ERTMS/ETCS
FFFIS TI – Safety Analysis
REF : SUBSET-120 ISSUE : 1.0.11 DATE : 2019-06-25

Company	Technical Approval	Management approval
ALSTOM		
ANSALDO STS		
AZD		
BOMBARDIER		
CAF		
FAIVELEY TRANSPORT		
HITACHI RAIL STS		
KNORR-BREMSE		
SIEMENS		

THALES		
VOITH TURBO		
VOSSLOH		

MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.1.0 2012-12-13	All	First draft	TIU safety group
0.2.0 2013-09-05	All	Submission to sector for review	FB
0.2.1	All	Changes see review sheet Unisig_RAMS_WG_COM_SS-120v0.2.0_v1.1.doc	JPG, FB
0.2.2	All	Changes see review sheet Unisig_SG_COM_SS-120v0.2.0_v1.0.doc, Unisig_RAMS_WG_COM_SS-120v0 2 0_v1 3.doc and Subset-120v020_review sheet_ERA_091013.doc; changed the FDT values to 48 h for regular functional tests and as typical FDT for TI inputs; changed the structure of the fault trees with redundancy; analysis added for Open MCB	TIU safety group
0.2.3	5.1.4.8 – 5.1.4.10 5.1.7.2.3.2; 6.1	SG comment 84 to Subset-119; corrections in the FMEA and consistency with Subset-080	FB
0.2.4	6.1	Failure reaction for sleeping changed according to discussion of SG comment 75 to Subset-119	FB
0.2.5	3 – 5	EB option 4 deleted and Test in Progress analyses reworked according to changes in Subset-119;	TI Meeting 01/2014

		analysis of serial transmission faults re-worked according to comment of Siemens; EBF analyses reworked, see RAMS WG comment	
0.2.6	3 – 5	OBU_TR_EB3_Cmd used for serial EB command instead of O_EB2_C; reworked FMEA and description for station platform, special brake and EB; Clarified question of UNISIG RAMS WG on the priority of human actions; Deleted alternative option for sleeping in chapter 5	TI Meeting 02/2014
0.2.7	all	Changes due to comments from UNISIG SG; for consistency with Subset-119 0.1.12 changed “option” to “solution” for variants of EB command	TI Meeting 09/2014
0.2.8	all	§3.3.1 and §5.1.4.4.1.1 changed according to comments of RAMS WG	FB, JM
0.2.9	all	Update according to changes in Subset-119 ed. 0.1.13, i.e. removed Test in progress, Emergency Brake Command Status, EB Command Feedback, Open MCB and Traction Current Cut-Off and set management of track conditions and train data information to “to be harmonized”	FB
0.2.10	3.4.7, 4.4.7, 5.1.5.6, 6.1	Update according to changes in Subset-119 ed.	FB

	and sections on STM orders	0.1.13, i.e. TCO, solution 1 deleted and added analysis for STM orders	
0.2.11	all	Changes according to RAMS WG internal comments and SG comments	FB, JM
1.0.0	1.2, 3, 4, 5, and 6.1	Modifications due to CR239, CR539, and CR1163 for BL3 R2	F. Bitsch
1.0.1	1.2, 3, 4, 5, and 6.1	Changes according to RAMS WG comments and update of Subset-080, ed. 3.1.3	F. Bitsch
1.0.2	1.2.1.2, 5.1.7.2.1.1.2, 5.1.7.2.1.2.2, 5.1.7.2.2.2, 5.1.7.2.8.2, FMEA ID 63	Update according to changes in Subset-080, ed. 3.1.4 and 3.1.5 and SG request to specify configuration requirements for which train data items driver validation is required.	F. Bitsch
1.0.3	3.4.5.1, FMEA ID 63, 5.1.7.2.3.2	Changes according to RAMS WG comments; Update according to changes in Subset-119, ed. 1.0.2: Other International Train Category deleted	F. Bitsch
1.0.4	all	Alignment with version 1.0.5 of SS-119 and incorporation of the answers for review comments	F. Bitsch
1.0.5	5 and 6	Changes according to RAMS WP comments	F. Bitsch, J. Marks
1.0.6	all	Changes according the update of SS-119 ed. 1.0.10, especially for train data	F. Bitsch, J. Marks
1.0.7	3-6	Changes according to RAMS WP comments	F. Bitsch, J. Marks
1.0.8	5.1.7.2.10.3,	Editorial changes according	F. Bitsch

	G-TBE-1 and G-TBE-2 in the FTA	to RAMS WP comments	
1.0.9	all	Changes according the update of SS-119 ed. 1.0.12 and decisions in the FFFIS TI conf call 24.05.2019: - Deletion of the alternative for TCO - Rework of Special Brake Status and Brake Position - Rework of Brake Percentage	F. Bitsch, J. Marks
1.0.10	3.6.2.8.1 and 5.1.7.2.5.2.2	Changes according the agreement in the FFFIS TI conf call 06.06.2019	F. Bitsch, J. Marks
1.0.11	3.6.2.8, 3.6.2.9, 5.1.7.2.4, 5.1.7.2.5.2.2, 5.1.7.2.6.2 and 6.2	Changes according to RAMS WP comments	F. Bitsch

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose

1.1.1.1 This document defines the generic safety requirements for Train interface information relating ETCS operating in either Level 1 or Level 2. The figures given are the minimum that must be achieved in order to ensure that ERTMS/ETCS on-board equipment may be safely integrated in any interoperable vehicles.

1.1.1.2 The architectures, signals and implementation functions described in Subset-119 were the subject of the safety analysis.

1.1.1.3 Alternatively to the analysis described in this document, further safety analyses with other safety measures can be provided which may result in product specific safety requirements.

1.1.1.4 If the technical solutions of Subset-119 are applied for a specific product then the results of this Subset can be used in the product specific safety analysis without further examinations. If another solution is selected than specified in Subset-119 then a solution specific safety analysis shall be provided.

1.2 References

1.2.1.1 The following documents, part of TSI CCS Annex A, were consulted in the development in this document:

- Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS) — EN 50126
- Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling — EN 50129
- Railway applications – Communication, signalling and processing systems — EN 50159
- System Requirements Specification — Subset-026
- FIS for the Train Interface — Subset-034
- Safety Requirements — Subset-091
- FFFIS for the Train Interface — Subset-119

1.2.1.2 The following documents, not part of TSI CCS Annex A, were consulted in the development in this document:

		Version
• Causal analysis process	Subset-077	3.0.0
• TIU FMEA	Subset-080	3.2.0
• Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-related Systems	IEC 61508	2010-04
• Industrial communication networks	IEC 61784-3	2010-06

1.3 Abbreviations and Glossary

1.3.1.1 In addition to the general UNISIG glossary, there are terms which are used in the following parts that benefit from defining as follows.

Information	Information is a datum which will be transmitted between a source and a receiver. This is independent from an implementation.
Hard-wired Interface	An interface where each signal is transmitted by a separate pair of wires.
Project	Integration project of an ERTMS/ETCS on-board equipment on a vehicle.
Serial Interface	An interface where multiple signals are transmitted via a bus/network or a point-to-point connection.
Signal	Signal is a part of information in case of a multiple-channel implementation (e.g. redundancy or anticoincidence). A signal is equivalent to information in case of a single-channel implementation.
Traction Cut Off	Inhibit positive traction effort (i.e. driving effort).

Table 1: Terms

ACC	Allowed Current Consumption
BW	Backward
CCS	Control-Command and Signalling
EB	Emergency Brake
ECS	Eddy current brake for service brake
ECE	Eddy current brake for emergency brake
FDT	Fault Detection Time

FR	Failure rate
FW	Forward
HR	Hazard Rate
MG	Magnetic shoe brake
MVB	Multifunction Vehicle Bus
OBU	On-board Unit
RB	Regenerative Brake
RST	Rolling Stock
TCMS	Train Control and Monitoring System
TFR	Tolerable Failure Rate
THR	Tolerable Hazard Rate
TR	Train
TSI	Technical Specification for Interoperability

Table 2: Abbreviations

1.4 Requirements Designation

1.4.1.1 A designation system for the quantified requirements has been introduced; TI_OB-xxx refers to a requirement on the ETCS on-board equipment and similarly TI_VE-xxx refers to a requirement on the vehicle equipment.

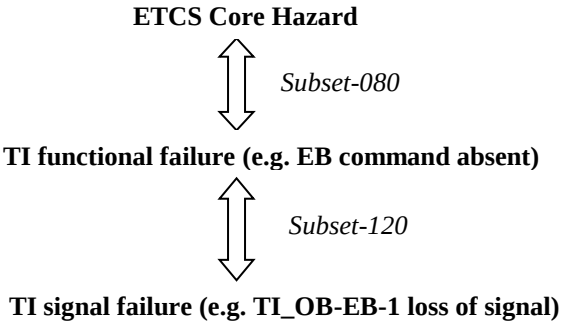
1.5 Methodology

1.5.1.1 Chapter 2 describes the system under consideration (Train Interface) for the safety analysis of this document.

1.5.1.2 The FMEA described in Annex A, chapter 6.1 is based on the description of chapter 2, the architectures and signals described in Subset-119 and the functional FMEA of Subset-080.

1.5.1.3 The purpose of the FMEA described in Annex A, chapter 6.1 is to analyse which single faults lead to which effects and in the end to which hazard.

1.5.1.4 The FMEA analyses the relationship between the TI signals and the TI functional failures already identified in Subset-080. Subset-080 and Subset-120 correspond in the TI functional failure. The Subset-080 considers the relation between TI functional failures and the ETCS Core Hazard. The Subset-120 considers the relation between TI signal failures and the TI functional failures, compare the following illustration:



1.5.1.5 Subset-120 provides an analysis for all failures which are considered as catastrophic or critical in Subset-080 or for which there is an additional architectural aspect to be considered. In these cases it is referenced to Subset-080 for the corresponding failure modes in Subset-120.

1.5.1.6 The failure modes are identified by using the failure mode guide-words listed in chapter 6.1.2 for the architectures described in Subset-119 for all TI functions.

1.5.1.7 Serial architecture has been analysed exemplarily for Sleeping.

1.5.1.8 Chapter 3 describes all events related to the functions for which a safety-related effect (severity catastrophic or critical) has been described in the FMEA. In general these single faults are used as basic events in the fault trees in annex A, chapter 6.2.

1.5.1.9 The safety targets used in the FTA are determined by TSI Loc&Pas (EB safety requirements) and UNISIG Subset-080 and Subset-091 (Hazardous TI events related to ETCS Core Hazard).

1.5.1.10 Chapter 3.8 lists all TI related events on ETCS on-board side which are hazardous according to FMEA and FTA.

1.5.1.11 Chapter 3.9 lists all TI related events on ETCS vehicle side which are hazardous according to FMEA and FTA.

1.5.1.12 Chapter 4 explains most of the gates (multiple fault effects), all barriers and all conditions used in the fault trees in annex A, chapter 6.2.

1.5.1.13 From FTA TFR values are derived for the basis events.

1.5.1.14 Chapter 5 summarizes all the results obtained (requirements for TI) including the exported constraints and the TFR and FDT values resulting from the FTA. Related assumptions are listed. This chapter is the input to Subset-119 and it is included in that document classified as safety requirements.

2. SYSTEM UNDER INSPECTION

2.1 Context

2.1.1.1 For different vehicle systems, different TI configurations might be necessary. The following figure outlines the TI configurations and their interaction with external entities (driver and trackside) in order to show how a safe implementation of TI configurations ensures the overall safety at TSI CCS/Loc&Pas system level. The black arrows show interactions in the system and the blue arrows show information flows which could lead to a hazard. Configurations define different interface types from where a wrong-side failure could be propagated up to the TSI CCS/Loc&Pas system level and thus failing to prevent the occurrence of hazardous situations (Top Hazard, e.g. a wrong-side failure at emergency brake interface could lead the vehicle braking system to not apply effectively the vehicle emergency brake).

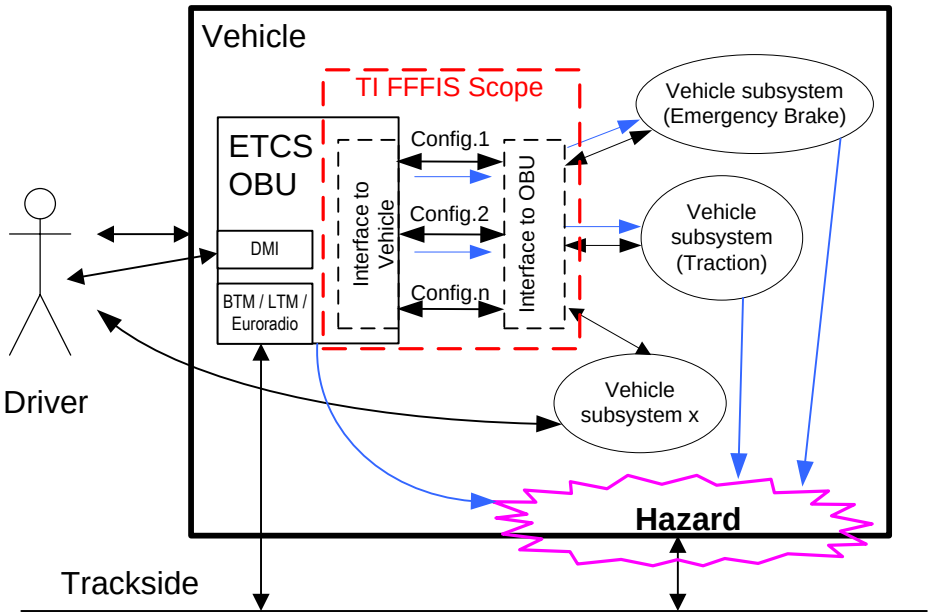


Figure 1: Safety Boundaries

2.1.1.2 From the figure above the following entities and their contribution to system definition are identified:

- Vehicle subsystems like Emergency Brake, Traction, Pantograph… as a Black Box – described in the TSI Loc&Pas.
- ETCS OBU (Black Box) – a subsystem inside the vehicle. This is part of the TSI CCS signalling subsystem providing the ETCS on-board functionality.
- Trackside – outside the scope of this document.

2.1.1.3 Note that from a safety point of view two relevant interfaces can be identified but none of them dealing with TI functionality. The first one is the ETCS data transmission interface for OBU transmission units interacting for data transmission between track and vehicle. The second interface is between the rail and vehicle wheels and provides the adhesion capability of vehicle to rails in order to ensure braking effect. Failures from these interfaces will be considered out of the scope of TI safety.

2.1.1.4 Driver – Outside the boundaries of TI safety. Driver interacts with ETCS OBU and vehicle systems. Failures from this interface (driver actions) will be considered out of the scope of TI safety.

2.1.1.5 Maintenance and Commissioning Staff are outside the boundaries of TI safety. They interact with ETCS OBU and vehicle systems at maintenance and/or commissioning work. Failures from this source will be considered out of the scope of TI safety.

2.1.1.6 Physically, the TI consists only of transmission components (cables and connectors). It is just an interface, which connects the ETCS OBU and the vehicle systems. The vehicle integrator (contract specific) is responsible for the engineering of the train interface including cable connections.

2.1.1.7 Note: The ETCS Core Hazard is related exclusively to the ETCS on-board unit as defined in Subset-091. It ends at the Train Interface.

3. SINGLE FAULTS DESCRIPTION

3.1 General

3.1.1.1 The intention of this chapter is to explain the hazardous events of the several functions used in the fault trees in annex A, 6.2.

3.1.1.2 The FR and FDT values used in this chapter are only examples to reach the safety target. Other values could be used if they reach the targets (e.g. higher FR value with shorter FDT).

3.1.2 Consideration of redundant and antivalent signals

3.1.2.1 Redundant signals are used in Subset-119 when it is necessary according to the analysis of multiple failures in Subset-120, chapter 4.

3.1.2.2 Antivalence is used as a measure against common mode failures and for fault detections.

3.1.2.3 If there are redundant or antivalent signals given by Subset-119 then this is considered in the single faults analysis (FMEA) already. As a consequence redundancy and antivalence are not used as barriers in the FMEA but are already considered in the failure effects (which failure effects are credible). In this way a too large FMEA table is avoided.

3.1.3 Consideration of serial transmission faults

3.1.3.1 Serial architecture a) (see Subset-119, chapter 4.2.2)

3.1.3.1.1 Analysis of serial architecture a) is performed using Sleeping signals, which can be used as an example for other safety-related TI inputs.

3.1.3.1.2 In architecture a) causes for transmission failures can be failures of a simple I/O device, failures of the bus interface card or undetected failures due to the performance of the transmission code (compare explanations and reasoning in the sections 3.2.1.1 and 4.2.1.4.4).

3.1.3.1.3 The failure rate R_a for serial transmission is determined by undetected failures due to the performance of the transmission code (R_{uf}) and hardware failures at transmission (R_{HW}).

