ANT+

ANT is a proprietary (but open access) multicast wireless sensor network technology designed and marketed by ANT Wireless. It defines a wireless communications protocol stack that enables hardware operating in the 2.4 GHz ISM band to communicate by establishing standard rules for co-existence, data representation, signaling, authentication, and error detection [28]. ANT-powered nodes are capable of acting as slaves or masters within a wireless sensor network concurrently. This means the nodes can act as transmitters, receivers, or transceivers to route traffic to other nodes. In addition, every node is capable of determining when to transmit based on the activity of its neighbors. [26]

ANT can be configured to spend long periods in a low-power “sleep” mode (consuming of the order of microamps of current), wake up briefly to communicate (when consumption rises to a peak of 22mA (at -5dB) during reception and 13.5mA (at -5 dB) during transmission) and return to sleep mode. [29]

Each ANT channel consists of one or more transmitting nodes and one or more receiving nodes, depending on the network topology. Any node can transmit or receive, so the channels are bi-directional. [30]

Acknowledged messaging confirms receipt of data packets. The transmitter is informed of success or failure, although there are no retransmissions. This technique is suited to control applications. [31]

ANT+ is an interoperability function that can be added to the base ANT protocol. This standardization allows for the networking of nearby ANT+ devices to facilitate the open collection

and interpretation of sensor data. For example, ANT+ enabled fitness monitoring devices such as heart rate monitors, pedometers, speed monitors, and weight scales can all work together to assemble and track performance metrics.

Features	Description
Points	Static or slow moving
Nodes	Static
Type	Master/Client – Point to multipoint
Data rate	12.8 kbit/s for Broadcast/ACK 20 kbit/s for Burst 60 kbit/s for Advanced Burst
Average throughput	0.5 Hz to 200 Hz (8 bytes data)
Range	30 m – 100 m
Frequency	2,4 GHz band, ISM band
Spectrum use	public
MIMO	n.a.
Latency	? ms

**Table 6-15 – ANT characteristics**

### 6.3.3.2 NarrowBand IoT (NB-IoT)

This part has been taken and compiled from Radio-Electronics.com. NB-IoT is a narrowband radio technology designed for the Internet of Things (IoT), and is one of a range of Mobile IoT (MIoT) technologies standardized by the 3rd Generation Partnership Project (3GPP). [32]

NB-IoT is a new 3GPP radio-access technology in the sense that it is not fully backward compatible with existing 3GPP devices. It is however designed to achieve excellent co-existence performance with legacy GSM, General Packet Radio Service (GPRS) and LTE technologies. NB-IoT requires 180 kHz minimum system bandwidth for both downlink and uplink, respectively.

NB-IoT reuses the LTE design extensively [33], including the numerologies, downlink orthogonal frequency-division multiple-access (OFDMA), uplink single-carrier frequency-division multiple-



access (SC-FDMA), channel coding, rate matching, interleaving, etc. In addition, it is expected that the time required for developing NB-IoT products will be significantly reduced for existing LTE equipment and software vendors. The core specifications for NB-IoT were completed in June 2016. [34]

NB-IoT focuses specifically on indoor coverage, low cost, long battery life, and enabling a large number of connected devices. NB-IoT targets latency insensitive applications. However, for applications like sending alarm signals, NB-IoT is designed to allow less than 10 s latency. The NB-IoT technology can either be deployed “in-band” in spectrum allocated to Long Term Evolution (LTE) - utilizing resource blocks within a normal LTE carrier, or in the unused resource blocks within a LTE carrier’s guard-band - or “standalone” for deployments in dedicated spectrum. It is also suitable for the re-farming of GSM spectrum.

Features	Description
Points	Static
Nodes	Static
Type	Master/Client – Point to multipoint
Data rate	250 kbit/s downlink, 20 – 250 kbit/s uplink
Average throughput	1 – 50 kbit/s
Range	above 10 km
Frequency	GSM/LTE bands
Spectrum use	licensed
MIMO	n.a.
Latency	typ. 1,6 – 10 s

**Table 6-16 – NB-IoT**

### 6.3.3.3 LoRaWAN

This part has been taken and compiled from Radio-Electronics.com, LoRa Alliance web pages and Link Labs white papers. LoRaWAN is a Low Power Wide Area Network with features that

support low-cost, mobile, and secure bi-directional communication for Internet of Things (IoT), machine-to-machine (M2M), and smart city, and industrial applications. LoRaWAN is optimized for low power consumption and is designed to support large networks with millions and millions of devices. Innovative features of LoRaWAN include support for redundant operation, geolocation, low-cost, and low-power – devices [35] can even run on energy harvesting technologies enabling the mobility and ease of use of Internet of Things. The frequency band used is ISM which is 868 MHz for Europe and 900-916 MHz for USA.

It is the low power, wide-area network (LPWAN) global standard for carrier-operated networks, adopted by the LoRa Alliance.

LoRaWAN network architecture is typically laid out in a star-of-stars topology in which gateways is a transparent bridge relaying messages between end-devices and a central network server in the backend. Gateways are connected to the network server via standard IP connections while end-devices use single-hop wireless communication to one or many gateways. All end-point communication is generally bi-directional, but also supports operation such as multicast enabling software upgrade over the air or other mass distribution messages to reduce the on air communication time.

Communication between end-devices and gateways is spread out on different frequency channels and data rates. The selection of the data rate is a trade-off between communication range and message duration. Due to the spread spectrum technology [36], communications with different data rates do not interfere with each other and create a set of "virtual" channels increasing the capacity of the gateway. LoRaWAN data rates range from 0.3 kbps to 50 kbps. To maximize both battery life of the end-devices and overall network capacity, the LoRaWAN network server is managing the data rate and RF output for each end-device individually by means of an adaptive data rate (ADR) scheme.

National wide networks targeting internet of things such as critical infrastructure, confidential personal data or critical functions for the society has a special need for secure communication. Several layers of encryption have solved this:

- Unique Network key (EUI64) ensure security on network level
- Unique Application key (EUI64) ensure end to end security on application level
- Device specific key (EUI128)

One of the big headache of LoRaWAN is complicated management of multiple per-device encryption keys both at the time of device production and on the server side.

ETSI specification imposes a 1 % duty cycle limit on the communication between end-devices and the gateway which limits the possibility to transfer larger data volumes. The protocol is asynchronous hence it doesn't support full acknowledgement of packet delivery so the packet losses may be significant.

The LoRaWAN Specification document describes the LoRaWAN™ network protocol including MAC layer commands, frame content, security, flexible network frequency management, device

EIRP and TX dwell time, power control, relay protection and more. Because LoRaWAN encrypts all traffic up and down on a one-to-one basis, implementing multicast transmissions is quite difficult. Operating a LoRaWAN network requires a paid license at the level of tens of KEUR annually. Hence operating it either autonomously or using some other's network considerably increases OPEX.

Features	Description
Points	Static
Nodes	Static
Type	Master/Client – Point to multipoint
Data rate	0.3 – 50 kbit/s uplink
Average throughput	3 – 500 bit/s
Range	up to 20 km
Frequency	ISM band (868 MHz Europe, 908/916 MHz USA)
Spectrum use	unlicensed
MIMO	n.a.
Latency	typ. 4 – 120 s

**Table 6-17 – LoRaWAN**

#### 6.3.3.4 UNB/Sigfox

This part has been taken and compiled from Radio-Electronics.com and SigFox company web pages. SigFox is a narrowband (or ultra-narrowband – UNB) technology. It uses a standard radio transmission method called binary phase-shift keying (BPSK), and it takes very narrow chunks of spectrum and changes the phase of the carrier radio wave to encode the data. This allows the receiver to only listen in a tiny slice of spectrum which mitigates the effect of noise. It requires an inexpensive endpoint radio and a more sophisticated basestation to manage the network.

Available data throughput is:

- Up to 140 messages per object per day

- Payload size for each message is 12 bytes
- Wireless throughput up to 100 bits per second

Sigfox uses BPSK, and it takes very narrow chunks of spectrum and changes the phase of the carrier radio wave to encode the data. The BPSK modulation allows for very narrow band usage but it also limits the percentage of time the end-point is transmitting. The network is based on one-hop star topology and requires a mobile operator to carry the generated traffic [37].

Features	Description
Points	Static
Nodes	Static
Type	Master/Client – Point to multipoint
Data rate	0,1 – 1 kbit/s uplink
Average throughput	10 – 100 bit/s (with additional limit on the number of transactions per day)
Range	50 km
Frequency	ISM band (868 MHz Europe, 908/916 MHz USA)
Spectrum use	licensed
MIMO	n.a.
Latency	typ. 1,6 – 10 s

**Table 6-18 – SigFox**

#### 6.3.3.5 Symphony Link

Symphony Link is a communication technology based on LoRa specifications but removes many various limitations. It is built on LoRa CSS physical layer technology [38]. It is a synchronous protocol allowing full acknowledgment of packet delivery which enables very low packet loss and, in addition, deploying repeaters which highly expand the range without increasing latency.

Repeaters are low-cost, low-power devices which brings higher range to users without adding major cost.

Symphony Link adds a QoS tiering system, which enables to prioritize traffic for important devices. While LoRaWAN security flaws [38] pose a small risk for most users, the use of pre-shaped keys and identities create vulnerabilities. Symphony Link uses PKI which is considered unbreakable by NSA. With Symphony Link the host device configuration is always the same for all devices of the same type and the key exchange is handled via a PKI-based AES architecture.

Features	Description
Points	Static
Nodes	Static
Type	Master/Client – Point to multipoint
Data rate	10 – 250 kbit/s uplink
Average throughput	0.1 – 50 kbit/s
Range	up to 50 km
Frequency	ISM band (868 MHz Europe, 908/916 MHz USA)
Spectrum use	unlicensed
MIMO	n.a.
Latency	typ. 100 ms – 120 s

**Table 6-19 – Symphony Link**

#### 6.3.3.6 EnOcean

This part has been taken and compiled from EnOcean company web pages, the ITU standard and Radio-Electronics.com. EnOcean technology combines energetically efficient exploitation of the principles of energy harvesting in order to produce usable electrical energy

The radio signals from these sensors and switches can be transmitted wirelessly over a distance of up to 300 meters in the open and up to 30 meters inside buildings.

EnOcean wireless data packets are relatively small, with the packet being only 14 bytes long and are transmitted at 125 kbit/s. RF energy is only transmitted for the 1's of the binary data, reducing the amount of power required. Three packets are sent at pseudo-random intervals reducing the possibility of RF packet collisions. Modules optimized for switching applications transmit additional data packets on release of push-button switches, enabling other features such as light dimming to be implemented. The transmission frequencies used for the devices are 902 MHz, 928.35 MHz, 868.3 MHz and 315 MHz.

A group of companies including EnOcean, Texas Instruments, Omnio, Sylvania, Masco, and MK Electric formed the EnOcean Alliance in April 2008 as a non-profit, mutual benefit corporation. The EnOcean Alliance has drawn up the application level protocols are referred to as EEPs (EnOcean Equipment Profiles).

The international wireless standard ISO/IEC 14543-3-10 and the Alliance's EEP lay the foundation for a fully interoperable, open wireless technology. More than 250 companies currently belong to the EnOcean Alliance. For applying the complete specification license fees have to be paid to the Alliance, unless the supplier develops a solution from scratch based on the public standard. But interoperability with COTS products cannot be achieved this way.

First 3 layers of the ISO/OSI model are defined in the standard.

There are several key aspects for the physical layer:

- GFSK modulation: The EnOcean radio interface uses a form of modulation known as GFSK: Gaussian Frequency Shift Keying. Frequency Shift Keying is a form of frequency modulation where the signal frequency is changed between two frequencies dependent upon the modulation. In the case of the EnOcean radio signal the shift is  $\pm 62.5$  kHz of the central carrier position. The +62.5 kHz position is for the code used to indicate logical "1" and the -62.5 kHz position is the code used to indicate a logical "0".
- The EnOcean standard allows for the use of different GFSK filter parameters dependent upon the required national regulation requirements.
- EnOcean Frequencies: The EnOcean radio interface specification states that the system can operate within a variety of ISM bands. However the individual frequencies are specified for which the system is to be used are specified within the standard. Currently two frequencies are specified: 902.875 MHz which is aimed at the North American market and 928.35 MHz which is aimed at the Japanese market. The standard states that the aim of the specification is to be frequency independent and therefore additional frequencies may be introduced as new markets or requirements arise.
- EnOcean Frame: Data to be transmitted is assembled into frames. This enables synchronisation, and the correct reception of the data, etc. Payload can range from 1 byte to 255 bytes.

Features	Description
Points	Static
Nodes	Static
Type	Master/Client – Point to multipoint
Data rate	125 kbit/s in the ISM band,
Average throughput	0.5 – 1.5 kbit/s
Range	30 m – 100 m indoor (up to 300 m outdoor)
Frequency	ISM band (868 MHz Europe, 908/916 MHz USA)
Spectrum use	public
MIMO	n.a.
Latency	typ. 30 ms

**Table 6-20 – EnOcean characteristics**

### 6.3.4 Satellite technologies and services

This chapter has been taken over and adapted from the NGTC project. The Satellite communications will be interesting for more advanced faces of the project. When the complete integrity and composition information should leave the train composition. As means of generating a connection with on ground premises. On the other hand, the geopositioning systems (GPS, Galileo ...) could be useful in first iterations of this project.

Technically Satellite communications are mainly classified according to one of three major ways of the satellites orbit above the Earth:

- Geosynchronous Orbit (GEO) which is 35 786 km from the Earth's surface. This connection produces a propagation Delay: 250-300 ms for a single hop, from Earth to Earth.
- Medium Earth Orbit (MEO) that ranges from 10 000 to 15 000 Km above the Earth. This connection produces a propagation Delay: 110-130 ms for a single hop.
- Low Earth orbit (LEO) that ranges from 700 to 1 400 Km above the Earth. This connection produces a propagation Delay: 20-25 ms.

These coverage characteristics have a big relevance in case of railway application. In particular, considering GEO, a drawback is a large link budget (near 200 dB), but many advantages are consequent:

- the link is not subjected to handover;
- the elevation angle is high, then the pointing of the antenna requires
  - minor adjustments, even in mobility,
  - minor mechanical problems for its assembly and for its life duration.

In case of GEO, the simplification does not stop to the antenna steering mechanism but involves also the mobile terminal that requires lower cost. This is valid also for fixed terminal and point-to-point connections are possible via a LES (Land Earth Station).

Considering the following SATCOM frequencies and their present allocation:

- L-band (1-2 GHz) is allocated for Mobile Satellite Services
- C-band (4-8 GHz) for Fixed Satellite Services
- X-band (8-12 GHz) for Military/Governmental (Fixed and Mobile services)
- Ku-band (12-18 GHz) for Fixed and Broadcast Satellite Services
- Ka-band (26-40 GHz) for Fixed and Mobile Satellite Services and Military/Governmental.

#### 6.3.4.1 **GEO L-band satellite services application for Railway Signalling**

Concerning already existing application of GEO satellite based communication, it is worth to mention the **“Train Integrated Safety Satellite System (3InSat) Demonstration project”**, funded by ESA in the ARTES 20 IAP programme,

One of the most relevant 3InSat objective was the new TLC paradigm introduced, consisting in a multi-bearer approach that uses a combination of existing public mobile networks (2G/3G) with satellite communication, in alternative to GSM-R based TLC network.

From the throughput point of view, a single BGAN terminal provides simultaneous voice and broadband data up to 492 kb/s, enabling simultaneous voice and data. In particular, BGAN supports a range of guaranteed on-demand streaming IP rates from 32 kb/s to at least 384 kb/s, and up to 450 kb/s with BGAN X-Stream™. The last one special streaming service could be helpful to avoid video or audio drop outs.

In the on-board side of 3InSat, the satellite BGAN terminal was connected to a steerable L-Band antenna on the roof of a train, travelling along a real operational railway line, and providing radio access to the forward and reverse link of the satellite.

Tests were performed on the RFI lines in Sardinia connecting Cagliari and Olbia (about 300 km) and with a speed up to 130 km/h. Two trips per day each lasting 3h 50m each way, have been performed for all the duration of the test campaign to get a significant set of experimental data.

#### 6.3.4.2 **IRIDIUM**

IRIDIUM is working for its upcoming constellation, Iridium NEXT. Thales Alenia Space has completed the Main Mission Antennas (MMAs), for which one goes on each NEXT satellite. On



2014, Iridium selected Radisys' T-Series Commercial Off-The-Shelf (COTS) platforms to upgrade the ground station infrastructure for NEXT, and support the so-called Certus service. The constellation provides L-band data speeds of up to 1.5 Mbit/s and High-speed Ka-Band service of up to 8 Mbit/s.

### 6.3.5 Available Wireless Sensors

This section is intended to provide a wide range perspective of the available kind of sensors, which could be developed or found in the market to provide train integrity features. The information, in this section, was adapted from the technology used in the DEWI project. [47]

The composition of the wireless sensor networks is:

- **Wireless nodes:** elements that send wirelessly and periodically the information measured from the sensors (connected to or integrated in them) to the network coordinator (integrity, waggon length, waggon weight, etc.).
- **Coordinator:** element that gathers up the information of the different sensors in order to send it to the On-board Central Unit.

The technology present must be transparent with the algorithms deployed to implement the train integrity functionalities. Therefore, a description of the different wireless sensors possibilities is provided.

Most of the Wireless sensor networks will make use of some of the sensors in section 6.1.5 Wireless Sensor Network (WSN). All of these sensorizations will give information on the distance between adjoining nodes or waggons.

In this section an analysis on how the OTI system could make use of these sensors will be given. There are two main ways to analyse:

1. Single sensor wireless nodes
2. Sensor combination wireless nodes

#### 6.3.5.1 Single sensor wireless nodes

The use of a single sensor wireless node has many advantages that may at first encourage at first the user to choose this option. The nodes energy consumption and price is reduced to the bare minimum of the communication system and the sensor. This is a great characteristic for devices being maintained on energy harvesting subsystems.

When this solution is analyzed further presents many disadvantages.

- **Safety:** The solution does not present high availability through subsystem redundancy. This could make the SIL4 certification more difficult to get.
- **Resistance to environmental conditions:** One sensor will always be affected by some kind of external condition rendering the system useless.
- **The results in single sensor nodes raised many alarms.** In average 17/4500 alarms for the DEWI demonstrator. The single sensor probability of error is  $P_e = 0.003753$ .

These disadvantages make this solution only applicable to very specific situations.

### 6.3.5.2 Combination wireless nodes

A candidate to provide integrity through location features could be provided by the combination of three different kind of measurements reported by three different kind of systems. Each of the systems will report the integrity data. If one of the systems reports the absence of integrity, an integrity alarm will be raised. However, only when two or more systems report the loss of integrity an alarm will be raised. This will follow the safety voting mechanisms. Consequently, this implementation provides a graduate state of alarm of the integrity.

An example of systems to tackle the integrity issue through location could be an accelerometer, a GNSS system, and the RSSI between several nodes. This could provide a low cost, low power multipurpose solution.

A combined solution for train integrity based on position and RSSI was studied in the DEWI project. The demonstrator run for over three hours on a real train after having passed many hours of laboratory testing. This system used a voting system and only when two of the three sensors raised a loss of integrity alarm a system alarm was raised. The sensors had the following specifications:

- GPS:
  - Velocity error < 1-3km/h
  - Position error < 2.5m
- Accelerometer:
  - Total error < 1mg

The demonstrator on a real train on the Gulbene-Alūksne railway threw the following false positive detections:

	ACC warnings	GPS warnings	RSSI warnings	Alarms
<b>Node 1</b>	6/4500	0/4500	0/4500	0
<b>Node 2</b>	27/4500	29/4500	6/4500	0
<b>Node 3</b>	72/4500	3/4500	9/4500	0

Table 6-21: Results in Gulbene-Alūksne railway testing

As shown on the table during the 3 hours of the test no loss of train integrity alarm was raised. When the error is calculated for the combination the probability of error decreases to  $P_e < 0.74 \cdot 10^{-4}$ .

### 6.3.5.3 Train composition extra parameters

From the ERTMS specification the following trigger can be found for starting the Train Integrity calculation:

(train is at standstill) AND (in SB/FS/LS/SR/OS/PT mode) AND (Driver ID is valid) AND (Train data are valid) AND (ERTMS/ETCS level is valid)

From this we can follow with the definition of the report of train rear end position for level 3 ERTMS according to SUBSET 026 [1]:

3.6.5.2.4 The safe train length information shall represent the distance between the min safe rear end (by subtracting the train length from the min. safe front end position at the time when integrity was established last time) and the estimated position of the train front.

3.6.5.2.5 The safe train length information shall be re-calculated for every position report using the same last value of min safe rear end position until a new min safe rear end position is established on-board taking into account the time to detect train integrity.

To be able to provide this information and supposedly knowing the location of the head of the train, the end of train location could be easily determined. Two different ways of determining the train length should be analysed:

- Direct head to tail measurement through radio link power: This analysis was further performed during the investigation on “WSN based on accelerometer, GPS and RSSI measurements for train integrity monitoring” in this paper different sensors are analysed and there is a specific one covering this point.

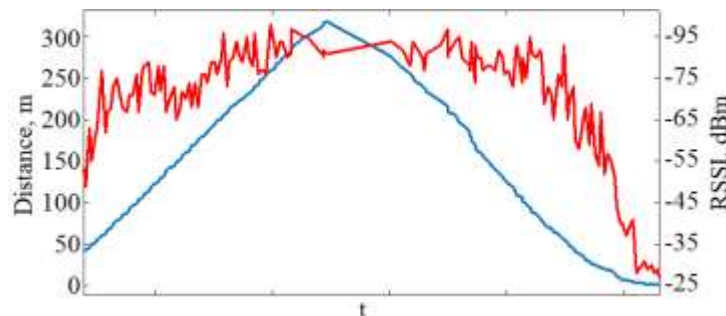


Figure 6-44 – Distance relation to RSSI measurement. The red line represents RSSI measurements, but the blue line the distance between the Coordinator and the WSN node.

This shows that the RSSI measurement have strong indication at short ranges diverging more and more from the real distance when this increases.

- Waggon length addition: As a different approach, the addition of the waggons lengths will total in the train length. If a Wireless Sensor Node is deployed in every waggon, and this node contains the Waggon length, it can be transmitted to the head of the train to calculate and report of train rear end position.

For this, every node should store certain information about the waggon that is mounted on. This information should include as a minimum the waggon length. For a more precise train length the following information should be included:

- Waggon length
- Waggon ID: For identifying possible duplication on the information
- Waggon weight: for braking capability calculation purposes

- Load weight: for braking capability calculation purposes
- Braking power: To be able to adjust the braking curve of the train

This data and the head of train location provided by any other ERTMS subsystem the train rear end position could be calculated. This will enable the report of train rear end position.

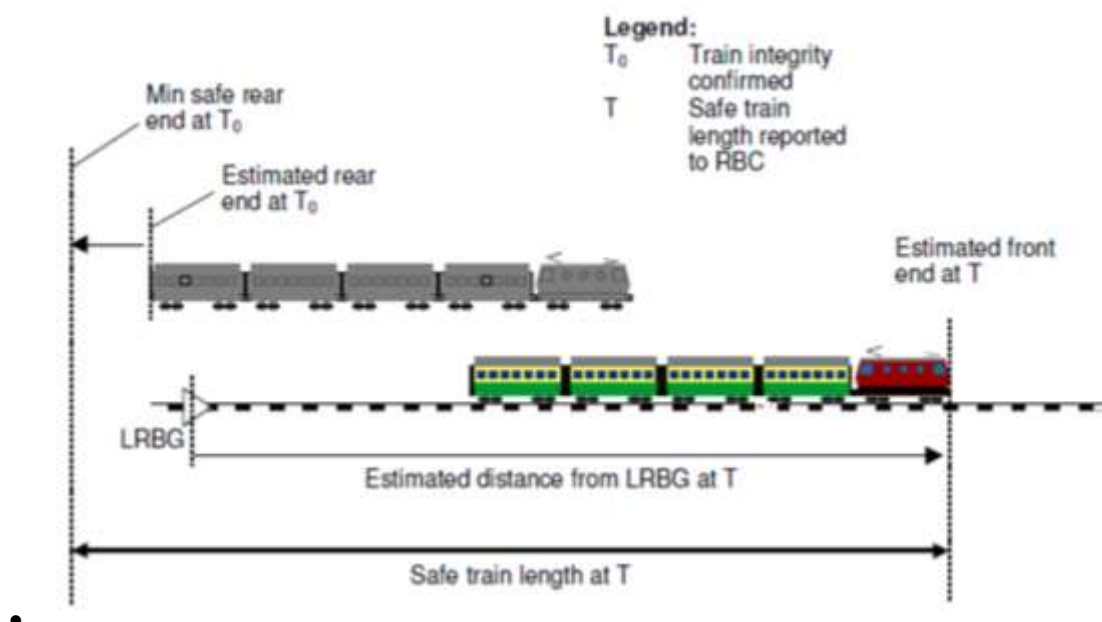


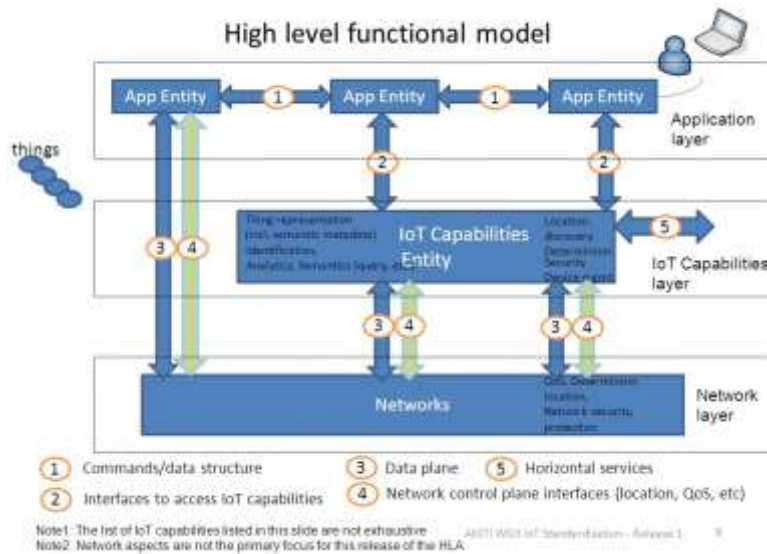
Figure 6-45 – Calculation of Safe Train Length when train integrity was established

### 6.3.6 Transponder Technologies

From the expertise acquired by INDRA, as partner and main leader of the rail domain in the DEWI project and SCOTT project, this section has been produced. Furthermore, S2R projects FR8RAIL and INNOWAG has been used to provide information about transponder technologies in the freight market.

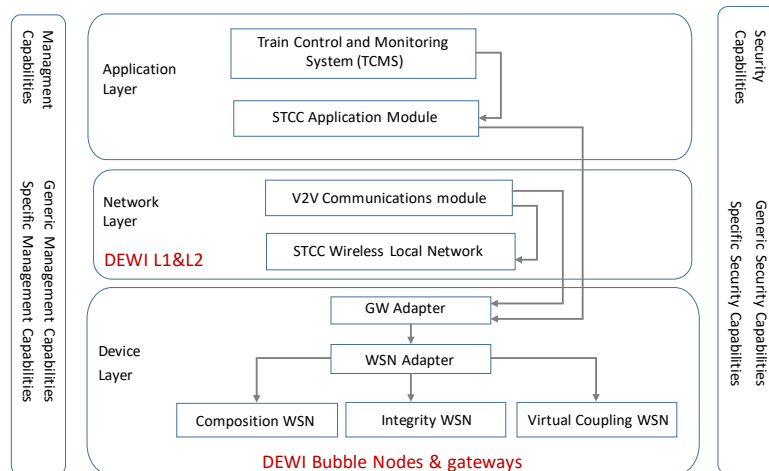
The transponder technologies are not understandable without a good comprehension of the architectures that make use of transponders and ad-hoc networks. This architectures mainly describe distributed and IoT solutions.

As the main entity defining IoT architectures and standardization in Europe the main architecture used is the HLA from AIOTI. On the following figure, the High Level Functional Model from the AIOTI is shown. [56]:



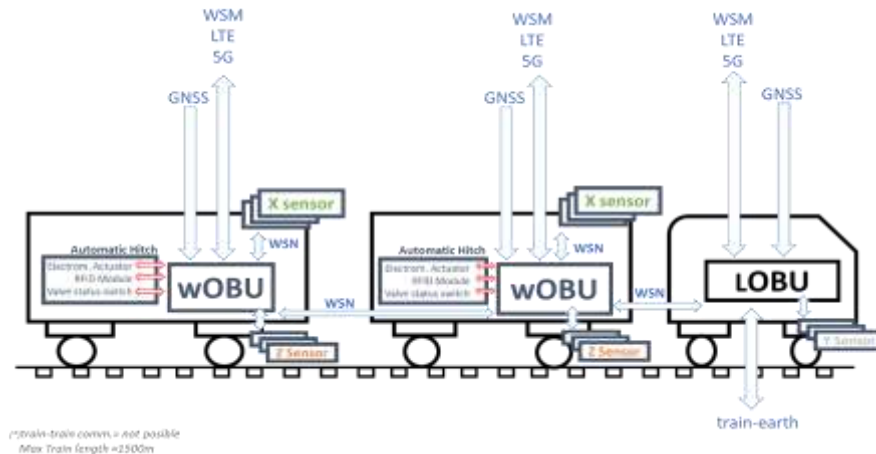
**Figure 6-46 - High Level Architecture AIOTI**

The SCOTT Project makes use of an architecture based on the AOITI architecture. In this project, a transponder for the rail domain has been defined in the way of a Gateway. For the scope of this project, the on-board Gateway for Smart Train Coupling described in the deliverable D19.1 [57] will be the most interesting. This gateway follows the following architecture for delivering a high safety level transponder for rail domain:



**Figure 6-47 - STCC GW architecture**

This architecture has been used in a similar fashion in the S2R consortium in the FR8RAIL project as a part of the WP3 Telematics and Electrification wireless on-board Unit (wOBU). [58]



**Figure 6-48 - wOBU proposed architecture**

A common point among all this architectures is the separation between the WSN/IoT layer, the communication layer and the application layers. In this case, the transponder will be part of the communications layer. A transponder will act as the wire in a wireless environment. In the DEWI project, the Gateway will be the transponder acting as a bridge between waggons.

The INNOWAG project [59] presents the integration of an RFID tag and reader in a sensor network to provide passive/semi-active wireless V2I communication. The tag operates as a passive RFID transponder when RF power is sufficient to operation. In this mode, if RF power is higher than battery voltage, the battery can be charged.

Otherwise, when the tag receives commands from readers but the RF power is not sufficient, the tag operates in the semi-active mode. For longer ranges or more complex data transmissions, the active transponders could have their own power supply in the form of a battery.

Many different frequency ranges are available for the data transmission. Table 18 shows some typical frequencies (SBB Cargo, 2013).

Frequency	Application	Feature
< 135 Hz	Low cost/low speed: Animal identification	<ul style="list-style-type: none"> <li>Short range</li> </ul>
6,78 MHz	Medium Speed: Goods identification	<ul style="list-style-type: none"> <li>ISM radio bands</li> <li>Relative High performance</li> </ul>
13.56 MHz	High speed (100 kBit/s): Goods identification	<ul style="list-style-type: none"> <li>ISM radio bands</li> <li>Longer range</li> </ul>
27.125 MHz	High speed (100 kBit/s):	<ul style="list-style-type: none"> <li>Short range</li> </ul>

	Special application	<ul style="list-style-type: none"> <li>• Lower performance than 13.56 MHz</li> </ul>
860-930 MHz	Goods identification with Electronic Product Code	<ul style="list-style-type: none"> <li>• ISM radio bands</li> <li>• Long range</li> </ul>

**Table 6-22 - Typical frequencies for transponder systems (SBB Cargo, 2013)**

### 6.3.7 Conclusions

This section is divided into three areas: wireless communication technologies, wireless sensors and transponder, all will be explained in this section.

First, the wireless communication technologies will be analyzed.

The status of the Freight Railway, the low density of certain Freight lines and corridors, reduces the possibility of cellular networks to be installed due to the economic impact. These constraints for the use of cellular networks in Freight environments do not limit its use on high speed lines or mainlines.

As shown on the corresponding section (6.3.2.4.1), the new cellular technologies (5G and above) provide the tools needed for connecting point-to-point.

Satellite communications, besides the great added latency to the communication system, have the problem with the shaded areas. In certain countries, like Switzerland, the use of satellite communications is nearly impossible due to the mountains and tunnels surrounding the lines and corridors. Several trials, studies and demonstrators have been carried out. From these studies, no conclusive results were obtained. Satellite communication systems may be useful in certain countries or areas and they may be considered as a very suitable communication mean.

The low cost of deployment of the receiver devices makes satellite technologies very competitive. This fact in combination with terrestrial technologies as TETRA (or others) to cover the shaded areas, results in a very good combination of technologies solution.

Two cases may be extracted from the previously exposed facts:

1. **Waggon-to-waggon communication:** This case implies the use of technologies designed to use point-to-point connections, within a mobile environment but in a short range. In this case the most suitable protocols are 802.11p, 6LoWPAN, and ANT/ANT+.
2. **V2I/I2V communication:** In this case, the use of technologies that allow the use of point-to-multipoint and broadcasting capabilities shall be considered. In this case, the most suitable protocol is WiMAX Release 2. This protocol covers big ranges, massive data rates and slow-moving systems. The protocol has the support of a major player that is IEEE. This point will provide trustworthiness and a level of security for the solution. The installation costs can be reduced below the cost of a cellular network. Although WiMAX is a good solution in terms of cost and features, it is becoming obsolete due to its lack of support from big companies. The future deployments are pointing towards the use of trendy technologies, as LTE release 14 and 15 or 5G. 5G technologies are not considered

in this study because they are still in a very early stage of specification for critical communications. However, the adoption of these technologies for both, waggon-to-waggon and V2I communications would allow a cellular system ubiquity using for both communications the same system, therefore simplifying the system. Another drawback would be the higher number of 5G devices, More radio links will be required in order to maintain the coverage because 5G uses higher frequencies.

These protocols offer good data rates, in short to medium distances among all kinds of devices. The consistency and the infrastructure independency provide them with enough tools to give a high level of security. With the low installation and buying costs, implementing them prove that these protocols are well suited.

In short, we must consider two different solutions for the two different cases. IoT (6LoWPAN, ANT/ANT+) or V2V (802.11p / LTE V2V) protocols for internal rail cases (OBU). WiMAX, TETRA and LTE technologies to be considered for medium and high railway deployments.

Once the wireless communication technologies candidates are chosen, the wireless sensors must be analysed.

In sections 6.3.5.1 and 6.3.5.2 a detailed analysis of possible Wireless sensor configurations was performed. This analysis is described in section 6.1.5 Wireless Sensor Network (WSN) where also the sensors composing the possible configurations are presented.

For this conclusions, INDRA gathered the knowledge obtained as leading partner of the rail domain in DEWI and SCOTT projects. The results are presented in sections 6.1.2 DEWI Project and 6.1.4 SCOTT Project.

A demonstrator was created and the results presented in 6.3.5.2 Combination wireless nodes. were extracted. From these results and the corresponding analysis, a clear conclusion can be extracted: the combination of multiple sensors is beneficial in most of the cases. The combination of sensors is in almost all cases better than the deployment of single sensor nodes.

The combination of multiple sensors reduces the probability of error from  $P_e=0.003753$  to  $P_e<0.74*10^{-4}$ . Taking into account that these probabilities have been obtained from only 3 days of testing greater improvements might be possible.

Finally, the transponder technologies must be analyzed.

On section 6.3.6 Transponder Technologies are shown. These transponders are the base for computation on the OTI system. That means the necessity to certify this system (transponders included) as SIL4.

Final note that needs to be taken into consideration. Despite not being deeply analyzed, energy consumption and the safety of the solutions were also taken into consideration in the following way:

- The technologies must be energy efficient. This was taken into consideration in order to build an energy efficient system.



- Safety, has to be mostly focused on the main processing unit. Since the secondary units will only act as pass-through of the data, the main safety concern (SIL4) shall be placed on the main device.

## 6.4 Installation analysis

This section includes the analysis of possible installation options, related to devices that could be required at train tail, considering operational and maintenance rules.

Installation analysis is intended as a preliminary analysis, based on identified product classes and related functionalities, thus identifying guidelines (e.g. size, weight, fixing solutions, position, packaging) as input for subsequent product development phase in Tasks 4.4 and Task 4.5.

### 6.4.1 Introduction

The OTI device presents two different ways, as shown on the chapter §6.2. This creates different installation procedures depending on the Product Class.

This division presents the dichotomy of the railway environment. The High speed lines and mainlines have a shorter rolling stock LLC. The regional lines and freight corridors, have the opposite option, the rolling stock life spans to 40 years in average. With this two different rolling stock LLC the installation analysis should consider it. For this, an Installation in production and an Installation in Operation should be analyzed.

This division relies on the difference between product classes that does not mean that this is a universal rule. A Product Class 1 may make use of an Installation in Production and another an Installation in Operation.

#### 6.4.1.1 Installation in Production

This installation solution applies to the cabled OTI solutions, Product Classes 1. This Product classes are mainly fixed compositions with a short lifespan. This enables the operator to await a new rolling stock order to start the OTI deployment on this segment of the rolling stock.

With these characteristics, the installation should be performed at production time. During the construction of the compositions, the cabled OTI solution should be installed as well. With this, the railway operators will get the new compositions with OTI solutions from the producer.

This would enable this solution to be protected from the environment conditions. As a drawback, the system must have a lifespan as long as the compositions lifespan. If the OTI solution has a shorter lifespan, the Train Integrity could not be proved for the duration of the composition.

#### 6.4.1.2 Installation in Operation

This installation solution applies to the wireless or to the rolling stock with long lifespan ahead OTI solutions, Product Classes 2. These Product Classes are mainly variable reconfigurable compositions with a long lifespan. This enables the operator to deploy OTI to variable length

compositions with long lifespan, as it desires. This removes the need to buy/order new rolling stock for replacing units that may be useful for many more years.

With these characteristics, the installation should be performed at operation time. This is useful to deploy OTI system in rolling stock that is already in use. For this, the OTI device must be simple to install and installable in accessible areas of the rolling stock.

This solution has to be prepared for the environmental conditions as it may be deployed in open surfaces. The system must have as long lifespan as possible, with a minimum of the time between the maintenance tasks, with this the maintenance task for the OTI device may only be added as one more component in the regular maintenance schedule. If the OTI solution has a shorter lifespan, new maintenance tasks should be added to the Maintenance schedule of the rolling stock.

#### **6.4.2 Shunting Process analysis in freight context**

The shunting process in a shunting area for freight waggons includes some elements which are standardized or at least the same for nearly all freight waggons:

1. The pressure tube with connector
2. The pressure valve
3. The hook
4. The holder for the taillight/tailboard

As example Figure 6-49 and Figure 6-50 depicted pressure pipes and Figure 6-51 depicts the holder of the backboard.



**Figure 6-49 – Pressure tube**



**Figure 6-50 – Connected pressure tubes**



**Figure 6-51 – Holder of the backboard**

In the following, some hypothesis for OTI device installation are reported:

Hypothesis 1: The pressure connector of the last waggon could be used as a holder for the OTI. Then it is ensured that the last waggon is really the last one. Further the pressure could be used for energy harvesting and as a power switch. Using the pressure as an indicator for train separation might lead to the problem that the pressure drop at train separation might be too slow.

Hypothesis 2.: The pressure valve (as well as the tube) is part of maintenance activities and can therefore be replaced quite easily. Replacing the valve by a valve with an additional electrical switch could be used to switch the OTI. It could then be assured that the electrical switch is only “on” when the pressure is “off” (which must be the case at the last waggon, and only at the last waggon).

Hypothesis 3.: Every waggon has at each side a hook and an eyelet. At the last waggon the eyelet of the same waggon should be hooked into the hook. This constellation as a prerequisite might be used as a mechanical constellation to put the OTI on.

Hypothesis 4. Every waggon has a holder for the backboard of the train. This is a simple mechanical holder usually marked with yellow or white colour. This holder may be used to plug in a device (OTI) which must then have a reflecting cover. The device (OTI) has then in addition the functionality of the backboard (which should not be a problem).

### **6.4.3 Installation analysis for existing freight rolling stocks**

In the following figures, different kind of freight waggons are analysed thus identifying mechanical installation constraints and guidelines.



Closed Rolling Stock with upper opening.  
Roof is unsuitable for any device installation.



Closed Rolling Stock with upper opening.  
Roof is unsuitable for any device installation.



Closed Rolling Stock with lateral openings.  
Lateral areas are unsuitable for any device installation.



Closed Rolling Stock



Open Rolling Stock

Operation procedures does not allow installation on the side. Bumper areas are suitable for OTI device installation.



Open Rolling Stock


Operation procedures does not allow installation on the side. Bumper areas are suitable for OTI device installation.



Open Rolling Stock.

Operation procedures does not allow installation on the side. Bumper areas are suitable for OTI device installation.



	<p>Rolling Stock open.</p> <p>Operation procedures does not allow installation on the side. Bumper areas are suitable for OTI device installation.</p>
	<p>Open Rolling Stock with light structure</p> <p>Lateral areas are unsuitable for any device installation. Bumper areas are suitable for OTI device installation.</p>

Considering the operational procedures and the different size and type of freight waggons, possible locations for OTI devices installation are the back/front bumper area or the lateral areas in lower part of the carriage (see Figure 6-55). Other areas are critical due to differences in carriages size, openings places and types of use (see Figure 6-56). Identified areas ensures an easy localization and fast access for installation and maintenance. OTI device can be directly fixed to the carriage or mounted with properly designed brackets.



**Figure 6-52 – Installation context: suitable areas**



**Figure 6-53 – Installation context: unsuitable areas.**



In general the OTI device could be designed for fixed installation or as portable solution. Portable solution requires responsibility of railway personnel in ensuring proper installation (i.e. portable OTI Slave device in last waggon). Anyway all waggons need to be equipped with a communication network with OTI Master in front cabin.

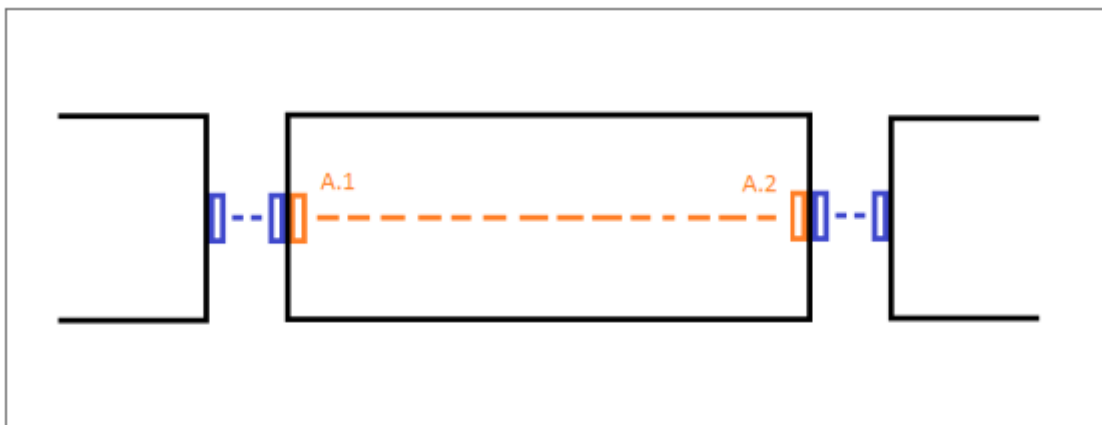
Fixed installation could require higher costs and offers further features (e.g. waggon/cargo diagnosis) and is suitable for future implementation of optional requirement related to train length determination (product class 3).

#### 6.4.4 Wireless Installation

In relation to the risk of pairing waggons that are part of different trains the following comments have been raised:

- Using antennas with high directionality;
- Avoiding installation in the corner of the waggons;
- Adopting one link/technology for communication between two subsequent waggons (blue link in Figure 6-54) and another link/technology for fixed pairing inside the two sides of the waggon (orange link in Figure 6-54) with fixed pairing rule (A.1 and A.2 fixed pairing).
- Standardize wireless interface between two subsequent waggons (blue link in Figure 6-54)

High availability of both links is required to ensure communication availability between train tail and front cabin and therefore train integrity function availability.



**Figure 6-54 – Wireless Installation: example for avoiding pairing waggon in near train**

Other solutions could use different network topology able to ensure communication between train tail and front cabin also in presence of faults to communication devices in some waggons. Anyway the risk of pairing waggons of near train has to be taken into account.

#### **6.4.5 Maintenance for freight waggons**

The maintenance period for the waggons depends on the type of waggons. The maintenance activities are defined in form of sequences and may be different depending on the number of the maintenance.

The shortest maintenance period for “regular” waggons on the SBB rail network is one year. The one year maintenance has to be applied to e.g. waggons transporting grain or sand. Typical periods are 3 years and 6 years depending on the type of the break of the waggon. The maximum maintenance period for waggons on the SBB network is 6 years. Some special waggons for track maintenance or emergency activities can have a maintenance period of 6 month.

#### **6.4.6 Feedback from users**

Coming from an interview of a railway freight operator concerning the feasibility and preference in a possible implementation of the train integrity for freight, the following opinions were expressed:

- the most simple and cost effective solution
- A very simple maintenance procedure
- Better wired solution

The max length of the freight train isn't so more than 700 meter, usually 600-650 meters. For this reason they prefer wired solution because the local power supply represent a problem in the case of “intelligent solution adopted for every waggon”.

They want a unique solution and since the cars are not all the same the lower part of the waggon should be used.

They don't close the door at other solutions but the cost is an important voice.

#### **6.4.7 Conclusion**

Performed preliminary installation analysis remarked that the most complex scenario refers to freight context with a wide range of existing waggons. Possible location, common to all waggon, was proposed for installing the OTI device. Analysis of coupling procedure in freight trains suggested possible options for detecting OTI device position (in tail or in intermediate waggon) or also as energy harvesting solution. Both fixed and portable solution have been considered for OTI device. Finally an analysis for wireless network installation was performed in relation to the issue of avoiding paring waggons from different trains.

## 6.5 Feasibility study about satellite based localization

### 6.5.1 Introduction to the GNSS technology

A global navigation satellite system (GNSS) is a system that uses satellites to provide autonomous geo-spatial positioning with global coverage. It allows electronic GNSS receivers installed on-board of the trains to determine their location (longitude, latitude, and altitude) using signals and data transmitted along a line of sight by radio from satellites. The system can be used for providing position, velocity or calculate the current time (UTC). GNSS user receivers can operate independently of any telephonic or internet reception, but require a direct visibility to the satellites for the full functionality.

#### 6.5.1.1 GNSS System description and Architecture

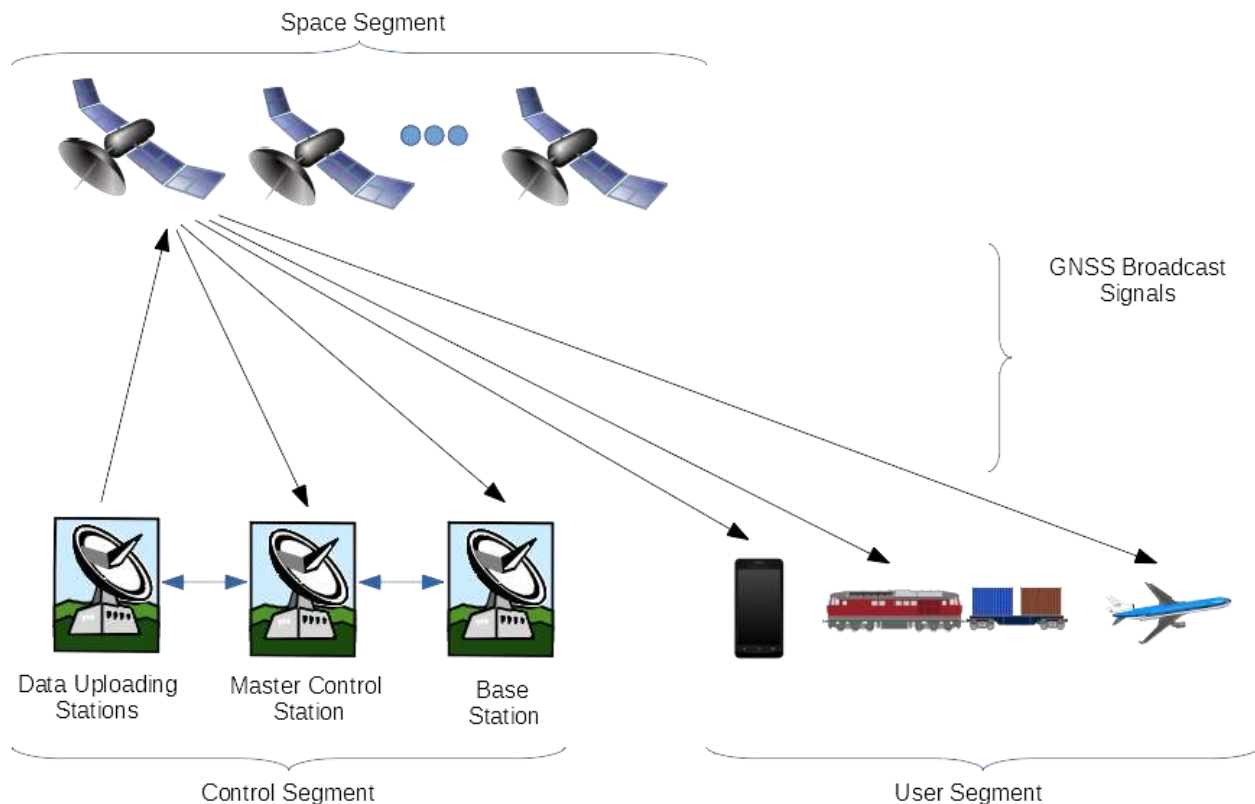


Figure 6-55 GNSS Segments

GNSS satellite systems consist of three major components or segments: space segment, control segment and user segment. The space segment consists of GNSS satellites, orbiting about

20,000 km above the earth. Each GNSS<sup>3</sup> has its constellation of satellites and each satellite in a GNSS constellation broadcasts a signal that identifies it and provides its time, orbit parameters and status.

The control segment comprises a ground-based network of master control stations, data uploading stations and monitor stations. The master control station adjusts the satellites' orbit parameters and onboard high-precision clocks when necessary to maintain accuracy.

Monitor stations, usually installed over a broad geographic area, monitor the satellites' signals and status, and relay this information to the master control station. The master control station analyses the signals then transmits orbit and time corrections to the satellites through data uploading stations.

The GNSS signals are broadcasted in several RF bands. The most common one is L1 band with central frequency about 1.5GHz. The user segment consists of equipment that processes the received signals from the GNSS satellites and uses them to derive and apply location and time information.

The primary components of the GNSS user segment are antennas and receivers, which process the satellite signals recovered by the antenna to calculate position, velocity and time.

Receivers may be designed to use signals from only one GNSS constellation or from more than one GNSS constellation. Exact configuration of the receiver shall be selected to meet the requirements of the application of GNSS.

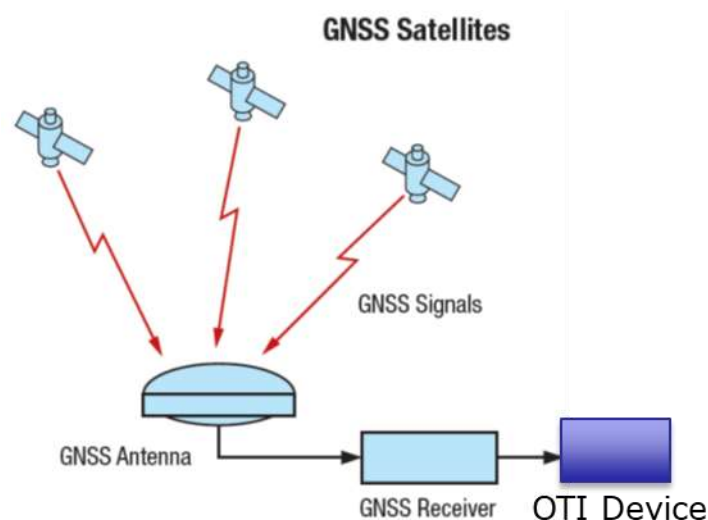


Figure 6-56 – GNSS interface to OTI device

---

<sup>3</sup> See chapter 6.5.1.2 for more details about types of GNSS systems.

### 6.5.1.2 GNSS Systems and Augmentation

Currently, there are four GNSS systems that are either in a full operation state or are scheduled to be fully operational within 2 years' time.

The United States' Global Positioning System (GPS) and Russia's GLONASS are the only two fully operational GNSSs on the global level. The European Union's Galileo GNSS is scheduled to be fully operational by 2020 and China is in the process of expanding its regional BeiDou Navigation Satellite System into the fully global BeiDou-2 GNSS by 2020.

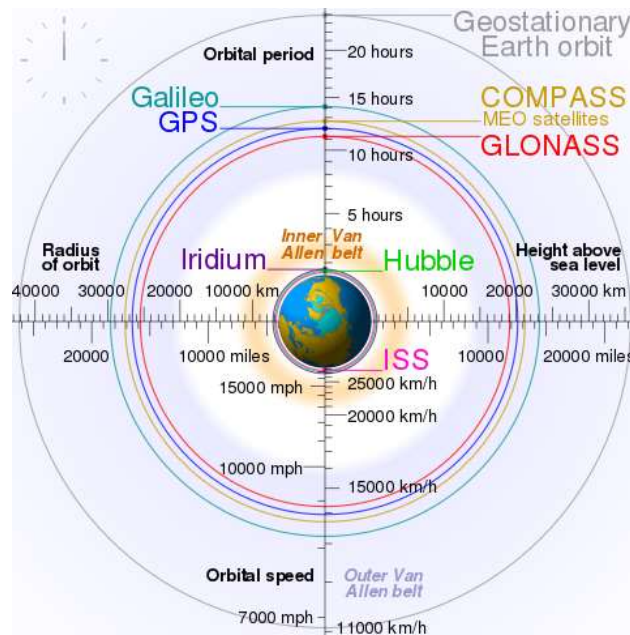


Figure 6-57 – Orbits of GNSS systems

From the application point of view, a designer of GNSS-based OTI function shall make a decision on which a specific GNSS or combination of GNSS to use. It's not a trivial task since a number of factors shall be considered:

- Technical and economic aspects:
  - Quality of the output information, including achievable precision.
  - Implementation of effective measures for minimising the influence of various factors having an impact on localisation precision, especially those relevant for rail environment.
  - Resistance against potential cyber-attacks.
  - Availability and the price of the needed equipment on the market (especially GNSS receivers, antennas, relevant simulation and development tools, etc.).
  - Selection of suitable GNSS systems, considering relevant development and application costs of having a combined GNSS solution.
- Political aspects: A commitment of the system's owner/operator to keep the system fully functional for civilian users regardless of the political or military situation (Note that some GNSS, such as GPS and GLONASS have been historically developed as part of the

strategic military infrastructure whereas Galileo is from the very beginning under civilian control).

#### 6.5.1.2.1 GNSS Augmentation

Augmentation of a global navigation satellite system (GNSS) is a method of improving the navigation system's attributes, such as accuracy, reliability, and availability, through the integration of external information into the calculation process. Augmentation information can be provided by remote devices as well as by devices installed in close location to the GNSS receiver. There are many such systems in place and they may generally provide 3 types of information:

- Specific information about sources of error (such as satellite clock drift, ephemeris, or ionosphere delays, etc.).
- Differential measurements: Error estimations performed thanks to reference stations.
- Additional information to improve the navigation performance, to be integrated in the calculation process (actual vehicle velocity derived from odometry, track topology, etc.).

GNSS augmentation systems are generally named or described based on how the GNSS user sensor receives the external information. The basic types include:

- Ground-based augmentation system (GBAS).
- Satellite-based augmentation system (SBAS).

European Union's version of SBAS, called EGNOS (The European Geostationary Navigation Overlay Service), supplements the GPS (*and later EGNOS versions will support Galileo*) by reporting on the reliability and accuracy of their positioning data and sending out corrections. Its Safety of Live Service allows pilots throughout Europe to land the aircraft using a GPS approach. The similar scheme could be also considered for future safety-related rail applications, including satellite-based OTI device<sup>4</sup>.

#### 6.5.1.3 GNSS receiver output data

A GNSS Receiver is a processor of radio signals capable of solving the navigation equations in order to determine the position, velocity and precise time (PVT) by processing the signals broadcasted by GNSS satellites. Any navigation solution provided by a GNSS Receiver is based on the computation of its distances to a set of satellites by means of extracting the propagation time of the incoming signals traveling through space at the speed of light, according to the satellite and receiver local clocks.

---

<sup>4</sup> Note: EGNOS signal propagated in a typical railway environment is significantly limited due to relatively low elevation of its geostationary satellites - about 30° above horizon in central Europe and much less in the North of Europe. It may be necessary to re-transfer EGNOS data using different communication channels.

Different sources can contribute to the error in PVT estimates, as summarised below:

- Ephemeris data: The accuracy of satellite position in space (broadcasted by GNSS satellites) at the time of the signal emission is not fully accurate (typical error is of several meters).
- Satellite clocks: Although typically each satellite includes several atomic clocks, the time base contains offsets. For example, a time error of 10ns immediately results in a distance error of about 3m.
- Effect of the ionosphere: Signals from the satellites travel through a vacuum at the speed of light. In the ionosphere, the velocity of these signals slows down and therefore can no longer be viewed as constant. The exact level of ionization is typically not known by the receiver<sup>5</sup>. Ionosphere related errors are frequency dependent and can be partially corrected by using dual frequency receivers.
- Effect of the troposphere: the troposphere is the atmospheric layer located between 0...15 km above the Earth's surface. The cause of the error here is the varying density of the gas molecules and the air humidity. The density decreases as the height increases. The increase in density or humidity retards the speed of the satellite signals. The effect can be partially eliminated using tropospheric models.
- Multipath (reflections and diffraction): GNSS signals can be reflected from buildings, trees, mountains etc. and/or bent around obstacle edges. As a consequence, also non-line of sight signals may arrive at the receiver antenna. The effect of multipath can be partially mitigated by the selection of the measuring location (applicable in static conditions), utilization of a specific antenna (often large) or receiver with a specific mitigation algorithm (e.g. MEDLL correlator).
- Signal attenuation or even signal blockage due to obstacles: in a complicated environment (urban areas, tree areas under dense foliage, etc.) the received GNSS signals can be attenuated due to diffraction caused by passage through obstacles. If the signal is slightly attenuated only signal processing is still possible in a receiver but resulting in more noisy measurements and thus PVT with worse quality (worse accuracy). If the signal is attenuated in higher level, the processing in a receiver is impossible and the receiver cannot utilize this measurement for PVT. This results to worse PVT quality (accuracy or even unavailability) due to worse satellite geometry.
- Effect of the receiver: further errors are produced due to GNSS receiver measurement noise, time delays and numerical errors in the receiver. Advanced technologies/methods can reduce this effect to certain limits.
- RF interference: interferences can be intentional or not. They can result in worse accuracy of PVT solution or even PVT unavailability if all the satellites signals are attenuated by the jamming. Spoofing can introduce false position.

---

<sup>5</sup> Effects can be partially estimated (and eliminated) using multi-frequency GNSS receiver.

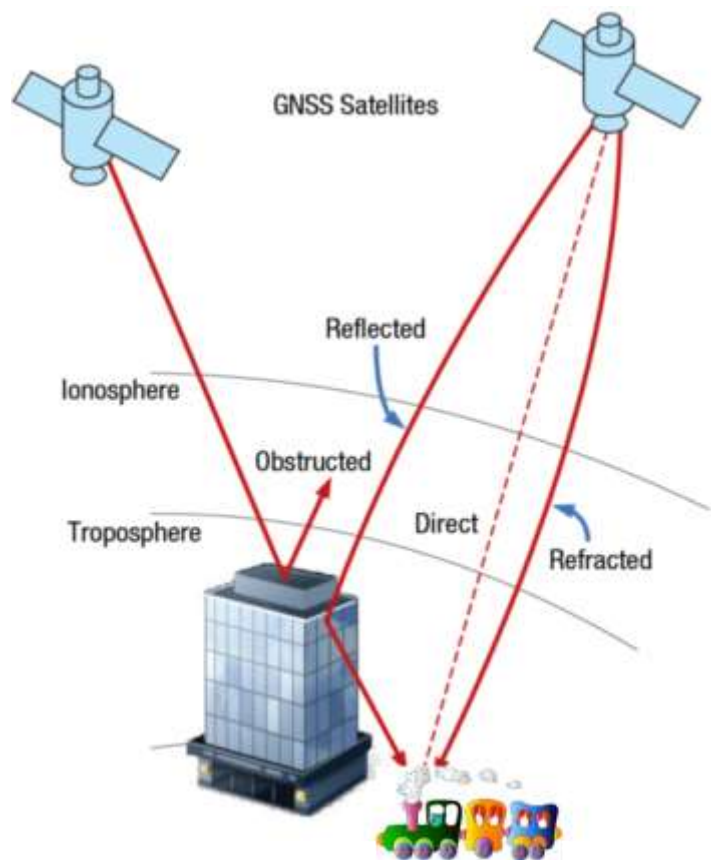
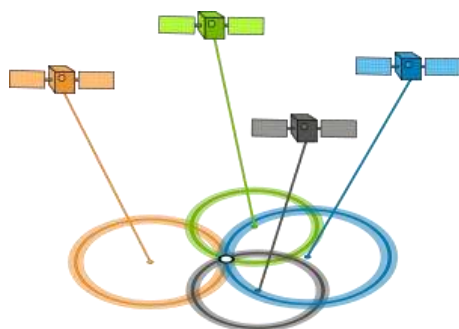


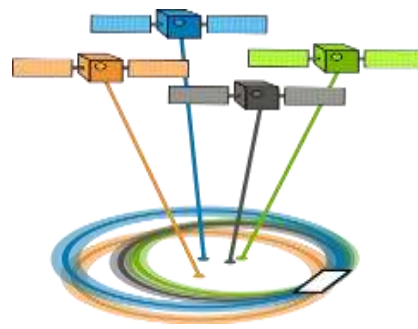
Figure 6-58 – Reflection, Refraction and Obscuration of GNSS signals

- Effect of the satellite geometry on imprecision. Actual geometric configuration of the satellites used in PVT solution has a significant effect on the resulting precision and is typically expressed by DOP – family of values (Dilution of Precision). Generally speaking, the total position error estimate model is an accumulation of other errors multiplied by the DOP value:

$$\text{TOTAL ERROR} = (\text{Position error through other influences}) \times (\text{DOP value})$$



Good DOP value in position domain  
(typically  $1 < \text{DOP} < 3$ )



Degraded DOP value in position domain  
(typically  $\text{DOP} > 3$ )

Figure 6-59 – GNSS Dilution of precision in position domain (PDOP)



#### 6.5.1.4 Past and ongoing projects relevant to satellite-based safe localisation function

The use of Global Navigation Satellite Systems (GNSS) will provide significant advantages for ensuring the control of train movements on railway networks where the trains can use satellite signals to calculate their position in an autonomous way. However, a challenging issue remains to demonstrate the safety level of the localization function and the train integrity realized by an on-board GNSS-based system. Two main aspects related to the use of GNSS were developed by various European projects to deal with RAMS aspects. These aspects focus on the development of *key performance indicators* and the *safety assessment* linked to identify usability scenarios of train localization. A recent review of GNSS-based research and development of European projects is detailed in flowing recent papers [62] and [63] to show their advantages and drawbacks. A safety assessment of GNSS railway application is developed in a recent paper [64].

##### 6.5.1.4.1 Key performance indicators

GNSS key performances are evaluated in terms of accuracy, availability, continuity and integrity attributes as used in aeronautical applications. Most of the solutions adopted in various projects aim at ensuring availability, accuracy and integrity aspects by combining GNSS with other heterogeneous sensors in order to compute PVT (Position, Velocity and Time) of the train. Several European projects developed various hybridized GNSS-based multi-sensor systems and different strategies to ensure high accuracy and integrity. LOCOPROL and GIRASOLE projects demonstrated that a GNSS standalone receiver is not able to provide a safe navigation solution, particularly in urban area where GNSS signals are subject to multipath effects. Various European projects were dedicated to multisensors solutions that allow the system to benefit from absolute localization solutions with GPS as well as continuous and high frequency localization with the help of inertial measurements (Gaderos, APOLO, Galoroi...). It can be noticed that EATS project integrates GNSS with wireless communications technology (WCT) positioning. WCT relies on GSM-R and UMTS mobile communication systems and improves in particular availability. 3inSat and NGTC proposed architecture for Virtual Balise detection based on GNSS receivers. STARS characterized the GNSS signal reception in the real railway environment.

Integrity monitoring is a first challenge to ensure that a GNSS solution can be used for railway safety critical applications (e.g. train integrity). The assurance for high accuracy and integrity performance can be based on hardware redundancy (hybridization of sensors) or/and information redundancy (e.g. Autonomous Integrity Monitoring and Assurance [62], [63]). *Hardware redundancy* (often with a fail-safe voter) improves the integrity of vital information. GaLoROI project hybridizes GNSS with sensors and uses architecture redundancy (with independent channels). GRAIL2 project uses 2 channels associated to a vote (in safe controllers) in order to check consistency between channels. *Information redundancy* is based on fault detection and tolerance and/or SBAS (Satellite-Based Augmentation System). Since the early introduction of GNSS in railway, fault detection algorithms have been proposed such as an Autonomous Integrity Monitoring and Assurance (AIMA) scheme for a multisensory positioning system (accelerometer,

gyroscope, odometer, GNSS [73]). Also, the GNSS-based altitude determination with the planned altitude contained in a 3D track- map was explored. EGNOS is the European system capable of providing ranging and correction data for accuracy enhancement but providing also integrity data. The improvement the availability and the accuracy, the 3inSat and STARS H2020 European projects explored a local integrity monitoring network (AIMN – Augmentation and Integrity Monitoring Network) approach. These approaches are consolidated in the RHINOS H2020 European project that aims to develop a Railway High Integrity Navigation Overlay System as a combination of GNSS, SBAS and ARAIM [69].

#### 6.5.1.4.2 *Key performance assessment*

The second challenge to use GNSS-based systems in railways is to assess the key performances, *in railway environments*, regarding the requirements of positioning performances (availability, accuracy) and safety (integrity-related). The evaluation of key performances was done by extended simulation and experimental campaigns. Simulation offers repeatability, control of all the test conditions, possibility to change the constellation (versus time and multi-constellation combinations) and anticipation of future systems (such as the complete Galileo). Some initiatives are in progress such as the ATLAS (Advanced Train Location Simulator) developed within the EATS project [70]. ATLAS platform aims to test various on-board localization systems, with various technologies along various infrastructures. In the SATLOC project, an innovative hybrid solution has also been proposed that combines experimental knowledge of the masking obstacles with a GNSS signal simulator [71]. Various European projects conducted a large experimentation campaigns in various areas for performance evaluation. LOCOPROL experienced its solution along a rural line in Belgium, line in South of France and high speed line in Italy. SATLOC conducted it in Romania on a low density traffic line. ERSAT EAV project performed a satellite measurement campaign in Sardinia along a double track equipped with multi constellation receivers [72].

#### 6.5.1.4.3 *Safety approval approaches*

The third challenge is the safety approval of the GNSS-based systems in railways application. Recent projects as GRAIL-2 and SATLOC agreed that the GNSS-based positioning subsystem is compliant with SIL2 requirements. Safety approval issues have been explored and a safety case structure was proposed in GaLoROI project for railway safety applications of GNSS. The GRAIL-2 project addressed the compliance with the Railway Safety Approval process by carrying out an Independent Safety Assessment of the proposed methodology. The GRAIL-2, with notified body, performed an assessment of proposed safety case delivered by the Consortium to comply with SIL 2 requirements. The ERSAT GGC project is adopting the same approaches.

#### 6.5.1.4.4 *Past and ongoing projects*

<b>Project Name (Funding program)</b>	<b>Start -End</b>	<b>Main characteristic and relevance to the OTI function</b>
APOLO	1998-2001	APOLO “Advanced Position Locator” results can contribute to key performance definition and assessment of OTI
GADEROS (5 <sup>th</sup> FP)	2001-2004	GADEROS “Galileo Demonstrator for Railway Operation System” results can contribute to key performance definition and assessment
LOCOPROL/LOCOLOC (5 <sup>th</sup> FP/ESA)	2001-2004	LOCOPROL “Low Cost satellite based train location system for signalling and train Protection for Low-density traffic railway line “  LOCOPROL results can support the key performance assessment of OTI using GNSS.
GRAIL (6 <sup>th</sup> FP/GJU) GRAIL 2 (7 <sup>th</sup> FP)	2005-2007 2010-2013	GRAIL “GNSS introduction in the RAIL Sector “ and GRAIL-2 “GNSS-based enhanced odometry for Rail” results can be used to develop the safety assessment and approval process of OTI
GALOROI (7 <sup>th</sup> FP)	2012-2014	GALOROI “Galileo Localization for Railway Operation Innovation” developed a methodologies for safety evaluation of GNSS based positioning solutions. GaLoROI results can support certification process of OTI.
SATLOC (7 <sup>th</sup> FP)	2012-2014	The project addresses the development and demonstration of innovative GNSS application for the train control, speed supervision, traffic control and traffic management of low traffic lines (LTL).  The approach proposed by SATLOC to an enhanced GNSS based train control system for low traffic density lines with high safety level can bring added values to OTI application.

<b>Project Name (Funding program)</b>	<b>Start -End</b>	<b>Main characteristic and relevance to the OTI function</b>
QualiSaR (7 <sup>th</sup> FP)	2012-2014	<p>Development of a Qualification Procedure for the Usage of Galileo Satellite Receivers for Safety Relevant Applications</p> <p>The proposal for a standardised qualification procedure can support OTI application..</p>
EATS ETCS	2012 - 2016	<p>EATS ETCS “Advanced Testing and Smart Train Positioning System” developed ATLAS “Advanced Train LocAtion Simulator “ platform to simulate the performance of location system.</p> <p>The ATLAS platform can support OTI validation through simulation and the integration of GNSS with wireless communications technology (WCT) positioning</p>
3inSat (ESA, ARTES 20 IAP)	2016-2018	<p>3inSat “Train Integrated Safety Satellite System “ project aimed at developing and validating a new satellite based platform to be integrated into a SIL 4 (Safety Integrity Level 4) Control and Management Signaling System based on the ERTMS/ETCS.</p>
RHINOS (H2020)	2016-2018	<p>RHINOS” Railway High Integrity Navigation Overlay System”aimed at increasing the use of EGNSS to support the safety critical train localization function for train control in emerging regional and global markets. The project contributed to the definition of augmentation and integrity system as well as on the definition and execution of the proof of concept.</p> <p>Rhinos project can bring added values to OTI on the GNSS integrity criterion and the use of mitigation of faults in order to reduce hazards.</p>

Project Name (Funding program)	Start -End	Main characteristic and relevance to the OTI function
ERSAT EAV (H2020)	2015-2017	ERSAT (EAV) ERTMS on SATELLITE (Enabling Application Validation) developed methodologies for GNSS based solutions dedicated to Virtual Balise use on ERTMS lines. The outcome of ERSAT-EAV is a priority for reusing the ERTMS standard architecture to satisfy the needs of the regional and local lines and for supporting the UNISIG Satellite Positioning Working Group.
NGTC (7 <sup>th</sup> FP)	2013-2016	NGTC “Next Generation Train Control” addressed the use of satellite positioning that will be of interest for X2Rail-2 WP4 “Train integrity” regarding applications of satellite positioning functionality for train integrity and safety analysis
STARS (H2020)	2016-2019	<p>The STARS project paved the way for the future EGNSS deployment in safety relevant railway applications. By evolving the highly developed and deployed ERTMS standard through the implementation of the satellite positioning functionality, it will be possible to reduce the cost of the future railway signalling systems, especially for lines with lower traffic density.</p> <p>STARS deals with the characterization of EGNSS reception in railway environment including multipath, interferences and GNSS performance models for safety and non-safety related applications.</p> <p>STARS results can help to bridge the gap between train integrity applications and GNSS services .</p>

Project Name (Funding program)	Start -End	Main characteristic and relevance to the OTI function
ERSAT GGC (H2020)	2018-2020	<p>ERSAT GGC is conceived for speeding up the certification process of EGNSS assets according to the ERTMS rules. It is a follow up of the ERSAT (ERtms + SATellite) program launched in 2012 by RFI in collaboration with Ansaldo STS for integrating satellite technologies on the ERTMS platform.</p> <p>ERSAT GGC will rely on the achievements of the most relevant EC and GSA funded projects such as NGTC, ERSAT EAV, STARS, RHINOS whose the individual coordinators are partners of the consortium. The consortium includes RFI, SNCF and ADIF as the main European rail stake-holders and two independent notified body, Italcertifier and Bureau Veritas which are already supporting the certification process.</p> <p>ERSAT GGC will be of interest for X2Rail-2 WP4 "Train integrity" regarding safety analysis and approval.</p>
X2Rail-2 (H2020)	2017-2021	<p>The X2Rail-2 WP3 (Fail-safe Train positioning) of X2R2 project will progress simultaneously with X2Rail-2 WP4 'train integrity), with very close targets in particular of OTI integrity and safety.</p>
<u>Recent or ongoing projects:</u>		
STEMS (ESA)	04/18-10/19	<p>To study the suitability of the current generation of SBAS for use in the evolution of the European Rail Traffic Management System (ERTMS) with virtual balise detection using GNSS, confirming the feasibility of current system allocations.</p>

Project Name (Funding program)	Start -End	Main characteristic and relevance to the OTI function
CAPRESE (ESA)	11/18-05/20	Techniques supporting resilience for high integrity train control applications  To study GNSS carrier phase integrity techniques for application in railway safety of life applications, and in particular, the evolution of the European Rail Traffic Management System (ERTMS) with virtual balise detection using GNSS.
Gate4rail (Shift2Rail)	12/18-11/20	GNSS Automated Virtualized Test Environment for RAIL
Astrail (Shift2Rail)	09/17-08/19	Contribute to enhancing the signalling and automation of the railway system thanks to innovative solutions that exploit cutting edge technologies already in use in sectors different from the rail, such as the aeronautic or the automotive sectors.

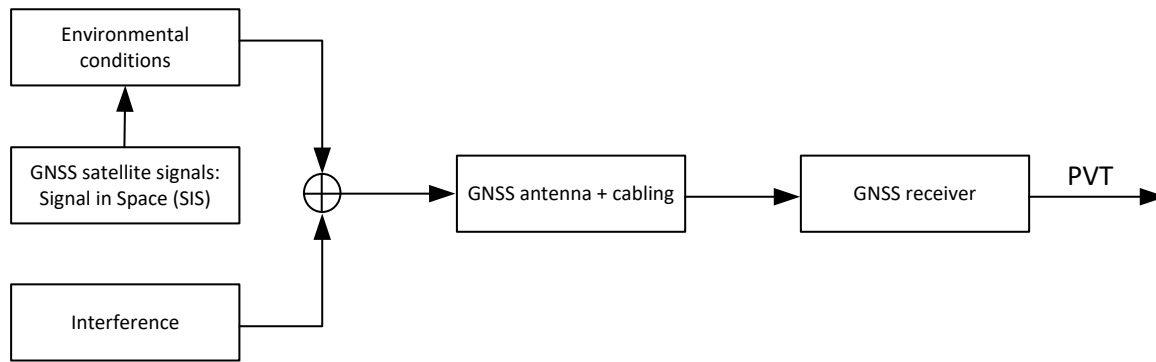
Table 6-23: Railway-related projects dealing with GNSS – related aspects

## 6.5.2 GNSS-based OTI function

### 6.5.2.1 RAM aspects

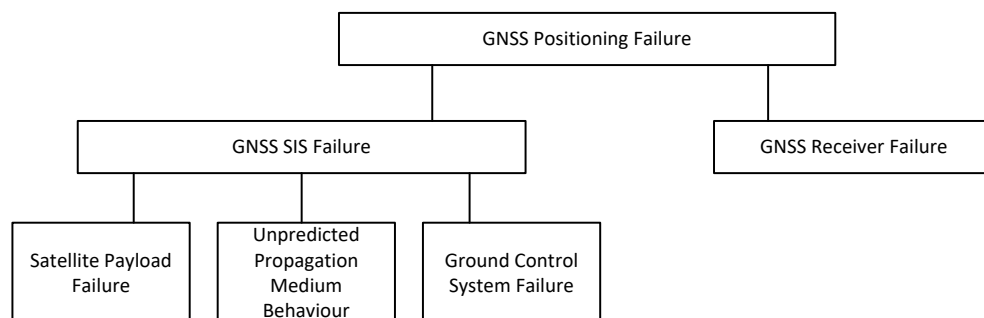
#### 6.5.2.1.1 Reliability

As previously mentioned in section 6.5.1.3, there are multiple sources of errors that may influence a reliability of the GNSS system itself. Figure 6-60 illustrates the propagation model of the GNSS signal coming from the satellite.



**Figure 6-60 Signal propagation model<sup>6</sup>**

The reliability of the GNSS signal can be affected from two main source groups before it arrives to the train, the environmental conditions and the intentional and unintentional Electromagnetic Interferences (EMI). However, for calculating the reliability values of the GNSS system as a whole in order to evaluate its suitability of its inclusion in the OTI function as a source of positioning information, there are additional conditions that have to be taken into account. Figure 6-61 illustrates the origin of possible GNSS related failures. It must be taken into account that for the OTI function, the master and slave OTI devices will use their position and velocity to compute the integrity check. Taking into account that both OTI devices make use of the same GNSS system (e.g. GPS), we could assume that the Satellite Payload Failure and Ground Control System Failure will be equal for both, the master and slave devices, independently if they are placed in the front or in the rear of the train. For calculations, the GNSS Receiver Failure rate of master and slave devices will be most probably equal. The Unpredictable Propagation Medium Behaviour (for GNSS signals) may vary between the master and slave devices. These failures may come as seen in section 6.5.1.3 from effect of the ionosphere, effect of the troposphere, signal reflections and from EMI. It is supposed that the ionosphere and troposphere conditions should not change abruptly in the time taken by the rear of the train to be in the position of the front taken as a reference to compute the integrity in the case of short trains. However, in the case of freight trains, which can be several kilometre-long and low speeds, this assumption should be closely re-evaluated.



<sup>6</sup> NGTC project, D7.2 Definition and quantification of the GNSS parameters to be measured in railway environment.



Figure 6-61 GNSS Positioning Failure Classification<sup>7</sup>

#### 6.5.2.1.2 *Availability*

To confirm the train integrity by GNSS-based OTI device, an availability of a minimum number of GNSS satellite signals is the elementary pre-condition. It is worth to mention that power of GNSS signals in an area of GNSS antenna is very low and below the thermal noise floor. The used frequency bands are shared among several systems and the concrete GNSS satellite can be detected only using Code Division Multiple Access (CDMA) technique by GNSS receiver.

GNSS signals are transmitted at a very low power and they arrive at a terrestrial receiver antenna below the noise floor (e.g. around -160 dBW for GPS L1). In case of receiving NLOS signals, their power is further negatively affected. All kinds of obscuration (so common in typical railway environment) decrease the GNSS based localisation function performance. All kinds of obscuration (so common in typical railway environment) will prevent receiver to process GNSS signals. The environmental conditions that block receiving of GNSS signals include: Tunnels, buildings, urban or natural canyons, anti-noise barriers, roofs (glass roof may also negatively influence GNSS signals), trains on parallel tracks, etc.

The actual weather condition usually doesn't have a significant effect on reception of GNSS signals, nevertheless, there is a well-known issue linked with a melting snow.

Electromagnetic interference may be relevant for the areas with strong source of electromagnetic fields.

As a conclusion, the availability of train integrity confirmation generated by GNSS-based OTI device is strongly dependent on several factors:

- A required minimal number of satellite signals in a good quality. Note: For safety reasons, there might be a requirement for a certain level of redundancy regarding satellite signals.
- Environmental conditions linked with the specific railway track from GNSS signal reception perspective. Note: GNSS-based solution may not be suitable for all types of tracks. For example, a track with significant number of tunnels, or track in a dense urban area (especially with high buildings) may not be effective for GNSS-based OTI solution.
- Presence of RF interference. Note: Currently, there is not a clear evidence regarding practical influence of RF interference from different electromagnetic field sources on GNSS-based function. Some initial results are expected from STARS project [65].

In order to compensate known drawbacks of satellite-based technology, it may be worth to consider several technical measures:

- Complement GNSS-based technology with COTS INS: The INS technology may provide a required redundancy as well as to support the train integrity function in cases with unavailable or reduced GNSS signals reception.
- Use of GNSS augmentation: The augmentation may provide additional data about the failure-free state of GNSS as well as to increase a performance of train integrity function in terms of positioning / velocity accuracy or speeding up the collection all the required GNSS-based data.
- Placement of GNSS antenna in locations with a good visibility of GNSS satellites: this measure will be hard to implement especially for the use-case where the Rear OTI device is considered as a removable part. Ideal position of GNSS antenna is on the train roof with no vicinity obstructing objects (to allow visibility of satellites in low elevation angles).
- Take an advantage of increasing number of available GNSS: Combination of two or several GNSSs may increase availability of GNSS-based solution dramatically. It is worth to mention that GALILEOs public service was designed from scratch to be fully compatible with GPS signals with a minimal impact on GNSS receiver design.

#### 6.5.2.1.3 *Maintainability*

In terms of maintainability, the main aspect to consider is linked with installation of the GNSS antenna. There are several requirements that should be further considered [66]:

- Bonding any exposed conductive part firmly to the vehicle frame prevents the antenna and cabling from rising to an excessive potential. This could be achieved by locally removing the existing insulating roof paint and replacing it with a conductive one, providing the roof is adequately bonded via the vehicle frame and running gear to the running rails.
- Protect the cable from being inadvertently used as the safety equipotential bond for the antenna ground plane and mounting plate.
- The cable between the antenna and the receiver is also a particular threat to EMC; the appropriate measures should apply.
- All the connections with antenna should be properly sealed and properly maintained whatever the design of the installation. It is recommended that the antenna is sealed to a minimum of IP66.
- It is recommended that the design of the installation will allow a roof access, in order to maintain or replace the antenna.

#### 6.5.2.2 **Safety aspects**

As explained in the previous section, PVT information derived from GNSS signals is prone to various type of errors and can be negatively influenced by potential failures and anomalies introduced by GNSS systems. If the actual GNSS-based information error is greater than the computed one, the safety-related function using this information may put a system into a hazardous state. Undetected GNSS-related errors may occur due to GNSS system's components failures, their deviations from expected behaviour and due to environmental aspects, strongly linked to the actual railway environment. It should be noted that no available GNSS system, as it

is today, have been developed according to the railway safety standards (CENELEC EN 50126 and related). In order to use GNSS for safety critical functions, it is necessary to closely analyse, study and understand all the GNSS related mechanisms that can potentially lead to undetected errors. Safety requirements linked to the GNSS based information shall be derived from OTI function hazard analysis developed on the system level.

Following the Figure 6-62: *GNSS receiver* (part of GNSS User Segment) is providing data derived from GNSS to be processed by *OTI function*. OTI function process all the received GNSS data and in case that these data are available, consistent and are in certain quality, function evaluates whether the data match the scenario of integer train.

The top level safety hazard happens for the scenario when *OTI function* wrongly evaluate the train integrity and provides this wrong status to a linked safety-related system, such as ETCS.

For more detailed analysis, let's consider the two basic underlying hazardous states:

- Hazard A – Hazard due to use of non-consistent, low quality or faulty GNSS data.
- Hazard B – Hazard due to a wrong estimate of train integrity (train integrity has been confirmed in the situation when the train is no longer complete).

It is possible that *Hazard A* won't lead to *Hazard B* due to internal measures implemented on the level of OTI function.

In case that OTI function will fail to detect a problem in GNSS data and will continue to use these GNSS data, OTI function may wrongly release a confirmation about train integrity (*Hazard B*). This situation may further lead to an accident after certain conditions are met (accident triggers).

For the simplicity and readiness, both *Hazard B* and *Hazard A* will be represented by a term: GNSS Hazards.