Bus information are evaluated by OBUs, only if these are constant over at least 2 Bus cycles. For a CRC-16 a failure rate of R_{uf} = 1E-5 /h can be assumed conservatively.

Most failures due to the transmission hardware are detected due to the check of the antivalency of the signals on application level in ERTMS/ETCS on-board equipment. But there are residual failures which have to be considered with the failure rate of the bus interface card. It is assumed that a typical failure rate of a bus interface card is R_{HW} = 1E-5 /h.

$R_a = R_{uf} + R_{HW}$ = 2E-5 /h

It is assumed that there is a transmission failure detection so that FDT < 1 min. But a failure in a bus interface card can be detected always when a telegram is received. In a conservative assumption it is supposed that every 24 h a telegram is received so that the bus interface card has a FDT=24 h.

3.1.3.1.4 Note: For examples for calculation of a hazardous failure rate of the complete transmission system see IEC 61784-3.

3.1.3.2 Serial architecture b) (see Subset-119, chapter 4.2.3)

3.1.3.2.1 Architecture b) has to be implemented strictly according to EN 50159. The hazardous failure rate of the transmission system is lower than the typical signal failure rate 1E-5 /h (compare the following sections). That means the influence on the hazards can be neglected. Therefore no specific analysis is necessary in addition to the analysis of the hard-wired interface.

3.1.3.2.2 The communication partners in architecture b) need at least the safety level of the information which is transmitted. The HR of the TCMS depends on the information which is transmitted.

3.1.3.2.3 Note: For examples for calculation of a hazardous failure rate of the complete transmission system see IEC 61784-3.

3.2 Hazardous Events of Mode Control

3.2.1 Sleeping

3.2.1.1 Event description (serial and hard-wired connection)

Event	Explanation
TI_OB-SL-1.1, TI_OB-SL-1.2, TI_VE-SL-1.1 and TI_VE-SL-1.2	It is assumed that a failure rate for the sleeping signals is FR = 1E-5 /h as typically for input signals from vehicle. As typical FDT for TI inputs 48 h are assumed for the vehicle side. For the ETCS on-board equipment side an FDT of 1 minute is assumed due to the fault detection based on antivalency. The antivalent sleeping signals T_SL_E_N and T_SL_E_I shall have two sources. Nevertheless common cause failures have to be taken into account. This is considered with a β-factor of 10% according to IEC 61508-6 on vehicle side. For OBU side the independence according to EN50129 has to be shown.
TI_OB-SL-1 and TI_VE-SL-1	It is assumed that a failure rate for the sleeping signal T_SL_E is FR = 1E-5 /h as typically for input signals from vehicle. As typical FDT for TI inputs 48 h are assumed for the vehicle and ETCS on-board equipment side.
TI_VE-BUS-1.0	It is assumed that a typical failure rate of a simple I/O device is FR = 5E-6 /h. A failure in a simple I/O device can be detected e.g. by the driver. In a conservative assumption it is supposed that FDT=24 h.
TI_VE-BUS-2.0	According to section 3.1.3.1.3 a failure rate for undetected failures due to the performance of the transmission code and hardware failures at transmission is assumed of FR = 2E-5 /h for architecture a). In case of architecture b) the transmission channel can be neglected in the fault trees. It is assumed that there is a transmission failure detection so that FDT = 1 min.

3.2.1.2 Event description for general analysis for serial communication with two inputs by means of sleeping.

Event	Explanation
TI_VE-SL-1.1 and TI_VE-SL-1.2	It is assumed that a failure rate for the sleeping signals is FR = 1E-5 /h as typically for input signals from vehicle. As typical FDT for TI inputs 48 h are assumed for the vehicle side. For the ETCS on-board equipment side an FDT of 1 minute is assumed due to the fault detection based on antivalency. The antivalent sleeping signals TR_OBU_TrainSleep and TR_OBU_TrainSleep_Not shall have two sources. Nevertheless common cause failures have to be taken into account. This is considered with a β-factor of 10% according to IEC 61508-6 on vehicle side. For OBU side the independence according to EN50129 has to be shown.
TI_VE-BUS-1.1 and TI_VE-BUS-1.2	It is assumed that a typical failure rate of a simple I/O device is FR = 5E-6 /h. Because there is only one bus connected to both simple I/O devices, common cause failures are possible. This is considered with a β-factor of 10% according to IEC 61508-6. It is the same common cause as for TI_OB-BUS1.1, TI_OB-BUS1.2, TI_VE-BUS-2.1, and TI_VE-BUS-2.2.
TI_VE-BUS-2.1 and TI_VE-BUS-2.2	According to section 3.1.3.1.3 a failure rate for undetected failures due to the performance of the transmission code and hardware failures at transmission is assumed of FR = 2E-5 /h for architecture a). In case of architecture b) the transmission channel can be neglected in the fault trees. It is assumed that there is a transmission failure detection so that FDT = 1 min. Most common cause failures are detected due to the check of the antivalency of the signals on application level in ERTMS/ETCS on-board equipment. Residual common cause failures due to only one bus connected to both simple I/O devices and due to only one bus interface card are considered with a β-factor of 10% according to IEC 61508-6. It is the same common cause as for TI_OB-BUS1.1, TI_OB-BUS1.2, TI_VE-BUS-1.1, and TI_VE-BUS-1.2.

3.2.2 Passive shunting

3.2.2.1 Event description

Event	Explanation
TI_OB-PS and TI_VE-PS	It is assumed that a failure rate for the Passive Shunting signal is FR = 1E-5 /h as typically for input signals from vehicle. As FDT for TI inputs 48 h are assumed (under condition that it is checked in the scope of the start-up tests or regular functional test).

3.2.3 Non leading

3.2.3.1 Event description

Event	Explanation
TI_OB-NL and TI_VE-NL	It is assumed that a failure rate for the Non Leading signal is FR = 1E-5 /h as typically for input signals from vehicle. As typical FDT for TI inputs 48 h are assumed (under condition that it is checked in the scope of the start-up tests or regular functional test).

3.2.4 Isolation

3.2.4.1 Under the assumptions described in chapter 5.1.3.4.2 single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.3 Hazardous Events of Control of Brakes

3.3.1 Service brake command

3.3.1.1 Safety does not rely on the service brake.

3.3.1.2 Assumption: No impact on emergency brake model.

3.3.1.3 A more detailed safety analysis is needed in order to show that, in case of use of service brake, a failure of service brake is recognized and the emergency brake is applied as safeguarding.

3.3.1.4 Single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.3.2 Brake pressure

3.3.2.1 Single failures have no safety-related effect in the system under inspection as defined in section 2 (see Subset-080, 5.2.2). According to Subset-026-3, clause A.3.10.1 only the SBI is effected by the signal.

3.3.3 Emergency brake command

3.3.3.1 Event description (solution 1 and 2)

Event	Explanation
TI_OB-EB-1, TI_OB-EB-2, TI_VE-EB-1 and TI_VE-EB-2	It is assumed that a failure rate for the emergency brake output signal on hard-wired interface is FR = 1E-7 /h on vehicle side and 3E-6 /h on ETCS/ERTMS on-board equipment side, compare note in §4.3.3.1.2. The two EB signals O_EB1_C and O_EB2_C shall be output physically independent according to EN 50129 by the ERTMS/ETCS on-board equipment. On vehicle side common cause failures are taken into account. This is considered with a β-factor of 1% according to IEC 61508-6. As typical FDT 48 h are assumed (under condition that it is checked in the scope of the start-up tests or regular functional test).

3.3.3.2 Event description (solution 3)

Event	Explanation
TI_OB-EB-3, TI_OB-EB-4, TI_VE-EB-3 and TI_VE-EB-4	The two EB signals O_EB1_C and OBU_TR_EB3_Cmd shall be output physically independent according to EN 50129 by the ERTMS/ETCS on-board equipment. The two EB signals O_EB1_C and OBU_TR_EB3_Cmd are output diverse due to O_EB1_C is output on hard-wired and OBU_TR_EB3_Cmd is output on serial interface. Due to the diversity no common cause failures have to be taken into account. It is assumed that a failure rate for the emergency brake output signal O_EB1_C on hard-wired interface is FR = 3E-6 /h on vehicle side and on ETCS/ERTMS on-board equipment side. For serial communication the FR value shall be 1E-7 /h for OBU_TR_EB3_Cmd on vehicle and on ERTMS/ETCS on-board equipment side. As typical FDT 48 h are assumed (under condition that it is checked in the scope of the start-up tests or regular functional test).

3.3.4 Special brake inhibition area – Trackside orders

3.3.4.1 Under the assumption described in 5.1.4.4.2 single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.3.5 Special brake inhibit – STM orders

3.3.5.1 Analysis is national system specific.

3.3.6 Special brake status

3.3.6.1 If vehicle is equipped with special brakes and if the OBU uses this status signal to switch between different brake models, then the special brake status is relevant to calculate the brake model, see clause 5.1.4.6.2.

3.3.7 Additional brake status

3.3.7.1 In case of additional brakes are equipped a more detailed safety analysis is needed.

3.4 Hazardous Events of Control of Train Functions

3.4.1 Change of traction system

3.4.1.1 Under consideration of the exported constraints specified in 5.1.5.1 single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.4.2 Powerless section with pantograph to be lowered – Trackside orders / Pantograph – STM orders

3.4.2.1 Single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.4.3 Air tightness area – Trackside orders / Air tightness – STM orders

3.4.3.1 Under consideration of the exported constraints specified in 5.1.5.3.2 single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.4.4 Station platform

3.4.4.1 Extensive single failure analysis is project specific, see 5.1.5.4.

3.4.4.2 Hint: The related function “door opening” is independent from the ETCS information. A function on vehicle side or an operational regulation is necessary to handle this information in a safe way.

3.4.5 Powerless section with main power switch to be switched off – Trackside orders

3.4.5.1 Single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.4.6 Main power switch – STM orders

3.4.6.1 Single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.4.7 Change of allowed current consumption (ACC)

3.4.7.1 Single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.4.8 Traction Cut Off

TCO with serial output OBU_TR_TCO_Cmd and hard-wired output O_TC1_C allows a safe TCO affecting the braking curves.

3.4.8.1 Event description

Event	Explanation
TI_OB-TCO-1, TI_OB-TCO-2, TI_VE-TCO-1, TI_VE-TCO-2	It is assumed that a failure rate for the TCO output signal on hard-wired interface (O_TC1_C hard-wired) is FR = 1E-5 /h on vehicle side and on ETCS/ERTMS on-board equipment side. For serial communication the FR value shall be 1E-7 /h for OBU_TR_TCO_Cmd on vehicle and on ERTMS/ETCS on-board equipment side. The two outputs have to be output physically independent according to EN 50129 by the ERTMS/ETCS on-board equipment. Due to the diversity of the output paths no common cause factors have to be taken into account. As typical FDT 48 h are assumed for hard-wired interface (under condition that EB is checked in the scope of the start-up tests or regular functional test). For serial interface conservatively a FDT of 1 h is assumed.

3.5 Hazardous Events of Train Status Information

3.5.1 Cab Status

3.5.1.1 Event description

Event	Explanation
TI_OB-CS-1, TI_OB-CS-2, TI_VE-CS-1 and TI_VE-CS-2	These events represent the cab status failures. The two Cab status signals TI_OB-CS-1 and TI_OB-CS-2 shall be physically independent according to EN 50129 by the ERTMS/ETCS on-board equipment. Due to Subset 034 2.5.1.3 each cab will be connected to its individual input on vehicle side. Nevertheless common cause failures have to be taken into account. This is considered with a β-factor of 10% according to IEC 61508-6 on vehicle side. For OBU side the independence according to EN50129 has to be shown. It is assumed that a failure rate for the cab status signal is FR = 1E-5 /h as typically for input signals from vehicle. As typical FDT for TI inputs 48 h are assumed.

3.5.2 Direction Controller

3.5.2.1 Event description

Event	Explanation
TI_OB-DC-1, TI_OB-DC-2, TI_VE-DC-1 and TI_VE-DC-2	These events represent the direction controller signal failures. T_FW_S / TR_OBU_DirectionFW failure (TI_OB-DC-1 and TI_VE-DC-1) is relevant for a downhill slope. T_BW_S / TR_OBU_DirectionBW (TI_OB-DC-2 and TI_VE-DC-2) failure would be relevant for an uphill slope. It is assumed that a failure rate for the direction signal is FR = 1E-5 /h as typically for input signals from vehicle. As typical FDT for TI inputs 48 h are assumed.

3.5.3 Train integrity

3.5.3.1 To be harmonized.

3.5.4 Traction Status

3.5.4.1 The traction status is forwarded to the STM. The information related to STMs is seen as out of scope of this safety analysis focusing on level 1 and level 2 aspects."

3.5.5 Set Speed

3.5.5.1 Single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.6 Hazardous Events of Train Data

3.6.1 Type of train data entry

3.6.1.1 Single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.6.2 Train data information

3.6.2.1 Train Composition

3.6.2.1.1 Train composition failures with related hazardous events are provided in each specific train data information where they could contribute.

3.6.2.2 Train Type

3.6.2.2.1 Train type failures with related hazardous events are provided in each specific train data information where they could contribute.

3.6.2.3 Tilting Health Status

3.6.2.3.1 Tilting health status failures with related hazardous events are provided in each specific train data information where they could contribute.

3.6.2.4 Train category / Cant deficiency

3.6.2.4.1 Event description

Event	Explanation
TI_OB-CD, TI_VE-CD, TI_OB-TT, TI_VE-TT, TI_OB-TC, TI_VE-TC, TI_OB-THS, and TI_VE-THS	The events TI_OB-CD and TI_VE-CD represent the cant deficiency value failures. A failure rate in the range of SIL2 is needed. In case the cant deficiency value is based on the train type input (TI_OB-TT and TI_VE-TT), or train composition input (TI_OB-TC and TI_VE-TC) and tilting health status input (TI_OB-THS and TI_VE-THS) then the failure rate of this input has to be also in the range of SIL2.
TI_OB-THS-1, TI_OB-THS-2, TI_VE-THS-1, and TI_VE-THS-2	In the case tilting health status input is a hard-wired input then two signals are needed (with the events TI_OB-THS-1/TI_VE-THS-1 and TI_OB-THS-2/TI_VE-THS-2) and it its assumed that a failure rate for a signal is FR = 1E-5 /h as typically for input signals from vehicle. As typical FDT for TI inputs 48 h are assumed. TR_OBU_TiltingHealthStatus-1 and TR_OBU_TiltingHealthStatus-2 shall be physically independent according to EN 50129 by the ERTMS/ETCS on-board equipment. Common cause failures have to be taken into account. This is considered with a β-factor of 10% according to IEC 61508-6 on vehicle side. For OBU side the independence according to EN50129 has to be shown.

3.6.2.4.2 Single failures can be regarded as having a ‘RAM Issue’ if adequate safety margin against derailment can be demonstrated for the vehicle exceeding maximum authorized speed for its train category; compare FMEA in Annex A, 6.1.

3.6.2.5 Train length

3.6.2.5.1 Event description

Event	Explanation
TI_OB-TL, TI_VE-TL, TI_OB-TT, TI_VE-TT, TI_OB-TC, TI_VE-TC	The events TI_OB-TL and TI_VE-TL represent the train length value failures. A failure rate in the range of SIL2 is needed. In case the train length value is based on the train type input (failure events TI_OB-TT and TI_VE-TT) or train composition input (failure events TI_OB-TC and TI_VE-TC) then the failure rate of this input has to be also in the range of SIL2.

3.6.2.6 Traction model

3.6.2.6.1 Event description

Event	Explanation
TI_OB-TM, TI_VE-TM, TI_OB-TT, TI_VE-TT, TI_OB-TC, TI_VE-TC	The events TI_OB-TT and TI_VE-TT represent train type input failure and TI_OB-TC and TI_VE-TC the train composition input failure which is the cause for a traction model failure (TI_OB-TM and TI_VE-TM). The failure rate of the used input has to be in the range of SIL2.

3.6.2.7 Brake build up time model and speed dependent deceleration model

3.6.2.7.1 Event description

Event	Explanation
TI_OB-TM, TI_VE-TM, TI_OB-TT, TI_VE-TT, TI_OB-TC, TI_VE-TC, TI_OB-SBS, and TI_VE-SBS,	The events TI_OB-TT and TI_VE-TT represent train type input failure, TI_OB-TC and TI_VE-TC the train composition input failure which can be a possible cause for a Brake build up time model or speed dependent deceleration model failure (TI_OB-TM and TI_VE-TM). The failure rate of the used input has to be in the range of SIL2.
TI_OB-SBS-1 and TI_OB-SBS-2	If special brake status is implemented via hard-wired interface a failure rate of FR = 1E-7 /h is needed for the respective status information which is based on the composition of status signals • T_EP_S_N and T_EP_S_I, • T_EC_S_N and T_EC_S_I, • T_RB_S_N and T_RB_S_I, or/and • T_MG_S_N and T_MG_S_I. As typical FDT for TI inputs 48 h are assumed.

3.6.2.8 Brake percentage

3.6.2.8.1 Event description

Event	Explanation
TI_OB-BP, TI_VE-BP, TI_OB-TT, TI_VE-TT, TI_OB-TC, TI_VE-TC	The events TI_OB-TT and TI_VE-TT represent train type input failure and TI_OB-TC and TI_VE-TC the train composition input failure which is the cause for a brake percentage failure (TI_OB-BP). The failure rate of the used input has to be in the range of SIL2. Note: For integrity requirements on preparation of data on the vehicle side (TI_VE-BP), see Subset-091, EXT_SR03. This is project specific.

3.6.2.9 Brake position

3.6.2.9.1 Event description

Event	Explanation
TI_OB_BPos, TI_VE_BPos, TI_OB-TT, TI_VE-TT, TI_OB-TC, and TI_VE-TC	The events TI_OB_BPos and TI_VE_BPos represent the brake position value failures. A failure rate in the range of SIL2 is needed. In case the brake position value is based on the train type input (TI_OB-TT and TI_VE-TT) or on train composition input (TI_OB-TC and TI_VE-TC) then the failure rate of this input has to be also in the range of SIL2.

Event	Explanation
TI_OB-BPos-1.1, TI_OB-BPos-1.2, TI_VE-BPos-1.1, and TI_VE-BPos-1.2	If brake position input is implemented via hard-wired interface a failure rate of FR = 1E-7 /h is needed for composition of T_BP_S1_N and T_BP_S1_I and a failure rate of FR = 1E-7 /h is needed for T_BP_S2 (composition of T_BP_S2_N and T_BP_S2_I). The events TI_OB-BPos-1.1, TI_OB-BPos-1.2, TI_VE-BPos-1.1, and TI_VE-BPos-1.2 represent the brake position value failures. As typical FDT for TI inputs 48 h are assumed.

3.6.2.10 Nominal rotating mass

3.6.2.10.1 Single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.6.2.11 Maximum train speed

3.6.2.11.1 Event description

Event	Explanation
TI_OB-MTS, TI_VE-MTS, TI_OB-TT, TI_VE-TT, TI_OB-TC, TI_VE-TC, TI_OB-THS, and TI_VE-THS	The events TI_OB-TT and TI_VE-TT represent train type input failure, TI_OB-TC and TI_VE-TC the train composition input failure and tilting health status input TI_OB-THS, and TI_VE-THS which is the cause for a maximum train speed value failure (TI_OB-MTS and TI_VE-MTS). The failure rate of the used input has to be in the range of SIL2.

Event	Explanation
TI_OB-THS-1, TI_OB-THS-2, TI_VE-THS-1, and TI_VE-THS-2	In the case tilting health status input is a hard-wired input then two signals are needed (with the events TI_OB-THS-1/TI_VE-THS-1 and TI_OB-THS-2/TI_VE-THS-2) and it its assumed that a failure rate for a signal is FR = 1E-5 /h as typically for input signals from vehicle. As typical FDT for TI inputs 48 h are assumed. TR_OBU_TiltingHealthStatus-1 and TR_OBU_TiltingHealthStatus-2 shall be physically independent according to EN 50129 by the ERTMS/ETCS on-board equipment. Common cause failures have to be taken into account. This is considered with a β-factor of 10% according to IEC 61508-6 on vehicle side. For OBU side the independence according to EN50129 has to be shown.

3.6.2.12 Loading gauge

3.6.2.12.1 Under the assumptions described in section 5.1.7.2.10 single failures have no safety-related effect in the system, compare FMEA in Annex A, 6.1.

3.6.2.13 Axle load category

3.6.2.13.1 Event description

Event	Explanation
TI_OB-ALC, TI_VE-ALC, TI_OB-TT, TI_VE-TT, TI_OB-TC, TI_VE-TC	The events TI_OB-ALC and TI_VE-ALC represent the axle load category value failures. A failure rate in the range of SIL2 is needed. In case the axle load category value is based on the train type input (failure events TI_OB-TT and TI_VE-TT) or train composition input (failure events TI_OB-TC and TI_VE-TC) then then the failure rate of this input has to be also in the range of SIL2.

3.6.2.14 Traction system(s) accepted by the engine

3.6.2.14.1 Single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1.

3.6.2.15 Train fitted with airtight system

3.6.2.15.1 Under consideration of the exported constraints specified in 5.1.7.2.13.4 single failures have a marginal safety effect.

3.7 Description of the Hazardous Events of National System Isolation

3.7.1 National System Isolation

3.7.1.1 This is level NTC only which is seen as out of scope of this safety analysis focusing on level 1 and level 2 aspects.

3.8 Hazardous Events Schedule ETCS on-board

Event Id.	Hazardous Event Description	Corresponding to FIS event	Reference to FTA
TI_OB-SL-1.1	Inappropriate reception of faulty Sleeping signal T_SL_E_N	TI-3	4.2.1.4.1_SL_PAR
TI_OB-SL-1.2	Inappropriate reception of faulty Sleeping signal T_SL_E_I	TI-3	4.2.1.4.1_SL_PAR
TI_OB-SL-1	Inappropriate reception of faulty Sleeping signal T_SL_E	TI-3	4.2.1.4.2_SL_PAR_ALT
TI_VE-BUS-2.0, TI_VE-BUS-2.1, TI_VE-BUS-2.2	Bus falsifies first telegram (serial transmission architecture a) - contribution on ERTMS/ETCS on-board equipment side: Bus interface card failure	It is related to the TI-x of the corresponding TI function for which the serial transmission is used (e.g.: TI-3)	e. g. 4.2.1.4.4_SL_BUS and 4.2.1.4.3_SL_BUS_ALT
TI_OB-PS,	Inappropriate reception of faulty Passive Shunting signal T_PS_E / TR_OBU_PassiveShunting	TI-7	4.2.2.1_PS_PAR
TI_OB-NL	Inappropriate reception of Non Leading signal T_NL_E / TR_OBU_NLEnabled	TI-8	4.2.3.1_NL_PAR
TI_OB-EB-1	Loss of Emergency Brake signal O_EB1_C	TI-1	4.3.3.1-0_EB_Solution1-2, 4.3.3.2_EB_Solution3
TI_OB-EB-2	Loss of Emergency Brake signal O_EB2_C (solution 1-2) or OBU_TR_EB3_Cmd (solution 3)	TI-1	4.3.3.1-0_EB_Solution1-2, 4.3.3.2_EB_Solution3
TI_OB-PD	Inappropriate output of Station Platform information	No relation to ETCS Core Hazard	-
TI_OB-CS	Wrong Cabin considered as Active due to falsification of both cab status signals T_CS_A / TR_OBU_CabStatusA and T_CS_B /	TI-6b, KERNEL-15	4.5.1.1_CS_PAR

Event Id.	Hazardous Event Description	Corresponding to FIS event	Reference to FTA
	TR_OBU_CabStatusB are falsified at the same time.		
TI_OB-DC-1	Loss of Direction Controller status signal T_FW_S / TR_OBU_DirectionFW	TI-5	4.5.2.1_DCP_PAR
TI_OB-DC-2	Loss of Direction Controller status signal T_BW_S / TR_OBU_DirectionBW	TI-5	No fault tree but equivalent to 4.5.2.1_DCP_PAR
TI_OB-TT	Inappropriate reception of Train Type Input	TI-10	4.6.2.4.1_Cant_Deficiency, 4.6.2.7.2.1_Brake_Model_BUS, 4.6.2.7.2.2_Brake_Model_PAR, 4.6.2.8.1_Brake_Percentage, 4.6.2.6.1_Traction_Model, 4.6.2.9.2.1_Brake_Pos_BUS, 4.6.2.10.2.1_Max_TS_BUS, 4.6.2.12.1_Axle_Load_Category 4.6.2.5.1_Train_Length
TI_OB-TC	Inappropriate reception of Train Composition Input	TI-10	4.6.2.4.1_Cant_Deficiency, 4.6.2.7.2.1_Brake_Model_BUS, 4.6.2.7.2.2_Brake_Model_PAR, 4.6.2.8.1_Brake_Percentage, 4.6.2.6.1_Traction_Model, 4.6.2.9.2.1_Brake_Pos_BUS, 4.6.2.10.2.1_Max_TS_BUS, 4.6.2.10.2.2_Max_TS_PAR, 4.6.2.10.2.3_Max_TS_PAR_ALT, 4.6.2.12.1_Axle_Load_Category 4.6.2.5.1_Train_Length
TI_OB-THS	Inappropriate reception of Tilting Health Status	TI-10	4.6.2.4.1_Cant_Deficiency, 4.6.2.10.2.1_Max_TS_BUS
TI_OB-THS-1	Inappropriate reception of Tilting Health Status	TI-10	4.6.2.10.2.2_Max_TS_PAR, 4.6.2.10.2.3_Max_TS_PAR_ALT
TI_OB-THS-2	Inappropriate reception of Tilting Health Status	TI-10	4.6.2.10.2.2_Max_TS_PAR, 4.6.2.10.2.3_Max_TS_PAR_ALT
TI_OB-CD	Inappropriate reception of Cant Deficiency	TI-10	4.6.2.4.1_Cant_Deficiency,4.6.2.10.2.1_Max_TS_BUS
TI_OB-TL	Inappropriate reception of Train Length	TI-10	4.6.2.5.1_Train_Length 4.6.2.12.1_Axle_Load_Category
TI_OB-ALC	Inappropriate reception of Axle Load Category	TI-10	4.6.2.9.1_Axle_Load_Category
TI_OB-TM	Inappropriate reception of Traction Model	TI-10	4.6.2.5.1_ Traction_Model
TI_OB-BM	Inappropriate reception of Brake build up time model and speed dependent	TI-10	4.6.2.7.2.1_Brake_Model_BUS, 4.6.2.7.2.2_Brake_Model_PAR

Event Id.	Hazardous Event Description	Corresponding to FIS event	Reference to FTA
	deceleration model		
TI_OB-SBS	Inappropriate output of Special Brake Status	TI-10	4.6.2.7.2.1_Brake_Model_BUS
TI_OB-SBS-1	Inappropriate output of Special Brake Status	TI-10	4.6.2.7.2.2_Brake_Model_PAR
TI_OB-SBS-2	Inappropriate output of Special Brake Status	TI-10	4.6.2.7.2.2_Brake_Model_PAR
TI_OB-BP	Inappropriate reception or loss of Brake percentage	TI-10	4.6.2.5.1_Brake_Percentage
TI_OB_BPos	Inappropriate reception of Brake position	TI-10	4.6.2.9.2.1_Brake_Pos_BUS
TI_OB-BPos-1.1	Inappropriate reception of Brake position	TI-10	4.6.2.9.2.2_Brake_Pos_PAR
TI_OB-BPos-1.2	Inappropriate reception of Brake position	TI-10	4.6.2.9.2.2_Brake_Pos_PAR
TI_OB-MTS	Inappropriate reception ofLoss of Maximum train speed	TI-10	4.6.2.10.2.1_Max_TS_BUS, 4.6.2.10.2.2_Max_TS_PAR, 4.6.2.10.2.3_Max_TS_PAR_ALT
TI_OB-TCO-1	Loss of TCO signal O_TC1_C on hard-wired output	TI-11	4.4.8.2-0_TCO
TI_OB-TCO-2	Loss of TCO signal OBU_TR_TCO_Cmd on serial bus	TI-11	4.4.8.2-0_TCO

3.9 Hazardous Events Schedule vehicle part

Event Id.	Hazardous Event Description	Reference to FTA
TI_VE-SL-1.1	Inappropriate output of faulty Sleeping signal T_SL_E_N	4.2.1.4.1_SL_PAR
TI_VE-SL-1.2	Inappropriate output of faulty Sleeping signal T_SL_E_I	4.2.1.4.1_SL_PAR
TI_VE-SL-1	Inappropriate output of faulty Sleeping signal T_SL_E	4.2.1.4.2_SL_PAR_ALT and 4.2.1.4.3_SL_BUS_ALT
TI_VE-BUS-1.0	Simple I/O device failure (serial transmission architecture a)	e.g. 4.2.1.4.3_SL_BUS_ALT
TI_VE-BUS-1.1	Simple I/O device 1 failure (serial transmission architecture a)	e.g. 4.2.1.4.4_SL_BUS
TI_VE-BUS-1.2	Simple I/O device 2 failure (serial transmission architecture a)	e.g. 4.2.1.4.4_SL_BUS

Event Id.	Hazardous Event Description	Reference to FTA
TI_VE-BUS-2.0	Bus falsifies first telegram (serial transmission architecture a)	e. g. 4.2.1.4.3_SL_BUS_ALT
TI_VE-BUS-2.1	Bus falsifies first telegram (serial transmission architecture a)	e. g. 4.2.1.4.4_SL_BUS
TI_VE-BUS-2.2	Bus falsifies second telegram (serial transmission architecture a)	e. g. 4.2.1.4.4_SL_BUS
TI_VE-BUS	Bus falsifies telegram undetected (serial transmission architecture b)	-
TI_VE-PS	Inappropriate output of faulty Passive Shunting signal T_PS_E / TR_OBU_PassiveShunting	4.2.2.1_PS_PAR
TI_VE-NL	Inappropriate output of Non Leading signal T_NL_E / TR_OBU_NLEnabled	4.2.3.1_NL_PAR
TI_VE-EB-1	Loss of emergency brake signal O_EB1_C (no brake command received when required)	4.3.3.1-0_EB_Solution1-2, 4.3.3.2_EB_Solution3
TI_VE-EB-2	Loss of emergency brake signal O_EB2_C (solution 1-2) or OBU_TR_EB3_Cmd (solution 3) (brake release command received when not required)	4.3.3.1-0_EB_Solution1-2, 4.3.3.2_EB_Solution3
TI_VE-PD	Inappropriate reception of Station Platform information	-
TI_OB-CS	Wrong Cabin considered as Active due to falsification of both cab status signals T_CS_A / TR_OBU_CabStatusA and T_CS_B / TR_OBU_CabStatusB are falsified at the same time.	4.5.1.1_CS_PAR
TI_VE-DC-1	Loss of direction controller status signal T_FW_S / TR_OBU_DirectionFW	4.5.2.1_DCP_PAR
TI_VE-DC-2	Loss of direction controller status signal T_BW_S / TR_OBU_DirectionBW	No fault tree but equivalent to 4.5.2.1_DCP_PAR
TI_VE-TT	Inappropriate output of Train Type Input	4.6.2.4.1_Cant_Deficiency, 4.6.2.7.2.1_Brake_Model_BUS, 4.6.2.7.2.2_Brake_Model_PAR, 4.6.2.8.1_Brake_Percentage, 4.6.2.6.1_Traction_Model, 4.6.2.9.2.1_Brake_Pos_BUS, 4.6.2.10.2.1_Max_TS_BUS,

Event Id.	Hazardous Event Description	Reference to FTA
		4.6.2.12.1_Axle_Load_Category, 4.6.2.5.1_Train_Length
TI_VE-TC	Inappropriate output of Train Composition Input	4.6.2.4.1_Cant_Deficiency, 4.6.2.7.2.1_Brake_Model_BUS, 4.6.2.7.2.2_Brake_Model_PAR, 4.6.2.8.1_Brake_Percentage, 4.6.2.6.1_Traction_Model, 4.6.2.9.2.1_Brake_Pos_BUS, 4.6.2.10.2.1_Max_TS_BUS, 4.6.2.10.2.2_Max_TS_PAR, 4.6.2.10.2.3_Max_TS_PAR_ALT, 4.6.2.12.1_Axle_Load_Category, 4.6.2.5.1_Train_Length
TI_VE-THS	Inappropriate output of Tilting Health Status	4.6.2.4.1_Cant_Deficiency, 4.6.2.10.2.1_Max_TS_BUS
TI_VE-THS-1	Inappropriate output of Tilting Health Status	4.6.2.10.2.2_Max_TS_PAR, 4.6.2.10.2.3_Max_TS_PAR_ALT
TI_VE-THS-2	Inappropriate output of Tilting Health Status	4.6.2.10.2.2_Max_TS_PAR, 4.6.2.10.2.3_Max_TS_PAR_ALT
TI_VE-CD	Inappropriate output of Cant Deficiency	4.6.2.4.1_Cant_Deficiency,4.6.2.10.2.1_Max_TS_BUS
TI_VE-TL	Inappropriate output of Train lLength	4.6.2.5.1_Train_Length
TI_VE-ALC	Inappropriate output of Axle Load Category	4.6.2.12.1_Axle_Load_Category
TI_VE-TM	Inappropriate output of Traction Model	4.6.2.6.1_Traction_Model
TI_VE-BM	Inappropriate output of Brake build up time model and speed dependent deceleration model	4.6.2.7.2.1_Brake_Model_BUS, 4.6.2.7.2.2_Brake_Model_PAR
TI_VE-SBS	Inappropriate output of Special Brake Status	4.6.2.7.2.1_Brake_Model_BUS
TI_VE-SBS-1	Inappropriate output of Special Brake Status	4.6.2.7.2.2_Brake_Model_PAR
TI_VE-SBS-2	Inappropriate output of Special Brake Status	4.6.2.7.2.2_Brake_Model_PAR
TI_VE-BP	Inappropriate output or loss of Brake percentage	4.6.2.5.1_Brake_Percentage
TI_VE_BPos	Inappropriate output of Brake position	4.6.2.9.2.1_Brake_Pos_BUS
TI_VE-BPos-1.1	Inappropriate output of Brake position	4.6.2.9.2.2_Brake_Pos_PAR

Event Id.	Hazardous Event Description	Reference to FTA
TI_VE-BPos-1.2	Inappropriate output of Brake position	4.6.2.9.2.2_Brake_Pos_PAR
TI_VE-MTS	Inappropriate output or Loss of Maximum train speed	4.6.2.10.2.1_Max_TS_BUS, 4.6.2.10.2.2_Max_TS_PAR, 4.6.2.10.2.3_Max_TS_PAR_ALT
TI_VE-TCO-1	Loss of TCO signal O_TC1_C on hard-wired output	4.4.8.2-0_TCO
TI_VE-TCO-2	Loss of TCO signal OBU_TR_TCO_Cmd on serial bus	4.4.8.2-0_TCO

4. MULTIPLE FAULTS EFFECTS DESCRIPTION

4.1 General

4.1.1.1 The intention of this chapter is to explain the TIU-related hazards, barriers and conditions of the fault trees included in annex A, 6.2.