Following, there is a detailed structure of possible causes leading to unexpected and negative GNSS-based information error:

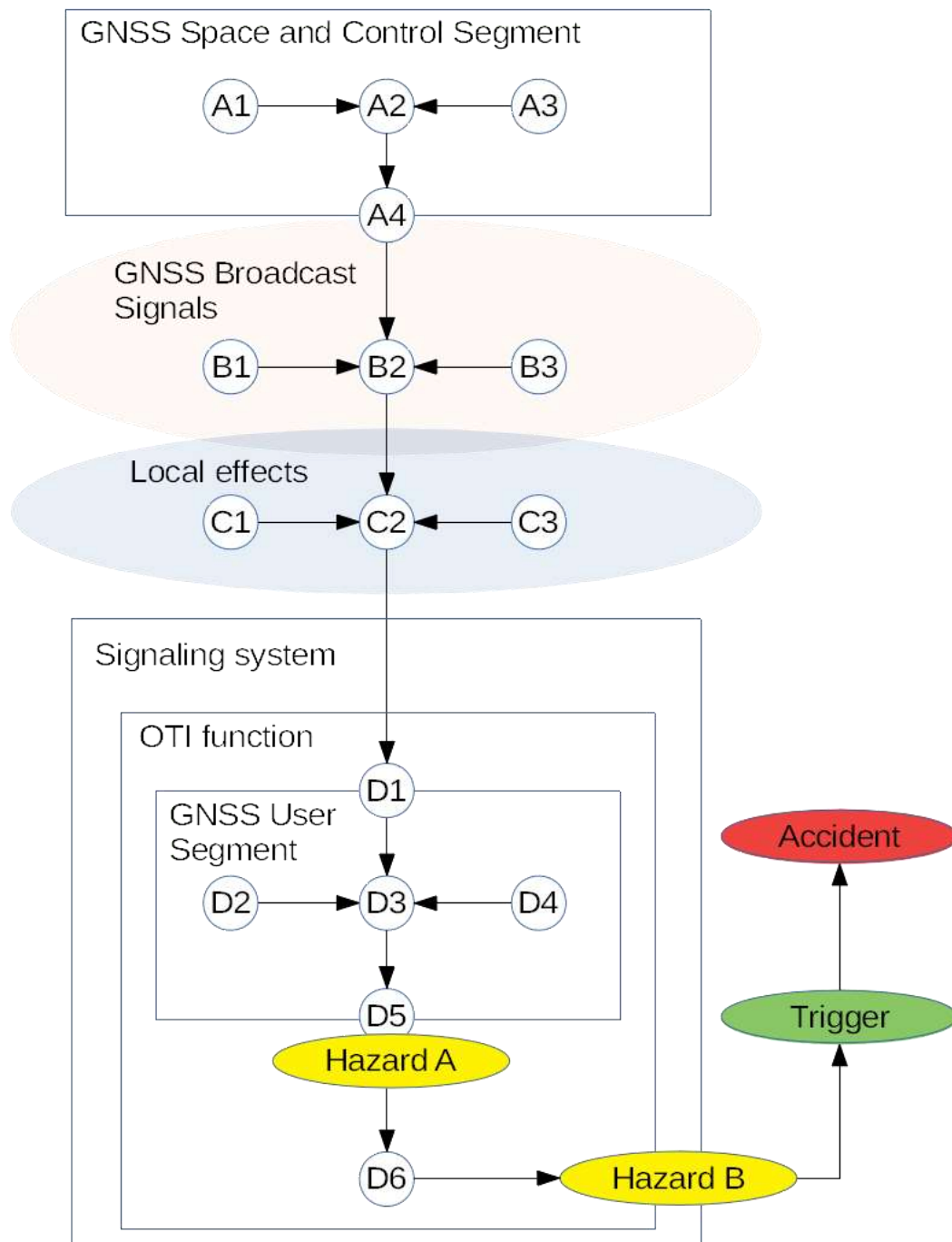


Figure 6-62 GNSS-related hazards and structure of causes (negative events)

- **Level A:** Negative events (e.g. failures) that may originate in GNSS control centrum facilities (GNSS control stations, Ground antennas, Monitor stations) or are related with

GNSS satellites malfunction. These negative hazardous events (A2) are composed from systematic functional and random errors of ground facilities (A1 – e.g. control station systematic algorithm errors, misleading monitoring data, etc.) and systematic functional and random errors of GNSS satellites (A3 – e.g. undetected satellite clock errors, satellite manoeuvring errors, etc.). There are also negative events linked to the transmission errors within control and space segment (A4, e.g. GNSS system navigation data are changed due to erroneous communication channel and weak transition security, etc.)

- **Level B:** These negative events are related to GNSS signals' propagation environment (B2), while specifically the influence of the ionosphere (B1) and troposphere (B3) could lead to longer than expected GNSS signals propagation times.
- **Level C:** These negative events originate in a railway environment (C2). They are caused by local environmental effects, disturbing a propagation of GNSS signals (C1, e.g. GNSS signal multipath, obscuration, etc.) or by sources of various kinds of disturbances (C3, e.g. malicious GNSS signals masquerade, close digital wide-spectrum transmission antenna causes negative influence on GNSS signals, etc.). These events are different for each OTI application and may occur differently for each type of track.
- **Level D:** These negative events are linked directly to OTI function implementation. Hazardous event D1 includes errors due to receiving and pre-processing of GNSS signals (e.g. failure in GNSS antenna, error in receiver correlation unit, etc.). Internal GNSS receiver function errors are represented by the D3 event. It is composed of functional errors (mostly systematic errors in algorithms determining PVT information, such as erroneous GNSS navigation message processing, etc.) and the technical failures (e.g. GNSS receiver processor failure, flash memory failure, etc.). D5 are events related to transmission error to the OTI function. D6 are negative events linked to further processing of the GNSS-PVT data directly by OTI function.

It is worth to mention that frequency of hazardous events together with their respective consequences could differ depending on GNSS signal design and properties. For example, new GNSS signals (e.g. Galileo services) tend to be less vulnerable to local effects such as interference and multipath.

From the OTI function perspective with respect to GNSS hazards, the procedure for finalising required hazard analysis could be the following:

1. Identify all the GNSS - based negative events that have a potential to cause undetected error in PVT information.
2. Each GNSS - based negative event should be further analysed to obtain the frequency of its occurrence and its potential consequence to OTI function.
3. For those GNSS - based negative events that have unacceptable consequences for OTI function, find and develop proper measures and demonstrate their efficiency.
4. Finally, it should be demonstrated that GNSS-based OTI function as whole meets the overall safety requirements.

It can be concluded that there is a need of ensuring the required integrity level of the GNSS-based data used by OTI device. Among the possible solutions, there is an option to use GNSS

augmentation system. Apart from building a specific infrastructure on the ground (GBAS) that may be costly if used only for OTI function, there is also a possibility to integrate into OTI function one of the existing SBAS (e.g. EGNOS in Europe and WAAS in USA). Using one of these augmentation systems generates new availability problems (see the measurements being carried out by STARS project). For example, EGNOS may not be available in all European railways due to limited coverage. In case of the GALILEO system, it will provide integrity information by its own network of satellites, so that this problem may be overcome.

### 6.5.2.3 Functional impacts

According to defined OTI product classes, the train integrity criteria for wireless communication scenarios includes the acquisition of train tail status to check coherent movement respect to front cabin. As example train tail position can be determined on the basis of GNSS solutions.

Scenarios with poor or temporary absent GNSS coverage generates temporary impossibility to localize the train tail, therefore impacting on OTI system capability to monitor train integrity (i.e. temporary “unavailable” train integrity information). In such situations the train integrity information shall change between “confirmed” and “unavailable”.

Scenarios with poor GNSS coverage results in a reduced availability and therefore in reduced capacity performances because the train tail position is refreshed slowly. Although the limited capacity, this solution allows reducing CAPEX, OPEX and LCC for trackside infrastructure (i.e. track circuits) in low traffic lines.

For these reasons OTI device need to be designed to allow transitions between “confirmed” and “unavailable”.

Temporary poor GNSS coverage could result in temporary higher and anyway variable localization error. For this reason false alarm filtering criteria, with spatial/temporal thresholds, need to be defined before declaring “loss” of integrity.

The generalization for above described scenario consists in considering “unavailable” and “lost” as different physical events that need to be managed differently by OTI device.

In terms of OTI master FSM the following guidelines results as appropriate for freight scenarios based on wireless on-board communication:

- **Temporary coverage unavailability:**
  - FSM master shall go from REGULAR to NON REGULAR state in case of unavailable satellite coverage and shall send “unknown” train integrity to ETCS;

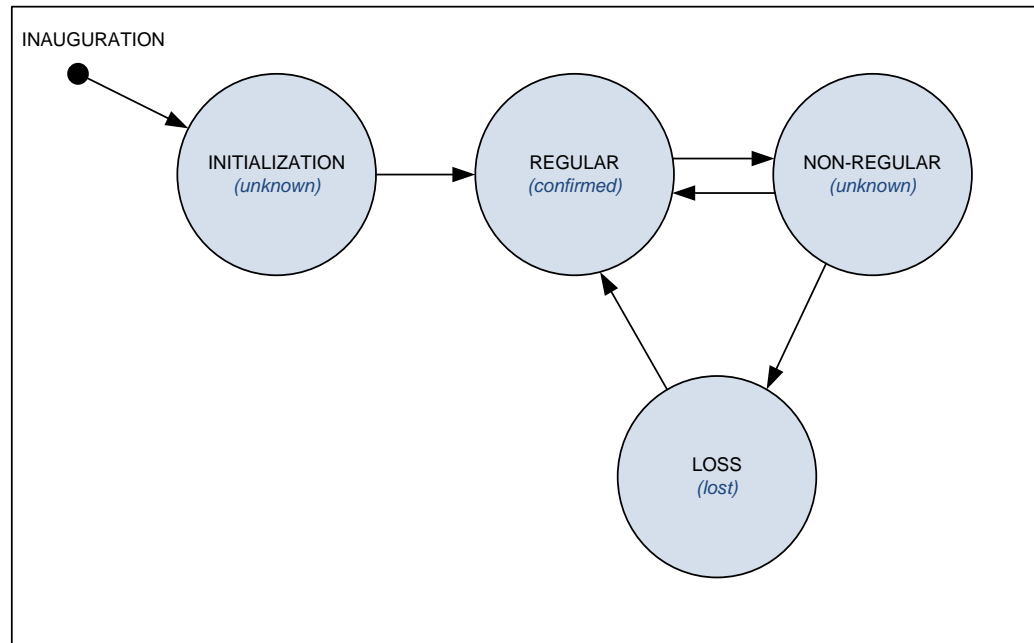


Figure 6-63 : OTI Master FSM in GNSS scenario

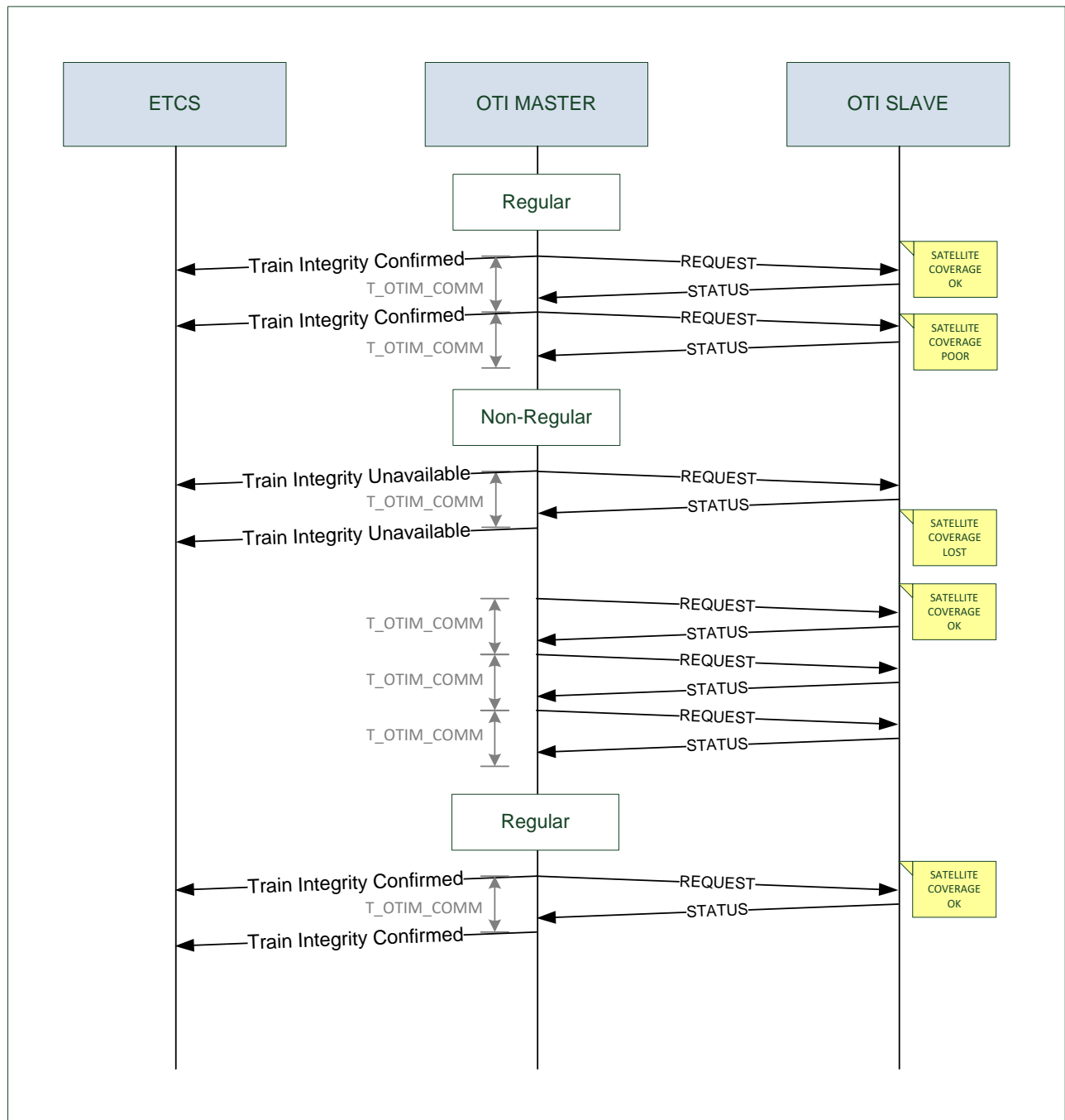


Figure 6-64 : Loss of coverage in GNSS scenario

- **Temporary localization error:**

- FSM Master shall remain in NON-REGULAR state until calculated train length differs from nominal train length for defined time and space thresholds;



- in case of reduced error in GNSS localization (i.e. within defined timeout) FSM shall go to REGULAR state thus sending confirmed train integrity information to ETCS and therefore allowing to restore normal operation;
- in case of expired time threshold, FSM shall go to LOSS state thus generating lost train integrity information to ETCS.

Finally a transition from LOST to REGULAR state need to be considered in OTI master FSM as recovery mechanism.

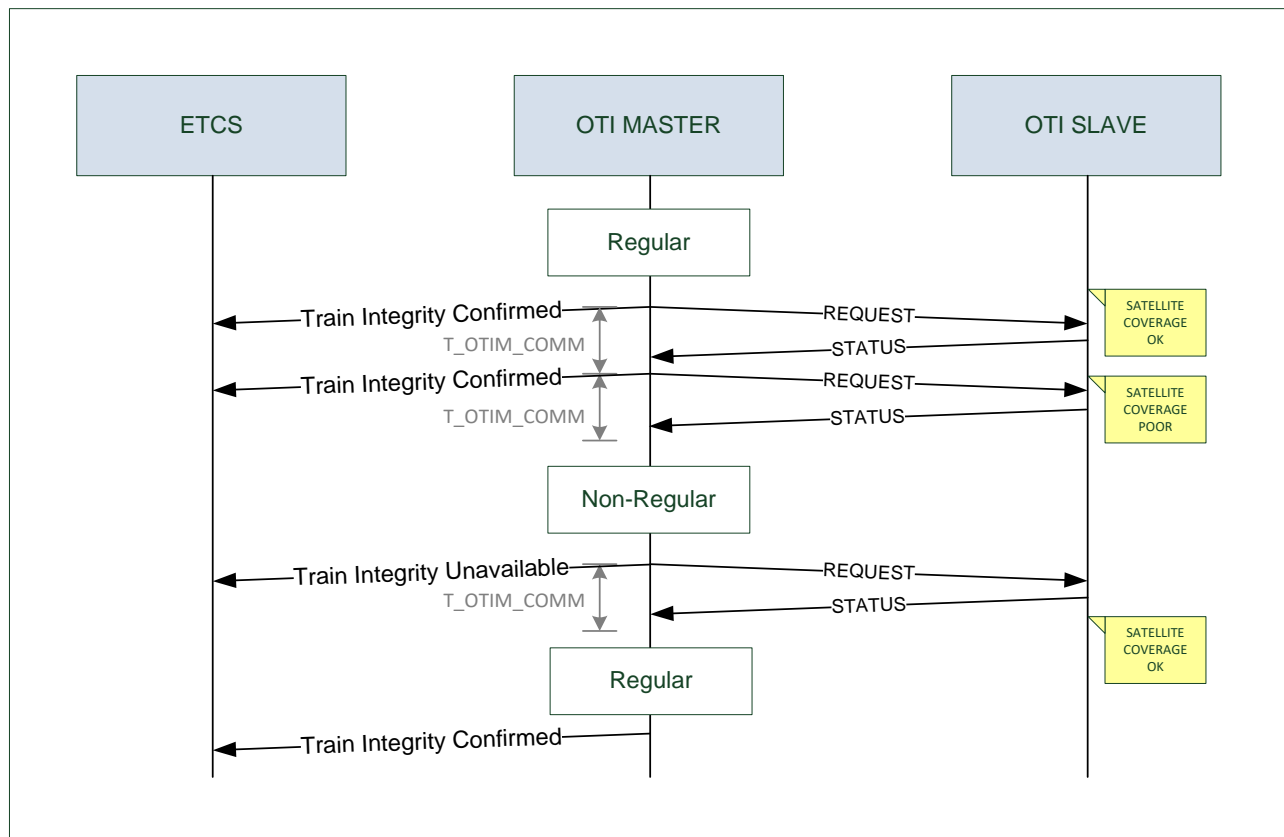


Figure 6-65: Localization error in GNSS scenario

#### 6.5.2.4 GNSS-based OTI function using GNSS data comparison method

This sub-chapter describes one of the potential functional realisation of the GNSS-based OTI function. Other uses of GNSS data are possible and the following description may not necessarily represent the most effective solution. Selection of the best approach is dependent on detailed both economic as well as technical analysis, which is beyond the scope of this study.

##### Assumptions:

- There is an accurate input of the train length provided by ETCS on-board unit to the OTI device.
- OTI device is comprised by the two major components:
  - 1) Front OTI device component: Installed in the front of the train and linked with ETCS on-board.
  - 2) Rear OTI device component: Installed at the very end of the train (end of rear waggon).
- Both OTI device components have an access to the electrical energy.
- Rear OTI device sends GNSS-based data to front OTI device wirelessly.
- Both OTI device components are equipped with GNSS Antenna, GNSS receiver, wireless communication and processing unit.
- Rear and Front OTI devices have implemented a mechanism for time synchronisation.

#### Functional allocation:

Front OTI device calculates and releases a final decision regarding the train integrity to the ETCS on-board unit. Rear OTI device collects the GNSS-based measured data and periodically sends them to the front OTI device. This approach may allow a lightweight design of Rear OTI device with minimised requirements regarding safety and energy consumption.

Front OTI device may benefit from an existing safe computation platform (supposedly installed in a driver cabin) as well as lowered energy consumption restrictions.

#### Main principle description:

Rear OTI device component periodically sends GNSS based data to the front OTI device component. Front OTI device component compares its own GNSS and/or odometry based data with those sent by the rear OTI device component. In case that GNSS data are not available (e.g. due to the tunnel) or are not in required quality from both OTI components, for the specific time, the train integrity will not be confirmed (train Integrity unknown). In case that front OTI device component can safely evaluate the consistency of its own measured data with those GNSS based available at the end of the train, the train integrity will be confirmed.

#### Evaluation whether the train is integer

OTI device can use the following values types:

- $D_{\text{TRAIN}}$  – Length of the train
- $P_{\text{FRONT}}(T_i)$  – GNSS-based position of the front OTI device, valid for time  $T_i$
- $P_{\text{REAR}}(T_i)$  – GNSS-based position of the rear OTI device, valid for time  $T_i$
- $V_{\text{FRONT}}(T_i)$  – GNSS and/or odometry-based velocity of the front OTI device, valid for time  $T_i$
- $V_{\text{REAR}}(T_i)$  – GNSS-based velocity of the rear OTI device, valid for time  $T_i$

The GNSS and/or odometry-based velocity information for the front OTI device in certain time  $V_{\text{FRONT}}(T_i)$  should be similar (within set limits) to the velocity information for the rear OTI device in certain time  $V_{\text{REAR}}(T_i)$ .

For the GNSS-based position comparison, front OTI device internally stores  $P_{\text{FRONT}}(T_i)$  data for the trajectory corresponding to the train length ( $D_{\text{TRAIN}}$ ). In case that the train is integer, the rear positioning data  $P_{\text{REAR}}(T_i)$  should copy the same trajectory as front positioning data  $P_{\text{FRONT}}(T_i)$ .

### Analysis

Principally, GNSS-based Velocity for the same Time obtained from the both components of the OTI device (front, rear) could be enough to evaluate whether the train is integer or not.

To increase a reliability and/or safety, front OTI device may utilise an on-board odometry and alternatively, Rear OTI device can integrate with microelectromechanical systems (MEMS) that are providing small and light inertial navigation systems (INS).

GNSS-based positioning can be add as an additional mechanism for confirming train integrity to increase a reliability / safety of the OTI function. This statement is based on the following assumptions:

- Redundancy: GNSS-based Position and Velocity can be derived in GNSS receiver using different physical principle. Although these variables are not independent, it is improbable that both will fail in the same way.
- Greater robustness towards the negative local environmental effects on GNSS signals: While the position will be compared for the very same location (shifted in time), the velocity will be measured for two different locations (front, rear). For the number of local influences (e.g. multipath effects), their influence on position comparison may be marginalised (subtracted from the equation).
- In case that GNSS signal will not be available for certain period of time (e.g. due to blockage), after recovery, the velocity information from both ends of the train may not be enough to safely confirm the train integrity.

### **6.5.3 Conclusions**

There are both economic and technical aspects that should be considered for introducing GNSS as a possible technology of choice for OTI device.

The study identified a number of technical challenges linked with the required level of reliability and safety of OTI function that should be effectively considered. Possible measures / solutions have been already identified in previous projects and will be further advanced by Shift2Rail experts within TD 2.4 activities. Some of the technical measures could be specific only for OTI function and will require an additional research and development effort.

Economic perspective is a crucial aspect for a decision whether GNSS can be regarded as a suitable technology for OTI function. The study demonstrates that there are certain technical

limitations of GNSS technology that limit its practical applicability for the complete range of railway applications. The main functional obstacle is a limited availability of GNSS signals in a typical railway line. Even though ETCS L3 moving block function can effectively deal with a temporary unavailability of train integrity confirmation (by virtually prolonging a train length), this state has a negative influence on line capacity. GNSS-based information is typically unavailable in all the situations where the GNSS antenna cannot reach a full sky visibility (e.g. tunnels, stations) or where sky visibility is significantly narrowed (e.g. urban canyons, forests). Therefore, it seems that GNSS is more suitable technology for low-density or specific freight lines, where track performance or high capacity is not a priority. For these applications, GNSS in combination with ETCS Level 3, may bring an interesting cost savings comparing to other solutions. In order to reach a cost effective solution and / or to compensate a temporary unavailability of GNSS signal, an integration with other COTS technologies, such as MEMS INS, may be considered.

For further and more detailed analysis of concrete technical GNSS-based OTI device solutions, it is necessary to formulate quantified requirements for external OTI function for ETCS L3 application, especially in terms of safety and performance. This input was not available during the period covering the work on this feasibility study.

## 7 Definition of Requirements

This section describes the functional requirements for On-board Train integrity functionality. Train length determination functionality is addressed at §8.

General note: the requirements specified in this section are still applicable even if an external device to ERTMS/ETCS On-board capable of providing the train length value is present on-board but for some reasons it is not able to provide a valid value of train length or it is in failure state. Otherwise, if the external device is able to provide a valid train length value then also the requirements specified in §8.7 shall be taken into account.

### 7.1 Functional Requirements Specification

ETCS regulation context relevant for OTI requirements specification is depicted in Figure 7-1.

- ETCS Logic is specified in SUBSET 026 [1].
- SUBSET 034 specify ETCS TIU including train integrity information [2]
- CR940 specify the requirements to manage the acquired train integrity information and the requirements to generate the Position Report messages to RBC [3]

The Scope of work of this section is to specify the requirements for OTI monitoring functional module that verify train integrity and communicate to ETCS TIU.

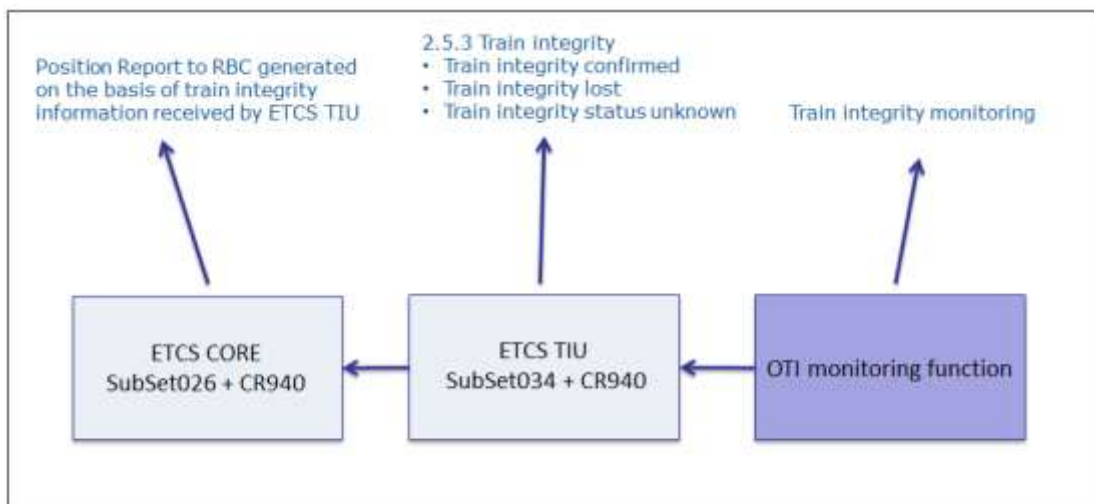
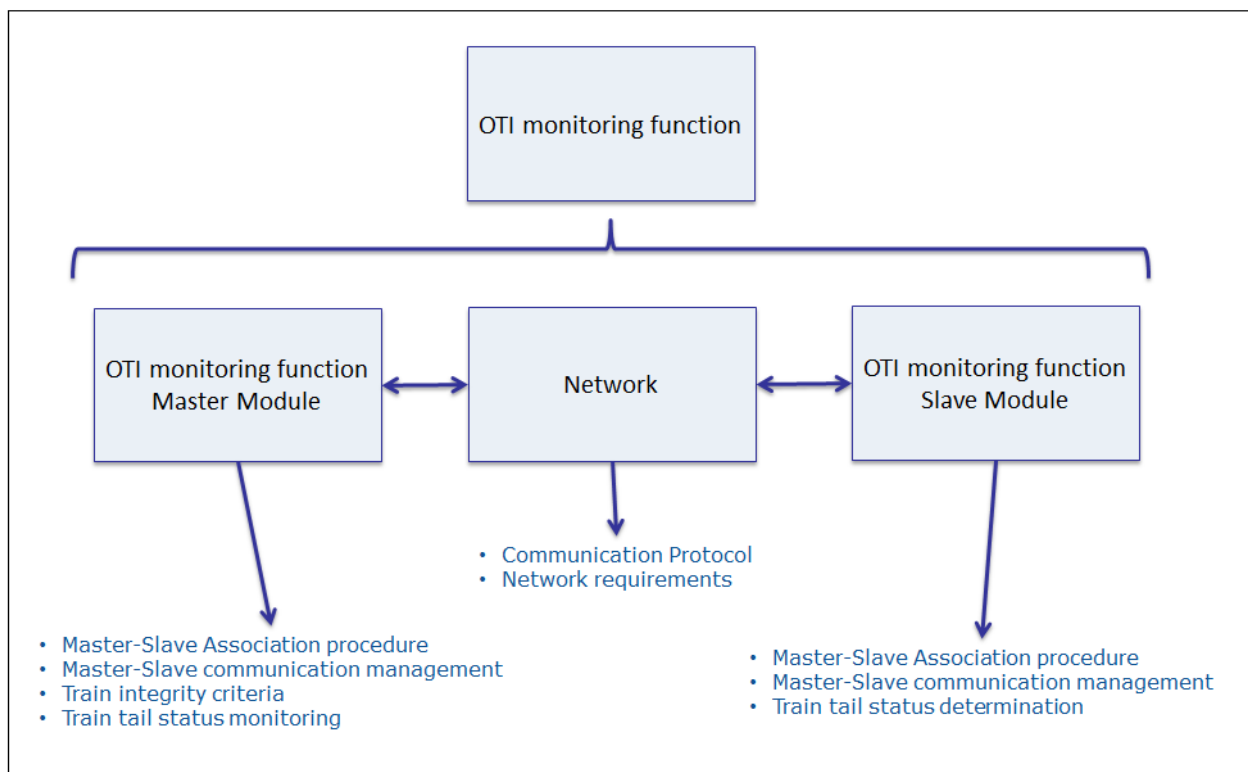


Figure 7-1 - ETCS regulations context for OTI

In general the OTI monitoring functional module, depicted in Figure 7-2, is composed of three functional parts: (i) OTI master functional module, (ii) on-board communication network and (iii) OTI slave module.



**Figure 7-2 - OTI functional module**

REQ\_7.1.1 OTI monitoring functional module shall be composed of the following functional modules:

- OTI Master (OTI-M)
- On-board Communication Network (OCN)
- OTI Slave (OTI-S)

REQ\_7.1.2 OTI monitoring functional module shall have a unique identifier OTI\_ID.

REQ\_7.1.3 OTI unique identifier OTI\_ID shall be the MAC address of OTI communication interface.

REQ\_7.1.4 OTI monitoring functional module shall include its unique identifier inside each transmitted message.

REQ\_7.1.5 At power-on, the OTI monitoring functional module shall manage a Mastership assignment procedure to assume Master or Slave role.

REQ\_7.1.6 After Mastership assignment procedure, the OTI monitoring functional module shall manage an inauguration phase composed of: (i) identification procedure and (ii) association procedure.

Note that Identification procedure is aimed at identifying all OTI modules connected to the OCN.

REQ\_7.1.7 After identification procedure, the OTI monitoring functional module shall manage association procedure to pair OTI Master in front cabin and OTI Slave at train tail.

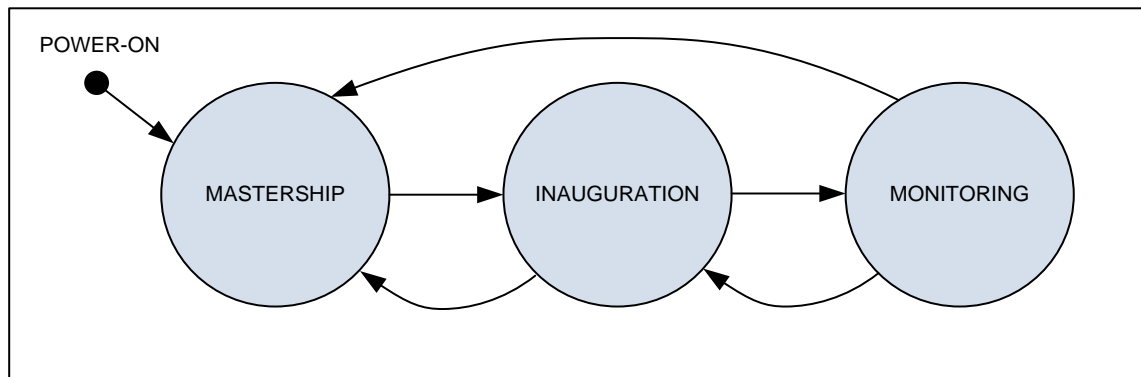
REQ\_7.1.8 Association procedure shall ensure that only one TAIL OTI Slave is present.

REQ\_7.1.9 After association procedure, the OTI monitoring functional module in monitoring state shall manage the communication between paired OTI Master and OTI Slave.

Note that Association procedure is aimed at ensuring that only OTI Slave module at train tail is active among all OTI Slave modules connected to OCN.

General high level FSM is depicted in Figure 7-3 composed of MASTERSHIP state aimed at identifying OTI module role (i.e. Master or Slave), INAUGURATION state aimed at pairing OTI Master module and OTI Slave module at train tail and MONITORING state aimed at performing train integrity monitoring.

Detailed FSM description for OTI Master and OTI Slave are reported at sections 7.1.1 and 7.1.5.



**Figure 7-3 - OTI Module: FSM High Level**

### 7.1.1 OTI Master Functional Module

OTI Master functional module, depicted in Figure 7-4, acquires the status of train tail from Slave module and verifies the coherence between train tail and front cabin movements. Detailed description of OTI Master high level functionalities are reported below in terms of in subsequent FSM and related requirements.

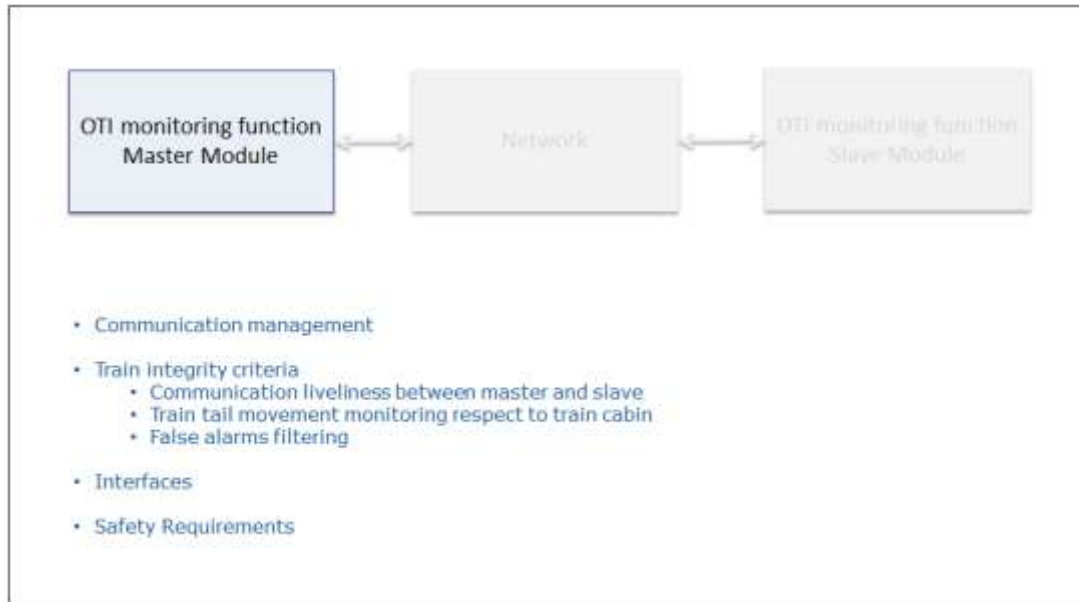


Figure 7-4 - OTI Master functional module

OTI Master high level Finite State Machine is depicted in Figure 7-5 (note: some transitions can be triggered by one or more events indicated by a number in a square bracket, e.g. [1]).

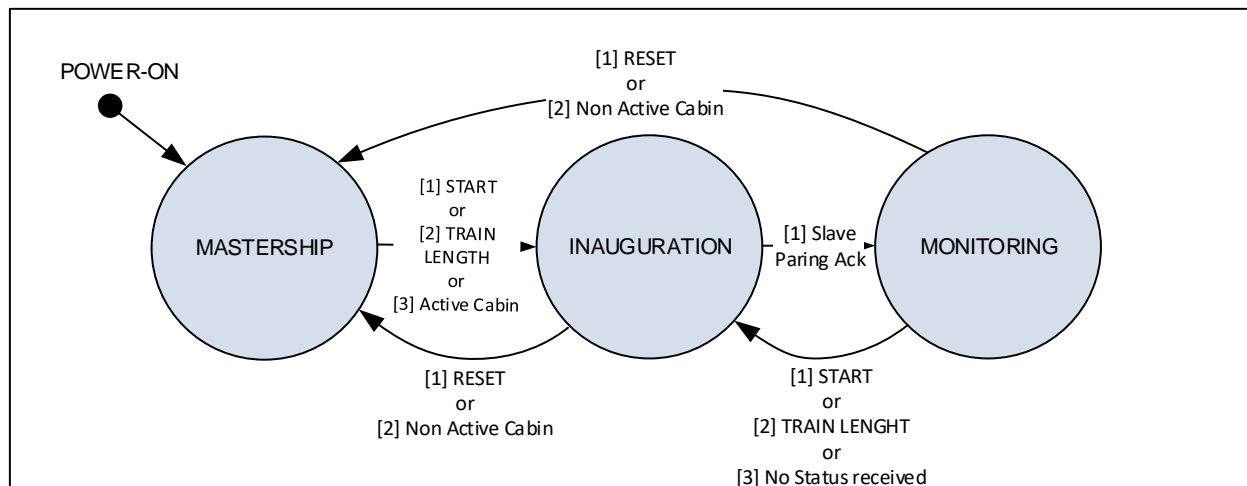


Figure 7-5 - OTI Master Module: FSM High Level



OTI Master FSM transitions are reported in Table 7-1. Notation “4>” means that condition 4 has to be fulfilled to trigger a transition from the state reported in column to the state reported in row and highlighted with the arrow “>”. For each cell, the arrow refers to the direction of the state transition and the number refers to the transition conditions. States are reported in blue cells with the following acronyms: MS = Mastership, IN = Inauguration, MN = Monitoring. Transition conditions are described in Table 7-2.

MS	<1	<4
>0	IN	<3
	2>	MN

**Table 7-1: OTI Master Module: FSM High Level Transitions**

Condition	Transition conditions from mode X to mode Y	Action in Y state
0	<b>From MASTERSHIP to INAUGURATION</b> OTI-M: START command received from ETCS or new Train Length received from ETCS or Active Cabin is acquired from rolling stock TIU.	OTI-M: MASTER role is acquired and “Identification Request” is sent to OTI Slave modules.
1	<b>From INAUGURATION to MASTERSHIP</b> OTI-M: RESET command received from ETCS or Non Active Cabin is acquired from rolling stock TIU.	OTI-M: Waits for START command or new Train Length or Active Cabin information.
2	<b>From INAUGURATION to MONITORING</b> OTI-M: OTI Master performed the paired with OTI Slave at train tail triggered by “Slave Pairing Ack” message from OTI Slave.	OTI-M: See FSM at section 7.1.1.3.
3	<b>From MONITORING to INAUGURATION</b> OTI-M: START command received from ETCS, or; new Train Length received from ETCS; or;	OTI-M: MASTER role is acquired and “Identification Request” is sent to OTI Slave modules.

	no Status messages received during the INITIALIZATION phase (see §7.1.1.3).	
4	<b>From MONITORING to MASTERSHIP</b> OTI-M: RESET command received from ETCS or Non Active Cabin is acquired from rolling stock TIU.	OTI-M: Waits for START command or Train Length from ETCS.

**Table 7-2: OTI Master module: FSM High Level Transition conditions**

The Table 7-3 below reports the priority between the states transition of the FSM described in Figure 7-5 if different transitions occur at the same time.

Px is the priority order. P1 has a higher priority than P2.

From:	To:	Comment
INAUGURATION	P1 => MASTERSHIP	Internal transition into INAUGURATON state (from “Identification” to “Pairing”) has a priority lower than transition to MASTERSHIP
	P2 => MONITORING	
MONITORING	P1 => MASTERSHIP	Any internal transition into MONITORING state (e.g. from “REGULAR” to “NON-REGULAR”) has a priority lower than transition to MASTERSHIP
	P2 => INAUGURATION	Any internal transition into MONITORING state (e.g. from “REGULAR” to “NON-REGULAR”) has a priority lower than transition to INAUGURATION

**Table 7-3: Priority table of OTI Master Module FSM**

#### 7.1.1.1 OTI Master Mastership State

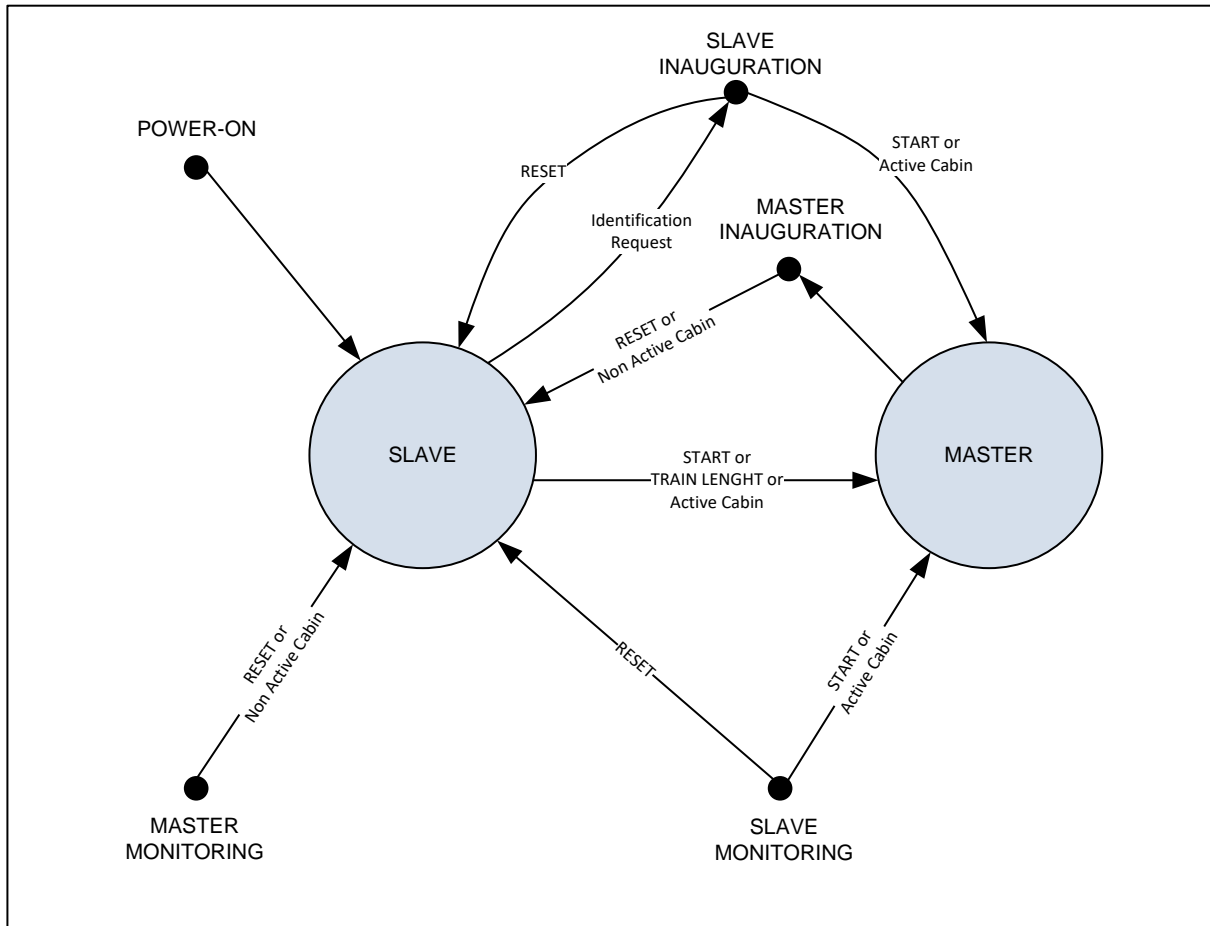
REQ\_7.1.1.1.1 OTI monitoring functional module shall behave as OTI Master or OTI Slave based on cabin status information.

REQ\_7.1.1.1.2 OTI monitoring functional module shall behave as OTI Master if connected to active cabin.

REQ\_7.1.1.1.3 OTI monitoring functional module shall behave as OTI Slave if connected to a non-active cabin OR if cabin status is not available.

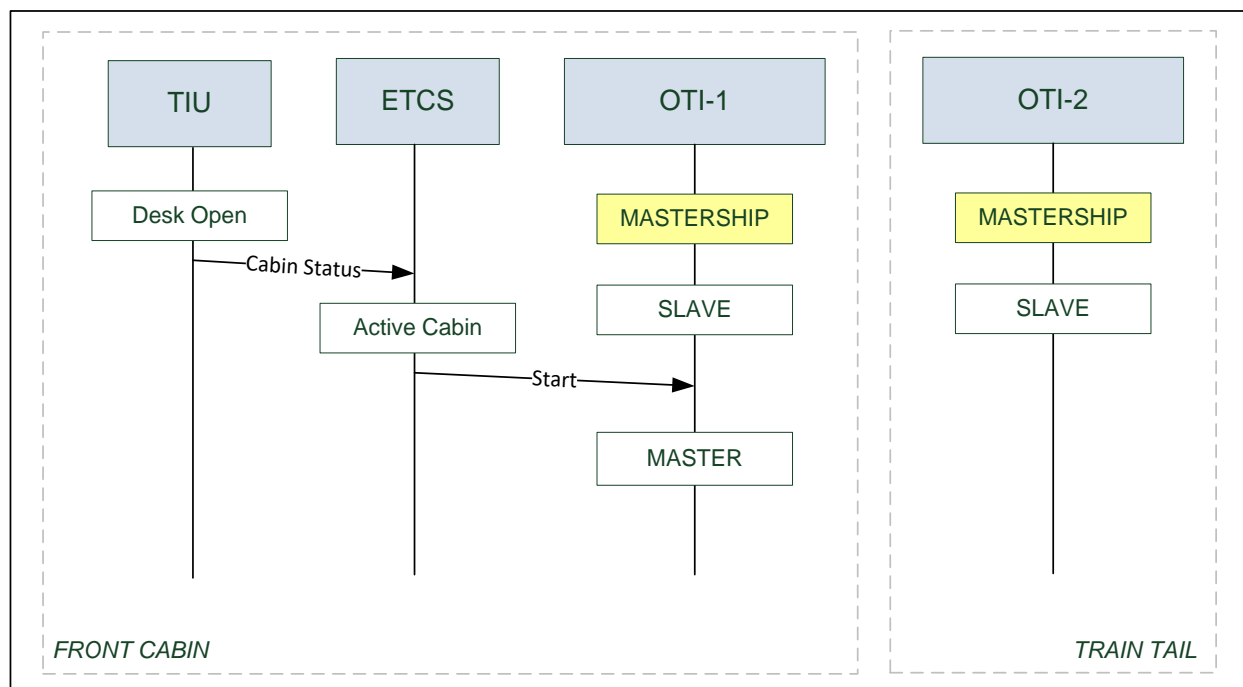
Note: the OTI Module connected to a slave engine in NON LEADING mode shall behave as OTI Slave.

Figure 7-6 depicts Mastership state and related transitions to other states described in details in subsequent sections.



**Figure 7-6 – OTI Master Module: Mastership state**

Figure 7-7 depicts an example of Mastership assignment with an on-board configuration including an OTI module in front cabin and an OTI module at train tail. More specifically ETCS TIU module sends a START command to OTI functional module in front cabin to trigger the transition to Master.

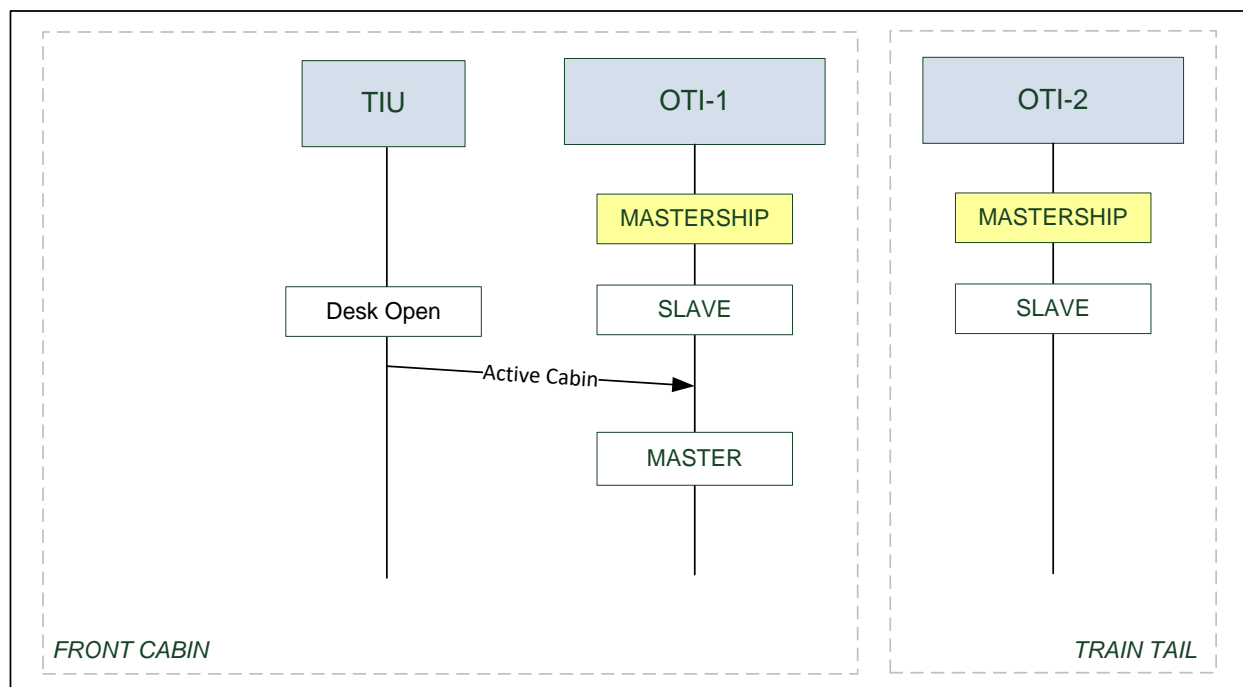


**Figure 7-7 – Mastership management – Example 1**

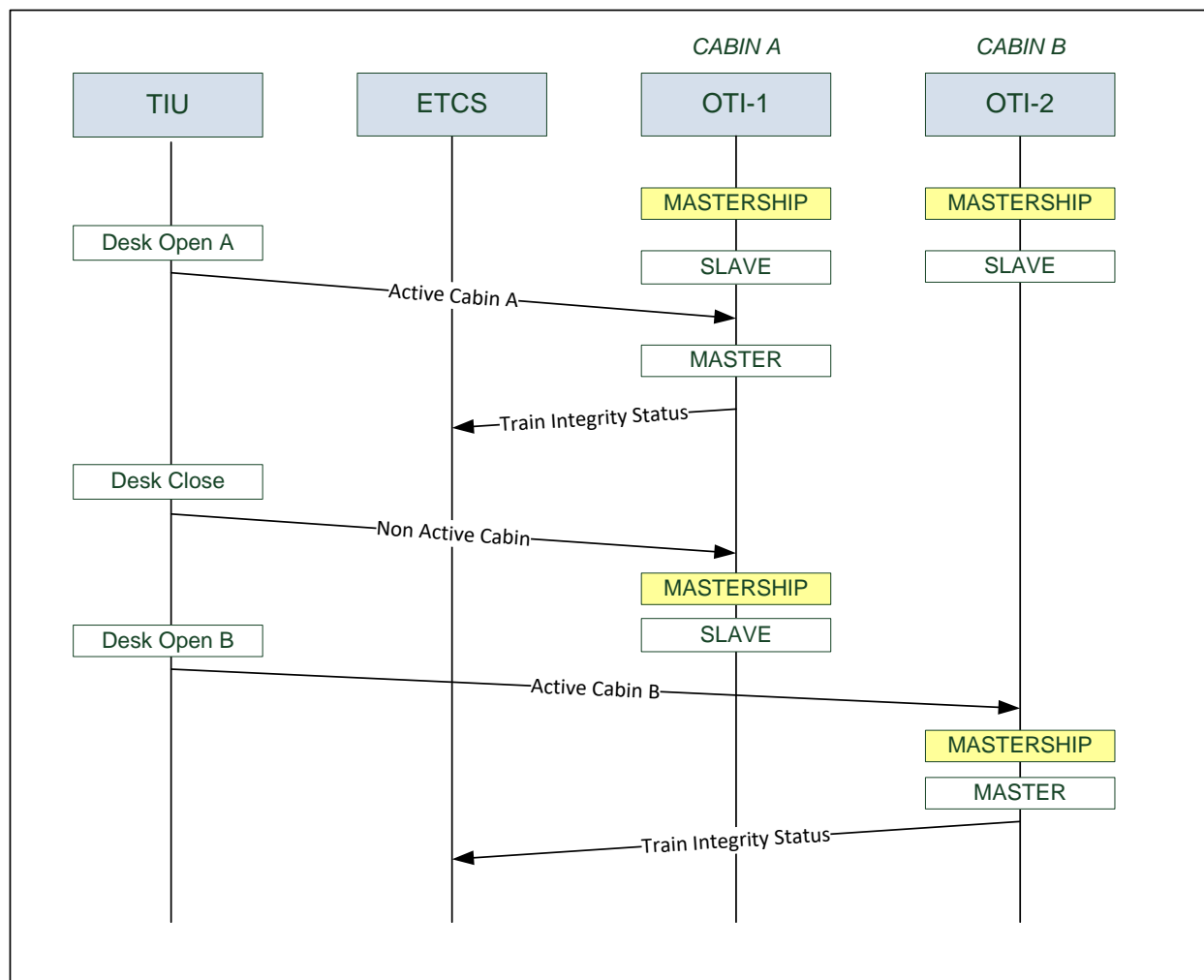
Figure 7-8 depicts an example of Mastership assignment with an on-board configuration including a central ETCS and two OTI modules for train set. More specifically ETCS TIU module uses Start and Reset commands to change OTI role between Master and Slave.



Page 165 of 511



**Figure 7-9 – Mastership management – Example 3**



**Figure 7-10 – Mastership management – Example 4**

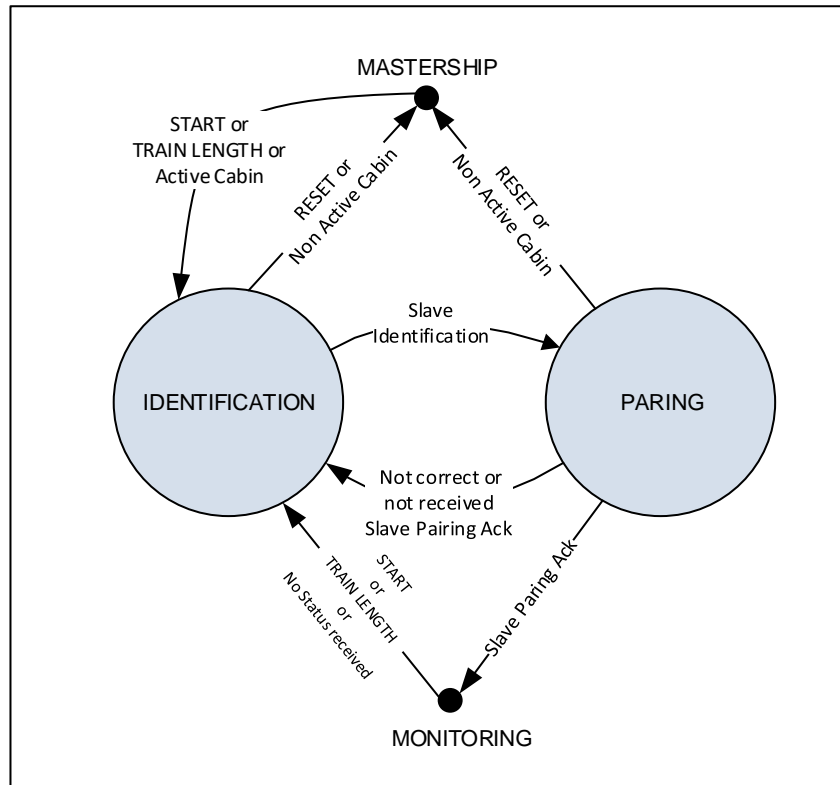
#### 7.1.1.2 OTI Master Inauguration State

Inauguration phase refers to: (i) identification of OTI modules connected to OCN and (ii) pairing between OTI Master in front cabin and OTI slave at train tail.

OTI Master shall send identification request messages to all OTI Slave modules and shall activate a pairing procedure only with OTI Slave module located at train tail.

START command from ETCS or TRAIN LENGTH from ETCS are trigger for inauguration process aimed at managing train joining and train splitting scenarios described at section 7.1.5.5.

Inauguration state is depicted in Figure 7-11 and includes an identification phase and a pairing phase.



**Figure 7-11 - OTI Master Module: Inauguration State**

REQ\_7.1.1.2.1 When the OTI Master transits to “Identification” state shall send an “Identification Request” as a broadcast message.

Note: if the wireless communication is performed with cellular networks, the OTI Master needs to know in advance the identifier of the OTI Slave TAIL (e.g. configuration parameter of info by trackside control center). In this case, the OTI Master shall contact directly the predefined OTI Slave TAIL. For more details refer to D4.2 [7].

REQ\_7.1.1.2.2 The OTI Master received the “Slave Identification Ack” message from the OTI Slave TAIL shall transit to “Pairing” state and it shall send a “Pairing Request” message only to the OTI Slave TAIL.

REQ\_7.1.1.2.3 The OTI Master in “Identification” state shall interrupt and repeat the Identification procedure if it receives two or more “Slave Identification Ack” messages from OTI Slave modules localized as “TAIL”.

Note that a timer shall be defined before declaring completed the Identification phase. This timer shall be dimensioned based on the specific application. If this timer has expired and the OTI Master has not received the “Slave Identification Ack” message from OTI Slave TAIL, then the OTI Master can restart the Identification procedure. For more details about communication between the OTI Modules refer to [7].



REQ\_7.1.1.2.4 The OTI Master in “Pairing” state shall accept the “Slave Pairing Ack” message only if:

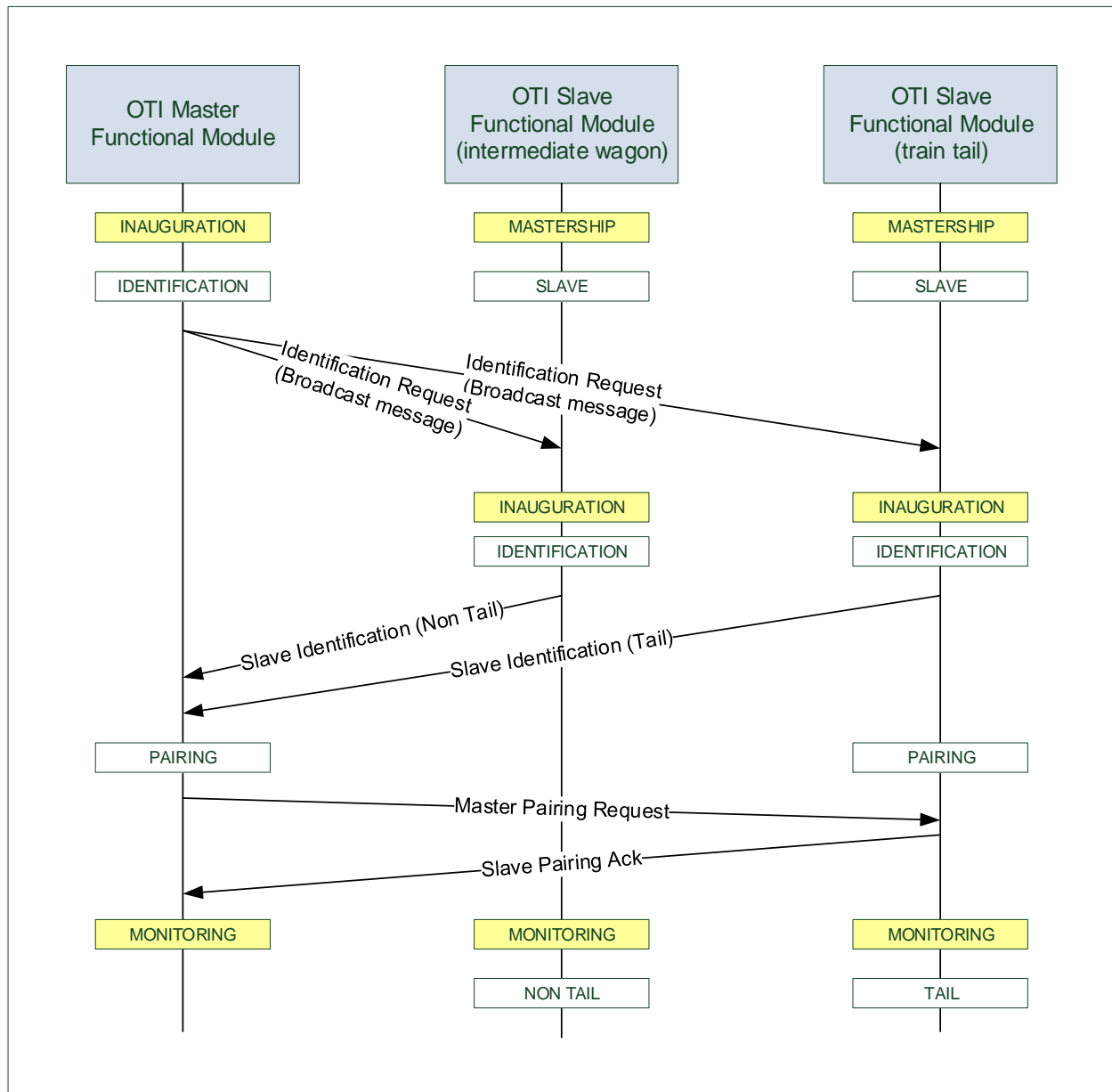
- a) the message is consistent (see REQ\_7.1.1.3.11) , AND;
- b) the message is sent by OTI Slave TAIL.

If the conditions a) and b) are not verified, the OTI Master shall reject the message and shall transit to “Identification” state.

REQ\_7.1.1.2.5 If the OTI Master in “Pairing” state does not receive the “Slave Pairing Ack” message then it shall transit to “Identification” state.

Note that a timer shall be defined for the “Pairing” state before OTI Master coming back to “Identification” state. This timer shall be dimensioned based on the specific application. For more details about communication between the OTI Modules refer to [7].

An example for inauguration phase is depicted in Figure 7-12.



**Figure 7-12 – Example of Master-Slave inauguration**

### 7.1.1.3 OTI Master Monitoring State

REQ\_7.1.1.3.1 Master Functional Module shall receive train tail status from OTI Slave Functional Module.

REQ\_7.1.1.3.2 OTI Master Functional Module shall check train tail status to verify train integrity.

Note that train integrity criteria are reported at section 7.1.1.5.

REQ\_7.1.1.3.3 OTI Master Functional Module shall provide train integrity information to ETCS TIU module.

Note that if OTI Master exits from Monitoring state due to an event described in Table 7-2, then it shall send to ETCS the information of train integrity status “unknown”.

REQ\_7.1.1.3.4 OTI Master Functional Module shall manage the communication with OTI Slave Functional Module according to FSM depicted in Figure 7-13 and according to transitions reported in Table 7-4 and transition conditions reported in Table 7-5.

REQ\_7.1.1.3.5 (OPTIONAL) OTI Master Functional Module shall acquire waggon/cargo diagnostic messages from OTI Slave modules.

REQ\_7.1.1.3.6 (OPTIONAL) OTI Master Functional Module shall determine train composition based on acquired waggon/cargo diagnostic messages from OTI Slave modules.

REQ\_7.1.1.3.7 (OPTIONAL) OTI Master Functional Module shall receive train composition from Wayside Maintenance Centre

Note that optional requirement related to train composition determination refers to two different cases: (i) OTI Slave provides composition data or (ii) Wayside Maintenance Centre provides train composition to OTI Master.

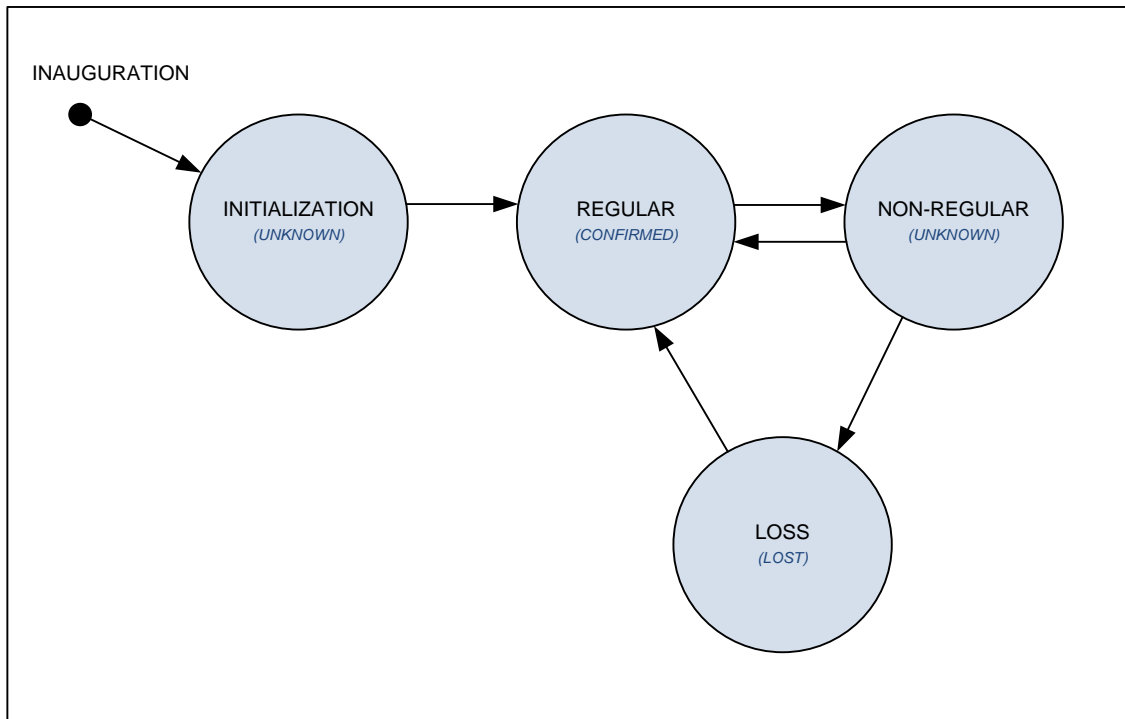
REQ\_7.1.1.3.8 (OPTIONAL) OTI Master Functional Module shall provide waggon/cargo diagnostic data to a Wayside Maintenance Centre.

REQ\_7.1.1.3.9 (OPTIONAL) OTI Master Functional Module shall provide waggon/cargo diagnostic data to train Driver.

Note that optional requirement related to providing cargo/waggon alarms to train Driver is aimed at reducing train Driver reaction time in case of emergencies.

REQ\_7.1.1.3.10 (OPTIONAL) OTI Master Functional Module shall record waggon/cargo diagnostic data received from OTI Slave modules.

Note that optional requirement related to recording cargo/waggon diagnostic data is aimed at managing situation of unavailable communication with Wayside Maintenance Centre.



**Figure 7-13 - OTI Master FSM – MONITORING STATE**

After the initialisation phase, the FSM transits to regular state that is the condition to confirm the train integrity. Non-regular state is introduced for false alarms filtering thus avoiding to impact regularity of the service.

Note that in freight scenarios with satellite based localisation the train tail localisation information could become temporary unavailable (e.g. temporary loss of satellites coverage). In this situation the FSM transits from Regular State to Non-Regular State and after a defined timeout, with non-available localisation, FSM transits to Loss State.

OTI Master FSM transitions are reported in Table 7-4. Notation “4>” means that condition 4 has to fulfilled to trigger a transition from the state reported in column to the state reported in row and highlighted with the arrow “>”. For each cell, the arrow refers to the direction of the state transition and the number refers to the transition conditions. States are reported in blue cells with the following acronyms: I = Initialization, R = Regular, NR = Non-Regular, L = Loss. Transition conditions are described in Table 7-5.

I			
1>	R	<3	<5
	2>	NR	
		4>	L

**Table 7-4: OTI Master: FSM Transitions**

Condition	Transition conditions from mode X to mode Y	Entry action in Y state
1	<b>Transition from I to R</b> (see REQ_7.1.1.3.13, REQ_7.1.1.3.14) <ul style="list-style-type: none"> <li>For Product Classes 1: OTI Master receives N% of consistent messages from paired OTI Slave within time-out T_OTIM_I.</li> <li>For Product Classes 2: OTI Master receives N% of consistent messages from paired OTI Slave within time-out T_OTIM_I and coherent train tail movement (see §7.1.1.5).</li> </ul>	Send to ETCS TIU the value <b>"Confirmed"</b> as Train Integrity Information.
2	<b>Transition from R to NR</b> <ul style="list-style-type: none"> <li>For Product Classes 1: OTI Master does not receive any message from paired OTI slave within time-out T_OTIM_COMM or receives a non-consistent message.</li> <li>For Product Classes 2: OTI Master does not receive any message from paired OTI slave or receives a non-consistent message within time-out T_OTIM_COMM or unavailable train tail movement for a time-out T_STATUS_TAIL or unavailable monitoring parameters for a time-out T_MONITORING_PARAM (e.g. no satellite coverage).</li> </ul>	<b>Send</b> to ETCS TIU the value <b>"Unknown"</b> as Train Integrity Information.
3	<b>Transition from NR to R</b> <ul style="list-style-type: none"> <li>For Product Classes 1: OTI Master receives a consistent message from paired OTI slave within time-out T_OTIM_COMM.</li> <li>For Product Classes 2:</li> </ul>	Send to ETCS TIU the value <b>"Confirmed"</b> as Train Integrity Information.

	OTI Master receives a consistent message from paired OTI slave within time-out T_OTIM_COMM or detect a coherent train tail movement (see §7.1.1.5).	
4	<b>Transition from NR to L</b> <ul style="list-style-type: none"> <li><u>For Product Classes 1:</u> OTI Master does not receives any consistent message from paired OTI slave within time-out T_OTIM_L.</li> <li><u>For Product Classes 2:</u> OTI Master does not receives any consistent message from paired OTI slave within time-out T_OTIM_L or detect a non-coherent train tail movement (see §7.1.1.5).</li> </ul>	Send to ETCS TIU the value “ <b>Lost</b> ” as Train Integrity Information.
5	<b>Transition from L to R</b> (see REQ_7.1.1.3.13, REQ_7.1.1.3.15, REQ_7.1.1.3.16) <ul style="list-style-type: none"> <li><u>For Product Classes 1:</u> OTI Master receives M% of consistent messages from paired OTI Slave within time-out T_OTIM_R.</li> <li><u>For Product Classes 2:</u> OTI Master receives M% of consistent messages from paired OTI Slave within time-out T_OTIM_R and detect a coherent train tail movement (see §7.1.1.5).</li> </ul>	Send to ETCS TIU the value “ <b>Confirmed</b> ” as Train Integrity Information.

**Table 7-5: OTI Master: FSM Transitions conditions**

REQ\_7.1.1.3.11 A message shall be considered as consistent if compliant to communication protocol.

Note: refer to [7] for more details about the communication protocol.

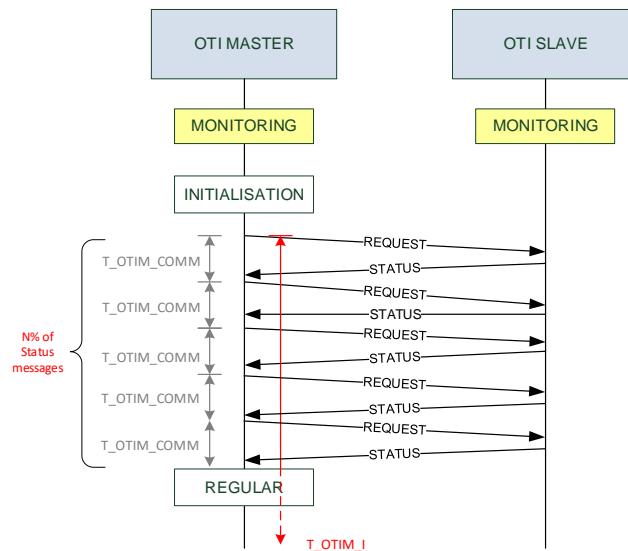
REQ\_7.1.1.3.12 N, M, T\_OTIM\_I, T\_OTIM\_COMM, T\_OTIM\_L, T\_OTIM\_R, T\_STATUS\_TAIL, T\_MONITORING\_PARAM shall be configuration parameters.

Values for configuration parameter shall be defined at design phase. In general configuration parameter values are fixed during a train mission.

REQ\_7.1.1.3.13 Parameters N% or M% are intended as percentages of messages respect to overall messages received in a defined time-out.

REQ\_7.1.1.3.14 Transition from INITIALIZATION to REGULAR is performed as soon as N% of Status consistent messages have been received by OTI-M.

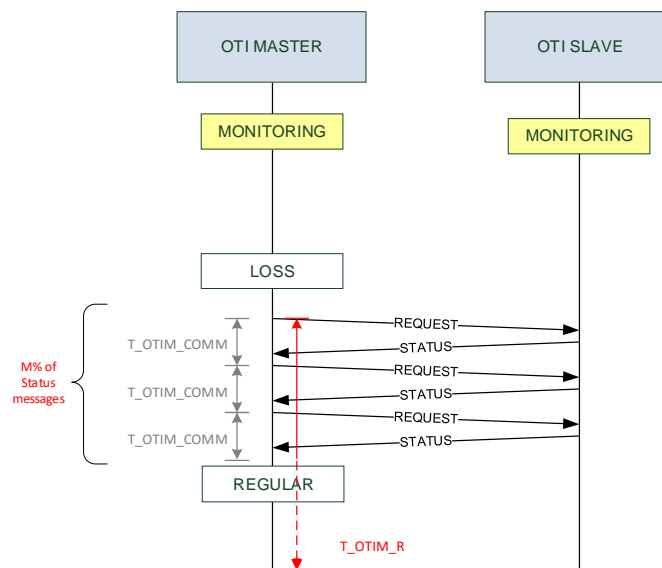
As example Figure 7-14 depicts a transition from INITIALIZATION to REGULAR performed before timer T\_OTIM\_I expires.



**Figure 7-14: Example of transition from Init to Regular before T\_OTIM\_I expires**

REQ\_7.1.1.3.15 Transition from LOSS to REGULAR is performed as soon as M% of Status consistent messages have been received by OTI-M.

As example Figure 7-15 depicts a transition from LOSS to REGULAR performed before that timer T\_OTIM\_R expires.

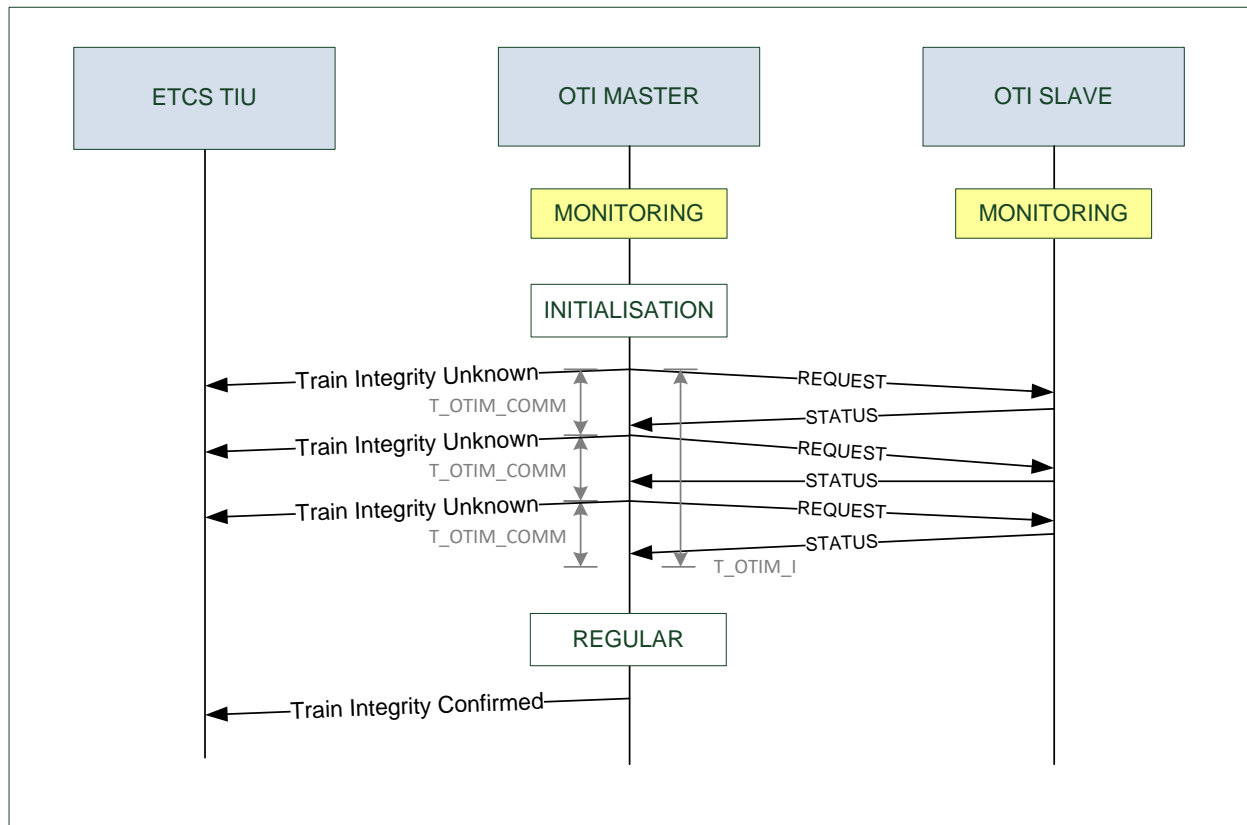


**Figure 7-15: Example of transition from Loss to Regular before T\_OTIM\_R expires**

REQ\_7.1.1.3.16 In case OTI Master does not receive M% of consistent messages from paired OTI Slave within time-out T\_OTIM\_R, then OTI Master shall remain in LOSS state until a condition described in Table 7-2 is verified.

#### 7.1.1.4 Sequence diagrams examples

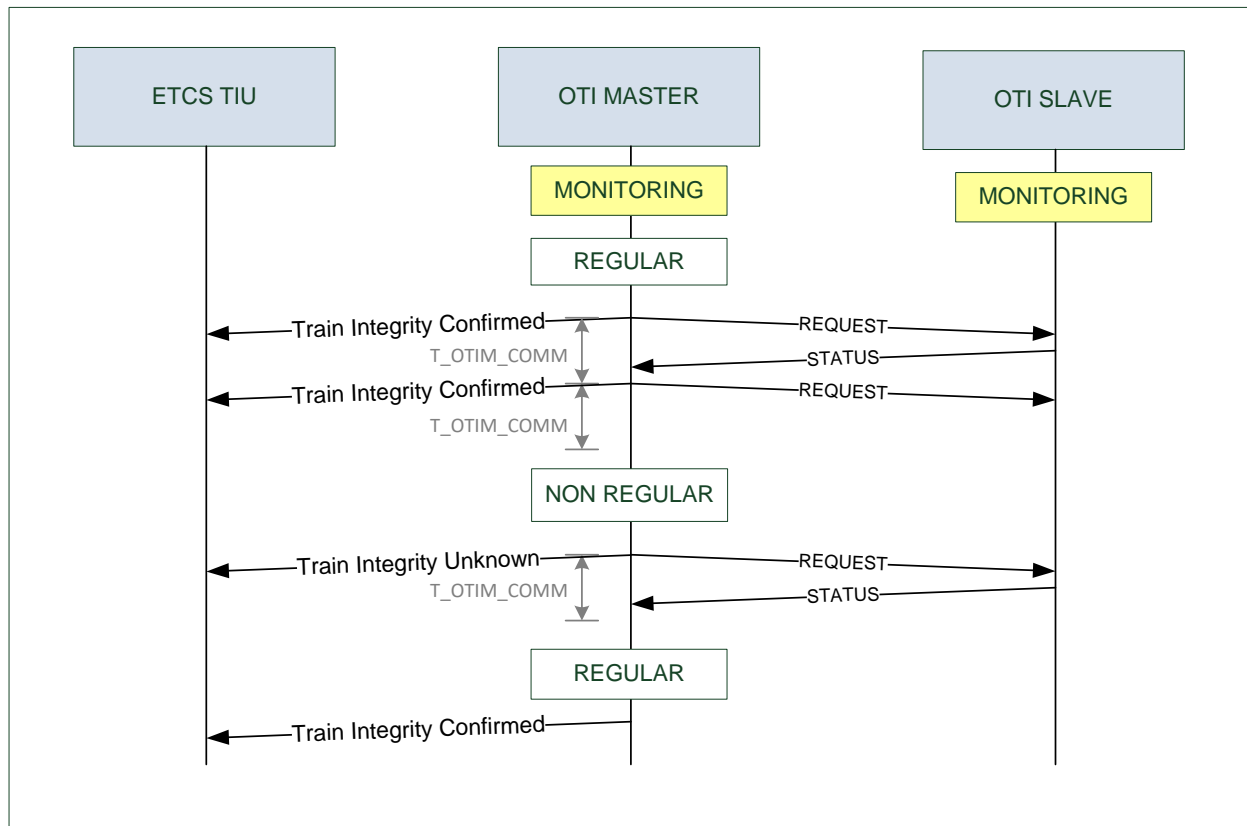
This section contains examples of sequence diagrams depicting some state transition in OTI Master FSM. Figure 7-16 refers to transition from INITIALISATION state to REGULAR state.



**Figure 7-16 – OTI Master Sequence Diagram: Initialisation**

Figure 7-17 depicts transition from REGULAR state to NON REGULAR state and vice versa related to a false alarm filtering situation.





**Figure 7-17 – OTI Master Sequence Diagram: False alarm filtering**

Figure 7-18 depicts a transitions to LOSS state due to loss of communication and then a transition to REGULAR referring to a restored communication (e.g. temporary network overload).

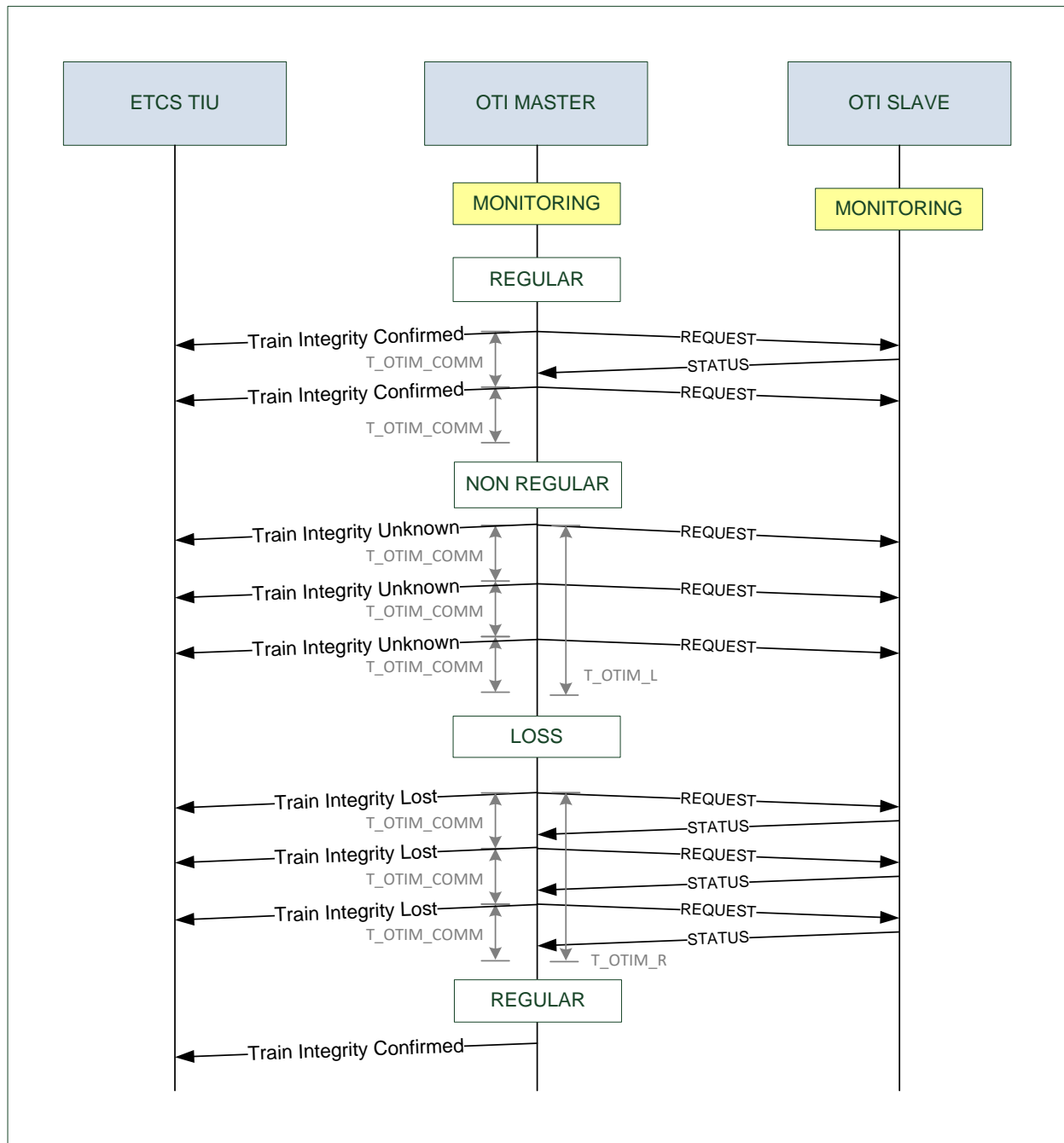


Figure 7-18 – OTI Master Sequence Diagram: Loss and Restore

#### 7.1.1.5 Train Integrity Criteria

Train integrity criteria depends on on-board communication network type (i.e. wired or wireless).