4.1.1.2 In all cases when a driver action is considered as barrier in a fault tree the driver error is modelled as a probability.

4.2 Description of the Fault Effects of Mode Control

4.2.1 Sleeping

4.2.1.1 Each single failure will be detected but safe reaction will be triggered not before standstill.

4.2.1.2 Assumptions of the cases considered in the fault trees:

- All cabs are closed (e.g. because the driver wanted to enter to mode SB from any mode or the driver wants to change the cab).
- ETCS mode is Stand-By.
- Vehicle is standing still.
- Vehicle is on a slope or there is heavy wind.

4.2.1.3 Barriers

Event	Explanation
E-ext-SPV	The vehicle is in charge to ensure the standstill. Before closing all the cabs, the vehicle has been obviously braked. To roll away the brakes have to be released which is assumed with a frequency of 1E-5 /h. Standstill information from ETCS odometer is only a mitigation for vehicle running but not for the described case of standstill.
E-ext-SPD	The driver or the vehicle is in charge to ensure the standstill (e.g. brakes applied). Before closing the cabs, the vehicle has been obviously braked. To roll away the brake would have been released already which is assumed with an unavailability of 1E-3. Standstill information from ETCS odometer is only a mitigation for vehicle running but not for the described case of standstill.

4.2.1.4 TIU-related hazards

4.2.1.4.1 Fault tree for the case of hard-wired interface with two sleeping signals (4.2.1.4.1_SL_PAR)

Gate	Explanation
G-SL-2	A failure leads to inappropriate transition to mode SL, only if there are two failures (T_SL_E_N and T_SL_E_I) at the same time. The antivalent sleeping signals T_SL_E_N and T_SL_E_I must be input from two sources in the vehicle. If this is not provided 4.2.1.4.2_SL_PAR_ALT is an alternative solution with only one sleeping signal and a standstill protection on vehicle side (E-ext-SPV), i.e. an ERTMS/ETCS on-board equipment independent system is in charge to ensure the standstill. Preconditions: Vehicle is at standstill AND all desks connected to the ERTMS/ETCS on-board equipment are closed (Subset-026, 4.6.3, [14]).

4.2.1.4.2 Fault tree for the case of hard-wired interface with one sleeping signal (4.2.1.4.2_SL_PAR_ALT)

Gate	Explanation
G-SL-7	A failure leads to inappropriate transition to mode SL, if there is a failure of T_SL_E. Preconditions: Vehicle is at standstill AND all desks connected to the ERTMS/ETCS on-board equipment are closed (Subset-026, 4.6.3, [14]).

4.2.1.4.3 Fault tree for the case of serial interface with one sleeping signal (4.2.1.4.3_SL_BUS_ALT)

Gate	Explanation
G-SL-9	A failure leads to inappropriate transition to mode SL, if there is a failure in the source of the sleeping signal TI_VE-SL-1, if there is a failure in the simple I/O device (TI_VE-BUS-1.0), if there is an undetected failure due to the performance of the transmission code (TI_VE-BUS-2.0): Preconditions: Vehicle is at standstill AND all desks connected to the ERTMS/ETCS on-board equipment are closed (Subset-026, 4.6.3, [14]). It can be neglected that other bus partners send wrong information. E.g. for MVB a reasoning could be that due to the functionality of MVB the following conditions would have to be fulfilled: • An unknown bus partner has to generate a complete and valid Slave Frame

Gate	Explanation
	(including checksum). • This slave frame has to be sent directly after the master frame was sent but before the slave frame of the answering simple I/O device. • The slave frame has to contain the identification of the addressed I/O device. • These failure combinations must succeed over two successive cycles. During this time failures must not have the effect that the bus communication is stopped (e.g. as in case of permanent wrong sending). Those failures cannot be excluded, in general. But they can be neglected in comparison to the other considered failures.

4.2.1.4.4 Fault tree for the case of serial interface with two sleeping signals (4.2.1.4.4_SL_BUS)

Gate	Explanation
G-SL-4.1	A failure leads to inappropriate transition to mode SL, only if there are two other failures at the same time: The first failure is depicted with G-SL-1.0 and the second one with G-SL-2.0. Preconditions: Vehicle is at standstill AND all desks connected to the ERTMS/ETCS on-board equipment are closed (Subset-026, 4.6.3, [14]). It can be neglected that other bus partners send wrong information. E.g. for MVB a reasoning could be that due to the functionality of MVB the following conditions would have to be fulfilled: • An unknown bus partner has to generate a complete and valid Slave Frame (including checksum). • This slave frame has to be sent directly after the master frame was sent but before the slave frame of the answering simple I/O device. • The slave frame has to contain the identification of the addressed I/O device. • These failure combinations must succeed over two successive cycles. During this time failures must not have the effect that the bus communication is stopped (e.g. as in case of permanent wrong sending). Those failures cannot be excluded, in general. But they can be neglected in comparison to the other considered failures. The simple I/O devices are separate physical components. The common influence by power supply and environmental conditions do not have to be considered because a similar falsification of telegrams does not have to be assumed due to these influences. Simple I/O devices are physically connected. Therefore possible common cause failures are considered with the β-factor according to IEC 61508-6.

4.2.1.4.5 Fault tree for hard-wired and serial interface (4.2.1.4.1_SL_PAR, 4.2.1.4.2_SL_PAR_ALT and 4.2.1.4.3_SL_BUS_ALT)

Gate	Explanation
G-SL-1 / G-SL-6 / G-SL-8	If the responsibility is on ETCS only, then two sleeping signals would be needed due to no single fault must lead to a hazard. With the additional technical barrier E-ext-SPV it is also fulfilled with one sleeping signal T_SL_E that no single fault leads to a hazard.
4.2.1.4.3_SL_BUS_ALT / 4.2.1.4.1_SL_PAR / 4.2.1.4.2_SL_PAR_ALT / 4.2.1.4.4_SL_BUS	Loss of standstill without driver on-board is a hazard which is not inherent to ETCS and was addressed previously with specific means which are still applicable. ETCS OBU is not able to improve the safety level of the “sleeping status” provided by the vehicle. Indeed the hazard rates of the TOP events 4.2.1.4.1_SL_PAR, 4.2.1.4.3_SL_BUS_ALT and 4.2.1.4.2_SL_PAR_ALT are directly resulting from the “sleeping status” provided by the vehicle. Therefore the THR of the ETCS Core Hazard does not have to be reached and it is sufficient that the initial end effect “exceedance of the safe speed because of failure in SL” is in the range of SIL4.

4.2.2 Passive shunting

4.2.2.1 Fault tree for the hard-wired interface (4.2.2.1_PS_PAR)

4.2.2.1.1 Safe reaction will be triggered immediately in case of single failure detection at passive shunting input signal. Other safety-related faults will be stored on-board until the vehicle leaves the PS mode (compare Subset-026, 4.4.20.1.6 and 4.4.20.1.10).

4.2.2.1.2 Preconditions of the considered case in the fault tree:

- Vehicle is standing still.
- Vehicle is on a slope.
- ETCS mode is Shunting.
- Cabs are closed after all the conditions are fulfilled (Subset-026, 4.6.3, [26]).

4.2.2.1.3 Barriers

Event	Explanation
E-ext-SPD	If no Cab is occupied the driver or the vehicle is in charge to ensure the standstill (e.g. brakes applied). Before closing the cabs, the vehicle has been obviously braked. To

Event	Explanation
	roll away the brake would have been released already which is assumed with an unavailability of 1E-3. Standstill information from ETCS odometer is only a mitigation for vehicle running but not for the described case of standstill.
MMI-1a	False acknowledgement of mode change to less restrictive mode (compare Subset-091). As a second failure there can be a driver request PS mode mistimed or a DMI failure. It is assumed that a conservatively failure rate of DMI is FR = 1E-5 /h with FDT=48 h. Fault of the driver input to DMI is neglected in the fault tree.
E-ext-DPS	Driver erroneously commands the transition to mode PS. Driver interaction failure with a frequency of 1E-3 is assumed as worst case.

4.2.2.1.4 TIU-related hazards

Gate	Explanation
G-PS-2	A failure leads to inappropriate transition to mode PS, only if there are three failures at the same time: - Passive Shunting signal T_PS_E / TR_OBU_PassiveShunting failure. - Loss of external standstill protection (driver or vehicle does not ensure the standstill before leaving the cab). - DMI failure. Information from the DMI is necessary to change to Mode PS. Therefore DMI failure leads unwanted to change to Mode PS so that there is no more movement protection.

4.2.3 Non Leading

4.2.3.1 Fault tree for the hard-wired interface (4.2.3.1_NL_PAR)

4.2.3.1.1 Assumptions of the cases considered in the fault trees:

- Vehicle is standing still.
- Vehicle is on a slope.
- ETCS mode is SB, SH, FS, LS, SR or OS

4.2.3.1.2 Barriers

Event	Explanation
E-ext-MDD	Driver does not realise the new mode displayed on DMI. Driver interaction failure with a unavailability of 1E-3 is assumed as worst case.

Event	Explanation
MMI-1b	False command to enter Non Leading mode (compare Subset-091). As a second failure there can be a driver request NL mode mistimed or a DMI failure. It is assumed that a conservatively failure rate of DMI is FR = 1E-5 /h with FDT=48 h. Fault of the driver input to DMI is neglected in the fault tree.
E-ext-DNL	Driver erroneously commands to enter NL mode. Driver interaction failure with a frequency of 1E-3 is assumed as worst case.

4.2.3.1.3 TIU-related hazards

Gate	Explanation
G-NL-2	A failure leads to inappropriate transition to mode NL, only if there are three failures at the same time so that there is no more movement protection: - Non Leading signal T_NL_E / TR_OBU_NLEnabled failure. - Driver does not realise of the new mode displayed on the DMI. - DMI failure leads to unwanted change to NL mode.

4.2.4 Isolation

4.2.4.1 Multiple failures have no effect in the system because another train protection system supervises the vehicle movement.

4.2.4.2 The driver knows when the OBU is isolated and it can be ensured that the driver will be informed of the isolation mode.

4.3 Description of the Fault Effects of Control of Brakes

4.3.1 Service brake command

4.3.1.1 Under the assumption described in clause 5.1.4.1.1 multiple failures have no effect in the system.

4.3.2 Brake pressure

4.3.2.1 Multiple failures have no effect in the system.

4.3.3 Emergency brake command

4.3.3.1 Fault tree for the case of hard-wired interface (4.3.3.1-0_EB_Solution1-2)

4.3.3.1.1 TIU-related hazards

Gate	Explanation
G-EB-1	A failure leads to EB command failure, only if there are two failures for loss of emergency brake signal (O_EB1_C and O_EB2_C) at the same time. The signals O_EB1_C and O_EB2_C must be output physically independent. The independence has to be shown in the project safety cases according to the valid standards. If necessary a beta factor has to be used in calculation or/and better TFRs have to be used for TI_OB-EB-1 and TI_OB-EB-2. The signals O_EB1_C and O_EB2_C must be processed in the vehicle with independence as required by TSI Loc&Pas, section 4.2.4.4.1.

4.3.3.1.2 Note: According to TSI Loc&Pas, safety target for EB on the vehicle side shall reach the tolerable hazard rate of 1E-09 per hour, which is lower than ETCS Core Hazard related to the ETCS on-board unit. According to the FTAs 4.3.3.1.2_OBU-EB and 4.3.3.1.2_VEHICLE-EB both values are reached.

4.3.3.2 Fault tree for the case of solution 3 (combined hard-wired and serial interface – 4.3.3.2_EB_Solution3)

4.3.3.2.1 There shall be only a serial EB output as a redundant output in combination with a hard-wired EB output.

4.3.3.2.2 TIU-related hazards

Gate	Explanation
G-EB3-1	A failure leads to EB command failure, only if there are two failures for loss of emergency brake signal (O_EB1_C and OBU_TR_EB3_C) at the same time. The signals O_EB1_C and OBU_TR_EB3_Cmd are output physically independent on hard-wired and on serial interface (diverse output). The signals O_EB1_C and OBU_TR_EB3_Cmd must be processed in the vehicle with independence as required by TSI Loc&Pas section 4.2.4.4.1.

4.3.4 Special brake inhibition area – Trackside orders

4.3.4.1 Under the assumption described in 5.1.4.4.2 multiple failures have no effect in the system.

4.3.5 Special brake inhibit – STM orders

4.3.5.1 Analysis is national system specific.

4.3.6 Special brake status

4.3.6.1 If vehicle is equipped with special brakes the special brake status can be relevant to calculate the brake model, see 5.1.4.6.

4.3.6.2 If vehicle is not equipped with special brakes, no failure may arise.

4.3.7 Additional brake status

4.3.7.1 See 5.1.4.7.1.

4.4 Description of the Fault Effects of Control of Train Functions

4.4.1 Change of traction system

4.4.1.1 Multiple failures have no effect in the system.

4.4.2 Powerless section with pantograph to be lowered – Trackside orders / Pantograph – STM orders

4.4.2.1 Multiple failures have no effect in the system.

4.4.3 Air tightness area – Trackside orders / Air tightness – STM orders

4.4.3.1 Under consideration of the exported constraint specified in 5.1.5.3.2 multiple failures have no effect in the system.

4.4.4 Station platform

4.4.4.1 Multiple failure analysis is project specific, see 5.1.5.4.

4.4.5 Powerless section with main power switch to be switched off – Trackside orders

4.4.5.1 Multiple failures have no effect in the system.

4.4.6 Main power switch – STM orders

4.4.6.1 Multiple failures have no effect in the system.

4.4.7 Change of allowed current consumption

4.4.7.1 Multiple failures have no effect in the system.

4.4.8 Traction Cut Off

4.4.8.1 TCO with hard-wired output O_TC1_C and serial output OBU_TR_TCO_Cmd allows a safe TCO affecting the braking curves (failure to cut the traction when EBI is exceeded). Fault tree for this case (FTA 4.4.8.2-0_TCO):

4.4.8.2 TIU-related hazards

Gate	Explanation
G-TCO-2.1, G-TCO-2.2	A failure leads to TCO command failure only if there are two failures for loss of TCO signal (O_TC1_C hard-wired and O_TC2_C serial) at the same time. The failure rate of the on-board part must be a part of the ETCS Core Hazard (6,7 E-10 /h) which is fulfilled according to the FTA 4.4.8.2-1_OBU-TCO. The signals O_TC1_C hard-wired and O_TC2_C serial must be output physically independent which is fulfilled due to the diversity of the output paths.

4.5 Description of the Fault Effects of Train Status Information

4.5.1 Cab status

4.5.1.1 Fault tree for the hard-wired interface (4.5.1.1_CS_PAR)

4.5.1.2 Single failures have no safety-related effect in the system; compare FMEA in Annex A, 6.1. Therefore it can be assumed that the first single failure of one of the two individual inputs is detected by ETCS and reaction is applied since cab A active /cab B active is a not admitted condition. But in addition to this consideration there is the following multiple failure analysis.

4.5.1.2.1 Assumption of the cases considered in the fault tree:

4.5.1.2.1.1 Mitigation condition according to analysis of KERNEL15 in Subset-088: MA points in the allowed direction.

4.5.1.2.1.2 Modes: All expect NP, SF and IS, see analysis of KERNEL15 in Subset-088.

4.5.1.2.2 Barriers

Event	Explanation
E-ext-IL	According to Subset-088 an exported condition against incorrect cab status is that the interlocking must protect against track occupancy and there must be appropriate

Event	Explanation
	operational rules. The interlocking system is designed as a safe system with an appropriate failure rate.

4.5.1.2.3 TIU-related hazards

Gate	Explanation
G-CS-1	The wrong desk reported open resulting in incorrect train position is reported to Trackside due to a multiple fault of T_CS_A / TR_OBU_CabStatusA = 1 and T_CS B / TR_OBU_CabStatusB = 0 fails to T_CS_A / TR_OBU_CabStatusA = 0 and T_CS B / TR_OBU_CabStatusB = 1, or vice versa.

4.5.2 Direction Controller status

4.5.2.1 Fault tree for the hard-wired interface (4.5.2.1_DCP_PAR)

4.5.2.1.1 Assumption of the cases considered in the fault tree:

Vehicle is on a downhill slope (T_FW_S / TR_OBU_DirectionFW failure is relevant for downhill slope and T_BW_S is not considered due to relevant for uphill only).

4.5.2.1.2 Barriers

Event	Explanation
E-ext-RP	The vehicle is in charge to ensure the roll away protection (e.g. brakes applied safely). Driver interaction failure with a frequency of 1E-3 is assumed as worst case. Standstill information from ETCS odometer is only a mitigation for vehicle running but not for the described case of standstill.
E-ext-DS	Driver's activity control function is supported by Fail-safe Dead-Man Supervision (TSI Loc Pas, chapter 4.2.9.3.1).

4.5.2.1.3 TIU-related hazards

Gate	Explanation
G-DCP-1	A single failure of the Direction Controller signals could lead to the direction controller information "no direction (neutral)" (coding T_FW_S / TR_OBU_DirectionFW = 0 and T_BW_S / TR_OBU_DirectionBW = 0) and consequently to loss of vehicle roll away protection.

4.5.3 Train integrity

4.5.3.1 To be harmonized.

4.5.4 Traction Status

4.5.4.1 The traction status is forwarded to the STM. The information related to STMs is seen as out of scope of this safety analysis focusing on level 1 and level 2 aspects."

4.5.5 Set Speed

4.5.5.1 Multiple failures have no effect in the system.

4.6 Description of the Hazardous Events of Train Data

4.6.1 Type of train data entry

4.6.1.1 Multiple failures have no effect in the system.

4.6.2 Train data information

4.6.2.1 Train Composition

4.6.2.1.1 Train composition failure effects are considered in train data information effects where they could contribute.

4.6.2.2 Train Type

4.6.2.2.1 Train type failure effects are considered in train data information effects where they could contribute.

4.6.2.3 Tilting Health Status

4.6.2.3.1 Tilting health status failure effects are considered in train data information effects where they could contribute.

4.6.2.4 Train category / Cant deficiency

4.6.2.4.1 Fault tree 4.6.2.4.1_Cant_Deficiency4.6.2.4.1_Cant_Deficiency

4.6.2.4.2 Barriers

Event	Explanation
E-ext-D-TDE	Driver erroneously validated the train data element. Driver interaction failure with a frequency of 1E-3 is assumed as worst case.

4.6.2.4.3 TIU-related hazards

Gate	Explanation
G-CD-1, G-CD-2	Inappropriate cant deficiency information (higher than real Cant Deficiency is assumed) can lead to an error in on-board evaluation of SSPs.

4.6.2.5 Train length

4.6.2.5.1 Tault tree Fault tree 4.6.2.5.1_Train_Length

4.6.2.5.2 Barriers

Event	Explanation
E-ext-D-TDE	Driver erroneously validated the train data element. Driver interaction failure with a frequency of 1E-3 is assumed as worst case.

4.6.2.5.3 TIU-related hazards

Gate	Explanation
G-TL-1, G-TL-2	Inappropriate train length information can lead to an error in supervision of SSPs and TSRs and a wrong brake build up time could be calculated.

4.6.2.6 Traction model

4.6.2.6.1 Tault tree 4.6.2.6.1_Traction_Model

4.6.2.6.2 Barriers

Event	Explanation
E-ext-D-TDE	Driver erroneously validated the train data element. Driver interaction failure with a frequency of 1E-3 is assumed as worst case.

4.6.2.6.3 TIU-related hazards

Gate	Explanation
G-TM-1, G-TM-2	Incorrect determination of time delay T_traction_cut_off value. As a consequence Traction cut-off command is triggered untimely.

4.6.2.7 Brake build up time model and Speed dependent deceleration model

4.6.2.7.1.1 Barriers

Event	Explanation
E-ext-D-TDE	Driver erroneously validated the train data element. Driver interaction failure with a frequency of 1E-3 is assumed as worst case.

4.6.2.7.2 TIU-related hazards

4.6.2.7.2.1 Fault tree for the use of serial interface, only (FTA 4.6.2.7.2.1_Brake_Model_BUS).

Gate	Explanation
G-TBE-1	Incorrect determination of time delay T_traction_cut_off value. As a consequence Traction cut-off command is triggered untimely.

4.6.2.7.2.2 Fault tree with special brakes on hard-wired interface (FTA 4.6.2.7.2.2_Brake_Model_PAR).

Gate	Explanation
G-TBE-1, G-TBE-2	Incorrect determination of time delay T_traction_cut_off value. As a consequence Traction cut-off command is triggered untimely.
G-TBE-4	In order to reach the required safety level 2 signals are needed which together provides an FR = 1E-7 /h for the status of the special brakes.

4.6.2.8 Brake Percentage

4.6.2.8.1 Fault tree 4.6.2.8.1_Brake_Percentage

4.6.2.8.1.1 Barriers

Event	Explanation
E-ext-D-TDE	Driver erroneously validated the train data element. Driver interaction failure with a frequency of 1E-3 is assumed as worst case.

4.6.2.8.1.2 TIU-related hazards

Gate	Explanation
G-BP-1	Wrong values of A_brake_emergency(V) and T_brake_emergency are derived from a a wrong brake percentage. As a consequence a conversion model is used although it is not suitable (see Subset-026, §3.13.3.2.1). Therefore a failure could lead to faulty EB curve calculation. In addition a wrong brake percentage can lead to a wrong speed dependent deceleration model which can be calculated by applying the conversion model to the brake percentage value.

4.6.2.9 Brake Position

4.6.2.9.1 Barriers

Event	Explanation
E-ext-D-TDE	Driver erroneously validated the train data element. Driver interaction failure with a frequency of 1E-3 is assumed as worst case.

4.6.2.9.2 TIU-related hazards

4.6.2.9.2.1 Fault tree for serial interface (4.6.2.9.2.1_Brake_Pos_BUS)

Gate	Explanation
G-BPos-3, G-BPos-4	Inappropriate output of Brake Position information can lead to assumptions of the wrong train type and as a consequence of a wrong kinematic behaviour of the train after a an emergency brake command has been initiated. As a consequence a conversion model is used although it is not suitable (see Subset-026, §3.13.3.2.1). Therefore a failure could lead to faulty EB curve calculation. In addition a wrong brake position can lead to a wrong brake build up time.

4.6.2.9.2.2 Fault tree for hard-wired interface (4.6.2.9.2.2_Brake_Pos_PAR)

Gate	Explanation
G-BPos-1	Inappropriate output of Brake Position information can lead to assumptions of the wrong train type and as a consequence of a wrong kinematic behaviour of the train after a an emergency brake command has been initiated. As a consequence a conversion model is used although it is not suitable (see Subset-026, §3.13.3.2.1). Therefore a failure could lead to faulty EB curve calculation.
G-BPos-2.1 / G-BPos-2.2	The coding of brake position requires two signals for brake position information. In order to reach the required safety level four signals are needed..

4.6.2.9.3 Nominal rotating mass

4.6.2.9.3.1 Multiple failures have no safety-related effect in the system.

4.6.2.10 Maximum Train Speed

4.6.2.10.1 Barriers

Event	Explanation
E-ext-D-TDE	Driver erroneously validated the train data element. Driver interaction failure with a frequency of 1E-3 is assumed as worst case.

4.6.2.10.2 TIU-related hazards

4.6.2.10.2.1 Fault tree for the case of serial interface only (FTA 4.6.2.10.2.1_Max_TS_BUS)

Gate	Explanation
G-MTS-1	The Most Restrictive Speed Profile (MRSP) could be wrongly determined (see SS-026 §3.13.7.2) due to a wrong maximum train speed. As a consequence ceiling supervision limits could be wrong.

4.6.2.10.2.2 Fault tree for the case of serial interface with one tilting health status signal on hard-wired interface (FTA 4.6.2.10.2.2_Max_TS_PAR)

Gate	Explanation
G-MTS-2, G-MTS-3	The Most Restrictive Speed Profile (MRSP) could be wrongly determined (see SS-026 §3.13.7.2) due to a wrong maximum train speed. As a consequence ceiling supervision limits could be wrong.
G-MTS-4	With only one tilting health status signal (FR = 1E-05 /h) the influence of an inappropriate output or reception of Tilting Health Status is too high on G-MTS-2 and as a consequence on the hazardous situation.

4.6.2.10.2.3 Fault tree for the case of serial interface with two tilting health status signal on hard-wired interface (FTA 4.6.2.10.2.3_Max_TS_PAR_ALT)

Gate	Explanation
G-MTS-5, G-MTS-3	The Most Restrictive Speed Profile (MRSP) could be wrongly determined (see SS-026 §3.13.7.2) due to a wrong maximum train speed. As a consequence ceiling supervision limits could be wrong.
G-MTS-6	This is an AND combination of the failure of two tilting health status signals. With two signals (FR = 1E-05 /h) the influence of an inappropriate output or reception of Tilting Health Status is on G-MTS-5 is tolerable.

4.6.2.11 Loading gauge

4.6.2.11.1 Under the assumptions/conditions specified in 5.1.7.2.10.3 and 5.1.7.2.10.4 multiple failures have no safety-related effect in the system.

4.6.2.12 Axle load category

4.6.2.12.1 Fault tree 4.6.2.12.1_Axle_Load_Category

4.6.2.12.1.1 Barriers

Event	Explanation
E-ext-D-TDE	Driver erroneously validated the train data element. Driver interaction failure with a frequency of 1E-3 is assumed as worst case.

4.6.2.12.1.2 TIU-related hazards

Gate	Explanation
G-AL-1	A failure could lead to the incident that a train enters a route although it is not suitable for this train.

4.6.2.13 Traction system(s) accepted by the engine

4.6.2.13.1 Multiple failures have no safety-related effect in the system.

4.6.2.14 Train fitted with airtight system

4.6.2.14.1 Under consideration of the exported constraint specified in 5.1.7.2.13.3 multiple failures have no safety-related effect in the system.

4.7 Description of the Fault Effects of National System Isolation

4.7.1 National System Isolation

4.7.1.1 This is level NTC only which is seen as out of scope of this safety analysis focusing on level 1 and level 2 aspects.

5. CONCLUSIONS: REQUIREMENTS FOR TI

5.1 Interface Requirements

5.1.1 General Considerations

5.1.1.1 In this chapter TFR values are required depending on certain FDT values and in some cases on certain common cause factors. Also other values can be used in project specific safety cases as long as the quantitative analysis (with the Fault Trees given in this Subset) demonstrates that the THR of the ETCS Core Hazard and the quantitative requirements of TSI Loc&Pas are reached.

5.1.2 Periodic Self Tests

5.1.2.1 If an FDT is required in section 5.1 it has to be shown project specific that an adequate measure is implemented for fault detection on the respective interface side (ERTMS/ETCS on-board equipment or vehicle).

5.1.2.2 Exported constraints to the ERTMS/ETCS on-board equipment: The ERTMS/ETCS on-board equipment shall ensure periodical self-tests according to the FDT specified for the different functions. If the ERTMS/ETCS on-board equipment cannot perform the technical solution there shall be an exported constraint to the vehicle.

5.1.2.3 Exported constraints to the vehicle: The vehicle shall ensure periodical self-tests according to the FDT specified for the different functions. If the vehicle cannot perform the technical solution there shall be an exported constraint to the operation.

5.1.3 Signals for Mode Control

5.1.3.1 Sleeping

5.1.3.1.1 Requirements for ERTMS/ETCS on-board equipment:

5.1.3.1.1.1 In case of a failure (inappropriate reception of faulty antivalent Sleeping signal / loss of Sleeping signal) ERTMS/ETCS on-board equipment shall memorize the fault.

5.1.3.1.1.2 ERTMS/ETCS on-board shall not be able to switch to SL mode as long as a failure (inappropriate reception of faulty antivalent Sleeping signal / loss of Sleeping signal) is memorized.

5.1.3.1.1.3 The alternative reaction is the transition to SF mode in case of the failure.

5.1.3.1.1.4 TFR of T_SL_E_N / TR_OBU_TrainSleep erroneously takes the value ‘Sleeping requested’: 1E-05 /h

5.1.3.1.1.5 TFR of T_SL_E_I / TR_OBU_TrainSleep_Not erroneously takes the value ‘Sleeping requested’: 1E-05 /h

5.1.3.1.1.6 FDT = 1 min

5.1.3.1.2 Requirements for vehicle:

5.1.3.1.2.1 TFR of T_SL_E_N / TR_OBU_TrainSleep erroneously takes the value ‘Sleeping requested’: 1E-05 /h

5.1.3.1.2.2 TFR of T_SL_E_I / TR_OBU_TrainSleep_Not erroneously takes the value ‘Sleeping requested’: 1E-05 /h

5.1.3.1.2.3 FDT = 48 h

5.1.3.1.3 Exported constraints to the ERTMS/ETCS on-board equipment: The antivalent sleeping signals shall be read independently according to EN50129.

5.1.3.1.4 Exported constraint to the vehicle: The antivalent sleeping signals shall have two sources (common cause failures considered with 10%).

5.1.3.1.5 Exported constraint to the vehicle or operation: In the case of vehicle is at standstill and all desks connected to the ERTMS/ETCS on-board equipment are closed, an ERTMS/ETCS on-board equipment independent system is in charge to ensure the standstill (e.g. the driver applied brakes) or a desk connected to another ERTMS/ETCS on-board equipment is open.

5.1.3.2 Passive shunting

5.1.3.2.1 Requirements for ERTMS/ETCS on-board equipment:

5.1.3.2.1.1 TFR of T_PS_E / TR_OBU_PassiveShunting erroneously takes the value ‘Passive Shunting permitted’: 1E-05 /h

5.1.3.2.1.2 FDT = 48 h

5.1.3.2.2 Requirements for vehicle:

5.1.3.2.2.1 TFR of T_PS_E / TR_OBU_PassiveShunting erroneously takes the value ‘Passive Shunting permitted’: 1E-05 /h

5.1.3.2.2.2 FDT = 48 h

5.1.3.2.3 Exported constraint to the vehicle or operation: In the case of vehicle is at standstill and all desks connected to the ERTMS/ETCS on-board equipment are closed, an ERTMS/ETCS on-board equipment independent function is in charge to ensure the standstill.

5.1.3.3 Non Leading

5.1.3.3.1 Requirements for ERTMS/ETCS on-board equipment:

5.1.3.3.1.1 TFR of T_NL_E / TR_OBU_NLEnabled erroneously takes the value ‘Non-Leading permitted’: 1E-05 /h

5.1.3.3.1.2 FDT = 48 h

5.1.3.3.2 Requirements for vehicle:

5.1.3.3.2.1 TFR of T_NL_E / TR_OBU_NLEnabled erroneously takes the value ‘Non-Leading permitted’: 1E-05 /h

5.1.3.3.2.2 FDT = 48 h

5.1.3.4 Isolation

5.1.3.4.1 O_IS_S is not safety-related.

5.1.3.4.2 Assumption: This signal is not used for safety purposes e.g. it is not used to isolate the ERTMS/ETCS on-board from brakes.

5.1.4 Signals for the Control of Brakes

5.1.4.1 Service brake command

5.1.4.1.1 O_SB_C / OBU_TR_ServiceBrake is not safety-related if the ETCS On-board is not implemented to use Service Brake to protect the train against undesirable movements. If it is, a more detailed safety analysis is needed in order to show that a failure of this signal is recognized and the EB is applied as safeguarding.

5.1.4.2 Brake pressure

5.1.4.2.1 TR_OBU_BrakePressure is not safety-related.

5.1.4.2.2 If the ETCS On-board is implemented using Service Brake to protect the train against undesirable movements and the Brake Pressure signal is used as Service Brake feedback, then a project specific safety analysis is needed.