In case of wired network the train integrity criteria is based on communication status (e.g. regular exchange of liveness messages).

In case of wireless network the train integrity criteria is based on verifying communication status and train tail status (i.e. train tail movement coherent with front cabin) based on train tail odometry data.

In case of wireless on-board communication network, the OTI Master shall evaluate the train tail movement coherence by checking that difference between position or speed or acceleration of train tail and front cabin is below a defined threshold.

REQ\_7.1.1.5.1 OTI Master Functional Module, in case of wireless communication network, shall consider train tail movement as “coherent” if OTI Slave status is regular and one of the following conditions are verified:

- difference between train tail position and front cabin position is equal to train length with a tolerance of POSITION\_TOLERANCE  
OR
- difference between train tail speed and front cabin speed is below a defined threshold  
SPEED\_TOLERANCE  
OR
- difference between train tail acceleration and front cabin acceleration is below a defined threshold  
ACCELERATION\_TOLERANCE

REQ\_7.1.1.5.2 POSITION\_TOLERANCE, SPEED\_TOLERANCE and ACCELERATION\_TOLERANCE shall be configuration parameters.

REQ\_7.1.1.5.3 In case of wired network, the Train integrity criterion is based on communication liveness between train tail and front cabin.

#### 7.1.1.6 Interfaces

REQ\_7.1.1.6.1 OTI Master Functional Module shall be able to acquire active cabin information or train length information or START/RESET commands.

Note: as depicted in Figure 7-9 and Figure 7-10, the OTI Module can acquire the cabin status information directly from TIU. This option permits the ETCS backward compatibility as explained in [7].

REQ\_7.1.1.6.2 OTI Master Functional Module shall provide to ETCS TIU functional module the train integrity information according to CR940 [3] with the following three values:

- Train integrity confirmed
- Train integrity lost

- Train integrity status unknown

REQ\_7.1.1.6.3 OTI Master shall communicate with OTI Slave at train tail for train integrity monitoring.

REQ\_7.1.1.6.4 (optional) OTI Master shall communicate with OTI Slaves for waggon/cargo diagnosis.

REQ\_7.1.1.6.5 (optional) OTI Master shall communicate with Wayside Maintenance Centre.

REQ\_7.1.1.6.6 (optional) OTI Master shall provide to train Driver waggon/cargo alarms.

REQ\_7.1.1.6.7 OTI Master shall provide On-Board Train Integrity Status and OTI device status to an OTI Dashboard

REQ\_7.1.1.6.8 OTI Master shall acquire active cabin and non-leading information from vehicle interface.

#### **7.1.1.7 Safety Requirement**

REQ\_7.1.1.7.1 OTI Master Functional Module shall be SIL4 in relation to Mastership management, inauguration phase and train integrity monitoring.

REQ\_7.1.1.7.2 The OTI Master shall not accept information received by other OTI modules configured as Master.

REQ\_7.1.1.7.3 In case of wireless communication, the OTI Master shall know the ID of OTI Slave with which a pairing procedure will be initiated.

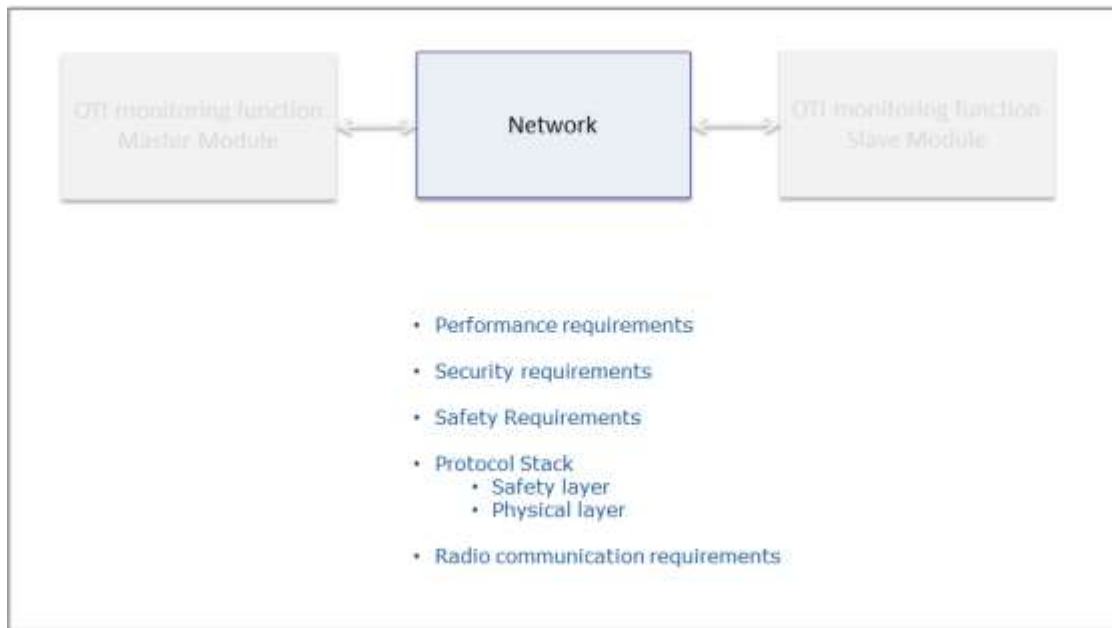
REQ\_7.1.1.7.4 (optional) If the OTI modules manage diagnostic information, the communication protocol between OTI modules shall use different messages for diagnostic and train integrity information.

REQ\_7.1.1.7.5 Packets exchanged between the OTI modules shall include a field that specifies the OTI identifier (OTI ID) and the OTI role (Master / Slave TAIL / Slave Non TAIL).

REQ\_7.1.1.7.6 OTI identifier shall be unique for each OTI module.

### **7.1.2 Network Functional Module**

Network functional module, depicted in Figure 7-19, refers to communication between OTI Master and OTI Slave modules and its detailed specification is reported at section 7.3.



**Figure 7-19 – Network functional module**

Network shall be no-safety related and communication safety shall be in charge to OTI module protocol stack.

Protocol stack implemented by OTI module shall be composed of:

- Application level managing OTI functionalities
- Safety Layer to ensure communication safety
- COTS lower layers

In general the application layer and safety layer are implemented in a safe processing unit, whereas no safety requirements are related to COTS lower layers. An example for OTI protocol stack is Safety Layer Euro-radio over TCP/IP [4].

Detailed interface specification is reported in D4.2 [7].

### **7.1.3 On-board Communication Network**

This section contains general requirements for an on-board communication network (wired or wireless) suitable for OTI functionality. In following, the On-board Communication Network is referred as OCN.

REQ\_7.1.3.1 OCN shall be non-vital.

REQ\_7.1.3.2 OCN shall support messages exchange between OTI master module and OTI slave modules.

REQ\_7.1.3.3 OCN shall support communication for a maximum number of  $N$  OTI modules.

Maximum number of OTI modules  $N$  depends on the specific application.

Note: Maximum number of OTI modules to be defined taking into account the product class 2C with waggon/cargo diagnosis (e.g. some hundreds).

REQ\_7.1.3.4 OCN shall support messages exchange with a rate of  $T$  sec.

Note that *transmission rate*  $T$  depends on the specific application. As example in passenger application, the rate could be around 1 sec and longer periods could be selected in freight applications.

REQ\_7.1.3.5 OCN shall support messages exchange with a size of  $S$  bytes.

Note that *message size*  $S$  depends on the application message size and protocol stack overhead. As example application message for product class 1 shall include only OTI Slave status, whereas product class 2-B shall include cargo/waggon diagnostic information.

REQ\_7.1.3.6 OCN shall ensure a transmission latency less than  $L$  sec.

*Note that transmission latency  $L$  depends on the transmission rate. As example passenger application with master slave communication mechanism and transmission rate of 1 sec.*

REQ\_7.1.3.7 OCN shall ensure communication between train tail and front cabin in LNOS situations in case of wireless communication.

REQ\_7.1.3.8 OCN shall provide high availability level.

Note that availability level of communication network impacts on overall availability of on-board train integrity functionality and therefore on overall railway service availability and capacity.

REQ\_7.1.3.9 OCN shall provide a mechanism to check that there are no connections between nodes of different trains.

#### **7.1.4 On-board Communication Protocol (OCP)**

This section contains general requirements related to safe communication protocol implemented by OTI modules. Same approach is applicable also to interface between OTI Master and ETCS. In general, the protocol stack implemented by OTI module shall be composed of:

- Application level managing OTI functionalities
- Safety Layer to ensure SIL4 communication
- COTS lower layers

REQ\_7.1.4.1 OCP shall be implemented by OTI module.

REQ\_7.1.4.2 OCP shall be defined to support SIL4 communication.

REQ\_7.1.4.3 OCP shall comply with CENELEC 50159 [5].

Detailed description of protocol stack is addressed in D4.2 [7] including security requirements.

Standard interface between OTI-M and OTI-S shall be proposed thus ensuring interoperability between products from different suppliers. Same approach is applicable also to interface between OTI Master and ETCS.

*Note: An example of existing safe protocol is Euro-radio safety layer [4].*

#### **7.1.4.1 Application Layer**

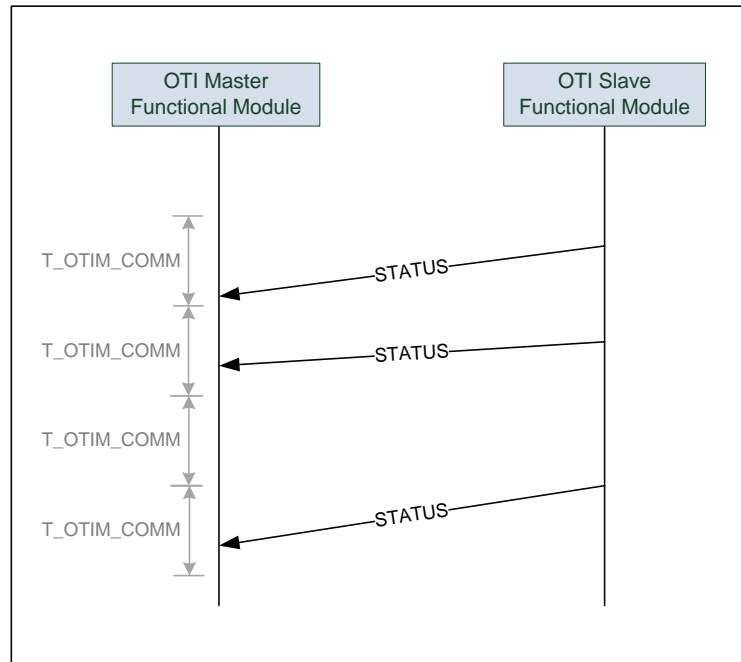
Application layer shall implement master-slave communication aimed at exchanging communication liveliness messages, status messages and diagnostic messages.

One possible approach consists in OTI Slave generating autonomously and periodically liveliness messages, however this solution does not keep into account the communication latency time and does not allow verifying the freshness of liveliness messages provided by OTI Slave.

Another alternative consists in adopting a master slave communication with OTI Slave generating messages only as answer to explicit requests from OTI Master.

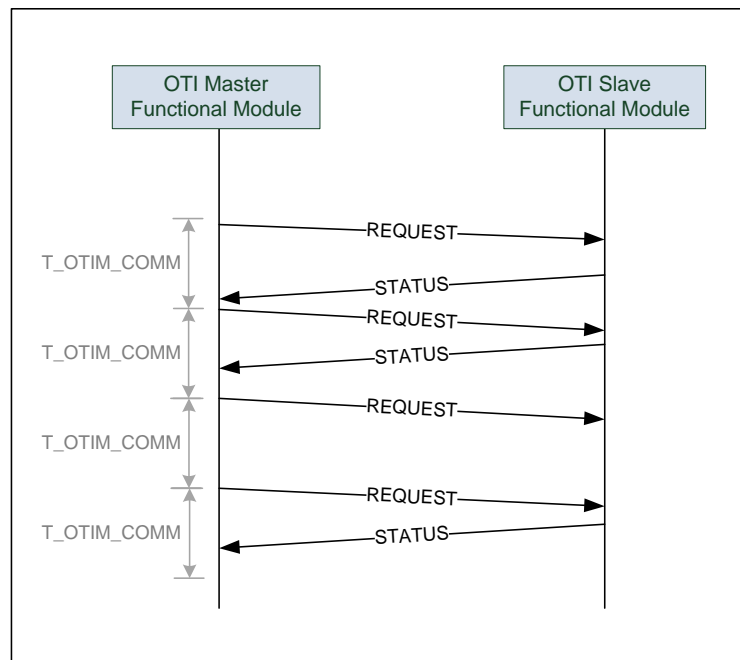
Assigning liveliness and time management to lower layer of protocol stack introduced relevant constraints to protocol stack and to on-board communication network.

Figure 7-20 depicts an example of asynchronous master-slave communication with OTI Slave generating autonomously status messages to OTI Master. This mechanism prevents OTI Master verifying freshness of received status message.



**Figure 7-20 – Example of asynchronous Master-Slave communication**

Figure 7-21 depicts an example of synchronous master-slave communication with OTI Master interrogating periodically the OTI Slave that provides an answer for each request received from OTI Master.



**Figure 7-21 – Example of synchronous Master-Slave communication**



REQ\_7.1.4.1.1 OTI Master shall start communication with OTI Slave.

REQ\_7.1.4.1.2 OTI Master shall send liveliness REQUEST messages to OTI Slave.

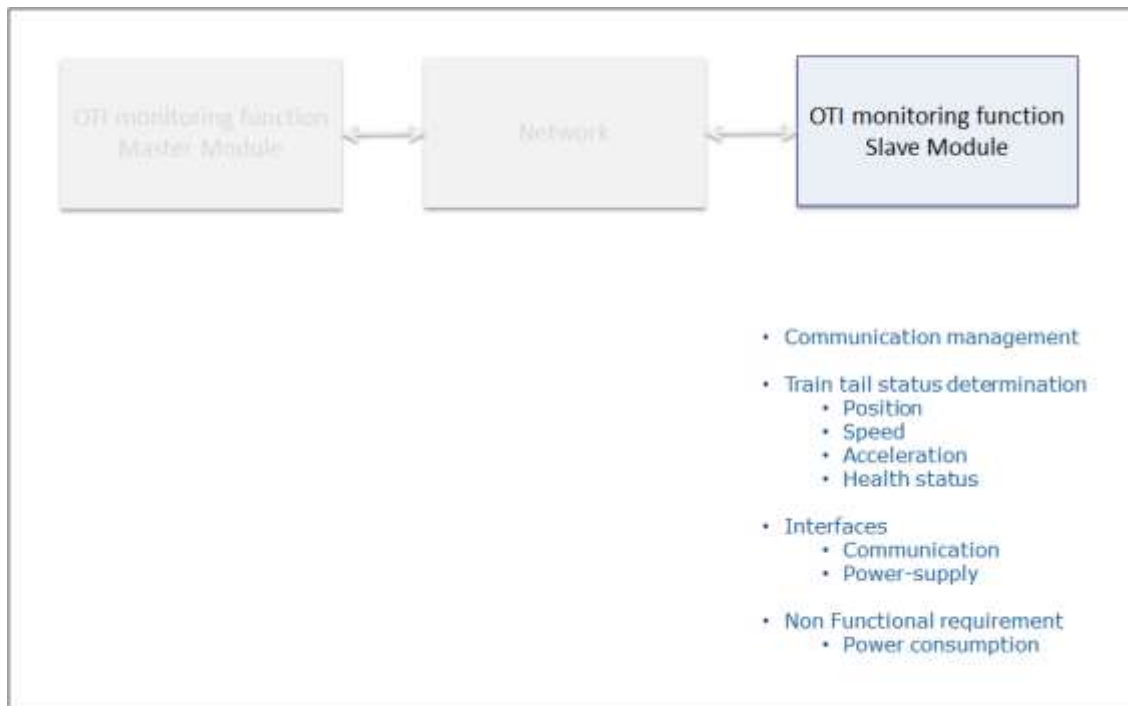
REQ\_7.1.4.1.3 OTI Master shall send liveliness REQUEST after that T\_OTIM\_COMM timeout is expired.

REQ\_7.1.4.1.4 OTI Master shall wait for an answer from OTI Slave for a time T\_OTIM\_COMM defined as configuration parameter.

REQ\_7.1.4.1.5 OTI Slave shall answer to liveliness REQUEST from OTI Master with a liveliness STATUS message.

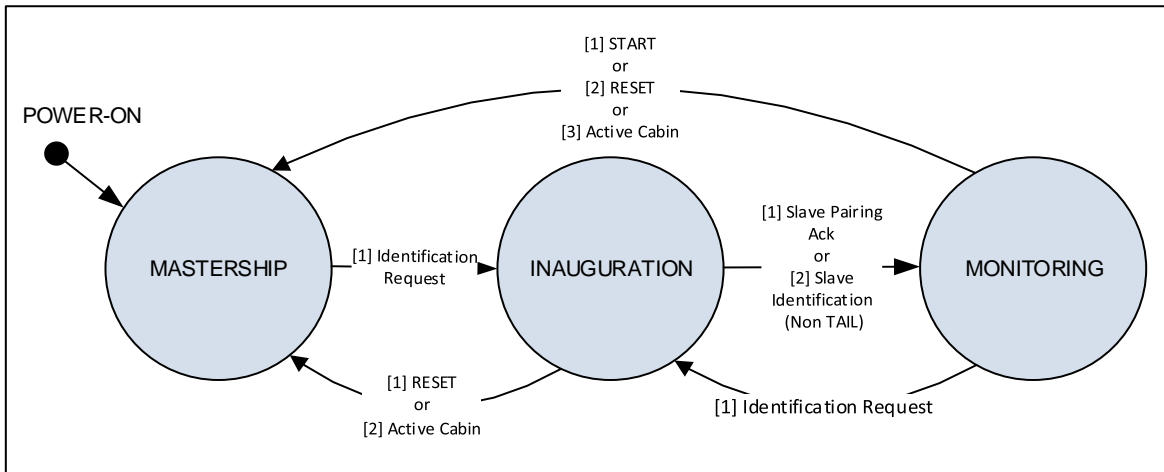
### 7.1.5 OTI Slave Functional Module

OTI Slave functional module, depicted in Figure 7-22, determines the status of train tail and communicate this information to OTI Master Module. Detailed description of OTI Slave high level functionalities are reported below in terms of FSM and related requirements.



**Figure 7-22 - OTI Slave functional module**

OTI Slave high level Finite State Machine is depicted in Figure 7-23 (note: some transitions can be triggered by one or more events indicated by a number in a square bracket, e.g. [1]).



**Figure 7-23 - OTI Slave Module: FSM**

OTI Slave FSM transitions are reported in Table 7-6. Notation “4>” means that condition 4 has to be satisfied to active transition from the state reported in column to the state reported in row and highlighted with the arrow “>”. For each cell, the arrow refers to the direction of the state transition and the number refers to the transition conditions. States are reported in blue cells with the following acronyms: MS = Mastership, IN = Inauguration, MN = Monitoring. Transition conditions are described in Table 7-7.

MS	<1	<4
>0	IN	<3
	2>	MN

**Table 7-6: OTI Slave Module: FSM Transitions**

Condition	Transition conditions from mode X to mode Y	Action in Y state
0	<b>From MASTERSHIP to INAUGURATION</b> OTI-S: “Identification Request” message received.	OTI-S: Provides “Slave Identification Ack” message to OTI Master as answer to received “Identification Request” message.
1	<b>From INAUGURATION to MASTERSHIP</b>	

	OTI-S: RESET command received from ETCS or Active Cabin is acquired from rolling stock TIU.	OTI-S: 1) Becomes MASTER if Active Cabin information is acquired from TIU; or; 2) Remains in Slave if RESET command is received.
2	<b>From INAUGURATION to MONITORING</b>  OTI-S: OTI Slave performed the paired with OTI Master or OTI Slave is Non-TAIL.	OTI-S: See FSM at section 7.1.5.2
3	<b>From MONITORING to INAUGURATION</b>  OTI-S: "Identification Request" sent by OTI Master.	OTI-S: Provides "Slave Identification Ack" message to OTI Master as answer to received "Identification Request" message.
4	<b>From MONITORING to MASTERSHIP</b>  OTI-S: START or RESET command received from ETCS or Active Cabin is acquired from rolling stock TIU.	OTI-S: Acquires MASTER role if it receives START o Active cabin information, otherwise remains Slave.

**Table 7-7: OTI Slave Module: FSM Transitions conditions**

Mastership state is described at sections 7.1.1.1.

The Table 7-8 below reports the priority between the states transition of the FSM described in Figure 7-23 if different transitions occur at the same time.

Px is the priority order. P1 has a higher priority than P2.

From:	To:	Comment
INAUGURATION	P1 => MASTERSHIP	Internal transitions into INAUGURATON state (e.g. from "Identification" to "Pairing") have a priority lower than transition to MASTERSHIP
	P2 => MONITORING	
MONITORING	P1 => MASTERSHIP	
	P2 => INAUGURATION	

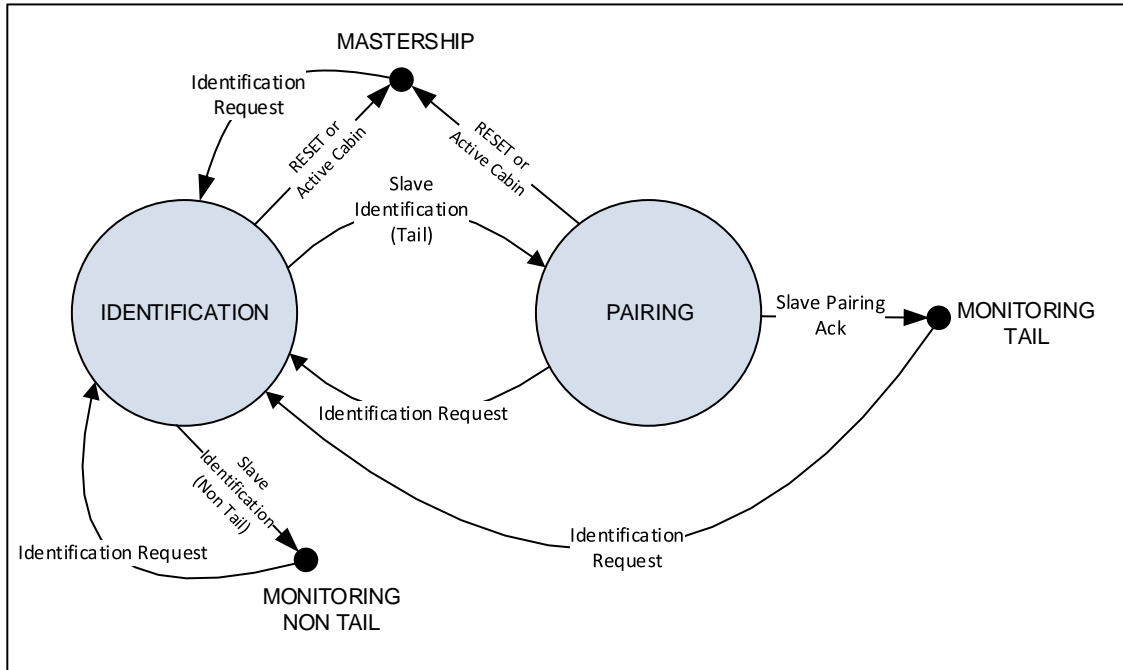
**Table 7-8: Priority table of OTI Slave Module FSM**

#### 7.1.5.1 OTI Slave Inauguration State

Inauguration phase refers to: (i) identification of OTI modules connected to OCN and (ii) pairing between OTI Master in front cabin and OTI slave at train tail.

OTI Slave shall identify itself on identification request from OTI Master. Only OTI Slave at train tail shall pair with OTI Master

Inauguration state is depicted in Figure 7-24 and includes an identification phase and a pairing phase.



**Figure 7-24 – FSM OTI Slave: Inauguration State**

REQ\_7.1.5.1.1 The OTI Slave module “Non TAIL” shall not accept the Pairing Request Message sent by OTI Master.

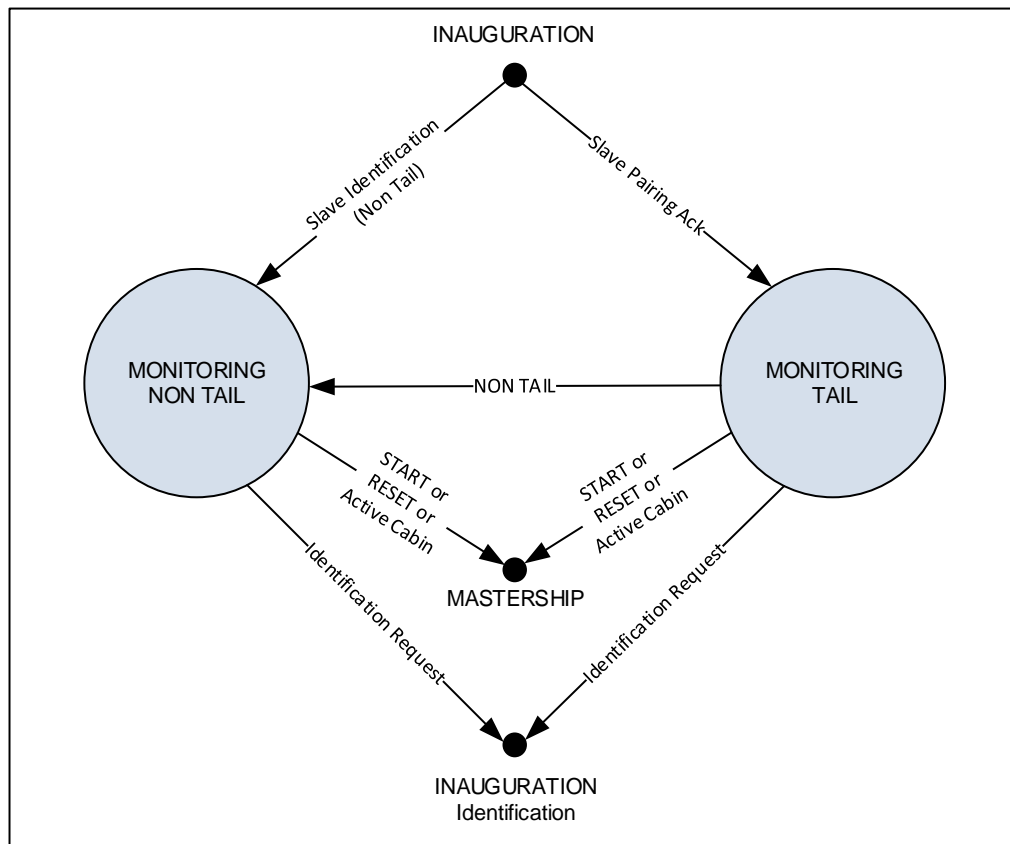
REQ\_7.1.5.1.2 The OTI Slave TAIL in “Identification” state shall transit to “Pairing” state when the “Slave Identification Ack” message is sent to OTI Master.

REQ\_7.1.5.1.3 The OTI Slave TAIL in “Pairing” state shall transit to “Identification” state if an “Identification Request” message sent by OTI Master is received.

For more details about communication between the OTI Modules refer to [7].

### 7.1.5.2 OTI Slave Monitoring State

REQ\_7.1.5.2.1 OTI Slave Functional Module Monitoring State shall behave according to FSM depicted in Figure 7-25.



**Figure 7-25 - OTI Slave FSM: Monitoring State**

REQ\_7.1.5.2.2 OTI Slave shall perform transition to TAIL state in case of last waggon.

REQ\_7.1.5.2.3 OTI Slave shall perform transition to NON TAIL state in case of intermediate waggon.

*Note that defining solutions to identify OTI Slave at train tail is part of D4.2 [7].*

REQ\_7.1.5.2.4 OTI Slave in TAIL or NON TAIL status:

- shall determine train tail status
- shall provide a status message to OTI Master as answer to each received request message

*Note that in GNSS scenario, the OTI Slave status includes tail position and satellite coverage.*

REQ\_7.1.5.2.5 OTI Slave in TAIL or NON TAIL status:

- shall not provide any train integrity status to ETCS

REQ\_7.1.5.2.6 (OPTIONAL) OTI Slave in TAIL or NON TAIL status:

- shall acquire waggon/cargo diagnostic data
- shall provide periodic waggon/cargo diagnostic message to OTI Master each T\_DIAG\_DATA.

Note that in general the diagnostic data shall be independent by train integrity monitoring data.

REQ\_7.1.5.2.7 (OPTIONAL) T\_DIAG\_DATA shall be a configuration parameter.

REQ\_7.1.5.2.8 (OPTIONAL) OTI Slave shall determine identifiers of nearby OTI modules.

REQ\_7.1.5.2.9 (OPTIONAL) OTI Slave shall provide to OTI Master the identifiers of nearby OTI modules.

*Note that determination of nearby OTI slave identifier is aimed at allowing OTI Master to determine train composition.*

REQ\_7.1.5.2.10 (OPTIONAL) OTI Slave shall provide waggon/cargo diagnostic data to Wayside Maintenance Centre.

Note that optional requirement related to providing diagnostic data to Wayside Centre is referred to situation of unavailable communication with OTI Master.

REQ\_7.1.5.2.11 (OPTIONAL) OTI Slave shall record waggon/cargo diagnostic data.

Note that optional requirement related to recording diagnostic data is aimed at managing situations of unavailable communication with OTI Master or Wayside Maintenance Centre.

### 7.1.5.3 Train tail status

REQ\_7.1.5.3.1 In case of wireless on-board communication network, the OTI Slave status message shall include odometry information: (i) position or (ii) speed or (iii) acceleration.

*Note: Evaluate other information for OTI Slave status determination (e.g. breaking pipe pressure).*

### 7.1.5.4 Interfaces

REQ\_7.1.5.4.1 OTI Slave Functional Module shall communicate with OTI Master Functional module.

REQ\_7.1.5.4.2 OTI Slave Functional Module shall acquire odometry data.

REQ\_7.1.5.4.3 OTI Slave Functional Module shall communicate with wireless communication sensors.

REQ\_7.1.5.4.4 (OPTIONAL) OTI Slave Functional Module shall communicate with waggon/cargo diagnostic wireless sensors.

REQ\_7.1.5.4.5 (OPTIONAL) OTI Slave Functional Module shall communicate with Wayside Maintenance Centre.

REQ\_7.1.5.4.6 The energy consumption level of OTI Slave Functional Module, for legacy freight applications, shall allow to use energy harvesting sources.

#### 7.1.5.5 Sequence diagrams examples

In the following some sequence diagrams are reported in relation to train joining and train splitting phases. OTI role change and re-inauguration process are performed to support the joining and splitting phases.

Figure 7-26 refers to joining scenario described at section 6.2.4.3 with two trains that are joined in a single longer train.

Figure 7-27 refers to splitting scenario described at section 6.2.4.5 with a train split in two parts. Note that train separation detection, in case of wireless communication, requires that waggons are moved for a minimum distance.

Figure 7-28 refers to shunting scenario described at section 6.2.4.8.

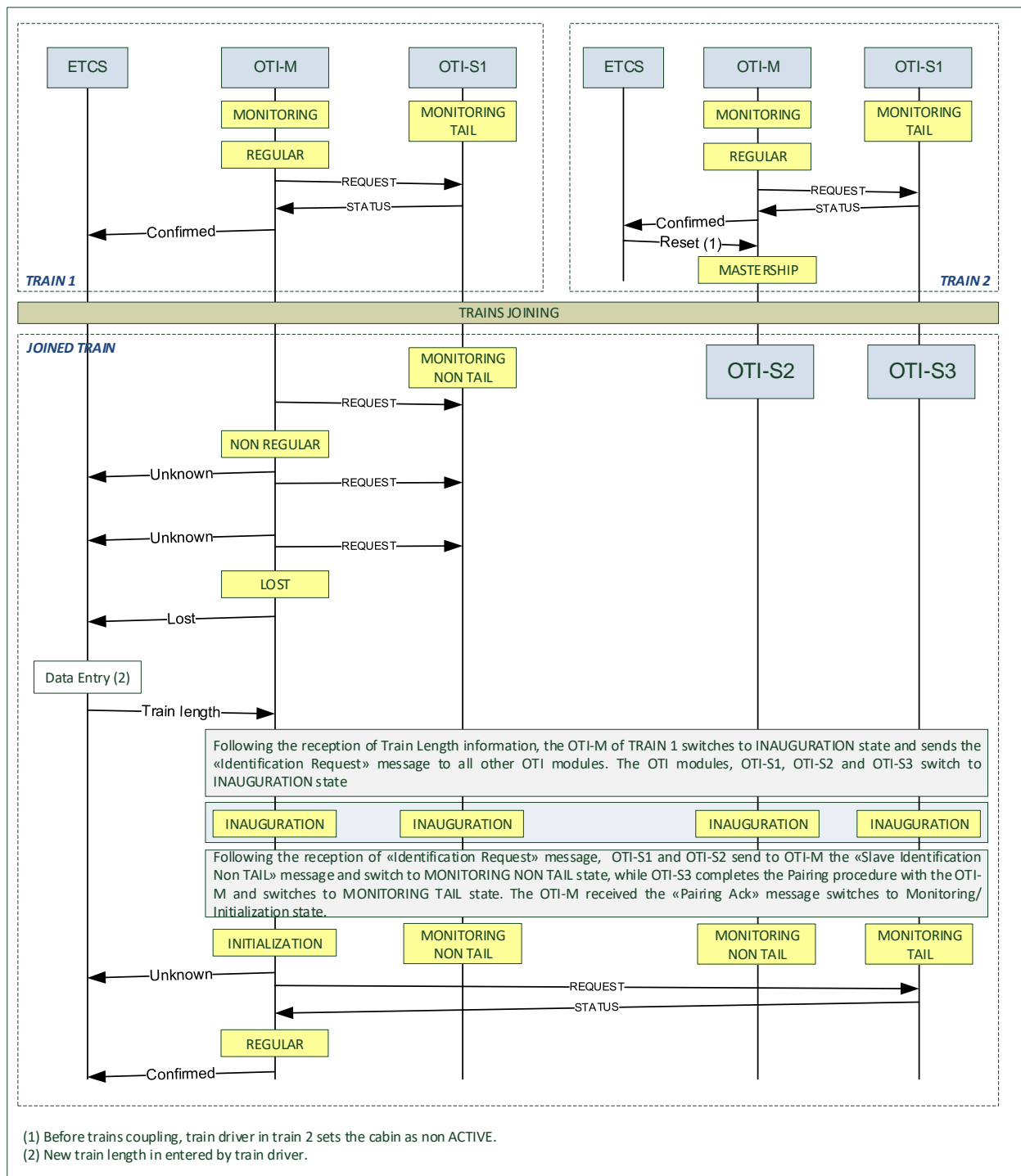
Note that OTI module role is defined in MASTERSHIP state and depends on cabin status:

- OTI modules acquire a SLAVE role in case of non-ACTIVE cabin
- OTI modules acquire a MASTER role in case of ACTIVE cabin.

A cabin is intended as ACTIVE in case of OTI module located in front cabin and the desk is open.

A cabin is intended as non-ACTIVE in all other cases, as example:

- OTI module is located in intermediate cabin
- OTI module is located in front cabin and the desk is closed
- OTI module located in a slave engine in Non-Leading mode



**Figure 7-26 – Sequence diagram in Train Joining scenario – Example 1**



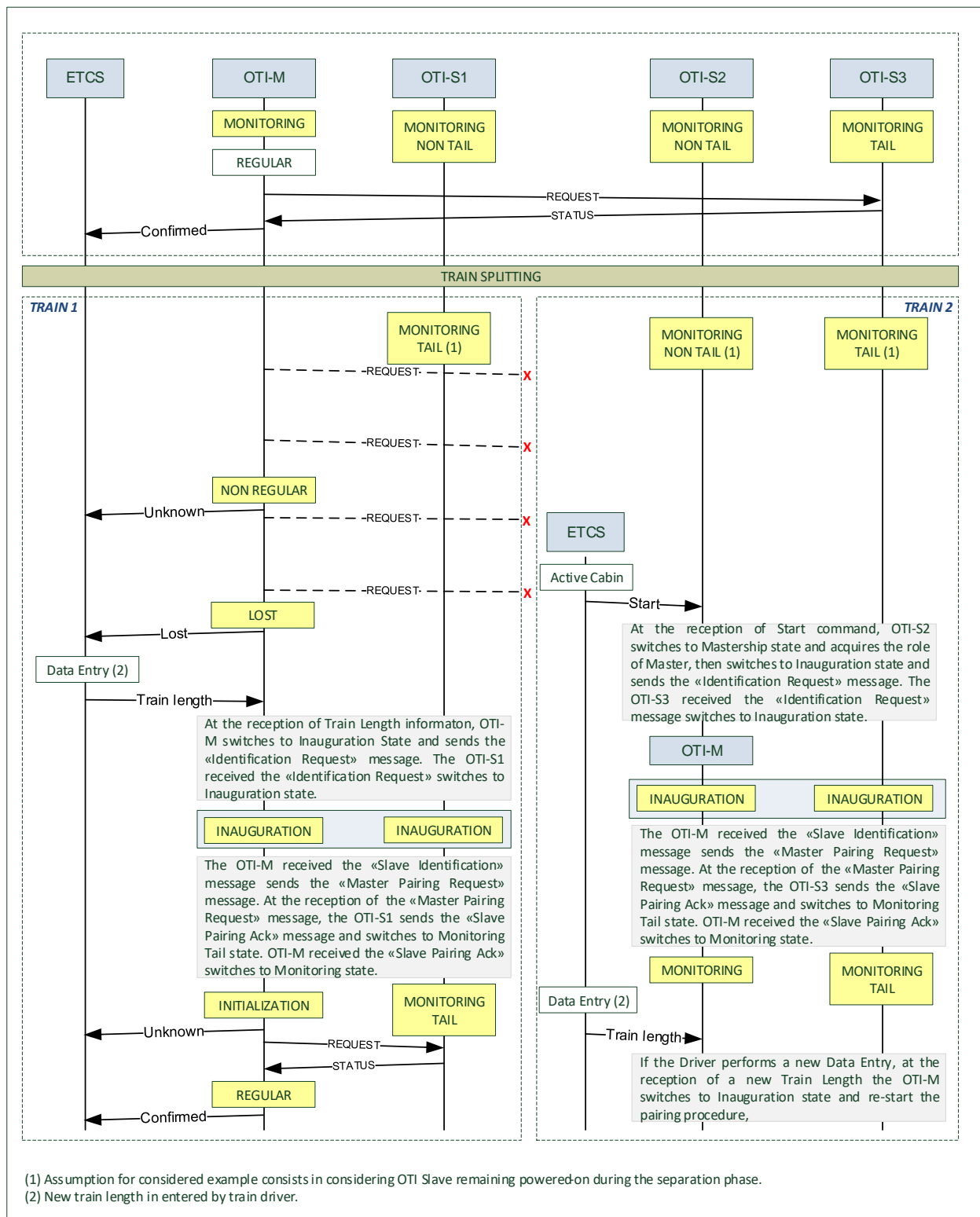
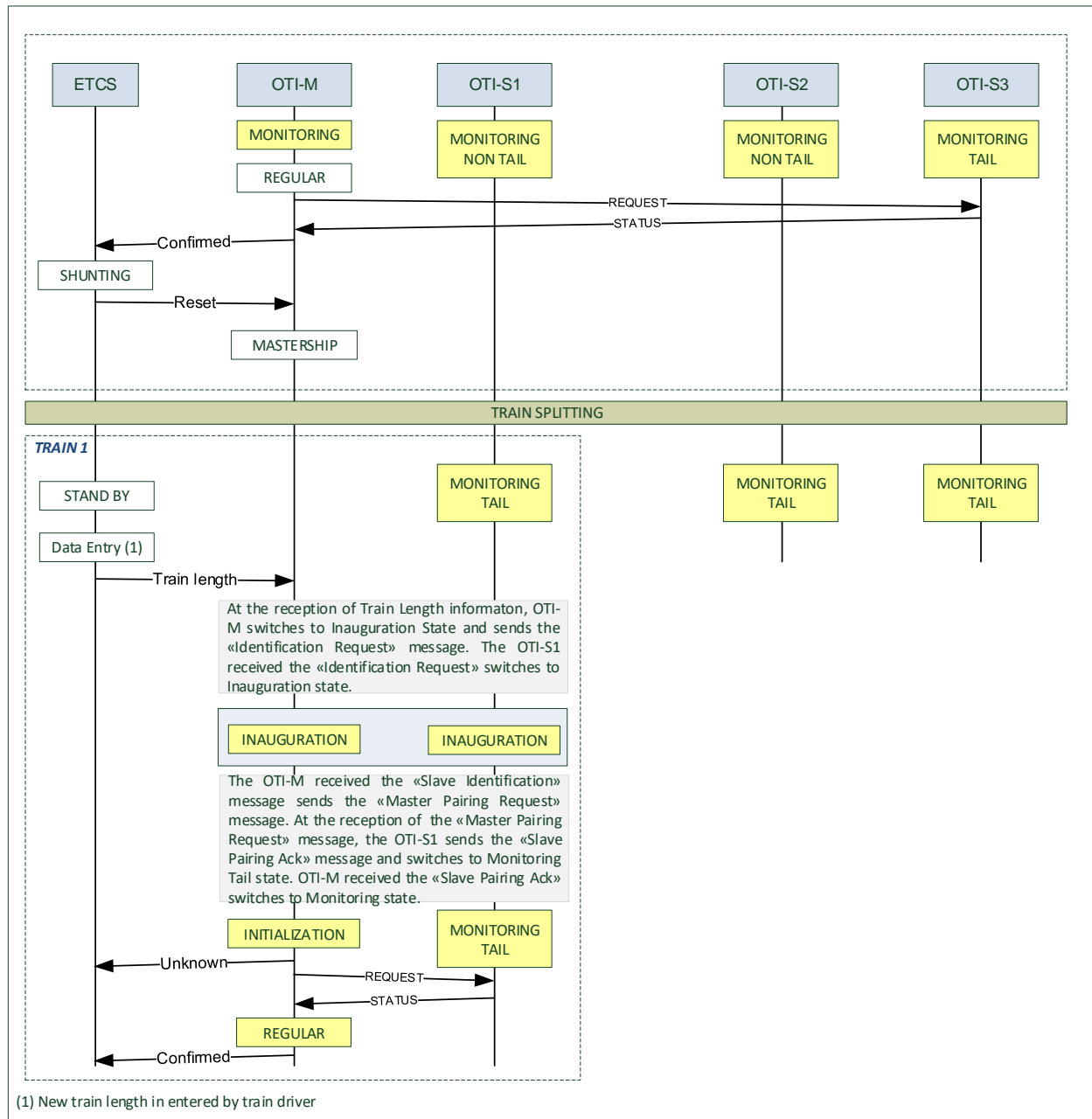


Figure 7-27 – Sequence diagram in Train Splitting scenario – Example 1



**Figure 7-28 – Example of OTI sequence diagram in Shunting scenario**

As alternative, train joining/splitting procedure can be performed with cabin status acquired from rolling stock TIU as depicted in Figure 7-29 and Figure 7-30.

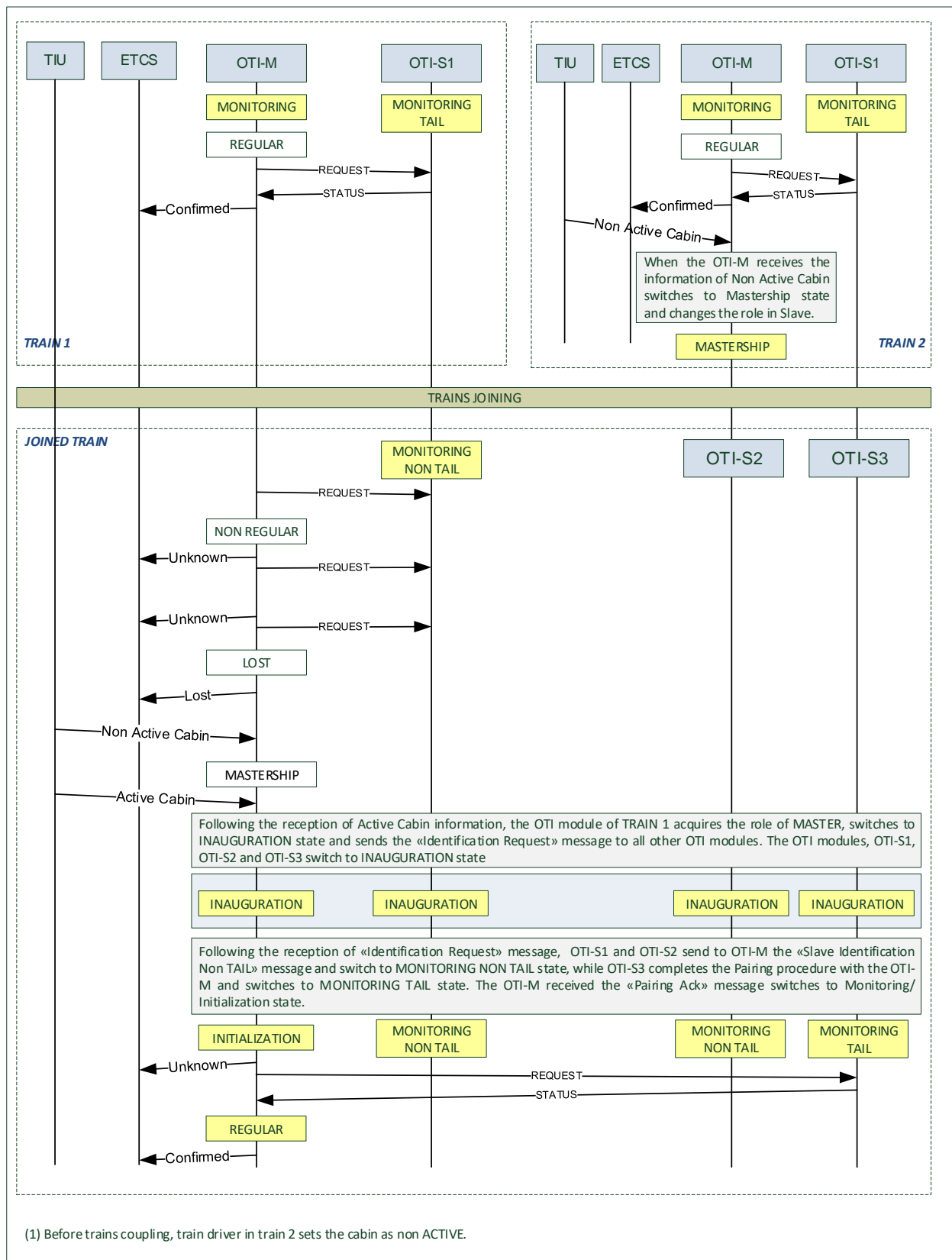


Figure 7-29– Sequence diagram in Train Joining scenario – Example 2

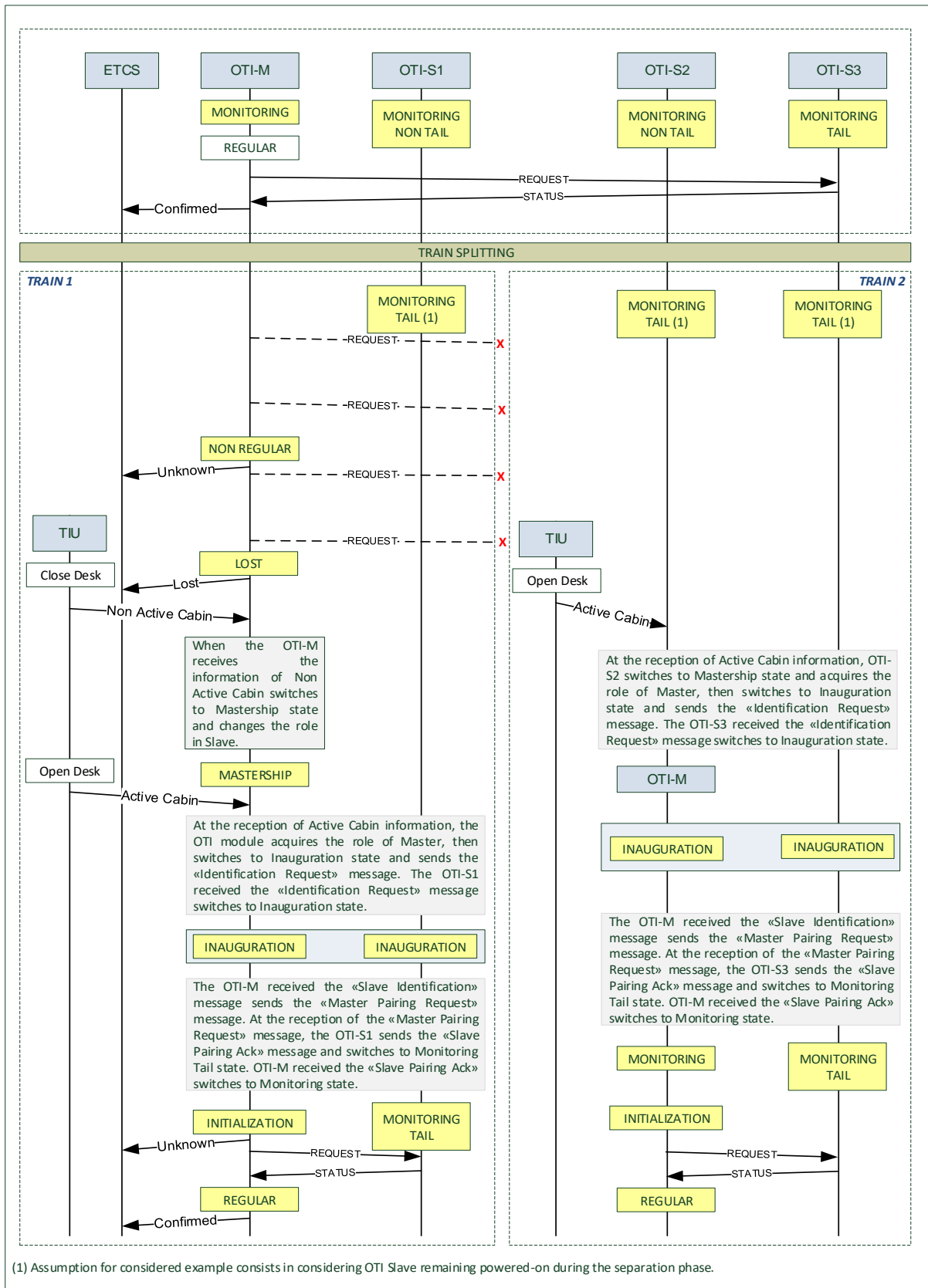


Figure 7-30 – Sequence diagram in Train Splitting scenario – Example 3

#### 7.1.5.6 Safety Requirement

REQ\_7.1.5.6.1 OTI Slave Functional Module shall be SIL4 in relation to Mastership management, Inauguration phase and Monitoring state.

REQ\_7.1.5.6.2 Packets exchanged between the OTI modules shall include a field that specifies the OTI identifier (OTI ID) and the OTI role (Master / Slave TAIL / Slave Non TAIL).

REQ\_7.1.5.6.3 OTI identifier shall be unique for each OTI module.

REQ\_7.1.5.6.4 (optional) If the OTI modules manage diagnostic information, the communication protocol between OTI modules shall use different messages for diagnostic and train integrity information.

#### 7.1.6 Virtual Coupling preliminary analysis

This section contains a separate preliminary analysis related to the impact at FSM level for implementing Virtual Coupling functionality according to preliminary analysis reported at section 6.2.5. As remarket at section 6.2.5, this topic can be fully analysed only after a complete analysis performed by TD2.8. Anyway this topic shall not be part of X2Rail-2 WP4 demonstrator.

##### 7.1.6.1 OTI Master

The OTI-M FSM need to be split in three collaborating FSMs:

- FSM0 manages interfaces with ETCS and starting/resetting commands to FSM1/FSM2
- FSM1 and FSM2 manages interfaces with OTI slaves

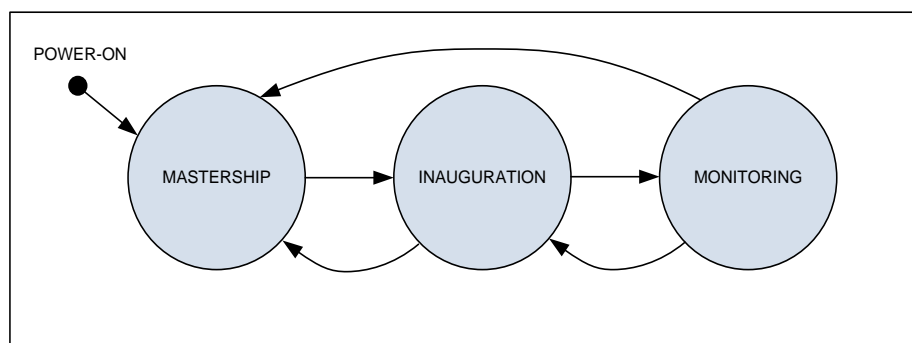
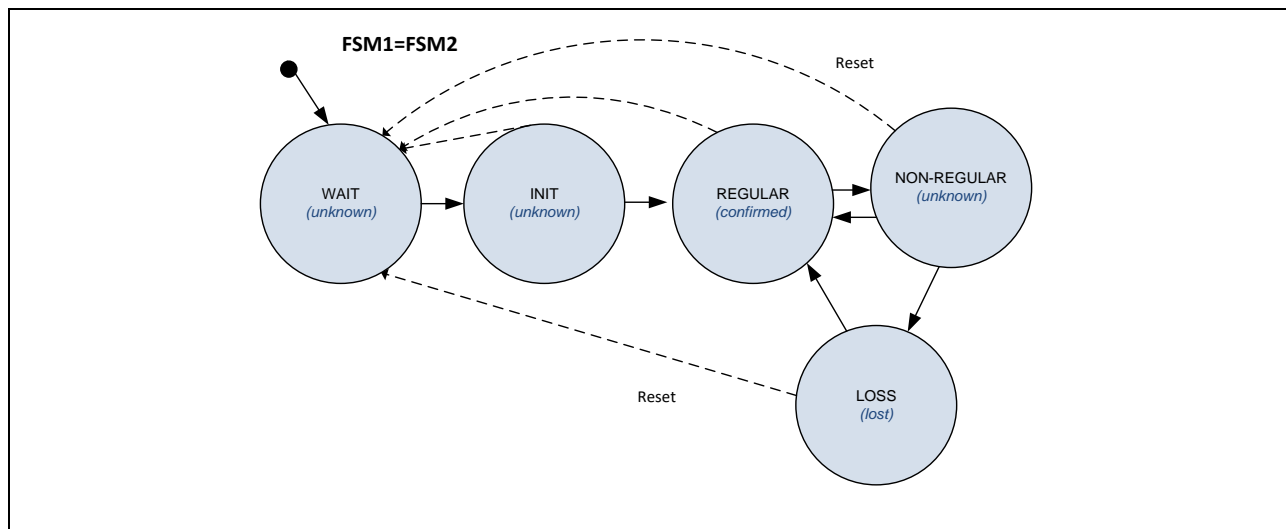


Figure 7-31 – Virtual Coupling - OTI Master: FSM0



**Figure 7-32 – Virtual Coupling - OTI Master: FSM1=FSM2**

Transition to WAIT State, on RESET Command, closes the communication with OTI-Master and therefore the pairing is also closed. A specific PAIRING\_CLOSE command is sent to OTI Slave.

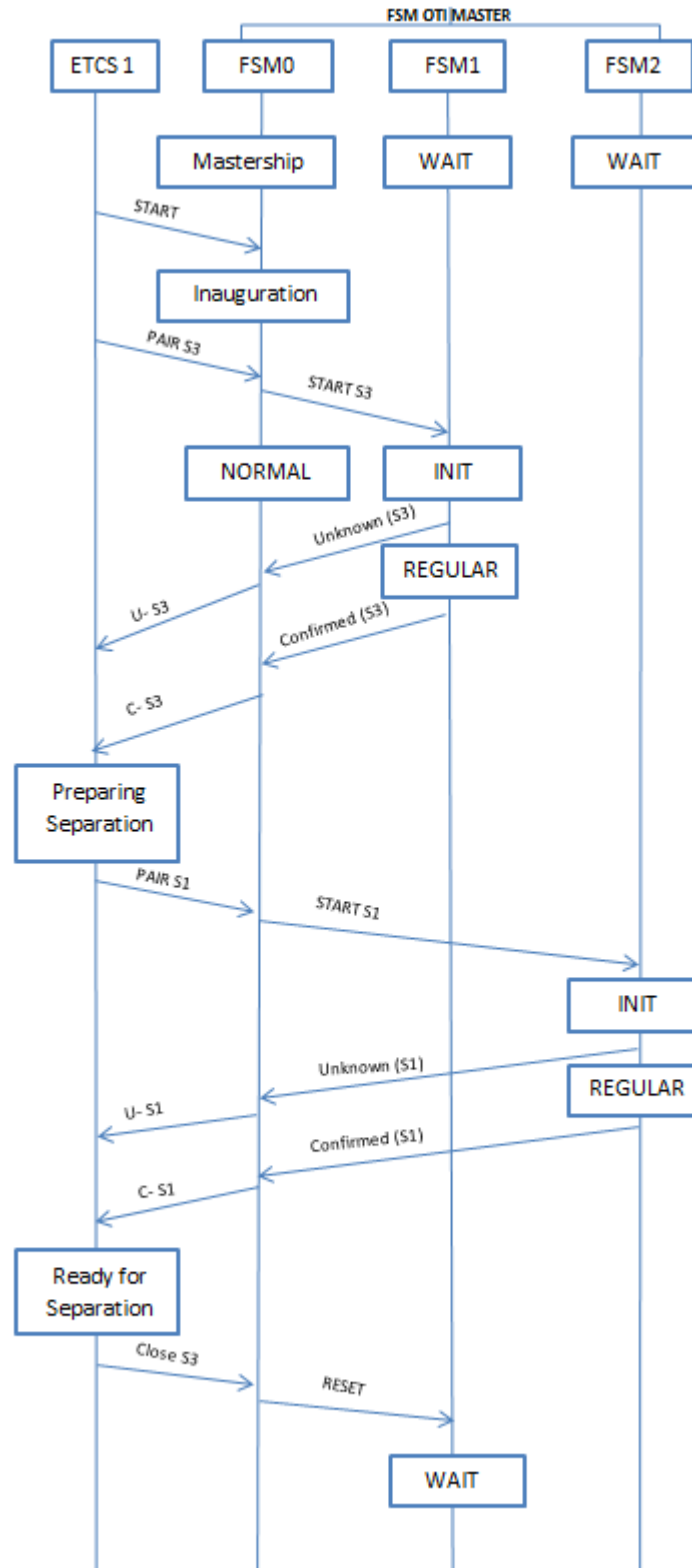
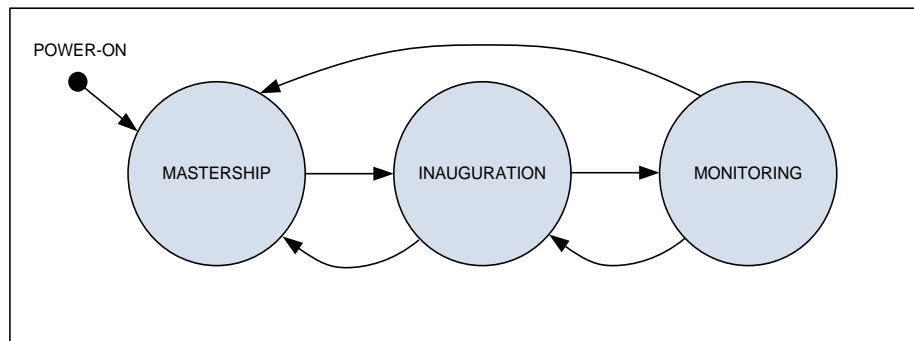


Figure 7-33 – Virtual Coupling - OTI Master: sequence diagram example

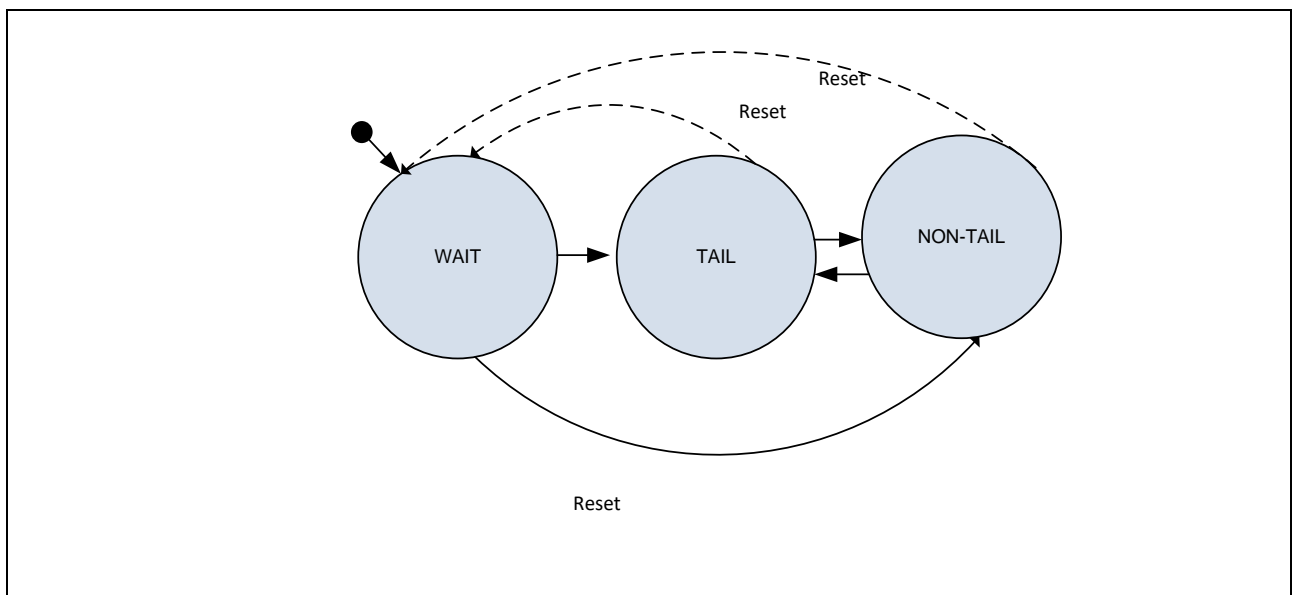
### 7.1.6.2 OTI Slave

The OTI-S FSM need to be split in three collaborating FSMs:

- FSM0 manages interfaces with OTI Master and starting/resetting commands to FSM1/FSM2
- FSM1 and FSM2 provide status reports on OTI-M request.



**Figure 7-34 – Virtual Coupling - OTI Slave: FSM0**



**Figure 7-35 – Virtual Coupling - OTI Slave: FSM1=FSM2**



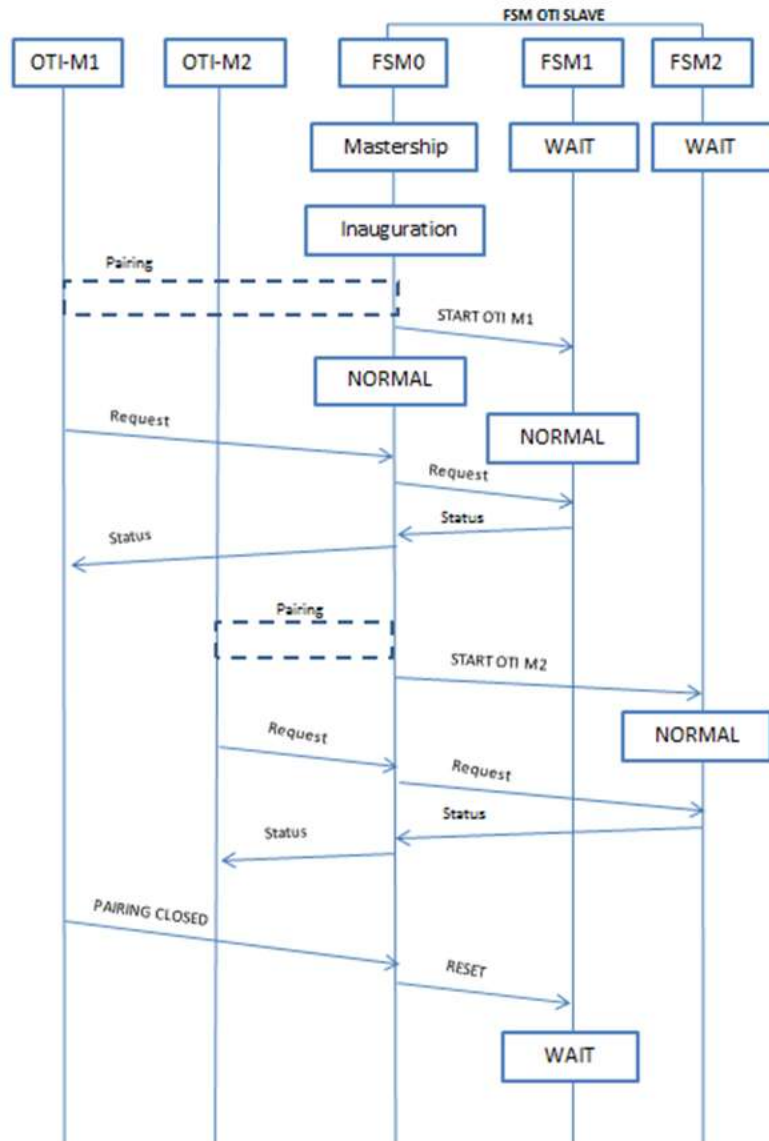


Figure 7-36 – Virtual Coupling - OTI Slave: sequence diagram example

### 7.1.6.3 Requirements

OTI predispositions to manage Virtual Coupling should require at least the following requirements:

REQ\_VC1: (M) OTI Master shall receive pairing command from ETCS specifying OTI Slave ID.

REQ\_VC2: (M) OTI Master shall pair with OTI Slave ID defined by ETCS.

REQ\_VC3: (M) OTI Master shall manage double pairings on ETCS request.

REQ\_VC4: (M) OTI Master shall stop a pairing on ETCS request.

REQ\_VC5: (M) OTI Slave shall accept simultaneous pairing with two OTI Master.

Other optional requirements should include:

REQ\_VC6: (O) OTI Master shall determine train composition.

REQ\_VC7: (O) OTI Master shall provide train composition information to ETCS

#### 7.1.6.4 Conclusion

This section reports an example of impact at FSM level for implementing the virtual coupling functionality according to the assumptions and preliminary analysis reported at section 6.2.5.

On the basis of identified assumptions, the result of preliminary analysis remarks that availability of full requirements specification from TD2.8 is mandatory to identify the expected functionalities from TD2.5.

Under identified assumption and on the basis of analysed decoupling scenario, introducing the support for virtual coupling functionality impacts at functional level and not at architectural level.

In conclusion a complete analysis and requirements specification for Virtual Coupling is part of TD2.8 and is out of TD2.5 scope of work.

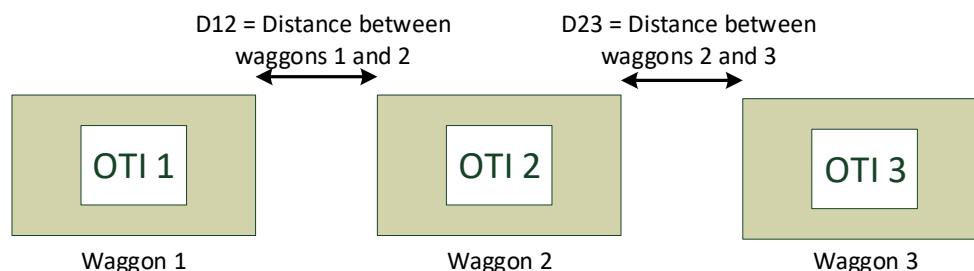
#### 7.1.7 Product Class 3

This section includes the functional requirements for the Product Class 3, as defined in Table 6-5. These requirements are defined starting from the requirements specified in §7.1 and specifying all the differences.

REQ.7.1.7.1 For Product Class 3, train integrity criterion consists in verifying separation between adjacent waggons. Train integrity shall be considered as not confirmed when:

- a) The distance between two adjacent waggons is greater than a specified value, or
- b) The distance between two adjacent waggons can not be evaluated.

Note: the limit value of the distance shall be determined based on the specific application.



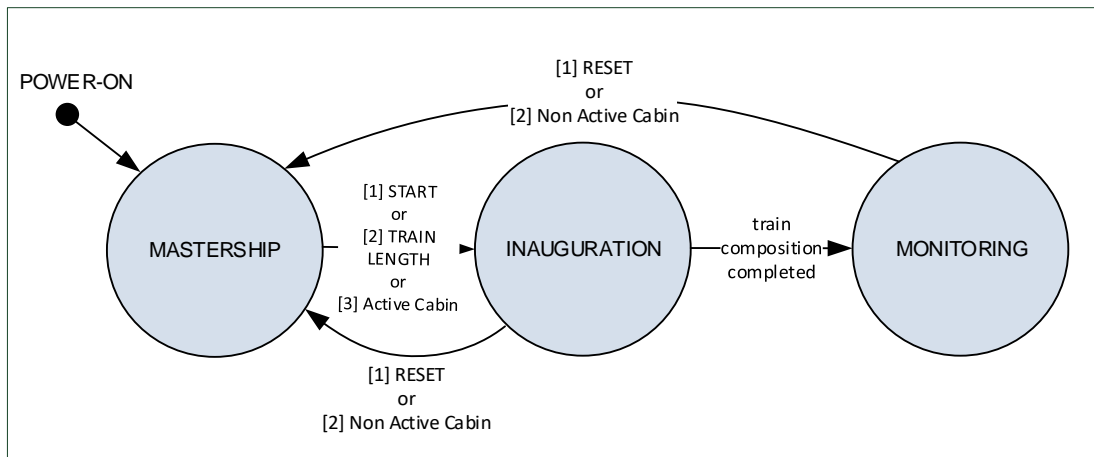
**Figure 7-37: Product Class 3: Distance between waggons**

REQ.7.1.7.2 The status of an OTI device is defined as “coupled” if it is able to determine the distance between the waggon where it is installed and the adjacent waggon(s) and this distance is less or equal to a specified value, “separated” if the distance is greater than a specified value, otherwise “unknown”.

Note: as depicted in Figure 7-37 the OTI 2 shall be able to determine distance with the waggon 1 on its left (D12) and the waggon 3 on its right (D23) and only if D12 and D23 are less or equal to Dlim its status will be “coupled” (Dlim = limit value of the distance).

#### 7.1.7.1 OTI Master Functional Module for Product Class 3

REQ.7.1.7.3 The OTI Master of Product Class 3 shall implement the FSM depicted in Figure 7-38 and the conditions for the transitions reported in Table 7-9 and Table 7-10.



**Figure 7-38: OTI Master Module: FSM High Level for Product Class 3**

OTI Master FSM transitions are reported in Table 7-9. Notation “3>” means that condition 3 has to fulfilled to trigger a transition from the state reported in column to the state reported in row and highlighted with the arrow “>”. For each cell, the arrow refers to the direction of the state transition and the number refers to the transition conditions. States are reported in blue cells with the following acronyms: MS = Mastership, IN = Inauguration, MN = Monitoring. Transition conditions are described in Table 7-10.

MS	<1	<3
>0	IN	-
	2>	MN

**Table 7-9: OTI Master Module: FSM High Level Transitions for Product Class 3**

Condition	Transition conditions from mode X to mode Y	Action in Y state
0	<b>From MASTERSHIP to INAUGURATION</b> OTI-M: START command received from ETCS or new Train Length received from ETCS or Active Cabin is acquired from rolling stock TIU.	OTI-M: MASTER role is acquired and “Identification Request” is sent to OTI Slave modules.

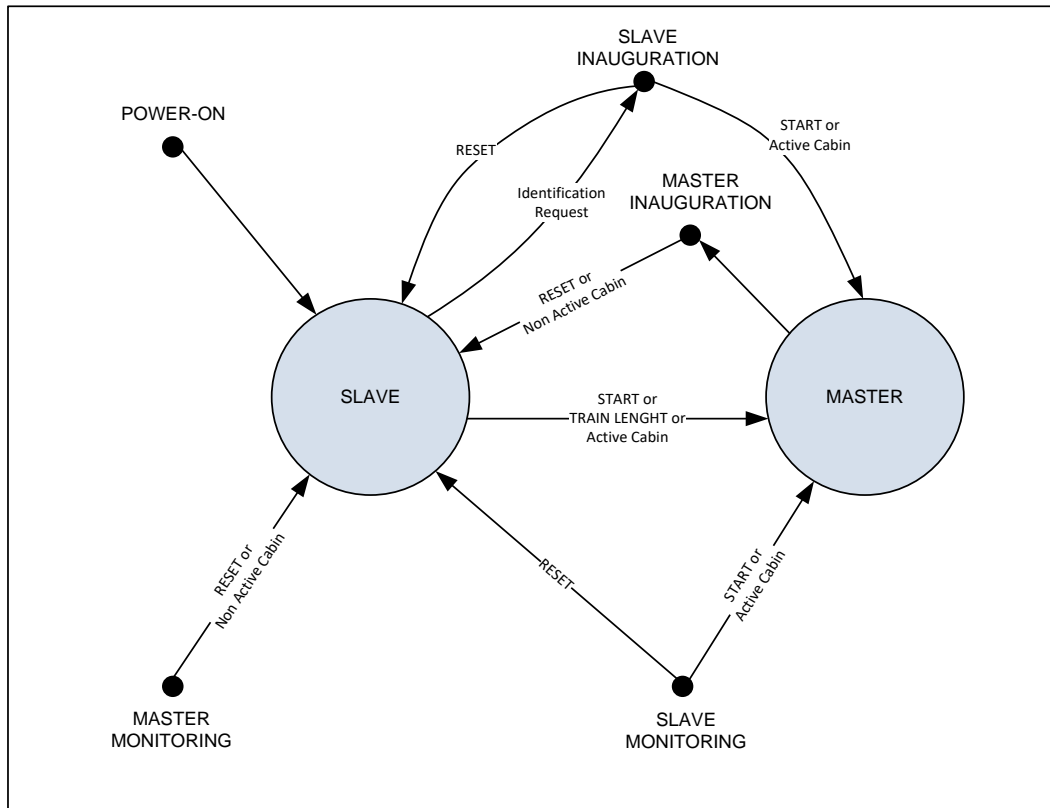
1	<b>From INAUGURATION to MASTERSHIP</b> OTI-M: RESET command received from ETCS or Non Active Cabin is acquired from rolling stock TIU.	OTI-M: Waits for START command or new Train Length or Active Cabin information.
2	<b>From INAUGURATION to MONITORING</b> OTI-M: OTI Master has completed the “train composition determination” phase (see details in §7.1.7.3).	OTI-M: See FSM at section 7.1.7.4
3	<b>From MONITORING to MASTERSHIP</b> OTI-M: RESET command received from ETCS or Non Active Cabin is acquired from rolling stock TIU	OTI-M: Waits for START command or Train Length from ETCS.
-	<b>From MONITORING to INAUGURATION</b> No transition	Not applicable

**Table 7-10: OTI Master module: FSM High Level Transition conditions for Product Class 3**

Note: during the “train composition determination” phase the OTI Slave device installed on each waggon communicates to the OTI Master its ID and the ID(s) of the adjacent waggon(s).

#### **7.1.7.2 OTI Master Mastership State for Product Class 3**

REQ.7.1.7.4 The OTI Master of Product Class 3 shall implement the Mastership state depicted in Figure 7-39.

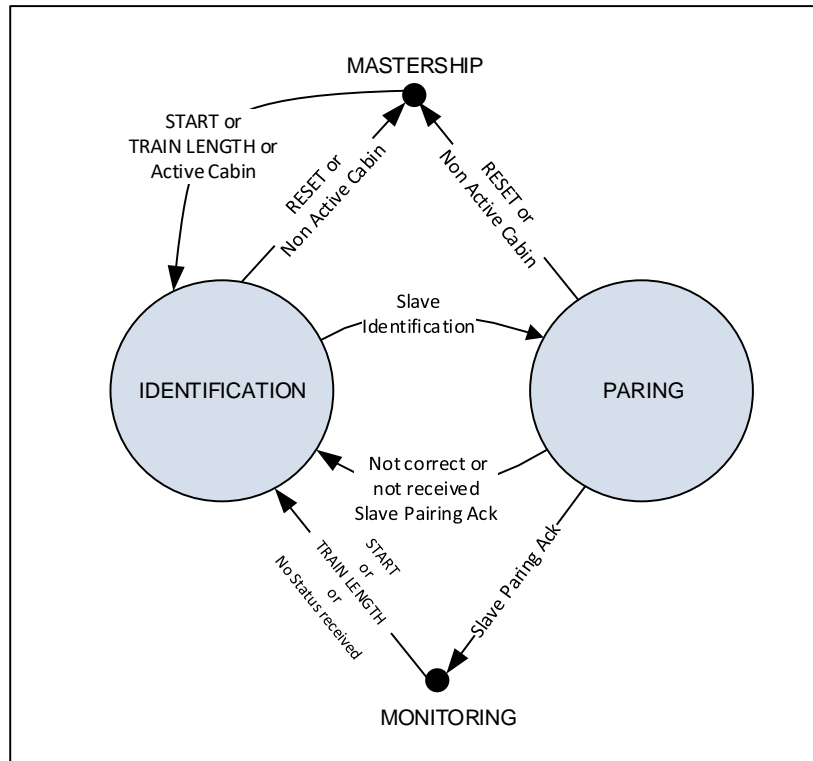


**Figure 7-39: OTI Master Module: Mastership state for Product Class 3**

Note that the requirements REQ\_7.1.1.1.1, REQ\_7.1.1.1.2 and REQ\_7.1.1.1.3 defined in §7.1.1.1 are still valid.

### 7.1.7.3 OTI Master Inauguration State for Product Class 3

REQ.7.1.7.5 The OTI Master of Product Class 3 shall implement the Inauguration state depicted in Figure 7-40.



**Figure 7-40: OTI Master Module: Inauguration State for Product Class 3**

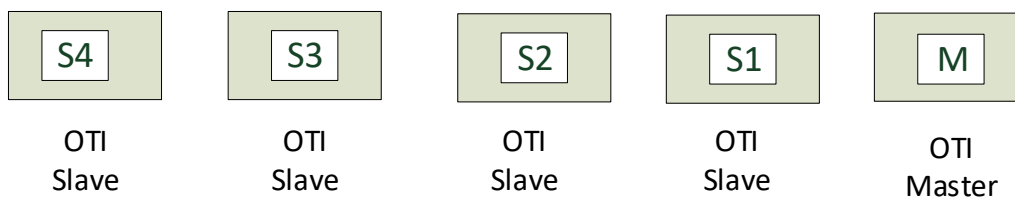
REQ.7.1.7.6 During the "Identification" phase the OTI Master shall:

- collects from the OTIs Slave that are part of the same train the following information: ID of each OTI device, the ID of the next and previous OTI device and their position (Tail/Non Tail);
- shall determine train composition (sequence of IDs);

The following Figure 7-41 depicts an example of train composition determination. In this example each OTI Slave communicates to OTI Master the following information:

- OTI Slave S1 => Identifiers: S2 – S1 – M. Position = Non TAIL;
- OTI Slave S2 => Identifiers: S3 – S2 – S1. Position = Non TAIL;
- OTI Slave S3 => Identifiers: S4 – S3 – S2. Position = Non TAIL;
- OTI Slave S4 => Identifiers: # – S4 – S3 (where # means that no OTI device is present). Position = TAIL.

From this information the OTI Master knowing its identifier is able to determine the train composition.



**Figure 7-41: Example of train composition**

REQ.7.1.7.7 During the "Identification" phase the OTI Master shall reject a "Slave Identification Ack" message sent by an OTI Slave including the following information:

- 1) TAIL position, and;
- 2) the IDs of two adjacent OTI Slave (only one is possible).

REQ.7.1.7.8 The OTI Master shall interrupt the Inauguration phase if it receives more than one "Slave Identification Ack" message with the information of "TAIL" position.

REQ.7.1.7.9 The OTI Master received the "Slave Identification Ack" message from the OTI Slave TAIL and waited for a defined time shall:

- transit to "Pairing" state and shall check the consistency of discovered train composition with the information provided by an external source (e.g. train driver or trackside control center);
- send a "Pairing Request" message to all the OTIs Slave in "TAIL" and "NON TAIL" position.

Note 1: for the Product Class 3, the concept of "Pairing" changes, in particular the OTI Master performs the pairing with all the OTIs Slave and not only with the OTI Slave TAIL.

Note 2: the time defined in REQ.7.1.7.9 is necessary because the OTI Master shall wait for receiving the "Slave Identification Ack" message from all OTI Slave and its value depends by the specific application.

REQ.7.1.7.10 The OTI Master in "Pairing" state shall accept the "Slave Pairing Ack" message only if the message is consistent (see REQ\_7.1.1.3.11). If the message is not consistent then the OTI Master shall reject the message and shall transit to "Identification" state.

Note that for Product Class 3 the requirements related to Inauguration state defined in §7.1.1.2 are still applicable with the following exceptions:

- REQ\_7.1.1.2.2 => OTI Master send a "Pairing Request" message to all the OTIs Slave;
- REQ\_7.1.1.2.4 => "Slave Pairing Ack" message is sent by all the OTIs Slave.

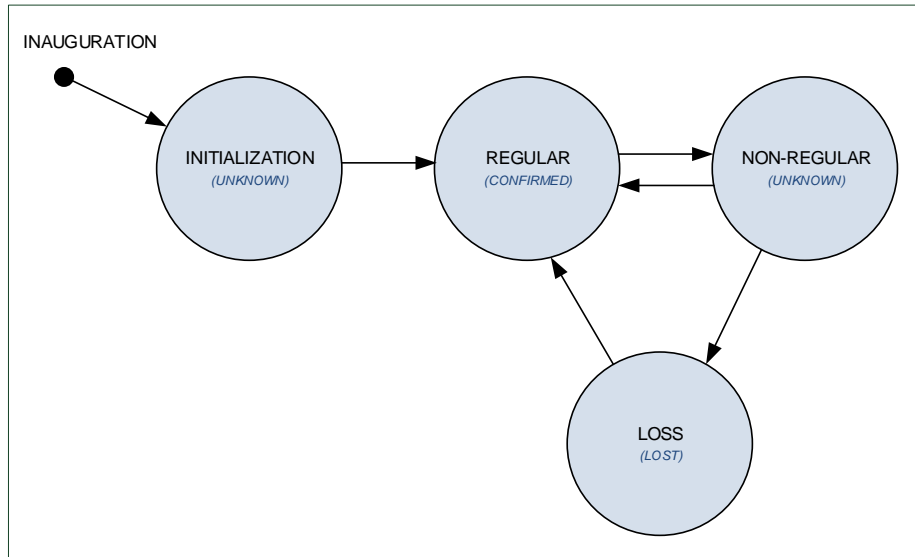
Depending on the technological solution adopted, faults in inauguration phase could prevent determining complete train composition with the result that train integrity criterion would be applied to non complete train. Possible mitigation for this hazard consists in comparing discovered train composition with data provided by an external source (e.g. train driver, trackside database) by means of a OTI dashboard.