5.1.4.3 Emergency brake command

5.1.4.3.1 Solution 1:

5.1.4.3.1.1 Requirements for ERTMS/ETCS on-board equipment:

5.1.4.3.1.1.1 TFR of O_EB1_C_1 and O_EB1_C_2 erroneously take the value ‘EB not commanded: 3E-06 /h (compare note in §4.3.3.1.2.)

5.1.4.3.1.1.2 TFR of O_EB2_C_1 and O_EB2_C_2 erroneously take the value ‘EB not commanded’: 3E-06 /h (compare note in §4.3.3.1.2.)

5.1.4.3.1.1.3 The two EB signals O_EB1_C_1 and O_EB1_C_2 on the one hand must be output physically independent according to EN 50129 from O_EB2_C_1 and O_EB2_C_2 on the other hand.

5.1.4.3.1.1.4 FDT = 48 h

5.1.4.3.1.2 Requirements for vehicle:

5.1.4.3.1.2.1 TFR of O_EB1_C_1 and O_EB1_C_2 erroneously take the value ‘EB not commanded’: 1E-07 /h

5.1.4.3.1.2.2 TFR of O_EB2_C_1 and O_EB2_C_2 erroneously take the value ‘EB not commanded’: 1E-07 /h

5.1.4.3.1.2.3 FDT = 48 h

5.1.4.3.1.3 Exported constraint to the operator: FDT = 48 h.

5.1.4.3.1.4 Exported constraint to the vehicle: The emergency brake signals O_EB1_C_1 and O_EB1_C_2 on the one hand shall be independent from O_EB2_C_1 and O_EB2_C_2 on the other hand (common cause failures considered with 1%).

5.1.4.3.2 Solution 2:

5.1.4.3.2.1 Requirements for ERTMS/ETCS on-board equipment:

5.1.4.3.2.1.1 TFR of O_EB1_C erroneously takes the value ‘EB not commanded’: 3E-06 /h (compare note in §4.3.3.1.2.)

5.1.4.3.2.1.2 TFR of O_EB2_C erroneously takes the value ‘EB not commanded’: 3E-06 /h (compare note in §4.3.3.1.2.)

5.1.4.3.2.1.3 The two EB signals O_EB1_C and O_EB2_C must be output physically independently according to EN 50129.

5.1.4.3.2.1.4 FDT = 48 h

5.1.4.3.2.2 Requirements for vehicle:

5.1.4.3.2.2.1 TFR of O_EB1_C erroneously takes the value ‘EB not commanded’: 1E-07 /h

5.1.4.3.2.2.2 TFR of O_EB2_C erroneously takes the value ‘EB not commanded’: 1E-07 /h

5.1.4.3.2.2.3 FDT = 48 h

5.1.4.3.2.3 Exported constraint to the operator: FDT = 48 h.

5.1.4.3.2.4 Exported constraint to the vehicle: The emergency brake signals O_EB1_C and O_EB2_C shall be independent (common cause failures considered with 1%).

5.1.4.3.3 Solution 3:

5.1.4.3.3.1 Requirements for ERTMS/ETCS on-board equipment:

5.1.4.3.3.1.1 TFR of O_EB1_C erroneously takes the value ‘EB not commanded’: 3E-06 /h

5.1.4.3.3.1.2 TFR of OBU_TR_EB3_Cmd erroneously takes the value ‘EB not commanded’: 1E-7 /h, serial communication of OBU_TR_EB3_Cmd has to be SIL2, i.e. 1E-07 /h ≤ THR < 1E-06 /h

5.1.4.3.3.1.3 FDT = 48 h

5.1.4.3.3.2 Requirements for vehicle:

5.1.4.3.3.2.1 TFR of O_EB1_C erroneously takes the value ‘EB not commanded’: 3E-06 /h

5.1.4.3.3.2.2 TFR of OBU_TR_EB3_Cmd erroneously takes the value ‘EB not commanded’: 1E-07 /h, serial communication of OBU_TR_EB3_Cmd has to be SIL2, i.e. 1E-07 /h ≤ THR < 1E-06 /h

5.1.4.3.3.2.3 FDT = 48 h

5.1.4.3.3.2.4 SIL for TCMS (incl. brake control or other electronic devices): SIL 2, i.e. 1E-07 /h ≤ THR < 1E-06 /h

5.1.4.3.3.3 Exported constraint to the operator: FDT = 48 h.

5.1.4.3.3.4 Exported constraint to the vehicle: The emergency brake signals O_EB1_C and OBU_TR_EB3_Cmd shall be processed in the vehicle with independence as required by TSI Loc&Pas, section 4.2.4.4.1..

5.1.4.4 Special brake inhibition area – Trackside orders

5.1.4.4.1 OBU_TR_RBI_D_Entry, OBU_TR_RBI_D_Exit, OBU_TR_MGI_D_Entry, OBU_TR_MGI_D_Exit, OBU_TR_ECS_D_Entry, OBU_TR_ECS_D_Exit, OBU_TR_ECS_D_Entry and OBU_TR_ECS_D_Exit are insignificant for safety under the following condition.

5.1.4.4.2 It is assumed that EB curve is calculated in such a way that EB distance is not extended by a faulty special brake inhibition signal. This can be achieved if the degree of reliability of OBU_TR_RBI_D_Entry, OBU_TR_RBI_D_Exit, OBU_TR_MGI_D_Entry, OBU_TR_MGI_D_Exit, OBU_TR_ECS_D_Entry, OBU_TR_ECS_D_Exit, OBU_TR_ECS_D_Entry, OBU_TR_ECS_D_Exit, and is considered adequately in the Kdry_rst (V, EBCL, set) values.

5.1.4.5 Special brake inhibit – STM orders

5.1.4.5.1 Analysis is national system specific.

5.1.4.6 Special brake status

5.1.4.6.1 If the vehicle is equipped with special brakes the special brake status can be relevant to calculate the brake model.

5.1.4.6.2 It is assumed that EB curve is calculated in such a way that EB distance is not extended by a faulty special brake status signal. This can be achieved if the degree of reliability of OBU_TR_RBI_D_Entry, OBU_TR_RBI_D_Exit, OBU_TR_MGI_D_Entry, OBU_TR_MGI_D_Exit, OBU_TR_ECS_D_Entry, OBU_TR_ECS_D_Exit, OBU_TR_ECS_D_Entry, and OBU_TR_ECS_D_Exit is considered adequately in the Kdry_rst (V, EBCL, set) values.

5.1.4.6.3 Application Constraint (see Subset-080): If using Special Brake as available and affecting the Emergency Brake curve, the failure of the input ‘Special Brake status’ could have catastrophic safety severity. A project specific safety analysis is required.

5.1.4.7 Additional brake status

5.1.4.7.1 Currently no Additional Brakes, in addition to the special brakes, are known. Additional brakes should be handled identically as the special brakes are.

5.1.5 Signals for the Control of Train Functions

5.1.5.1 Change of traction system

5.1.5.1.1 Change of traction system is not safety-related.

5.1.5.2 Powerless section with pantograph to be lowered – Trackside orders / Pantograph – STM orders

5.1.5.2.1 Pantograph information is not safety-related.

5.1.5.3 Air tightness area – Trackside orders / Air tightness – STM orders

5.1.5.3.1 Air tightness is insignificant for safety.

5.1.5.3.2 Exported constraint to the vehicle or operation: A function on vehicle side or an operational regulation is necessary to handle this information in an appropriate manner.

5.1.5.4 Station platform

5.1.5.4.1 The related hazard (vehicle allows opening of passenger doors untimely or at the wrong location, compare FMEA) is not part of the ETCS Core Hazard.

5.1.5.4.2 Therefore the safety target and the hazard analysis are project specific.

5.1.5.4.3 The serial communication between ERTMS/ETCS on-board equipment and TCMS or a door control system must fulfill the safety target, see 5.1.5.4.2.

5.1.5.4.4 Exported constraint to the vehicle and operation: A function on vehicle side or an operational regulation is necessary to handle this information in a safe way.

5.1.5.5 Powerless section with main power switch to be switched off – Trackside orders / Main Power Switch – STM orders

5.1.5.5.1 Main power switch information is not safety-related.

5.1.5.6 Change of allowed current consumption (ACC)

5.1.5.6.1 ACC is not safety-related.

5.1.5.7 Traction Cut Off

5.1.5.7.1 TCO with hard-wired output O_TC1_C and serial output OBU_TR_TCO_Cmd allowing a safe TCO affecting the braking curves:

5.1.5.7.1.1 Requirements for ERTMS/ETCS on-board equipment:

5.1.5.7.1.1.1 TFR of O_TC1_C hard-wired erroneously takes the value ‘Do not cut off traction’: 1E-5 /h

5.1.5.7.1.1.2 FDT of O_TC1_C hard-wired = 48 h

5.1.5.7.1.1.3 TFR of OBU_TR_TCO_Cmd serial erroneously takes the value ‘Do not cut off traction’ < 1E-06 /h, serial communication of OBU_TR_TCO_Cmd serial has to be SIL2, i.e. 1E-07 /h ≤ THR < 1E-06 /h

5.1.5.7.1.1.4 FDT of OBU_TR_TCO_Cmd serial = 1 h

5.1.5.7.1.2 Requirements for vehicle:

5.1.5.7.1.2.1 TFR of O_TC1_C hard-wired erroneously takes the value ‘Do not cut off traction’: 1E-05 /h

5.1.5.7.1.2.2 FDT of O_TC1_C hard-wired = 48 h

5.1.5.7.1.2.3 TFR of OBU_TR_TCO_Cmd serial erroneously takes the value ‘Do not cut off traction’ < 1E-06 /h, serial communication of OBU_TR_TCO_Cmd serial has to be SIL2, i.e. 1E-07 /h ≤ THR < 1E-06 /h

5.1.5.7.1.2.4 FDT of OBU_TR_TCO_Cmd serial = 1 h

5.1.5.7.1.2.5 SIL for TCMS (incl. brake control or other electronic devices): SIL 2, i.e. 1E-07 /h ≤ THR < 1E-06 /h.

5.1.5.7.1.3 Exported constraint to the operator: FDT of O_TC1_C hard-wired = 48 h.

5.1.5.7.1.4 Exported constraint to the vehicle: The TCO signals O_TC1_C and OBU_TR_TCO_Cmd shall be processed in the vehicle with independence as required by TSI Loc&Pas, section 4.2.4.4.1.

5.1.6 Signals for Train status Information

5.1.6.1 Cab Status

5.1.6.1.1 Requirements for ERTMS/ETCS on-board equipment:

5.1.6.1.1.1 TFR of T_CS_A / TR_OBU_CabStatusA erroneously takes the value of the opposite boolean value: 1E-05 /h

5.1.6.1.1.2 TFR of T_CS_B / TR_OBU_CabStatusB erroneously takes the value of the opposite boolean value: 1E-05 /h

5.1.6.1.1.3 FDT = 48 h.

5.1.6.1.2 Requirements for vehicle:

5.1.6.1.2.1 TFR of T_CS_A / TR_OBU_CabStatusA erroneously takes the value of the opposite boolean value: 1E-05 /h

5.1.6.1.2.2 TFR of T_CS_B / TR_OBU_CabStatusB erroneously takes the value of the opposite boolean value: 1E-05 /h

5.1.6.1.2.3 FDT = 48 h.

5.1.6.1.3 Exported constraints to the ERTMS/ETCS on-board equipment: The cab status signals T_CS_A / TR_OBU_CabStatusA and T_CS_B / TR_OBU_CabStatusB shall be read independently according to EN50129.

5.1.6.1.4 Exported constraint to the vehicle: The cab status signals T_CS_A / TR_OBU_CabStatusA and T_CS_B / TR_OBU_CabStatusB shall have two independent sources (common cause failures considered with 10%).

5.1.6.2 Direction Controller

5.1.6.2.1 Requirements for ERTMS/ETCS on-board equipment:

5.1.6.2.1.1 TFR of T_FW_S / TR_OBU_DirectionFW erroneously takes the value ‘Forward’: 1E-05 /h

5.1.6.2.1.2 TFR of T_BW_S / TR_OBU_DirectionBW erroneously takes the value ‘Backward’: 1E-05 /h

5.1.6.2.1.3 FDT = 48 h.

5.1.6.2.2 Requirements for vehicle:

5.1.6.2.2.1 TFR of T_FW_S / TR_OBU_DirectionFW erroneously takes the value ‘Forward’: 1E-05 /h

5.1.6.2.2.2 TFR of T_BW_S / TR_OBU_DirectionBW erroneously takes the value ‘Backward’: 1E-05 /h

5.1.6.2.2.3 FDT = 48 h.

5.1.6.2.3 Exported constraint to the vehicle or operation: In case of vehicle is at standstill an ERTMS/ETCS on-board equipment independent system is in charge to ensure the roll away protection.

5.1.6.3 Train integrity

5.1.6.3.1 To be harmonized.

5.1.6.4 Traction status

5.1.6.4.1 The traction status is forwarded to the STM. The information related to STMs is seen as out of scope of this safety analysis focusing on level 1 and level 2 aspects.

5.1.6.5 Set Speed

5.1.6.5.1 Set speed is not safety-related.

5.1.7 Train Data

5.1.7.1 Type of train data entry

5.1.7.1.1 Type of train data entry is not safety-related.

5.1.7.1.2 Exported constraint to the operation (see Subset-080): Driver shall be informed on the type of train when Train Data entry is selected.

5.1.7.2 Train data information

5.1.7.2.1 Train category / Cant deficiency

5.1.7.2.1.1 Note: The train interface allows the ETCS on-board to determine the cant deficiency value based on the

- value of the cant deficiency which is transferred via train interface or
- train type input or
- train composition input and tilting health status input.

5.1.7.2.1.2 Requirements for ERTMS/ETCS on-board equipment and vehicle:

5.1.7.2.1.2.1 SIL 2 is needed for the serial transmission of the cant deficiency value, train type input, train composition input, and tilting health status input.

5.1.7.2.1.2.2 Requirements for ERTMS/ETCS on-board equipment:

5.1.7.2.1.2.2.1 TFR of TR_OBU_ TiltingHealthStatus _1 is inappropriate received or lost: 1E-05 /h

5.1.7.2.1.2.2.2 TFR of TR_OBU_ TiltingHealthStatus _2 is inappropriate received or lost: 1E-05 /h

5.1.7.2.1.2.2.3 FDT = 48 h.

5.1.7.2.1.2.3 Requirements for vehicle:

5.1.7.2.1.2.3.1 TFR of TR_OBU_ TiltingHealthStatus _1 is inappropriate output or lost: 1E-05 /h

5.1.7.2.1.2.3.2 TFR of TR_OBU_ TiltingHealthStatus _2 is inappropriate output or lost: 1E-05 /h

5.1.7.2.1.2.3.3 FDT = 48 h.

5.1.7.2.1.2.4 The on-board configuration shall require driver validation for changes in Cant Deficiency Train Data information (see Subset-026, 3.18.3.3 and 5.17.2.2).

5.1.7.2.1.2.5 Exported constraint to the vehicle: The ATP system assumes that the train manufacturer has checked the safety of the whole function cant deficiency considering the transmission between OBU and vehicle. Therefore a specific project can regard the failure mode of this input as having a ‘RAM Issue’ only if adequate safety margin against derailment can be demonstrated for the vehicle exceeding maximum authorized speed for its train category. This shall be done specific for the respective vehicle.

5.1.7.2.2 Train length

5.1.7.2.2.1 Note: The train interface allows the ETCS on-board to determine the train length value based on the

- value of the train length which is transferred via train interface or
- train type input or
- train composition input.

5.1.7.2.2.2 Note: The brake build up time using the conversion models can be based on ‘brake position’ and ‘train length’.

5.1.7.2.2.3 Requirements for ERTMS/ETCS on-board equipment and vehicle:

5.1.7.2.2.3.1 SIL 2 is needed for the serial transmission of the train length value, train type input and train composition input.

5.1.7.2.2.4 The on-board configuration shall require driver validation for changes in Train length Train Data information (see Subset-026, 3.18.3.3 and 5.17.2.2).

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

5.1.7.2.3 Traction model

5.1.7.2.3.1 Note: The train interface allows the ETCS on-board to determine the traction model value based on the

- train type input or
- train composition input.

5.1.7.2.3.2 Requirements for ERTMS/ETCS on-board equipment and vehicle:

5.1.7.2.3.2.1 SIL 2 is needed for the serial transmission of train type input and train composition input.

5.1.7.2.3.2.2 The on-board configuration shall require driver validation for changes in Traction model Train Data information (see Subset-026, 3.18.3.3 and 5.17.2.2).

5.1.7.2.4 Brake build up time model and speed dependent deceleration model

5.1.7.2.4.1 Note:

- The train interface allows the ETCS on-board to determine the brake build up time model and speed dependent deceleration model based on the train type input plus the status of special brakes.
- The train interface allows the ETCS on-board to determine the brake build up time model and speed dependent deceleration model based on the train composition input plus the status of special brakes
- Calculation of the brake build up time using the conversion models based on ‘brake position’ and ‘train length’ and calculation of the speed dependent deceleration models by applying the conversion model to the brake percentage value.

5.1.7.2.4.2 Requirement for ERTMS/ETCS on-board equipment and vehicle:

5.1.7.2.4.2.1 SIL 2 is needed for the serial transmission of train type input and special brake status.

5.1.7.2.4.3 Requirements for ERTMS/ETCS on-board equipment:

5.1.7.2.4.3.1 The on-board configuration shall require driver validation for changes in brake build up time model and speed dependent deceleration model Train Data information (see Subset-026, 3.18.3.3 and 5.17.2.2).

5.1.7.2.4.3.2 TFR of composition of T_EP_S_N and T_EP_S_I / composition of T_EC_S_N and T_EC_S_I / composition of T_RB_S_N and T_RB_S_I / composition of T_MG_S_N and T_MG_S_I is inappropriate received or lost: 1E-07 /h

5.1.7.2.4.3.3 FDT = 48 h.

5.1.7.2.4.4 Requirements for vehicle:

5.1.7.2.4.4.1 TFR of composition of T_EP_S_N and T_EP_S_I / composition of T_EC_S_N and T_EC_S_I / composition of T_RB_S_N and T_RB_S_I / composition of T_MG_S_N and T_MG_S_I is inappropriate received or lost: 1E-07 /h

5.1.7.2.4.4.2 FDT = 48 h.

5.1.7.2.5 Brake percentage

5.1.7.2.5.1 Note: The train interface allows the ETCS on-board to determine the brake percentage (TR_OBU_BrakePercentage) based on the

- value of brake percentage is transferred via train interface,
- train type input or
- train composition input.

5.1.7.2.5.2 Requirements for ERTMS/ETCS on-board equipment and vehicle:

5.1.7.2.5.2.1 SIL 2 is needed for the serial transmission of the brake percentage value, train type input and train composition input.

5.1.7.2.5.2.2 Note: For integrity requirements on preparation of data on the vehicle side see Subset-091, EXT_SR03. This is project specific.

5.1.7.2.5.2.3 The on-board configuration shall require driver validation for changes in brake percentage Train Data information (see Subset-026, 3.18.3.3 and 5.17.2.2).

5.1.7.2.6 Brake position

5.1.7.2.6.1 Note: The train interface allows the ETCS on-board to determine the brake position (TR_OBU_BrakePosition1 and TR_OBU_BrakePosition2) based on the

- value of brake position is transferred via train interface or
- train type input or
- train composition input.

5.1.7.2.6.2 Requirements for ERTMS/ETCS on-board equipment and vehicle:

5.1.7.2.6.2.1 SIL 2 is needed for the serial transmission of the brake position value, train type input and train composition input.

5.1.7.2.6.2.2 Requirements for ERTMS/ETCS on-board equipment:

5.1.7.2.6.2.2.1 TFR of composition of T_BP_S1_N and T_BP_S1_I is inappropriate received or lost : 1E-07 /h

5.1.7.2.6.2.2.2 TFR of composition of T_BP_S2_N and T_BP_S2_I is inappropriate received or lost: 1E-07 /h

5.1.7.2.6.2.2.3 FDT = 48 h.

5.1.7.2.6.2.3 Requirements for vehicle:

5.1.7.2.6.2.3.1 TFR of composition of T_BP_S1_N and T_BP_S1_I is inappropriate output or lost : 1E-07 /h

5.1.7.2.6.2.3.2 TFR of composition of T_BP_S2_N and T_BP_S2_I is inappropriate output or lost: 1E-07 /h

5.1.7.2.6.2.3.3 FDT = 48 h.

5.1.7.2.6.2.4 The on-board configuration shall require driver validation for changes in brake position Train Data information (see Subset-026, 3.18.3.3 and 5.17.2.2).

5.1.7.2.7 Nominal rotating mass

5.1.7.2.7.1 Nominal rotating mass Train Data information is not safety-related.

5.1.7.2.8 Maximum train speed

5.1.7.2.9 Note: The train interface allows the ETCS on-board to determine the maximum train speed based on the

- train type input or
- train composition input and tilting health status input.

5.1.7.2.9.1 Requirements for ERTMS/ETCS on-board equipment and vehicle:

5.1.7.2.9.1.1 SIL 2 is needed for the serial transmission of train type input, train composition input and tilting health status.

5.1.7.2.9.1.2 Requirements for ERTMS/ETCS on-board equipment:

5.1.7.2.9.1.2.1 TFR of TR_OBU_TiltingHealthStatus_1 is inappropriate received or lost: 1E-05 /h

5.1.7.2.9.1.2.2 TFR of TR_OBU_TiltingHealthStatus_2 is inappropriate received or lost: 1E-05 /h

5.1.7.2.9.1.2.3 FDT = 48 h.

5.1.7.2.9.1.3 Requirements for vehicle:

5.1.7.2.9.1.3.1 TFR of TR_OBU_TiltingHealthStatus_1 is inappropriate output or lost: 1E-05 /h

5.1.7.2.9.1.3.2 TFR of TR_OBU_TiltingHealthStatus_2 is inappropriate output or lost: 1E-05 /h

5.1.7.2.9.1.3.3 FDT = 48 h.

5.1.7.2.9.1.4 The on-board configuration shall require driver validation for changes in maximum train speed Train Data information (see Subset-026, 3.18.3.3 and 5.17.2.2).

5.1.7.2.10 Loading gauge

5.1.7.2.10.1 Note: The train interface allows the ETCS on-board to determine the loading gauge value based on the

- value of loading gauge is transferred via train interface or
- train type input or
- train composition input and tilting health status input.

5.1.7.2.10.2 Loading gauge is safety-related.

5.1.7.2.10.3 Under assumption that Traffic planning, lineside signs and driver´s route knowledge shall prevent any hazardous situation a specific project can regard the failure mode of this input as having a ‘RAM Issue’..

5.1.7.2.10.4 Inappropriate value of loading gauge is not part of the ETCS Core Hazard. In case of a project specific safety target a specific analysis is necessary.

5.1.7.2.11 Axle load category

5.1.7.2.11.1 Note: The train interface allows the ETCS on-board to determine the axle load category value based on the

- value of axle load category is transferred via train interface or
- train type input or
- train composition input.

5.1.7.2.11.2 Requirements for ERTMS/ETCS on-board equipment and vehicle:

5.1.7.2.11.2.1 SIL 2 is needed for the serial transmission of axle load category value, train type input, and train composition input.

5.1.7.2.11.2.2 The on-board configuration shall require driver validation for changes in axle load category Train Data information (see Subset-026, 3.18.3.3 and 5.17.2.2).

5.1.7.2.11.3 In addition it is assumed that traffic planning, lineside signs and driver´s route knowledge prevent hazardous situations.

5.1.7.2.12 Traction system(s) accepted by the engine

5.1.7.2.12.1 Note: The train interface allows the ETCS on-board to determine the traction system(s) accepted by the engine value based on the

- value of traction system(s) accepted by the engine is transferred via train interface or
- train type input or
- train composition input.

5.1.7.2.12.2 Traction system(s) accepted by the engine is not safety-related.

5.1.7.2.13 Train fitted with airtight system

5.1.7.2.13.1 Note: The train interface allows the ETCS on-board to determine the train fitted with airtight system value based on the

- value of the train fitted with airtight system is transferred via train interface or
- train type input or
- train composition input.

5.1.7.2.13.2 The information whether the train fitted with airtight system is marginal for safety.

5.1.7.2.13.3 The on-board configuration shall require driver validation for changes in Train fitted with airtight system Train Data information (see Subset-026, 3.18.3.3 and 5.17.2.2).

5.1.7.2.13.4 Exported constraint to the vehicle and operation: The driver shall have the possibility to open/close the air conditioning intake independently from the ETCS information.

5.1.8 National System Isolation

5.1.8.1.1 This is level NTC only which is seen as out of scope of this safety analysis focusing on level 1 and level 2 aspects.

5.2 Serial transmission

5.2.1 Example for serial input with two inputs

5.2.1.1 In the following a safe serial input on two channels input signal is described by means of sleeping with the two channels antivalent sleeping signal (TR_OBU_TrainSleep and TR_OBU_TrainSleep_Not), see section 5.1.3.1.

5.2.1.1.1 Requirements for ERTMS/ETCS on-board equipment:

5.2.1.1.1.1 TFR of TR_OBU_TrainSleep erroneously takes the value '1': 1E-05 /h

5.2.1.1.1.2 TFR of TR_OBU_TrainSleep_Not erroneously takes the value '0': 1E-05 /h

5.2.1.1.1.3 FDT = 1 min

5.2.1.1.2 Requirements for vehicle:

5.2.1.1.2.1 TFR of TR_OBU_TrainSleep erroneously takes the value '1': 1E-05 /h

5.2.1.1.2.2 TFR of TR_OBU_TrainSleep_Not erroneously takes the value '0': 1E-05 /h

5.2.1.1.2.3 FDT = 48 h

5.2.1.1.3 Exported constraints to the ERTMS/ETCS on-board equipment: The antivalent sleeping signals TR_OBU_TrainSleep and TR_OBU_TrainSleep_Not shall be read independently (common cause failures considered with 10%).

5.2.1.1.4 Exported constraint to the vehicle: The antivalent sleeping signals TR_OBU_TrainSleep and TR_OBU_TrainSleep_Not shall have two sources (common cause failures considered with 10%).

5.2.1.1.5 Exported constraint to the vehicle or operation: In the case of vehicle is at standstill and all desks connected to the ERTMS/ETCS on-board equipment are closed an ERTMS/ETCS on-board equipment independent system is in charge to ensure the standstill (e.g. the driver applied brakes).

5.2.2 Architecture a)

5.2.2.1 Requirement for ERTMS/ETCS on-board equipment and vehicle:

5.2.2.1.1 With assumptions made in 3.1.3.1.3 the following example is valid. On basis of subset-120 a safety case has to be created on ERTMS/ETCS on-board equipment side in which these assumptions have to be confirmed or the calculation has to be adopted accordingly.

5.2.2.1.2 Example:

5.2.2.1.2.1 TFR and FDT of signals as for hard-wired interface.

5.2.2.1.2.2 Two simple I/O devices with respectively TFR = 5E-6 /h and a FDT = 24 h.

5.2.2.1.2.3 TFR = 1,65E-5 /h for bus transmission failures with CRC-16 as transmission code and a bus cycle of 128 ms, and a bus interface card (OBU side) with TFR = 1E-5 /h and a FDT = 24 h.

5.2.2.1.2.4 TFR = 1,32E-5 /h for bus transmission failures with CRC-16 as transmission code and a bus cycle of 256 ms, and a bus interface card (OBU side) with TFR = 1E-5 /h and a FDT = 24 h.

5.2.3 Architecture b)

5.2.3.1 Requirement for ERTMS/ETCS on-board equipment and vehicle:

5.2.3.1.1 Architecture b) has to be implemented strictly according to EN 50159.

5.2.3.1.2 The communication partners need at least the safety level of the information which is transmitted. The ERTMS/ETCS on-board equipment fulfils this in all cases with a HR of 6,7E-10 /h. The THR of the TCMS depends on the information which is transmitted.

5.2.3.1.3 All signals requiring a higher SIL than provided by the TCMS shall be transmitted using the Hard-wired Interface, so that signals are transmitted directly from the source to the ERTMS/ETCS on-board equipment without using TCMS in any part of the transmission.

5.2.3.1.4 With assumptions made in 3.1.3.2.3 the following example is valid. On basis of Subset120 a safety case has to be created on ERTMS/ETCS on-board equipment side in which these assumptions have to be confirmed or the calculation has to be adopted accordingly.

5.2.3.1.5 Example:

5.2.3.1.5.1 Assumptions: Hardware failure rate of the non-trusted transmission system R_{HW} = 2E-5 /h, CRC-8 as transmission code, CRC-32 as safety code, a bus cycle of 128ms respectively 256ms and a time of 1 sec as time span T. If more than a defined number of corrupted messages were received within this time T, the safe fall back state will be entered.

5.2.3.1.5.2 Hazardous failure rate of hardware faults (with consideration of the safety code) without transmission code checker R_{H1} = 4,6 E-14 / h.

5.2.3.1.5.3 Hazardous failure rate of EMI R_{H2} = 2,6E-8 /h for 128ms

5.2.3.1.5.4 Hazardous failure rate of EMI R_{H2} = 1,3E-8 /h for 256ms

5.2.3.1.5.5 Hazardous failure rate of transmission code checker R_{H3} = 8,2E-11 /h

5.2.3.1.5.6 FDT = 1 min.

6. ANNEX A – SAFETY ANALYSIS

6.1 FMEA

6.1.1 Objective

6.1.1.1 The purpose of this FMEA is to analyse, based on architectures described in Subset-119, which single failures lead to which effects and in the end to which hazard.

6.1.2 Assumptions

Column “Ref ID”:

Reference to Subset-119.

Column “Macro function: Data item”:

Macro functions have been numerated taking into account Subset-026, 4.5.2 Active Function Table.

Column “Failure Mode”:

Corruption, deletion, insertion, repetition, re-sequence, delay will be considered, the Failure Mode Guide-words for Data Transmission recommended in Subset-077. Every type of failure can be classified in one or more of these categories.

Column “Failure Cause”:

Possible failure causes are identified in order to estimate its probability of occurrence and to devise corrective action.

Column “Operational mode”:

NP, TR, SF and IS are modes without speed or distance supervision so that they do not have to be mentioned in this column.

Column “Failure Effects”:

Local effect refers to the related interface function.

Intermediate effect refers to the related ETCS supervision function.

Initial End Effect gives a description of the result of this failure. This could be a hazardous situation on system level.

Column “External Protection / Mitigation / Barriers“:

It defines the constraints to be considered for each interface implementation.

Column “Severity“:

A severity level will be assigned to each Initial End Effect, repeated for every failure mode associated with it. The categorisation system to be used will be as the example in EN 50126 for a passenger, part of which is repeated here for convenience, and also complemented with events without safety effect. Classification is according to Subset-077:

Severity Level	Consequence
Catastrophic	Single fatality and/or multiple injuries
Critical	Single severe injury
Marginal	Minor injury
Insignificant	Possible minor injury
RAM issue	Service impact not safety-related
No effect	None

Column “Event-ID”:

Event-ID replaces the former one named as “Failure Rate” (originally in FMEA template). This column will be used to provide the link of all failure effects to TI_OB-xxx and TI_VE-xxx hazardous events in chapter 3.8 (see chapter 1.4).

Column “Internal Barriers”:

References to Subset-026 or other Subsets are contained in brackets.

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
1.	5.1.1.2	Mode Control – Sleeping request information (with two sleeping signals)	**Corruption / Deletion / Insertion**: Inappropriate reception of faulty antivalent Sleeping signal (T_SL_E_N or T_SL_E_I)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	SH, FS, LS, SR, OS, NL, UN, PT, SN, RV	ERTMS/ETCS on-board does not change the current mode.			-	RAM issue		

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
2.			**Corruption / Deletion / Insertion**: Inappropriate reception of faulty antivalent Sleeping signal (T_SL_E_N or T_SL_E_I)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	SB	ERTMS/ETCS on-board does not change the current mode.			-	RAM issue		E.g. ERTMS/ETCS on-board equipment shall memorize the fault. ERTMS/ETCS on-board shall not be able to switch to SL mode as long as the failure is memorized. Alternative reaction e.g.: Transition to SF mode.

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
3.			**Corruption / Deletion / Insertion**: Inappropriate reception of faulty antivalent Sleeping signal (T_SL_E_N or T_SL_E_I)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	SL	ERTMS/ETCS on-board equipment shall memorize the fault and shall also try to send an error information to the RBC (Subset-026, 4.4.6.1.6).	Transition to SB mode if the vehicle is at standstill (Subset-026, 4.4.6.1.8).	In case of leaving a tunnel (leading engine in mode RV) then reverse movement will not be possible if the slave engine is in mode SB. TI-3	-	Marginal	TI_OB-SL-1.2TI_VE-SL-1.2TI_OB-SL-1.1 TI_VE-SL-1.1	The engine is remote controlled by the leading engine (Subset-026, 4.4.6.1.3). In addition e. g. ERTMS/ETCS on-board shall not be able to switch to SL mode as long as the failure is memorized.