REQ.7.1.7.11 (Optional) The OTI Master shall show discovered train composition on OTI dashboard for confirmation by the driver.

REQ.7.1.7.12 (Optional) The OTI Master shall retrieve train composition from a trackside database and shall show it on OTI dashboard for confirmation by the driver.

#### 7.1.7.4 OTI Master Monitoring State for Product Class 3

REQ.7.1.7.13 The OTI Master of Product Class 3 shall manage the communication with OTI Slave Functional Module according to FSM depicted in Figure 7-42 and according to transitions reported in Table 7-11.



**Figure 7-42: OTI Master FSM – MONITORING STATE for Product Class 3**

Condition	Transition conditions from mode X to mode Y	Entry action in Y state
1	<b>Transition from I to R</b> OTI Master receives N% of consistent messages from each paired OTIs Slave within time-out T_OTIM_I and no change is detected in the previously determined train composition.	Send to ETCS TIU the value <b>“Confirmed”</b> as Train Integrity Information.
2	<b>Transition from R to NR</b> <ul style="list-style-type: none"> <li>▪ OTI Master does not receive consistent message from at least one paired OTI Slave within time-out T_OTIM_COMM, OR;</li> <li>▪ OTI Master receives a non-consistent message within time-out T_OTIM_COMM, OR;</li> <li>▪ OTI Master receives “unknown” coupled waggon status for a time-out T_COUPLING_STATUS, OR;</li> <li>▪ OTI Master receives uncoupled waggon status from one or many OTIs Slave, OR;</li> </ul>	<b>Send</b> to ETCS TIU the value <b>“Unknown”</b> as Train Integrity Information.



	<ul style="list-style-type: none"> <li>OTI Master detects a change in the previously determined train composition.</li> </ul>	
3	<b>Transition from NR to R</b> OTI Master receives a consistent message from all paired OTIs Slave within time-out T_OTIM_COMM with coupled waggon status AND no change is detected in the previously determined train composition.	Send to ETCS TIU the value <b>"Confirmed"</b> as Train Integrity Information.
4	<b>Transition from NR to L</b> OTI Master does not receive consistent messages from at least one paired OTI Slave OR receives non-consistent messages from at least one paired OTI Slave within time-out T_OTIM_L OR receives uncoupled waggon status from one or many OTI Slave OR a change is detected in the previously determined train composition.	Send to ETCS TIU the value <b>"Lost"</b> as Train Integrity Information.
5	<b>Transition from L to R</b> OTI Master receives M% of consistent messages from each paired OTI Slave within time-out T_OTIM_R with coupled waggon status AND no change is detected in the previously determined train composition	Send to ETCS TIU the value <b>"Confirmed"</b> as Train Integrity Information.

**Table 7-11:** OTI Master of Product Class 3: Monitoring State Transitions conditions

REQ.7.1.7.14 N, M, T\_OTIM\_I, T\_OTIM\_COMM, T\_OTIM\_L, T\_OTIM\_R, T\_COUPLING\_STATUS shall be configuration parameters.

Values for configuration parameter shall be defined at design phase. In general configuration parameter values are fixed during a train mission.

Note that for Product Class 3 the requirements related to Monitoring state defined in §7.1.1.3 are still applicable with the following exceptions:

- REQ\_7.1.1.3.1 => the OTI Master for Product Classe 3 receives messages from all OTIs Slave;
- REQ\_7.1.1.3.2 => for Product Class 3 the train integrity criterion is defined in REQ.7.1.7.1;
- REQ\_7.1.1.3.4 => refer to REQ.7.1.7.13;
- REQ\_7.1.1.3.12 => not all the parameters defined in this requirement are applicable to Product Class 3, refer to REQ.7.1.7.14;

#### 7.1.7.5 OTI Master Interfaces for Product Class 3

All the requirements defined in §7.1.1.6 are applicable with the following exceptions:

- REQ\_7.1.1.6.3 => train integrity criterion for Product Class 3 is defined in REQ.7.1.7.1;

#### 7.1.7.6 OTI Master Safety Requirements for Product Class 3

All the requirements defined in §7.1.1.7 are applicable for Product Class 3 and in addition:

REQ.7.1.7.15 The function performed by the OTI module about the determination of the distance with the adjacent waggon(s) shall be safety related.

#### 7.1.7.7 On-board Communication Network for Product Class 3

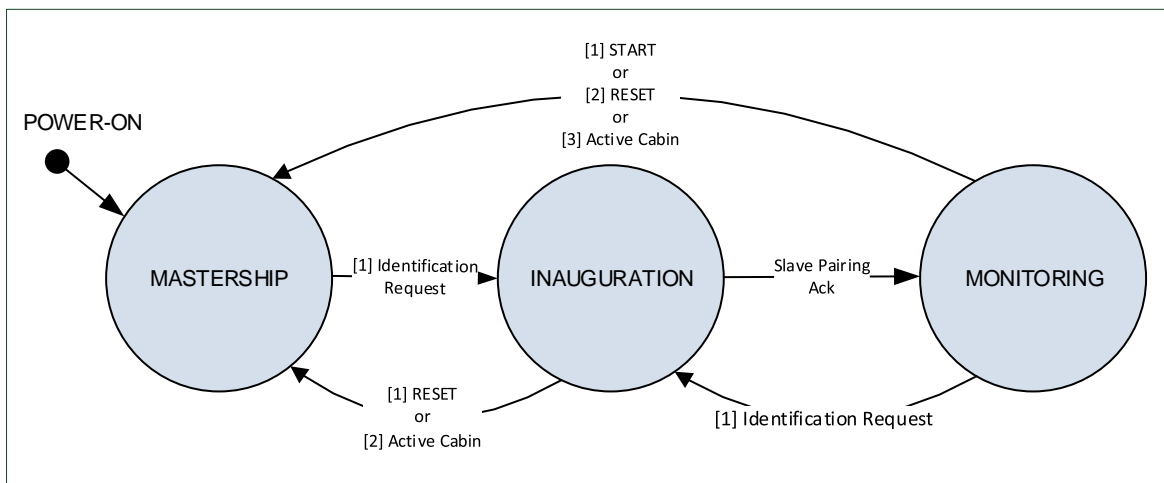
All the requirements defined in §7.1.3 are applicable for Product Class 3.

#### 7.1.7.8 On-board Communication Protocol for Product Class 3

All the requirements defined in §7.1.4 are applicable for Product Class 3.

#### 7.1.7.9 OTI Slave Functional Module for Product Class 3

REQ.7.1.7.16 The OTI Slave of Product Class 3 shall implement the FSM depicted in Figure 7-43 and the conditions for the transitions reported in Table 7-12 and Table 7-13:



**Figure 7-43: OTI Slave Module: FSM for Product Class 3**

OTI Slave FSM transitions are reported in Table 7-12. Notation “4>” means that condition 4 has to satisfied to active transition from the state reported in column to the state reported in row and highlighted with the arrow “>”. For each cell, the arrow refers to the direction of the state transition and the number refers to the transition conditions. States are reported in blue cells with the following acronyms: MS = Mastership, IN = Inauguration, MN = Monitoring. Transition conditions are described in Table 7-13.

MS	<1	<4
>0	IN	<3

	2>	MN
--	----	----

**Table 7-12: OTI Slave Module: FSM Transitions for Product Class 3**

Condition	Transition conditions from mode X to mode Y	Action in Y state
0	<b>From MASTERSHIP to INAUGURATION</b> OTI-S: "Identification Request" message received.	OTI-S: Provides "Slave Identification Ack" message to OTI Master as answer to received "Identification Request" message.
1	<b>From INAUGURATION to MASTERSHIP</b> OTI-S: RESET command received from ETCS or Active Cabin is acquired from rolling stock TIU.	OTI-S: 1) Becomes MASTER if Active Cabin information is acquired from TIU; or; 2) Remains in Slave if RESET command is received.
2	<b>From INAUGURATION to MONITORING</b> OTI-S: OTI Slave performed the paired with OTI Master.	OTI-S: See FSM at §7.1.7.12
3	<b>From MONITORING to INAUGURATION</b> OTI-S: "Identification Request" sent by OTI Master.	OTI-S: Provides "Slave Identification Ack" message to OTI Master as answer to received "Identification Request" message.
4	<b>From MONITORING to MASTERSHIP</b> OTI-S: START or RESET command received from ETCS or Active Cabin is acquired from rolling stock TIU.	OTI-S: Acquires MASTER role if it receives START or Active cabin information, otherwise remains Slave.

**Table 7-13: OTI Slave Module: FSM Transitions conditions for Product Class 3**

#### 7.1.7.10 OTI Slave Mastership State for Product Class 3

Mastership state of OTI Slave for Product Class 3 is described at §7.1.1.1.

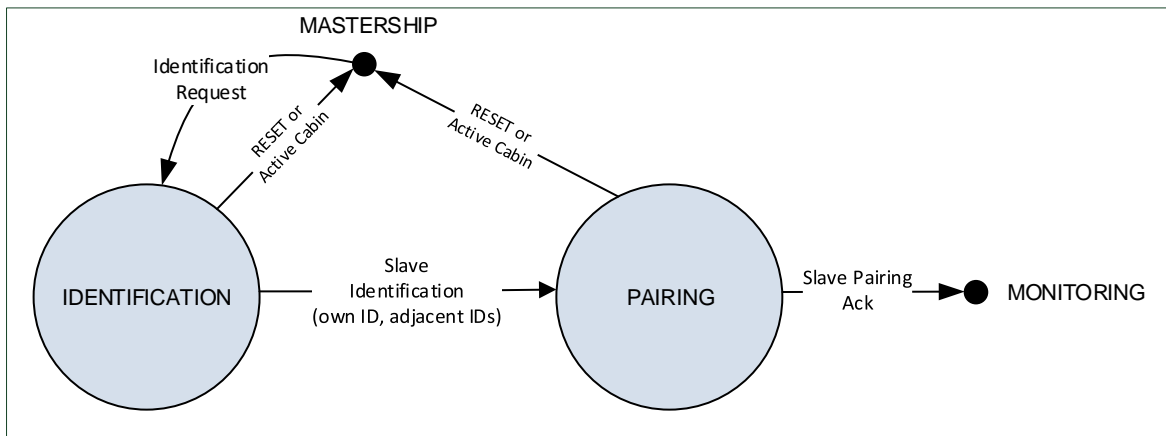
#### 7.1.7.11 OTI Slave Inauguration State for Product Class 3

In case of Product Class 3, the “Paring” status is applied to all OTI Slaves and there is no difference between “Tail” and “Non Tail”. In both cases the OTI Slave sends its status to paired OTI Master.

REQ.7.1.7.17 The OTI Slave of Product Class 3 shall implement the Inauguration state depicted in Figure 7-44.

REQ.7.1.7.18 In the IDENTIFICATION state, the OTI Slave shall determine the identifiers of the adjacent OTIs and consequently its position (Tail, Non Tail) and shall include this information in the “Slave Identification Ack” message with its own identifier.

Note: if the OTI Slave detects only one adjacent ID then it is in Tail position.



**Figure 7-44: FSM OTI Slave: Inauguration State for Product Class 3**

Note that for Product Class 3 the following requirements related to Inauguration state defined in §7.1.5.1 are not applicable:

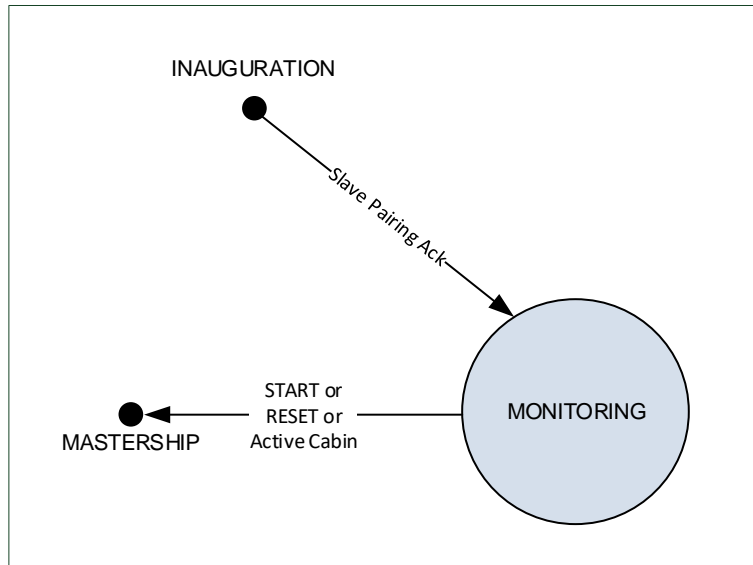
- REQ\_7.1.5.1.1 => for Product Class 3 there is no difference between “Tail” and “Non Tail”;
- REQ\_7.1.5.1.2 => for Product Class 3 there is no difference between “Tail” and “Non Tail”. All the OTIs Slave transit to Pairing state;
- REQ\_7.1.5.1.3 => for Product Class 3 there is no difference between “Tail” and “Non Tail”;

#### 7.1.7.12 OTI Slave Monitoring State for Product Class 3

REQ.7.1.7.19 The OTI Slave of Product Class 3 shall implement the Monitoring state as depicted in the Figure 7-45.

REQ.7.1.7.20 The OTI Slave Tail or Non Tail in the Monitoring state:

- shall determine its status, “coupled” or “separated”, based on the distance with the adjacent OTIs;
- shall provide a status message to the OTI Master as answer to each received request message including its status (“coupled”, “separated” or “unknown”).



**Figure 7-45: FSM OTI Slave: Monitoring State for Product Class 3**

Note that for Product Class 3 the requirements related to Monitoring state defined in §7.1.5.2 are still valid with the followign exceptions:

- REQ\_7.1.5.2.1 => replaced by REQ.7.1.7.19;
- REQ\_7.1.5.2.2 => for Product Class 3 there is no difference between “Tail” and “Non Tail”, each OTI Slave provides to the OTI Master its status (coupled/separated/unknown);
- REQ\_7.1.5.2.3 => for Product Class 3 there is no difference between “Tail” and “Non Tail”, each OTI Slave provides to the OTI Master its status (coupled/separated/unknown);
- REQ\_7.1.5.2.4 => replaced by REQ.7.1.7.20.

#### **7.1.7.13 OTI Slave Interfaces for Product Class 3**

All the requirements defined in §7.1.5.4 are applicable.

REQ.7.1.7.21 The OTI Slave of Product Class 3 shall interface with «separation sensors».

#### **7.1.7.14 OTI Slave Safety Requirements for Product Class 3**

All the requirements defined in §7.1.5.6 are applicable.

## 7.2 Functional Hazard Analysis

This section reports the results of the Preliminary Hazard Analysis (PHA) performed for On-board Train Integrity Monitoring System.

An FMECA approach is used for this functional analysis. The main steps followed are:

- 1) Definition of the System to be analysed
- 2) Identification of the functions performed by the system components
- 3) Hazard identification
  - List of failure modes
  - Identification of possible causes
  - Identification of consequences
- 4) Risk evaluation without mitigations (qualitative analysis)
  - For each failure mode a frequency of occurrence is evaluated;
  - To each failure mode a severity classification is assigned;
  - Risk classification;
- 5) Mitigations Identification
- 6) Risk evaluation with mitigations (qualitative analysis)

At this stage of the project only a preliminary and qualitative risk analysis can be performed and the estimation of some hazards and risks and the related mitigation actions could be rather high-level and not fully detailed. As the design progresses the analysis will be repeated to take into account changes and it will be extended to cover extra details.

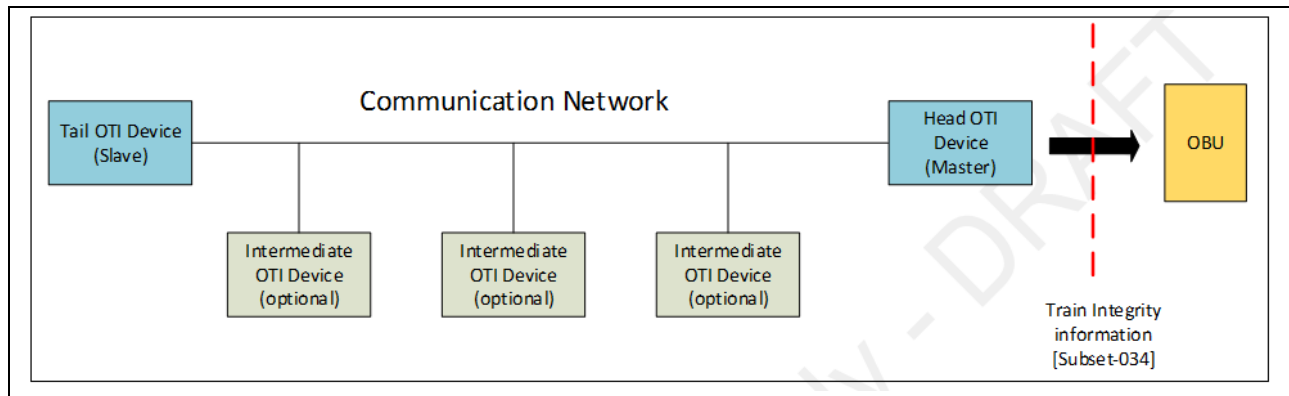
The output of this preliminary hazard analysis are:

- a) a set of safety requirements to be considered in the development of the On-board Train Integrity Monitoring System;
- b) a set of application conditions exported to other on-board subsystem or train operator, driver etc.

Finally, the Appendix B reports the Fault Tree Analysis of Product Classes analysed.

### 7.2.1 System Definition

The preliminary hazard analysis is carried out on the system architecture represented in the block diagram below:



**Figure 7-46: Logical System Architecture**

Where:

- **Tail OTI Device (OTI Slave or OTI-S):** device installed on the tail of the vehicle;
- **NON TAIL OTI Device (OTI-I):** device installed along the vehicle (e.g. installed on each car). Optional device;
- **Communication Network (OCN):** communication channel for the train integrity information. Wired (e.g. cable or Ethernet solution) or Wireless and Open or Closed (see definition EN 50159-2010). In general, the communication between the OTI modules can be bi-directional.
- **Head OTI Device (OTI Master or OTI-M):** device installed on the head of the vehicle. It receives the information of train integrity status by tail OTI device and send it to ETCS TIU module;
- **On-Board Unit (OBU):** it receives the information of train integrity by OTI Master and informs trackside equipment of the status of the vehicle via Position Report.

The ERTMS/ETCS On-Board Unit (OBU) is out of scope of this analysis. The ERTMS/ETCS on-board has to manage the information of train integrity received by OTI monitoring modules as described in UNISIG SUBSET 026 (Ref. [1]) and Change Request 940 (Ref. [3]).

The interface between the ERTMS/ETCS on-board equipment and the vehicle is specified in [2] and [9].

## 7.2.2 Functions Identification

The following sections list the functions performed by each elements identified in Figure 7-46.

### 7.2.2.1 OTI Slave

For the OTI Slave eight (8) functions have been identified:

- FS1: Input acquisition to determine the OTI module role;
- FS2: [Only Product Class 1 and 2] OTI module localisation (TAIL/Non TAIL);
- FS3: Pairing procedure Master-Slave;

- FS4: [Only Product Class 1] Send of Liveliness (Vitality) Message to OTI Master in case of wired communication between OTI Slave and OTI Master;
- FS5: [Only Product Class 2] Acquisition and sending odometer information in case of wireless communication between OTI Slave and OTI Master;
- FS6: [Optional] Acquisition and distribution of cargo/waggon diagnostic information (non vital function);
- FS7: [Only Product Class 3] Identification of adjacent OTIs and sending of this information to OTI Master;
- FS8: [Only Product Class 3] Determination of the status: “coupled”, “separated” or “unknown” and sending of this information to OTI Master.

#### 7.2.2.2 **NON TAIL OTI Module**

For the NON TAIL OTI Module (OTI-I) two (2) functions have been identified:

- FI1: [Only Product Class 1 and 2] OTI module localisation (NON TAIL);
- FI2: [Optional] Acquisition and distribution of cargo/waggon diagnostic information (non vital function);

#### 7.2.2.3 **OTI Master**

For the OTI Master eight (8) functions have been identified:

- FM1: Input acquisition to determine the OTI module role;
- FM2: Pairing procedure Master-Slave;
- FM3: [Only Product Class 1] Reception of Liveliness (Vitality) Message from OTI Slave in case of wired communication;
- FM4: [Only Product Class 2] Reception of odometer information sent from OTI Slave in case of wireless communication between OTI Slave and OTI Master;
- FM5: [Only Product Class 2] Check of train tail movement coherent with front cabin in case of wireless communication between OTI Slave and OTI Master (to perform this check the OTI Master needs to acquire odometer information and train length from an independent source (see Figure 7-57) ;
- FM6: Evaluate and send of Train Integrity information to ERTMS/ETCS on-board equipment;
- FM7: [Optional] Acquisition of cargo/waggon diagnostic information and delivery to train Driver and/or wayside maintenance center (non-vital function);
- FM8: [Only Product Class 3] Determination of train composition (sequence of IDs);

### 7.2.3 **Hazard identification**

For the hazard identification, the FMECA technique is used. The approach used for accomplishing the FMECA is the functional approach. Each element identified in §7.2.1 is designed to perform a number of functions (specified in §7.2.2) and for each function possible failure modes are analysed. For the analysis, each single item failure is to be considered the only failure in the system.



### 7.2.3.1 Failure Modes

This section lists the failure modes applicable sequentially to each element defined in §7.2.1. Typical failure modes considered include:

- failure to perform the function;
- incorrect performance of output function;
- incorrect timing of output function.

The selected set of guidewords is defined in UNISIG SUBSET 077 (Ref. [10]) with one change:

1. “Delay” has been substituted with “Early” and “Late”;

The following Table 7-14 reports the list of the failure mode considered in the analysis and their interpretation:

Failure Mode	Interpretation
Corruption	Failure to transmit correct data; or Input data not correct; or Function performed but not correctly
Deletion	Failure to transmit data; or Input/Output data deleted Function not performed
Early	Flow of Input/Output data occurs before it was intended; or Function operated too soon
Late	Flow of input/output data occurs after it was required; or Function operated too late
Insertion	Additional message received or transmitted
Masquerade	A non-authentic message is designed to appear to be authentic
Repetition	Single message is sent or received more than once
Re-sequence	Order of messages is changed (Wrong order)

**Table 7-14: Failure Mode**

### 7.2.3.2 Failure Causes

For each failure mode described in Table 7-14, all probable failure causes will be identified and described.

### 7.2.3.3 Failure Effects

Three possible failure effects will be identified:

**Local:** Local effects concentrate specifically on the impact the assumed failure mode has on the operation and function of the *item under consideration*. The local effect can be the failure mode itself;

**Intermediate:** Intermediate effects will define the impact that the assumed failure mode has on the *other OTI monitoring module or on-board functions*;

**Initial End Effect:** End Effect will define the total effect the assumed single macro function failure has on the *operation, function or status of the system*.

[Note: 'Initial' refers to 'before credit for barriers', see SUBSET 077 page 12 §7.2.2.1]

#### 7.2.4 Risk evaluation without mitigation

A **severity** classification is assigned to each failure mode according to the failure consequences. Severity categories are defined in **EN 50126** Standard (Ref. [11]) and are reported in the Table 7-15:

Severity Level	Consequence to Persons or Environment
Catastrophic	Fatalities and/or multiple severe injuries and/or major damage to the environment
Critical	Single fatality and/or severe injuries and/or significant damage to the environment
Marginal	Minor injury and/or significant threat to the environment
Insignificant	Possible minor injury

Table 7-15: Severity Level (EN 50126)

For each failure mode a **frequency** (or **probability**) of occurrence is evaluated. Frequencies of occurrence are defined in **EN 50126** Standard (Ref. [11]) and are reported in the Table 7-16:

Category	Description
Frequent	Likely to occur frequently
Probable	it will occur several times
Occasional	likely to occur several time
Remote	likely to occur sometime in the system life cycle

**Table 7-16: Frequency or Probability of Occurrence**

A first risk evaluation is performed by combining the frequency of occurrence of a hazardous event with the severity of its consequences. To establish the risk level generated by the hazardous event, the categories defined in **EN 50126** Standard (Ref. [11]) are used and are reported in the table below:

<b>Risk Category</b>	<b>Action to be applied</b>
Intolerable	The risk shall be eliminated
Undesirable	Shall only be accepted when the risk reduction is impracticable and with the agreement of the Railway Authority
Tolerable	Acceptable with adequate control and the agreement of the Railway Authority
Negligible	Acceptable without any agreement of the Railway Authority

**Table 7-17: Risk Categories**

The following matrix, defined in **EN 50126** (Ref. [11]), identifies an example of risk evaluation and acceptance:

	<b>Insignificant</b>	<b>Marginal</b>	<b>Critical</b>	<b>Catastrophic</b>
<b>Frequent</b>	Undesirable	Intolerable	Intolerable	Intolerable
<b>Probable</b>	Tolerable	Undesirable	Intolerable	Intolerable
<b>Occasional</b>	Tolerable	Undesirable	Undesirable	Undesirable
<b>Remote</b>	Negligible	Tolerable	Undesirable	Undesirable
<b>Improbable</b>	Negligible	Negligible	Tolerable	Tolerable
<b>Incredible</b>	Negligible	Negligible	Negligible	Negligible

**Table 7-18: Risk evaluation and acceptance**

### 7.2.5 Mitigations Identification

In this step of the analysis, all possible measures to protect or mitigate against the effect of the failure shall be identified. Such measures could be for example requirements to be implemented by the OTI module or operation rules/actions.

### 7.2.6 Risk evaluation with mitigation

Risk evaluation considering all the mitigations identified.

### 7.2.7 FMECA Worksheet

The FMECA worksheet includes the following fields:

1. **Element:** This field identifies the element to be analysed: OTI Slave, NON TAIL OTI module, OTI Master;
2. **Function:** This field identifies the functions of each element to be analysed (see §7.2.2);
3. **Input/Output Flow:** This column specifies if the function needs a data input to be performed or provides a data output;
4. **Failure Modes:** This field specifies the failure modes applied (see §7.2.3.1, Table 7-14);
5. **Possible Cause:** list of possible failure causes;
6. **Failure Effects:** local, intermediate and end possible effects (see §7.2.3.3)
7. **Safety Status:** This field specifies what the end impact of the failure is. Possible values:
  - Safety issue, or
  - RAM issue, or
  - No effect;
8. **Hazard ID:** This field reports the hazard ID in the form of “*OTI\_HZ\_XXX*” where XXX is a progressive number (see §7.2.7.2);
9. **Risk evaluation without mitigation** (frequency/severity/risk classification): first qualitative risk evaluation without considering any mitigation (see §7.2.4). The risk evaluation is performed only if the “Safety Status” field specifies an impact on the safety of the system;
10. **Mitigations:** This field lists the mitigations identified to mitigate the hazard in the form of “*OTI\_MIT\_XXX*” where XXX is a progressive number of three digits. For each mitigation is specified:
  - if it is “safety-related” or “not safety-related”;
  - if it is Internal or External to the OTI Monitoring System;

- the equipment (e.g. OTI Slave, OTI Master, etc.) or the entity (e.g. Driver, Maintainer, etc.) in charge to implement the mitigation;
- the Product Class for which the mitigation is applicable;
- the evidence of correct Mitigation implementation;

See §7.2.7.3.

11. **Risk evaluation with mitigation** (frequency/severity/risk classification): final qualitative risk evaluation considering all the mitigations identified (see §7.2.6);

12. **Comments**

#### 7.2.7.1 FMECA Worksheet Structure

Element	Function	Input/Output Flow	Failure Mode	Possible Cause	Failure Effects			Safety Status	Hazard ID
					Local	Intermediate	Initial End Effect		

Risk evaluation without mitigation			Mitigations	Risk evaluation with mitigation			Comments
Probability	Severity	Risk		Probability	Severity	Risk	

Figure 7-47: FMECA Worksheet

#### 7.2.7.2 Hazard Description sheet

ID	Hazardous situation description	Note
OTI_HZ_001	Hazard description	

Figure 7-48: Hazard description sheet

### 7.2.7.3 Mitigation sheet

Mitigation ID	Mitigation description	Safety related (Y/N)	Internal/ External	Mitigation Assigned to	Product Class	Mitigation Implementation (reference)

Figure 7-49: Mitigation sheet

## 7.2.8 Product Classes Hazard Analysis

A hazard analysis is performed for each Product Class defined in Table 6-4 and Table 6-5.

The assumptions for the analysis are:

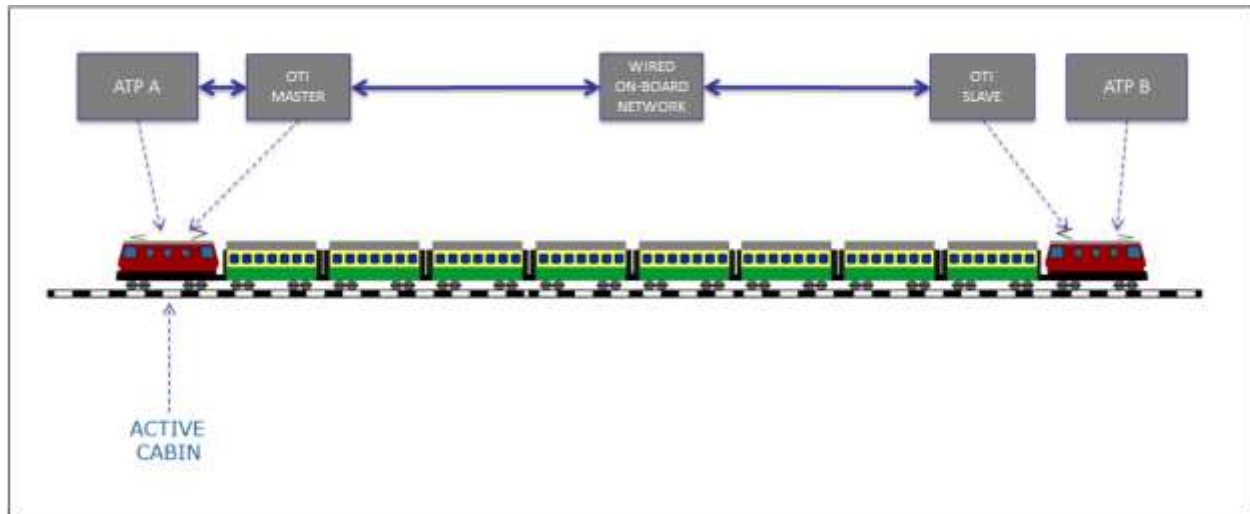
- A1. The OTI role is determined by the information received by ERTMS/ETCS On-board equipment (START command or TRAIN LENGTH) or by the Cabin status acquired by TIU.
- A2. The OTI Master communicates to ERTMS/ETCS On-board the following information about the integrity of the vehicle (Ref. [2] and [3]):
  - a. Train integrity confirmed;
  - b. Train integrity lost;
  - c. Train integrity status unknown;
- A3. The communication type between the OTI modules is Master – Slave (see §7.1.4.1, REQ\_7.1.4.1.2 and REQ\_7.1.4.1.5). Each OTI module shall evaluate the consistent of received messages (see REQ\_7.1.1.3.11).
- A4. Each single item failure is to be considered the only failure in the system.

To simplify the analysis reported in Appendix A, the following abbreviations will be used:

Info Id	information	Description
Info_1	[Cab Status = Cab Active] AND [Engine = Lead]	This information allows to an OTI module to become MASTER.  Note 1: as explained in REQ_7.1.1.1.2, OTI module behaves as OTI Master if connected to active cabin;  Note 2: it is specified also the role of the locomotive (Lead Engine or Slave Engine) to include the case of a loco in Non-Leading mode;
Info_2	Cab Status = Cab No Active	This information allows to an OTI module to become MASTER or remains as SLAVE.
	[Cab Status = Cab Active] AND [Engine = No Lead]	
	No info received about the Cab Status	

### 7.2.8.1 Hazard Analysis for Product Class 1-A

This section includes the hazard analysis performed for the Product Class 1-A (see definition in Table 6-4) with ERTMS/ETCS On-board at train tail, wired communication and no NON TAIL OTI module (see Figure 7-50 below).



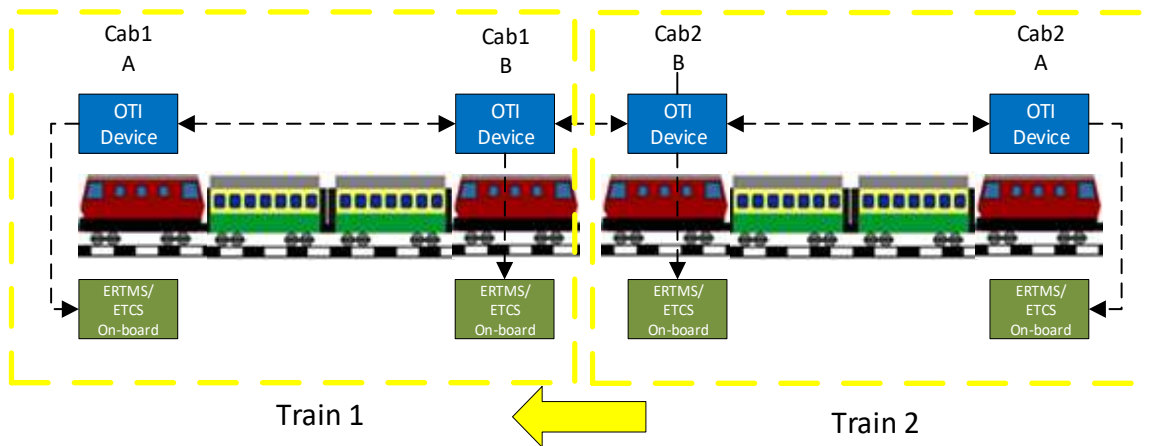
**Figure 7-50: Example of Product Class 1-A**

The analysis is reported in Appendix C.

#### 7.2.8.1.1 Hazard Analysis for Product Class 1-A in case of joining train scenario

This section includes the analysis for the joining scenario as depicted in Figure 7-51 (Train 2 is joined to Train 1). In this scenario the main risk could be that the OTI Master receives the vitality messages from a NON TAIL OTI Slave module. For example, the OTI Master of cabin Cab1 A receives the vitality messages from the OTI Slave of cabin Cab1 B instead from OTI Slave of cabin Cab2 A of Train 2 with impact on the safety of the system (a break of Train 2 is not detected). See §7.1.5.5 for an example of train joining.





**Figure 7-51: Product class 1-A: example of joining scenario**

The assumptions for the analysis are:

- A1. The analysis for the OTI Master and OTI Slave in this configuration is the same as the one performed for single train (§7.2.8.1);
- A2. The joining procedure, that's how the electrical and mechanical links between the two trains have to be managed, is out of scope of the analysis.

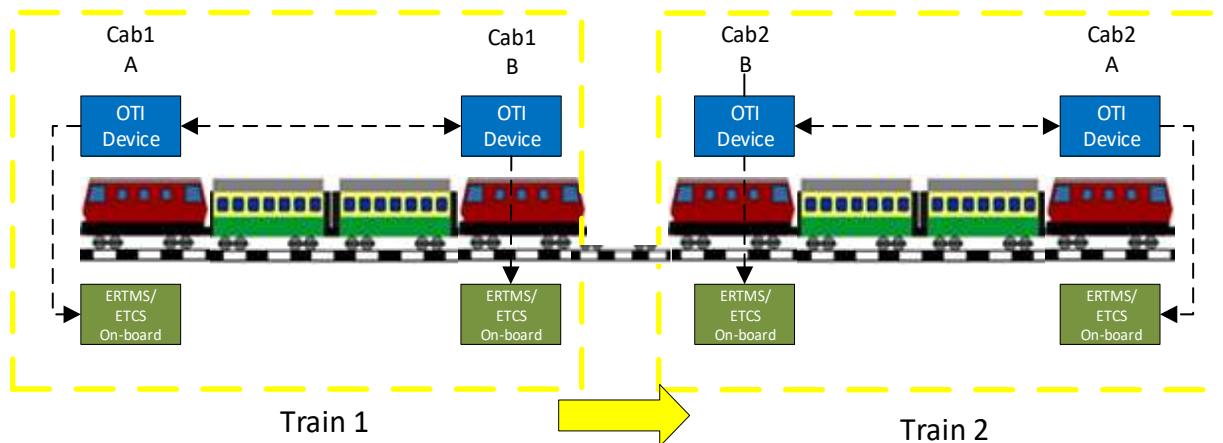
The analysis is reported in Appendix D.

#### 7.2.8.1.2 Hazard Analysis for Product Class 1-A in case of splitting train scenario

Figure 7-52 shows an example of splitting operation where Train 2 is splitting from Train 1.

If the On-board Train Integrity Monitoring System is not restarted after the separation, the OTI Master does not receive any more the vitality messages and declares the train integrity lost with an impact on the availability of the system. The analysis of train separation is the same for single train, so it is possible to refer to the analysis performed in Appendix C.

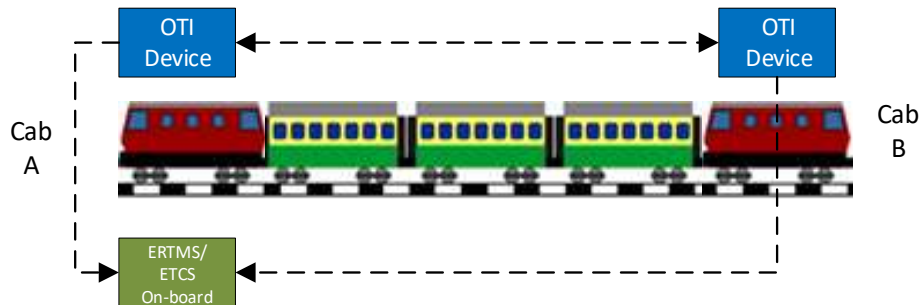
Note: The splitting procedure, that's how the electrical and mechanical links between the two trains have to be managed, is out of the scope of the analysis.



**Figure 7-52: Product class 1-A: example of splitting scenario**

### 7.2.8.2 Hazard Analysis for Product Class 1-B

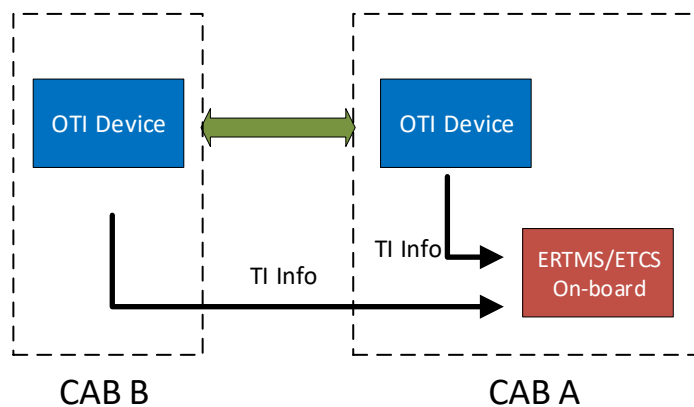
This section includes the hazard analysis performed for the Product Class 1-B (see definition in **Table 6-4**) with no ERTMS/ETCS On-board at train tail, wired communication and no NON TAIL OTI module (see Figure 7-53 below).



**Figure 7-53: Example of Product Class 1-B**

The assumptions for the analysis are:

- A1. Train consist includes two cabins (Cab A and Cab B) and is equipped with one ETCS/ERTMS On-board system (e.g. installed in cabin A). This means that the OTI modules, at the head and at tail of train, shall be connected to same ETCS/ERTMS On-board system:

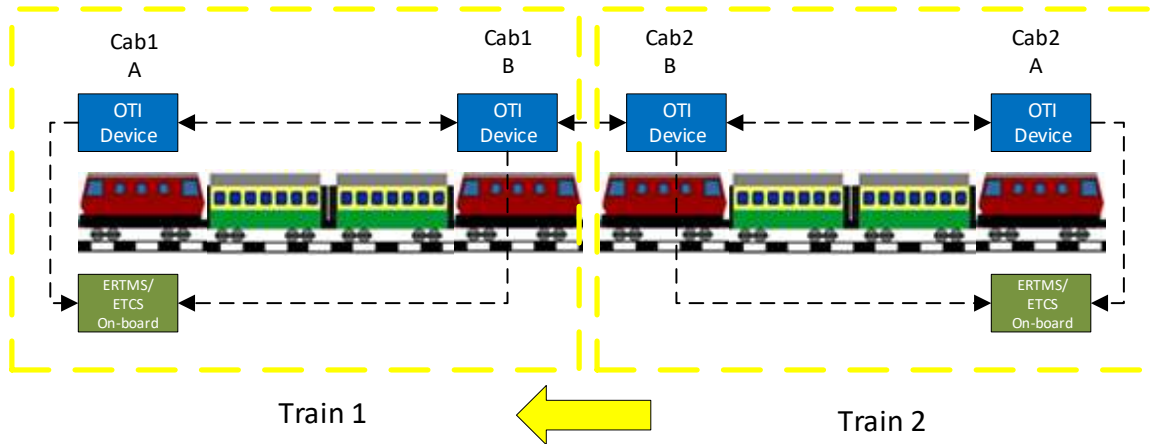


**Figure 7-54: OTI modules configuration with two cabins and one ETCS/ERTMS On-board system**

The analysis is reported in in Appendix E.

#### 7.2.8.2.1 Hazard Analysis for Product Class 1-B in case of joining train scenario

This section includes the analysis for the joining scenario as depicted in Figure 7-55 (Train 2 is joined to Train 1). In this scenario, the main risk could be that the OTI Master receives the vitality messages from a NON TAIL OTI Slave module. For example, the OTI Master of cabin Cab1 A receives the vitality messages from the OTI Slave of cabin Cab1 B instead from OTI Slave of cabin Cab2 A of Train 2 with impact on the safety of the system (a break of Train 2 is not detected).



**Figure 7-55: Product class 1-B: example of joining scenario**

The assumptions for the analysis are:

- A1. The analysis for the OTI Master and OTI Slave in this configuration is the same as the one performed for single train (§7.2.8.2);
- A2. The joining procedure, that's how the electrical and mechanical links between the two trains have to be managed, is out of scope of the analysis;

The analysis is reported in Appendix F.

#### 7.2.8.2.2 Hazard Analysis for Product Class 1-B in case of splitting train scenario

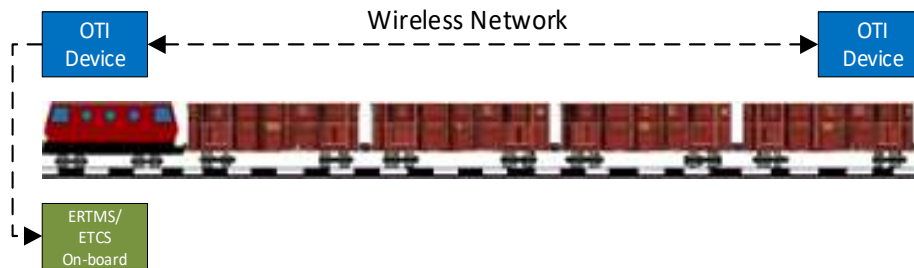
In the splitting train operation, if the On-board Train Integrity Monitoring System is not restarted, after the separation, the OTI Master does not receive any more the vitality messages and declares the train integrity lost with an impact on the availability of the system. The analysis of train separation is the same for single train, so it is possible to refer to the analysis performed in the in Appendix E.

Note: The splitting procedure, that's how the electrical and mechanical links between the two trains have to be managed, is out of the scope of the analysis.

See §7.1.5.5 for an example of splitting train.

#### 7.2.8.3 Hazard Analysis for Product Class 2-A

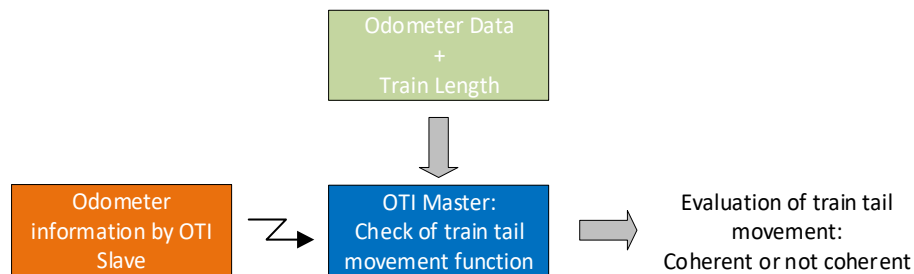
This section includes the hazard analysis performed for the Product Class 2-A (see definition in Table 6-4) with no ERTMS/ETCS On-board at train tail, wireless communication and no NON TAIL OTI module (see Figure 7-56 below).



**Figure 7-56: Example of Product Class 2-A**

The assumptions for the analysis are:

- A1. The OTI module installed on the last waggon/car of the consist is not connected to any ERTMS/ETCS on-board equipment;
- A2. About the requirements REQ\_7.1.1.5.1, REQ\_7.1.5.3.1 and REQ\_7.1.5.4.2: no specific odometer information source is specified for OTI Slave and OTI Master;
- A3. About the requirement REQ\_7.1.2.3.1: no specific source is considered for train length value acquired by OTI Master. See figure below:



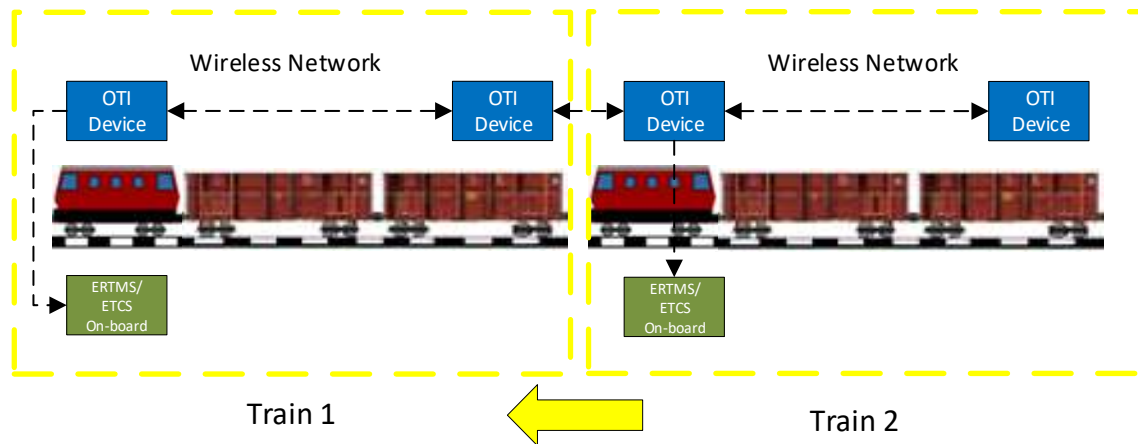
**Figure 7-57: OTI Master: Check of train tail movement function**

The analysis is reported in Appendix G.

#### 7.2.8.3.1 Hazard Analysis for Product Class 2-A in case of joining train scenario

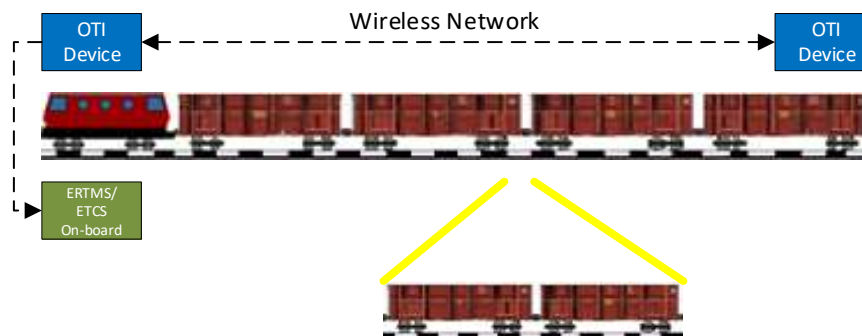
This section includes the analysis for the joining scenario. Three possible scenarios are depicted in the following:

- 1) In the first scenario, the joining is performed between two consists; Train 2 is joined to Train 1 (see Figure 7-58). In this scenario, the main risk could be that the OTI Master receives the odometer information from a NON TAIL OTI Slave module. For example, the OTI Master of Train 1 receives the odometer information from the OTI Slave of Train 1 instead from OTI Slave of Train 2 with impact on the safety of the system (a break of Train 2 is not detected).



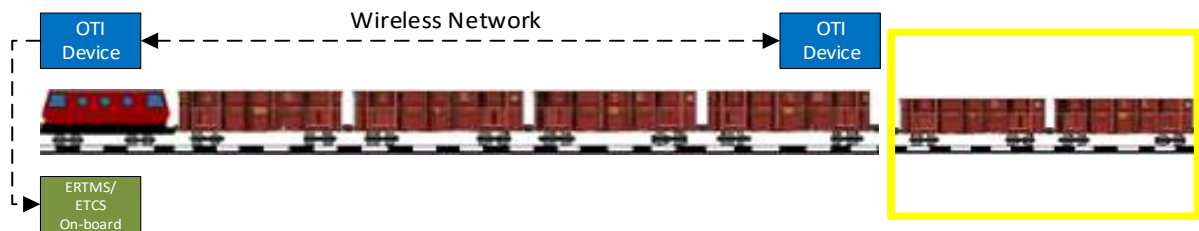
**Figure 7-58: Product Class 2-A: joining between two consists**

- 2) Figure 7-59 describes the scenario where some cars/wagons are added into the middle of original train consist. In this scenario, the main risk could be that the OTI Master does not receive the update of the train length value (greater than the first one) with impact on the availability of the system. In fact, in this case the OTI Master could evaluate the movement of train tail not coherent with the head and consequently declares the loss of train integrity.



**Figure 7-59: Product Class 2-A: cars/wagons added into the middle of consist**

- 3) Figure 7-60 describes the scenario where some cars/wagons are added at the end of the original consist. In this scenario the following two risks shall be considered:
- the OTI Master receives the odometer information from the OTI Slave module not installed on the last waggon with impact on the safety of the system (a break of some waggons after the OTI module is not detected);
  - The OTI Master does not receive the update of the train length value (greater than the first one). The OTI Master could evaluate the movement of train tail not coherent with the head and consequently declares the loss of train integrity with an impact on the availability of the system.



**Figure 7-60: Product Class 2-A: cars/waggons added at the end of consist**

The assumptions for the analysis are:

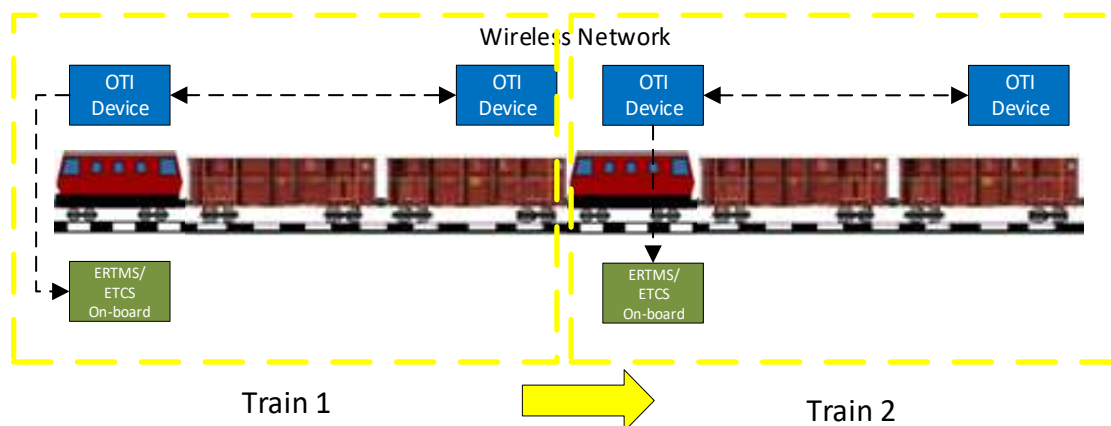
- A1. The analysis for the OTI Master and OTI Slave after the joining procedure is the same as the one performed for single train (§7.2.8.3);
- A2. The joining procedure, that's how the electrical and mechanical links between the two trains have to be managed, is out of scope of the analysis.

The analysis is reported in Appendix H.

#### 7.2.8.3.2 Hazard Analysis for Product Class 2-A in case of splitting train scenario

This section includes the analysis for the splitting scenario. Three possible scenarios are depicted in the following:

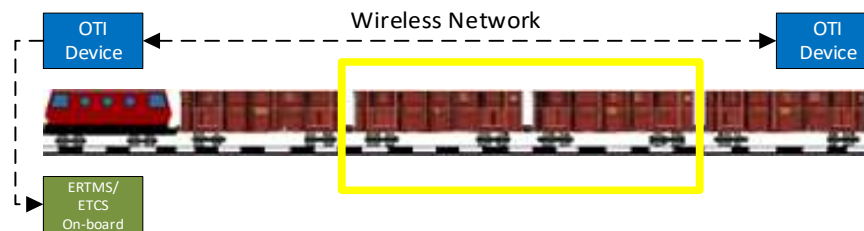
- 1) In the first scenario (Figure 7-61), the splitting is performed between two consists, Train 1 and Train 2. In this scenario, the main risk could be that the OTI Master of Train 1 continues receiving for a short period of time the odometer information from OTI Slave of Train 2 until the OTI Master declares the train integrity lost. The only impact is on the availability of the system.



**Figure 7-61: Product Class 2-A: splitting between two consists**

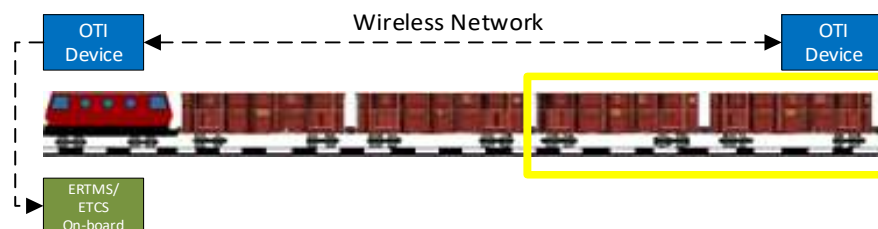
- 2) Figure 7-62 describes the scenario where some cars/waggons are detached from the middle of original train consist. In this scenario, the risk could be that the OTI Master does not receive the update of the train length value (less than the first one) with impact on the safety of the system. In fact, in this case the OTI Master could evaluate the movement of train tail coherent

with the head even if some car/waggons have been lost due to a train broken and consequently declares the train integrity as confirmed.



**Figure 7-62: Product Class 2-A: cars/waggons detached from the middle of consist**

- 3) Figure 7-63 describes the scenario where some cars/waggons are detached from the end of the original consist. In this scenario, the following two events shall be considered depends on if each car/waggon is equipped with an OTI module (case b.) or not (case a.):
- After the splitting operation, the OTI Slave is not installed on the new last car/waggon with the impossibility to realise the Master – Slave communication. Impact on the availability.
  - if the On-board OTI Monitoring System is not restarted after the splitting operation, the OTI Master could not receive the update of the train length value (less than the first one). The OTI Master could evaluate the movement of train tail coherent with the head and consequently declares the train integrity as confirmed. Impact on the safety.



**Figure 7-63: Product Class 2-A: cars/waggons detached from the end of consist**

The assumptions for the analysis are:

- The analysis for the OTI Master and OTI Slave after the splitting procedure is the same as the one performed for single train (§7.2.8.3);
- The splitting procedure, that's how the electrical and mechanical links between the two trains have to be managed, is out of the scope of the analysis.

The analysis is reported in Appendix H.

#### 7.2.8.4 Hazard Analysis for Product Class 2-B

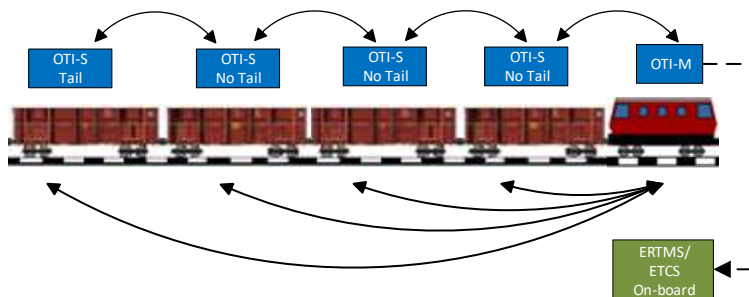
Product Class 2-B differs from Product Class 2-A only for the presence of the energy harvesting system (see Table 6-4). The hazard analysis performed for Product Class 2-A can be repeated for Product Class 2-B.

A malfunctioning of the energy harvesting system can lead to a malfunctioning of the OTI module with an impact on the availability of the OTI system.

Refer to Appendix G.

#### 7.2.8.5 Hazard Analysis for Product Class 3-A

This section includes the hazard analysis performed for the Product Class 3-A (see definition in Table 6-5) with no ERTMS/ETCS On-board at train tail and wireless communication between the OTIs installed on each waggon and on the locomotive (see Figure 7-64).



**Figure 7-64: Example of Product Class 3-A**

The assumptions for the analysis are:

A.1 The position TAIL/NON TAIL of an OTI Slave is determined on the capacity to establish a communication with the adjacent OTI devices.

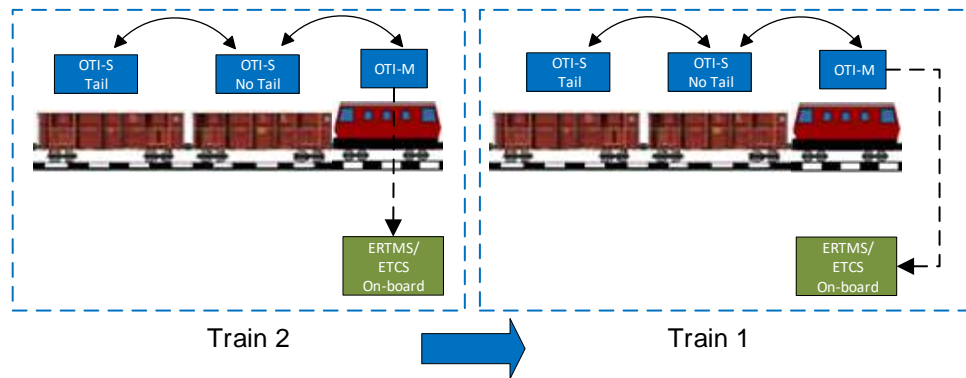
The analysis is reported in Appendix I.

##### 7.2.8.5.1 Hazard Analysis for Product Class 3-A in case of joining train scenario

This section includes the analysis for the joining scenario. Three possible scenarios are depicted in the following:

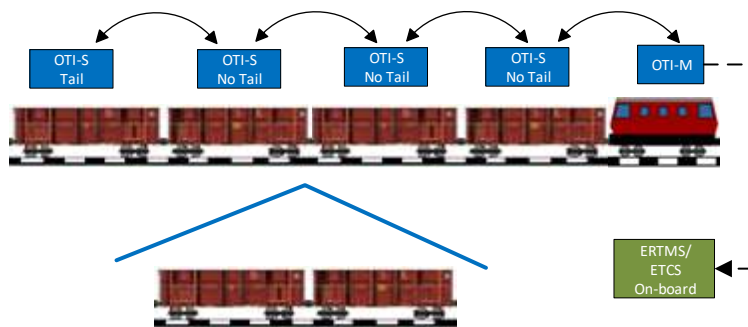
- 1) In the first scenario, the joining is performed between two consists; Train 2 is joined to Train 1 (see Figure 7-65). In this scenario, the main risk could be that the TAIL OTI Slave of Train 1 does not update its position (from TAIL to NON TAIL). In this case the OTI Master continues to evaluate the train integrity considering only the Train 1 (any break of Train 2 is not detected).





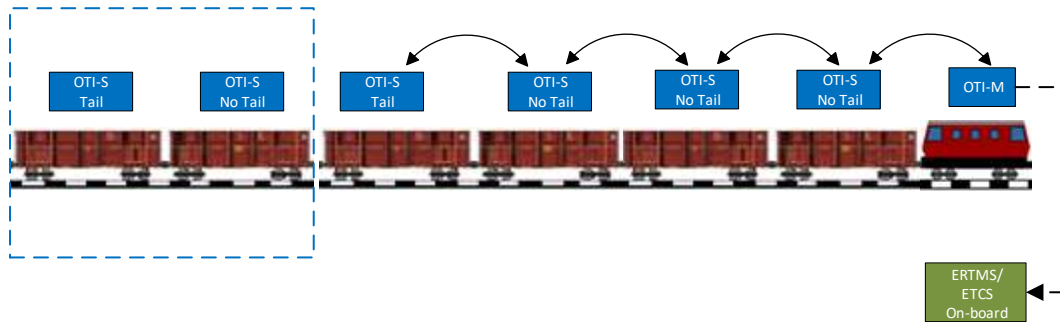
**Figure 7-65: Product Class 3-A: joining between two consists**

- 2) Figure 7-66 describes the scenario where some cars/waggon(s) are added into the middle of original train consist. In this scenario, the main risk could be that the OTI Master does not update the train composition not including the new waggon(s)/car(s) and does not perform the pairing with it(them) with possible impact on the safety. In this case the OTI Master does not know the status (“coupled” or “separated”) of new waggon(s)/car(s).



**Figure 7-66: Product Class 3-A: cars/waggon(s) added into the middle of consist**

- 3) Figure 7-67 describes the scenario where some cars/waggon(s) are added at the end of the original consist. In this scenario, the main risk could be that the initial TAIL OTI Slave does not update its position (from TAIL to NON TAIL) and does not evaluate the distance between the waggon where it is installed and the new joined waggon/car. In this case the OTI Master continues to evaluate the train integrity not including the new waggon(s)/cars.



**Figure 7-67: Product Class 3-A: cars/waggons added at the end of consist**

The assumptions for the analysis are:

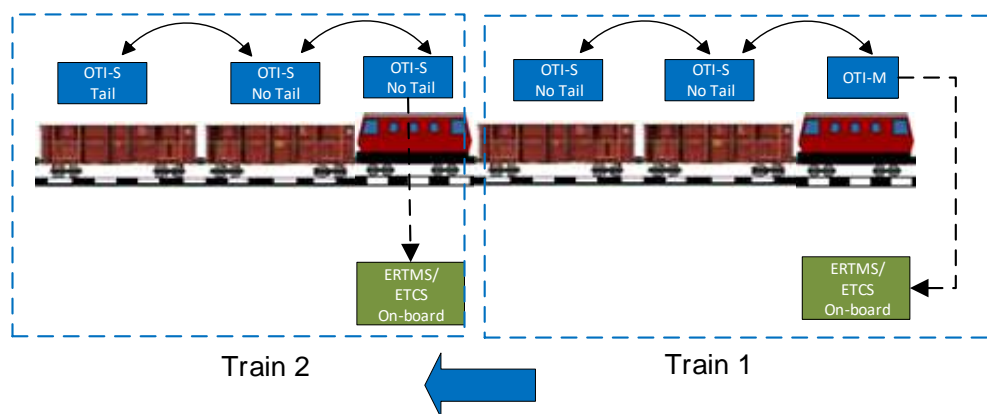
- A1. The analysis for joining scenarios is the same performed for single train in §7.2.8.5 plus the analysis of the transition from TAIL to NON TAIL described in scenario 1);
- A2. The joining procedure, that's how the electrical and mechanical links between the two trains have to be managed, is out of scope of the analysis.

The analysis is reported in Appendix J.

#### 7.2.8.5.2 Hazard Analysis for Product Class 3-A in case of splitting train scenario

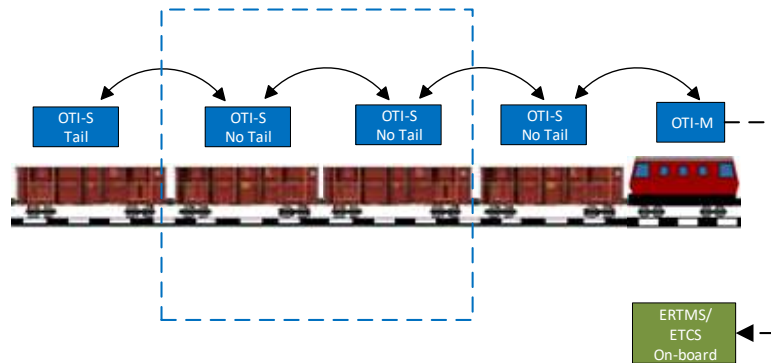
This section includes the analysis for the splitting scenario. Three possible scenarios are depicted in the following:

- 1) In the first scenario, the splitting is performed between two consists; Train 1 and Train 2 (see Figure 7-68). In this scenario, the main risk could be that the OTI Master of Train 1 continues receiving the information from OTI device of Train 2 and the last OTI Slave of Train 1 does not change its position from NON TAIL to TAIL. In this case when the Train 1 starts to move the OTI Master declares the train integrity lost with impact on the availability.



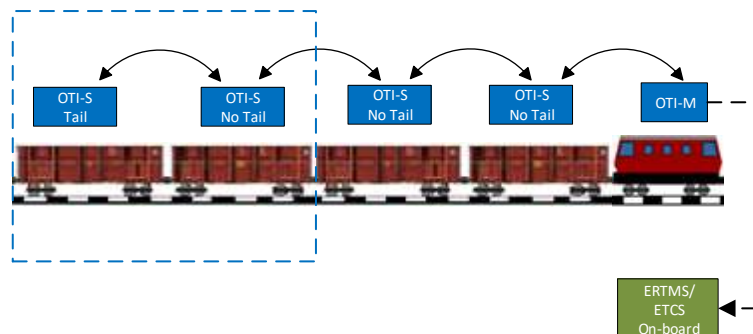
**Figure 7-68: Product Class 3-A: splitting between two consists**

- 2) Figure 7-69 describes the scenario where some cars/waggon(s) are detached from the middle of original train consist. In this scenario, the main risk could be that the OTI Master does not update the train composition not excluding the detached waggon(s)/car(s). In this case the OTI Master does not receive the status of the detached waggon(s)/car(s) and declares the train integrity lost with availability impact.



**Figure 7-69: Product Class 3-A: cars/waggon(s) detached from the middle of consist**

- 3) Figure 7-70 describes the scenario where some cars/waggon(s) are detached from the end of the original consist. In this scenario, the main risk could be that the OTI Master continues receiving the information from the initial OTI Slave TAIL and the last OTI Slave does not change its position from NON TAIL to TAIL. In this case when the train starts to move the OTI Master declares the train integrity lost with impact on the availability.



**Figure 7-70: Product Class 3-A: cars/waggon(s) detached from the end of consist**

The assumptions for the analysis are:

- A1. The analysis for splitting scenarios is the same performed for single train in §7.2.8.5;
- A2. The splitting procedure, that's how the electrical and mechanical links between the two trains have to be managed, is out of scope of the analysis.

#### **7.2.8.6 Hazard Analysis for Product Class 3-B**

Product Class 3-B differs from Product Class 3-A only for the presence of the energy harvesting system (see Table 6-5). The hazard analysis performed for Product Class 3-A can be repeated for Product Class 3-B.

A malfunctioning of the energy harvesting system can lead to a malfunctioning of the OTI module with an impact on the availability of the OTI system.

Refer to Appendix I.

## 7.2.9 Hazards List

Table 7-19 includes the list of identified hazards. Column “Note” specifies for which Product Class the hazard is applicable. Refer also to Hazard table included in Appendix K.

ID	Hazardous situation description	Note
OTI_HZ_001	OTI Slave sends incorrect liveness messages.	Applicable for the Product Class: 1-A 1-B
OTI_HZ_002	The ERTMS/ETCS On-board equipment receives inappropriate Train Integrity Confirmation (incorrect or earlier information)	Applicable for the Product Class: 1-A 1-B 2-A 2-B 3-A 3-B
OTI_HZ_003	OTI Slave is not installed on the last car/waggon but it localizes itself on the last waggon/car or the OTI Master receives an incorrect identification message from OTI Slave ("TAIL" instead of "Non TAIL")	Applicable for the Product Class: 1-A 1-B 2-A 2-B
OTI_HZ_004	The OTI Master receives inappropriate Train Integrity information (incorrect information, earlier or later, masquerade, etc.).	Applicable for the Product Class: 1-A 1-B
OTI_HZ_005	The OTI Slave sends to OTI Master incorrect odometer information	Applicable for the Product Class: 2-A 2-B
OTI_HZ_006	OTI Master receives inappropriate odometer information by OTI Slave (incorrect information, inserted information, masquerade information, etc.)	Applicable for the Product Class: 2-A 2-B
OTI_HZ_007	OTI Master receives incorrect information (odometer data and train length value) for the evaluation of the train tail movement	Applicable for the Product Class: 2-A 2-B
OTI_HZ_008	OTI Master pairs with NON TAIL OTI Slave module.	Applicable for the Product Class: 1-A 1-B 2-A 2-B

ID	Hazardous situation description	Note
OTI_HZ_009	OTI Master establishes a communication with an OTI Slave not belonging to the same consist.	Applicable for the Product Class: 2-A 2-B
OTI_HZ_010	The OTI Master receives an inappropriate change of cabin status (from "active" to "not active") and becomes Slave.	Applicable for the Product Class: 1-A 1-B 2-A 2-B 3-A 3-B
OTI_HZ_011	The OTI Slave erroneously receives the information of "Cab status = Cab active" and becomes Master	Applicable for the Product Class: 1-B
OTI_HZ_012	The OTI Master receives the diagnostic message by OTI Slave but it appears as the vitality message	Applicable for the Product Class: 2-A 2-B 3-A 3-B
OTI_HZ_013	The OTI Master receives incorrect OTI Slave status ("coupled" instead of "separated") or does not receive the status from at least one OTI Slave	Applicable for the Product Class: 3-A 3-B
OTI_HZ_014	OTI Master considers an OTI Slave as TAIL when it is not. In this case a waggon/car that belongs to a consist it is erroneously considered as not part of it.	Applicable for the Product Class: 3-A 3-B

**Table 7-19: List of identified hazards**

### 7.2.10 Mitigation List

This section includes the list of mitigations identified during the analysis split in safety-related and not safety-related (see Table 7-20). Refer also to Mitigation table of Appendix K (Table 10-3).

Mitigation ID	Mitigation description	Safety related (Y/N)	Internal/ External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)
OTI_MIT_001	An installation procedure shall be defined for OTI modules Slave to avoid the following availability issues: 1) the OTI module receives an incorrect cabin input and configures itself as Master with the impossibility to establish the	N	External	Railway operator	1-A 2-B 2-A 2-B 3-A 3-B	

Mitigation ID	Mitigation description	Safety related (Y/N)	Internal/ External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)
	communication with the real OTI Master; 2) Following joining/splitting operations, the OTI Slave is not moved or installed on the last waggon/car, consequently, it configures itself as Non-TAIL instead of TAIL.					
OTI_MIT_002	OTI module shall manage communication in compliancy to 50159:2010	Y	Internal	OTI module (Master and Slave)	1-A 1-B 2-A 2-B 3-A 3-B	REQ_7.1.4.3
OTI_MIT_003	If the OTI Master receives inconsistent messages or does not receive any message from OTI Slave or receives messages in incorrect time, then it shall communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity Lost".	Y	Internal	OTI Master	1-A 1-B 2-A 2-B	REQ_7.1.1.3.12 REQ_7.1.1.3.4
OTI_MIT_004	Evaluating defining an installation procedure with the operator in relation to composition phase before starting train mission	Y	External	Railway operator	1-A 1-B 2-A 2-B	
OTI_MIT_005	The procedure of automatic OTI module localisation shall be performed in safe manner, i.e. each OTI modules shall localize itself in the correct position in the vehicle, the OTI Slave TAIL in the last waggon/car and the NON TAIL OTI modules in intermediate position.	Y	Internal	OTI module	1-A 1-B 2-A 2-B	REQ_7.1.5.2.2 REQ_7.1.5.2.3 REQ_7.1.5.6.1
OTI_MIT_006	The OTI module configured as Slave (TAIL or Non TAIL)	Y	Internal	OTI Slave	1-A 1-B 3-A	REQ_7.1.5.2.5

Mitigation ID	Mitigation description	Safety related (Y/N)	Internal/ External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)
	shall not communicate any train integrity information to the ERTMS/ETCS On-board equipment or shall communicate the information of "Train integrity status unknown".				3-B	
OTI_MIT_007	The OTI modules shall acquire the cab status information via a vital input. The OTI module connected to the "active" cabin shall be configured as "Master". The OTI module connected to the "not active" cabin shall be configured as "Slave".	Y	Internal	OTI module (Master and Slave)	1-A 1-B 3-A 3-B	REQ_7.1.1.1.1 REQ_7.1.1.1.2 REQ_7.1.1.1.3 REQ_7.1.1.7.1 REQ_7.1.5.6.1
OTI_MIT_008	Intentionally deleted					
OTI_MIT_009	The OTI module shall provide to the ERTMS/ETCS On-board equipment a vital Train Integrity information	Y	Internal	OTI Master	1-A 1-B 2-A 2-B 3-A 3-B	REQ_7.1.1.3.3 REQ_7.1.1.7.1
OTI_MIT_010	The interface between the OTI module and the ERTMS/ETCS On-board equipment shall be vital.	Y	Internal/ External	OTI Module // ERTMS/ETCS On-board equipment	1-A 1-B 2-A 2-B 3-A 3-B	REQ_7.1.1.7.1 REQ_7.1.5.6.1
OTI_MIT_011	The OTI Master shall not accept the Pairing ACK message if it is received by an OTI Slave module NON TAIL.	Y	Internal	OTI module (Master)	1-A 1-B 2-A 2-B	REQ_7.1.1.2.4
OTI_MIT_012	The OTI Slave module Non TAIL shall not accept the Pairing Request Message sent by OTI Master	Y	Internal	OTI module (Slave Non TAIL)	1-A 1-B 2-A 2-B	REQ_7.1.5.1.1
OTI_MIT_013	If the OTI modules manage diagnostic information, the communication	Y	Internal	OTI module (Master and Slave)	2-A 2-B 3-A 3-B	REQ_7.1.1.7.4 REQ_7.1.5.6.4



Mitigation ID	Mitigation description	Safety related (Y/N)	Internal/ External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)
	protocol between OTI modules shall use different messages for diagnostic and train integrity information					
OTI_MIT_014	The information of odometer data and train length value shall be acquired by OTI Master via vital input	Y	Internal	OTI Master	2-A 2-B	REQ_7.1.1.7.1
OTI_MIT_015	The information of odometer data and train length value sent to OTI Master shall be safety related	Y	External	Odometer source for OTI Master	2-A 2-B	
OTI_MIT_016	The ERTMS/ETCS On-board equipment shall be able to distinguish the source of the Train Integrity information (if Master or Slave and via a unique identifier).	Y	External	ERTMS/ETCS On-board equipment	1-B	
OTI_MIT_017	If the OTI Master receives more than one message from two or more OTI Slave modules with TAIL identification, then it shall stop or repeat the Inauguration procedure. A timer shall be defined before declaring completed the Inauguration phase. This timer shall be dimensioning based on the specific application.	Y	Internal	OTI Master	1-A 1-B 2-A 2-B	REQ_7.1.1.2.3
OTI_MIT_018	The OTI Master shall not accept information received by other OTI modules configured as Master.	Y	Internal	OTI Master	1-B	REQ_7.1.1.7.2
OTI_MIT_019	Packets exchanged between the OTI modules shall include a field that specifies the OTI identifier (OTI ID) and the OTI role	Y	Internal	OTI module (Master and Slave)	1-A 1-B 2-A 2-B	REQ_7.1.1.7.5 REQ_7.1.5.6.2 REQ_7.1.5.6.3

Mitigation ID	Mitigation description	Safety related (Y/N)	Internal/ External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)
	(Master / Slave TAIL / Slave Non TAIL). OTI identifier shall be unique for each OTI module.					
OTI_MIT_020	The Odometer information acquired by OTI Slave shall be safety related	Y	External	Odometer source	2-A 2-B	
OTI_MIT_021	In case of wireless communication, the OTI Master shall know the ID of OTI Slave with which a pairing procedure will be initiated	Y	Internal	OTI Master	2-A 2-B	REQ_7.1.1.7.3
OTI_MIT_022	If the ERTMS/ETCS On-board equipment receives new valid Train Data (e.g. when the Driver enters, modifies or revalidates the Train Data), then the ERTMS/ETCS On-board equipment shall communicate these operations to OTI Master to start the OTI Master reset procedure	Y	External	ERTMS/ETCS On-board equipment	1-A 1-B 2-A 2-B	
OTI_MIT_023	Following joining/splitting operations, the driver must modify the Train Data such that it fits with the new train composition	Y	External	Driver	1-A 1-B 2-A 2-B	
OTI_MIT_024	The OTI Master shall determine the train composition (sequence of IDs) and shall check the consistency of discovered train composition with the information provided by an external source	Y	Internal	OTI Master	3-A 3-B	REQ.7.1.7.6 REQ.7.1.7.9
OTI_MIT_025	The OTI Master shall reject a "Slave Identification Ack" message sent by an OTI Slave including	Y	Internal	OTI Master	3-A 3-B	REQ.7.1.7.7

Mitigation ID	Mitigation description	Safety related (Y/N)	Internal/ External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)
	the following information: 1) TAIL position, and; 2) the IDs of two adjacent OTI Slave (only one is possible)					
OTI_MIT_026	The OTI Master shall interrupt the Inauguration phase if it receives more than one "Slave Identification Ack" message including the following information: 1) TAIL position;	Y	Internal	OTI Master	3-A 3-B	REQ.7.1.7.8
OTI_MIT_027	The OTI module shall determine its status of "coupled", "separated" or "unknown" in a safe way.	Y	Internal	OTI module (Master and Slave)	3-A 3-B	REQ.7.1.7.15
OTI_MIT_028	The OTI Master shall consider the train integrity as lost if it does not receive the status from at least one OTI Slave into a defined time-out or receives corrupted messages.	Y	Internal	OTI Master	3-A 3-B	REQ.7.1.7.13
OTI_MIT_029	An Installation/Maintenance procedure shall be defined for OTI modules to guarantee the correct functioning in determining the distance between the waggons/cars where they are installed	Y	External	Installer / Maintainer	3-A 3-B	To be exported to Installer / Maintainer

**Table 7-20: List of safety-related mitigations**

### 7.2.11 PHA Conclusion

This first part of PHA has analysed from a safety point of view the functions of the elements of the OTI monitoring system for Product Classes 1, 2 and 3.

These safety analyses have led to express:

- A list of hazards reported in §7.2.9;
- A list of mitigations (reported in Table 7-20) classified into:
  - Internal: mitigations to be implemented by OTI modules;
  - External: mitigations to be implemented by external equipment, such as the ERTMS/ETCS On-board system, or operational procedures for Maintainer/Driver/Installer.

The analysis has also highlighted that the information of train integrity status provided by the OTI modules to ERTMS/ETCS On-board equipment shall be safety-related.

OTI Master shall implement the following safety-related functionalities (see §7.2.2):

- FM1: Input acquisition to determine the OTI module role;
- FM2: Pairing procedure Master-Slave;
- FM3: [Only Product Class 1] Reception of Liveliness (Vitality) Message from OTI Slave in case of wired communication;
- FM4: [Only Product Class 2] Reception of odometer information sent from OTI Slave in case of wireless communication between OTI Slave and OTI Master;
- FM5: [Only Product Class 2] Check of train tail movement coherent with front cabin in case of wireless communication between OTI Slave and OTI Master (to perform this check the OTI Master needs to acquire odometer information and train length from an independent source);
- FM6: Evaluate and send of Train Integrity information to ERTMS/ETCS on-board equipment;
- FM8: [Only Product Class 3] Determination of train composition;

OTI Slave shall implement the following safety-related functionalities (see §7.2.2):

- FS1: Input acquisition to determine the OTI module role;
- FS2: [Only Product Class 1 and 2] OTI module localisation (TAIL/Non TAIL);
- FS3: Pairing procedure Master-Slave;
- FS4: [Only Product Class 1] Send of Liveliness (Vitality) Message to OTI Master in case of wired communication between OTI Slave and OTI Master;
- FS5: [Only Product Class 2] Acquisition and sending odometer information in case of wireless communication between OTI Slave and OTI Master;
- FS7: [Only Product Class 3] Identification of adjacent OTIs and sending of this information to OTI Master;
- FS8: [Only Product Class 3] Determination of the status: “coupled”, “separated” or “unknown” and sending of this information to OTI Master.

In conclusion, the results of this first qualitative analysis shows that:

- OTI Master module shall be SIL4

- OTI Slave module shall be SIL4
- Communication protocol shall be SIL4

The quantitative analysis will be performed in subsequent of the project.

## 7.3 Radio Communication Requirements Specification

This section contains the requirements for Radio Communication, extracted from the knowledge gathered by INDRA in several projects where it was involved. Besides that knowledge, the general standards related with Radio Communication systems from different agencies have been taking into account.

### 7.3.1 Human Exposure requirements

With regards to human exposure to Electromagnetic Fields, the following general standards are applicable to the definition of the applicable limits (basic restrictions and reference levels):

- Council Recommendation 1999/519/EC of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz), Official Journal L 199 of 30 July 1999"
- GUIDELINES FOR LIMITING EXPOSURE TO TIME-VARYING ELECTRIC, MAGNETIC, AND ELECTROMAGNETIC FIELDS (UP TO 300 GHz)

According to these standards and regulations, the following radio communication requirements can be extracted:

- Basic restrictions for electric, magnetic and electromagnetic fields are shown in Table 7-21. Protection against adverse health effects requires that these basic restrictions must not be exceeded.
- The reference levels are given taking into account the condition of maximum coupling of the field to the exposed individual, in order to provide the maximum protection. Reference levels for electric, magnetic and electromagnetic fields are shown in Table 7-22.

Frequency range	Magnetic flux density (mT)	Current density (mA/m <sup>2</sup> ) (rms)	Whole body average SAR (W/kg)	Localised SAR (head and trunk) (W/kg)	Localised SAR (limbs) (W/kg)	Power density, S (W/m <sup>2</sup> )
0 Hz	40	—	—	—	—	—
>0-1 Hz	—	8	—	—	—	—
1-4 Hz	—	8/f	—	—	—	—
4-1 000 Hz	—	2	—	—	—	—
1 000 Hz-100 kHz	—	f/500	—	—	—	—
100 kHz-10 MHz	—	f/500	0,08	2	4	—
10 MHz-10 GHz	—	—	0,08	2	4	—
10-300 GHz	—	—	—	—	—	10

**Table 7-21: Basic restrictions for electric, magnetic and electromagnetic fields (0-300 GHz)**

Frequency range	E-field strength (V/m)	H-field strength (A/m)	B-field (μT)	Equivalent plane wave power density $S_{eq}$ (W/m <sup>2</sup> )
0-1 Hz	—	$3,2 \times 10^4$	$4 \times 10^4$	—
1-8 Hz	10 000	$3,2 \times 10^4/f^2$	$4 \times 10^4/f^2$	—
8-25 Hz	10 000	$4\,000/f$	$5\,000/f$	—
0,025-0,8 kHz	$250/f$	$4/f$	$5/f$	—
0,8-3 kHz	$250/f$	5	6,25	—
3-150 kHz	87	5	6,25	—
0,15-1 MHz	87	$0,73/f$	$0,92/f$	—
1-10 MHz	$87/f^{1/2}$	$0,73/f$	$0,92/f$	—
10-400 MHz	28	0,073	0,092	2
400-2 000 MHz	$1,375\ f^{1/2}$	$0,0037\ f^{1/2}$	$0,0046\ f^{1/2}$	$f/200$
2-300 GHz	61	0,16	0,20	10

**Table 7-22: Reference levels for electric, magnetic and electromagnetic fields (0-300 GHz)**

### 7.3.2 Testing Radio requirements

In terms of testing procedure, several CENELEC standards of CT 106 currently address specific testing framework developed on the basis of the nature/typology of the considered Radio equipment. As a general guideline, the following standard may be used:

- EN 62311 “ASSESSMENT OF ELECTRONIC AND ELECTRICAL EQUIPMENT RELATED TO HUMAN EXPOSURE RESTRICTIONS FOR ELECTROMAGNETIC FIELDS (0 Hz – 300 GHz)”

According to these standards and regulations, the following radio communication requirements can be extracted:

- Concerning susceptibility and emission tests for radio-electric interference, all tests must be carried out with the equipment arranged as closely as possible to the installation conditions. If the cable going to and from the equipment is not specified, unshielded cable must be used and left exposed to the field for a length of 1 m. from the point of connection to the equipment under test.
- The temperature condition for tests shall be between +15°C and +35°C. The relative humidity shall be between 20% and 75%.
- For test at extreme temperatures (-20°C minimum - +55°C maximum), the equipment shall be switched off during the temperature stabilizing period. This stabilizing period must last at least one hour when thermal balance is not checked by measurements.

### 7.3.3 Frequency selection requirements

As far as frequency allocation matters are concerned, frequency plans are defined by national telecommunication authorities on the basis of “spectrum management” considerations. At European level this topic is addressed by:

- Frequency allocation matters: European Radio-communications Committee (ERC) within the European Conference of Postal and Telecommunications Administrations (CEPT), and
- Spectrum management standardization activities: European Telecommunications Standards Institute (ETSI)

In relation to this, the following general document is applicable at European level:

- THE EUROPEAN TABLE OF FREQUENCY ALLOCATIONS AND APPLICATIONS IN THE FREQUENCY RANGE 8.3 kHz to 3000 GHz (ECA TABLE) – October 2017

Furthermore, ETSI standards also regulate train to wayside communication for signalling purposes (e.g. GRM-R communication between ETCS and RBC).

The use of unlicensed ISM bands (e.g. Wi-Fi, Zig-Bee, Bluetooth) is also suitable for railway-metro application. As example CBTC spectrum management for IEEE 802.11 applications (i.e. Wi-Fi) is defined in:

- ETSI EN 300 328-1 (f= 2.4 GHz);
- ETSI EN 300 328-2 (f= 2.4 GHz);
- ETSI EN 302 502 (f =5.8 GHz)

According to these standards and regulations, the following radio communication requirements can be extracted:

- If the equipment can be adjusted to different operating frequencies, a minimum of two must be chosen to ensure that the lower and upper limits of the operating range are covered. For all equipment the frequency range shall be within the band 2,4 GHz to 2,4835 GHz
- FHSS modulation: It must make use of at least 20 well-defined, non-overlapping channels or hopping positions separated by the channel bandwidth as measured at 20 dB below peak power. Best time per channel must not exceed 0.4 seconds. The peak power density shall be limited to -10 dBW per 100 kHz EIRP.
- For equipment using a modulation different from FHSS, the peak power density must be limited to -20 dBW per MHz EIRP.
- The effective radiated power shall be equal to or less than -10 dBW EIRP, for any combination of power level and intended antenna assembly.
- Narrowband spurious emissions: The spurious emissions of the transmitter shall not exceed -30 dBm (when operating) and -47 dBm (in standby) for a frequency range from 1GHz to 12,75 GHz. The spurious emission limit for the receivers must be set in -47 dBm for this frequency range.
- Wideband spurious emissions: The spurious emissions of the transmitter shall not exceed -80 dBm (when operating) and -97 dBm (in standby) for a frequency range from 1GHz to 12,75 GHz. The spurious emission limit for the receivers must be set in -97 dBm for this frequency range.



### 7.3.4 High Level Radio Communication Requirements

Based on the analysis performed in sections 7.3.1 to 7.3.3 the following High-level requirements were distilled and distributed in different specific type of requirement to be intended as general guidelines (i.e. optional requirements):

- Requirements on power limitations for human exposure are:

REQ\_7.3.1 (O) RC shall produce an E field value below 61V/m

REQ\_7.3.2 (O) RC shall produce an H field value below 0.16A/m

REQ\_7.3.3 (O) RC shall produce a B field value below 0.2uT

REQ\_7.3.4 (O) RC shall have an equivalent plane wave power density value below 10W/m<sup>3</sup>

REQ\_7.3.5 (O) RC shall have a SAR value below 4W/kg for the limb section in the human body

- Requirements on testing limitations

REQ\_7.3.6 RC shall be able to work in extreme weather conditions meaning that it may fall in the TX class as defined in CENELEC EN50155

- Requirements on frequency selection

REQ\_7.3.7 (O) RC shall transmit less than

- -30dBm during operation and -47dBm in standby mode for narrowband technologies
- -80dBm during operation and -97dBm in standby mode for wideband technologies

- Requirements related to the railway domain conditions:

REQ\_7.3.8 RC shall be able to communicate moving objects from 0km/h to 350km/h

REQ\_7.3.9 RC shall be able to ensure communication between train tail and front cabin also in NLOS situations.

REQ\_7.3.10 (O) RC shall be able to cover a minimum distance greater than the double of the maximum length of a waggon

Note that maximum distance depends on the adopted network topology. As example network based on communication between each node in each adjacent waggon would require shorter transmission distance. As alternative, to managing situations of faulty nodes or to reduce the latency time, the networks could allow communicating with subsequent waggon, not just with the adjacent. In general the risk of pairing waggons from different trains should be kept into account. Further investigation shall be performed in D4.2 as part of Candidate Technology selection.

REQ\_7.3.11 (O) RC module shall have power requirements that fits the energy harvesting requirements reported at section 7.4.

## 7.4 Energy Harvesting Requirement Specification

In general a train mission in ETCS L3 shall be possible with train at stand still, powered OTI system and confirmed train integrity. For this reason the energy harvesting device need a storage that provide energy also with train at stand-still and need to provide information about EHD efficiency and information about stored energy level. Maximum required power depends on the specific technological solution adopted for OTI device and wireless network and also. As example OTI Slave could have GNSS receiver, wireless communication device, separation sensors, tail detection sensors and other optional diagnostic waggon/cargo sensors. In terms on network, the required energy depends on communication requirements (e.g. communication frequency between OTI Slave and OTI Master, maximum size of the packets, transmission rate) and in general depends on network availability in terms of possible redundancy.

For this reason, at this stage, the figures from INDRA experience was proposed as starting point. Further details about energy harvesting shall be defined in a later stage of the project as candidate technology selection that shall be reported in D4.2 [7].

This section contains general guidelines for Energy Harvesting Device (hereafter referred as EHD).

The following information has been extracted from the knowledge gathered by INDRA as partner and leader of the rail domain of the DEWI project. These values were extracted from the Train integrity demonstrator presented in the DEWI project.

This demonstrator, as shown in section §6.1.2, is based in a combination of multiple sensors (accelerometer, GNSS and RSSI). From a market analysis the average nominal consumption values of these devices are the following:

- Transponder
  - Voltage 24V
  - Current 375mA
  - Power Consumption < 9W
- Accelerometer
  - Voltage 3.3 V
  - Current 3.27 mA
  - Power Consumption 10.8mW
- GNSS
  - Voltage 3.3V
  - Current 545mA
  - Power Consumption 1.8W
- RSSI

- Voltage 3.3V
- Current 3.27mA
- Power Consumption 825mW

Based on the indicated values the following High-level requirements were distilled to be intended as guidelines (i.e. optional requirements):

REQ\_7.4.1. EHD shall provide power supply for SIL4 equipment according to CENELEC 50155 [6].

REQ\_7.4.2. EHD shall provide power supply both in case of train at stand still and in case of train in running phase.

REQ\_7.4.3. (O) EHD shall provide power supply with a minimum power of sensitisation of:

- 2.025 W at peak power consumption.
- 1.3 W during continuous power consumption.

REQ\_7.4.4. (O) EHD shall provide a minimum power supply of 5V for small wireless nodes. This value is not CENELEC 50155 certified but it may not block the SIL4 certification. In order to be EN50155 compliant a voltage level of 24V [6] as minimum nominal voltage. The minimum voltage provided by the EHD must be greater or equal than 16.8V and the maximum voltage must be smaller or equal than 30V.

REQ\_7.4.5. (O) EHD shall provide power supply with a minimum current level of 84.4 mA.

REQ\_7.4.6. (O) EHD shall include a storage to guarantee power supply availability also in case of vehicle at standstill for 13 months for the Product Class 2-B.

REQ\_7.4.7. EHD shall provide efficiency status.

REQ\_7.4.10. EHD shall provide energy level of storage device.

## 7.5 Non Functional Requirement Specification

### 7.5.1 Configuration and Maintenance Requirements

7.5.1.1 OTI devices configuration shall be performed by local maintenance personnel or by remote maintenance centre.

7.5.1.2 OTI device SW upgrade shall be performed by local maintenance personnel or by remote maintenance centre.

### 7.5.2 Mechanical Requirements

7.5.2.1 According to [61], the IP level of the OTI devices shall be:

- IP 40 for installation inside the cabin;
- IP 65 for external installation.

### 7.5.3 Environment Requirements

7.5.3.1 The maximum altitude is defined up to 2000m as class Ax according to [6].

7.5.3.2 The temperature range for the system is TX according to [6].

7.5.3.3 The humidity conditions are defined in the §4.1.4 of [6].

7.5.3.4 The OTI device shall be compliant with the fire protection requirements [60].

7.5.3.5 The OTI devices shall comply to EN50155 and EN50121-3-2 for the EMC immunity.

### 7.5.4 Safety

7.5.4.1 The whole standard CENELEC [50126, 50128, 50129, 50155, 50159] shall be the main reference for hardware and software design of the equipment.

### 7.5.5 Maintenance

REQ\_7.5.5.1: The OTI maintenance period for freight application shall keep into account the waggon maintenance periods ranging from 6 months to 6 years.

### 7.5.6 RAM Requirements

This section contains general guidelines based on SBB experience.

The SBB uses classes for the degree of extend. The Degree of extend is determined by the duration of the failure, the impact to each train, the spatial extension and the criticality of the place of failure (Figure 7-71).

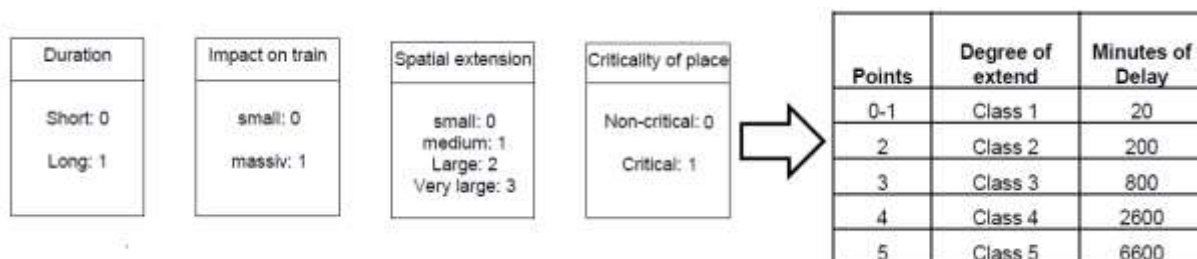


Figure 7-71: Classes for degree of extend

The following class could result for the OTI:

- Duration: Long
- Impact: massive

- Extension: medium
- Criticality: Non-critical

Therefore **Class 3** as degree of extend for OTI.

Each minute of delay leads to costs depending on the type of affected train (freight or passenger) and the degree of extend. Using mean values leads for **Class 3 to about 100.000 CHF/failure event** (for freight trains only the value would be about the half).

Informative: Typical goal for the minutes of delay for the complete CCS: 120.000 minutes/year

With 10% related to the OTI: 12.000 minutes/year leading to 15 events/year.

With 10.000 train rides per day: failure rate < 4.1E-06 per train ride.

## 8 Train Length Determination

---

This section includes the analysis of train length determination functionality. This section is structured in the following sub-sections:

- 1) analysis of the current ETCS specifications (§8.1): this section includes an overview of the ERTMS/ETCS requirements ([1], [3], [9], [74]) related to Train Length acquisition and Train Integrity information managed by On-board equipment;
- 2) Section §8.2 describes the approach used for the identification of the possible scenarios;
- 3) Section §8.3 includes the general assumptions for train length determination;
- 4) identification and analysis of reference scenarios (§8.4): this section includes the analysis of possible scenarios with the scope to identify specific requirements for train length determination functionality;
- 5) results of the analysis of main scenarios (§8.5): this section reports the results of analysis of the point 2) and the new scenarios defined starting from there results;
- 6) hazard analysis (§8.6, Appendix L): this section reports the hazard analysis of the scenarios identified in 3);
- 7) requirements specifications (§8.7): section with the requirements for train length determination functionality.

### 8.1 Analysis of ERTMS/ETCS specification

This section includes an overview of the ERTMS/ETCS requirements ([1], [3], [9], [74]) related to Train Length acquisition and Train Integrity information managed by On-board equipment.

In general, the Train Length (part of Train Data) can be inserted by Driver through the DMI or can be received from an external source, while the status of the train integrity is provided by an external device or can be confirmed by Driver.

Note 1: external means outside the ERTMS/ETCS On-board as defined in Subset 026-2 ([1]).

Note 2: ERTMS/ETCS requirements ([1]) include also the possibility for the Driver to confirm the integrity of the train through the DMI. This aspect is not included in the following analysis.

#### 8.1.1 CR 940

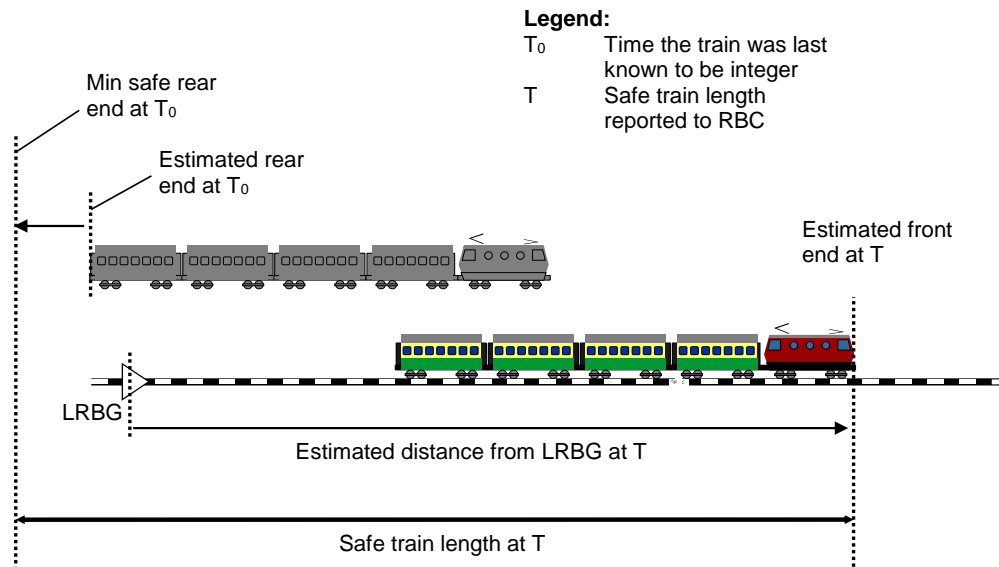
According to the CR 940 (ERA\_solution\_for\_CR940\_140617.docx), the Train Length is an “input” parameter for the calculation of “Safe Train length” as depicted in Figure 8-1.

The formula for the Safe Train Length calculation is:

F1. <b>Safe_Train_Length</b> ( $T$ ) = <i>Estimated_Front_End</i> ( $T$ ) - <i>Min_Safe_Rear_End</i> ( $T_0$ )
--

where:  $\text{Min\_Safe\_Rear\_End}(T_0) = \text{Estimated\_Front\_End}(T_0) - \text{Train\_Length} - L_{\text{DOUBTOVER}}$ .

(refer to [1] § 3.6.4.4.1 for the definition of L\_DOUBTOVER).



**Figure 8-1: CR940 - Calculation of Safe Train Length**

Note that **Train Length** is an input parameter provided by Train Data. No periodic or repetitive acquisition for **Train Length** value is specified in CR940, it can be provided by any means.

As reported in the CR940, the train integrity information reported to the RBC shall consist of:

- a) Train integrity status information
  - No train integrity information
  - Train integrity confirmed by external device
  - Train integrity confirmed (entered) by driver
  - Train integrity lost
- b) Safe train length information (only available when train integrity confirmation is reported).

The transitions between the different values of the train integrity status information to be sent to the relevant RBC shall be executed as described in Table 8-1 according to the conditions in Table 8-2.

Note: Notation “1>” means that condition 1 has to be fulfilled to trigger a transition from the state reported in column to the state reported in row and highlighted with the arrow “>”. For each cell, the arrow refers to the direction of the state transition and the number refers to the transition conditions.

<b>No Integrity information</b>	< 5 -p1-	< 1,5,7,8 -p3-	< 1,6 -p3
2 > -p1-	<b>Integrity confirmed by driver</b>	< 2 -p2-	< 2 -p1-
3 > -p3-		<b>Integrity confirmed by external device</b>	< 3 -p2-
4 > -p2-		4 > -p1-	<b>Integrity lost</b>

**Table 8-1:** Transitions between values of the train integrity status information to be reported to the RBC (CR940)

<b>Condition Id</b>	<b>Content of the conditions</b>
[1]	No valid Train data is available
[2]	(Train is at standstill) AND (valid Train Data is available and has been acknowledged by the RBC) AND (the train integrity is confirmed by the driver)
[3]	(The information "Train integrity confirmed" is received from an external device) AND (valid Train Data is available and has been acknowledged by the RBC) AND (Train Data regarding train length has not changed since the time the train was last known to be integer) AND (the train position is valid and is referred to an LRBG) AND (the train position was valid and was referred to an LRBG at the time the train was last known to be integer) AND (no reverse movement is currently performed nor has been performed since the time the train was last known to be integer)



[4]	(The information "Train integrity lost" is received from an external device) AND (valid Train Data is available since the time the train integrity was last known to be lost)
[5]	A position report indicating that the train integrity is confirmed is sent to the RBC
[6]	The information "Train integrity status unknown" is received from an external device
[7]	Train Data regarding train length is changed
[8]	A reverse movement is performed

**Table 8-2:** Transition conditions for the train integrity status information to be reported to the RBC (CR940)

### 8.1.2 Subset-026

- Section §3.18.3.2 of Subset 026-3 ([1]) refers to “Train Length” as part of the Train Data.
- Section §3.18.3.4 of Subset 026-3 ([1]) states that following any entry/modification of Train Data, the ERTMS/ETCS on-board of the leading engine shall send the Train Data to the RBC (including the Train Length).
- Section §3.18.3.4.1 of Subset 026-3 ([1]) states that the RBC shall acknowledge the reception of this set of Train Data.
- Section §A.3.4 of Subset 026-3 ([1]) reports the handling of accepted and stored information in specific situations. In particular for the Train data, if the Driver closes the desk during the Start of Mission, it shall re-validate the Train Data (see table below)

U = Unchanged; TBR = To Be Revalidated

Data Stored on-board	Situations listed above		
	a – d, f, n	e, g – j, l, m	k
Train Data	U	U	TBR

**Table 8-3: extract of Handling of Accepted and Stored Information in specific Situations table defined in Subset026-3 ([1])**

Note 3: “k” in the last column means “driver closes the desk during SoM”.

- Section §4.5.2 of Subset 026-4 ([1]) reports the active functions depending on the ERTMS operational modes. In particular, for the “*Manage change of Train Data from external sources*” and “*Report train position when loss of train integrity is detected*” functions, the following table is applied:

ONBOARD-FUNCTIONS	RELATED SRS §	N P	S B	P S	S H	F S	L S	S R	O S	S L	N L	U N	T R	P T	S F	I S	S N	R V
Report train position when loss of train integrity is detected	3.6.5.1.4 d)		X			X	X	X	X			X	X	X			X	X
Manage change of Train Data from external sources	5.17		X			X	X	X	X			X	X	X			X	

**Table 8-4:** extract of Active Functions table defined in Subset026-4 ([1])

Note 4: the red “X” in Table 8-4 represents the changes introduced by CR 940 compared with [1].

As reported in Table 8-4, the “*Train Data from external sources*” are managed in the following modes:

- Stand-by (SB);
- Full Supervision (FS);
- Limited Supervision (LS);
- Staff Responsible (SR)
- On-sight (OS);
- Unfitted (UN);
- Trip (TR);
- Post Trip (PT);
- National System (SN);

While the sending of the Position Report when train integrity is lost is performed in the following case:

- Stand-by (SB);
- Full Supervision (FS);
- Limited Supervision (LS);
- Staff Responsible (SR)
- On-sight (OS);
- Unfitted (UN)
- Trip (TR);
- Post Trip (PT);
- National System (SN)
- Reversing (RV);

- Section §4.7.2 of Subset 026-4 ([1]) reports the ETCS operational mode that allows the entry of Train Data by Driver at standstill.

A = Available, NA = Not Applicable

Input information	N P	S B	P S	S H	F S	L S	S R	O S	S L	N L	U N	T R	P T	S F	I S	S N	R V
Train Data (refer to 3.18.3.2)		A			A	A	A	A			A			NA	NA	A	

**Table 8-5:** extract of DMI Input table defined in Subset026-4 ([1])

- Section §4.8.3 of Subset 026-4 ([1]) reports the conditions for the acceptance of the information depending on the level and transmission media. In particular, for the acceptance of the Movement Authority the following condition is valid:

A = Accepted R = Rejected

Information	From RBC	Onboard operating level				
		0	NTC	1	2	3
Movement Authority + (optional) Mode Profile + (optional) List of Balises for SH area	No	R [1]	R [1]	A [4]	R [1]	R [1]
	Yes	R [2]	R [2]	R [2]	A [3] [4] [5]	A [3] [4] [5]

**Table 8-6:** extract of “Accepted information depending on the level and transmission media” table defined in Subset026-4 ([1])

Note 5: the exception [3] reported in the above table states:

[3] exception: rejected if Train Data has been sent to the RBC and the “Acknowledgement of Train Data” has not been received yet.

The ERTMS/ETCS On-board shall accept a Movement Authority sent by RBC only if the acknowledgement of Train Data has been received.

- Section §4.10 of Subset 026-4 ([1]) explains how the information stored onboard is influenced by a mode transition.

D = Deleted TBR = To Be Revalidated U = Unchanged NR = Not relevant R = Reset

Data Stored on-board	Entered Mode																
	NP	SB	PS	SH	FS	LS	SR	OS	SL	NL	UN	TR	PT	SF	IS	SN	RV
Train Data	D	TBR	U	TBR	U	U	U	U	U	U	U	U	U	NR	NR	U	U

**Table 8-7:** extract of “What happens to accepted and stored information when entering a given mode” table defined in Subset026-4 ([1])

Note 6: Train data shall be re-validated (TBR in the table) by Driver in case of the entered mode is Stand-by (SB) or Shunting (SH). These two modes represent mainly End of Mission (see 5.5.2.1 and 5.5.2.3 of [1]), means for a new mission the current stored Train data needs to be revalidated.

Note 7: if the ERTMS/ETCS On-board is switched off (this means that the Enter Mode is No Power (NP)), Train Data are deleted.

Example: if the current mode is Staff Responsible (SR) and it changes into Full Supervision (FS), then the Train Data remain unchanged (U).

- Section §5.17 Subset 026-5 ([1]) reports how the ERTMS/ETCS On-board shall manage the Train Data received from an external source. The following Figure 8-2 describes the procedure to be implemented by the ERTMS/ETCS On-board when a train data is received from an external source:

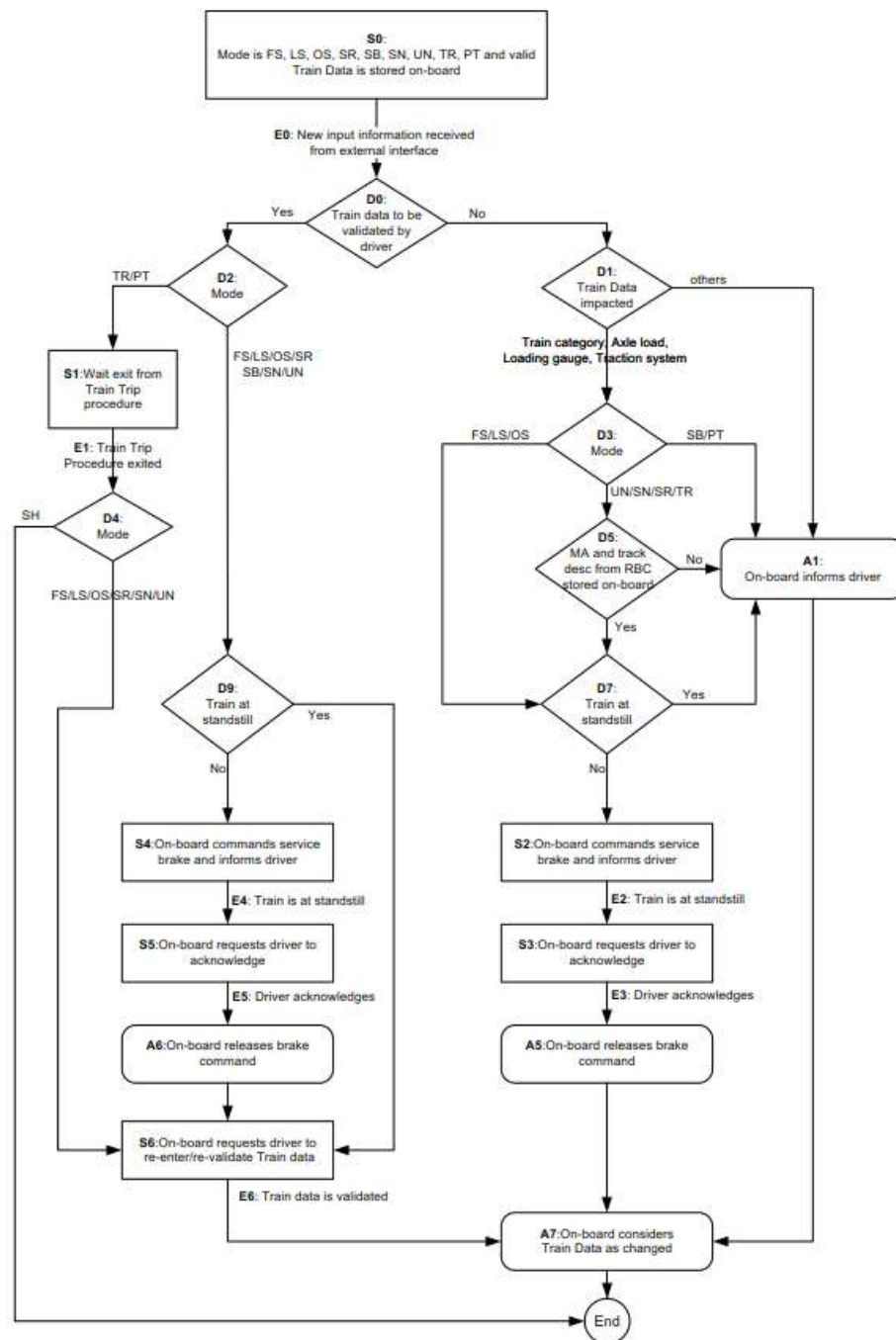


Figure 8-2: SUBSET 026 §5.17- Changing Train Data from sources different from the driver

Note 8: ERTMS/ETCS requirements (§5.17, [1]) offer the possibility to choose if new data received from an external source shall be validated, by Driver, or not and this is dependent by the specific application. This procedure is applicable only if Train Data are stored on-board, this means that Train Data are validated by Driver. Note that as reported in the Subset-120 ([75]), requirement 5.1.7.2.2.4, driver validation for changes in Train length is required. In this case, after the state **D0** in Figure 8-2, the branch to be followed is the one with “Yes”.

Note 9: In the state **S0** of Figure 8-2, valid train data stored on-board are required.

- Section §7.4.3 Subset 026-7 ([1]) describes the packet used by ERTMS/ETCS on-board to send the train integrity status and the safe train length to RBC. The packet used is the Position Report and the related variables are Q\_LENGTH and L\_TRAININT. Below the description of these variables:

#### Q\_LENGTH:

<b>Name</b>	Qualifier for train integrity status		
<b>Description</b>	Qualifier, identifying the train integrity information available. The related safe train length information is given by L_TRAININT		
<b>Length of variable</b>	<b>Minimum Value</b>	<b>Maximum Value</b>	<b>Resolution/formula</b>
2 bits			
<b>Special/Reserved Values</b>	0	No train integrity information available	
	1	Train integrity confirmed by integrity monitoring device	
	2	Train integrity confirmed by driver	
	3	Train integrity lost	

#### L\_TRAININT:

<b>Name</b>	Safe Train length		
<b>Description</b>			
<b>Length of variable</b>	<b>Minimum Value</b>	<b>Maximum Value</b>	<b>Resolution/formula</b>
15 bits	0 m	32767 m	1 m

Note 10: As reported in §7.4.3 Subset 026-7 ([1]), L\_TRAININT is sent to RBC if Q\_LENGTH = “Train integrity confirmed by integrity monitoring device” or “Train integrity confirmed by driver”.

#### 8.1.2.1 SoM Diagram

The following Figure 8-3 shows the Start of Mission diagram as reported in §5.4.4 of Subset026-5 ([1]):

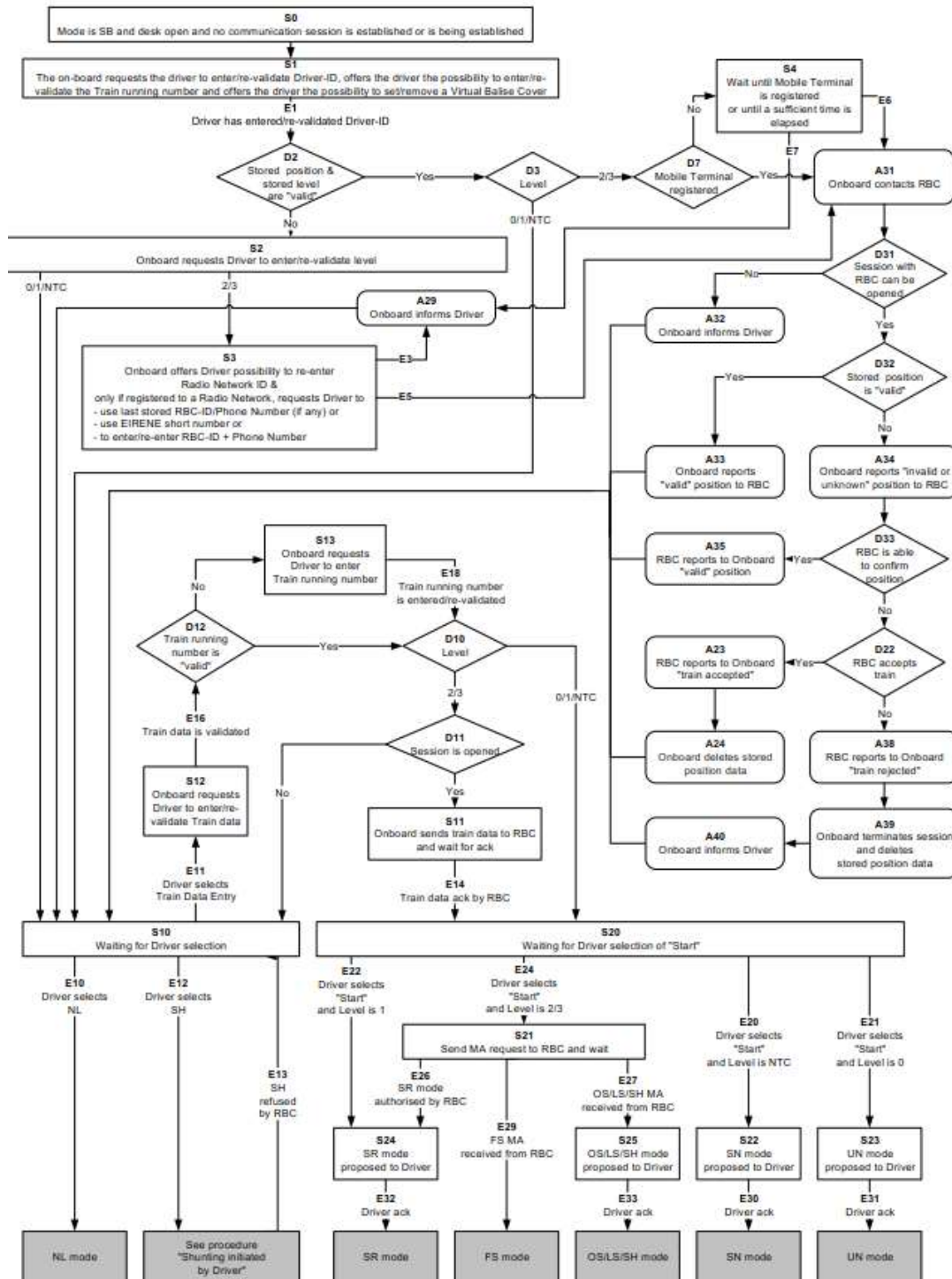


Figure 8-3: Start of Mission diagram

### 8.1.3 Subset-119

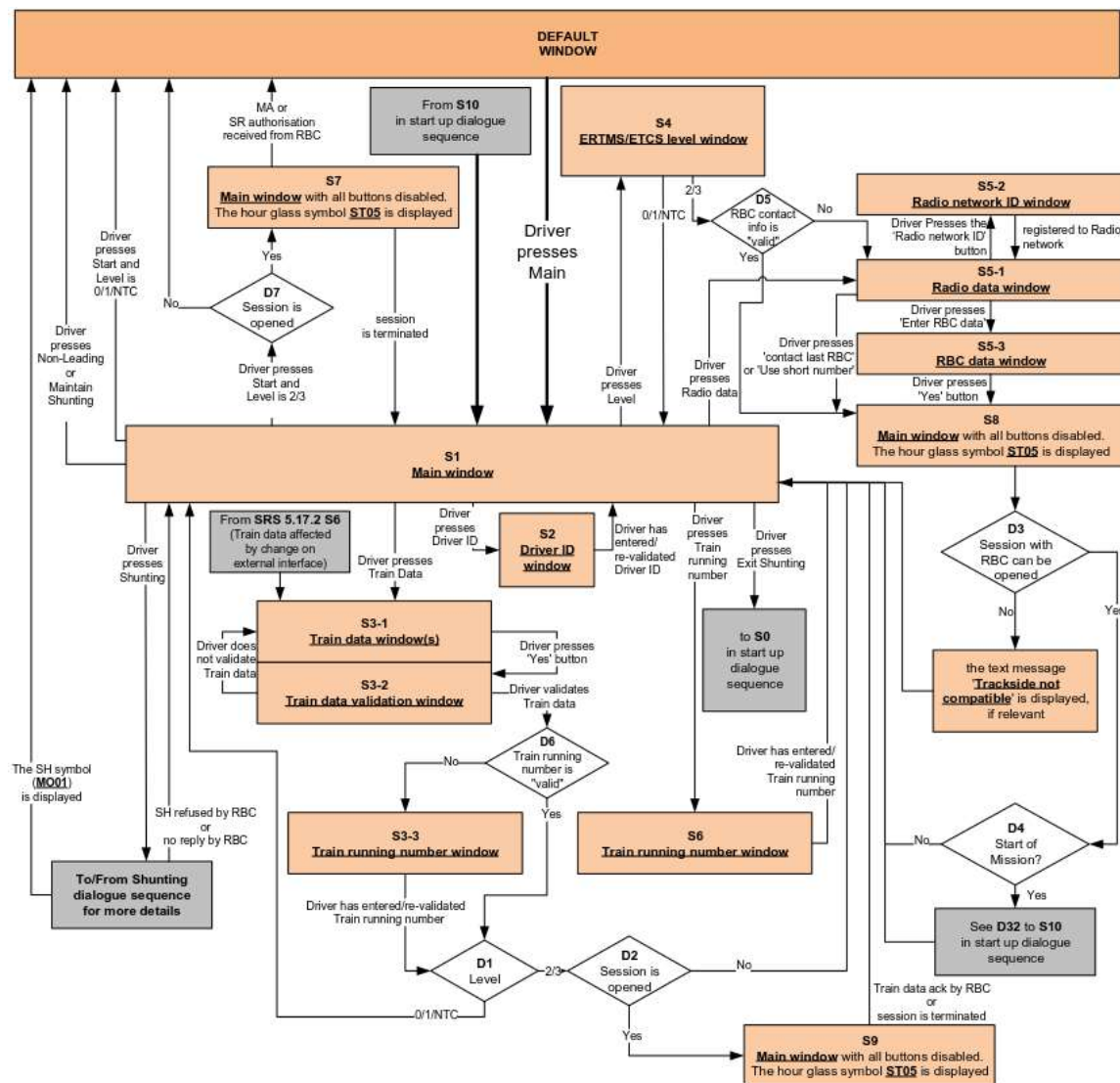
Subset 119 ([9]) describes the train length as input data for ETCS sent via a serial interface. The train length is transmitted to the ERTMS/ETCS on-board as 12 bit variable in meter.

Function	maximum cycle time for MVB and CAN / ECN [ms]	signal size[Bit]	signal type for transmission	name on serial interface	Comment
Train Data	256 / 200	12	UNSIGNED16	TR_OBU_TrainLength	Train data: train length Coding: bit 0..11 see 5.5.3.3.3.1 bit 12..15 set to 0

**Table 8-8: Extract from Subset-119**

#### 8.1.4 DMI

The following Figure 8-4 shows the DMI windows sequence (for more details refer to §11.7.3 of [74]):



**Figure 8-4:** DMI Main window dialogue sequence

Note 11: as reported in Figure 8-4, if a train data is received from external source, then the “Train data window” (state S3-1) is presented to the driver.

Note 12: as explained in DMI ERA document (§11.3.9.6 of [74]) and UNISIG Subset-034 ([2]), Train Data entry procedure can be performed in three ways:

- a) *Fixed train data entry*: the Train data window shall contain only one input field allowing the Driver to enter a train type amongst a number of pre-configured ones. Once a train type is selected, the on-board shall not offer any possibility for the driver to change any value of a specific train data composing the selected train type.
- b) *Flexible train data entry*: the Train data entry window(s) shall contain one or more input fields for the specific train data the driver has to enter/modify.
- c) *Switchable train data entry*: the Train data entry window(s) shall offer the possibility to switch from a “Fixed train data entry” layout to a “Flexible train data entry” layout or vice versa.

Note 13: As reported in requirement 11.7.3.3 of [74], for the state S3-1 of Figure 8-4 the following behaviour is applicable:

If **S3-1** is entered from **S1** (i.e. the train data entry / validation process starts following a driver action on the ‘Train data’ button):

- When the status of train data is “valid”, the proposed value for each input field shall be the corresponding train data value stored onboard.
- When the status of train data is “invalid”, if a value is proposed, it can be either the value of the corresponding train data stored onboard, a value pre-configured onboard or a value received from another ERTMS/ETCS external source (e.g. from the train interface).
- When the status of train data is “unknown”, if a value is proposed, it can be either a value pre-configured onboard or a value received from another ERTMS/ETCS external source (e.g. from the train interface).

If **S3-1** is entered from step **SRS 5.17.2 S6** (i.e. the train data entry / validation process starts due to a change on the ERTMS/ETCS external interface that affects the Train data):

- For each input field affected by the change on the ERTMS/ETCS external interface, if a value is proposed, it can be either a value pre-configured onboard or a value received from another ERTMS/ETCS external source.
- For all other input fields, since the status of train data is “valid”, the proposed value for those input fields shall be the corresponding train data value stored onboard.

## 8.2 Approach Description

This section describes the approach used for the identification of the possible scenarios reported in §8.4.

Use cases description, as example:

- Train Length determined available before moving the train (i.e. based on train composition determination);
- Train Length determined dynamically (e.g. distances measurement in shunting areas by means of euro-balises);



- Train Integrity criteria based on determined train length;

The identified “Uses cases” are analyzed in terms of:

- Operational implications
- Hazard identification
- Contextualization of sequence diagrams

### 8.3 Assumptions

This section includes the general assumptions for train length determination:

- 1) Train splitting: track occupation of removed waggons is managed by MB functionalities;
- 2) ATO: train length is available after waking-up, coupling or uncoupling activities;
- 3) Train composition: changes to train length are triggered by START/RESET commands at standstill;
- 4) Determined train length includes a margin to keep into account potential train length variations due to train expansion/contraction;
- 5) Train length determination is a SIL 4 function;
- 6) Train length is defined as the physical length of each waggon/locomotives plus the couplers at maximum extension;
- 7) Virtual coupling: not taken into account;

### 8.4 Reference Scenarios

This section addresses the identification and analysis of reference scenarios in relation to train length acquisition and train integrity management considering the ERTMS/ETCS requirements reported in §8.1 and train integrity requirements defined in §7.1.

In general, the train length evaluation could be performed:

- 1) with the train at standstill or on moving depending on the technical solution adopted;
- 2) during the Start of Mission (Stand-by mode) or during the mission (for example following joining/splitting operation). In the second case, the operation mode could be: FS, LS, SR, OS, UN, TR, PT or SN (as reported in Table 8-4).

Train integrity status evaluated by OTI system is provided to the ERTMS/ETCS On-board independently from ERTMS/ETCS operative mode and train speed. The conditions for sending the train integrity status to RBC are described in Table 8-2. Train integrity criteria implemented by OTI system depend on on-board communication network type (i.e. wired or wireless). In case of wired network the train integrity criterion is based on communication status (e.g. regular exchange of liveness messages). In case of wireless communication network, the criterion takes into

consideration also the train length (for more details refer to §7.1.1.5). In this case, a correlation between train length and train integrity exists.

Furthermore, both functionalities, train length evaluation and train integrity monitoring, are independent from ERTMS/ETCS level.

From the above considerations the use cases identified are:

Use case	Train speed (V)	ERTMS/ETCS Operational Mode	Reception of Train Length (TL) and Train Integrity (TI) information by the ERTMS/ETCS On-board
1	Standstill (V = 0)	Stand-by (SB)	TL before TI
2	Standstill (V = 0)	Stand-by (SB)	TI before TL
3	Standstill (V = 0)	Different from Stand-by (SB)	TL before TI
4	Standstill (V = 0)	Different from Stand-by (SB)	TI before TL
5 (see (*) below)	Moving (V > 0)	Different from Stand-by (SB)	TL before TI
6 (see (*) below)	Moving (V > 0)	Different from Stand-by (SB)	TI before TL

**Table 8-9:** Uses Cases

The analysis of the following scenarios considers the independences between the FSM(s) of OTI-I and OTI-L and the sequence diagram of ERTMS/ETCS Start of Mission procedure. This means that the information of train length or train integrity can be received by the ERTMS/ETCS On-board in each state of SoM (see Figure 8-3).

As specified in §8.1, the reception of a new train length value has an impact on the Train Data and on the information of train integrity (L\_TRAININT variable, see also the formula F1).

(\*) Use Cases 5 and 6 are not in line with the assumption number 3 reported in §8.3. These use cases are added to take into account: a) the possibility to use the Balise Group as solution to evaluate the train length, and b) degraded scenarios, where the OTI-L could send the train length value with the train not at standstill.

### 8.4.1 Use Case n. 1

This section describes and analyses the Use Case number 1 (see Table 8-9):

Use case	Train speed (V)	ERTMS/ETCS Operational Mode	Reception of Train Length (TL) and Train Integrity (TI) information by the ERTMS/ETCS On-board
1	Standstill (V = 0)	Stand-by (SB)	TL before TI

The ERTMS/ETCS On-board is in Stand-By mode, train is at standstill and the Driver is performing the Start of Mission (SoM).

To simplify the analysis, it is performed considering some scenarios where the On-board receives only the Train Length information and some scenarios where it receives the information of new Train Length and Train Integrity:

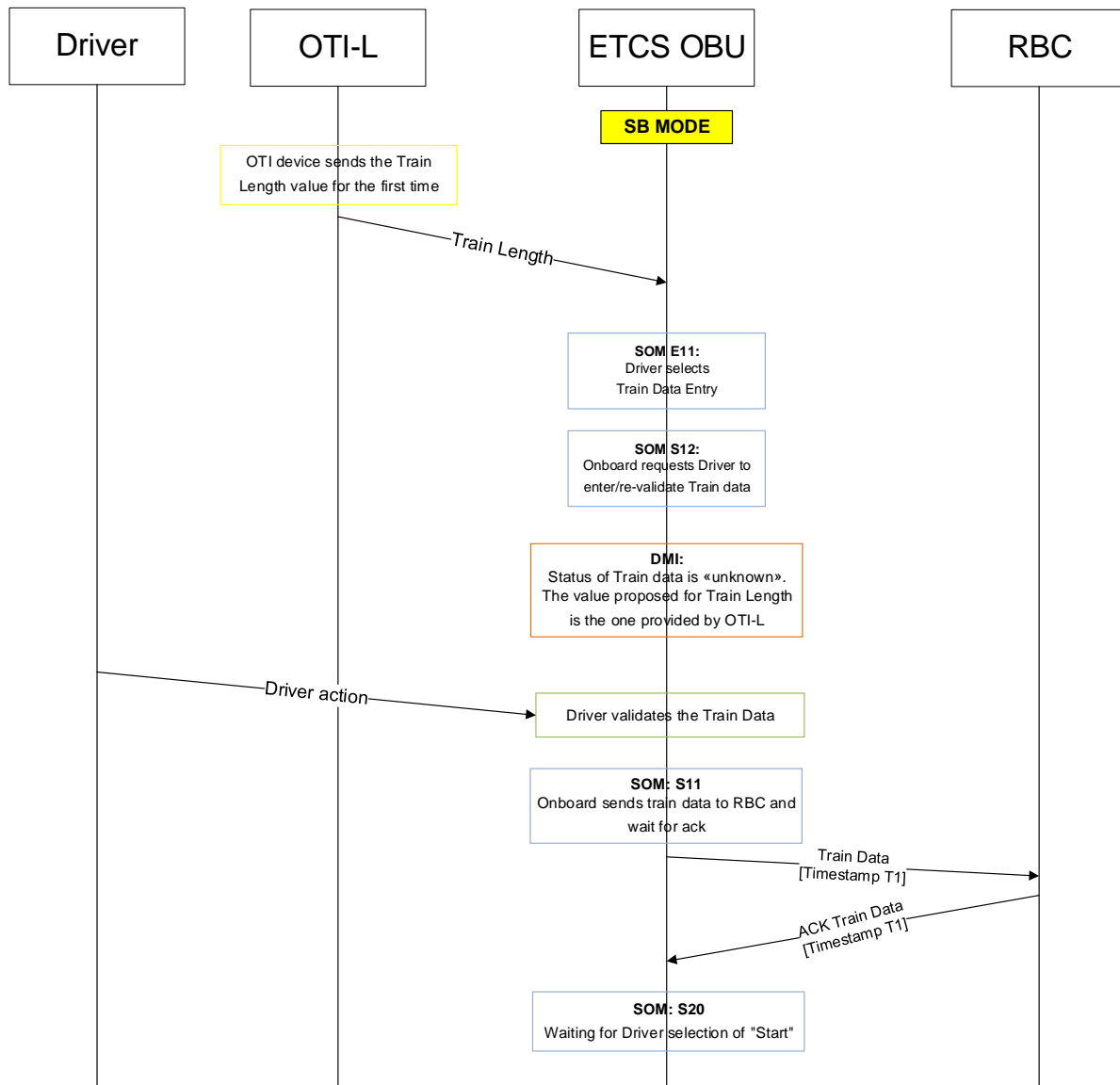
- Example 1 (§8.4.1.1) analyses the case where the value of train length by OTI-L is provided to ERTMS/ETCS On-board before Driver starts the Train Data validation procedure.
- Examples 2 (§8.4.1.2) and 3 (§8.4.1.3) analyse the cases where the OTI-L provides the train length value only after the Driver has just validated the Train Data. These two scenarios cover the procedure described in §5.17 of [1] and reported in Figure 8-2 with Driver re-validation required or not.
- Example 4 (§8.4.1.4) shows the case where during the Start of Mission the Driver closes and opens the desk.

Finally, example 5 (§8.4.1.5) and example 6 (§8.4.1.6) show the scenarios when the ERTMS/ETCS On-board receives the Train Length and Train Integrity information.

#### 8.4.1.1 Use Case 1: Example 1 (only Train Length) – Nominal scenario

In this example the ERTMS/ETCS On-board sub-system receives the Train Length data sent by OTI-L device before the Driver has performed the Train Data entry.

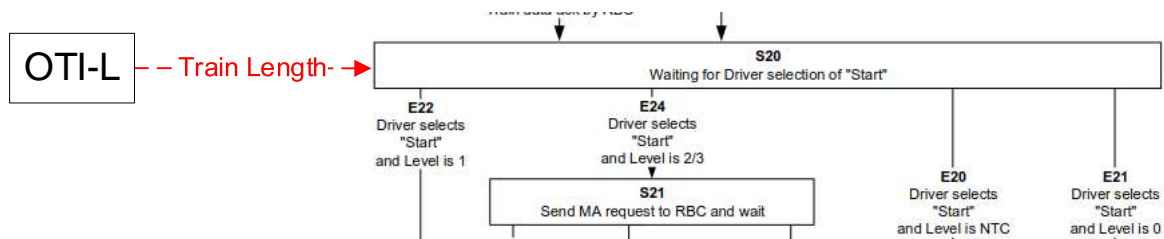
The Driver switches the system on and the status of Train Data in “unknown”. The OTI-L device sends the train length value before the validation of Train Data by the Driver. When the Driver selects the Train Data entry procedure, the DMI shows as train length value the one sent by the OTI-L (see Note 13). The Driver validates the Train Data.



**Figure 8-5: Use Case 1 - Example 1 (only Train Length)**

#### 8.4.1.2 Use Case 1: Example 2 (only Train Length) – Nominal scenario

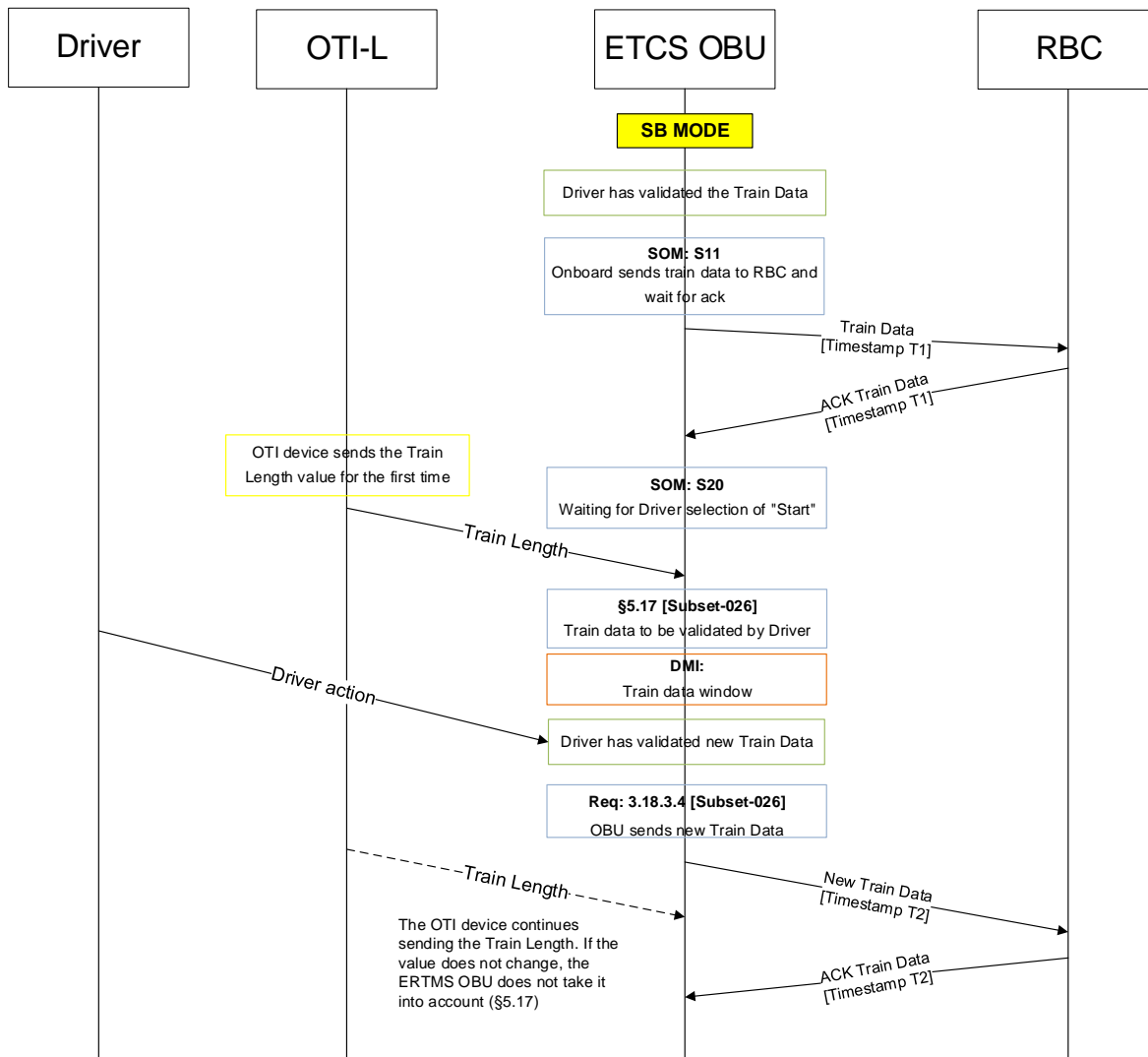
In this example, Figure 8-6 and Figure 8-7, the ERTMS/ETCS On-board sub-system receives the Train Length data sent by OTI-L device when the state during the SoM is **S20** and a re-validation of this data is required to the Driver:



**Figure 8-6:** Receiving of train length during SoM in S20 state

The hypotheses before reaching the state S20 are:

- 1) Driver has entered/revalidated the Train Data (including the Train Length), state **E16** of SoM diagram (Figure 8-3). In this phase, the train length value could be equal to the value used in the previous mission and revalidated by Driver or could be a default value proposed by the system and modified by Driver. In both cases, the value is different from the real one provided by OTI-L;
- 2) Driver has entered/revalidated the Train running number, the selected level is 2/3 and the session with RBC is open;
- 3) The ERTMS/ETCS On-board sub-system has sent the Train Data to RBC and has received the acknowledgement message.

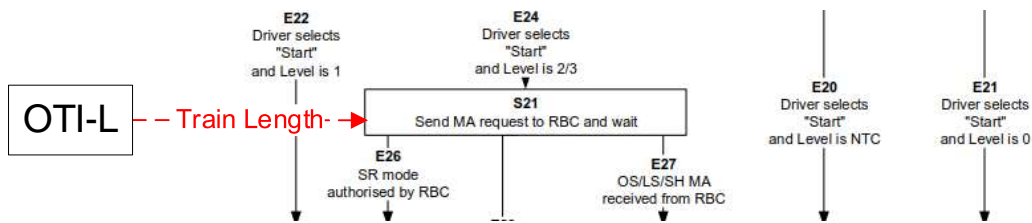


**Figure 8-7: Use Case 1 - Example 2 (only Train Length)**

In this example, the Driver has to validate the Train Length twice, one during the normal procedure of Start of Mission and another time when its value is provided to the ERTMS/ETCS On-board sub-system by the OTI-L device. The On-board sends the Train Data to RBC two times.

#### 8.4.1.3 Use Case 1: Example 3 (only Train Length) – Nominal scenario

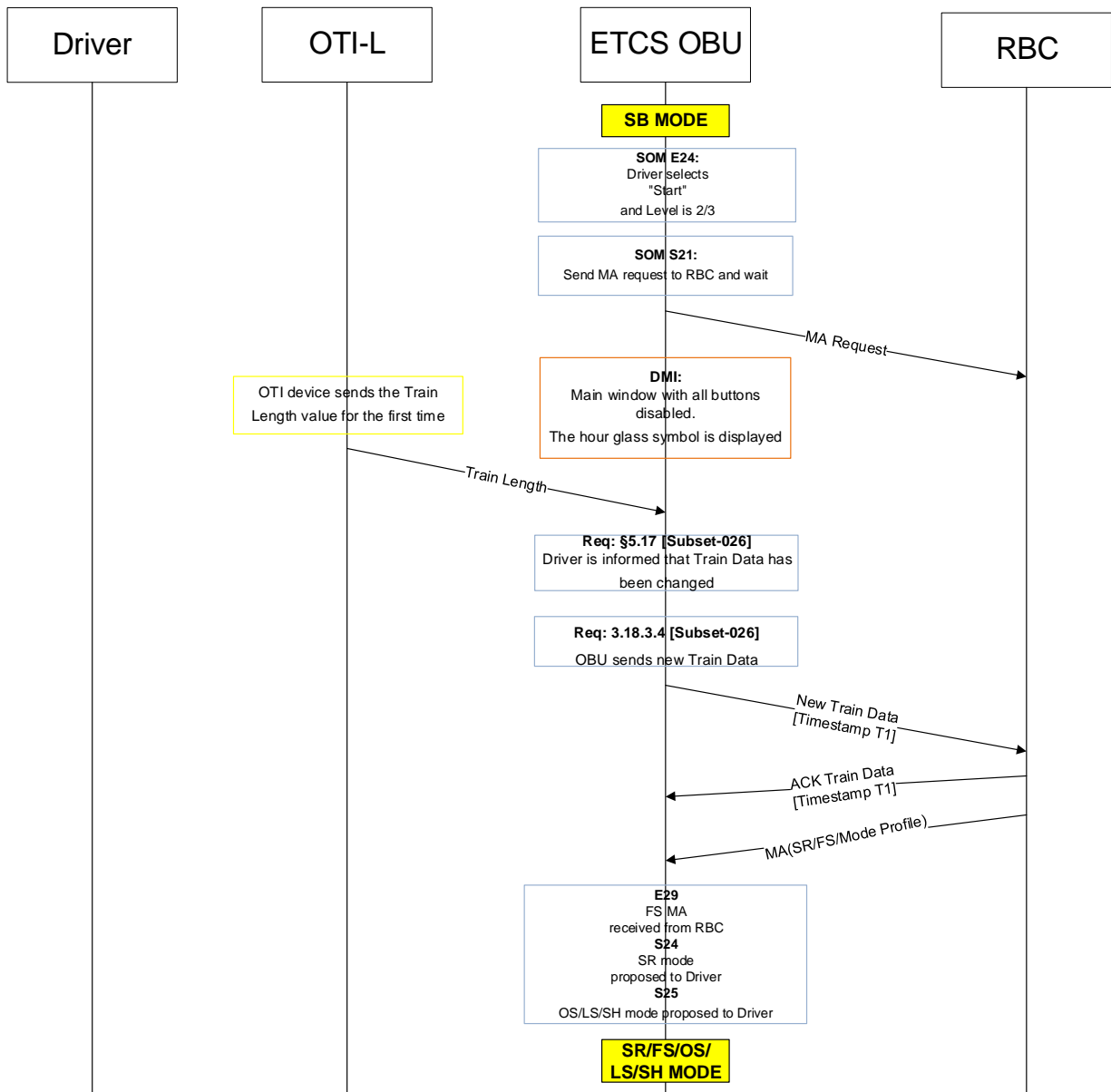
In this example, Figure 8-8 and Figure 8-9, the ERTMS/ETCS On-board sub-system receives the Train Length data sent by OTI device when the state during the SoM is **S21** and no re-validation of the new data is required to the Driver.



**Figure 8-8:** Receiving of train length during SoM in S21 state

The hypotheses before reaching the state S21 are:

- 1) Driver has entered/revalidated the Train Data (including the Train Length), state **E16** of SoM diagram (Figure 8-3). In this phase, the train length value could be equal to the value used in the previous mission and revalidated by Driver or could be a default value proposed by the system and modified by Driver. In both cases, the value is different from the real one provided later by OTI-L;
- 2) Driver has entered/revalidated the Train running number, the selected level is 2/3 and the session with RBC is open;
- 3) The ERTMS/ETCS On-board sub-system has sent the Train Data to RBC and has received the acknowledgement message.
- 4) The Driver has selected "START" and the ERTMS/ETCS On-board sub-system has sent to RBC a request of MA.



**Figure 8-9: Use Case 1 - Example 3 (only Train Length)**

Note: in this scenario, the ERTMS/ETCS On-board sub-system could reject the Movement Authority sent by RBC if received before the "Train Data Acknowledgement" (see exception 3 in Table 8-6). In this case the ERTMS/ETCS mode remains Stand-by mode.

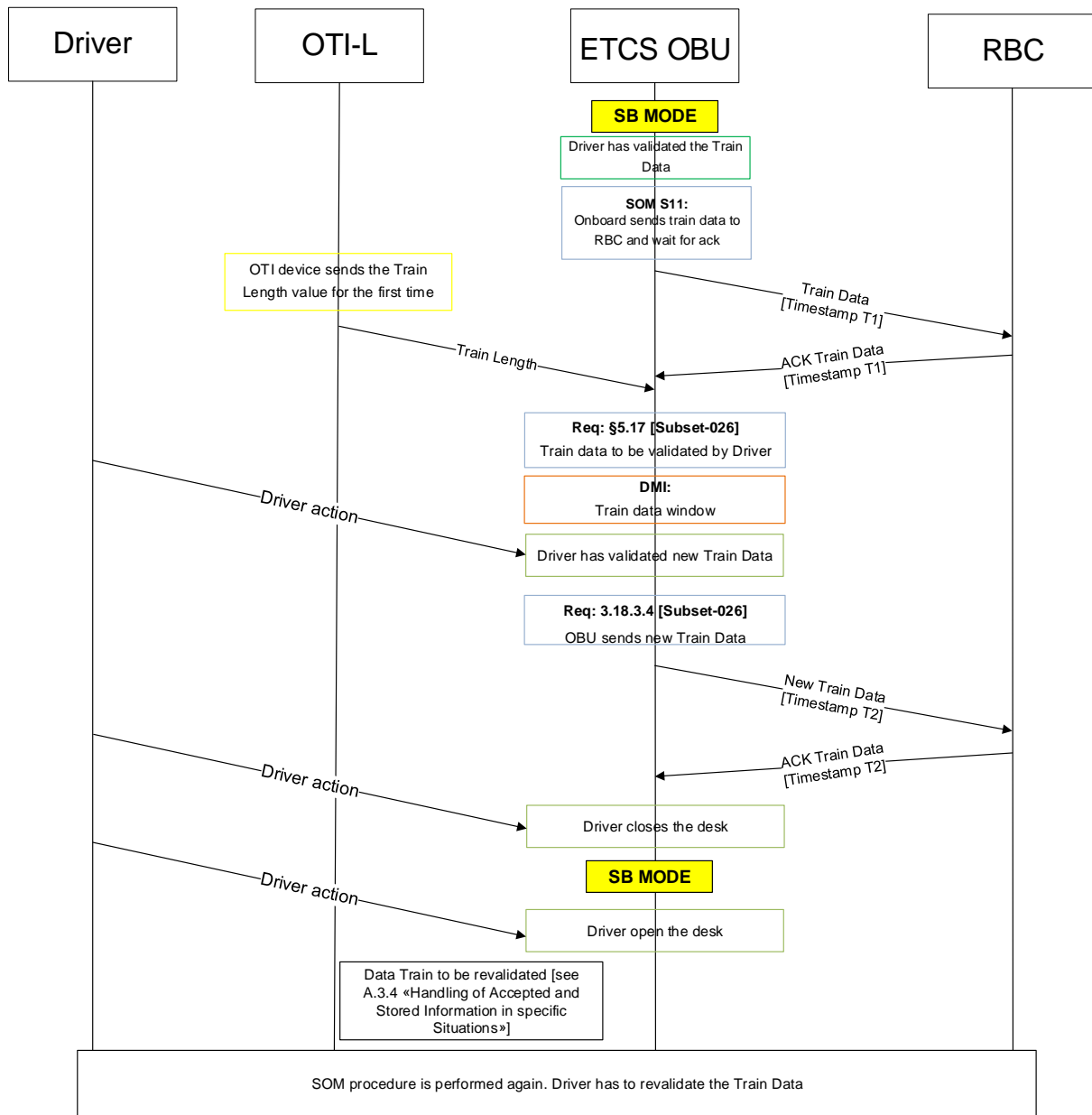
#### 8.4.1.4 Use Case 1: Example 4 (only Train Length) – Nominal scenario

In this example the Driver closes and opens the desk during the Start of Mission.

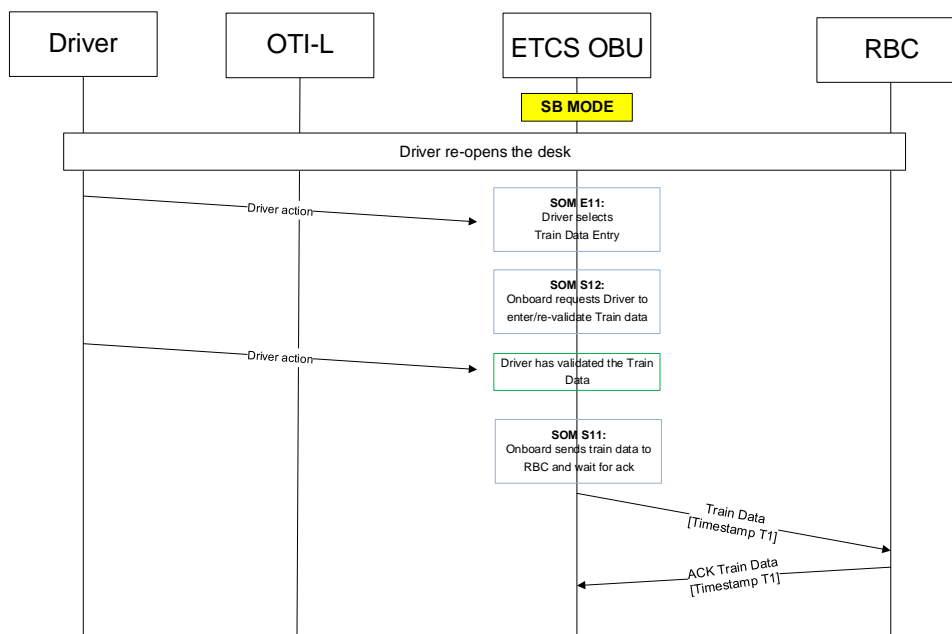


Figure 8-10 shows the first part of scenario where the Driver validates the train length value received by OTI-L and then closes the desk. After the Driver validation, the status of Train Data is “valid” and they are stored on-board. After the closure of the desk the status of Train Data remains as “valid”.

Figure 8-11 shows the second part of the scenario when the Driver opens the desk. When the SoM arrives at state S12, the values of Train Data (including the Train Length) are the corresponding train data values stored on-board as reported in requirement 11.7.3.3 of [74] (see Note 13). In this case the value of train length proposed by the ERTMS/ETCS On-board and to be revalidated by Driver is the one received previously by the OTI-L device.



**Figure 8-10: Use Case 1 - Example 4 – First part (only Train Length)**



**Figure 8-11:** Use Case 1 - Example 4 – Second part (only Train Length)

#### 8.4.1.5 Use Case 1: Example 5 – Train Length and Train Integrity

This example, Figure 8-12, shows the ERTMS/ETCS On-board sub-system behaviour when it receives the Train Length information by OTI-L and then the Train integrity status by OTI-I.

The following points are taken into account for this scenario:

- the ERTMS/ETCS On-board sub-system is in SB mode, state S12 of SoM diagram (S12: On-board requests Driver to enter/re-validate Train data ), see Figure 8-3;
- Position of the train is valid (see condition [3] of Table 8-2);
- On-board receives the Train Length data sent by OTI-L device when the state during the SoM is S20 (S20: Waiting for Driver selection of "Start");
- The Train Length provided by external source shall be validated by Driver;
- T = Period of Position report;
- Backward Compatibility: the scenario is related to the Backward compatibility as explained in D4.2 ([7]);
- The states of OTI-L device reported in the yellow boxes in Figure 8-12 (Idle, Running/Unknown and Running /Known) are described in §8.7.1;
- The states of OTI-I device reported in the yellow boxes in Figure 8-12 (Mastership, Inauguration and Monitoring) are described in §7.1.

During the SoM, the Driver pushes the “START” button (note: this “START” button is different from the “START” button of DMI) and activates the FSM of OTI-I and OTI-L functionalities. When the ERTMS/ETCS On-board sub-system receives the Train Length value by OTI-L (state Running /Known), the Driver validates this value and the On-board sends the Train Data to RBC and waits

for the acknowledgement message. Before receiving the “Train Integrity Confirmed” information by OTI-I, the Position Report sent by the On-board to RBC includes the information of “No train integrity information available” (variable Q\_LENGTH = 0 of packet number 0, see chapter 7 of [1]). When the ERTMS/ETCS On-board sub-system receives the information of “Train integrity confirmed” by OTI-I and the acknowledgement message sent by RBC (see condition [3] of Table 8-2), then it sends to RBC the information of “Train integrity confirmed by integrity monitoring device” (variable Q\_LENGTH = 1).



#### **8.4.1.6 Use Case 1: Example 6 – Train Length and Train Integrity**

This example is the same of example 5 (§8.4.1.5) but with the following exception:

- No re-validation is required to the Driver if a new value of Train length is provided to OBU by OTI-L.



### 8.4.2 Use Case n. 2

This section describes and analyses the Use Case number 2 (see Table 8-9):

Use case	Train speed (V)	ERTMS/ETCS Operational Mode	Reception of Train Length (TL) and Train Integrity (TI) information by the ERTMS/ETCS On-board
2	Standstill (V = 0)	Stand-by (SB)	TI before TL

The ERTMS/ETCS On-board sub-system is in Stand-By mode, train is at standstill and the Driver is performing the Start of Mission (SoM). Differently from Use Case 1, in this case the On-board sub-system receives the information of Train Integrity before the information of Train Length.

#### 8.4.2.1 Use Case n. 2: Example 1 - Train Integrity and Train Length

This example, Figure 8-14, shows the ERTMS/ETCS On-board sub-system behaviour when it receives the Train Integrity status by OTI-I and then the Train Length information by OTI-L.

The following points are taken into account for this scenario:

- the ERTMS/ETCS On-board sub-system is in SB mode, state S12 of SoM diagram (S12: On-board requests Driver to enter/re-validate Train data ), see Figure 8-3;
- Position of the train is valid (see condition [3] of Table 8-2);
- On-board receives the Train Length data sent by OTI-L device when the state during the SoM is S20 (S20: Waiting for Driver selection of "Start"), see Figure 8-3;
- The Train Length provided by external source shall be validated by Driver;
- T = Period of Position report;
- Backward Compatibility: the scenario is related to the Backward compatibility as explained in D4.2 ([7]);
- The states of OTI-L device reported in the yellow boxes in Figure 8-14 (Idle, Running/Unknown and Running /Known) are described in §8.7.1;
- The states of OTI-I device reported in the yellow boxes in Figure 8-14 (Mastership, Inauguration and Monitoring) are described in §7.1.

During the SoM, the Driver pushes the “START” button (note: this “START” button is different from the “START” button of DMI) and activates the FSM of OTI-I and OTI-L functionalities. Before receiving the “Train Integrity Confirmed” information by OTI-I, the Position Report sent by the On-board to RBC includes the information of “No train integrity information available” (variable Q\_LENGTH = 0 of packet number 0, see chapter 7 of [1]). When the ERTMS/ETCS On-board sub-system receives the information of “Train integrity confirmed” by OTI-I, then it sends to RBC the information of “Train integrity confirmed by integrity monitoring device” (variable Q\_LENGTH = 1 and L\_TRAININT evaluated taken into account the train length value not provided by OTI-L).



When the ERTMS/ETCS On-board sub-system receives the Train Length value by OTI-L (state Running/Known), the Driver validates this value and the ERTMS/ETCS On-board sends the Train Data to RBC and waits for the acknowledgement message. Note that even if the OBU receives the information of “Train integrity confirmed” by OTI-I, it sends to RBC the information of “No train integrity information available” until Train Data acknowledgement message is received (as specified in CR 940, condition [3], Table 8-2). Furthermore, the OBU in the next messages including the information of “Train integrity confirmed by integrity monitoring device” uses for the evaluation of the Safe Train Length (L\_TRAININT) the new value of TL received by OTI-L.



### 8.4.3 Use Case n. 3

This section describes and analyses the Use Case number 3 (see Table 8-9):

Use case	Train speed (V)	ERTMS/ETCS Operational Mode	Reception of Train Length (TL) and Train Integrity (TI) information by the ERTMS/ETCS On-board
3	Standstill (V = 0)	Different from Stand-by (SB)	TL before TI

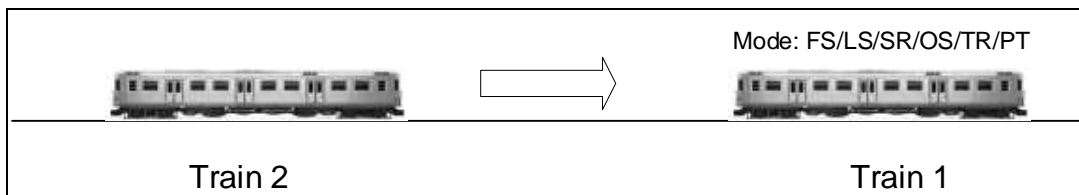
The ERTMS/ETCS On-board sub-system is in a mode different from Stand-By mode (e.g. Full Supervision, Staff Responsible, etc.), train is at standstill. This Use Case covers joining and splitting scenarios.

To simplify the analysis, the following figures show some examples of the On-board behaviour when it receives only the information of new Train Length without considering the Train Integrity input. Finally, examples 3 and 4 (Figure 8-21 and Figure 8-24) show examples of Train Length and Train Integrity reception.

#### 8.4.3.1 Use Case n. 3: Example 1 (only Train Length) – Nominal scenario

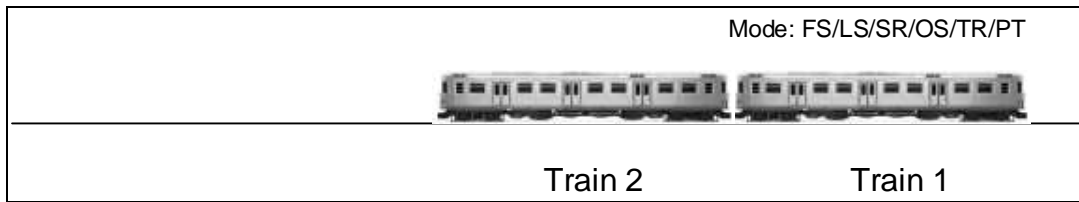
In the following scenario, Train 1 is at standstill and its ERTMS/ETCS operational mode is one of the following: FS/LS/SR/OS/TR/PT.

Train 2 is moving and is approaching Train 1. The operational mode of Train 2 is not relevant.



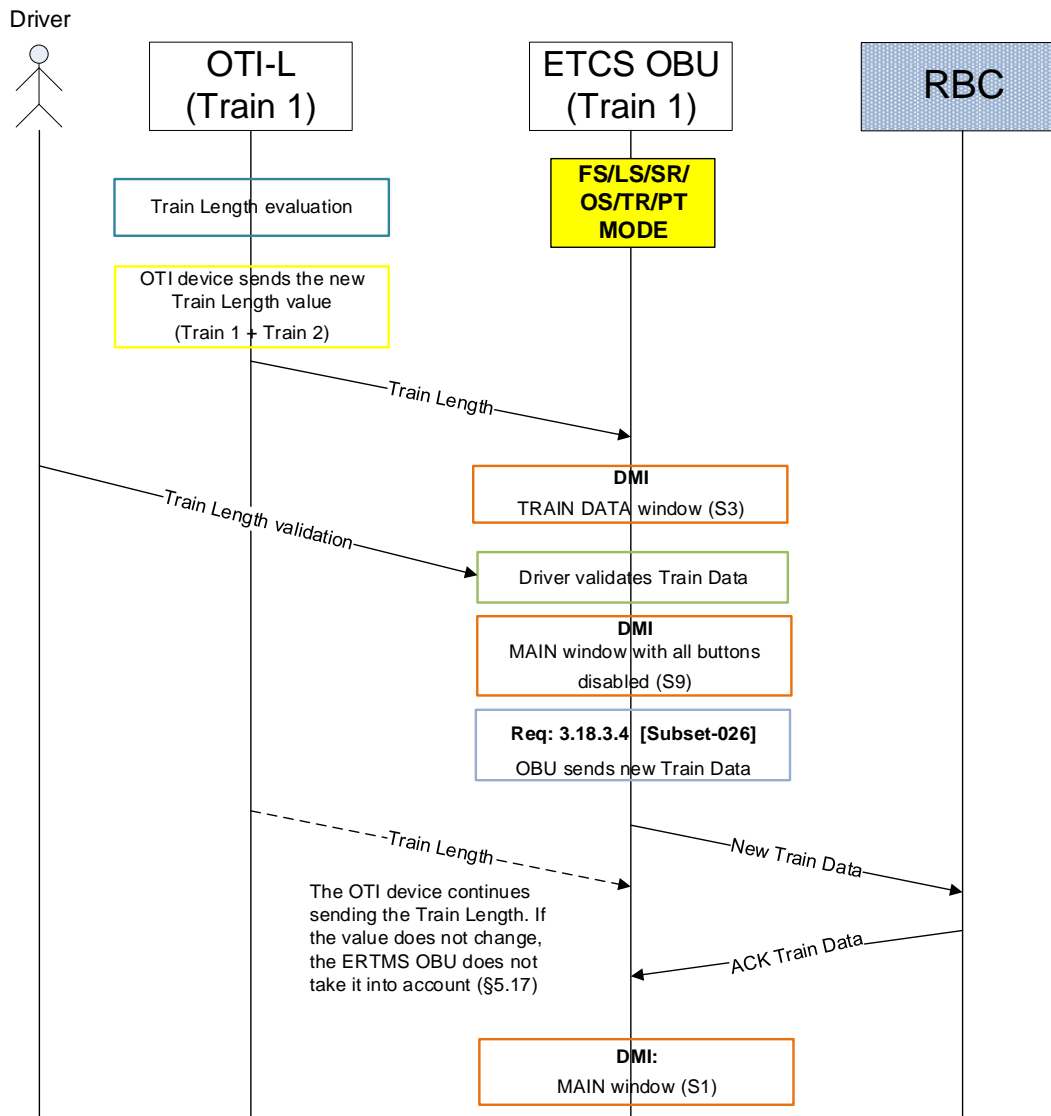
**Figure 8-15: Use Case 3 - Joining procedure – Step 1 – Nominal scenario**

Train 2 is mechanically joined to Train 1. OTI-L device evaluates and sends the new Train Length value to the ATP of Train 1.



**Figure 8-16: Use Case 3 - Joining procedure – Step 2 – Nominal scenario**

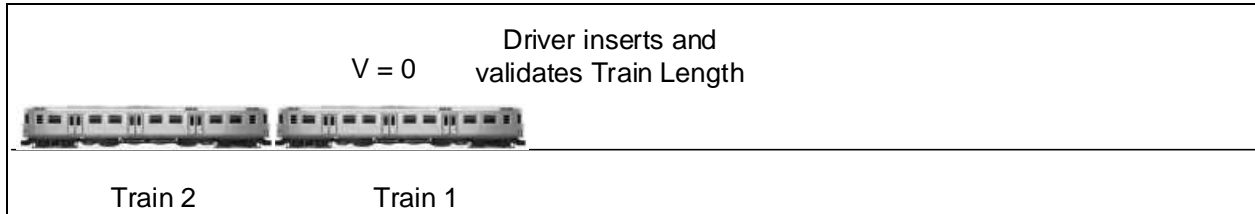
Following the sequence diagram of joining scenario:



**Figure 8-17: Use Case 3 - Example 1 (only Train Length)**

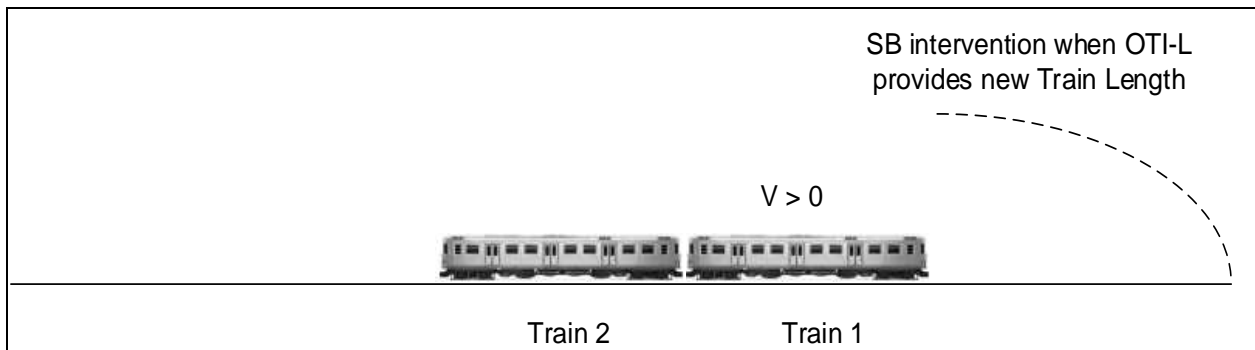
#### 8.4.3.2 Use Case n. 3: Example 2 (only Train Length) – Degraded scenario

In this example, after the joining operation, the OTI-L is not able to provide to the ERTMS/ETCS On-board sub-system the new Train Length value. In this case the Driver is responsible to insert and validate the new Train Length.



**Figure 8-18: Use Case 3 - Joining procedure – Step 1 – Degraded scenario**

The new train (Train 1 and Train 2) starts moving and the OTI-L provides the Train Length value different from the one inserted previously by the Driver. Due to requirements §5.17 Subset 026-5 ([1]), the OBU applies the Service Brake. The Driver has to acknowledge the brake intervention and has to validate the new Train Length value.



**Figure 8-19: Use Case 3 - Joining procedure – Step 2 – Degraded scenario**

Following the sequence diagram of this degraded scenario:

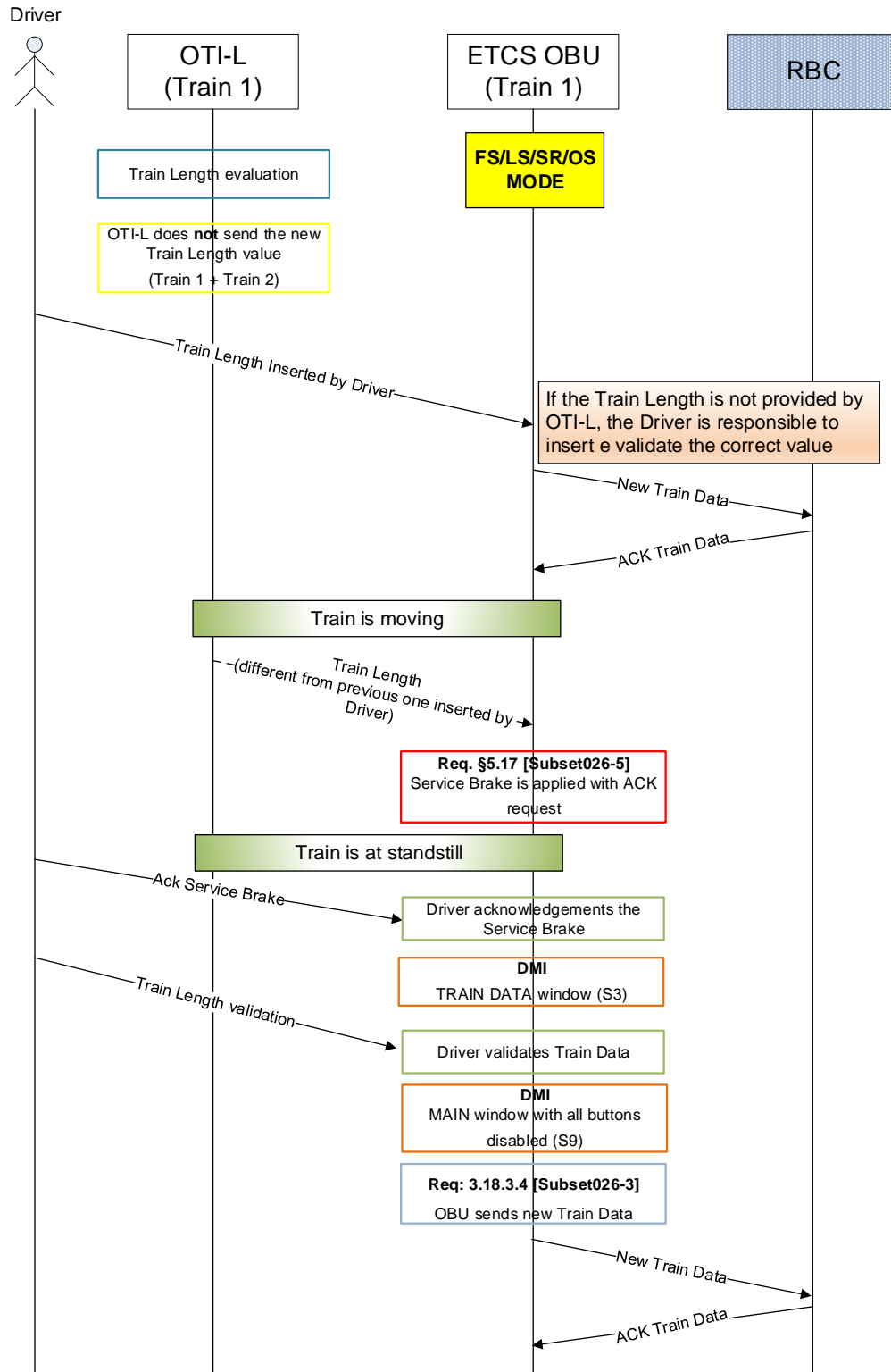


Figure 8-20: Use Case 3 - Example 2 (only Train Length)

#### 8.4.3.3 Use Case n. 3: Example 3 - Train Length and Train Integrity – Nominal scenario

In this scenario, after the joining procedure between Train 1 and Train 2, the ERTMS/ETCS On-board sub-system receives the Train Length information by OTI-L and then the Train Integrity Status by OTI-I.

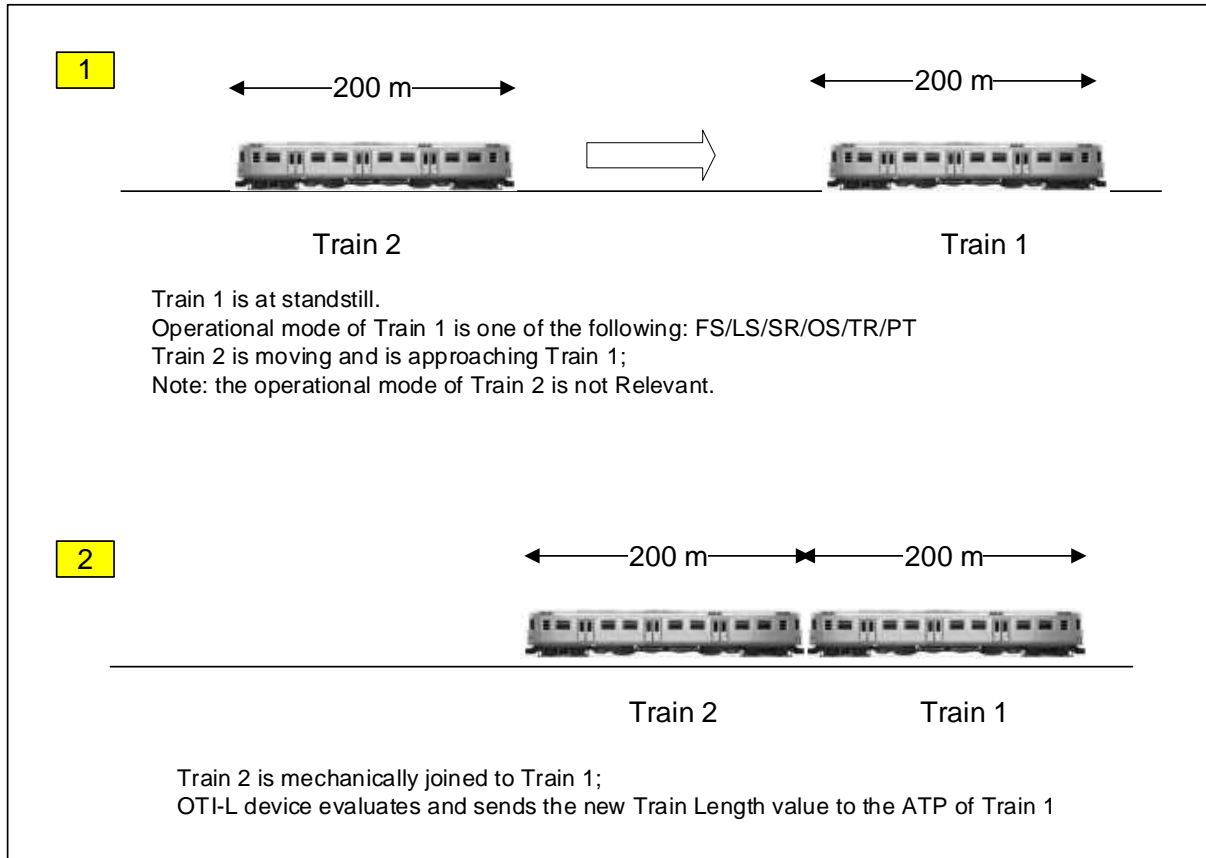


Figure 8-21 shows the sequence diagram of this scenario.

The following points are taken into account for this scenario:

- the ERTMS/ETCS On-board sub-system of Train 1 is in one of the following modes: FS/LS/SR/OS/TR/PT. Train 1 is at standstill;
- Backward Compatibility: the scenario is related to the Backward compatibility as explained in D4.2 ([7]). Driver presses the “Reset” and “Start” buttons to reset and start the FSM of OTI-L and OTI-I (note: this “START” button is different form the “START” button of DMI);
- T = Period of Position report;
- The states of OTI-L device reported in the yellow boxes in Figure 8-21 (Idle, Running/Unknown and Running/Known) are described in §8.7.1;
- The states of OTI-I device reported in the yellow boxes in Figure 8-21 (Mastership, Inauguration and Monitoring) are described in §7.1.

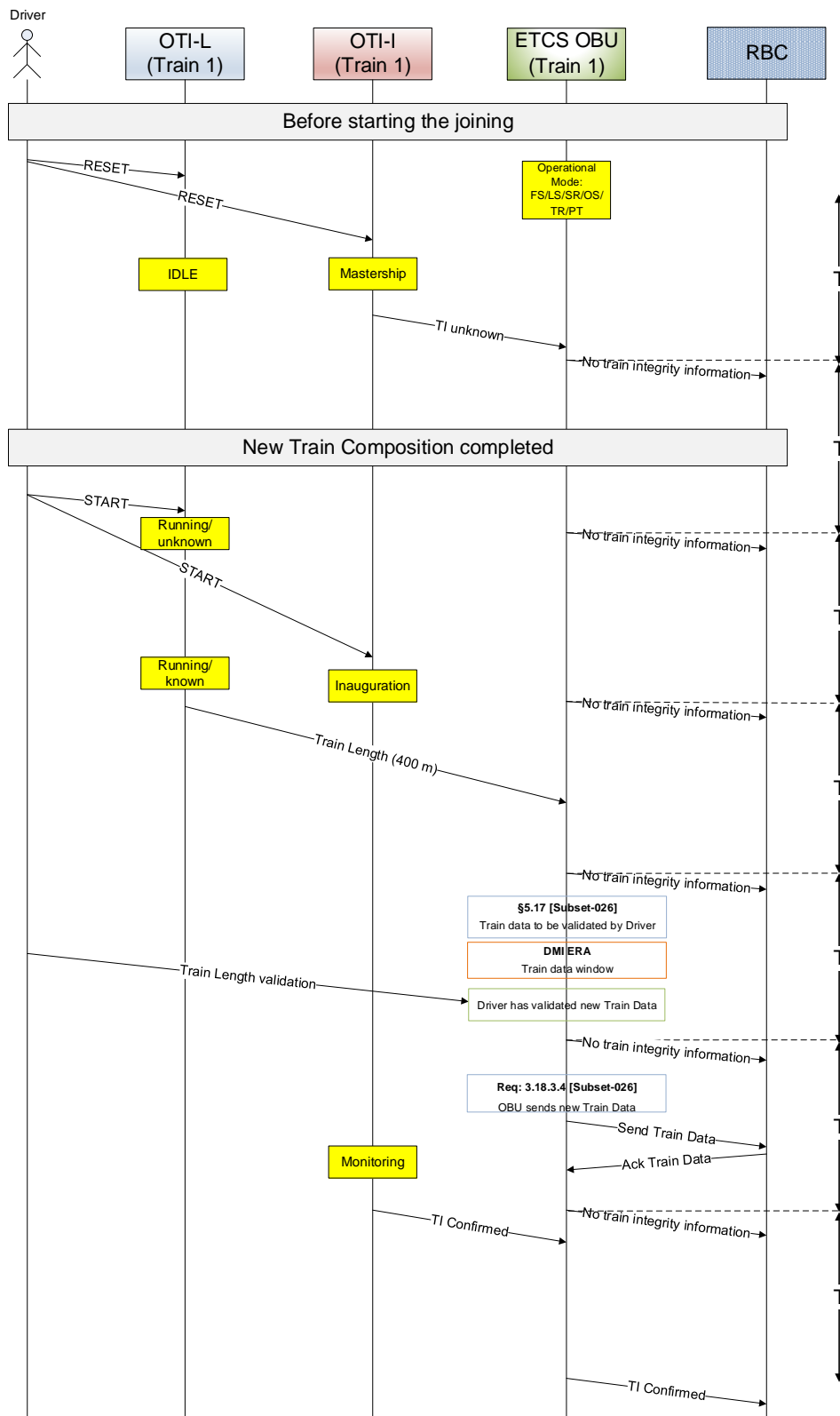
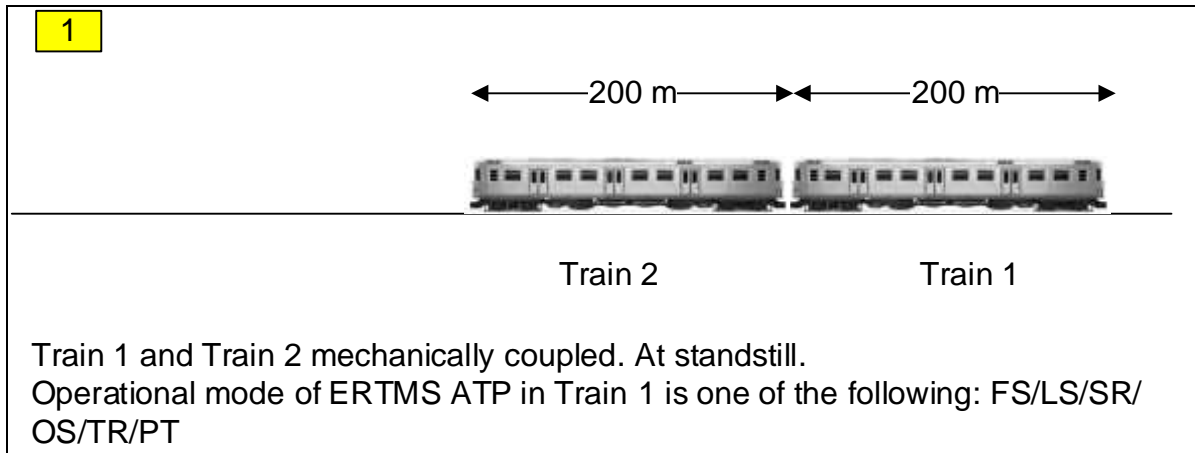


Figure 8-21: Use Case 3 - Example 3 (Train Length and Train Integrity)



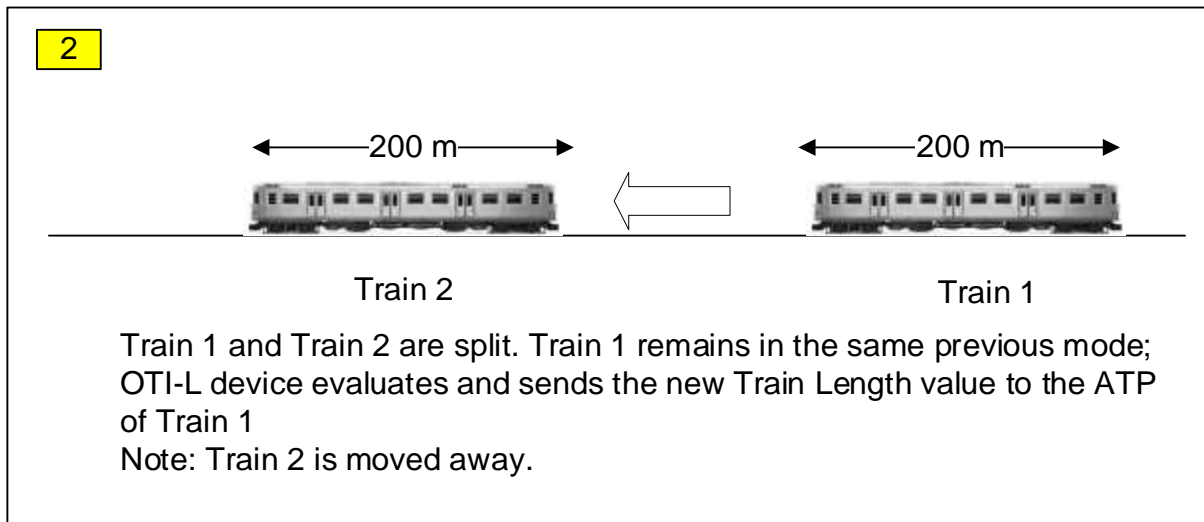
#### 8.4.3.4 Use Case n. 3: Example 4 - Train Length and Train Integrity – Nominal scenario

In this example, the train is composed by two trains (Train 1 and Train 2) mechanically coupled. It is at standstill and the ERTMS/ETCS Operational Mode is one between: FS/LS/SR/OS/TR/PT.



**Figure 8-22: Use Case 3 - Splitting procedure – Step 1 – Nominal scenario**

Train 1 and Train 2 are split. Train 1 remains in the same previous mode while Train 2 is moved away.



**Figure 8-23: Use Case 3 - Splitting procedure – Step 2 – Nominal scenario**

Figure 8-24 shows the sequence diagram of this scenario.

The following points are taken into account for this scenario:

- the ERTMS/ETCS On-board sub-system of Train 1 is in one of the following modes: FS/LS/SR/OS/TR/PT. Train 1 is at standstill;
- Backward Compatibility: the scenario is related to the Backward compatibility as explained in D4.2 ([7]). Driver presses the “Reset” and “Start” buttons to reset and start the FSM of OTI-L and OTI-I (note: this “START” button is different form the “START” button of DMI);

- T = Period of Position report;
- The states of OTI-L device reported in the yellow boxes in Figure 8-24 (Idle, Running/Unknown and Running /Known) are described in §8.7.1;
- The states of OTI-I device reported in the yellow boxes in Figure 8-24 (Mastership, Inauguration and Monitoring) are described in §7.1.

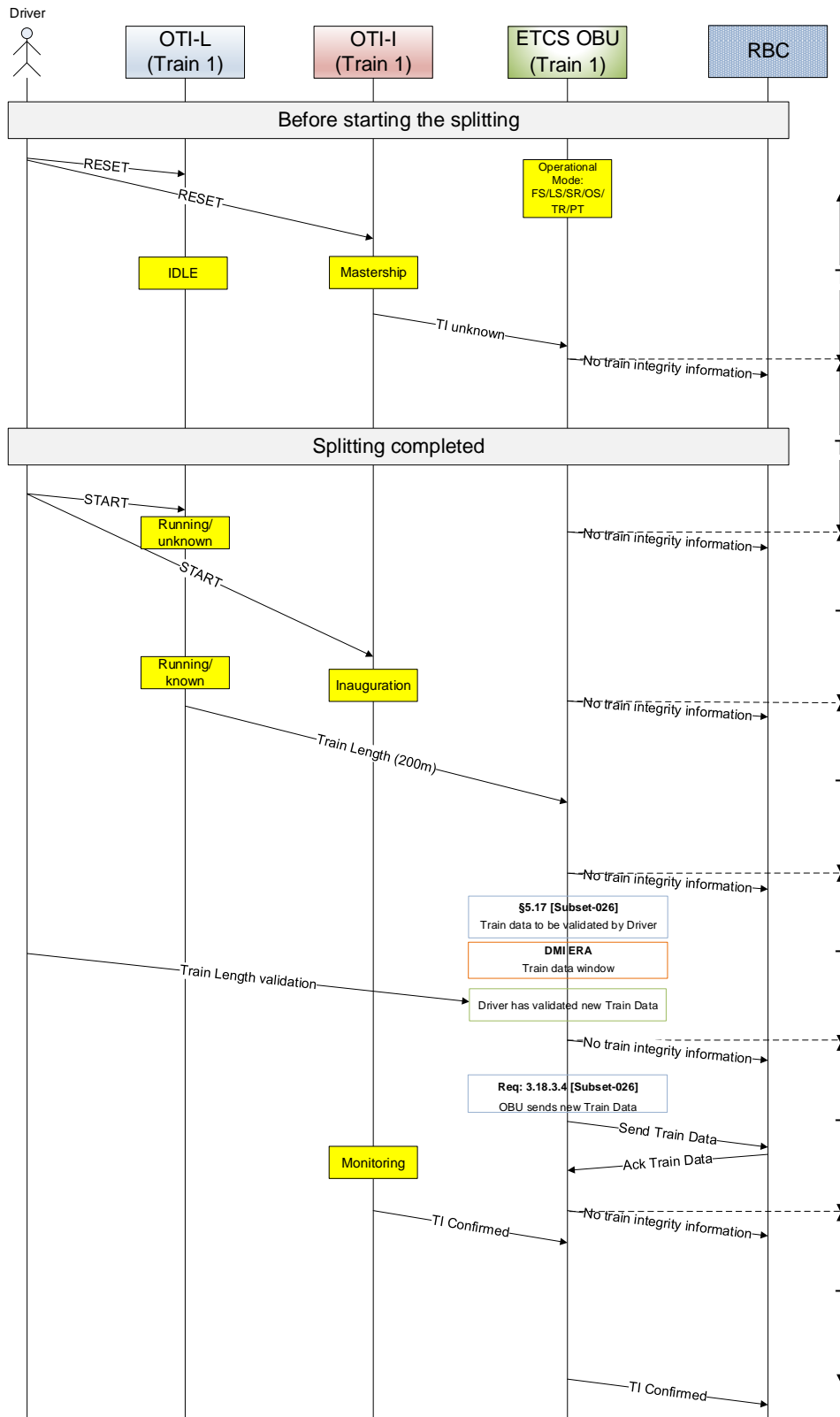


Figure 8-24: Use Case 3 - Example 4 (Train Length and Train Integrity)

#### 8.4.4 Use Case n. 4

This section describes and analyses the Use Case number 4 (see Table 8-9):

Use case	Train speed (V)	ERTMS/ETCS Operational Mode	Reception of Train Length (TL) and Train Integrity (TI) information by the ERTMS/ETCS On-board
4	Standstill (V = 0)	Different from Stand-by (SB)	TI before TL

The ERTMS/ETCS On-board sub-system is in a mode different from Stand-By mode (e.g. Full Supervision, Staff Responsible, etc.), train is at standstill. This Use Case covers joining and splitting scenarios.

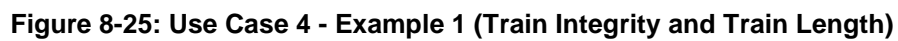
Differently from example 3 of Use Case 3, in this case the On-board sub-system receives the information of Train Integrity before the information of Train Length.

##### 8.4.4.1 Use Case n. 4: Example 1 - Train Integrity and Train Length

This example, Figure 8-25, shows the ERTMS/ETCS On-board sub-system behaviour when it receives the Train Integrity status by OTI-I and then the Train Length information by OTI-L.

The following points are taken into account for this scenario:

- the ERTMS/ETCS On-board sub-system of Train 1 is in one of the following modes: FS/LS/SR/OS/TR/PT. Train 1 is at standstill;
- Backward Compatibility: the scenario is related to the Backward Compatibility as explained in D4.2 ([7]). Driver presses the “Reset” and “Start” buttons to reset and start the FSM of OTI-L and OTI-I (note: this “START” button is different from the “START” button of DMI);
- T = Period of Position report;
- The states of OTI-L device reported in the yellow boxes in Figure 8-25 (Idle, Running/Unknown and Running/Known) are described in §8.7.1;
- The states of OTI-I device reported in the yellow boxes in Figure 8-25 (Mastership, Inauguration and Monitoring) are described in §7.1.



#### 8.4.5 Use Case n. 5

This section describes and analyses the Use Case number 5 (see Table 8-9):

Use case	Train speed (V)	ERTMS/ETCS Operational Mode	Reception of Train Length (TL) and Train Integrity (TI) information by the ERTMS/ETCS On-board
5	Moving ( $V > 0$ )	Different from Stand-by (SB)	TL before TI

The ERTMS/ETCS On-board sub-system is in a mode different from Stand-By mode (e.g. Full Supervision, Staff Responsible, etc.), train is moving. This Use Case covers joining and splitting scenarios.

Differently from Use Case 3, in this case the On-board sub-system receives the information of Train Length when the train is moving. The only difference with the Use Case 3 is the intervention of the Service Brake when the ERTMS/ETCS On-board sub-system receives the Train Length by OTI-L as requested by requirements in §5.17 of Subset 026-5 ([1]). So, the analysis of Use Case 3 is valid also for this Use Case 5.

#### 8.4.6 Use Case n. 6

This section describes and analyses the Use Case number 6 (see Table 8-9):

Use case	Train speed (V)	ERTMS/ETCS Operational Mode	Reception of Train Length (TL) and Train Integrity (TI) information by the ERTMS/ETCS On-board
6	Moving ( $V > 0$ )	Different from Stand-by (SB)	TI before TL

The ERTMS/ETCS On-board sub-system is in a mode different from Stand-By mode (e.g. Full Supervision, Staff Responsible, etc.), train is moving. This Use Case covers joining and splitting scenarios.

Differently from Use Case 4, in this case the ERTMS/ETCS On-board sub-system receives the information of Train Length when the train is moving. The only difference with the Use Case 4 is the intervention of the Service Brake when the ERTMS/ETCS On-board sub-system receives the Train Length by OTI-L as requested by requirements in §5.17 of Subset 026-5 ([1]). So, the analysis of Use Case 4 is valid also for this Use Case 6.

## 8.5 Results of the analysed scenarios

The analysis of the scenarios identified in §8.4 has highlighted the following points:

- 1) Driver could be required to validate Train Data twice during the Start of Mission as showed in the examples §8.4.1.2, §8.4.1.5, §8.4.2.1;
- 2) The ETCS On-board could send to RBC the information of Train Integrity status using a wrong value of Train Length, see examples in §8.4.2.1; §8.4.4.1;
- 3) Driver is required to select the RESET/START button to reset and re-start the FSM(s) of OTI-I and OTI-L, see examples in §8.4.3.3, §8.4.3.4, §8.4.4.1;

Point 1) has an operational impact (more actions are required to the Driver), point 2) could have an impact on the safety of the system and point 3) has operational and safety impact. For these reasons, the following requirements are required for OTI-L and for OTI-I when it operates in presence of OTI-L:

Req\_1: During the Start of Mission, The OTI-L shall provide to ERTMS/ETCS On-board the value of Train Length before the Driver performs the Train Data entry procedure;

*Rationale:* this requirement allows to avoid the double acknowledgement of Train Data by Driver during the SoM. Furthermore, the value of train length displayed on the DMI for the Train Data validation will be the one provided by OTI-L.

Req\_2: The OTI-I shall provide the status of train integrity “Confirmed” to the ERTMS/ETCS On-board only when it has received the value of train length provided by OTI-L.  
OTI-L shall send the information of train length value to OTI-I periodically.

*Rationale:* this requirement permits to exclude the scenario described in point 2). Furthermore, the justification for the periodic sending is that the value of train length is used by OTI-I to evaluate the train integrity status in case of wireless communication (see §7.1.1.5).

Note: this requirement is applicable for all Product Classes (see §6.2.3).

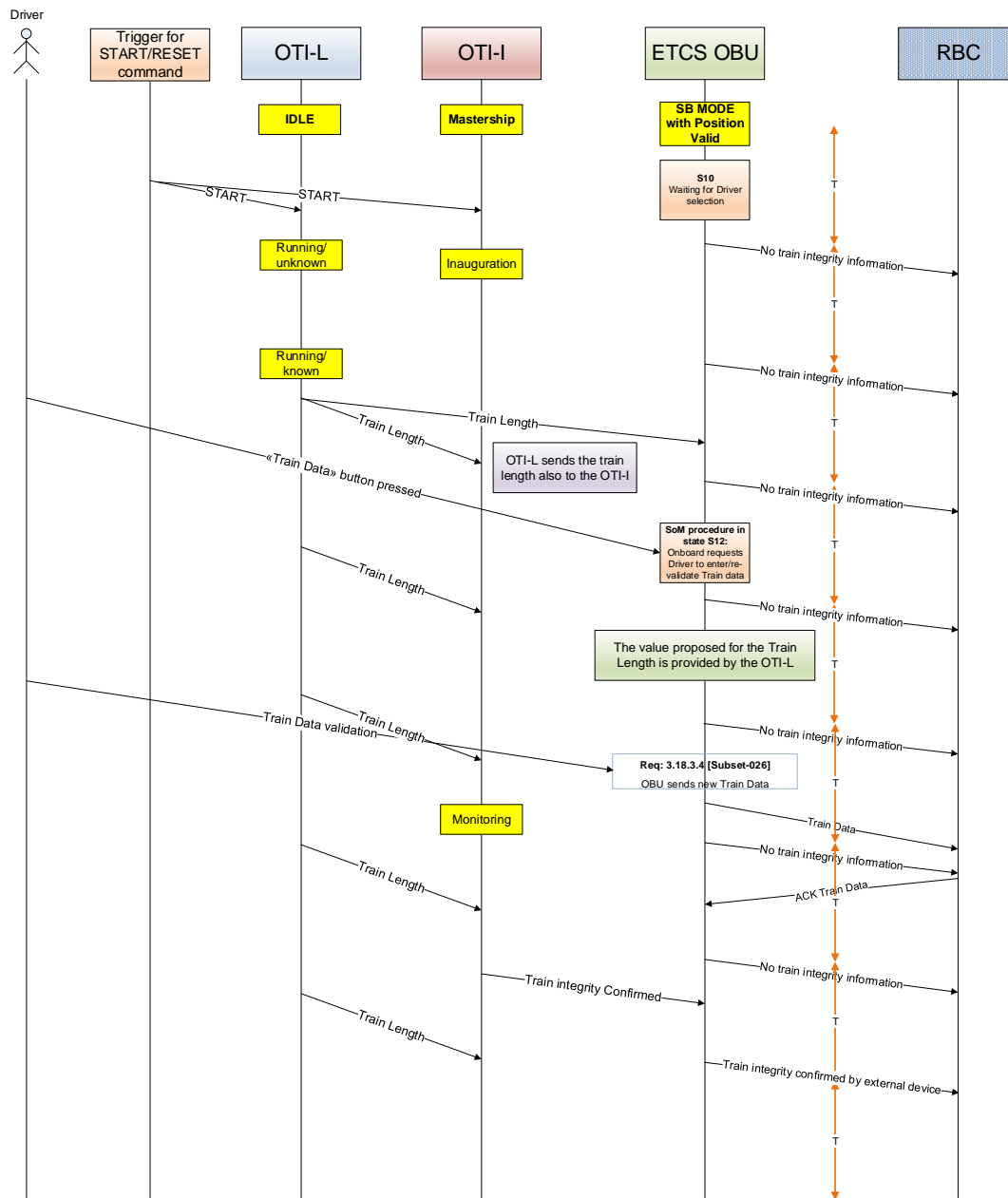
Req\_3: The OTI-L shall provide the value of train length to the ERTMS/ETCS On-board only when it receives a trigger command (START/RESET).

*Rationale:* this requirement allows to avoid a periodic sending of train length value by OTI-L to the ERTMS/ETCS On-board. Trigger command could be for example the opening of the desk or other mechanical actions linked to joining/splitting operations avoiding in this way to request to the Driver to press START/RESET button (note: this “START” button is different from the “START” button present on ETCS DMI).

Taking into account these requirements, it is possible to define the following scenarios:

S1. The ERTMS/ETCS On-board is in SB mode with “valid” position. On-board receives the Train Length data sent by OTI-L device before the Driver starts the Train Data entry procedure. Driver presses “Train Data” button on DMI and the ERTMS/ETCS On-board goes to state S12 (“S12: On-board requests Driver to enter/re-validate Train data”). Driver validates the Train Data. The OTI-I provides the Train Integrity status. T = Period of Position report.

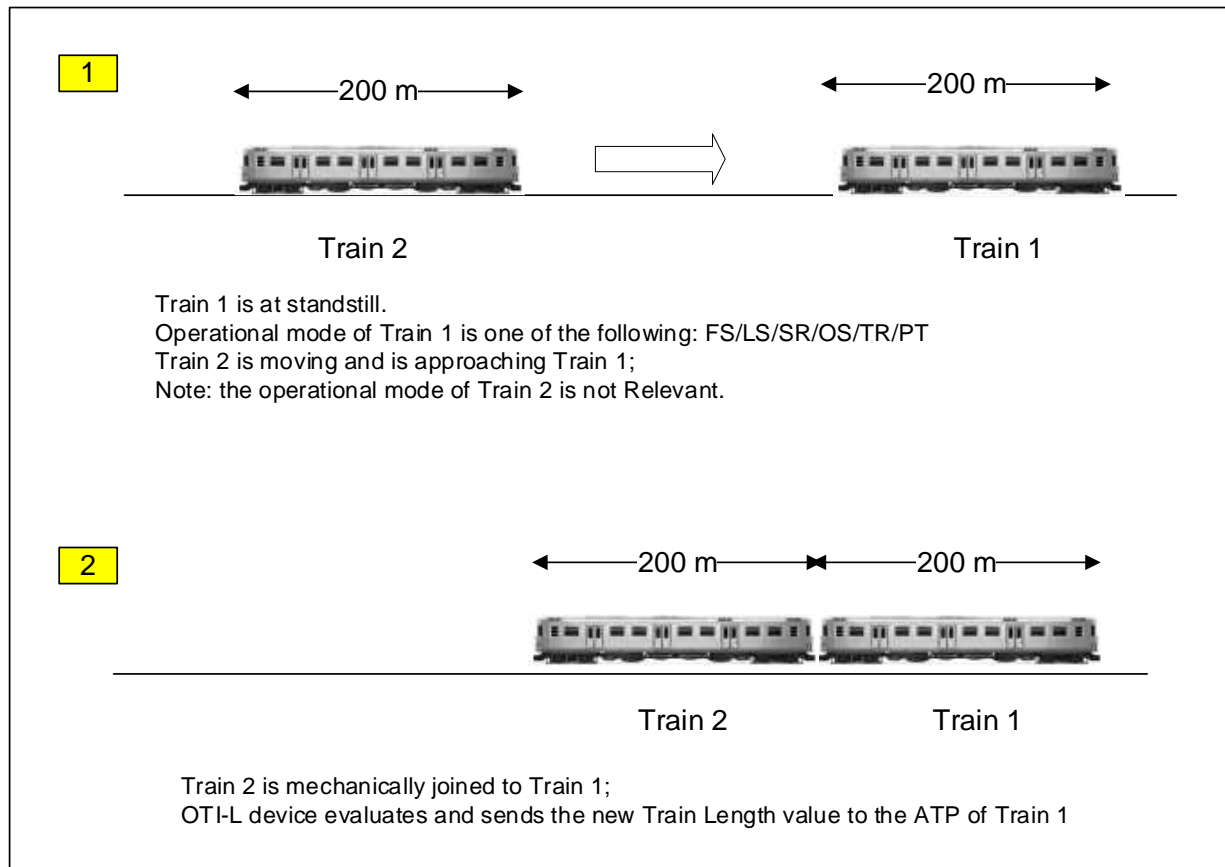
In the following sequence diagram (Figure 8-26) is not specified the event that triggers the START/RESET commands.



**Figure 8-26:** Example of Train Length and Train Integrity reception during SoM



S2. Joining scenario (see Figure 8-27 below). The ERTMS/ETCS On-board of Train 1 is in one of the following mode: FS/LS/SR/OS/TR/PT. The On-board receives the Train Length data sent by OTI-L device. Driver validates the new train length. The OTI-I provides the Train Integrity status. T = Period of Position report. Note: this scenario does not consider the solution used for train length determination and if the joined trains are at standstill or not when new train length is received (if the train is moving the requirements of §5.17 [1] shall be taken into account).

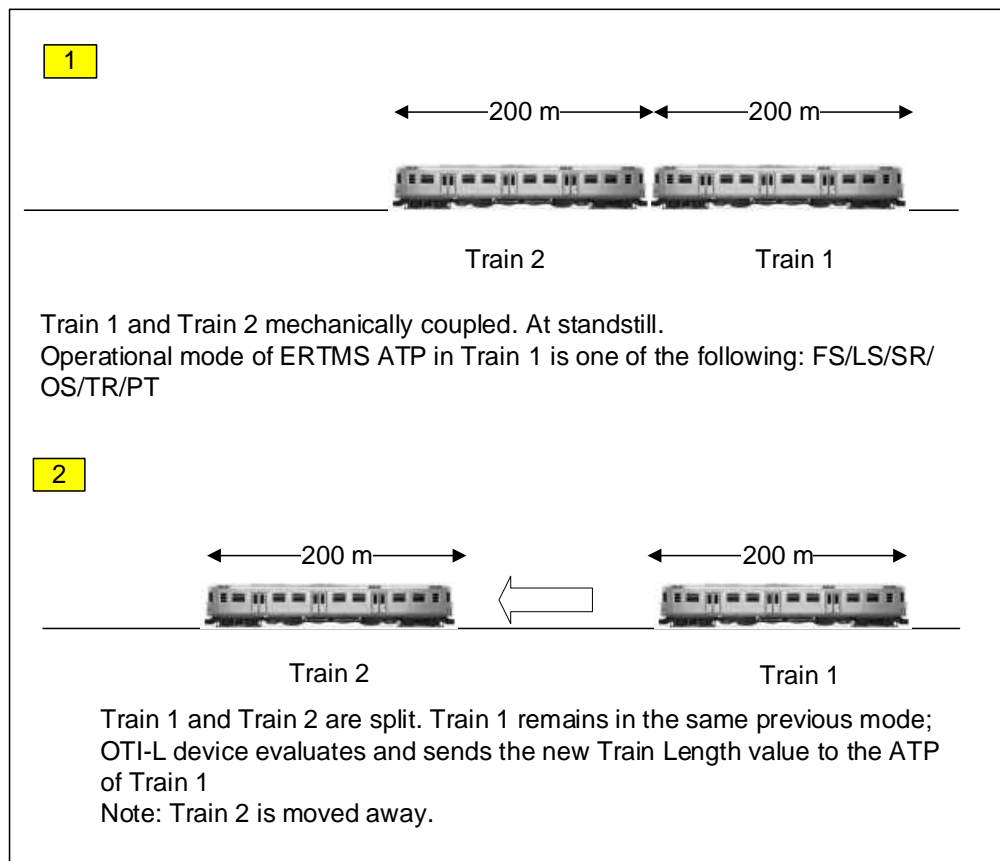


**Figure 8-27:** Example of Joining operation

In the following sequence diagram (Figure 8-28) is not specified the event that triggers the START/RESET commands.

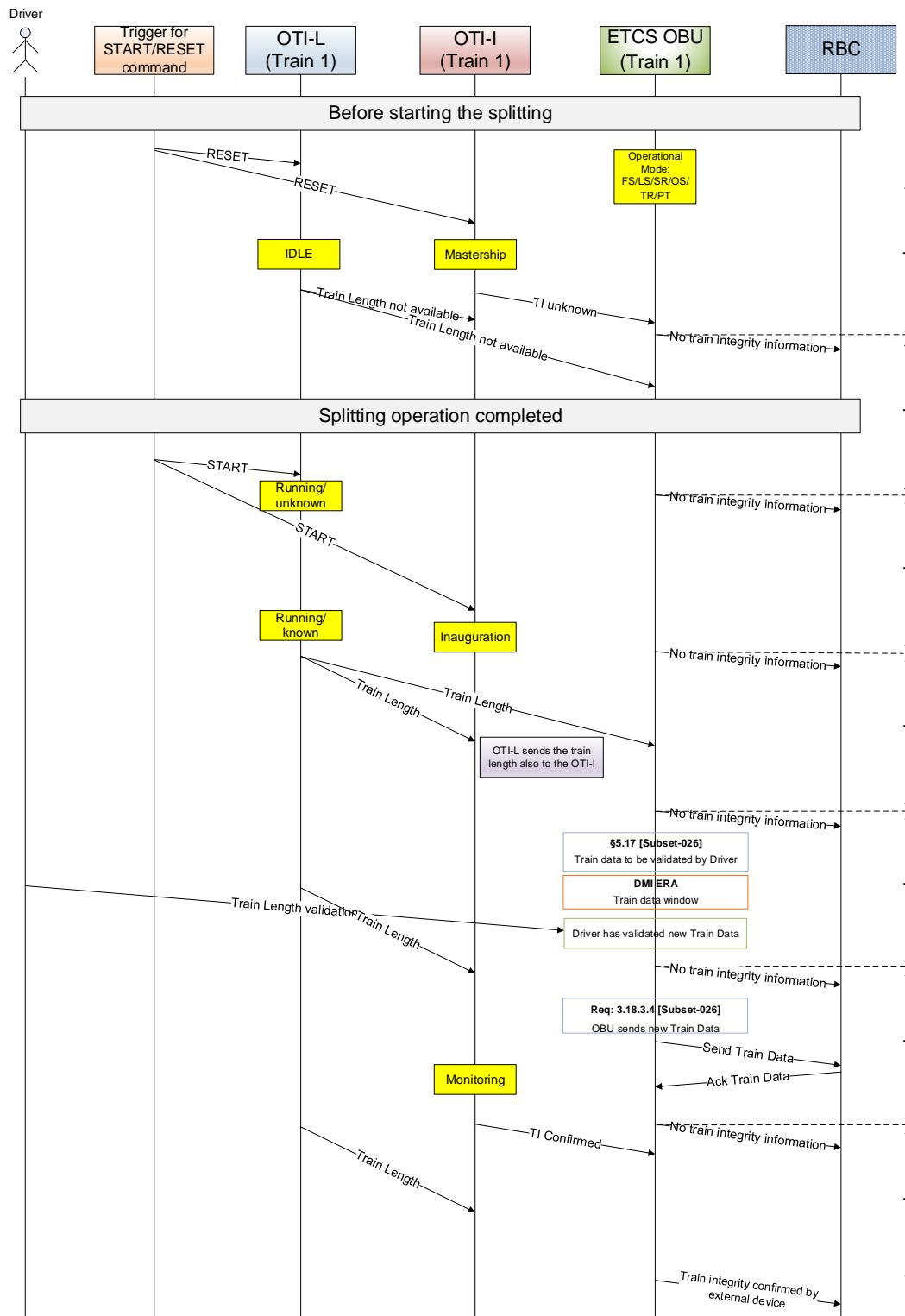


S3. Splitting scenario (see Figure 8-29 below). The ERTMS/ETCS On-board of Train 1 is in one of the following mode: FS/LS/SR/OS/TR/PT and receives the Train Length data sent by OTI-L device. Driver validates the new train length. The OTI-I provides the Train Integrity status. T = Period of Position report. Note: this scenario does not consider the solution used for train length determination and if the splitted trains are at standstill or not when new train length is received (if the train is moving the requirements of §5.17 [1] shall be taken into account).



**Figure 8-29:** Example of Splitting operation

In the following sequence diagram (Figure 8-30) is not specified the event that triggers the START/RESET commands.



**Figure 8-30:** Example of Train Length and Train Integrity reception after splitting operation

## 8.6 Hazard Analysis

This section includes the hazard analysis of the scenarios identified in §8.5:

- 1) Train length and train integrity status received during SoM (see scenario S1 in §8.5);
- 2) Joining procedure (see scenario S2 in §8.5);
- 3) Splitting procedure (see scenario S3 in §8.5);

And the analysis of the requirements related to the reception of train length by OTI-I when it is sent by ERTMS/ETCS On-board (see condition 0 and 3 in Table 7-2) and when it is sent by OTI-L (see “Req\_1:”, “Req\_2:” and “Req\_3:” defined in §8.5). This analysis is reported in §L.4

The hazard analysis of the previous scenarios is performed considering wired and wireless solutions (see §6.2.3):

- a) In case of wired network the train integrity criterion is based on communication status (e.g. regular exchange of liveness messages).
- b) In case of wireless network the train integrity criterion is based on verifying communication status and train tail status (i.e. train tail movement coherent with front cabin) based on train tail odometry data.

In case of wireless communication (case b)), the OTI Master shall evaluate the difference between train tail position and front cabin position and to perform this operation it needs to know the train length value that will be provided by the OTI-L.

The analysis is conducted identifying the main interfaces included in the scenarios (e.g. Driver, OTI-L, OTI-I and etc.), their main actions performed during the operation and applying the following failure conditions:

- a) Early/Late: function operated too soon or too late;
- b) Deletion: function failed to operate when required, or input/output data deleted;
- c) Corruption: function performed but with errors, or input/output data not correct;
- d) Repetition: function failed to stop operating, or data sent or received more times.

Finally, the failure effects at system level are identified.

Note that this analysis aims at identifying possible impacts of new equipment OTI-I and OTI-L on the Driver and ERTMS/ETCS system operation. It is out of scope of work the analysis of the current ERTMS/ETCS system requirements.

The details of the analysis are reported in §Appendix L.

Following Table 8-10 includes the list of all identified hazards / RAM equivalent (note: RAM equivalent to hazard is a condition that could lead to commercial loss related to RAM).

- HZ ID: hazard identifier;
- HZ Text: text of the hazard;
- Safety/RAM: this column specifies if the hazard impacts the safety of the system or RAM aspects (e.g. availability).

HZ ID	HZ Text	Safety/RAM
HZ_001	The ERTMS/ETCS On-board does not receive the Train Length value by OTI-L or receives it too late or uses a wrong value (less or greater than physical one).	Safety related
HZ_002	OTI-I provides to ERTMS/ETCS On-board the "Train Integrity Unknown" information or "Train integrity lost" when the integrity of the train should be confirmed.	No safety related
HZ_003	OTI-L provides to the ERTMS/ETCS On-board the train length value continuously, or the ERTMS/ETCS On-board receives the train length value continuously.	No safety related

**Table 8-10:** List of hazards for Train Integrity and Train Length Determination functions

Following Table 8-11 includes the list of mitigations.

- MIT ID: mitigation identifier;
- MIT Text: text of the mitigation;
- Safety related (Y/N): specifies if the mitigation is safety related (Y=Yes) or not (N=not);
- Mitigation Type: describes the type of mitigation, if it is an application condition to be exported (AC) or a requirement (REQ) to be implemented by the system;
- Assigned to: owner in charge to implement the mitigation;
- Mitigation implementation reference: reference to a requirement that covers the mitigation;

MIT ID	MIT Text	Safety related (Y/N)	Mitigation type	Assigned To:	Mitigation implementation reference
MIT_001	If defined by the system architecture, Driver shall be trained on the functionality of the OTI system (OTI-L and OTI-I) and in particular for the use of "START/RESET" command	Y	AC	Driver	This AC shall be exported to the Railway Undertakings
MIT_002	The OTI-L and OTI-I shall manage the "START/RESET" commands via a vital input. If these commands are received via serial interface, then OTI-L and OTI-I shall comply with 50159 Standard.	Y	REQ	OTI-I OTI-L	REQ.8.7.14 in §8.7.3
MIT_003	The Driver shall be informed (e.g. a message is displayed on DMI) if an OTI-L equipment is connected to ERTMS/ETCS On-board. If an OTI-L is present but it is not able to provide the train length value (during the Start of Mission procedure or during a mission, e.g. after joining or splitting operation),	Y	AC	ERTMS/ETCS On-board / Driver	REQ.8.7.21 in §8.7.3

	then the Driver shall be informed and it becomes the responsible to enter and validate the train length value.  [A timer shall be defined dependent by the specific application]				
MIT_004	The Train Length evaluation function performed by OTI-L shall be safety-related.	Y	REQ	OTI-L	REQ.8.7.15 in §8.7.3
MIT_005	The communication between the OTI-L and the ERTMS/ETCS On-board shall comply with 50159 Standard.	Y	AC	OTI-L / ERTMS/ETCS On-board	REQ.8.7.16 in §8.7.3
MIT_006	Determined train length shall include a margin to keep into account potential train length variations due to train expansion/contraction	N	REQ	OTI-L	REQ.8.7.2 in §8.7.3
MIT_007	If defined by the system architecture, the Train Interface Unit shall provide to the OTI system (OTI-L and OTI-I) the “START/RESET” command in a safe way. If this interface is based on serial communication, then it shall comply with 50159 Standard.	Y	AC	TIU	REQ.8.7.17 in §8.7.3
MIT_008	If defined by the system architecture, the ERTMS/ETCS On-board shall provide to the OTI system (OTI-L and OTI-I) the “START/RESET” command in a safe way. If this interface is based on serial communication, then it shall comply with 50159 Standard	Y	AC	ERTMS/ETCS On-board	REQ.8.7.18 in §8.7.3
MIT_009	The console used by Driver for “START/RESET” commands shall send this information via vital output. If this interface is based on serial communication, then it shall comply with 50159 Standard	Y	AC	Console	REQ.8.7.19 in §8.7.3
MIT_010	The communication between the OTI-L and the OTI-I shall comply with 50159 Standard.	Y	REQ	OTI-I OTI-L	REQ.8.7.20 in §8.7.3

**Table 8-11:** List of Mitigations for Train Integrity and Train Length Determination hazards

The following table reports the link between the hazards and the mitigation:

Hazard ID	Mitigation ID
HZ_001	MIT_001
	MIT_002
	MIT_003
	MIT_004
	MIT_005
	MIT_007
	MIT_008
	MIT_009
	Req_1
HZ_002	MIT_001
	MIT_002
	MIT_007
	MIT_008
	MIT_009
	MIT_010
HZ_003	Req_2
	MIT_001
	MIT_002
	MIT_005
	MIT_006
	MIT_007
	MIT_008
	MIT_009
	Req_3

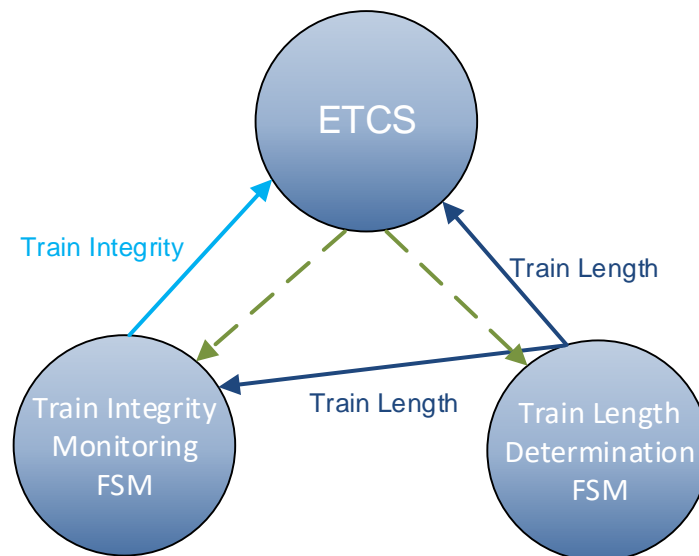
**Table 8-12:** Traceability: Hazards Train Length Determination – Mitigations



## 8.7 Requirements Specification

### 8.7.1 Functional Requirements

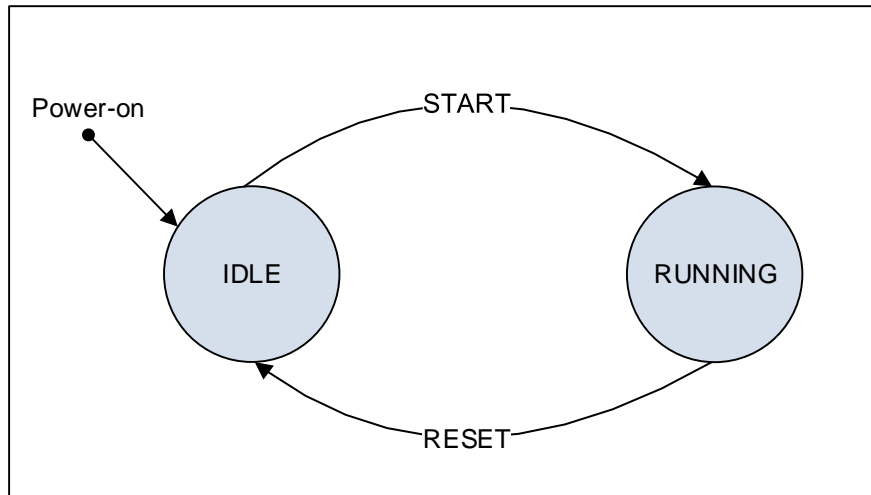
Train length determination function is provided by an additional FSM (OTI-L) independent from the train integrity monitoring function provided by FSM OTI-I (see Figure 7-3). As depicted in Figure 8-31, OTI-I and OTI-L provide their output to ERTMS/ETCS On-board. Similarly ERTMS/ETCS On-board sends messages to both FSMs (e.g. Start and Reset Commands). Note that OTI-I for Product Class 2 can use the train length information provided by OTI-L as input for train integrity criterion.



**Figure 8-31:** FSM for train length determination

REQ.8.7.1 The OTI-L shall implement the FSM depicted in Figure 8-32 and Figure 8-33, the transition conditions and actions described in Table 8-14 and Table 8-15.

OTI-L high level Finite State Machine is depicted in the following figure:



**Figure 8-32: OTI-L FSM**

OTI-L FSM transitions are reported in the following Table 8-13. Notation “1>” means that condition 1 has to be fulfilled to trigger a transition from the state reported in column to the state reported in row and highlighted with the arrow “>”. For each cell, the arrow refers to the direction of the state transition and the number refers to the transition conditions. States are reported in blue cells.

IDLE	<2
1>	RUNNING

**Table 8-13: OTI-L: FSM Transitions**

The following Table 8-14 describes the transition conditions:

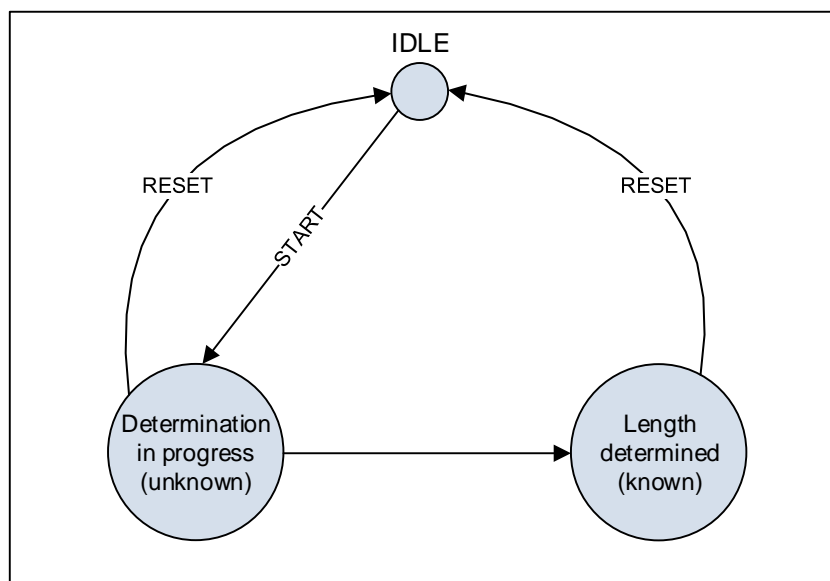
Condition	Transition conditions from mode X to mode Y	Entry action in Y state
1	<b>Transition from IDLE to RUNNING</b> OTI-L receives the START command	The OTI-L starts to evaluate the Train Length.  [Note: initially, the variable “ <i>Status Length Determination</i> ” (see [7]) assumes the value “ <i>Init</i> ”.]
2	<b>Transition from RUNNING to IDLE</b> OTI-L receives the RESET command	The OTI-L stops to evaluate the Train Length and deletes Train Length value previously calculated.  [Note: the variable “ <i>Status Length Determination</i> ” (see [7]) assumes the value “ <i>Not Available</i> ”. The OTI-L sends this information to the

		OTI-I and ERTMS/ETCS On-board.]
--	--	---------------------------------

**Table 8-14:** OTI-L: FSM Transitions conditions

Figure 8-33 below shows the macro-state RUNNING made of two internal sub-states:

- 1) Unknown: train length determination is in progress;
- 2) Known: train length determined.



**Figure 8-33:** OTI-L: RUNNING State

The following Table 8-15 describes the transition condition and the action to be performed when the sub-state changes to “Known”:

Transition from <b>UNKNOWN</b> to <b>KNOWN</b>	Action in <b>KNOWN</b> state
Train length has been determined	<p>The OTI-L sends to the ERTMS/ETCS On-board sub-system the Train Length value;</p> <p>The OTI-L sends periodically to the OTI-I the Train Length value.</p> <p>[Note: the variable “<i>Status Length Determination</i>” (see [7]) assumes the value “<i>Available</i>”.]</p>

**Table 8-15:** RUNNING State internal transition condition

REQ.8.7.2 Determined train length shall include a margin to keep into account potential train length variations due to train expansion.

*Rationale:* this requirement covers the “MIT\_006” defined in §8.6 (see Table 8-11).

Note 1: *margin* is intended as the difference between the maximum stretched length of a train and the length as determined.

Note 2: For example, as suggested by Infrastructure Manager, for long freight trains this expansion is estimated to be up to 5% of train length. In other cases the margin is 10 meters for freight trains composed of a maximum of 82 waggons. In general the margin value is a *configuration parameter* for specific application.

REQ.8.7.3 During the Start of Mission, the OTI-L shall provide to ERTMS/ETCS On-board the value of Train Length before the Driver performs the Train Data entry procedure.

*Rationale:* this requirement covers the “Req\_1:” defined in §8.5. See also REQ8.7.13 defined in §8.7.2.

REQ.8.7.4 The OTI-L shall provide the value of train length to the ERTMS/ETCS On-board only when it receives a trigger command (START).

*Rationale:* this requirement covers “Req\_3:” defined in §8.5.

REQ.8.7.5 The OTI-L shall provide the train length value and OTI-L status to the OTI-I. OTI-L shall send this information to the OTI-I periodically.

*Rationale:* this requirement with REQ.8.7.6 covers the “Req\_2:” defined in §8.5.

Note: the periodic sending of Train Length by OTI-L for the Product Class 1 could be disabled by using a Configuration Parameter. For Product Class 1, the train integrity criterion is not based on the management of train length values by OTI Master.

Note: OTI-L Status should be provided either in regular or fault state.

REQ.8.7.6 The OTI-I shall provide the status of train integrity to the ERTMS/ETCS On-board only when it has received a train length value from an external source if present.

Note: External source is intended as OTI-L.

*Rationale:* this requirement with REQ.8.7.5 covers the “Req\_2:” defined in §8.5.

The following requirements come from the analysis reported in §L.4 and related to the fact that the OTI-I can receive the Train Length information by ERTMS/STCS On-board (see condition 0 and 3 in Table 7-2) and by OTI-L (see REQ.8.7.5).

REQ.8.7.7 The ERTMS/ECTS On-board shall send to OTI-I the information of Train Length with the attribute of “validated” or “to be revalidated” (TBR).

Note: Use of “Validated” and “to be revalidated” attribute is depicted in Figure 10-1.

REQ.8.7.8 The OTI-I shall consider as “new” a Train Length value provided by ERTMS/ECTS On-board only if it has been “validated” and is different from the train length value received previously.

Note: A new train length value is used to trigger OTI-I FSM transitions, see Conditions 0 and 3 in Table 7-2.

REQ.8.7.9 The ERTMS/ECTS On-board shall send to OTI-I the information of Train Length “validated” if Driver has validated it or Train Length has been received by an external source and no Driver validation is required (see Figure 8-2 and Note 8).

REQ.8.7.10 The ERTMS/ECTS On-board shall send to OTI-I the information of Train Length “to be revalidated” (TBR) in the following case:

- 1) as specified in UNISIG Subset - 026 [1] (for example in case of a transition to Stand-by mode, see Table 8-7);
- 2) when the ERTMS/ETCS On-board sends the “Reset” Command to OTI-I;
- 3) when the ERTMS/ETCS On-board receives from the OTI-L the information of Train Length “Not Available”.

REQ.8.7.11 (optional) When the OTI-I receives the train length value by OTI-L and the “validated” train length value by ERTMS/ECTS On-board then it shall perform a comparison and shall verify if the values are equal or not. If the values are different then the OTI-I shall consider as correct the train length value provided by ERTMS/ECTS On-board.

Note: the train length values may be used by OTI Master of Product Class 2 as train integrity criterion. REQ 8.7.11 is product specific and is not applicable to all classes, therefore has been marked as optional.

REQ.8.7.12 When train driver changes, during ERTMS/ETCS data entry procedure, the train length value provided by OTI-L, the OTI-L shall be reset (e.g. by means of OTI dashboard or by ETCS).

Note: This requirement represents a mitigation in case OTI-L can't be resetted or OTI-L is not able to communicate to OTI-I.

## **8.7.2 Performance Requirements**

REQ.8.7.13 During the Start of Mission, the OTI-L shall be able to provide to ERTMS/ETCS On-board the value of Train Length in one (1) minute starting from the switching on of all systems (ERTMS/ETCS on-board, OTI-I and OTI-L).

*Rationale:* the time of one minute should be enough to guarantee that when the Driver performs the Train Data Entry procedure the value of train length is available and provided by the OTI-L.

Note: OTI-I and OTI-L functions are switched on simultaneously and START/RESET commands are used to trigger them simultaneously.

## **8.7.3 Safety Requirements**

REQ.8.7.14 The OTI-L and OTI-I shall manage the “START/RESET” commands via a vital input. If these commands are received via serial interface, then OTI-L and OTI-I shall comply with 50159 Standard ([5]).

*Rationale:* this requirement covers the mitigation MIT\_002 (see Table 8-11).

REQ.8.7.15 The Train Length evaluation function performed by OTI-L shall be safety-related. The Safety Integrity Level required is SIL4.

*Rationale:* this requirement covers the mitigation MIT\_004 (see Table 8-11) and the assumption in §8.3.

REQ.8.7.16 The communication between the OTI-L and the ERTMS/ETCS On-board shall comply with 50159 Standard.

*Rationale:* this requirement covers the mitigation MIT\_005 (see Table 8-11).

REQ.8.7.17 If defined by the system architecture, the Train Interface Unit shall provide to the OTI system (OTI-L and OTI-I) the “START/RESET” command in a safe way. If this interface is based on serial communication, then it shall comply with 50159 Standard ([5]).

*Rationale:* this requirement covers the mitigation MIT\_007 (see Table 8-11).

REQ.8.7.18 If defined by the system architecture, the ERTMS/ETCS On-board shall provide to the OTI system (OTI-L and OTI-I) the “START/RESET” command in a safe way. If this interface is based on serial communication, then it shall comply with 50159 Standard ([5]).

*Rationale:* this requirement covers the mitigation MIT\_008 (see Table 8-11).

REQ.8.7.19 The console used by Driver for “START/RESET” commands shall send this information via vital output. If this interface is based on serial communication, then it shall comply with 50159 Standard ([5]).

*Rationale:* this requirement covers the mitigation MIT\_009 (see Table 8-11).

REQ.8.7.20 The communication between the OTI-L and the OTI-I shall comply with 50159 Standard ([5]).

*Rationale:* this requirement covers the mitigation MIT\_010 (see Table 8-11).

REQ.8.7.21 If an OTI-L is not present or is present but it is not able to provide the train length value (during the Start of Mission procedure or during a mission, e.g. after joining or splitting operation), then the driver shall be informed (e.g. OTI Dashboard, ETCS).

[A timer shall be defined dependent by the specific application].

*Rationale:* this requirement covers the mitigation MIT\_003 (see Table 8-11).

## 9 Conclusions

---

This document focused on OTI concept definition and functional requirements specification. Analysis of application domains and reference scenarios resulted in identifying specific requirements related to train integrity functionality and resulted in defining three OTI product classes. First product class is referred to trains with wired on-board communication network and train integrity criteria is based on communication liveliness between an OTI Slave module located at train tail and OTI Master module located in front cabin. Second product class is referred to trains with wireless on-board communication network and train integrity criteria is based on comparing kinematic data of train tail and front cabin (e.g. position, speed, acceleration). Product class 1 and 2 required installing OTI Slave module at train tail and OTI Master module in front cabin. Installing OTI Slave in all waggons is an optional possibility to increase the flexibility in joining/splitting phases.

Product Class 1 and 2 provides train integrity functionality with a limited cost, whereas Product Class 3 offers further optional functionality with a higher cost.

An installation analysis is also reported for freight application domain. Identified guidelines refers to mechanical constraints in terms of device size and position in a freight waggon. Also reference to joining/splitting procedure are considered in relation to brake pipe connection between adjacent waggons. Fixed OTI modules installation and portable OTI module options are considered for Product Classes 1 and 2.

On the basis of defined product classes, OTI Finite State Machine was defined in terms of behaviour in each state and transition conditions. OTI behaviour is also described with sequence diagrams in identified reference scenarios (e.g. joining/splitting). A preliminary analysis for Virtual Coupling is also considered to support dynamic joining/splitting. This topic requires further investigation in the basis of complete functional requirements specification that shall be defined and delivered by TD2.8.

Functional hazard analysis is also considered to identify safety related requirements and to provide a qualitative SIL identification.

The document explored also wireless and GNSS technologies that shall be explored in more details in development phase of the project.

The functional requirements for train length determination are specified based on an analysis of existing ETCS specification, the identifying of use case scenarios and execution of functional hazard analysis.

Functional specifications constitute the input for logical architecture and interfaces specification and for subsequent development phase.

## 10 References

---

- [1] SUBSET 026 - ERTMS/ETCS - System Requirement Specification - v3.6.0
- [2] SUBSET 034 - ERTMS/ETCS - Train Interface FIS - v3.2.0
- [3] CR940 – Modifications related to Train Integrity functionalities - 14.06.2017
- [4] SUBSET 037 - ERTMS/ETCS - EuroRadio FIS - v3.2.0
- [5] CENELEC EN 50159 – Railway Applications - Communication, Signalling And Processing Systems - Safety-Related Communication In Transmission Systems - 2010
- [6] CENELEC EN 50155 – Railway Applications - Rolling Stock - Electronic Equipment - 2017
- [7] X2Rail-2 D4.2 Functional architecture & Interfaces specifications & Candidate technologies selection
- [8] X2Rail-2 D4.4 System architecture specifications
- [9] SUBSET 119 - ERTMS/ETCS - Train Interface FFFIS – 1.0.15
- [10] SUBSET 077 – UNISIG Causal Analysis Process – v3.0.0
- [11] CENELEC EN 50126 - Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - 2000
- [12] Tammy Parker (2013-09-02). "Wi-Fi preps for 900 MHz with 802.11ah". FierceWirelessTech.com. Retrieved 2014-06-25.
- [13] Sun, Weiping; Choi, Munhwan; Choi, Sunghyun (July 2013). "IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz" (PDF). Journal of ICT Standardization. 1 (1): 83–108.
- [14] IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE)". U.S. Department of Transportation. April 13, 2013. Retrieved 2014-11-14.
- [15] Final draft ETSI ES 202 663 V1.1.0 (2009-11)". European Telecommunications Standards Institute. Retrieved 2013-04-16.
- [16] Bilging B.E.; Gungor V.C. Performance Comparison of IEEE 802.11p and IEEE 802.11b for Vehicle-to-Vehicle Communications in Highway, Rural, and Urban Areas. November 2013.
- [17] "Bluetooth Core Specification v5.0". www.bluetooth.org.
- [18] "Bluetooth Radio Interface, Modulation & Channels". Radio-Electronics.com.
- [19] Wang et. al. ZigBee® network protocols and applications
- [20] Park, S.; Kim, K.; Haddad, W.; Chakrabarti, S.; Laganier, J. (March 2011). IPv6 over Low Power WPAN Security Analysis. IETF. I-D draft-daniel-6lowpan-security-analysis-05. Retrieved 10 May 2016.
- [21] "Introducing Thread". SI Labs. Retrieved 21 October 2014.
- [22] Olsson, Jonas (2013). "6LoWPAN Demystified", Texas Instruments.
- [23] "Thread Stack Fundamentals". Thread Group. 2015. Retrieved 1 April 2017
- [24] WiMAX vs. WiFi. Circleid.com (2008-02-20). Retrieved on 2013-09-18.
- [25] Wimax Technology, <http://freewimaxinfo.com/>
- [26] Harold Stark, "The Ultimate Guide To Building Your Own Smart Home In 2017,"Forbes, May 22, 2017.
- [27] "Z-Wave 500 series," Aeotc.com. Accessed July 30, 2017.
- [28] Lou Frenzel (29 November 2012). "What's The Difference Between Bluetooth Low Energy And ANT?". Electronics Design.



- [29] "Nordic Semiconductor figures for nRF24AP1". Nordic Semiconductor. Archived from the original on 29 October 2007. Retrieved 11 Dec 2007.
- [30] Khssibi, Sabri; Idoudi, Hanen; Van Den Bossche, Adrien; Saidane, Leila Azzouz (2013). "Presentation and analysis of a new technology for low-power wireless sensor network". *International Journal of Digital Information and Wireless Communications*
- [31] "Connectivity Options Explained". ANT+ Explained. 27 Oct 2015
- [32] Grant, Svetlana: 3GPP Low Power Wide Area Technologies - GSMA White Paper, GSMA. p. 49. September 1, 2016.
- [33] Y.-P. Eric Wang ; Xingqin Lin ; Ansuman Adhikary ; Asbjorn Grovlen ; Yutao Sui ; Yufei Blankenship ; Johan Bergman ; Hazhir S. Razaghi: A Primer on 3GPP Narrowband Internet of Things, *IEEE Communications Magazine* (Volume: 55, Issue: 3, March 2017), p. 117-123.
- [34] Z. Jenipher Wang: Unlocking the Potentials of Smart IoT with LPWA Technologies, *The WIOMAX SmartIoT Blog*.
- [35] "LoRaWAN For Developers". [www.lora-alliance.org](http://www.lora-alliance.org).
- [36] Qusay F. Hassan, Atta ur Rehman Khan, Sajjad A. Madani: *Internet of Things: Challenges, Advances, and Applications*, Chapman & Hall/CRC Computer and Information Science Series
- [37] Giedre Dregvaite; Robertas Damasevicius: *Information and Software Technologies: 22nd International Conference, ICIST 2016, Druskininkai, Lithuania, October 13-15, 2016, Proceedings*. Springer. pp. 665
- [38] Symphony Link vs LoRaWAN-Difference between Symphony Link and LoRaWAN, Link Labs, Annapolis, MD 21401
- [39] "TETRA - PST". PST. January 2017.
- [40] Terrestrial Trunked Radio (TETRA); Release 2, ETSI TR 102 580 V1.1.1 (2007-10)
- [41] TETRA (Terrestrial Trunked Radio), *Global Telecoms Inside*. <http://www.mobilecomms-technology.com>
- [42] TETRA Technology Advantages & Benefits, TETRA association, January 2016.
- [43] LTE System Overview, *LTE Encyclopedia*.
- [44] LTE for Critical Communications, Rohill, LTEetraNode, June 2015.
- [45] Juergen Merkel: 3GPP drives GSM-R to a new track, 3GPP, August 2016.
- [46] Werner R., Robles R., Priller P., Dominguez L., Rivilla J., Koivusaari J., Komi M., van Driel W. – DEWI – Wirelessly into the Future – 2015, CISTER-TR-150706
- [47] Dominguez L. - Wireless for safety Demonstrator – 2017, D4.7.2
- [48] L. Pushparatnam, T. Taylor, Other contributors - GSM-R Implementation and Procurement Guide - 2009, 978-2-7461-1631-3
- [49] FRMCS - Future Railway Mobile Communication System – 2016, <https://uic.org/frmcs>
- [50] Parrilla F., Alonso M., Batista D., Alberdi A., Goya J., de Miguel G., Mendizabal J. - Technologies Evaluation for Freight Train's Wireless Backbone – 2018, *nets4trains*
- [51] Winkler V. - "Range Doppler Detection for automotive FMCW Radars" - October 2007, *Proc. of the 37th European Microwave Conference*.
- [52] Arastounia M. - "Automated Recognition of Railroad Infrastructure in Rural Areas from LIDAR Data" - 2015, *Remote Sens*.
- [53] Elberink S. O., Khoshelham K. - Automatic Extraction of Railroad Centerlines from Mobile Laser Scanning Data. – 2015, *Remote Sens*.
- [54] RFID in RAIL. European Guideline for the Identification of Railway Assets using GS1 Standards – 2012, GS1

- [55] Amanna A., Agrawal A., Manteghi M. - Active RFID for Enhanced Railway Operations – 2010, American Society of Mechanical Engineers, Rail Transportation Division (Publication) RTD. 10.1115/RTDF2010-42006
- [56] AIOTI WG03 - High Level Architecture (HLA) - June 2017, AIOTI ALLIANCE FOR INTERNET OF THINGS INNOVATION
- [57] Parrilla F., Dominguez L. – Smart Train Coupling Use Case Specification – December 2017, D19.1 SCOTT Project
- [58] Parrilla F. – D3.1 – Requirement Analysis and Technologies Evaluation for Train's Wireless Backbone – March 2018, S2R Consortium FR8R Project
- [59] Ulianov C., Hyde P. - Benchmark and market drivers for an integrated intelligent and lightweight waggon solution – March 2017, D1.1 730863 - S2R-OC-IP5-03-2015
- [60] CENELEC EN 45545-2:2013+A1:2015- Railway applications. Fire protection on railway vehicles. Requirements for fire behaviour of materials and components
- [61] CENELC EN 60529
- [62] J. Marais, J. Beugin, and M. Berbineau, "A survey of GNSS-based Research and Developments for the European railway signaling," IEEE Trans. Intell. Transp. Syst., vol. 18, no. 10, pp. 2602–2618, Oct. 2017.
- [63] J. Otegui, A. Bahillo, I. Lopetegi, and L. E. Díez, "A survey of train positioning solutions," IEEE Sensors J., vol. 17, no. 20, pp. 6788–6797, Oct. 2017
- [64] J. Beugin, C. Legrand, J. Marais, M. Berbineau, E.M. El Kursi, février 2018, Safety Appraisal of Localization Systems Based on GNSS Used in Train Spacing Control, IEEE Access.
- [65] STARS H2020 project, <http://www.stars-rail.eu>
- [66] RSSB GE/GN8578 Guidance on the Use of On-Train Satellite Positioning Technology Based Locator for Railway Applications Issue Three December 2015 Rail Industry Guidance Note.
- [67] Alexey Khoryaev, "Evolution of Cellular-V2X (C-V2X) Technology", IEEE ComSocWebinar, 2018
- [68] A. Millán – D7.1 – Analysis of existing lines and economic models – June 2017, S2R Consortium X2R-1 Project
- [69] Stallo, C., Neri, A., Salvatori, P., Capua, R., & Rispoli, F. (2018). GNSS Integrity Monitoring for Rail Applications: 2-tiers method. IEEE Transactions on Aerospace and Electronic Systems
- [70] Goya, J., Zamora-Cadenas, L., Arrizabalaga, S., Brazález, A., Meléndez, J., & Mendizabal, J. (2015). Advanced Train Location Simulator (ATLAS) for developing, testing and validating on-board railway location systems. European Transport Research Review, 7(3), 24
- [71] Marais, J., Meurie, C., Flancquart, A., Lithgow, S., & Barbu, G. (2014, January). Innovative simulations of GNSS performances in a realistic railway environment. In Proc. Int. Symp. Certification GNSS Syst. Services (CERGAL) (p. 5)
- [72] Falco, Gianluca, Nicola, Mario, Falletti, Emanuela, "An HW-In-the-Loop Approach for the Assessment of GNSS Local Channel Effects in the Railway Environment," Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, Florida, September 2018, pp. 3463-3477
- [73] Zhu, N., Marais, J., Bétaille, D., & Berbineau, M. (2018). GNSS position integrity in urban environments: A review of literature. IEEE Transactions on Intelligent Transportation Systems, (99), 1-17
- [74] ERA\_ERTMS\_015560 - ETCS Driver Machine Interface v3.6.0

[75] SUBSET 120 - FFFIS TI – Safety Analysis – v1.0.11

[76] SUBSET 023 - Glossary of Terms and Abbreviations – 3.3.0

## APPENDIX A PHA

This appendix includes the Preliminary Hazard Analysis as specified in §7.2.8:

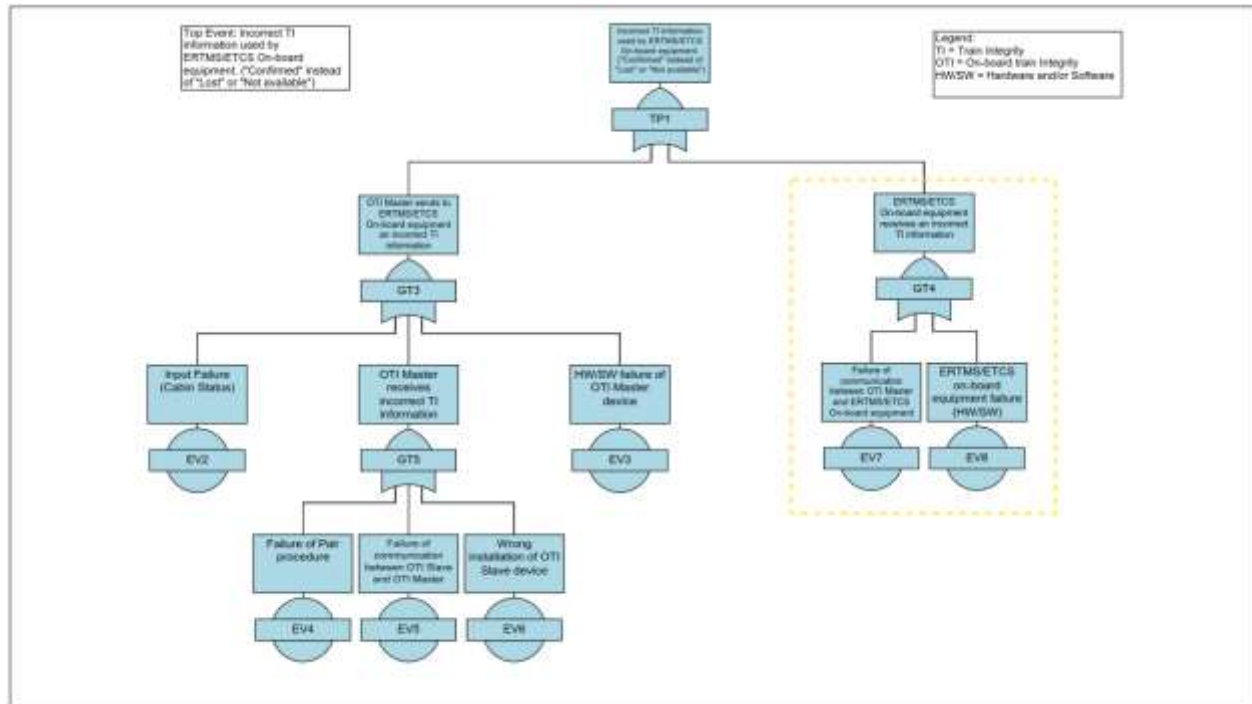
- **OTI\_PHA\_PC\_1A:** hazard analysis of the Product Class 1-A, see Appendix C;
- **OTI\_PHA\_PC\_1A\_Join:** hazard analysis of the Product Class 1-A in case of joining trains, see Appendix D;
- **OTI\_PHA\_PC\_1B:** hazard analysis of the Product Class 1-B: see Appendix E;
- **OTI\_PHA\_PC\_1B\_Join:** hazard analysis of the Product Class 1-B in case of joining train, see Appendix F;
- **OTI\_PHA\_PC\_2A\_2B:** hazard analysis of the Product Class 2-A and 2-B, see Appendix G;
- **OTI\_PHA\_PC\_2A\_2B\_JoinSplit:** hazard analysis of the Product Class 2-A and 2-B in case of joining/splitting trains, see Appendix H;

## APPENDIX B PRODUCT CLASS FTA

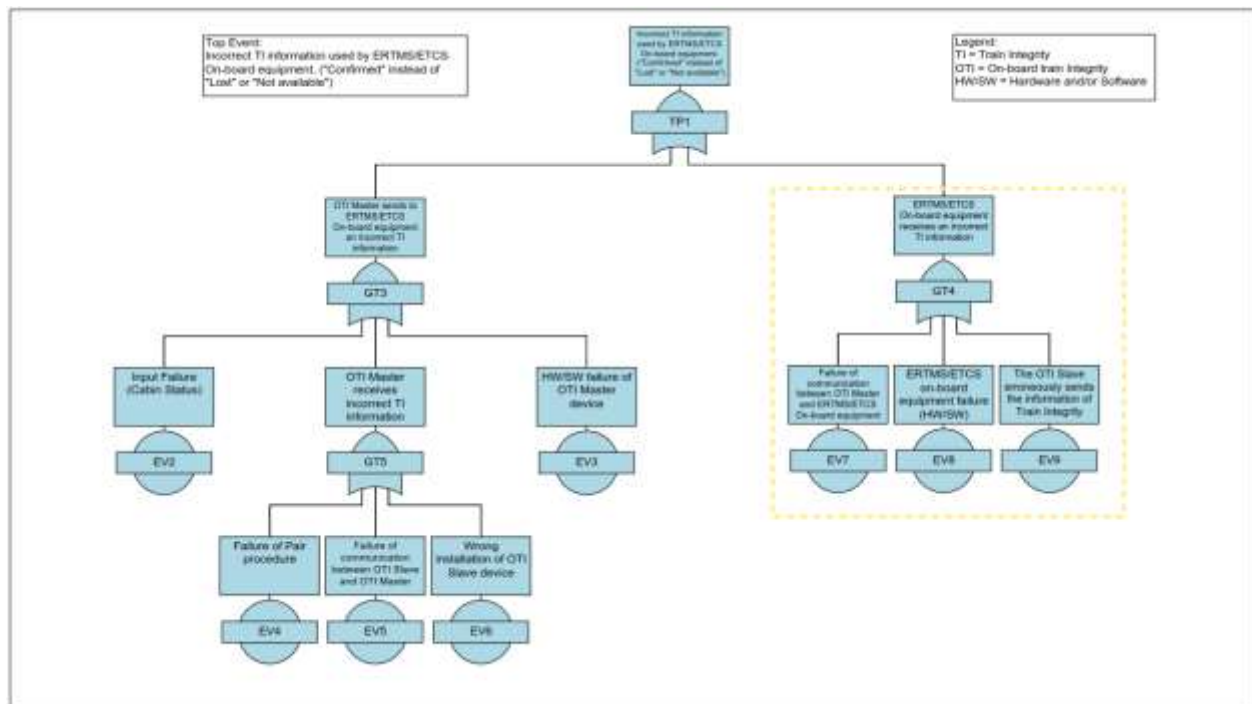
This Appendix includes the FTA for the Product Classes 1-A, 1-B, 2-A, 2-B.

Note that the branches of these FTAs related to ERTMS/ETCS equipment (reported in yellow dotted lines) are out of scope of the OTI system analysis and are included only for completeness.

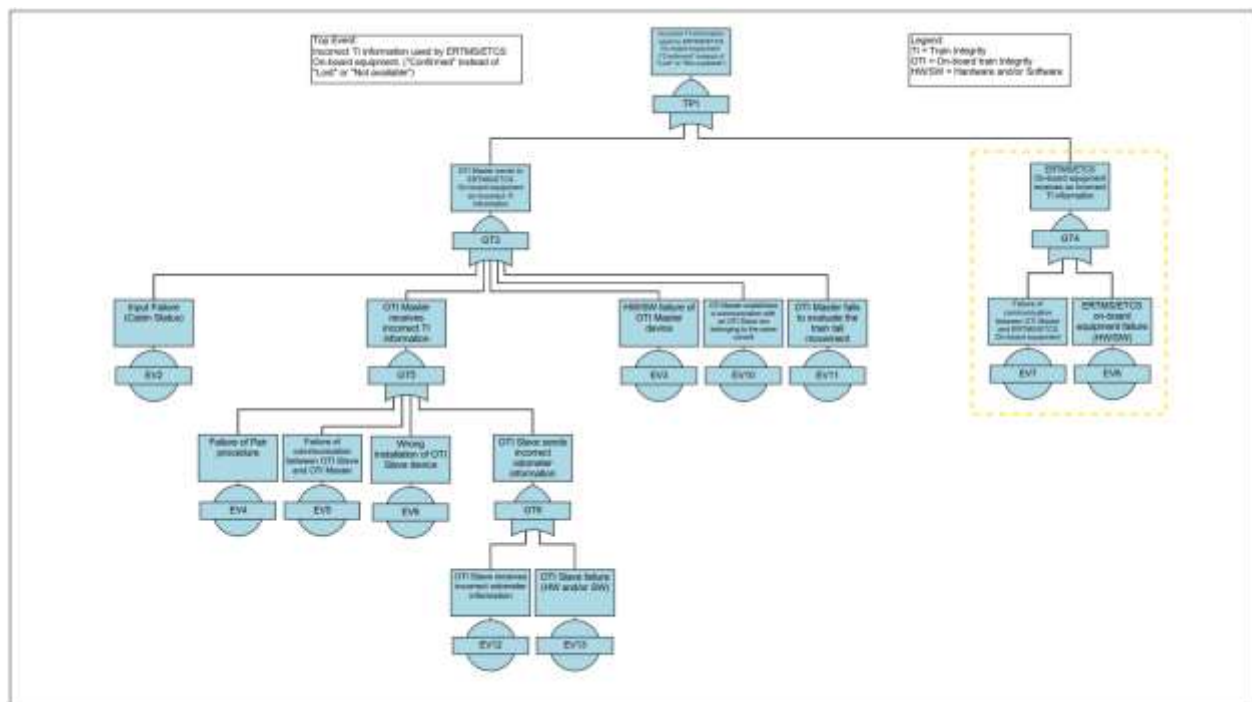
### FTA PC 1-A:



### FTA PC 1-B:



#### FTA PC 2-A (2-B):



## APPENDIX C OTI\_PHA\_PC\_1A

Comments	Risk evaluation with mitigation			Mitigations	Risk evaluation without mitigation			Safety Status	Hazard ID	Failure Effects			Possible Cause	Failure Mode	Input/Output Flow	Function	Element	
	Risk	Severity	Probability		Risk	Severity	Probability			Initial End Effect	Intermediate	Local						
Product Class 1A: ETCS AT TRAIN TAIL - Wired Communication - No intermediate OTI module																		
				OTI_MIT_001						RAM Issue	Impossibility to establish the Master-Slave communication. The OTI Master communicates to ERTMS/ETCS on-board equipment the information of the train integrity "Unknown" => availability issue	The OTI module of the head loco correctly receives the information of "Info_1" and becomes the Master	At the start of Mission, the OTI module of the tail locomotive erroneously receives the information of "Info_1" and becomes Master	Failure of the OTI Slave (software or hardware) OR; Inappropriate reception of "Info_1" information; OR; Installation error	Corruption	Input	FS1: Input acquisition to determine the OTI module role	OTI Slave

OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Corruption	Failure of the OTI Slave (software or hardware) OR; Inappropriate reception of "Info_1" information;	During the Mission, the OTI Slave erroneously receives the information of "Info_1" and becomes Master	The OTI Master of the head loco receives messages from another OTI Master	The OTI Master of the head loco considers the received messages as inconsistent and communicates to ERTMS/ETCS on-board equipment the loss of the train integrity => availability issue	RAM Issue								
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Deletion	Failure of the OTI Slave (software or hardware) OR; No reception of "Info_2" information (vehicle interface failure); OR; Installation error	The OTI module of the tail locomotive doesn't receive the information of "Info_2" and cannot complete its configuration process (Mastership assignment procedure)	The OTI Master doesn't receive messages from OTI Slave	The OTI Master communicates to ERTMS/ETCS on-board equipment the information of the train integrity "Unknown" => availability issue	RAM Issue						OTI_MIT_001 OTI_MIT_007		
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Early	N/A	N/A	N/A	N/A									





[illegible]

OTI Slave	FS2: OTI module localisation (TAIL/NON TAIL)	I/O	Deletion	Failure of the OTI Slave (software or hardware) OR; Installation error	OTI Slave doesn't know its location	The OTI Master doesn't receive data from OTI Slave	The OTI Master communicates to the ERTMS/ETCS on-board equipment the information of Train Integrity unknown => availability issue	RAM Issue										
OTI Slave	FS2: OTI module localisation (TAIL/NON TAIL)	I/O	Masquerade	See "Corruption" (case 3: Communication channel failure)														
OTI Slave	FS2: OTI module localisation (TAIL/NON TAIL)	I/O	Early Late Insertion Repetition Re-sequence	N/A	N/A	N/A	N/A											
OTI Slave	FS3: Pairing procedure Master-Slave	Input	Corruption	Failure of the OTI module Master/Slave (software or hardware) OR; On-board Communication Network failure	OTI Slave receives an incorrect pairing request	OTI Slave does not send a pairing ack	OTI Master does not complete the Inauguration procedure => Availability issue	RAM Issue										

OTI Slave	FS3: Pairing procedure Master-Slave	Input	Deletion	Failure of the OTI module Master/Slave (software or hardware) OR; On-board Communication Network failure	OTI Slave does not receive a pairing request	OTI Slave can not send a pairing ack	OTI Master does not complete the Inauguration procedure => Availability issue	RAM Issue										
OTI Slave	FS3: Pairing procedure Master-Slave	Input	Early Late Insertion Masquerade Repetition Re-sequence	N/A	N/A	N/A	N/A											
OTI Slave	FS3: Pairing procedure Master-Slave	Output	Corruption	Failure of the OTI Slave (software or hardware) OR; On-board Communication Network failure	OTI Slave sends an incorrect pairing ack or the ack message is corrupted by the network	OTI Master does not receive the correct pairing ack and considers the pairing procedure as not completed.	OTI Master does not complete the Inauguration procedure => impact on availability	RAM Issue										
OTI Slave	FS3: Pairing procedure Master-Slave	Output	Deletion	Failure of the OTI Slave (software or hardware) OR; On-board Communication Network failure	OTI Slave does not send a pairing ack or the ack message is deleted by the network	OTI Master does not receive the pairing ack and cannot consider the pairing procedure as completed.	OTI Master does not complete the Inauguration procedure => Availability issue	RAM Issue										

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

OTI Slave	FS4: Send of Vitality Message (wired comm.)	Output	Early	Failure of the Tail OTI module (software or hardware)	The OTI Slave transmits the data before it was intended	The OTI Master receives the message in incorrect time	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment Train Integrity confirmed.	No Effect												
OTI Slave	FS4: Send of Vitality Message (wired comm.)	Output	Late	Failure of the Tail OTI module (software or hardware)	The OTI Slave transmits the data after it was required	The OTI Master receives the message in incorrect time	The ERTMS/ETCS on-board equipment doesn't update the Safe Train Length until receive a new Train Integrity Information	RAM Issue						OTI_MIT_003						
OTI Slave	FS4: Send of Vitality Message (wired comm.)	Output	Insertion	Failure of the Tail OTI module (software or hardware)	The OTI Slave transmits new vitality message when not required	The OTI Master receives the vitality message when it shouldn't	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.	Safety Issue	OTI_HZ_001	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_003	Incredible	Catastrophic	Negligible				
OTI Slave	FS4: Send of Vitality Message (wired comm.)	Output	Masquerade	N/A	N/A	N/A	N/A													

OTI Slave	FS4: Send of Vitality Message (wired comm.)	Output	Repetition	Failure of the Tail OTI module (software or hardware)	The OTI Slave repeats the sending of vitality message when not required	The OTI Master continues to receive the vitality message	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.	Safety Issue	OTI_HZ_001	Probable	Catastrophic	Intolerable	OTI_MIT_003 OTI_MIT_002	Incredible	Catastrophic	Negligible
OTI Slave	FS4: Send of Vitality Message (wired comm.)	Output	Re-sequence	Failure of the Tail OTI module (software or hardware)	the OTI Slave sends the vitality message in incorrect sequence	The OTI Master continues to receive the vitality message	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.	Safety Issue	OTI_HZ_001	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_003	Incredible	Catastrophic	Negligible
OTI Slave	FS5: Acquisition and Send Odometer information (wireless comm.)	Not applicable for this Product Class	-													

OTI Slave	FS6: Diagnostic information (non vital function)	Not analysed being this function a not vital function	Deletion Early Late Insertion Masquerade Repetition Re-sequence	N/A	N/A	N/A	N/A										
Intermediate OTI module		Not applicable for this Product Class	-														
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Corruption	Failure of the OTI Master (software or hardware) OR; Inappropriate reception of "Info_2" information; OR; Installation error	The OTI module of the head locomotive erroneously does not receive the "Info_1" information and remains Slave	The both OTI modules are configured as "Slave". Impossibility to establish the Master-Slave communication	The ERTMS/ETCS on-board equipment receives the information of the train integrity "Unknown" => availability issue	RAM Issue									



OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Corruption	Failure of the OTI Master (software or hardware) OR; Inappropriate reception of "Info_2" information (e.g. OTI Master receives an inappropriate change of the cabin status);	During the mission, the OTI Master erroneously receives the information of "Info_2" and becomes Slave	The OTI module of the head locomotive becomes Slave	The OTI module of the head loco continues to communicate to ERTMS/ETCS on-board equipment the information of the train integrity confirmed => safety issue	Safety Issue	OTI_HZ_010	Probable	Catastrophic	Intolerable	OTI_MIT_006 OTI_MIT_007	Incredible	Catastrophic	Negligible
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Deletion	Failure of the OTI Master (software or hardware) OR; No reception of "Info_1" information; OR; Installation error	The OTI module of the head locomotive doesn't receive the information of "Info_1" (e.g. it doesn't receive the information of "Cab status = Cab active") and does not become Master	The both OTI modules are configured as "Slave". Impossibility to establish the Master-Slave communication	The ERTMS/ETCS on-board equipment receives the information of the train integrity "Unknown" => availability issue	RAM Issue								
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Late	See "Deletion"												

OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Masquerade	See "Corruption"															
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Early Insertion Repetition Re-sequence	N/A	N/A	N/A	N/A												
OTI Master	FM2: Pairing procedure Master-Slave	Output	Corruption	Failure of the OTI Master (software or hardware) OR; On-board Communication Network failure	The OTI Master sends a wrong Pairing Message or the message is corrupted by network	The OTI Slave receives an incorrect pairing request and does not send the pairing ack	OTI Master can not complete the Inauguration procedure => Availability issue	RAM Issue											
OTI Master	FM2: Pairing procedure Master-Slave	Output	Deletion	Failure of the OTI Master (software or hardware) OR; On-board Communication Network failure	The OTI Master doesn't send the pairing request message or the pairing request message is deleted by the network	The OTI Slave doesn't receive the Pairing request	Impossibility to complete the initialization procedure, the OTI Master communicates to ERTMS/ETCS on-board equipment the information of the train integrity "unknown" => availability issue	RAM Issue											

OTI Master	FM2: Pairing procedure Master-Slave	Output	Early Late Insertion Masquerade Repetition Re-sequence	N/A	N/A	N/A	N/A											
OTI Master	FM2: Pairing procedure Master-Slave	Input	Corruption	Failure of the OTI module Master/Slave (software or hardware) OR; On-board Communication Network failure	The OTI Master receives an incorrect ack pairing message	-	OTI Master cannot complete the Inauguration procedure => availability issue	RAM Issue										
OTI Master	FM2: Pairing procedure Master-Slave	Input	Deletion	Failure of the OTI module Master/Slave (software or hardware) OR; On-board Communication Network failure	The OTI Master does not receive the ack pairing message		OTI Master cannot complete the Inauguration procedure => availability issue	RAM Issue										
OTI Master	FM2: Pairing procedure Master-Slave	Input	Early Late Insertion Masquerade Repetition Re-sequence	N/A	N/A	N/A	N/A											

OTI Master	FM3: Reception of Vitality Message (wired comm.)	Input	Corruption	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure	OTI Master receives corrupted vitality messages	The OTI Master receives incorrect information	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.	Safety Issue	OTI_HZ_004	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_003	Incredible	Catastrophic	Negligible	
OTI Master	FM3: Reception of Vitality Message (wired comm.)	Input	Deletion	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure, OR; Installation error	During the start-up of the mission or when the mission is on- going, OTI Master doesn't receive any vitality messages	-	The OTI Master not receiving any information from the OTI Slave communicates, depending on the status of the mission, to the ERTMS/ETCS on-board equipment: 1) the unknown status of the train integrity, or; 2) the loss of the train integrity when it isn't	RAM Issue									

OTI Master	FM3: Reception of Vitality Message (wired comm.)	Input	Early	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure	OTI Master receives the vitality messages before they were expected	-	The OTI Master continues to communicate to ERTMS/ETCS on-board equipment the information of the train integrity confirmed => no issue	No Effect										
OTI Master	FM3: Reception of Vitality Message (wired comm.)	Input	Late	Failure of the OTI modules Master/Slave (software or hardware) OR; On-board Communication Network failure	OTI Master receives the vitality messages after they were expected	-	The OTI Master communicates to ERTMS/ETCS on-board equipment the information of the train integrity confirmed with a delay. The ERTMS/ETCS on-board equipment doesn't update the Safe Train Length => availability issue	RAM Issue										
OTI Master	FM3: Reception of Vitality Message (wired comm.)	Input	Insertion	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure	OTI Master receives an additional vitality messages	The OTI Master receives the message when it shouldn't	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle	Safety Issue	OTI_HZ_004	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_003	Incredible	Catastrophic	Negligible		

OTI Master	FM3: Reception of Vitality Message (wired comm.)	Input	Masquerade	Communication Network used on-board is open, an unauthorised vitality message is sent to OTI Master	OTI Master receives the vitality messages by an unauthorised element	The OTI Master receives the message when it shouldn't	could be broken. The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.	Safety Issue	OTI_HZ_004	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_003	Incredible	Catastrophic	Negligible
OTI Master	FM3: Reception of Vitality Message (wired comm.)	Input	Repetition	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure	A new vitality message is received by OTI Master	The OTI Master continues to receive the vitality message when it shouldn't	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.	Safety Issue	OTI_HZ_004	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_003	Incredible	Catastrophic	Negligible
OTI Master	FM3: Reception of Vitality Message (wired comm.)	Input	Re-sequence	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure	OTI Master receives the vitality messages in incorrect order	The OTI Master continues to receive the vitality message when it shouldn't	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.	Safety Issue	OTI_HZ_004	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_003	Incredible	Catastrophic	Negligible

OTI Master	FM4: Reception Odometer information (wireless comm.)	Not applicable for this Product Class																	
OTI Master	FM5: Check of train tail movement (wireless comm.)	Not applicable for this Product Class																	
OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Corruption	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master doesn't send the correct train integrity information or TIU interface fails to transmit the correct value of Train Integrity or ERTMS/ETCS on-board doesn't receive the correct value of Train Integrity due to its failure	The ERTMS/ETCS on-board equipment receives an incorrect value of the train integrity information	The ERTMS/ETCS on-board equipment updates the Safe Train Length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible			

OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Deletion	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master doesn't send the train integrity information or TIU interface fails to transmit the value of Train Integrity or ERTMS/ETCS on-board doesn't receive anymore the value of Train Integrity due to its failure	The ERTMS/ETCS on-board equipment doesn't receive train integrity information	The ERTMS/ETCS on-board equipment doesn't update the Safe Train length information => availability issue	RAM Issue												
OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Early	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends train integrity information before it was intended, or ERTMS/ETCS on-board equipment receives a new train integrity information before it was intended due to TIU failure or its internal failure	The ERTMS/ETCS on-board equipment receives train integrity information before it was intended	The ERTMS/ETCS on-board equipment updates the Safe Train length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_003 OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible				



OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Late	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends train integrity information after it was required, or ERTMS/ETCS on-board equipment receives a new train integrity information after it was required due to TIU failure or its internal failure	The ERTMS/ETCS on-board equipment receives train integrity information after it was required	The ERTMS/ETCS on-board equipment updates the Safe Train length information with a delay => availability issue	RAM Issue										
OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Insertion	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends inappropriate train integrity information, or ERTMS/ETCS on-board equipment receives an inappropriate train integrity information due to TIU failure or its internal failure	The ERTMS/ETCS on-board equipment receives an inappropriate train integrity information when it shouldn't	The ERTMS/ETCS on-board equipment updates the Safe Train length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible		


		ion a not vital funct ion																	
--	--	---------------------------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

## APPENDIX D OTI\_PHA\_PC\_1A\_JOIN

Comments		Risk	Risk evaluation with mitigation		Mitigations	Risk evaluation without mitigation			Hazard ID	Safety Status	Failure Effects		Possible Cause	Failure Mode	Input/Output Flow	Function	Element							
			Severity	Probability		Risk	Severity	Probability																
Product Class 1A: Joining Scenario																								
		Negligible	Catastrophic	Incredible	OTI_MIT_002 OTI_MIT_004 OTI_MIT_005 OTI_MIT_017 OTI_MIT_019	Intolerable	Catastrophic	Probable	OTI_HZ_003	Safety Issue								The OTI Master completes the pairing procedure with wrong OTI Slave => impact on the safety	OTI Master receives during the initialisation phase a TAIL identification from two or more OTI Slave modules	OTI Master receives an incorrect information from intermediate OTI modules (TAIL instead of Non TAIL)	Failure of the Intermediate OTI module (software or hardware) OR; Installation error OR; On-board Communication Network (OCN) failure	Corruption (1)	I/O	FI1: OTI module localisation (intermediate)

Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Corruption (2)	On-board Train Integrity Monitoring System is not restarted and the OTI Slave modules do not update their position (TAIL/Non TAIL)	OTI Slave does not update its position from TAIL to "Non TAIL"	OTI Master receives the vitality messages from intermediate OTI modules	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but not the entire train is monitored => impact on the safety	Safety Issue	OTI_HZ_003	Probable	Catastrophic	Intolerable	OTI_MIT_005 OTI_MIT_022 OTI_MIT_023	Incredible	Catastrophic	Negligible
Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Deletion	Failure of the Intermediate OTI module (software or hardware) OR; Installation error OR; On-board Communication Network (OCN) failure	OTI Master does not receive information from intermediate OTI modules (or does not receive information from all intermediate OTI modules)	OTI Master receives the information only by OTI Slave TAIL	The On-board Train Integrity Monitoring System can monitor the status of the vehicle (even if the OTI Master does not know all the Intermediate OTI modules)	No Effect								
Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Early Late	See "Corruption"												
Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Masquerade	See "Corruption"												

Intermediate OTI	FI1: OTI module localisation (intermediate)	I/O	Insertion Repetition Re-sequence	N/A	N/A	N/A	N/A											
Intermediate OTI Module	FI2: Diagnostic information (non vital function)	Not analysed being this function a not vital function																
OTI Master	FM2: Pairing procedure Master-Slave	Output	Corruption	Failure of the OTI Master (software or hardware) OR; On-board Communication Network failure	The OTI Master sends a Pairing Message to an intermediate OTI module instead of the Tail OTI module or due to a network failure a Pairing Message is forwarded to an intermediate OTI slave module.	The intermediate OTI Slave module receives the pairing request and sends the pairing ack	The OTI Master completes the pairing procedure with an intermediate OTI Slave module => impact on the safety	Safety Issue	OTI_HZ_008	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_011 OTI_MIT_012 OTI_MIT_019	Incredible	Catastrophic	Negligible		
OTI Master	FM2: Pairing procedure Master-Slave	Output	Early Late Insertion Masquerade Repetition Re-sequence	N/A	N/A	N/A	N/A											

## APPENDIX E OTI\_PHA\_PC\_1B

Comments	Risk evaluation with mitigation			Mitigations	Risk evaluation without mitigation	Hazard	Safety Status	Failure Effects			Possible Cause	Failure Mode	Input/Output Flow	Function	Element
	Risk	Severity	Probability					Initial End Effect	Intermediate	Local					
Product Class 1B: ETCS NOT AT TRAIN TAIL - Wired Communication															
							RAM Issue							FS1: Input acquisition to determine the OTI module role	OTI Slave

OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Corruption	Failure of the OTI Slave (software or hardware) OR; Inappropriate reception of "Info_1" information;	During the Mission, the OTI Slave erroneously receives the information of "Info_1" and becomes Master	The OTI Master of the head loco receives messages from another OTI Master	The ERTMS/ETCS on-board equipment receives the information of the train integrity by two Master => possible impact on the safety	Safety Issue	OTI_HZ_011	Probable	Catastrophic	Intolerable	OTI_MIT_003 OTI_MIT_007 OTI_MIT_018 OTI_MIT_019	Incredible	Catastrophic	Negligible
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Deletion	Failure of the OTI Slave (software or hardware) OR; No reception of "Info_2" information (vehicle interface failure); OR; Installation error	The OTI module of the tail locomotive doesn't receive the information of "Info_2" and cannot complete its configuration process (Mastership assignment procedure)	The OTI Master doesn't receive messages from OTI Slave	The OTI Master communicates to ERTMS/ETCS on-board equipment the information of the train integrity "Unknown" => availability issue	RAM Issue					OTI_MIT_001 OTI_MIT_007			
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Early	N/A	N/A	N/A	N/A									
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Late	See "Deletion"												





OTI Slave	FS2: OTI module localisation (TAIL/NON TAIL)	I/O	Corruption	Failure of the OTI Slave (software or hardware)	OTI Slave is installed on the last waggon but it does not localize itself on the last waggon/car	OTI Master does not receive the identification message from the OTI Slave module and does not activate a pairing procedure	The OTI Master communicates to the ERTMS/ETCS on-board equipment the information of Train Integrity unknown => availability issue	RAM Issue										
OTI Slave	FS2: OTI module localisation (TAIL/NON TAIL)	I/O	Corruption	On-board Communication Network failure	OTI Slave is not installed on the last waggon and it localizes itself correctly but the OTI Master receives an incorrect message	OTI Master receives a wrong identification message from the OTI Slave module and it activates a pairing procedure	The OTI Master communicates to the ERTMS/ETCS on-board equipment the information of Train Integrity confirmed but the Train Integrity system is not monitoring the entire train => potential impact on the safety	Safety Issue	OTI_HZ_003	Probable	Catastrophic	Intolerable	OTI_MIT_002	Incredible	Catastrophic	Negligible		
OTI Slave	FS2: OTI module localisation (TAIL/NON TAIL)	I/O	Deletion	Failure of the OTI Slave (software or hardware) OR; Installation error	OTI Slave doesn't know or cannot determine its location	The OTI Master doesn't receive data from OTI Slave	The OTI Master communicates to the ERTMS/ETCS on-board equipment the information of Train Integrity unknown => availability issue	RAM Issue										

OTI Slave	FS2: OTI module localisation (TAIL/NON TAIL)	I/O	Masquerade	See "Corruption" (case 3: Communication channel failure)														
OTI Slave	FS2: OTI module localisation (TAIL/NON TAIL)	I/O	Early Late Insertion Repetition Re-sequence	N/A	N/A	N/A	N/A											
OTI Slave	FS3: Pairing procedure Master-Slave	Input	Corruption	Failure of the OTI module Master/Slave (software or hardware) OR; On-board Communication Network failure	OTI Slave receives an incorrect pairing request	OTI Slave does not send a pairing ack	OTI Master does not complete the Inauguration procedure => Availability issue	RAM Issue										
OTI Slave	FS3: Pairing procedure Master-Slave	Input	Deletion	Failure of the OTI module Master/Slave (software or hardware) OR; On-board Communication Network failure	OTI Slave does not receive a pairing request	OTI Slave cannot send a pairing ack	OTI Master does not t complete the Inauguration procedure => Availability issue	RAM Issue										

OTI Slave	FS3: Pairing procedure Master-Slave	Input	Early Late Insertion Masquerade Repetition Re-sequence	N/A	N/A	N/A	N/A													
OTI Slave	FS3: Pairing procedure Master-Slave	Output	Corruption	Failure of the OTI Slave (software or hardware) OR; On-board Communication Network failure	OTI Slave sends an incorrect pairing ack or the ack message is corrupted by the network	OTI Master does not receive the correct pairing ack and considers the pairing procedure as not completed.	OTI Master does not complete the Inauguration procedure => impact on availability	RAM Issue												
OTI Slave	FS3: Pairing procedure Master-Slave	Output	Deletion	Failure of the OTI Slave (software or hardware) OR; On-board Communication Network failure	OTI Slave does not send a pairing ack or the ack message is deleted by the network	OTI Master does not receive the pairing ack and cannot consider the pairing procedure as completed.	OTI Master does not complete the Inauguration procedure => Availability issue	RAM Issue												
OTI Slave	FS3: Pairing procedure Master-Slave	Output	Early Late Insertion Masquerade Repetition Re-sequence	N/A	N/A	N/A	N/A													
OTI Slave	FS4: Send of Vitality Message (wired comm.)	Output	Corruption	Failure of the OTI Slave (software or hardware);	Due to OTI Slave failure, an incorrect vitality message is	The OTI Master continues to receive the vitality message	The OTI Master continues to communicate to the ERTMS/ETCS on-board	Safety Issue	OTI_HZ_001	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_003	Incredible	Catastrophic	Negligible				

					sent to OTI Master		equipment the information of "Train Integrity confirmed" but the vehicle could be broken.													
OTI Slave	FS4: Send of Vitality Message (wired comm.)	Output	Deletion	Failure of the OTI Slave (software or hardware)	No information is sent by OTI Slave to OTI Master during the start-up of the mission or when the mission is on-going	The OTI Master doesn't receive any data	The OTI Master not receiving any information from the OTI Slave communicates to the ERTMS/ETCS on-board equipment: 1) the unknown status of the train integrity, or; 2) the lost of the train integrity when it isn't	RAM Issue												
OTI Slave	FS4: Send of Vitality Message (wired comm.)	Output	Early	Failure of the Tail OTI module (software or hardware)	The OTI Slave transmits the data before it was intended	The OTI Master receives the message in incorrect time	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment Train Integrity confirmed.	No Effect												
OTI Slave	FS4: Send of Vitality Message (wired comm.)	Output	Late	Failure of the Tail OTI module (software or hardware)	The OTI Slave transmits the data after it was required	The OTI Master receives the message in incorrect time	The OTI Master communicates to the ERTMS/ETCS on-board equipment	RAM Issue							OTI_MIT_003					

[illegible]

[illegible]





OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Deletion	Failure of the OTI Master (software or hardware) OR; Inappropriate reception of "Info_2" information; OR; Installation error	The OTI module of the head locomotive doesn't receive the information of "Info_1" (e.g. it doesn't receive the information of "Cab status = Cab active") and does not become Master	The both OTI modules are configured as "Slave". Impossibility to establish the Master-Slave communication	The ERTMS/ETCS on-board equipment receives the information of the train integrity "Unknown" => availability issue	RAM Issue										
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Late	See "Deletion"														
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Masquerade	See "Corruption"														
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Early Insertion Repetition Re-sequence	N/A	N/A	N/A	N/A											

OTI Master	FM2: Pairing procedure Master-Slave	Output	Corruption	Failure of the OTI Master (software or hardware) OR; On-board Communication Network failure	The OTI Master sends a wrong Pairing Message or the message is corrupted by network	The OTI Slave receives an incorrect pairing request and does not send the pairing ack	OTI Master can not complete the Inauguration procedure => Availability issue	RAM Issue										
OTI Master	FM2: Pairing procedure Master-Slave	Output	Deletion	Failure of the OTI Master (software or hardware) OR; On-board Communication Network failure	The OTI Master doesn't send the pairing request message or the pairing request message is deleted by the network	The OTI Slave doesn't receive the Pairing request	Impossibility to complete the initialization procedure, the OTI Master communicates to ERTMS/ETCS on-board equipment the information of the train integrity "unknown" => availability issue	RAM Issue										
OTI Master	FM2: Pairing procedure Master-Slave	Output	Early Late Insertion Masquerade Repetition Re-sequence	N/A	N/A	N/A	N/A											

OTI Master	FM2: Pairing procedure Master-Slave	Input	Corruption	Failure of the OTI module Master/Slave (software or hardware) OR; On-board Communication Network failure	The OTI Master receives an incorrect ack pairing message	-	OTI Master cannot complete the Inauguration procedure => availability issue	RAM Issue											
OTI Master	FM2: Pairing procedure Master-Slave	Input	Deletion	Failure of the OTI module Master/Slave (software or hardware) OR; On-board Communication Network failure	The OTI Master does not receive the ack pairing message		OTI Master cannot complete the Inauguration procedure => availability issue	RAM Issue											
OTI Master	FM2: Pairing procedure Master-Slave	Input	Early Late Insertion Masquerade Repetition Re-sequence	N/A	N/A	N/A	N/A												
OTI Master	FM3: Reception of Vitality Message (wired comm.)	Input	Corruption	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure	OTI Master receives corrupted vitality messages	The OTI Master receives incorrect information	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.	Safety Issue	OTI_HZ_004	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_003	Incredible	Catastrophic	Negligible			

OTI Master	FM3: Reception of Vitality Message (wired comm.)	Input	Deletion	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure, OR; Installation error	During the start-up of the mission or when the mission is on- going, OTI Master doesn't receive any vitality messages	-	The OTI Master not receiving any information from the OTI Slave communicates, depending on the status of the mission, to the ERTMS/ETCS on-board equipment: 1) the unknown status of the train integrity, or; 2) the lost of the train integrity when it isn't	RAM Issue										
OTI Master	FM3: Reception of Vitality Message (wired comm.)	Input	Early	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure	OTI Master receives the vitality messages before they were expected	-	The OTI Master continues to communicate to ERTMS/ETCS on-board equipment the information of the train integrity confirmed => no issue	No Effect										

[illegible]

[illegible]

[illegible]

OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Deletion	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master doesn't send the train integrity information or TIU interface fails to transmit the value of Train Integrity or ERTMS/ETCS on-board doesn't receive anymore the value of Train Integrity due to its failure	The ERTMS/ETCS on-board equipment doesn't receive train integrity information	The ERTMS/ETCS on-board equipment doesn't update the Safe Train length information => availability issue	RAM Issue												
OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Early	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends train integrity information before it was intended, or ERTMS/ETCS on-board equipment receives a new train integrity information before it was intended due to TIU failure or its internal failure	The ERTMS/ETCS on-board equipment receives train integrity information before it was intended	The ERTMS/ETCS on-board equipment updates the Safe Train length information when it shouldn't	OTI_HZ_002 Safety Issue	Probable	Catastrophic	Intolerable	OTI_MIT_003 OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible					



OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Late	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends train integrity information after it was required, or ERTMS/ETCS on-board equipment receives a new train integrity information after it was required due to TIU failure or its internal failure	The ERTMS/ETCS on-board equipment receives train integrity information after it was required	The ERTMS/ETCS on-board equipment updates the Safe Train length information with a delay => availability issue	RAM Issue												
OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Insertion	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends inappropriate train integrity information, or ERTMS/ETCS on-board equipment receives an inappropriate train integrity information due to TIU failure or its internal failure	The ERTMS/ETCS on-board equipment receives an inappropriate train integrity information when it shouldn't	The ERTMS/ETCS on-board equipment updates the Safe Train length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible				

OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Insertion	Failure of the OTI Slave (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	Cab B is the active cabin, the OTI module of Cabin A (not active) is the OTI Slave. The OTI Slave connected to the ERTMS/ETCS on-board equipment sends inappropriate train integrity information (e.g. TI confirmed), or ERTMS/ETCS on-board equipment receives an inappropriate train integrity information from OTI Slave due to TIU failure or its internal failure <b>(See Note)</b>	The OTI Master of active cabin B does not receive the vitality messages from OTI Slave due to broken train and do not communicate anymore with the ERTMS/ETCS on-board equipment	The ERTMS/ETCS on-board equipment continues to receive the information of train integrity confirmed by OTI Slave	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_006 OTI_MIT_009 OTI_MIT_010 OTI_MIT_016	Incredible	Catastrophic	Negligible	See figure reported in doc file
------------	---	--------	-----------	---	---	--	--	--------------	------------	----------	--------------	-------------	--	------------	--------------	------------	---------------------------------

OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Masquerade	Communication Network between OTI Master and ERTMS/ETCS on-board equipment is open, an unauthorised train integrity information is sent to ERTMS/ETCS on-board equipment	The ERTMS/ETCS on-board equipment receives a non-authentic message that appear to be authentic	The ERTMS/ETCS on-board equipment receives an inappropriate train integrity information when it shouldn't	The ERTMS/ETCS on-board equipment updates the Safe Train length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible
OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Repetition Re-sequence	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends inappropriate train integrity information, or ERTMS/ETCS on-board equipment receives an inappropriate train integrity information due to TIU failure or its internal failure	The ERTMS/ETCS on-board equipment receives an inappropriate train integrity information when it shouldn't	The ERTMS/ETCS on-board equipment updates the Safe Train length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible
OTI Master	FM7: Acquisition and send of Diagnostic information (non vital function)	Not analysed being this function a not vital function														

## APPENDIX F OTI\_PHA\_PC\_1B\_JOIN

Comments	Risk evaluation with mitigation		Mitigations	Risk evaluation without mitigation	Hazard	Safety Status	Failure Effects			Possible Cause	Failure Mode	Input/Output Flow	Function	Element
	Risk	Severity					Probability	Initial End Effect	Intermediate					
Product Class 1B: Joining Scenario														
												</		

							confirmed" but not the entire train is monitored => impact on the safety												
Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Deletion	Failure of the Intermediate OTI module (software or hardware) OR; Installation error OR; On-board Communication Network failure	OTI Master does not receive information from intermediate OTI modules (or does not receive information from all intermediate OTI modules)	OTI Master receives the information only by OTI Slave TAIL	The On- board Train integrity Monitoring System can monitor the status of the vehicle (even if the OTI Master does not know all the Intermediate OTI modules)	No Effect											
Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Early Late	See "Corruption"															
Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Masquerade	See "Corruption"															
Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Insertion Repetition Re- sequence	N/A	N/A	N/A	N/A												



## APPENDIX G OTI\_PHA\_PC\_2A\_2B

Comments	Risk evaluation with mitigation	Mitigations	Risk evaluation without mitigation	Failure Effects			Possible Cause	Failure Mode	Input/Output Flow	Function	Element
				Initial End Effect	Intermediate	Local					
	Risk		Risk								
	Severity		Severity								
	Probability		Probability								
Product Class 2A(2B): ETCS NOT AT TRAIN TAIL - Wireless Communication - No intermediate OTI Module											
						Impossibility to establish the Master-Slave communication. The OTI Master communicates to ERTMS/ETCS on-board equipment the information of the train integrity "Unknown" => availability issue	The OTI module of the head loco correctly receives the information of "Info_1" and becomes the Master	At the start of Mission, the OTI module installed on the last waggon/car of the consist erroneously receives the information of "Info_1" and becomes Master	Failure of the OTI Slave (software or hardware)	Corruption	Input
										FS1: Input acquisition to determine the OTI module role	OTI Slave

OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Corruption	Failure of the OTI Slave (software or hardware)	During the Mission, the OTI Slave erroneously receives the information of "Info_1" and becomes Master	The OTI Master of the head loco receives messages from another OTI Master	The OTI Master of the head loco considers the received messages as inconsistent and communicates to ERTMS/ETCS on-board equipment the lost of the train integrity => availability issue	RAM Issue										
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Deletion	N/A	N/A	N/A	N/A											
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Early	N/A	N/A	N/A	N/A											
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Late	See "Deletion"														



OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Insertion	See "Corruption"															
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Masquerade	See "Corruption"															
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Repetition	N/A	N/A	N/A	N/A												
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Re-sequence	N/A	N/A	N/A	N/A												
OTI Slave	FS2: OTI module localisation (TAIL/NON TAIL)	I/O	Corruption (1)	Failure of the OTI Slave (software or hardware) OR; Installation error	OTI Slave is not installed on the last car/waggon but it localizes itself on the last waggon/car and sends the vitality message	OTI Master receives a wrong identification message from the OTI Slave module and it activates a pairing procedure	The OTI Master communicates to the ERTMS/ETCS on-board equipment the information of Train Integrity confirmed but the Train Integrity system is not	Safety Issue	OTI_HZ_003	Probable	Catastrophic	Intolerable	OTI_MIT_04 OTI_MIT_05	Improbable	Catastrophic	Tolerable			

[illegible]

[illegible]

OTI Slave	FS2: OTI module localisation (TAIL/NON TAIL)	I/O	Early Late Insertion Repetition Re-sequence	N/A	N/A	N/A	N/A											
OTI Slave	FS3: Pairing procedure Master-Slave	Input	Corruption	Failure of the OTI module Master/Slave (software or hardware) OR; On-board Communication Network failure	OTI Slave receives an incorrect pairing request	OTI Slave does not send a pairing ack	OTI Master does not complete the Inauguration procedure => Availability issue	RAM Issue										
OTI Slave	FS3: Pairing procedure Master-Slave	Input	Deletion	Failure of the OTI module Master/Slave (software or hardware) OR; On-board Communication Network failure	OTI Slave does not receive a pairing request	OTI Slave cannot send a pairing ack	OTI Master does not complete the Inauguration procedure => Availability issue	RAM Issue										
OTI Slave	FS3: Pairing procedure Master-Slave	Input	Early Late Insertion Masquera de Repetition Re-sequence	N/A	N/A	N/A	N/A											

OTI Slave	FS3: Pairing procedure Master-Slave	Output	Corruption	Failure of the OTI Slave (software or hardware) OR; On-board Communication Network failure	OTI Slave sends an incorrect pairing ack or the ack message is corrupted by the network	OTI Master does not receive the correct pairing ack and considers the pairing procedure as not completed.	OTI Master does not complete the Inauguration procedure => impact on availability	RAM Issue									
OTI Slave	FS3: Pairing procedure Master-Slave	Output	Deletion	Failure of the OTI Slave (software or hardware) OR; On-board Communication Network failure	OTI Slave does not send a pairing ack or the ack message is deleted by the network	OTI Master does not receive the pairing ack and cannot consider the pairing procedure as completed.	OTI Master does not complete the Inauguration procedure => Availability issue	RAM Issue									
OTI Slave	FS3: Pairing procedure Master-Slave	Output	Early Late Insertion Masquera de Repetition Re-sequence	N/A	N/A	N/A	N/A										
OTI Slave	FS4: Send of Vitality Message (wired comm.)	Not applicable for this Product Class															
OTI Slave	FS5: Acquisition and Send Odometer information (wireless comm.)	Input	Corruption	Failure of the OTI Slave (software or hardware) OR; ODO Sensors failure	OTI Slave receives incorrect odometer information	OTI Slave sends to OTI Master incorrect odometer information	OTI Master can consider coherent the movement of the train tail with the train head and evaluates the train integrity	Safety Issue	OTI_HZ_005	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_020	Incredible	Catastrophic	Negligible	

[illegible]

OTI Slave	FS5: Acquisition and Send Odometer informatio n (wireless comm.)	Output	Deletion	Failure of the OTI Slave (software or hardware)	During the start-up of the mission or when the mission is on-going, the OTI Slave does not transmit any odometer information	OTI Master does not receive any odometer information	The OTI Master not receiving any information from the OTI Slave communicates to the ERTMS/ETCS on-board equipment: 1) the unknown status of the train integrity (start-up of the mission), or; 2) the lost of the train integrity when it isn't (if the mission is on- going)	RAM Issue										
OTI Slave	FS5: Acquisition and Send Odometer informatio n (wireless comm.)	Output	Early	Failure of the OTI Slave (software or hardware)	The OTI Slave transmits the odometer data before it was intended	The OTI Master receives the message in incorrect time	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment Train Integrity confirmed.	No Effect										

OTI Slave	FS5: Acquisition and Send Odometer informatio n (wireless comm.)	Output	Late	Failure of the OTI Slave (software or hardware)	The OTI Slave transmits the odometer data after it was required	The OTI Master receives the message in incorrect time	The OTI Master cannot send to the ERTMS/ETCS on-board equipment the new information of Train Integrity and the ERTMS/ETCS on-board equipment cannot update the Safe Train Length until receive a new Train Integrity Information	RAM Issue										
OTI Slave	FS5: Acquisition and Send Odometer informatio n (wireless comm.)	Output	Insertion Masquera de Repetition Re- sequence	N/A	N/A	N/A	N/A											
OTI Slave	FS6: Diagnostic informati on (non vital function)	Output	Corruption	Failure of the OTI Slave (software or hardware) OR; On-Board Communicatio n Network failure	The OTI Slave transmits the diagnostic message	The OTI Master receives the diagnostic message by OTI Slave but it appears as the vitality message	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" when the vehicle could be broken => safety issue	Safety Issue	OTI_HZ_012	Probable	Catastrophic	Intolerable	OTI_MIT_0 13	Incredible	Catastrophic	Negligible		



[illegible]

OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Deletion	Failure of the OTI Master (software or hardware) OR; No reception of "Info_1" information; OR; Installation error	The OTI module of the head locomotive doesn't receive the information of "Info_1" and does not become Master	The both OTI modules are configured as "Slave". Impossibility to establish the Master-Slave communication	The ERTMS/ETCS on-board equipment receives the information of the train integrity "Unknown" => availability issue	RAM Issue										
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Late	See "Deletion"														
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Masquerade	See "Corruption"														
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Early Insertion Repetition Re-sequence	N/A	N/A	N/A	N/A											

OTI Master	FM2: Pairing procedure Master- Slave	Output	Corruption	Failure of the OTI Master (software or hardware) OR; On-board Communicatio n Network failure	The OTI Master sends a wrong Pairing Message or the message is corrupted by network	The OTI Slave receives an incorrect pairing request and does not send the pairing ack	OTI Master cannot complete the Inauguration procedure => Availability issue	RAM Issue										
OTI Master	FM2: Pairing procedure Master- Slave	Output	Deletion	Failure of the OTI Master (software or hardware) OR; On-board Communicatio n Network failure	The OTI Master doesn't send the pairing request message or the pairing request message is deleted by the network	The OTI Slave doesn't receive the Pairing request and does not send the pairing ack	Impossibility to complete the initialization procedure, the OTI Master communicates to ERTMS/ETCS on-board equipment the information of the train integrity "unknown" => availability issue	RAM Issue										
OTI Master	FM2: Pairing procedure Master- Slave	Output	Early Late Insertion Masquera de Repetition Re- sequence	N/A	N/A	N/A	N/A											

OTI Master	FM2: Pairing procedure Master- Slave	Input	Corruption	Failure of the OTI module Master/Slave (software or hardware) OR; On-board Communicatio n Network failure	The OTI Master receives an incorrect ack pairing message	-	OTI Master cannot complete the Inauguration procedure => Availability issue	RAM Issue										
OTI Master	FM2: Pairing procedure Master- Slave	Input	Deletion	Failure of the OTI module Master/Slave (software or hardware) OR; On-board Communicatio n Network failure	The OTI Master does not receive the ack pairing message		OTI Master cannot complete the Inauguration procedure => availability issue	RAM Issue										
OTI Master	FM2: Pairing procedure Master- Slave	Input	Early Late Insertion Masquera de Repetition Re- sequence	N/A	N/A	N/A	N/A											
OTI Master	FM3: Reception of Vitality Message (wired comm.)	Not applicabl e for this Product Class																

OTI Master	FM4: Reception Odometer information (wireless comm.)	Input	Corruption	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure	OTI Master receives corrupted odometer information	The OTI Master evaluates the movement of the train tail coherent with the head	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.	Safety Issue	OTI_HZ_006	Probable	Catastrophic	Intolerable	OTI_MIT_02 OTI_MIT_03	Incredible	Catastrophic	Negligible	
OTI Master	FM4: Reception Odometer information (wireless comm.)	Input	Deletion	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure, OR; Installation error OR; OTI modules not on view	During the start-up of the mission or when the mission is on-going, OTI Master doesn't receive any Odometer information	-	The OTI Master not receiving any Odometer information from the OTI Slave communicates , depending on the status of the mission, to the ERTMS/ETCS on-board equipment: 1) the unknown status of the train integrity, or; 2) the lost of the train integrity when it isn't	RAM Issue									

OTI Master	FM4: Reception Odometer informatio n (wireless comm.)	Input	Early	Failure of the OTI module Master (software or hardware) OR; On-board Communicatio n Network (OCN) failure	OTI Master receives the Odometer information before they were expected	-	The OTI Master continues to communicate to ERTMS/ETCS on-board equipment the information of the train integrity confirmed => no issue	No Effect										
OTI Master	FM4: Reception Odometer informatio n (wireless comm.)	Input	Late	Failure of the OTI module Master (software or hardware) OR; On-board Communicatio n Network (OCN) failure	OTI Master receives the Odometer information after they were expected	-	The OTI Master communicates to ERTMS/ETCS on-board equipment the information of the train integrity confirmed with a delay. The ERTMS/ETCS on-board equipment doesn't update the Safe Train Length => availability issue	RAM Issue						OTI_MIT_0 03				

Negligible													
Catastrophic													
Incredible													
OTI_MIT_0 02 OTI_MIT_0 03													
Intolerable													
Catastrophic													
Probable													
OTI_HZ_006													
Safety Issue													
The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.													
Failure of the OTI module Master (software or hardware) OR; On-board Communication Network (OCN) failure													
Insertion Repetition Re-sequence													
Input													
FM4: Reception Odometer information (wireless comm.)													
OTI Master													
Negligible													
Catastrophic													
Incredible													
OTI_MIT_0 02 OTI_MIT_0 03													
Intolerable													
Catastrophic													
Probable													
OTI_HZ_006													
Safety Issue													
The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.													
Communication Network used on-board is open, unauthorised odometer information are sent to OTI Master													
Masquerade (1)													
Input													
FM4: Reception Odometer information (wireless comm.)													
OTI Master													

		Negligible	
	Catastrophic		Catastrophic
	Incredible		Incredible
	OTI_MIT_02 OTI_MIT_019 OTI_MIT_021		OTI_MIT_014 OTI_MIT_015
	Undesirable		Intolerable
	Catastrophic		Catastrophic
	Remote		Probable
	OTI_HZ_009		OTI_HZ_007
	Safety Issue		Safety Issue
	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.		The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.
	The OTI Master evaluates the movement of the train tail coherent with the head		-
	OTI Master receives the Odometer information by an OTI Slave installed on a close consist		OTI Master evaluates the movement of consist tail coherent with the movement of consist front cabin
	OTI Master installed on one consist receives the odometer information by an OTI Slave installed on a close consist.		Failure of the OTI Master (software or hardware) OR; Incorrect information (odometer and train length) received by OTI Master via external source OR; Configuration Parameter error
	Masquera de (2)		Corruption
	Input		I/O
FM4: Reception Odometer information (wireless comm.)			FM5: Check of train tail movement (wireless comm.)
OTI Master			OTI Master



OTI Master	FM5: Check of train tail movement (wireless comm.)	I/O	Deletion	Failure of the OTI Master (software or hardware) OR; No information (odometer and train length) received by OTI Master via external source	OTI Master does not receive any more the information about the odometer and the train length	OTI Master cannot check the movement coherence between the tail and the head of the consist	The OTI Master communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity lost" => Impact on the availability	RAM Issue										
OTI Master	FM5: Check of train tail movement (wireless comm.)	I/O	Early Late Insertion Masquera de Repetition Re-sequence	N/A	N/A	N/A	N/A											
OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Corruption	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master doesn't send the correct train integrity information or TIU interface fails to transmit the correct value of Train Integrity or ERTMS/ETCS on-board doesn't receive the correct value of	The ERTMS/ETCS on-board equipment receives an incorrect value of the train integrity information	The ERTMS/ETCS on-board equipment updates the Safe Train Length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_09 OTI_MIT_10	Incredible	Catastrophic	Negligible		

					Train Integrity due to its failure														
OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Deletion	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master doesn't send the train integrity information or TIU interface fails to transmit the value of Train Integrity or ERTMS/ETCS on-board doesn't receive anymore the value of Train Integrity due to its failure	The ERTMS/ETCS on-board equipment doesn't receive train integrity information	The ERTMS/ETCS on-board equipment doesn't update the Safe Train length information => availability issue	RAM Issue											

OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Early	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends train integrity information before it was intended, or ERTMS/ETCS on-board equipment receives a new train integrity information before it was intended due to TIU failure or its internal failure	The ERTMS/ETCS on-board equipment receives train integrity information before it was intended	The ERTMS/ETCS on-board equipment updates the Safe Train length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_003 OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible	
OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Late	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends train integrity information after it was required, or ERTMS/ETCS on-board equipment receives a new train integrity information after it was required due to TIU failure or its internal failure	The ERTMS/ETCS on-board equipment receives train integrity information after it was required	The ERTMS/ETCS on-board equipment updates the Safe Train length information with a delay => availability issue	RAM Issue									



OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Repetition Re-sequence	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends inappropriate train integrity information, or ERTMS/ETCS on-board equipment receives an inappropriate train integrity information due to TIU failure or its internal failure	The ERTMS/ETCS on-board equipment receives an inappropriate train integrity information when it shouldn't	The ERTMS/ETCS on-board equipment updates the Safe Train length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_09 OTI_MIT_10	Incredible	Catastrophic	Negligible	
OTI Master	FM7: Acquisition and send of Diagnostic information (non vital function)	Not analysed being this function a not vital function															

## APPENDIX H TI\_PHA\_PC\_2A\_2B\_JOINSPLIT

Comments		Risk	Severity	Probability	Mitigations	Risk evaluation without mitigation			Hazard	Safety Status	Failure Effects			Possible Cause	Failure Mode	Input/Output Flow	Function	Element
						Probability	Severity	Risk			Initial End Effect	Intermediate	Local					
Product Class 2-A(2-B): Joining Scenario																		
		Negligible	Catastrophic	Incredible	OTI_MIT_002 OTI_MIT_004 OTI_MIT_005 OTI_MIT_017 OTI_MIT_019	Intolerable	Catastrophic	Probable	OTI_HZ_003	Safety Issue	The OTI Master completes the pairing procedure with Non TAIL OTI Slave => impact on the safety	OTI Master receives during the initialisation phase: 1) a TAIL identification from two or more OTI Slave modules; OR: 2) a TAIL identification from a Non TAIL OTI module	OTI Master receives an incorrect information from intermediate OTI modules (TAIL instead of Non TAIL)	Failure of the Intermediate OTI module (software or hardware) OR; Installation error OR; On-board Communication Network (OCN) failure	Corruption (1)	I/O	FI1: OTI module localisation (intermediate)	Intermediate OTI Module

Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Corruption (2)	The On-board Train Integrity Monitoring System is not restarted and the OTI Slave modules do not update their position (TAIL/Non TAIL)	OTI Slave does not update its position from TAIL to "Non TAIL"	OTI Master receives the odometer information from intermediate OTI modules	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but not the entire train is monitored => impact on the safety	Safety Issue	OTI_HZ_003	Probable	Catastrophic	Intolerable	OTI_MIT_005 OTI_MIT_023	Incredible	Catastrophic	Negligible
Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Deletion	Failure of the Intermediate OTI module (software or hardware) OR; Installation error OR; On-board Communication Network (OCN) failure	OTI Master does not receive information from intermediate OTI modules (or does not receive information from all intermediate OTI modules)	OTI Master receives the information only by OTI Slave TAIL	The On-board Train integrity Monitoring System can monitor the status of the vehicle (even if the OTI Master does not know all the Intermediate OTI modules)	No Effect								
Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Early Late	See "Corruption"												
Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Masquerade	See "Corruption"												

Intermediate OTI Module	FI1: OTI module localisation (intermediate)	I/O	Insertion Repetition Re-sequence	N/A	N/A	N/A	N/A											
Intermediate OTI Module	FI2: Diagnostic information (non vital function)	Not analysed being this function a not vital function																
OTI Master	FM2: Pairing procedure Master-Slave	Output	Corruption (1)	Failure of the OTI Master (software or hardware) OR; On-board Communication Network failure	The OTI Master sends a Pairing Message to an intermediate OTI module instead of the Tail OTI module or due to a network failure a Pairing Message is forwarded to an intermediate OTI slave module.	The intermediate OTI Slave module receives the pairing request and sends the pairing ack	The OTI Master completes the pairing procedure with an intermediate OTI Slave module => impact on the safety	Safety Issue	OTI_HZ_008	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_011 OTI_MIT_012 OTI_MIT_019	Incredible	Catastrophic	Negligible		



OTI Master	FM2: Pairing procedure Master-Slave	I/O	Corruption (2)	Joining operation: cars/waggons added at the end of original train consist	Following joining operation, OTI Slave is not moved at the end of train, so the OTI Master receives the Non TAIL information by OTI Slave.	The OTI Master can not realise the Master – Slave communication	The OTI Master communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity unknown" => Impact on the availability	RAM Issue						OTI_MIT_001				
OTI Master	FM2: Pairing procedure Master-Slave	Output	Early Late Insertion Masquerade Repetition Re-sequence	N/A	N/A	N/A	N/A											
OTI Master	FM5: Check of train tail movement (wireless comm.)	I/O	Corruption (2)	Joining operation: cars/waggons added into the middle or at the end of original train consist	Following joining operation, the OTI Master does not receive the new value of train length (greater than the first value before the joining operation).	The OTI Master does not evaluate the movement of consist tail coherent with the movement of consist front cabin	The OTI Master communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity lost" => Impact on the availability	RAM Issue										
Product Class 2-A(2-B): Splitting Scenario																		

OTI Master	FM2: Pairing procedure Master-Slave	I/O	Deletion	Splitting operation: cars/waggon detached from the end of consist	Following splitting operation, OTI Slave is not installed on the new last car/waggon, so the OTI Master does not receive the TAIL information by OTI Slave.	The OTI Master cannot realise the Master – Slave communication	The OTI Master communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity unknown" => Impact on the availability	RAM Issue					OTI_MIT_001					
OTI Master	FM5: Check of train tail movement (wireless comm.)	I/O	Corruption	Splitting operation: cars/waggon detached from the middle or from the end of consist	Following splitting operation, the OTI Master does not receive the new value of train length (less than the first value before the splitting operation).	The OTI Master could evaluate the movement of consist tail coherent with the movement of consist front cabin	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the consist could be broken. => Impact on safety	Safety Issue	OTI_HZ_007	Probable	Catastrophic	Intolerable	OTI_MIT_014 OTI_MIT_015 OTI_MIT_022	Incredible	Catastrophic	Negligible		

**APPENDIX I    TI\_PHA\_PC\_3A\_3B**

	Risk	
Risk evaluation with mitigation	Severity	
	Probability	
Mitigations		
	Risk	
Risk evaluation without mitigation	Severity	
	Probability	
Hazard		
Safety Status		
Failure Effects	Initial End Effect	Impossibility to establish the Master-Slave communication. The OTI Master communicates to ERTMS/E TCS on-board equipment the information of the train integrity
	Intermediate	The OTI module of the head loco correctly receives the information of "Info_1" and becomes the Master
	Local	At the start of Mission , the OTI module installed on the last waggon /car of the consist erroneously receives the information of "Info_1 " and
Possible Cause		Failure of the OTI Slave (software or hardware)
Failure Mode		Corruption
Input/Output Flow		Input
Function		FS1: Input acquisition to determine the OTI module role
Element		OTI Slave

					becomes Master		"Unknown" => availability issue									
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Corruption	Failure of the OTI Slave (software or hardware)	During the Mission, the OTI Slave erroneously receives the information of "Info_1" and becomes Master	The OTI Master of the head loco receives messages from another OTI Master	The OTI Master of the head loco considers the received messages as inconsistent and communicates to ERTMS/E TCS on-board equipment the lost of the train integrity	RAM Issue								

							=> availability issue									
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Deletion	N/A	N/A	N/A	N/A									
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Early	N/A	N/A	N/A	N/A									
OTI Slave	FS1: Input acquisition to determine the OTI module role	Input	Late	See "Deletion"												

OTI Slave	FS1: Input acquisiti on to determi ne the OTI module role	Input	Inserti on	See "Corruption"												
OTI Slave	FS1: Input acquisiti on to determi ne the OTI module role	Input	Masqu erade	See "Corruption"												
OTI Slave	FS1: Input acquisiti on to determi ne the OTI module role	Input	Repetit ion	N/A	N/A	N/A	N/A									
OTI Slave	FS1: Input acquisiti on to determi ne the OTI	Input	Re- sequen ce	N/A	N/A	N/A	N/A									

	module role															
OTI Slave	FS2: OTI module localisation (TAIL/N ON TAIL)	Not applic able for this Prod uct Class														
OTI Slave	FS3: Pairing procedu re Master- Slave	Input	Corrup tion	Failure of the OTI module Master/Slave (software or hardware) OR; On-Board Communicatio n Network failure	One or more OTIs Slave receive an incorre ct pairing request	One or more OTIs Slave do not send a paring ack	OTI Master does not complete the Inaugura tion procedur e => Availabili ty issue	RA M Iss ue								
OTI Slave	FS3: Pairing procedu re Master- Slave	Input	Deletio n	Failure of the OTI module Master/Slave (software or hardware) OR; On-Board Communicatio n Network failure	One or more OTIs Slave receive an incorre ct pairing request	One or more OTIs Slave do not send a paring ack	OTI Master does not complete the Inaugura tion procedur e =>	RA M Iss ue								

							Availabili ty issue									
OTI Slave	FS3: Pairing procedu re Master-Slave	Input	Early Late Inserti on Masqu erade Repetit ion Re- sequen ce	N/A	N/A	N/A	N/A									
OTI Slave	FS3: Pairing procedu re Master-Slave	Outp ut	Corrup tion	Failure of the OTI Master/Slave (software or hardware) OR; On-Board Communicatio n Network failure	OTI Slave sends an incorre ct pairing ack or the ack messag e is corrupt ed by	OTI Master does not receive the correct pairing ack and consid ers the pairing procedu re as not	OTI Master does not complete the Inaugura tion procedur e => impact on	RA M Iss ue								



					the network or the OTI Master does not receive a correct message	completed.	availability									
OTI Slave	FS3: Pairing procedure Master-Slave	Output	Deletion	Failure of the OTI Master/Slave (software or hardware) OR; On-Board Communication Network failure	OTI Slave does not send a pairing ack or the ack message is deleted by the network or the OTI Master does not receive any message	OTI Master does not receive the pairing ack and cannot consider the pairing procedure as completed.	OTI Master does not complete the Inauguration procedure => Availability issue	RAM Issue								

OTI Slave	FS3: Pairing procedu re Master- Slave	Outp ut	Early Late Inserti on Masqu erade Repetit ion Re- sequen ce	N/A	N/A	N/A	N/A									
OTI Slave	FS4: Send of Vitality Messag e (wired comm.)	Not applic able for this Prod uct Class														
OTI Slave	FS5: Acquisit ion and Send Odomet er informa tion (wireles s comm.)	Not applic able for this Prod uct Class														

OTI Slave	FS6: Diagnostic information (non vital function )	Output	Corruption	Failure of the OTI Slave (software or hardware) OR; On-Board Communication Network failure	The OTIs Slave transmit an erroneous diagnostic message	The OTI Master receives the diagnostic message s by OTIs Slave but they appear as the status message of "coupled "	The OTI Master continues to communicate to the ERTMS/E TCS on-board equipment the information of "Train Integrity confirmed" when the vehicle could be broken => safety issue	Safety Issue	OTI_H Z_012	Probable	Catastrophic	Intolerable	OTI_MIT_013	Incredible	Catastrophic	Negligible
OTI Slave	FS6: Diagnostic information (non vital function )	Output	Deletion Early Late Insertion Masquerade Repetition	N/A	N/A	N/A	N/A									

			ion Re- sequen ce													
OTI Slave	FS7: Identific ation of adjacen t OTIs and sending of this informa tion to OTI Master	Input	Corrup tion	Failure of the OTI Slave (software or hardware) OR; Failure of Communicatio n between the OTIs	OTI Slave receive s or determi nes incorre ct identifi ers from adjacen t OTI devices	OTI Slave sends to OTI Master incorrect OTIs identifie rs	OTI Master can not determin e the sequenc e of IDs. OTI Master sends to ERTMS/E TCS On- board the informati on of train integrity unknown => availabili ty issue	RA M Iss ue								

OTI Slave	FS7: Identification of adjacent OTIs and sending of this information to OTI Master	Input	Deletion (1)	Failure of the OTI Slave (software or hardware) OR; Failure of Communication between the OTIs OR; Installation error	OTI Slave does not receive any identifiers from adjacent OTI devices	OTI Slave can not send to OTI Master the list of adjacent OTI identifiers	OTI Master can not determine the sequence of IDs. OTI Master sends to ERTMS/E TCS On-board the information of train integrity unknown => availability issue	RA M Issue									
-----------	--	-------	--------------	--	--	---	---	------------	--	--	--	--	--	--	--	--	--

OTI Slave	FS7: Identification of adjacent OTIs and sending of this information to OTI Master	Input	Deletion (2)	Failure of the OTI Slave (software or hardware) OR; Failure of Communication between the OTIs	OTI Slave in NON TAIL position receives only one ID instead of two and localises itself in TAIL position	OTI Slave sends to OTI Master an incomplete list of adjacent OTI identifiers and position TAIL	OTI Master determines an incorrect sequence of IDs and an incorrect OTI Slave TAIL. The OTI Master communicates to the ERTMS/E TCS on-board equipment the information of Train Integrity confirmed but the Train Integrity system is not monitoring the entire	Safety Issue	OTI_HZ_014	Probable	Catastrophic	Intolerable	OTI_MIT_024 OTI_MIT_025 OTI_MIT_026	Incremental	Catastrophic	Negligible
-----------	--	-------	--------------	---	--	--	--	--------------	------------	----------	--------------	-------------	---	-------------	--------------	------------

							train (a waggon belonging to a composition is erroneously not considered as part of it) => potential impact on the safety										
OTI Slave	FS7: Identification of adjacent OTIs and sending of this information to OTI Master	Input	Masquerade (1)	2 consists are on parallel tracks. OTI devices of the two consists can communicate between them	An OTI Slave NON TAIL of consist 1 receives one identifier from an adjacent OTI device of consist 1 and another	OTI Slave sends to OTI Master the list with its wrong adjacent OTI identifiers	OTI Master can not determine the sequence of IDs. OTI Master sends to ERTMS/E TCS On-board the information of train integrity	RAM Issue									

					from consist 2		unknown => availability issue									
OTI Slave	FS7: Identification of adjacent OTIs and sending of this information to OTI Master	Input	Masquerade (2)	a waggon/car not belonging to the consist 1 is close to it	The OTI Slave in TAIL position of consist 1 receives the identifier from an adjacent OTI device	OTI Slave originally belonging to consist 1 sends to OTI Master the list with its adjacent OTI identifiers and position NON TAIL and the new waggon sends it information with position TAIL	OTI Master determine an incorrect sequence of Ids and includes in the consist a waggon not really belonging to it. When the consist starts to move the OTI Master detects train integrity	RAM Issue								



							lost and sends to ERTMS/E TCS On-board this information => availability issue									
OTI Slave	FS7: Identification of adjacent OTIs and sending of this information to OTI Master	Input	Early Late Insertion Repetition Re-sequen ce	N/A	N/A	N/A	N/A									
OTI Slave	FS7: Identification of adjacent OTIs and sending of this information to OTI Master	Output	Corruption	Failure of the OTI Slave/Master (software or hardware) OR; Failure of Communication between the OTIs	OTI Slave sends incorrect identifiers of adjacent OTI devices	OTI Master receives incorrect OTIs identifiers	OTI Master can not determine the sequence of IDs. OTI Master sends to ERTMS/E TCS On-	RAM Issue								

							board the information of train integrity unknown => availability issue									
OTI Slave	FS7: Identification of adjacent OTIs and sending of this information to OTI Master	Output	Deletion	Failure of the OTI Slave/Master (software or hardware) OR; Failure of Communication between the OTIs	OTI Slave does not send the identifiers of adjacent OTI devices or OTI Master does not receive the list of adjacent OTI devices	OTI Master does not receive the list of adjacent OTI identifiers from all OTI Slave	OTI Master can not determine the sequence of IDs. OTI Master sends to ERTMS/E TCS On-board the information of train integrity unknown => availability issue	RAM Issue								

OTI Slave	FS7: Identification of adjacent OTIs and sending of this information to OTI Master	Output	Early Late Insertion Repetition Masquerade Re-sequencing	N/A	N/A	N/A	N/A									
OTI Slave	FS8: Determination of the status: "coupled" or "separated" and sending of this information to OTI Master	Input	Corruption	Failure of the OTI Slave (software or hardware); OR; Installation/Maintenance error	OTI Slave determines its status as "coupled" instead of "separated" or "unknown"	OTI Slave sends to OTI Master an incorrect status	OTI Master receives incorrect status information by at least one OTI Slave and evaluates the train integrity as confirmed when it is not	Safety Issue	OTI_HZ_013	Probable	Catastrophic	Intolerable	OTI_MIT_027 OTI_MIT_029	Incremental	Catastrophic	Negligible

OTI Slave	FS8: Determination of the status: "couple d" or "separa ted" and sending of this informa tion to OTI Master	Input	Deletio n	Failure of the OTI Slave (software or hardware), OR; Installation/M aintenance error	OTI Slave is not able to determi ne its status, "couple d" or "separa ted"	OTI Slave sends to OTI Master an "unknow n" status	OTI Master receives unknown status informati on by at least one OTI Slave and evaluate s the train integrity as lost when it could not	RA M lss ue								
OTI Slave	FS8: Determination of the status: "couple d" or "separa ted" and sending of this informa tion to OTI Master	Input	Late	Failure of the OTI Slave (software or hardware), OR; Installation/M aintenance error	OTI Slave determi ne its "couple d" status too late	OTI Slave sends to OTI Master an "unknow n" status	OTI Master receives unknown status informati on by at least one OTI Slave and evaluate s the train integrity as lost when it could not	RA M lss ue								

OTI Slave	FS8: Determination of the status: "couple d" or "separated" and sending of this information to OTI Master	Input	Early Insertion Repetition Masquerade Re-sequen ce	N/A	N/A	N/A	N/A									
OTI Slave	FS8: Determination of the status: "couple d" or "separated" and sending of this information to OTI Master	Output	Corruption	Failure of the OTI Slave/Master (software or hardware), OR; Failure of Communication between the OTIs	OTI Slave determines its status of "separated"	OTI Master receives an incorrect status of "coupled " (instead of "separated")	OTI Master evaluates the train integrity as confirmed when it is not	Safety Issue	OTI_H Z_013	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_027	Incredible	Catastrophic	Negligible

OTI Slave	FS8: Determination of the status: "couple d" or "separated" and sending of this information to OTI Master	Output	Corruption	Failure of the OTI Slave/Master (software or hardware), OR; Failure of Communication between the OTIs	OTI Slave determines its status of "separated"	OTI Master receives an incorrect status of "coupled" (instead of "separated")	OTI Master evaluates the train integrity as confirmed when it is not	Safety Issue	OTI_HZ_013	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_028	Incredible	Catastrophic	Negligible
OTI Slave	FS8: Determination of the status: "couple d" or "separated" and sending of this information to OTI Master	Output	Deletion	Failure of the OTI Slave/Master (software or hardware), OR; Failure of Communication between the OTIs	OTI Slave determines its status of "separated"	OTI Master does not receive the status of at least one OTI Slave	OTI Master continues evaluating the train integrity as confirmed when it is not	Safety Issue	OTI_HZ_013	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_028	Incredible	Catastrophic	Negligible

OTI Slave	FS8: Determination of the status: "couple d" or "separated" and sending of this information to OTI Master	Output	Early Late Insertion Repetition Masquerade Re-sequencing		See "Corruption" and "Deletion" analysis											
Intermediate OTI module		Not applicable for this Product Class. See OTI Slave														

OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Corruption	Failure of the OTI Master (software or hardware) OR; Inappropriate reception of "Info_2" information; OR; Installation error	The OTI module of the head locomotive erroneously does not receive the "Info_1" information and remains Slave	All OTI modules are configured as "Slave". Impossibility to establish the Master-Slave communication	The ERTMS/E TCS on-board equipment receives the information of the train integrity "Unknown" => availability issue	RAM Issue								
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Corruption	Failure of the OTI Master (software or hardware) OR; Inappropriate reception of "Info_2" information (e.g. OTI Master receives an inappropriate change of the cabin status);	During the mission, the OTI Master erroneously receives the information of "Info_2" and	The OTI module of the head locomotive becomes Slave	The OTI module of the head loco continues to communicate to ERTMS/E TCS on-board equipment the informati	Safety Issue	OTI_HZ_010	Probable	Catastrophic	Intolerable	OTI_MIT_006 OTI_MIT_007	Incredible	Catastrophic	Negligible



					becomes Slave		on of the train integrity confirmed => safety issue								
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Deletion	Failure of the OTI Master (software or hardware) OR; No reception of "Info_1" information; OR; Installation error	The OTI module of the head locomotive doesn't receive the information of "Info_1" and does not become Master	All OTI modules are configured as "Slave". Impossibility to establish the Master-Slave communication	The ERTMS/ETCS on-board equipment receives the information of the train integrity "Unknown" => availability issue	RAM Issue							

OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Late	See "Deletion"												
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Masquerade	See "Corruption"												
OTI Master	FM1: Input acquisition to determine the OTI module role	Input	Early Insertion Repetition Re-sequence	N/A	N/A	N/A	N/A									

OTI Master	FM2: Pairing procedure Master-Slave	Output	Corruption	Failure of the OTI Master (software or hardware) OR; On-Board Communication Network failure	The OTI Master sends a wrong Pairing Message or the message is corrupted by network	One or more OTIs Slave receive an incorrect pairing request and does not send the pairing ack	Impossibility to complete the initialization procedure, the OTI Master communicates to ERTMS/E TCS on-board equipment the information of the train integrity "unknown" => availability issue	RAM Issue								
OTI Master	FM2: Pairing procedure Master-Slave	Output	Deletion	Failure of the OTI Master (software or hardware) OR; On-Board Communication	The OTI Master doesn't send the pairing request message	One or more OTIs Slave do not receive a pairing request	Impossibility to complete the initialization procedure, the	RAM Issue								

				n Network failure	e or the pairing request message is deleted by the network	and does not send the pairing ack	OTI Master communicates to ERTMS/E TCS on-board equipment the information of the train integrity "unknown" => availability issue									
OTI Master	FM2: Pairing procedure Master-Slave	Output	Early Late Insertion Masquerade Repetition Re-sequencing	N/A	N/A	N/A	N/A									

OTI Master	FM2: Pairing procedure Master-Slave	Input	Corruption	Failure of the OTI module Master/Slave (software or hardware) OR; On-Board Communication Network failure	The OTI Master receives one or more incorrect acknowledgement pairing messages	-	Impossibility to complete the initialization procedure, the OTI Master communicates to ERTMS/ETCS on-board equipment the information of the train integrity "unknown" => availability issue	RAM Issue								
------------	-------------------------------------	-------	------------	--	--	---	---	-----------	--	--	--	--	--	--	--	--

OTI Master	FM2: Pairing procedure Master-Slave	Input	Deletion	Failure of the OTI module Master/Slave (software or hardware) OR; On-Board Communication Network failure	The OTI Master does not receive one or more pairing acknowledgement messages		Impossibility to complete the initialization procedure, the OTI Master communicates to ERTMS/E TCS on-board equipment the information of the train integrity "unknown" => availability issue	RAM Issue								
OTI Master	FM2: Pairing procedure Master-Slave	Input	Early Late Insertion Masquerade Repetition	N/A	N/A	N/A	N/A									

			Re- sequen ce													
OTI Master	FM3: Recepti on of Vitality Messag e (wired comm.)	Not applic able for this Prod uct Class														
OTI Master	FM4: Recepti on Odomet er informa tion (wireles s comm.)	Not applic able for this Prod uct Class														
OTI Master	FM5: Check of train tail movem ent (wireles s comm.)	Not applic able for this Prod uct Class														

OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Corruption	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master doesn't send the correct train integrity information or TIU interface fails to transmit the correct value of Train Integrity or ERTMS/ETCS on-board doesn't receive the correct value of Train Integrity due	The ERTMS/ETCS on-board equipment receives an incorrect value of the train integrity information	The ERTMS/ETCS on-board equipment updates the Safe Train Length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible
------------	---	--------	------------	--	---	--	---	--------------	------------	----------	--------------	-------------	----------------------------	------------	--------------	------------



					to its failure											
OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Deletion	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master doesn't send the train integrity information or TIU interface fails to transmit the value of Train Integrity	The ERTMS/ETCS on-board equipment doesn't receive train integrity information	The ERTMS/ETCS on-board equipment doesn't update the Safe Train length information => availability issue	RAM Issue								

					y or ERTMS/ ETCS on- board doesn't receive anymore the value of Train Integrity due to its failure											
OTI Master	FM6: Send of Train Integrity information to ERTMS/ ETCS on-board	Output	Early	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends train integrity information before it was intended, or ERTMS/ ETCS on-board equipment receive	The ERTMS/ ETCS on- board equipment receives train integrity information before it was intended	The ERTMS/E TCS on- board equipment updates the Safe Train length information when it shouldn't	Safety Issue	OTI_H Z_002	Probable	Catastrophic	Intolerable	OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible



					s a new train integrity information after it was required due to TIU failure or its internal failure											
OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Insertion	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends inappropriate train integrity information, or ERTMS/ETCS on-board equipment receives an inappropriate train integrity information when it shouldn't	The ERTMS/ETCS on-board equipment receives an inappropriate train integrity information when it shouldn't	The ERTMS/ETCS on-board equipment updates the Safe Train length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible

					private train integrity information due to TIU failure or its internal failure											
OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Masquerade	Communication Network between OTI Master and ERTMS/ETCS on-board equipment is open, an unauthorised train integrity information is sent to ERTMS/ETCS on-board equipment	The ERTMS/ETCS on-board equipment receives a non-authentic message that appears to be authentic	The ERTMS/ETCS on-board equipment receives an inappropriate train integrity information when it shouldn't	The ERTMS/ETCS on-board equipment updates the Safe Train length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible

OTI Master	FM6: Send of Train Integrity information to ERTMS/ETCS on-board	Output	Repetition Re-sequen- ce	Failure of the OTI Master (software or hardware) OR; TIU failure OR; ERTMS/ETCS on-board equipment failure	OTI Master sends inappropriate train integrity information, or ERTMS/ETCS on-board equipment receives an inappropriate train integrity information due to TIU failure or its internal failure	The ERTMS/ETCS on-board equipment receives an inappropriate train integrity information when it shouldn't	The ERTMS/ETCS on-board equipment updates the Safe Train length information when it shouldn't	Safety Issue	OTI_HZ_002	Probable	Catastrophic	Intolerable	OTI_MIT_009 OTI_MIT_010	Incredible	Catastrophic	Negligible
------------	---	--------	-----------------------------	--	---	---	---	--------------	------------	----------	--------------	-------------	----------------------------	------------	--------------	------------

OTI Master	FM7: Acquisition and send of Diagnostic information (non vital function )	Not analysed being this function a not vital function														
OTI Master	FM8: Determination of train composition (sequence of IDs)	Input	Corruption	Failure of the OTI Master (software or hardware)	OTI Master determines an incorrect train composition (not correct sequence IDs) and considers as OTI Slave TAIL an OTI Slave NON TAIL	The OTI Master is not monitoring the entire consist (a waggon belonging to a composition is erroneously not considered as part of it. )	The OTI Master communicates to the ERTMS/E TCS on-board equipment the information of Train Integrity confirmed but the Train Integrity system is not monitoring the	Safety Issue	OTI_HZ_014	Probable	Catastrophic	Intolerable	OTI_MIT_024	Incredible	Catastrophic	Negligible

							entire consist => potential impact on the safety									
OTI Master	FM8: Determination of train composition (sequence of IDs)	Input	Deletion	Failure of the OTI Master (software or hardware)	OTI Master doesn't determine the train composition	The OTI Master does not start to monitor the train integrity status	Availability issue (OTI Master sends to ERTMS/E TCS On-board the information of train integrity unknown)	RAM Issue								
OTI Master	FM8: Determination of train composition (sequence of IDs)	Input	Early Late Insertion Repetition Masquerade Re-	N/A	N/A	N/A	N/A									



			sequen ce														
--	--	--	--------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--

## APPENDIX J TI\_PHA\_PC\_3A\_3B\_JOINSPLIT

Element	Function	Input/Output	Failure Mode	Possible Cause	Failure Effects			Safety Status	Hazard	Risk evaluation without mitigation			Mitigations	Risk evaluation with mitigation		
					Local	Intermediate	Initial End Effect			Probability	Severity	Risk		Probability	Severity	Risk
OTI Slave	FS7: Identification of adjacent OTIs and sending of this information to OTI Master	Input	Corruption	Failure of the OTI Slave (software or hardware) OR; Failure of Communication between the OTIs	Train 1 and Train 2 are joined. The OTI Slave TAIL of train 1 changes its position in NON TAIL (new near wagg on is detected)	OTI Slave sends to OTI Master incorrect OTIs identifiers	OTI Master can not determine the sequence of IDs. OTI Master sends to ERTMS/ETCS On-board the information of train integrity unknown => availability	RAM Issue								

					but receives or determines incorrect identifiers from adjacent OTI devices		lity issue									
OTI Slave	FS7: Identification of adjacent OTIs and sending of this information to OTI Master	Input	Deletion	Failure of the OTI Slave (software or hardware) OR; Failure of Communication between the OTIs	Train 1 and Train 2 are joined. The OTI Slave TAIL of train 1 does not receive any identifiers from	OTI Slave TAIL of train 1 does not send to OTI Master the updated list of adjac	OTI Master determines an incorrect sequence of IDs and an incorrect OTI Slave TAIL. The OTI Master communicates to the	Safety Issue	OTI_HZ_014	Probable	Catastrophic	Intolerable	OTI_MIT_024 OTI_MIT_026	Incredible	Catastrophic	Negligible

[illegible]

							impact on the safety												
--	--	--	--	--	--	--	----------------------------	--	--	--	--	--	--	--	--	--	--	--	--

## APPENDIX K HAZARD LOG

This appendix includes the Hazard Log split in the following table:

- **Hazard module** (Table 10-1): includes the identified safety related hazard and the relative information about risk assessment, mitigations and status of the hazard;
- **Hazard field description** (Table 10-2): this table includes the meaning of all fields of the Hazard module;
- **Mitigation module** (Table 10-3): list of identified requirements that must be met for the listed hazards to be successfully mitigated;
- **Mitigation field description** (Table 10-4): this table includes the meaning of all fields of the Mitigation module;

**Hazard Module:** the following table includes the identified safety related hazard and the relative information about risk assessment, mitigations and status of the hazard:

Comment	Hazard State	Hazard Status	Hazard Residual	Hazard Residual	Hazard Residual	Mitigation ID	Hazard Initial Risk	Hazard Initial	Hazard Initial	Hazard Applicability	Hazard Consequence	Hazard Cause	Hazard Description	Hazard Opening/Revision	Hazard Source	Hazard Revision ID	Hazard ID
		Solved	Negligible	Catastrophic	Incredible	OTI_MIT_002 OTI_MIT_003	Intolerable	Catastrophic	Probable	1-A 1-B	The OTI Master continues to receive the vitality message when it shouldn't or receives incorrect vitality message	Failure of the OTI Slave (software or hardware);	OTI Slave sends incorrect liveliness messages.	30/04/2018	PHA	00	OTI_HZ_001

OTI_HZ_002	00	PHA	30/04/2018	The ERTMS/ETCS On-board equipment receives inappropriate Train Integrity Confirmation (incorrect or earlier information)	Failure of the OTI Master (software or hardware) OR; TIU (interface between OTI Master and ERTMS/ETCS on-board equipment) failure OR; ERTMS/ETCS on-board equipment failure; OR; OTI Slave failure (software or hardware) (configuration with 1 central ERTMS/ETCS on-board equipment); OR; Unauthorised train integrity information	The ERTMS/ETCS on-board equipment updates the Safe Train length information when it shouldn't	1-A 1-B 2-A 2-B 3-A 3-B	Probable	Catastrophic	Intolerable	OTI_MIT_003 OTI_MIT_006 OTI_MIT_009 OTI_MIT_010 OTI_MIT_016	Incredible	Catastrophic	Negligible	Solved		
------------	----	-----	------------	--	--	---	--	----------	--------------	-------------	---	------------	--------------	------------	--------	--	--

OTI_HZ_003	00	PHA	30/04/2018	OTI Slave is not installed on the last car/waggon but it localizes itself on the last waggon/car or the OTI Master receives an incorrect identification message from OTI Slave ("TAIL" instead of "Non TAIL")	Failure of the OTI Slave (software or hardware) OR; Installation error; OR; On-board Communication Network (OCN) between OTI Slave and OTI Master failure; OR; Failure of the Intermediate OTI module (software or hardware); OR; On-board Train Integrity Monitoring System is not restarted	Train Integrity monitor system does not monitor the entire length of the train	1-A 1-B 2-A 2-B	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_004 OTI_MIT_005 OTI_MIT_017 OTI_MIT_019 OTI_MIT_022 OTI_MIT_023	Incredible	Catastrophic	Negligible	Solved		
OTI_HZ_004	00	PHA	30/04/2018	The OTI Master receives inappropriate Train Integrity information (incorrect information, earlier or later, masquerade, etc.).	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure, OR; Installation error OR; Communication Network open used on-board	The OTI Master continues to communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity confirmed" but the vehicle could be broken.	1-A 1-B	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_003	Incredible	Catastrophic	Negligible	Solved		



OTI_HZ_005	00	PHA	30/04/2018	The OTI Slave sends to OTI Master incorrect odometer information	Failure of the OTI Slave (software or hardware) OR; ODO Sensors failure	OTI Slave sends to OTI Master incorrect odometer information. OTI Master can consider coherent the movement of the train tail with the train head	2-A 2-B	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_003 OTI_MIT_020	Incredible	Catastrophic	Negligible	Solved		
OTI_HZ_006	00	PHA	30/04/2018	OTI Master receives inappropriate odometer information by OTI Slave (incorrect information, inserted information, masquerade information, etc.)	Failure of the OTI Master (software or hardware) OR; On-board Communication Network (OCN) failure OR; Communication Network used on-board is open, unauthorised access	The OTI Master evaluates the movement of the train tail coherent with the head	2-A 2-B	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_003	Incredible	Catastrophic	Negligible	Solved		

OTI_HZ_007	00	PHA	30/04/2018	OTI Master receives incorrect information (odometer data and train length value) for the evaluation of the train tail movement	Failure of the OTI Master (software or hardware) OR; Incorrect information (odometer and train length) received by OTI Master via external source OR; Configuration Parameter error	The OTI Master evaluates the movement of the train tail coherent with the head	2-A 2-B	Probable	Catastrophic	Intolerable	OTI_MIT_014 OTI_MIT_015 OTI_MIT_022 OTI_MIT_023	Incredible	Catastrophic	Negligible	Solved		
OTI_HZ_008	00	PHA	30/04/2018	OTI Master pairs with NON TAIL OTI Slave module.	Failure of the OTI Master (software or hardware) OR; On-board Communication Network failure	Train Integrity Monitoring System does not monitor the entire length of the train	1-A 1-B 2-A 2-B	Probable	Catastrophic	Intolerable	OTI_MIT_002 OTI_MIT_011 OTI_MIT_012 OTI_MIT_019	Incredible	Catastrophic	Negligible	Solved		
OTI_HZ_009	00	PHA	30/04/2018	OTI Master establishes a communication with an OTI Slave not belonging to the same consist.	2 consists are on parallel tracks	OTI Master receives information by a wrong OTI Slave and can communicate an erroneous train integrity information to ERTMS/ETCS on-board equipment	2-A 2-B	Remote	Catastrophic	Undesiderable	OTI_MIT_002 OTI_MIT_019 OTI_MIT_021	Incredible	Catastrophic	Negligible	Solved		

OTI_HZ_010	00	PHA	30/04/2018	The OTI Master receives an inappropriate change of cabin status (from "active" to "not active") and becomes Slave.	Failure of the OTI Master (software or hardware) OR; Inappropriate reception of Cab Status;	The OTI module of the head loco continues to communicate to ERTMS/ETCS on-board equipment the information of the train integrity confirmed when it couldn't	1-A 1-B 2-A 2-B 3-A 3-B	Probable	Catastrophic	Intolerable	OTI_MIT_006 OTI_MIT_007	Incredible	Catastrophic	Negligible	Solved		
OTI_HZ_011	00	PHA	30/04/2018	The OTI Slave erroneously receives the information of "Cab status = Cab active" and becomes Master	Failure of the OTI Slave (software or hardware) OR; Inappropriate reception of Cab Status;	The ERTMS/ETCS on-board equipment receives the information of the train integrity by two Master	1-B	Probable	Catastrophic	Intolerable	OTI_MIT_003 OTI_MIT_007 OTI_MIT_018 OTI_MIT_019	Incredible	Catastrophic	Negligible	Solved		



OTI_HZ_014	00	PHA	02/05/2020	OTI Master considers an OTI Slave as TAIL when it is not. In this case a waggon/car that belongs to a consist it is erroneously considered as not part of it	Failure of the OTI Slave/Master (software or hardware), OR; Failure of Communication between the OTIs	The OTI Master communicates to the ERTMS/ETCS on-board equipment the information of Train Integrity confirmed but the Train Integrity system is not monitoring the entire train (a waggon belonging to a composition is erroneously not considered as part of it. )	3-A 3-B	Probable	Catastrophic	Intolerable	OTI_MIT_024 OTI_MIT_025 OTI_MIT_026	Incredible	Catastrophic	Negligible	Solved		
------------	----	-----	------------	--	--	---	------------	----------	--------------	-------------	---	------------	--------------	------------	--------	--	--

**Table 10-1: Hazard Module**

**Hazard field description:** the following table includes the meaning of all fields of the Hazard module

Field Name	Field Value	Field Description	Note
<b>Hazard ID</b>	"OTI_HZ_XXX" Where: _XXX": is a progressive number of 3 digits, starting from "001".	It is the unique identifier for the Hazard.	
<b>Hazard Revision ID</b>	XX: start from 00.	This field contains the last hazard revision number	
<b>Hazard Source</b>	Text.	Initial generic source from which the hazard was identified, e.g. PHA	
<b>Hazard Opening/Revision Date</b>	"DD/MM/YYYY" Day/Month/Year	This field contains the date in which the hazard has been opened/revised.	
<b>Hazard Description</b>	Text.	A complete exhaustive description of the hazard scenario with all the information necessary for its clear definition.	
<b>Hazard Cause</b>	Text.	All possible failure of functions/subsystems/equipment/components which could lead to the hazard (including functional unavailability, incorrect functional behaviour, incorrect operator/user action, incorrect maintenance).	
<b>Hazard Consequence</b>	Text.	It is the possible accidents to which the hazard could lead.	
<b>Hazard Applicability</b>	1-A 1-B 2-A 2-B All	Product class for which the hazard is applicable	
<b>Hazard Initial Frequency</b>	One out of possible values: "Incredible", "Improbable", "Remote", "Occasional", "Probable" or "Frequent".	This field evaluates the frequency of the hazard pre mitigation based on previous experiences, previous evaluations, expert judgment, statistical analysis and by considering the existing mitigations of legacy system (if any) and so it will be based on the data/information already available.	Field Value reports the values according to the CENELEC 50126. To be customized according to specific project requirements.

<b>Hazard Initial Severity Level</b>	One out of possible values: "Catastrophic", "Critical", "Marginal" or "Insignificant".	This field evaluates the severity of the consequences pre mitigation related to the hazard according, based on previous experiences, previous evaluations, expert judgment, statistical analysis and by considering the existing mitigations of legacy system (if any) and so it will be based on the data/information already available.	Field Value reports the values according to the CENELEC 50126. To be customised according to specific project requirements.
<b>Hazard Initial Risk Evaluation</b>	One out of possible values: "Undesirable", "Intolerable", "Tolerable" or "Negligible".	It is the combination of Severity pre mitigation and frequency pre mitigation. It establishes the level of risk generated by the hazardous event.	Field Value reports the values according to the Cenelec 50126. To be customised according to specific project requirements.
<b>Mitigation ID</b>	"OTI_MIT_XXX" Where: _XXX": is a progressive number of 3 digits, starting from "001".	ID of possible mitigations	
<b>Hazard Residual Frequency</b>	One out of possible values: "Incredible", "Improbable", "Remote", "Occasional", "Probable" or "Frequent".	This field reports the frequency post mitigation of the hazard.	Field Value reports the values according to the Cenelec 50126. To be customised according to specific project requirements.
<b>Hazard Residual Severity Level</b>	One out of possible values: "Catastrophic", "Critical", "Marginal" or "Insignificant".	This field reports the severity post mitigation of the consequences related to the hazard.	Field Value reports the values according to the Cenelec 50126. To be customised according to specific project requirements.
<b>Hazard Residual Risk Evaluation</b>	One out of possible values: "Undesirable", "Intolerable", "Tolerable" or "Negligible".	This field reports the combination of severity post mitigation and frequency post mitigation..	Field Value reports the values according to the Cenelec 50126. To be customised according to specific project requirements.

<b>Hazard Status</b>	One out of possible values: "Open", "Solved", "Covered", "Deleted" or "Closed".	<p>1) OPEN: A hazard is "open" when it is first identified. Mitigations are yet to be defined and confirmed.</p> <p>2) DELETED: When the hazard is no longer considered applicable to the project. "Deleted" state shall be justified.</p> <p>3) SOLVED: A hazard is solved when the mitigations have been identified and confirmed by the Engineering department as requirements.</p> <p>4) COVERED: A hazard shall be classified as "covered" when it is completely covered by one or more different hazards.</p> <p>5) CLOSED: A hazard is closed when all the mitigation measures have state "implemented"</p>	To be customised according to specific project requirements.
<b>Hazard State Justification</b>	Free text	It can be used to provide a justification for the state of the hazard.	
<b>Comment</b>	Free text	This field reports some comments	

**Table 10-2: Hazard field description**



**Mitigation Module:** the following table lists the identified requirements that must be met for the listed hazards to be successfully mitigated:

Mitigation ID	Mitigation Revision ID	Mitigation Description	Safety related (Y/N)	Internal/External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)	Mitigation Status	Notes
OTI_MIT_001	01	An installation procedure shall be defined for OTI modules Slave to avoid the following availability issues: 1) the OTI module receives an incorrect cabin input and configures itself as Master with the impossibility to establish the communication with the real OTI Master; 2) Following joining/splitting operations, the OTI Slave is not moved or installed on the last waggon/car, consequently, it configures itself as Non-TAIL instead of TAIL.	N	External	Railway operator	1-A 1-B 2-A 2-B 3-A 3-B		Transferred	

Mitigation ID	Mitigation Revision ID	Mitigation Description	Safety related (Y/N)	Internal/External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)	Mitigation Status	Notes
OTI_MIT_002	00	OTI module shall manage communication in compliancy to 50159:2010	Y	Internal	OTI module (Master and Slave)	1-A 1-B 2-A 2-B 3-A 3-B	REQ_7.1.4.3	Resolved	
OTI_MIT_003	00	If the OTI Master receives inconsistent messages or does not receive any message from OTI Slave or receives messages in incorrect time, then it shall communicate to the ERTMS/ETCS on-board equipment the information of "Train Integrity Lost".	Y	Internal	OTI Master	1-A 1-B 2-A 2-B	REQ_7.1.1.3.4 REQ_7.1.1.3.12	Resolved	
OTI_MIT_004	00	Evaluating defining an installation procedure with the operator in relation to composition phase before starting train mission	Y	External	Railway operator	1-A 1-B 2-A 2-B		Transferred	
OTI_MIT_005	00	The procedure of automatic OTI module localisation shall be performed in safe manner, i.e. each OTI modules shall localize itself in the correct	Y	Internal	OTI module	1-A 1-B 2-A 2-B	REQ_7.1.5.2.2 REQ_7.1.5.2.3 REQ_7.1.5.6.1	Resolved	

Mitigation ID	Mitigation Revision ID	Mitigation Description	Safety related (Y/N)	Internal/External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)	Mitigation Status	Notes
		position in the vehicle, the OTI SLAVE TAIL in the last waggon/car and the Intermediate OTI modules (No TAIL) in intermediate position.							
OTI_MIT_006	00	The OTI module configured as Slave (TAIL or Non TAIL) shall not communicate any train integrity information to the ERTMS/ETCS On-board equipment or shall communicate the information of "Train integrity status unknown".	Y	Internal	OTI Slave	1-A 1-B 3-A 3-B	REQ_7.1.5.2.5	Resolved	
OTI_MIT_007	00	The OTI modules shall acquire the cab status information via a vital input. The OTI module connected to the "active" cabin shall be configured as "Master". The OTI module connected to the "not active" cabin shall be configured as "Slave".	Y	Internal	OTI module (Master and Slave)	1-A 1-B 3-A 3-B	REQ_7.1.1.1.1 REQ_7.1.1.1.2 REQ_7.1.1.1.3 REQ_7.1.1.7.1 REQ_7.1.5.6.1	Resolved	

Mitigation ID	Mitigation Revision ID	Mitigation Description	Safety related (Y/N)	Internal/External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)	Mitigation Status	Notes
OTI_MIT_008	00	Intentionally deleted							
OTI_MIT_009	00	The OTI module shall provide to the ERTMS/ETCS on-board equipment a vital Train Integrity information	Y	Internal	OTI Master	1-A 1-B 2-A 2-B 3-A 3-B	REQ_7.1.1.3.3 REQ_7.1.1.7.1	Resolved	
OTI_MIT_010	00	The interface between the OTI module and the ERTMS/ETCS On-board equipment shall be vital.	Y	Internal/External	OTI Master // ERTMS/ETCS On-board equipment	1-A 1-B 2-A 2-B 3-A 3-B	REQ_7.1.1.7.1 REQ_7.1.5.6.1	Resolved	
OTI_MIT_011	00	The OTI Master shall not accept the Pairing ACK message if it is received by an OTI Slave module NON TAIL.	Y	Internal	OTI module (Master)	1-A 1-B 2-A 2-B	REQ_7.1.1.2.4	Resolved	
OTI_MIT_012	00	The OTI Slave module Non TAIL shall not accept the Pairing Request Message sent by OTI Master	Y	Internal	OTI module (Slave Non TAIL)	1-A 1-B 2-A 2-B	REQ_7.1.5.1.1	Resolved	
OTI_MIT_013	00	If the OTI modules manage diagnostic information, the communication	Y	Internal	OTI module (Master and Slave)	2-A 2-B 3-A 3-B	REQ_7.1.1.7.4 REQ_7.1.5.6.4	Resolved	

Mitigation ID	Mitigation Revision ID	Mitigation Description	Safety related (Y/N)	Internal/External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)	Mitigation Status	Notes
		protocol between OTI modules shall use different messages for diagnostic and train integrity information							
OTI_MIT_014	00	The information of odometer data and train length value shall be acquired by OTI Master via vital input	Y	Internal	OTI Master	2-A 2-B	REQ_7.1.1.7.1	Resolved	
OTI_MIT_015	00	The information of odometer data and train length value sent to OTI Master shall be safety related	Y	External	Odometer source for OTI Master	2-A 2-B		Transferred	
OTI_MIT_016	00	The ERTMS/ETCS on-board equipment shall be able to distinguish the source of the Train Integrity information (if Master or Slave and via a unique identifier).	Y	External	ERTMS/ETCS On-board equipment	1-B		Transferred	
OTI_MIT_017	00	If the OTI Master receives more than one message from two or more OTI Slave modules with TAIL identification, then it shall stop or repeat the Inauguration procedure. A timer shall be defined	Y	Internal	OTI Master	1-A 1-B 2-A 2-B	REQ_7.1.1.2.3	Resolved	

Mitigation ID	Mitigation Revision ID	Mitigation Description	Safety related (Y/N)	Internal/External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)	Mitigation Status	Notes
		before declaring completed the Inauguration phase. This timer shall be dimensioning based on the specific application.							
OTI_MIT_018	00	The OTI Master shall not accept information received by other OTI modules configured as Master.	Y	Internal	OTI Master	1-B	REQ_7.1.1.7.2	Resolved	
OTI_MIT_019	00	Packets exchanged between the OTI modules shall include a field that specifies the OTI identifier (OTI ID) and the OTI role (Master / Slave TAIL / Slave Non TAIL). OTI identifier shall be unique for each OTI module.	Y	Internal	OTI module (Master and Slave)	1-A 1-B 2-A 2-B	REQ_7.1.1.7.5 REQ_7.1.5.6.2	Resolved	
OTI_MIT_020	00	The Odometer information acquired by OTI Slave shall be safety related	Y	External	Odometer source	2-A 2-B		Transferred	
OTI_MIT_021	00	In case of wireless communication, the OTI Master shall know the ID of OTI Slave with which a pairing	Y	Internal	OTI Master	2-A 2-B	REQ_7.1.1.7.3	Resolved	

Mitigation ID	Mitigation Revision ID	Mitigation Description	Safety related (Y/N)	Internal/External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)	Mitigation Status	Notes
		procedure will be initiated							
OTI_MIT_022	00	If the ERTMS/ETCS on-board equipment receives new valid Train Data (e.g. when the Driver enters, modifies or revalidates the Train Data), then the ERTMS/ETCS on-board equipment shall communicate these operations to OTI Master to start the OTI Master reset procedure	Y	External	ERTMS/ETCS On-board equipment	1-A 1-B 2-A 2-B		Transferred	
OTI_MIT_023	00	Following joining/splitting operations, the driver must modify the Train Data such that it fits with the new train composition)	Y	External	Driver	1-A 1-B 2-A 2-B		Transferred	
OTI_MIT_024	00	The OTI Master shall determine the train composition (sequence of IDs) and shall check the consistency of discovered train	Y	Internal	OTI Master	3-A 3-B	REQ.7.1.7.6 REQ.7.1.7.9	Resolved	

Mitigation ID	Mitigation Revision ID	Mitigation Description	Safety related (Y/N)	Internal/External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)	Mitigation Status	Notes
		composition with the information provided by an external source							
OTI_MIT_025	00	The OTI Master shall reject a "Slave Identification Ack" message sent by an OTI Slave including the following information: 1) TAIL position, and; 2) the IDs of two adjacent OTI Slave (only one is possible)	Y	Internal	OTI Master	3-A 3-B	REQ.7.1.7.7	Resolved	
OTI_MIT_026	00	The OTI Master shall interrupt the Inauguration phase if it receives more than one "Slave Identification Ack" message including the following information: 1) TAIL position;	Y	Internal	OTI Master	3-A 3-B	REQ.7.1.7.8	Resolved	
OTI_MIT_027	00	The OTI module shall determine its status of "coupled", "separated" or "unknown" in a safe way.	Y	Internal	OTI module (Master and Slave)	3-A 3-B	REQ.7.1.7.15	Resolved	



Mitigation ID	Mitigation Revision ID	Mitigation Description	Safety related (Y/N)	Internal/External	Mitigation Assigned To	Product Class	Mitigation Implementation (reference)	Mitigation Status	Notes
OTI_MIT_028	00	The OTI Master shall consider the train integrity as lost if it does not receive the status from at least one OTI Slave into a defined time-out or receives corrupted messages.	Y	Internal	OTI Master	3-A 3-B	REQ.7.1.7.13	Resolved	
OTI_MIT_029	00	An Installation/Maintenance procedure shall be defined for OTI modules to guarantee the correct functioning in determining the distance between the waggons/cars where they are installed	Y	External	Installer / Maintainer	3-A 3-B	To be exported to Installer / Maintainer	Transferred	

**Table 10-3: Mitigation list**

**Mitigation field description:** the following table includes the meaning of all fields of the Mitigation table:

Field Name	Field Value	Field Description	Note
<b>Mitigation ID</b>	“OTI_MIT”  “XXX”: is a progressive number of three digits, starting from “001”.	This is a unique mitigation identifier.	
<b>Mitigation Revision ID</b>	XX: start from 00.	This field contains the last Mitigation revision number	
<b>Mitigation Description</b>	Text.	Define the countermeasure/s. It could be a technological or procedural mitigation.	
<b>Safety related (Y/N)</b>	Possible values are: Y (= Yes); N (= No)	In this field shall be described the type of mitigation, if it is safety related or not	
<b>Internal/External</b>	Possible values are: Internal; External;	In this field shall be described if the mitigation is internal to the Train Integrity System Monitoring or external	
<b>Mitigation Assigned To</b>	One or more out of possible values: 1) Railway operator; 2) OTI module (Master and/or Slave) 3) Odometer source; 4) ERTMS/ETCS On-board equipment	It is the name of the owner in charge to implement the mitigation (system, subsystems, third parties).	To be customised according to specific project requirements.
<b>Product Class</b>	1-A 1-B 2-A 2-B All	Product class for which the mitigation is applicable	
<b>Mitigation Implementation (reference)</b>	Text	Provide the evidence of correct Mitigation implementation. Depending on the specific project requirements: document reference (eventual chapter/page/ID), link to Requirement IDs, the specifications, Reports, Drawings, Procedures, and other items giving evidence that the mitigation has been implemented.	

<b>Mitigation Status</b>	One of the following possible values: Open; Resolved; Cancelled; Implemented; Transferred.	<p>1) OPEN: When the mitigation has been identified but not implemented yet nor linked to requirements;</p> <p>2) CANCELLED: When the implementation of a proposed mitigation is not applicable;</p> <p>3) RESOLVED: When the mitigation identified has been linked with one (or more) requirements;</p> <p>4) IMPLEMENTED: When the mitigation has been identified and implemented;</p> <p>5) TRANSFERRED: When the mitigation is deemed to be implemented by another system/subsystem, third party.</p> <p>When a mitigation is identified it is in state “Not implemented”. Then, when it links to one or more requirements it becomes “resolved”. Finally, when documentary evidences are given providing proof of the correct implementation of the mitigation, it can pass to the state “Implemented”.</p> <p>If the mitigation is deemed necessary to be implemented by another system/subsystem, third party and it has been agreed as responsible for the implementation of the identified mitigation it is marked as “Transferred” and the state will change to “Resolved” and “Implemented” only when the evidence of correct mitigation implementation is provided.</p>	To be customised according to specific project requirements.
<b>Notes</b>	Free Text	Included to provide any supplementary information.	

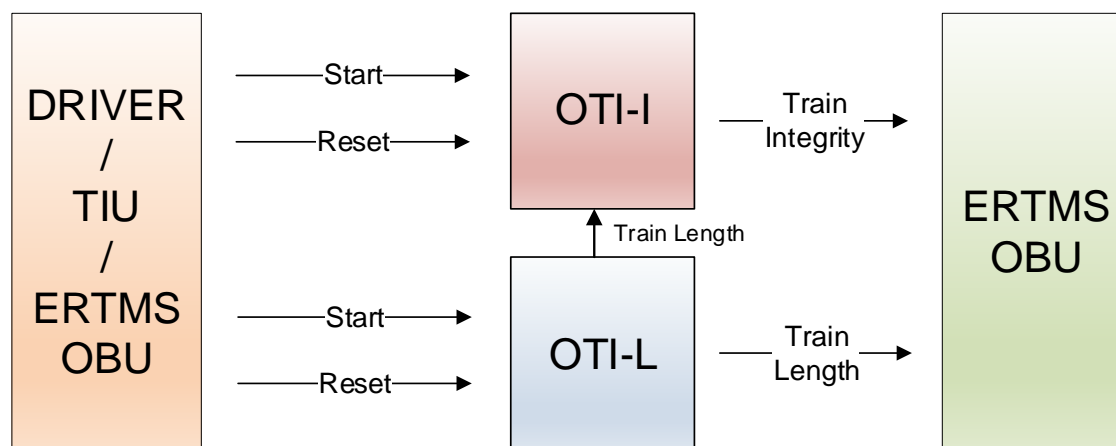
**Table 10-4: Mitigation field description**

## APPENDIX L HAZARD ANALYSIS FOR OTI-I AND OTI-L SCENARIOS

This section includes the hazard analysis of the scenarios identified in §8.5:

- S1: Start of Mission
- S2: Joining
- S3: Splitting

The following logical diagram allows to identify the interfaces and the information exchanged between them that are analysed in this section:



OTI-I: on-board functional interface providing to the ERTMS/ETCS On-board the train integrity status;

OTI-L: on-board functional interface providing to the ERTMS/ETCS On-board the train length value;

Driver/TIU/OBU: interfaces providing the START/RESET commands to the OTI-I and OTI-L.

Note 1: the OTI-L provides the train length information also to OTI-I (see Req\_2: in §8.5). The the train length value is used by OTI-I of Product Class 2 where the train integrity criterion is based on the checked of train tail movement, see REQ\_7.1.1.5.1.

Note 2: in the following analysis the term “packet 0/1” represents the packet number 0 “Position Report” and packet number 1 “Position Report based on two balise groups” as described in Subset-026-7 [1].

## L.1 Hazard Analysis for SoM scenario

See the sequence diagram reported in Figure 8-26.

Note 1: trigger for “Start” command can be provided by:

- Driver: via a dedicated console the Driver can send the “Start” command;
- Train Interface Unit (TIU): as an example: trigger is provided when the cabin is activated;
- ERTMS/ETCS On-board (OBU): as an example. Driver presses the “Train Data” button on the DMI and the OBU sends the “Start” command.

Note 2: the analysis of OTI-I is performed only considering the relationship with the train length value provided by OTI-L. The analysis of the interface between the OTI-I device and ERTMS/ETCS On-board is performed in §7.2.

Nota 3: the actions “Train Data button pressed” and “Train Data Validation” performed by Driver are not linked to the presence of OTI-L/OTI-I systems and consequently are out of scope of this analysis.

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
1	Driver / TIU / OBU	Start command	a) Early/Late	Driver/TIU/OBU error; Communication error; OTI-I and OTI-L error	Early: no impact.  Late: the OTI-L and OTI-I provide the values of TL and TI when the SoM procedure is completed and the mission is on going. Train starts moving with a possible wrong Train Length value (e.g. less than physical one). Consequences: wrong supervision of speed profile, train	HZ_001;	MIT_001; MIT_002; MIT_003; MIT_007; MIT_008; MIT_009	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					integrity not provided to ERTMS/ETCS On-board (availability issue if the system operates at Level 3) and wrong evaluation of the braking curves. Safety impact			
2	Driver / TIU / OBU	Start command	b) Deletion	Driver/TIU/OBU error; Communication error; OTI-I and OTI-L error	<p>1) Both OTI-I and OTI-L do not receive the Start command. OTI-I sends to ERTMS/ETCS On-board the information of train integrity unknown and the OTI-L sends the information of train length not available. See “Early/Late” analysis.</p> <p>2) OTI-I receives the “Start” command while the OTI-L not. The OTI-I can start to evaluate the train integrity status. The OTI-L cannot evaluate the train length and does not send to the OTI-I (see Req_2) a valid value of train length, so the OTI-I cannot communicate to the ERTMS/ETCS On-board the TI status. After Start of mission, train starts moving with a possible wrong Train Length value (less than physical one). Consequences: wrong supervision of speed profile and wrong evaluation of the braking curves with consequent safety impact. Furthermore, the train integrity status is “unknown” with</p>	<p>1) See “Early/Late” analysis.</p> <p>2) HZ_001; HZ_002; 3) HZ_002</p>	<p>2) MIT_001; MIT_002; MIT_003; MIT_007; MIT_008; MIT_009; 3) MIT_001; MIT_002; MIT_003; MIT_007; MIT_008; MIT_009;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					<p>availability impact if the system operates at ERTMS level 3.</p> <p>3) OTI-L receives the “Start” command while the OTI-I not. The OTI-L can evaluate the train length while the OTI-I is not able to evaluate the status of the train integrity, so it sends to ERTMS/ETCS On-board the information of train integrity “unknown”. Availability issue if the system operates al ETCS Level 3.</p>			
3	Driver / TIU / OBU	Start command	c) Corruption	<p>Driver/TIU/OBU error;</p> <p>Communication error;</p> <p>OTI-I and OTI-L error</p>	<p>1) Both OTI-I and OTI-L receive the “Reset” command instead of “Start”. OTI-I sends to ERTMS/ETCS On-board the information of train integrity unknown and the OTI-L sends the information of train length not available. See “Deletion” analysis, case 1).</p> <p>2) OTI-I receives the right command (“Start”) while the OTI-L receives the wrong command (“Reset”). In this case the OTI-I can evaluate the train integrity status while OTI-L is not able to evaluate the train length. Without the information of train length, the OTI-I cannot send to ERTMS/ETCS On-board the train integrity information (see Req_2) while the OTI-L sends</p>	<p>1) see “Early/late” analysis;</p> <p>2) HZ_002;</p> <p>3) see “Early/late” analysis;</p>	<p>2) MIT_002;</p> <p>MIT_007;</p> <p>MIT_008;</p> <p>MIT_009;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					<p>the information of train length not available. See case 1).</p> <p>3) OTI-L receives the right command ("Start") while the OTI-I receives the wrong command ("Reset"). OTI-L sends to ERTMS/ETCS On-board the train length while OTI-I sends train integrity unknown. Availability issue if the system operates at ETCS Level 3.</p>			
4	Driver / TIU / OBU	Start command	d) Repetition	Driver/TIU/OBU error; Communication error;	<p>1) Both OTI-I and OTI-L receive the "Start" command continuously. The repetition of the "Start" command has no effect on OTI-L FSM (see requirement in §8.7). While, OTI-I is not able to send to ERTMS/ETCS On-board a stable value of train integrity status. Availability issue if the system operates at ETCS Level 3.</p> <p>2) OTI-I receives the "Start" command continuously while OTI-L receives it one time. OTI-I is not able to send a stable value of the train integrity status to the ERTMS/ETCS On-board. Availability issue if the system operates at ETCS Level 3.</p> <p>3) OTI-L receives the "Start" command continuously while OTI-I receives it one time. The repetition of the Start</p>	<p>1) HZ_002; 2) HZ_002</p>	<p>1) and 2) MIT_001; MIT_002; MIT_007; MIT_008; MIT_009;</p>	



ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					command has no effect on OTI-L FSM (see requirement in §8.7). No impact.			
5	OTI-L	Providing TL value	a) Early/Late	OTI-L error; Communication error; ERTMS/ETCS On-board error; OTI-I error	<p>1) Early: OTI-L provides the train length value too early. No impact. (The value is available when the Driver enters Train Data).</p> <p>2) Late: the TL value is provided to ERTMS/ETCS On-board too late (while OTI-I receives it in the correct time), for example when the mission is on-going. Train starts moving with a possible wrong Train Length value (e.g. less than physical one). Consequences: wrong supervision of speed profile, wrong train integrity monitoring (wrong value of L_TRAININT used in packet 0/1) and wrong evaluation of the braking curves. Safety impact.</p> <p>3) Late: the TL value is provided to OTI-I too late (while ERTMS/ETCS On-board receives it in the correct time). Consequences: OTI-I provides to ERTMS/ETCS On-board train integrity status unknown until it receives the TL. Availability impact if the system operates at Level 3.</p>	<p>1) No hazard;</p> <p>2) HZ_001;</p> <p>3) HZ_002;</p>	<p>1) Not applicable;</p> <p>2) Req_1; MIT_003;</p> <p>3) Req_2;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
6	OTI-L	Providing TL value	b) Deletion	OTI-L error; Communication error; ERTMS/ETCS On-board error; OTI-I error	<p>1) The TL value is not provided to ERTMS/ETCS On-board (while OTI-I receives it). Train starts moving with a possible wrong Train Length value (e.g. less than physical one). Consequences: wrong supervision of speed profile, wrong train integrity monitoring (wrong value of L_TRAININT used in packet 0/1) and wrong evaluation of the braking curves. Safety impact.</p> <p>2) The TL value is not provided to OTI-I (while ERTMS/ETCS On-board receives it). Consequences: OTI-I provides to ERTMS/ETCS On-board train integrity status unknown until it receives the TL. Availability impact if the system operates at Level 3.</p> <p>3) The TL value is not provided neither to ERTMS/ETCS On-board nor to OTI-I. Train starts moving with a possible wrong Train Length value (e.g. less than physical one). Consequences: wrong supervision of speed profile and wrong evaluation of the braking curves. Safety impact. Furthermore, no train integrity monitoring is possible. Availability impact if the system operates at Level 3.</p>	<p>1) HZ_001; 2) HZ_002; 3) HZ_001; HZ_002</p>	<p>1) MIT_003; 2) Req_2; 3) MIT_003; Req_2;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
7	OTI-L	Providing TL value	c) Corruption	OTI-L error; Communication error; ERTMS/ETCS On-board error; OTI-I error	<p>1) The TL value used by ERTMS/ETCS On-board is wrong while OTI-I receives the correct value. Train starts moving with a wrong Train Length value (less or greater than physical one). Consequences are: wrong supervision of speed profile, wrong train integrity monitoring (wrong value of L_TRAININT used in packet 0/1) and wrong evaluation of the braking curves. Safety impact.</p> <p>[Note: If the value used by ERTMS/ETCS On-board is greater than physical one, this determines an availability impact for the supervision of speed profile].</p> <p>2) OTI-I receives a wrong value of train length, while ERTMS/ETCS On-board receives the correct one =&gt;</p> <p>a) if the value used is less than physical one =&gt; the OTI Master declares the train integrity as lost for Product Class 2 with availability impact if the system operates at Level 3, no impact instead for Product Class 1 (note: the train length value is used by OTI-I of Product Class 2 where the</p>	<p>1) HZ_001; 2.a) HZ_002; 2.b) see analysis in §7.2.8.3 and §7.2.8.4 and hazard OTI_HZ_007; 3) see point 1) and point 2)</p>	<p>1) MIT_004: MIT_005; 2.a) MIT_010; 2.b) for the mitigations related to hazard OTI_HZ_007 refer to Appendix K;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					<p>train integrity criterion is based on the checked of train tail movement, see REQ_7.1.1.5.1);</p> <p>b) if the value used is greater than the physical one =&gt; the OTI Master is not able to detect immediately the loss of the train integrity for Product Class 2 with safety impact, no impact instead for Product Class 1 (note: the train length value is used by OTI-I of Product Class 2 where the train integrity criterion is based on the checked of train tail movement, see REQ_7.1.1.5.1).</p> <p>3) Both ERTMS/ETCS On-board and OTI-I receive a wrong value of train length =&gt; see point 1) and 2);</p>			
8	OTI-L	Providing TL value	d) Repetition	<p>OTI-L error;</p> <p>Communication error;</p> <p>ERTMS/ETCS On-board error;</p> <p>OTI-I error</p>	<p>1) ERTMS/ETCS On-board receives continuously the train length by OTI-L (with possible minor changes in the values due to expansion/compression phenomena). Possible impacts:</p> <p>a) ERTMS/ETCS On-board could apply the Service Brake and Driver may have to validate the new train length value (see Note 8);</p> <p>b) the new train length value is used by train integrity functionality</p>	1) HZ_003;	1) MIT_005; Req_3; MIT_006	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					<p>(L_TRAININT variable used in packet 0/1) and sent to RBC;</p> <p>2) OTI-I receives continuously the train length by OTI-L (with possible minor changes in the values due to expansion/compression phenomena) =&gt; no impact</p>			
9	OTI-I	Providing TI status	a) Early/Late	OTI-I error; Communication error; ERTMS/ETCS On-board error;	<p>1) Early: the ERTMS/ETCS On-board receives the TI status by OTI-I before the train length value. If the Driver does not validate the Train Data, the OBU does not send Train Data to RBC and RBC does not send the acknowledgement message, the condition [3] of Table 8-2 is not satisfied. No impact.</p> <p>2) Late: the ERTMS/ETCS On-board receives the TI status by OTI-I too late compared with train length value sent by OTI-L. The mission starts without any information about the train integrity status. Possible impact on the availability if the system operates at Level 3.</p>	2) see analysis in §7.2.8 function "FM6: Send of Train Integrity information to ERTMS/ETCS on-board" defined in §7.2.2.3		
10	OTI-I	Providing TI status	b) Deletion	OTI-I error; Communication error;	The TI status is not provided to ERTMS/ETCS On-board. The mission starts without any information about the train integrity status. Possible	See analysis in §7.2.8 function "FM6: Send of Train		

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
				ERTMS/ETCS On-board error;	impact on the availability if the system operates at Level 3.	Integrity information to ERTMS/ETCS on-board" defined in §7.2.2.3.		
11	OTI-I	Providing TI status	c) Corruption	OTI-I error; Communication error; ERTMS/ETCS On-board error;	The TI status used by ERTMS/ETCS On-board is wrong. Train starts moving with a wrong Train Integrity status ("Train integrity confirmed" instead of "Train integrity lost" or "Train integrity status unknown")	See analysis in §7.2.8 function "FM6: Send of Train Integrity information to ERTMS/ETCS on-board" defined in §7.2.2.3		
12	OTI-I	Providing TI status	d) Repetition	OTI-I error; Communication error; ERTMS/ETCS On-board error;	See analysis in §7.2.			

## L.2 Hazard Analysis for joining scenario

See the sequence diagram reported in Figure 8-28.

Note 1: trigger for “Start” and “Reset” commands could arrive by:

- Driver: via a dedicated console the Driver can send the “Start” and “Reset” command;
- Train Interface Unit (TIU): train interface provides the “Start” and “Reset” commands;
- ERTMS On-board (OBU): as an example. Driver presses a button on the DMI and the OBU sends the “Start”/”Reset” command.

Note 2: the analysis of OTI-I is performed only considering the relationship with the train length value provide by OTI-L. The analysis of the interface between the OTI-I device and ERTMS/ETCS On-board is performed in §7.2.

Nota 3: the action “Train Length Validation” performed by Driver is not linked to the presence of OTI-L/OTI-I system and consequently is out of scope of this analysis

Note 4: As described in §7.1.5.5 (Figure 7-26), following the joining procedure, the TI status becomes “Lost”. The OTI-I Slave Tail installed on the Train 1 (see Figure 8-27), after the joining procedure, changes the status from “TAIL” to “No TAIL” and consequently the OTI Master of Train 1 does not receive valid answers and declares the integrity lost.

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
1	Driver / TIU / OBU	Reset command	a) Early/Late	Driver/TIU/OBU error; Communication error; OTI-I and OTI-L error	Early: no impact.  Late: the OTI-L and OTI-I FSMs are not reset when the Joining procedure is completed. Train starts moving with a wrong Train Length value (less than physical one). Consequences: wrong supervision of speed profile and wrong evaluation of the braking curves. Safety impact  Note: about the TI status. As described in §7.1.5.5 (Figure 7-26), following the joining procedure, the TI status becomes “Lost”. Consequently,	HZ_001; HZ_002;	MIT_001; MIT_002; MIT_003; MIT_007; MIT_008; MIT_009	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					without the reset of the OTI-I FSM the TI status is lost. Availability issue if the system operates al ETCS Level 3.			
2	Driver / TIU / OBU	Reset command	b) Deletion	Communication error; OTI-I and OTI-L error; Driver/TIU/OBU error	<p>1) Both OTI-I and OTI-L do not receive the “Reset” command. See “Early/Late” analysis;</p> <p>2) OTI-I receives the “Reset” command while the OTI-L not. The OTI-I can reconfigure its FSM and can monitor the TI status. The OTI-L sends the old Train Length to the OTI-I (see “Req_2:”) and to the ERTMS/ETCS On-board. After joining procedure, train starts moving with a wrong Train Length value (less than physical one). Consequences:</p> <p>a) wrong supervision of speed profile, wrong train integrity monitoring (wrong value of L_TRAININT used in packet 0/1) and wrong evaluation of the braking curves by the ERTMS/ETCS On-board. Safety impact.</p> <p>b) Furthermore, for Product Class 2 (Table 6-4), considering the train integrity criterion (REQ_7.1.1.5.1), the OTI-I communicates a wrong status of train integrity lost. Availability issue if the system operates al ETCS Level 3.</p>	<p>1) See “Early/Late” analysis;</p> <p>2.a) HZ_001;</p> <p>2.b) HZ_002;</p> <p>3) HZ_002;</p>	<p>1) See “Early/Late” analysis;</p> <p>2.a) and 2.b) MIT_001;</p> <p>MIT_002;</p> <p>MIT_007;</p> <p>MIT_008;</p> <p>MIT_009;</p> <p>3) MIT_001;</p> <p>MIT_002;</p> <p>MIT_007;</p> <p>MIT_008;</p> <p>MIT_009;</p>	



ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					<p>No impact instead for Product Class 1 where the train integrity criterion is based on liveness message.</p> <p>3) OTI-L receives the Reset command while the OTI-I not. The OTI-L can reconfigure its FSM and can re-evaluate the new train length at the end of joining procedure. About the TI status. As described in §7.1.5.5 (Figure 7-26), following the joining procedure, the TI status becomes "Lost". Consequently, without the reset of the OTI-I FSM the TI status is lost. Availability issue if the system operates at ETCS Level 3.</p>			
3	Driver / TIU / OBU	Reset command	c) Corruption	<p>Communication error;</p> <p>OTI-I and OTI-L error;</p> <p>Driver/TIU/OBU error</p>	<p>1) Both OTI-I and OTI-L receive the "Start" command instead of "Reset". OTI-L does not reset its FSM, while the OTI-I can do it. See "Deletion" analysis, case 2).</p> <p>2) OTI-I receives the "Reset" command while the OTI-L receives "Start" command. In this case the OTI-I resets its FSM while OTI-L not. See case 1).</p> <p>3) OTI-L receives the right command ("Reset") while the OTI-I receives wrong command ("Start"). Both, OTI-I</p>	1) See "Deletion" analysis, case 2);		

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					and OTI-L, reset their FSMs. No impact.			
4	Driver / TIU / OBU	Reset command	d) Repetition	Communication error; OTI-I and OTI-L error; Driver/TIU/OBU error	<p>1) Both OTI-I and OTI-L receive the “Reset” command continuously. OTI-I and OTI-L are not able to send to ERTMS/ETCS On-board stable values of train length and train integrity status. Availability issue.</p> <p>2) OTI-I receive the “Reset” command continuously while OTI-L receives it one time. OTI-I is not able to send a stable value of the train integrity status to the ERTMS/ETCS On-board. Availability issue if the system operates at ETCS Level 3.</p> <p>3) OTI-L receives the “Reset” command continuously while OTI-I receives it one time. OTI-L is not able to send a stable value of train length to the ERTMS/ETCS On-board and to OTI-I. Availability issue if the system operates at ETCS Level 3.</p>	<p>1) HZ_002 and HZ_003;</p> <p>2) HZ_002</p> <p>3) HZ_003</p>	<p>1) MIT_001; MIT_002; MIT_007; MIT_008; MIT_009; 2) MIT_001; MIT_002; MIT_007; MIT_008; MIT_009; 3) MIT_001; MIT_002; MIT_007; MIT_008; MIT_009;</p>	
5	Driver / TIU / OBU	Start command	a) Early/Late	Driver/TIU/OBU error; Communication error;	<p>Early: The START command is provided before joining is completed:</p> <p>a) OTI-I completes all the steps and starts to monitor the train integrity status. When the joining procedure is</p>	<p>Early/Late: HZ_001; HZ_002;</p>	<p>MIT_001; MIT_002; MIT_003; MIT_007;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
				OTI-I and OTI-L error	<p>completed, the OTI Slave TAIL becomes NO TAIL, so the train integrity status becomes "Lost". Availability issue.</p> <p>b) OTI-L starts to compute the train length and provides the TL value to ERTMS/ETCS On-board and to OTI-I. When the joining procedure is completed, the OTI-L does not restart to evaluate the new value, so the ERTMS/ETCS On-board uses a not correct value of train length (less than the physical one). Consequences: wrong supervision of speed profile and wrong evaluation of the braking curves. Safety impact.</p> <p>Late: the OTI-L and OTI-I provide the values of TL and TI when the joining procedure has been completed and the train is moving. Train is moving with a wrong Train Length value (less than physical one). Consequences: wrong supervision of speed profile and wrong evaluation of the braking curves. Safety impact.</p> <p>Furthermore, train integrity is not provided to ERTMS/ETCS On-board due to "Req_2:". Availability issue if the system operates at Level 3.</p>		MIT_008; MIT_009;	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
6	Driver / TIU / OBU	Start command	b) Deletion	Driver/TIU/OBU error; Communication error; OTI-I and OTI-L error	<p>1) Both OTI-I and OTI-L do not receive the “Start” command. OTI-I sends to ERTMS/ETCS On-board the information of train integrity unknown and the OTI-L sends the information of train length not available. See “Early/Late” analysis.</p> <p>2) OTI-I receives the “Start” command while the OTI-L not. The OTI-I can reconfigure its FSM while the OTI-L not. The OTI-L does not send to the OTI-I (see “Req_2:”) a valid value of train length, so the OTI-I cannot communicate to the ERTMS/ETCS On-board the TI status. After joining procedure, train starts moving with a wrong Train Length value (less than physical one). Consequences: wrong supervision of speed profile and wrong evaluation of the braking curves by the ERTMS/ETCS On-board with consequent safety impact. Furthermore, the train integrity status is unknown with availability impact if the system operates at ERTMS level 3.</p> <p>3) OTI-L receives the “Start” command while the OTI-I not. The OTI-L can reconfigure its FSM and can re-</p>	<p>1) See “Early/Late” analysis.</p> <p>2) HZ_001; HZ_002;</p> <p>3) HZ_002</p>	<p>2) MIT_001; MIT_002; MIT_003; MIT_007; MIT_008; MIT_009;</p> <p>3) MIT_001; MIT_002; MIT_007; MIT_008; MIT_009;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					evaluate the new train length at the end of joining procedure. About the TI status, OTI-I has received previously the “Reset” command, so it sends to ERTMS/ETCS On-board the information of train integrity “unknown”. Availability issue if the system operates at ETCS Level 3.			
7	Driver / TIU / OBU	Start command	c) Corruption	Driver/TIU/OBU error; Communication error; OTI-I and OTI-L error	<p>1) Both OTI-I and OTI-L receive the “Reset” command instead of “Start”. OTI-I sends to ERTMS/ETCS On-board the information of train integrity unknown and the OTI-L sends the information of train length not available. See “Deletion” analysis, case 1).</p> <p>2) OTI-I receives the right command (“Start”) while the OTI-L receives the wrong command (“Reset”). In this case the OTI-I can evaluate the train integrity status while OTI-L is not able to evaluate the train length. Without the information of train length, the OTI-I cannot send to ERTMS/ETCS On-board the train integrity information (see Req_2) while the OTI-L sends the information of train length not available. See case 1).</p>	<p>1) see “Deletion” analysis;</p> <p>2) See case 1);</p> <p>3) HZ_002;</p>	<p>3) MIT_001; MIT_002; MIT_007; MIT_008; MIT_009;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					3) OTI-L receives the right command ("Start") while the OTI-I receives the wrong command ("Reset"). OTI-L sends to ERTMS/ETCS On-board the train length while OTI-I sends train integrity unknown. Availability issue if the system operates at ETCS Level 3.			
8	Driver / TIU / OBU	Start command	d) Repetition	Driver/TIU/OBU error; Communication error; OTI-I and OTI-L error	<p>1) Both OTI-I and OTI-L receive the "Start" command continuously. The repetition of the Start command has no effect on OTI-L FSM (see requirement in §8.7.1). While, OTI-I is not able to send to ERTMS/ETCS On-board a stable value of train integrity status. Availability issue if the system operates at ETCS Level 3.</p> <p>2) OTI-I receives the "Start" command continuously while OTI-L receives it one time. OTI-I is not able to send a stable value of the train integrity status to the ERTMS/ETCS On-board. Availability issue if the system operates at ETCS Level 3.</p> <p>3) OTI-L receives the "Start" command continuously while OTI-I receives it one time. The repetition of the "Start" command has no effect on OTI-L FSM (see requirement in §8.7.1). No impact.</p>	1) HZ_002; 2) HZ_002	1) and 2) MIT_001; MIT_002; MIT_007; MIT_008; MIT_009;	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
9	OTI-L	Providing TL value	a) Early/Late	OTI-L error; Communication error; ERTMS/ETCS On-board error; OTI-I error	<p>1) Early: OTI-L provides the train length value too early. No impact.</p> <p>2) Late: the Train Length value is provided to ERTMS/ETCS On-board too late (while OTI-I receives it in the correct time), for example when the mission is on-going. Train starts moving with a wrong Train Length value (less than physical one). Consequences: wrong supervision of speed profile, wrong train integrity monitoring (wrong value of L_TRAININT used in packet 0/1) and wrong evaluation of the braking curves. Safety impact.</p> <p>3) Late: the Train Length (TL) value is provided to OTI-I too late (while ERTMS/ETCS On-board receives it in the correct time). Consequences: OTI-I provides to ERTMS/ETCS On-board train integrity status unknown until it receives the TL. Availability impact if the system operates at Level 3.</p>	<p>1) No hazard;</p> <p>2) HZ_001;</p> <p>3) HZ_002;</p>	<p>1) Not applicable;</p> <p>2) MIT_003;</p> <p>3) Req_2:</p>	
10	OTI-L	Providing TL value	b) Deletion	OTI-L error; Communication error;	<p>1) The TL value is not provided to ERTMS/ETCS On-board (while OTI-I receives it). Train starts moving with a wrong Train Length value (less than</p>	<p>1) HZ_001;</p> <p>2) HZ_002;</p>	<p>1) MIT_003;</p> <p>2) Req_2;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
				ERTMS/ETCS On-board error; OTI-I error	<p>physical one). Consequences: wrong supervision of speed profile, wrong train integrity monitoring (wrong value of L_TRAININT used in packet 0/1) and wrong evaluation of the braking curves. Safety impact.</p> <p>2) The TL value is not provided to OTI-I (while ERTMS/ETCS On-board receives it). Consequences: OTI-I provides to ERTMS/ETCS On-board train integrity status unknown until it receives the TL. Availability impact if the system operates at Level 3.</p> <p>3) The TL value is not provided neither to ERTMS/ETCS On-board nor to OTI-I. Train starts moving with a wrong Train Length value (less than physical one). Consequences: wrong supervision of speed profile and wrong evaluation of the braking curves. Safety impact. Furthermore, no train integrity monitoring is possible (see "Req_2:"). Availability impact if the system operates at Level 3.</p>	3) HZ_001; HZ_002	3) MIT_003; Req_2;	
11	OTI-L	Providing TL value	c) Corruption	OTI-L error; Communication error;	1) The TL value used by ERTMS/ETCS On-board is wrong while OTI-I receives the correct value. Train starts moving with a wrong Train Length value (less or greater than the	1) HZ_001; 2.a) HZ_002; 2.b) see analysis in	1) MIT_004: MIT_005; 2.a) MIT_010;	



ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
				ERTMS/ETCS On-board error; OTI-I error	<p>physical one). Consequences are: wrong supervision of speed profile, wrong train integrity monitoring (wrong value of L_TRAININT used in packet 0/1) and wrong evaluation of the braking curves. Safety impact</p> <p>[Note: If the value used by ERTMS/ETCS On-board is greater than physical one, this determines an availability impact for the supervision of speed profile].</p> <p>2) OTI-I receives a wrong value of train length, while ERTMS/ETCS On-board receives the correct one =&gt;</p> <p>a) if the value used is less than physical one =&gt; the OTI Master declares the train integrity as lost for Product Class 2 with availability impact if the system operates at Level 3, no impact instead for Product Class 1 (note: the train length value is used by OTI-I of Product Class 2 where the train integrity criterion is based on the checked of train tail movement, see REQ_7.1.1.5.1);</p> <p>b) if the value used is greater than the physical one =&gt; the OTI Master is not able to detect immediately the loss of the train integrity for Product Class 2</p>	§7.2.8.3 and §7.2.8.4 and hazard OTI_HZ_007; 3) see point 1) and point 2)	2.b) for the mitigations related to hazard OTI_HZ_007 refer to Appendix K;	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					<p>with safety impact, no impact instead for Product Class 1 (note: the train length value is used by OTI-I of Product Class 2 where the train integrity criterion is based on the checked of train tail movement, see REQ_7.1.1.5.1).</p> <p>3) Both ERTMS/ETCS On-board and OTI-I receive a wrong value of train length =&gt; see point 1) and 2);</p>			
12	OTI-L	Providing TL value	d) Repetition	<p>OTI-L error;</p> <p>Communication error;</p> <p>ERTMS/ETCS On-board error;</p> <p>OTI-I error</p>	<p>1) ERTMS/ETCS On-board receives continuously the train length by OTI-L (with possible minor changes in the values due to expansion/compression phenomena). Possible impacts:</p> <p>a) ERTMS/ETCS On-board could apply the Service Brake and Driver may have to validate the new train length value (see Note 8);</p> <p>b) the new train length value is used by train integrity functionality (L_TRAININT variable used in packet 0/1) and sent to the RBC;</p> <p>2) OTI-I receives continuously the train length by OTI-L (with possible minor changes in the values due to expansion/compression phenomena) =&gt; no impact.</p>	1) HZ_003;	1) MIT_005; Req_3;	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
13	OTI-I	Providing TI status	a) Early/Late	OTI-I error; Communication error; ERTMS/ETCS On-board error;	<p>1) Early: the ERTMS/ETCS On-board receives the TI status by OTI-I before the train length value. If the Driver does not validate the Train Data, the OBU does not send Train Data to RBC and RBC does not send the acknowledgement message, the condition [3] of Table 8-2 is not satisfied. No impact.</p> <p>2) Late: the ERTMS/ETCS On-board receives the TI status by OTI-I too late compared with train length value sent by OTI-L. The mission starts without any information about the train integrity status. Possible impact on the availability if the system operates at Level 3.</p>	2) see analysis in §7.2.8 function “FM6: Send of Train Integrity information to ERTMS/ETCS on-board” defined in §7.2.2.3;		
14	OTI-I	Providing TI status	b) Deletion	OTI-I error; Communication error; ERTMS/ETCS On-board error;	The TI status is not provided to ERTMS/ETCS On-board. The mission starts without any information about the train integrity status. Possible impact on the availability if the system operates at Level 3.	See analysis in §7.2.8 function “FM6: Send of Train Integrity information to ERTMS/ETCS on-board” defined in §7.2.2.3.		

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
15	OTI-I	Providing TI status	c) Corruption	OTI-I error; Communication error; ERTMS/ETCS On-board error;	The TI status used by ERTMS/ETCS On-board is wrong. Train starts moving with a wrong Train Integrity status ("Train integrity confirmed" instead of "Train integrity lost" or "Train integrity status unknown")	See analysis in §7.2.8 function "FM6: Send of Train Integrity information to ERTMS/ETCS on-board" defined in §7.2.2.3.		
16	OTI-I	Providing TI status	d) Repetition	OTI-I error; Communication error; ERTMS/ETCS On-board error;	See analysis in §7.2.8 function "FM6: Send of Train Integrity information to ERTMS/ETCS on-board" defined in §7.2.2.3.			

### L.3 Hazard Analysis for splitting scenario

See the sequence diagram reported in Figure 8-30.

Note 1: trigger for "Start" and "Reset" commands could arrive by:

- Driver: via a dedicated console the Driver can send the "Start" and "Reset" command;
- Train Interface Unit (TIU): train interface provides the "Start" and "Reset" commands;
- ERTMS/ETCS On-board (OBU): as an example. Driver presses a button on the DMI and the OBU sends the "Start"/"Reset" command.

Note 2: the analysis of OTI-I is performed only considering the relationship with the train length value provide by OTI-L. The analysis of the interface between the OTI-I device and ERTMS/ETCS On-board is performed in §7.2.

Nota 3: the action “Train Length Validation” performed by Driver is not linked to the presence of OTI-L/OTI-I system and consequently is out of scope of this analysis.

Note 4: As described in in §7.1.5.5 (Figure 7-27), following the splitting procedure, the TI status becomes “Lost”.

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
1	Driver / TIU / OBU	Reset command	a) Early/Late	Driver/TIU/OBU error; Communication error; OTI-I and OTI-L error	Early: no impact.  Late: the OTI-L and OTI-I FSMs are not reset when the splitting procedure is completed. Train starts moving with a wrong Train Length value (greater than physical one). Consequences: wrong supervision of speed profile and wrong evaluation of the braking curves. Safety issue.  [Note: If the value used by ERTMS/ETCS On-board is greater than physical one, this determines an availability impact for the supervision of speed profile].  Note: about the TI status. As described in §7.1.5.5 (Figure 7-27), following the splitting procedure, the TI status becomes	HZ_001;  HZ_002;	MIT_001;  MIT_002;  MIT_003;  MIT_007;  MIT_008;  MIT_009	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					"Lost". Consequently, without the reset of the OTI-I FSM the TI status is lost. Availability issue if the system operates at ETCS Level 3.			
2	Driver / TIU / OBU	Reset command	b) Deletion	Communication error;  OTI-I and OTI-L error;  Driver/TIU/OBU error	1) Both OTI-I and OTI-L do not receive the "Reset" command. See "Early/Late" analysis;  2) OTI-I receives the "Reset" command while the OTI-L not. The OTI-I can reconfigure its FSM and can monitor the TI status. The OTI-L sends the old Train Length to the OTI-I (see "Req_2:") and to the ERTMS/ETCS On-board. After splitting procedure, train starts moving with a wrong Train Length value (greater than physical one). Consequences:  a) wrong supervision of speed profile, wrong train integrity monitoring (wrong value of L_TRAININT used in packet 0/1) and wrong evaluation of the braking curves by the ERTMS/ETCS On-board. Safety issue.	1) See "Early/Late" analysis;  2.a) HZ_001;  2.b) see analysis in §7.2.8.3 and §7.2.8.4 and hazard OTI_HZ_007;  3) HZ_002;	1) See "Early/Late" analysis;  2.a) MIT_001;  MIT_002;  MIT_003;  MIT_007;  MIT_008;  MIT_009;  2.b) for the mitigations related to hazard OTI_HZ_007 refer to Appendix K;  3) ) MIT_001;  MIT_002;  MIT_007;	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					<p>b) Furthermore, the OTI Master is not able to detect immediately the lost of the train integrity for Product Class 2 with safety impact, no impact instead for Product Class 1 (note: the train length value is used by OTI-I of Product Class 2 where the train integrity criterion is based on the checked of train tail movement, see REQ_7.1.1.5.1).</p> <p>3) OTI-L receives the “Reset” command while the OTI-I not. The OTI-L can reconfigure its FSM and can re-evaluate the new train length at the end of splitting procedure. About the TI status. As described in §7.1.5.5 (Figure 7-27), following the splitting procedure, the TI status becomes “Lost”. Consequently, without the reset of the OTI-I FSM the TI status is lost. Availability issue if the system operates al ETCS Level 3.</p>		MIT_008; MIT_009;	
3	Driver / TIU / OBU	Reset command	c) Corruption	Communication error;	1) Both OTI-I and OTI-L receive the “Start” command instead of “Reset”. OTI-L does not reset its			

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
				OTI-I and OTI-L error;  Driver/TIU/OBU error	FSM, while the OTI-I can do it. See "Deletion" analysis, case 2).  2) OTI-I receives the "Reset" command while the OTI-L receives "Start" command. In this case the OTI-I resets its FSM while OTI-L not. See case 1).  3) OTI-L receives the right command ("Reset") while the OTI-I receives wrong command ("Start"). Both, OTI-I and OTI-L, reset their FSMs. No impact.			
4	Driver / TIU / OBU	Reset command	d) Repetition	Communication error;  OTI-I and OTI-L error;  Driver/TIU/OBU error	1) Both OTI-I and OTI-L receive the "Reset" command continuously. OTI-I and OTI-L are not able to send to ERTMS/ETCS On-board stable values of train length and train integrity status. Availability issue.  2) OTI-I receives the "Reset" command continuously while OTI-L receives it one time. OTI-I is not able to send a stable value of the train integrity status to the ERTMS/ETCS On-board. Availability issue if the system operates at ETCS Level 3.	1) HZ_002 and HZ_003;  2) HZ_002  3) HZ_003	1) MIT_001; MIT_002; MIT_007; MIT_008; MIT_009; 2) MIT_001; MIT_002; MIT_007; MIT_008; MIT_009; 3) MIT_001; MIT_002;	



ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					3) OTI-L receives the "Reset" command continuously while OTI-I receives it one time. OTI-L is not able to send a stable value of train length to the ERTMS/ETCS On-board and to OTI-I. Availability issue if the system operates at ETCS Level 3.		MIT_007; MIT_008; MIT_009;	
5	Driver / TIU / OBU	Start command	a) Early/Late	Driver/TIU/OBU error; Communication error; OTI-I and OTI-L error	Early: The START command is provided before splitting is completed:  a) OTI-I completes all the steps and starts to monitor the train integrity status. When the splitting procedure is completed:  - for the Product Class 1 and 3, the train integrity status becomes "Lost" (the communication between the OTI Master and OTI Slave Tail is interrupted). Availability issue;  - for Product Class 2 the risk is that the OTI Master continues to communicate with an OTI Slave TAIL not belonging to the train anymore. The OTI Master detects the train integrity lost when the	Early:  a) HZ_002 for the Product Class 1 and 3 and see analysis in §7.2.8.3 and §7.2.8.4 for Product Class 2 (OTI_HZ_007) ;  b) HZ_001  Late:  a) HZ_001;  b) HZ_002;	Early:  a) for HZ_002: MIT_001; MIT_002; MIT_007; MIT_008; MIT_009;  For the mitigations related to hazard OTI_HZ_007 refer to Appendix K;  b) MIT_001; MIT_002;	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					<p>train starts moving. Safety impact.</p> <p>b) OTI-L starts to compute the train length and provides the TL value to ERTMS/ETCS On-board and to OTI-I. When the splitting procedure is completed, the OTI-L does not restart to evaluate the new value, so the ERTMS/ETCS On-board uses a not correct value of train length (greater than the physical one). Consequences: wrong supervision of speed profile, wrong train integrity monitoring (wrong value of L_TRAININT used in packet 0/1) and wrong evaluation of the braking curves. Safety impact.</p> <p>Late: the OTI-L and OTI-I provide the values of TL and TI when the splitting procedure has been completed and the train is moving. Train is moving with a wrong Train Length value (greater than physical one). Consequences:</p> <p>a) wrong supervision of speed profile and wrong evaluation of</p>		<p>MIT_007; MIT_008; MIT_009; Late: MIT_001; MIT_002; MIT_003; MIT_007; MIT_008; MIT_009;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					<p>the braking curves by ERTMS/ETCS On-board. Safety impact.</p> <p>b) Furthermore, train integrity is not provided to ERTMS/ETCS On-board due to "Req_2:". Availability issue if the system operates at Level 3.</p>			
6	Driver / TIU / OBU	Start command	b) Deletion	<p>Driver/TIU/OBU error;</p> <p>Communication error;</p> <p>OTI-I and OTI-L error</p>	<p>1) Both OTI-I and OTI-L do not receive the "Start" command. OTI-I sends to ERTMS/ETCS On-board the information of train integrity unknown and the OTI-L sends the information of train length not available. See "Early/Late" analysis.</p> <p>2) OTI-I receives the "Start" command while the OTI-L not. The OTI-I can reconfigure its FSM while the OTI-L not. The OTI-L does not send to the OTI-I (see "Req_2:") a valid value of train length, so the OTI-I cannot communicate to the OBU the TI status. After splitting procedure, train starts moving with a wrong Train Length value (greater than physical one). Consequences:</p>	<p>1) See "Early/Late" analysis.</p> <p>2.a) HZ_001;</p> <p>2.b) HZ_002;</p> <p>3) HZ_002</p>	<p>2.a) and 2.b)</p> <p>MIT_001;</p> <p>MIT_002;</p> <p>MIT_003;</p> <p>MIT_007;</p> <p>MIT_008;</p> <p>MIT_009;</p> <p>3) MIT_001;</p> <p>MIT_002;</p> <p>MIT_007;</p> <p>MIT_008;</p> <p>MIT_009;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					<p>a) wrong supervision of speed profile and wrong evaluation of the braking curves by the ERTMS/ETCS On-board with consequent safety impact.</p> <p>b) Furthermore, the train integrity status is unknown with availability impact if the system operates at ERTMS level 3.</p> <p>3) OTI-L receives the “Start” command while the OTI-I not. The OTI-L can reconfigure its FSM and can re-evaluate the new train length at the end of splitting procedure. About the TI status, OTI-I has received previously the “Reset” command, so it sends to ERTMS/ETCS On-board the information of train integrity “unknown”. Availability issue if the system operates al ETCS Level 3.</p>			
7	Driver / TIU / OBU	Start command	c) Corruption	Driver/TIU/OBU error; Communication error; OTI-I and OTI-L error	1) Both OTI-I and OTI-L receive the “Reset” command instead of “Start”. OTI-I sends to ERTMS/ETCS On-board the information of train integrity unknown and the OTI-L sends the information of train length not	1) see “Deletion” analysis; 2) See case 1); 3) HZ_002;	3) MIT_001; MIT_002; MIT_007; MIT_008; MIT_009;	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					<p>available. See “Deletion” analysis, case 1).</p> <p>2) OTI-I receives the right command (“Start”) while the OTI-L receives the wrong command (“Reset”). In this case the OTI-I can evaluate the train integrity status while OTI-L is not able to evaluate the train length. Without the information of train length, the OTI-I cannot send to ERTMS/ETCS On-board the train integrity information (see “Req_2:”) while the OTI-L sends the information of train length not available. See case 1).</p> <p>3) OTI-L receives the right command (“Start”) while the OTI-I receives the wrong command (“Reset”). OTI-L sends to ERTMS/ETCS On-board the train length while OTI-I sends train integrity unknown. Availability issue if the system operates at ETCS Level 3.</p>			
8	Driver / TIU / OBU	Start command	d) Repetition	Driver/TIU/OBU error;	1) Both OTI-I and OTI-L receive the “Start” command continuously. The repetition of the “Start” command has no effect on	1) HZ_002; 2) HZ_002	1) and 2) MIT_001; MIT_002;	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
				Communication error;  OTI-I and OTI-L error	<p>OTI-L FSM (see requirement in §8.7.1). While, OTI-I is not able to send to ERTMS/ETCS On-board a stable value of train integrity status. Availability issue if the system operates at ETCS Level 3.</p> <p>2) OTI-I receive the “Start” command continuously while OTI-L receives it one time. OTI-I is not able to send a stable value of the train integrity status to the ERTMS/ETCS On-board. Availability issue if the system operates at ETCS Level 3.</p> <p>3) OTI-L receive the “Start” command continuously while OTI-I receives it one time. The repetition of the “Start” command has no effect on OTI-L FSM (see requirement in §8.7.1). No impact.</p>		MIT_007;  MIT_008;  MIT_009;	
9	OTI-L	Providing TL value	a) Early/Late	OTI-L error;  Communication error;  ERTMS/ETCS On-board error;	<p>1) Early: OTI-L provides the train length value too early. No impact.</p> <p>2) Late: the Train Length value is provided too late to ERTMS/ETCS On-board (while OTI-I receives it in the correct</p>	<p>1) No hazard;</p> <p>2) HZ_001;</p> <p>3) HZ_002;</p>	<p>1) Not applicable;</p> <p>2) MIT_001;</p> <p>MIT_002;</p> <p>MIT_003;</p> <p>MIT_007;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
				OTI-I error	<p>time), for example when the mission is on-going. Train starts moving with a wrong Train Length value (greater than physical one). Consequences: wrong supervision of speed profile, wrong train integrity monitoring (wrong value of L_TRAININT used in packet 0/1) and wrong evaluation of the braking curves. Safety impact.</p> <p>[Note: In the value used by ERTMS/ETCS On-board is greater than physical one, this determines an availability impact for the supervision of speed profile]</p> <p>3) Late: the Train Length (TL) value is provided to OTI-I too late (while ERTMS/ETCS On-board receives it in the correct time). Consequences: OTI-I provides to ERTMS/ETCS On-board train integrity status unknown until it receives the TL. Availability impact if the system operates at Level 3.</p>		MIT_008; MIT_009; 3) Req_2	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
10	OTI-L	Providing TL value	b) Deletion	OTI-L error; Communication error; ERTMS/ETCS On-board error; OTI-I error	<p>1) The TL value is not provided to ERTMS/ETCS On-board (while OTI-I receives it). Train starts moving with a wrong Train Length value (greater than physical one). Consequences: wrong supervision of speed profile, wrong train integrity monitoring (wrong value of L_TRAININT used in packet 0/1) and wrong evaluation of the braking curves. Safety impact.</p> <p>2) The TL value is not provided to OTI-I (while ERTMS/ETCS On-board receives it). Consequences: OTI-I provides to ERTMS/ETCS On-board train integrity status unknown until it receives the TL. Availability impact if the system operates at Level 3.</p> <p>3) The TL value is not provided neither to ERTMS/ETCS On-board nor to OTI-I. Train starts moving with a wrong Train Length value (greater than physical one). Consequences: wrong supervision of speed profile and wrong evaluation of the braking</p>	<p>1) HZ_001; 2) HZ_002; 3) HZ_001; HZ_002</p>	<p>1) MIT_001; MIT_002; MIT_003; MIT_007; MIT_008; MIT_009; 2) Req_2; 3) MIT_001; MIT_002; MIT_003; MIT_007; MIT_008; MIT_009; Req_2</p>	



ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					curves. Safety impact. Furthermore, no train integrity monitoring is possible. Availability impact if the system operates at Level 3.			
11	OTI-L	Providing TL value	c) Corruption	OTI-L error; Communication error; ERTMS/ETCS On-board error; OTI-I error	<p>1) The TL value used by ERTMS/ETCS On-board is wrong while OTI-I receives the correct value. Train starts moving with a wrong Train Length value (less or greater than the physical one). Consequences are: wrong supervision of speed profile, wrong train integrity monitoring (wrong value of L_TRAININT used in packet 0/1) and wrong evaluation of the braking curves. Safety impact</p> <p>[Note: If the value used by ERTMS/ETCS On-board is greater than physical one, this determines an availability impact for the supervision of speed profile].</p> <p>2) OTI-I receives a wrong value of train length, while ERTMS/ETCS On-board receives</p>	<p>1) HZ_001; 2.a) HZ_002; 2.b) see analysis in §7.2.8.3 and §7.2.8.4 and hazard OTI_HZ_007; 3) see point 1) and point 2)</p>	<p>1) MIT_004; MIT_005; 2.a) MIT_010; 2.b) for the mitigations related to hazard OTI_HZ_007 refer to Appendix K;</p>	

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
					<p>the correct one =&gt; a) if the value used is less than physical one =&gt; the OTI Master declares the train integrity as lost for Product Class 2 with availability impact if the system operates at Level 3, no impact instead for Product Class 1 (note: the train length value is used by OTI-I of Product Class 2 where the train integrity criterion is based on the checked of train tail movement, see REQ_7.1.1.5.1);</p> <p>b) if the value used is greater than the physical one =&gt; the OTI Master is not able to detect immediately the lost of the train integrity for Product Class 2 with safety impact, no impact instead for Product Class 1 (note: the train length value is used by OTI-I of Product Class 2 where the train integrity criterion is based on the checked of train tail movement, see REQ_7.1.1.5.1).</p> <p>3) Both ERTMS/ETCS On-board and OTI-I receive a wrong value of train length =&gt; see point 1) and 2);</p>			

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
12	OTI-L	Providing TL value	d) Repetition	OTI-L error; Communication error; ERTMS/ETCS On-board error; OTI-I error	1) ERTMS/ETCS On-board receives continuously the train length by OTI-L (with possible minor changes in the values due to expansion/compression phenomena). Possible impacts: a) ERTMS/ETCS On-board could apply the Service Brake and Driver may have to validate the new train length value (see Note 8); b) the new train length value is used by train integrity functionality (L_TRAININT variable used in packet 0/1) and sent to the RBC; 2) OTI-I receives continuously the train length by OTI-L (with possible minor changes in the values due to expansion/compression phenomena) => no impact	1) HZ_003;	1) MIT_005; Req_3;	
13	OTI-I	Providing TI status	a) Early/Late	OTI-I error; Communication error;	1) Early: the ERTMS/ETCS On-board receives the TI status by OTI-I before the train length value. If the Driver does not validate the Train Data, the ERTMS/ETCS On-board does	2) see analysis in §7.2.8 function "FM6: Send of Train Integrity information to		

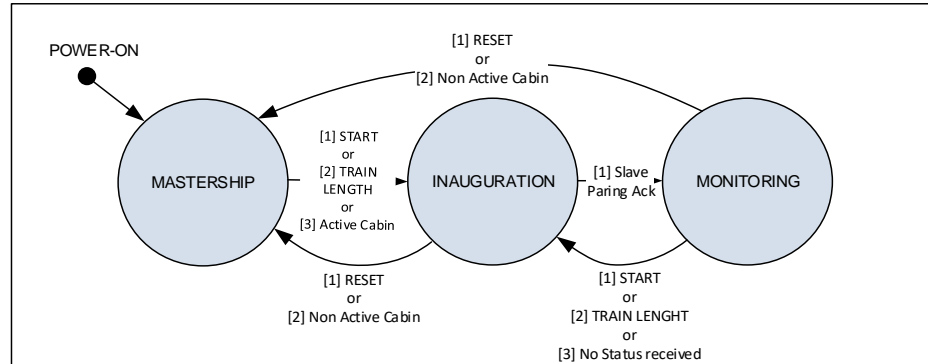
ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
				ERTMS/ETCS On-board error;	<p>not send Train Data to RBC and RBC does not send the acknowledgement message, the condition [3] of Table 8-1 is not satisfied. No impact.</p> <p>2) Late: the ERTMS/ETCS On-board receives the TI status by OTI-I too late compared with train length value sent by OTI-L. The mission starts without any information about the train integrity status. Possible impact on the availability if the system operates at Level 3.</p>	ERTMS/ETCS on-board" defined in §7.2.2.3;		
14	OTI-I	Providing TI status	b) Deletion	OTI-I error; Communication error; ERTMS/ETCS On-board error;	The TI status is not provided to ERTMS/ETCS On-board. The mission starts without any information about the train integrity status. Possible impact on the availability if the system operates at Level 3.	2) see analysis in §7.2.8 function "FM6: Send of Train Integrity information to ERTMS/ETCS on-board" defined in §7.2.2.3;		
15	OTI-I	Providing TI status	c) Corruption	OTI-I error; Communication error;	The TI status used by ERTMS/ETCS On-board is wrong. Train starts moving with a wrong Train Integrity status	2) see analysis in §7.2.8 function "FM6: Send of Train		

ID	Interface	Information	Failure Mode	Failure Cause	Failure Effects	Hazard/Ram equivalent ID	Mitigation	Note
				ERTMS/ETCS On-board error;	("Train integrity confirmed" instead of "Train integrity lost" or "Train integrity status unknown")	Integrity information to ERTMS/ETCS on-board" defined in §7.2.2.3;		
16	OTI-I	Providing TI status	d) Repetition	OTI-I error; Communication error; ERTMS/ETCS On-board error;	2) see analysis in §7.2.8 function "FM6: Send of Train Integrity information to ERTMS/ETCS on-board" defined in §7.2.2.3;			

## L.4 Analysis of Train Length provided to OTI-I from OTI-L and ERTMS/ETCS On-board

Scope of this section is to analyse the behaviour of OTI-I when it receives the information of Train Length by OTI-L and by ERTMS/ETCS On-board considering the following requirements:

1) transitions from “Mastership” state to “Inauguration” state and from “Monitoring” state to “Inauguration” state described in Table 7-2 and Figure 7-5 (reported below).



2) “Req\_1:”, “Req\_2:” and “Req\_3:” defined in §8.5.

### L.4.1 Start of Mission

In this example the Start of Mission is analysed.

Initial conditions:

- 1) ERTMS/ETCS On-board is in Stand-by mode and the Train Data are to be revalidated (TBR) by Driver as defined in [1];
- 2) As reported in deliverable D4.2 [7], the ERTMS/ETCS On-board provides to OTI-I Master the train length value and this value is used by OTI-I for the state transition as explained in Table 7-2.

Following the sequence diagram during the SoM:

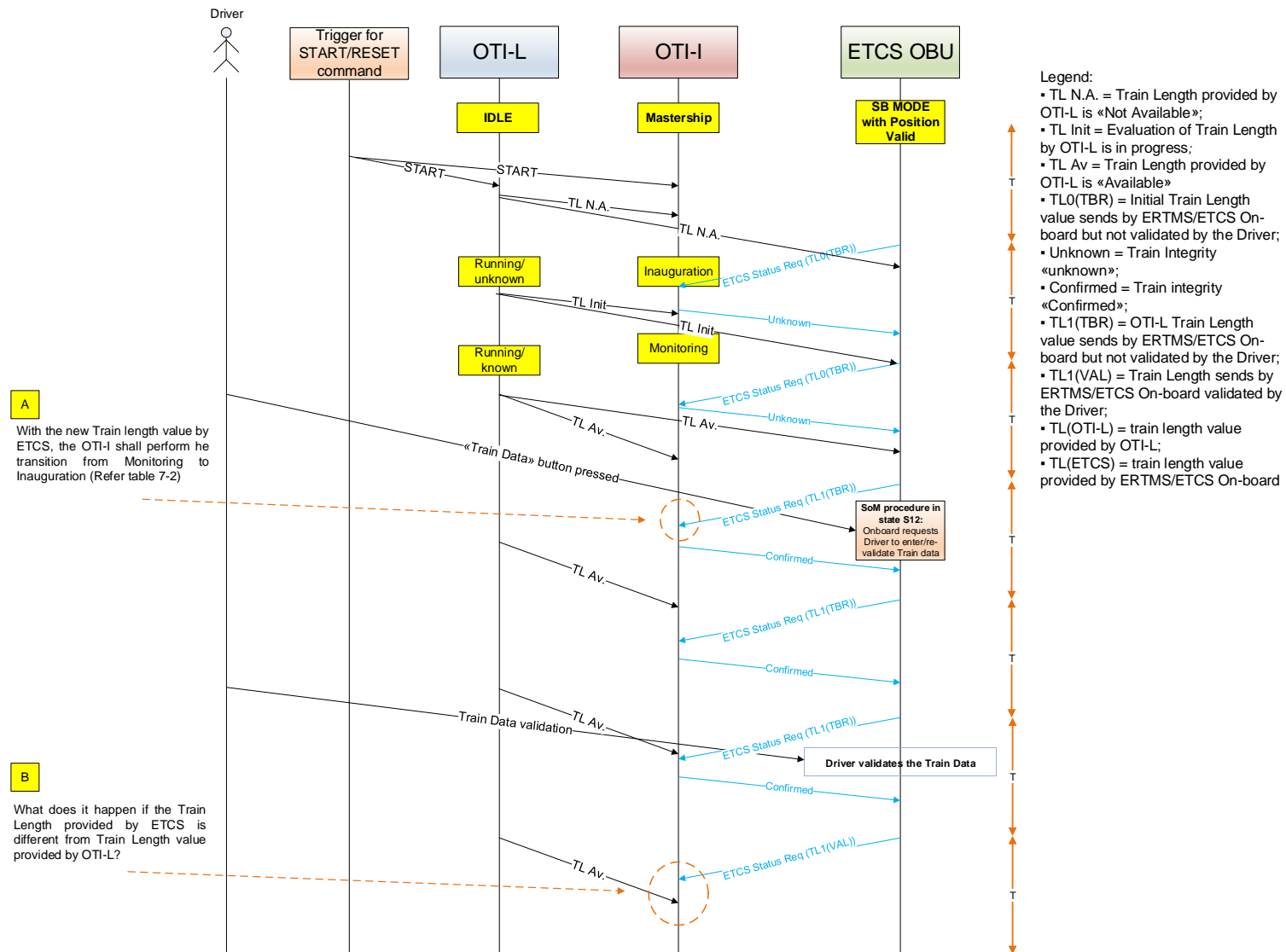


Figure 10-1: Management of Train Length by OTI-I

Two points shall be analysed as highlighted in Figure 10-1:

- Point A => when the OTI-I receives the train length sent by ERTMS/ECTS On-board (TL1(TBR) in figure), it should perform the transition from Monitoring to Inauguration as reported in Table 7-2 condition 3;
- Point B => at this point of SoM the OTI-I has received the Train Length value provided by OTI-L (TL(OTI-L)) and the Train Length value provided by the ERTMS/ECTS On-board and validated by Driver (TL1(VAL) in figure)

Point A could lead to reset the OTI-FSM with an impact on the availability of system (delay in providing the correct status of train integrity).

For Point B, it shall be considered the following situations:

- 1) Nominal Condition => Train Length value provided by OTI-L is equal to Train Length value provided by the ERTMS/ECTS On-board [TL Av = TL1(VAL)];
- 2) Degraded Condition 1 => for some reasons, the Driver before validating the Train Length value provided by OTI-L changes the value, consequently, the OTI-I receives two different values of train length by OTI-L and ERTMS/ECTS On-board [TL Av  $\neq$  TL1(VAL)]. Refer to Figure 10-2.
- 3) Degraded Condition 2 => due to a fault of OTI-L, the OTI-I receives before the train length sent by ERTMS/ECTS On-board and validated by the Driver and then the train length value sent by OTI-L. Refer to Figure 10-3.
- 4) Degraded Condition 3 => The OTI-L is not able to provide the train length. Refer to Figure 10-4. In this case, as reported in MIT\_003 in Table 8-11, the Driver is responsible to enter and to validate the train length.



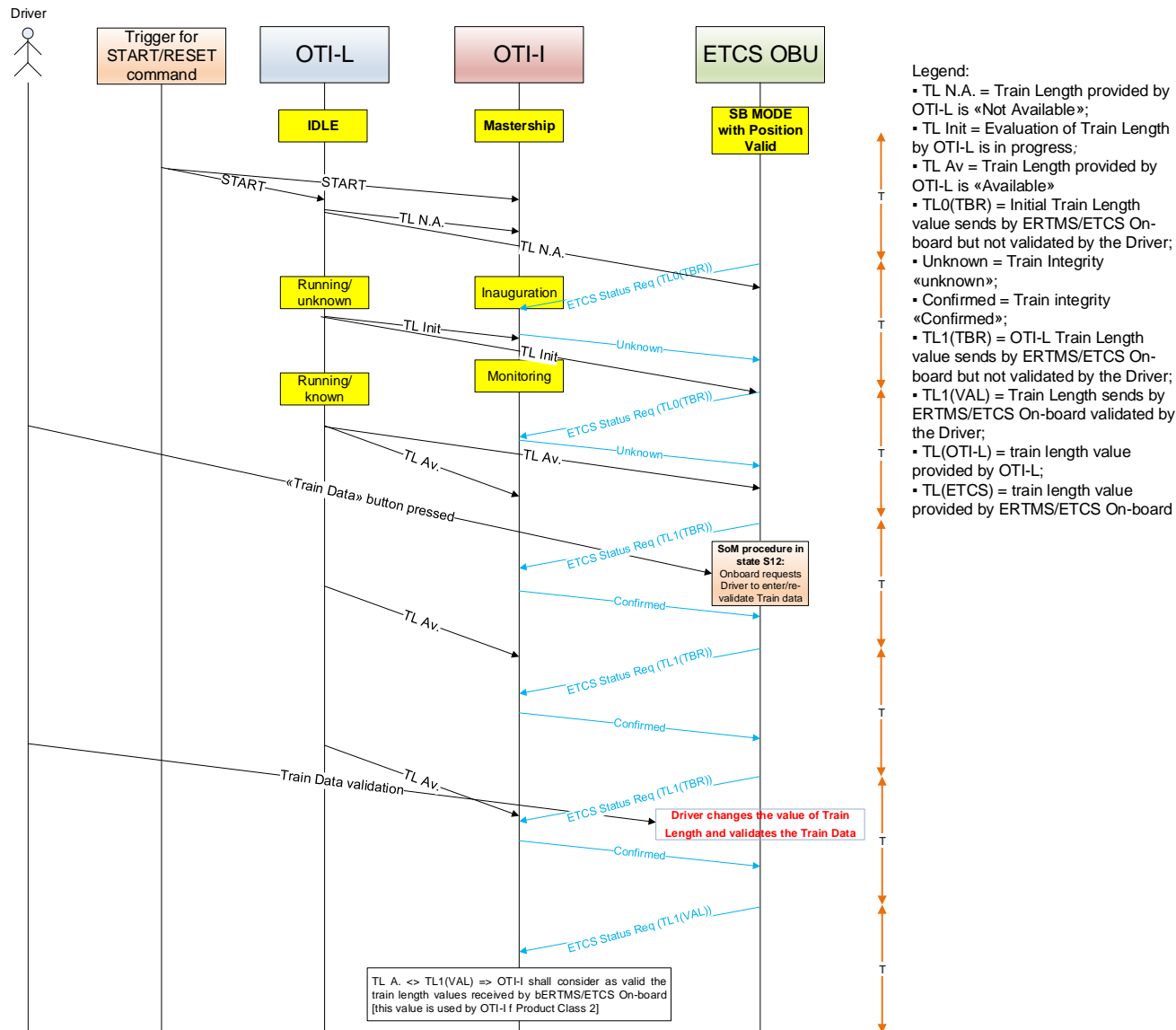


Figure 10-2: Management of Train Length by OTI-I – Degraded condition 1

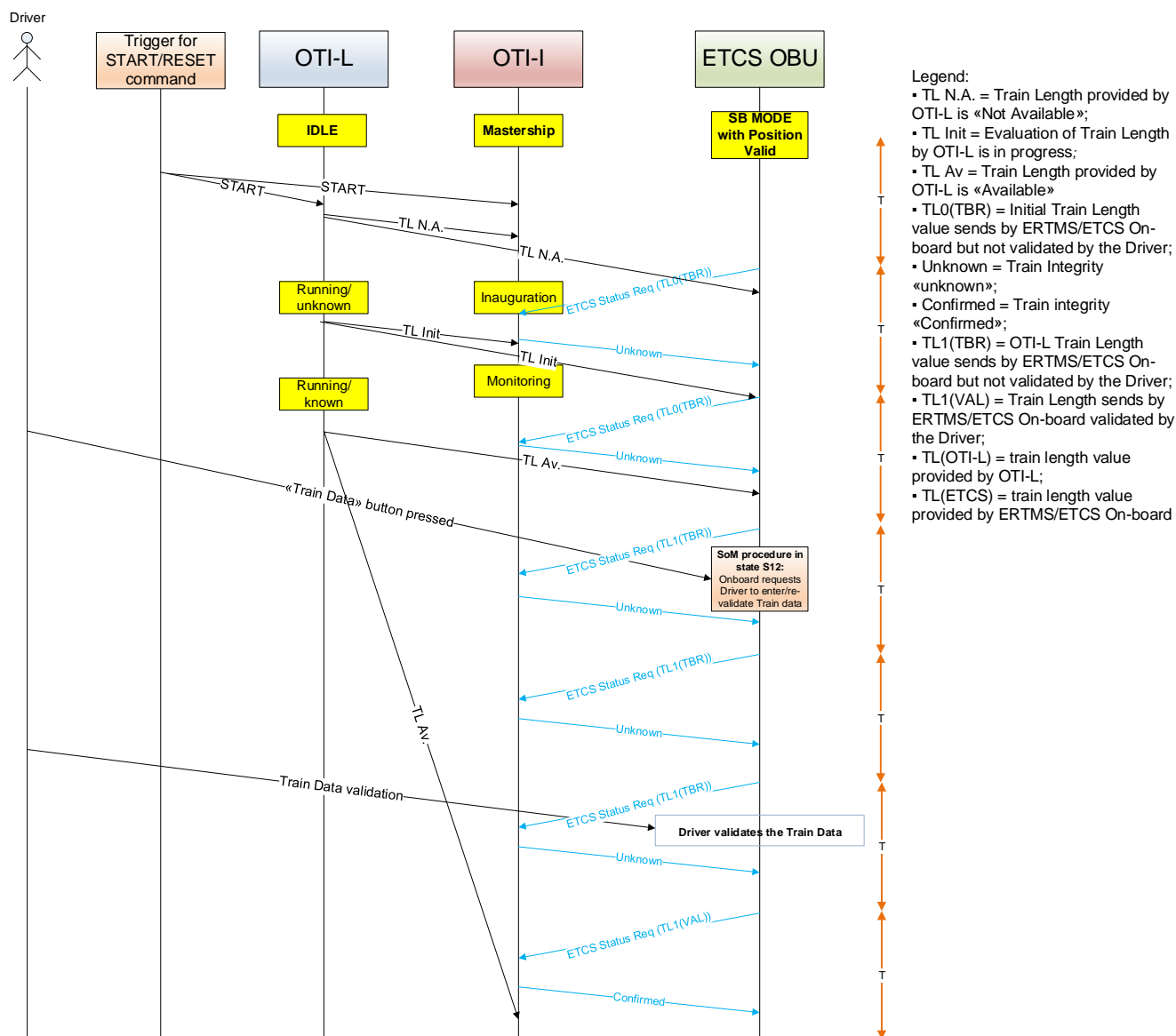


Figure 10-3: Management of Train Length by OTI-I – Degraded condition 2

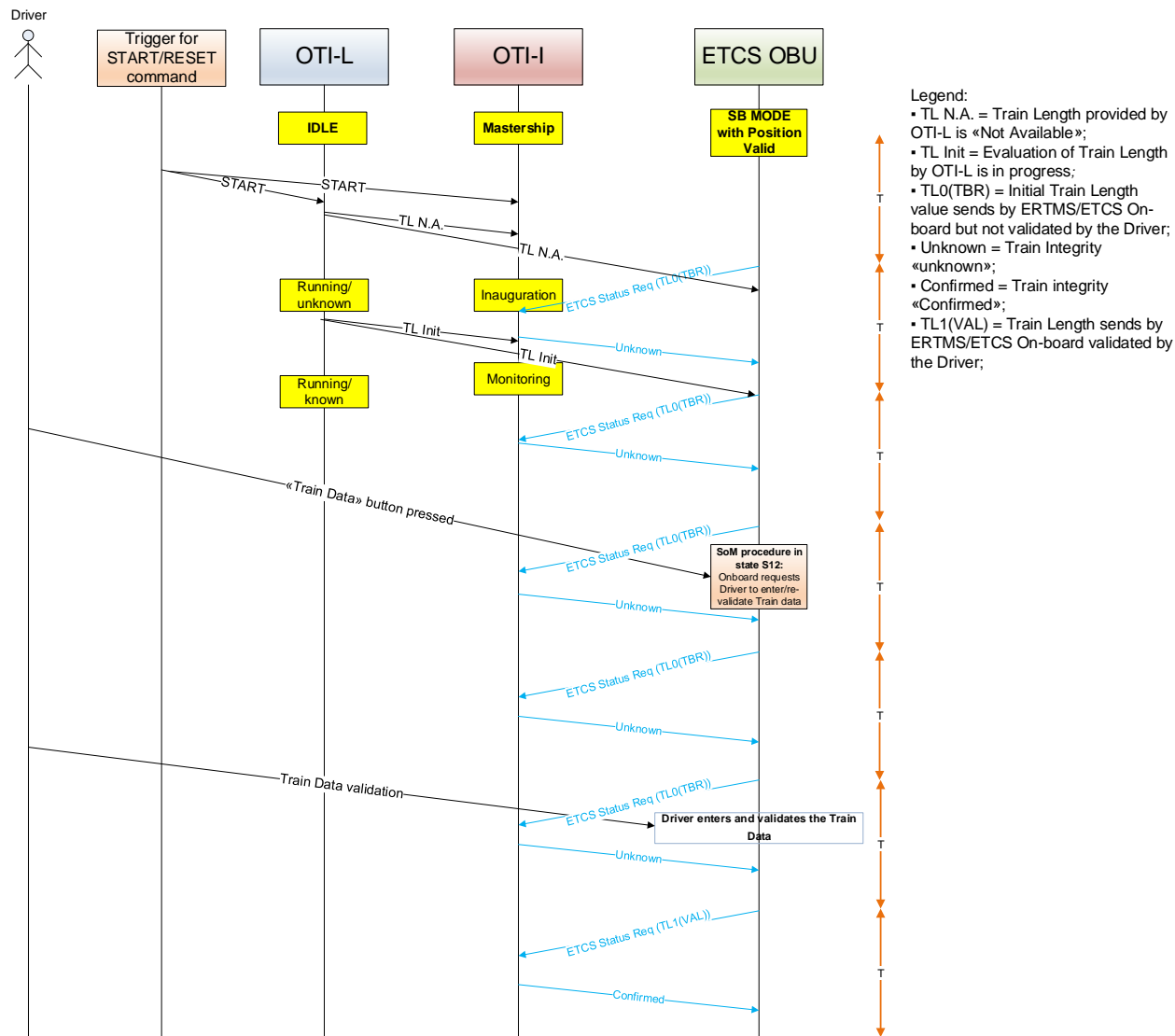


Figure 10-4: Management of Train Length by OTI-I – Degraded condition 3

The following requirements are defined:

Req\_TL\_01: The OTI-I shall consider as “new” a Train Length value provided by ERTMS/ECTS On-board only if:

- a) it is has been “validated”, AND;
- b) it replaces a Train Length value provided by ERTMS/ECTS On-board and just “validated”,

Note: see Conditions 0 and 3 in Table 7-2;

Req\_TL\_02: The ERTMS/ECTS On-board shall send to OTI-I the information of Train Length with the attribute of “validated” or “to be revalidated” (TBR).

Req\_TL\_03: The ERTMS/ECTS On-board shall send to OTI-I the information of Train Length “validated” if Driver has validated it or Train Length has been received by an external source and no Driver validation is required (see Figure 8-2 and Note 8).

Req\_TL\_04: The ERTMS/ECTS On-board shall send to OTI-I the information of Train Length “to be revalidated” (TBR) in the following case:

- 1) as specified in UNISIG Subset - 026 [1] (for example in case of a transition to Stand-by mode, see Table 8-7);
- 2) when the ERTMS/ETCS On-board sends the “Reset” Command to OTI-I;
- 3) when the ERTMS/ETCS On-board receives from the OTI-L the information of Train Length “Not Available”.

Req\_TL\_05: When the OTI-I receives the train length value by OTI-L and by ERTMS/ECTS On-board (with attribute “validated”) then it shall perform a check and verify if the values are equal or not. If this check fails then the OTI-I shall consider as correct the train length value provided by ERTMS/ECTS On-board.

Note: the train length values is used by OTI Master of Product Class 2.

#### **L.4.2     Joining/Splitting scenario**

The requirements specified in §L.4.1 are applicable also for the joining and splitting scenarios. Below (Figure 10-5 and Figure 10-6) two sequence diagrams of these two scenarios are reported as examples.