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
4.			**Corruption / Deletion / Insertion**: Inappropriate reception of faulty antivalent Sleeping signal (T_SL_E_N or T_SL_E_I)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	PS	ERTMS/ETCS on-board equipment shall try to memorize the fault and shall also try to send an error information to the RBC (Subset-026, 4.4.20.1.10)..			-	RAM issue		

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
5.	5.1.1	Mode Control – Sleeping request information (with single sleeping signal)	**Insertion**: Inappropriate reception of Sleeping signal (T_SL_E)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	SB	"Sleeping requested" state unduly selected during normal operation	Loss of Standstill protection	TI-3	In the case of vehicle is at standstill and all desks connected to the ERTMS/ETCS on-board equipment are closed an ERTMS/ETCS on-board equipment independent system is in charge to ensure the standstill	Catastrophic	TI_OB-SL-1, TI_VE-SL-1	

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
6.			**Insertion**: Inappropriate reception of faulty Sleeping signal (T_SL_E) **Already analysed in Subset-080**	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	SL, PS							
7.	5.1.1.2	Mode Control – Sleeping request information (solution 1 – serial transmission with architecture a) on two channels input, no safety layer is used)	**Insertion / Corruption/ Re-sequence**: Inappropriate reception of faulty antivalent Sleeping signal (TR_OBU_TrainSleep or TR_OBU_TrainSleep_Not)	Simple I/O-device failure (vehicle part) or bus falsifies telegram	SH, FS, LS, SR, OS, NL, UN, PT, SN, RV	ERTMS/ETCS on-board does not change the current mode.			-	RAM issue		

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
8.		Mode Control – Sleeping request information (solution 1 – serial transmission with architecture a) on two channels input, no safety layer is used)	**Insertion / Corruption/ Re-sequence**: Inappropriate reception of faulty antivalent Sleeping signal (TR_OBU_TrainSleep or TR_OBU_TrainSleep_Not)	Simple I/O-device failure (vehicle part) or bus falsifies telegram or Bus interface card failure (OBU part)	SB	ERTMS/ETCS on-board does not change the current mode.			-	RAM issue		E.g. ERTMS/ETCS on-board equipment shall memorize the fault. ERTMS/ETCS on-board shall not be able to switch to mode SL as long as the failure is memorized. Alternative reaction e.g.: Transition to SF mode.

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
9.			**Insertion / Corruption/ Re-sequence**: Inappropriate reception of faulty antivalent Sleeping signal (TR_OBU_TrainSleep or TR_OBU_TrainSleep_Not)	Simple I/O-device failure (vehicle part) or bus falsifies telegram	PS	ERTMS/ETCS on-board equipment shall try to memorize the fault and shall also try to send an error information to the RBC (Subset-026, 4.4.20.1.10).			-	RAM issue		ERTMS/ETCS on-board shall not be able to switch to SL mode as long as the failure is memorized

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
10.			**Insertion / Corruption / Re-sequence**: Inappropriate reception of faulty antivalent Sleeping signal on two channels input (TR_OBU_TrainSleep and TR_OBU_TrainSleep_Not)	Bus interface card failure (OBU part)	SH, FS, LS, SR, OS, NL, UN, PT, SN, RV	Transition to SL mode not possible; current mode is not changed.				No effect		

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
11.			**Insertion / Corruption / / Re-sequence**: Inappropriate reception of faulty antivalent Sleeping signal on two channels input (TR_OBU_TrainSleep or TR_OBU_TrainSleep_Not)	Simple I/O-device failure (vehicle part) Or bus falsifies telegram or bus interface failure (OBU part)	SL	ERTMS/ETCS on-board equipment shall memorize the fault and shall also try to send an error information to the RBC (Subset-026, 4.4.6.1.6).	Transition to SB mode if the vehicle is at standstill (Subset-026, 4.4.6.1.8).	In case of leaving a tunnel (leading engine in mode RV) then reverse movement will not be possible if the slave engine is in mode SB. TI-3	-	Marginal	TI_OB-SL-1.2TI_VE-SL-1.2TI_OB-SL-1.1 TI_VE-SL-1.1	The engine is remote controlled by the leading engine (Subset-026, 4.4.6.1.3). In addition e. g. ERTMS/ETCS on-board shall not be able to switch to SL mode as long as the failure is memorized

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
12.	5.1.2.2	Mode Control – Passive Shunting information	**Corruption / Insertion**: Inappropriate reception of faulty Passive Shunting signal (T_PS_E)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	SH	Transition to PS mode during normal operation.	No more movement protection, unable to apply brakes.	TI-7	Driver has to ensure the standstill (e.g. by applying the parking brake before leaving the cab).	Catastrophic	TI_OB-PS,TI_VE-PS	Second information from the DMI is necessary to change to PS mode.
13.			**Corruption / Deletion**: Loss of Passive Shunting signal (T_PS_E)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	SH	No transition to PS mode when required.	SH mode is kept.			RAM issue		

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
14.	5.1.3.2	Mode Control – Non Leading information	**Corruption / Insertion**: Inappropriate reception of Non Leading signal (T_NL_E)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	SB, SH, FS, LS, SR, OS	Transition to Non Leading mode if vehicle is at standstill and driver selects Non Leading in the DMI.	No more movement protection, unable to apply brakes.	TI-8	New mode is displayed on the DMI. Driver is not going to leave the cab.	Catastrophic	TI_OB-NL, TI_VE-NL	Vehicle at standstill and second information from the DMI are necessary to change to NL mode (Subset-026, 4.6.3, [46]).
15.			**Corruption / Deletion**: Loss of Non Leading signal (T_NL_E) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
16.	5.1.4.2	Mode Control – Isolation	**Deletion / Delay**: Loss of Isolation signal (O_IS_S) (O_IS_S = 0 instead of 1) **Already analysed in Subset-080**									
17.			**Corruption / Insertion**: Inappropriate output of isolation signal (O_IS_S = 1 instead of 0) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
18.	5.2.1.2	Signals for the Control of Brakes – Service Brake command	**Deletion/ Delay**: Loss of SB command signal (O_SB_C = 0 instead of 1) **Already analysed in Subset-080**									
19.			**Corruption/ Insertion**: Inappropriate output of SB command signal (O_SB_C is = 1 instead of 0) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
20.	5.2.2.2	Signals for the Control of Brakes – Brake pressure	**Corruption/ Insertion**: Inappropriate reception of Brake pressure signal (TR_OBU_BrakePressure) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
21.	5.2.3.2.10	Signals for the Control of Brakes – Emergency Brake command (solution 1 - 3)	**Deletion/ Delay**: Loss of Emergency Brake command signal (Failure to Command Emergency Brake Application when required) (solution 1/2: O_EB1_C, O_EB2_C; solution 3: O_EB1_C, OBU_TR_EB3_Cmd)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components.	SB, SH, FS, LS, SR, OS, UN, PT, SN, RV	EB application command not transmitted to the vehicle	EB Not activated when required	TI-1	Two independent EB lines (e.g. brake valves) are necessary	Catastrophic	TI_OB-EB-1, TI_VE-EB-1, , TI_OB-EB-2, TI_VE-EB-2	

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
22.			**Corruption/ Insertion**: Inappropriate output of Emergency Brake command signal (commanded when not required) (solution 1/2: O_EB1_C, O_EB2_C; solution 3: O_EB1_C, OBU_TR_EB3_Cmd) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
23.	5.2.4	Signals for the Control of Brakes – Special brake inhibition area – Trackside orders	**Deletion/ Delay**: Loss of any Inhibition of Special Brakes information (OBU_TR_xx_D_Entry or OBU_TR_xx_D_Exit = 8000h instead of another value) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
24.			**Corruption/ Insertion:** Inappropriate output of any Inhibition of Special Brakes signal (OBU_TR_xx_D_Entry or OBU_TR_xx_D_Exit = any value instead of 8000h)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	All modes except SL, NL, PS, SH, SB, RV	Special Brake is erroneously inhibited and Special Brake Status informs OBU of this inhibition.	OBU updates SB / EB braking curves according to current special brake status.	Updated SBI / EBI curve is used by OBU.		Insignificant		If EBI is affected by special brake inhibition, EB model (Kdry_rst) is calculated in such a way that EB distance is exceeded only according to the actual EBCL.

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
25.	5.2.5	Signals for the Control of Brakes – Special Brake inhibit – STM Orders	**Deletion/ Delay**: Loss of any Inhibition of Special Brakes signal (O_RB_I, O_MG_I, O_ECS_I or O_ECE_I = 0 instead of 1) **Already analysed in Subset-080**	Analysis is national system specific.								

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
26.			**Corruption/ Insertion:** Inappropriate output of any Inhibition of Special Brakes signal (O_RB_I, O_MG_I, O_ECS_I or O_ECE_I = 1 instead of 0)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	SN	Analysis is national system specific.						
27.	5.2.6.3	Signals for the Control of Brakes – Special Brake Status	**Deletion/ Delay**: Loss of active state information (special brake enabled) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
28.			**Insertion / Incorrect:** Inappropriate output of active state information (special brake enabled)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	All modes except SL, NL, PS, SH, SB, RV	Special Brake is erroneously not used for EB.	OBU assumes too optimistic braking curves.	TI-1		Insignificant		EB model (Kdry_rst) is calculated in such a way that EB distance is exceeded only according to the actual EBCL.
29.	5.3.2	Signals for the Control of Train Functions – Change of traction system (CTS)	**Corruption:** Inappropriate output of Change of traction system information **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
30.	5.3.3	Signals for the Control of Train Functions – Powerless section with pantograph to be lowered – Trackside orders	**Corruption:** Inappropriate output of Pantograph information **Already analysed in Subset-080**									
31.	5.3.4	Signals for the Control of Train Functions – Pantograph – STM orders	**Corruption:** Inappropriate output of Pantograph information **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
32.	5.3.5	Signals for the Control of Train Functions – Air tightness area – Trackside orders	**Corruption:** Inappropriate output of Air tightness information **Already analysed in Subset-080**									
33.	5.3.6	Signals for the Control of Train Functions – Air tightness – STM orders	**Corruption:** Inappropriate output of Air tightness information **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
34.	5.3.7	Signals for the Control of Train Functions - Station platform	**Corruption:** Inappropriate output of Station platform information (wrong location e.g. vehicle side)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	All	Inappropriate Station platform information sent to the vehicle.	Vehicle allows opening of passenger doors in a wrong location.	Passengers could be severe injured when leaving the train.	Project specific, doors shall be controlled independent from ERTMS/ETCS on-board system.	Critical	TI_OB-PD, TI_VE-PD	

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
35.	5.3.8	Signals for the Control of Train Functions – Powerless section with main power switch to be switched off – Trackside orders	**Corruption:** Inappropriate output of Main Power Switch information **Already analysed in Subset-080**									
36.	5.3.9	Signals for the Control of Train Functions – Main Power Switch – STM orders	**Corruption:** Inappropriate output of Main Power Switch information **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
37.	5.3.10	Signals for the Control of Train Functions – Change of allowed current consumption (ACC)	**Corruption:** Inappropriate output of Change of allowed current consumption information **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
38.	4.3.5.3	Signals for the Control of Train Functions – Track conditions of the generic telegram structure listed in SS-119 §5.3.1.3	**Corruption / Insertion:** Inappropriate output of track condition ID (OB_TR_TC_IDx is set to a wrong ID) or Track Condition Type (OB_TR_TC_TYPEx is set to a wrong type) is sent	Variables for Generic Telegram Structures are corrupted / inserted		Inappropriate output of the respective track condition; see the respective failure modes AND Loss of the overwritten respective track condition; see the respective failure modes						

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
39.	4.3.5.3	Signals for the Control of Train Functions – Track conditions of the generic telegram structure listed in SS-119 §5.3.1.3	**Deletion/ Delay**: Inappropriate output of track condition ID (OB_TR_TC_IDx is set to 0 or to a spare value) or Track Condition Type (OB_TR_TC_TYPEx is set to a spare value) is sent	Variables for Generic Telegram Structures are deleted / delayed		Loss of the respective track condition; see the respective failure modes						

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
40.	4.3.5.5	Signals for the Control of Train Functions – Track conditions of the generic telegram structure listed in SS-119 §5.3.1.3	**Corruption / Insertion:** Inappropriate output of flag "initial state is to be resumed" is sent (OBU_TR_IS is set to 1 instead of 0)	Variables for Generic Telegram Structures are corrupted / inserted		Inappropriate output of the respective track condition; see the respective failure modes						
41.	4.3.5.5	Signals for the Control of Train Functions – Track conditions of the generic telegram structure listed in SS-119 §5.3.1.3	**Deletion/ Delay**: Inappropriate output of flag "initial state is to be resumed" is sent (OBU_TR_IS is set to 0 instead of 1)	Variables for Generic Telegram Structures are deleted / delayed		Loss of the respective track condition; see the respective failure modes						

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
42.	5.3.11	Signals for the Control of Train Functions – Traction Cut Off	**Corruption / Insertion:** Inappropriate output of Traction Cut Off (request when not required) for **Already analysed in Subset-080**									
43.			Loss of TCO Signal (O_TC1_C) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
44.			**Corruption / Deletion:** Loss of TCO Signal (O_TC1_C or OBU_TR_TCO_Cmd)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	All modes except SL, NL, PS, SH, SN, RV	TCO application command (CUT OFF TRACTION state) transmitted to the vehicle via second path.	Traction is cut off at warning limit		Two diverse TCO paths	Catastrophic	TI_OB-TCO-1, TI_OB-TCO-2, TI_VE-TCO-1, TI_VE-TCO-2	
45.	5.4.1.2	Signals for Train Status Information – Cab Status	**Deletion/ Delay**: Loss of Cab Status signal (T_CS_A or T_CS_B) (cases 1/0 or 0/1 fails to 0/0) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
46.			**Corruption/ Insertion**: Inappropriate reception of Cab Status signal (T_CS_A or T_CS_B) (cases 1/0 or 0/1 fails to 1/1) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
47.			**Corruption/ Insertion**: Inappropriate reception of Cab Status signal (T_CS_A or T_CS_B) (cases 0/0 fails to 0/1 or 1/0) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
48.			**Corruption/ Insertion**: Inappropriate reception of Cab Status signal (T_CS_A or T_CS_B) (cases 0/0 fails to 0/1 or 1/0) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
49.			**Corruption/ Insertion**: Inappropriate reception of Cab Status signal (T_CS_A or T_CS_B) (cases 0/0 fails to 0/1 or 1/0) Case: driver changes the Cab **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
50.			**Corruption/ Insertion**: Inappropriate reception of Cab Status signal (T_CS_A or T_CS_B) (cases 0/0 fails to 0/1 or 1/0) Case: Slave engine **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
51.			**Corruption/ Insertion**: Inappropriate reception of Cab Status signal (T_CS_A or T_CS_B) (cases 0/0 fails to 0/1 or 1/0) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
52.			**Deletion/ Delay**: Loss of Cab Status signal (T_CS_A or T_CS_B) (cases 1/0 or 0/1 fails to 0/0) **Already analysed in Subset-080**									
53.			**Deletion/ Delay**: Loss of Cab Status signal (T_CS_A or T_CS_B) (cases 1/0 or 0/1 fails to 0/0) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
54.			**Deletion/ Delay**: Loss of Cab Status signal (T_CS_A or T_CS_B) (cases 1/0 or 0/1 fails to 0/0) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
55.	5.4.2.2	Signals for Train Status Information – Direction Controller status	**Deletion/ Delay**: Loss of Direction Controller status signal (T_FW_S or T_BW_S) (cases 1/0 or 0/1 fails to 0/0) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
56.			**Corruption/ Insertion**: Loss of Direction Controller status signal (T_FW_S or T_BW_S) (cases 1/0 or 0/1 fails to 1/1)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	SH, SR, OS, NL, UN, PT, RV, FS, LS, SR	Incorrect Direction Controller status (fault condition).	Transition to SF mode and EB applied.	Vehicle will be at standstill.		RAM issue	-	

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
57.			**Corruption/ Insertion**: Inappropriate reception of Direction Controller status signal (T_FW_S or T_BW_S) (cases 0/0 to 0/1 or 1/0) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
58.			**Corruption/ Insertion**: Inappropriate reception of Direction Controller status signal (T_FW_S or T_BW_S) (cases 0/0 to 0/1 or 1/0)		SH, SR, OS, UN, PT, RV, FS, LS	Incorrect Direction Controller status.	Roll away protection is deactivated	No more protection of the vehicle by ETCS. TI-5	1.) Driver (knows the direction controller position) 2.) Safety-related function: Roll away protection and driver's activity control function is supported by Fail-safe Dead-Man Supervision (TSI Loc Pas, chapter 4.2.9.3.1) or additionally other vehicle side roll away protection systems 3.) The driver has to ensure the standstill before leaving the cab.	Catastrophic	TI_OB-DC-1, TI_OB-DC-2, TI_VE-DC-1, TI_VE-DC-2	Reverse movement protection.

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
59.			**Corruption/ Insertion**: Inappropriate reception of Direction Controller status signal (T_FW_S or T_BW_S) (cases 0/0 to 0/1 or 1/0) **Already analysed in Subset-080**		NL, SB							
60.	5.4.3	Signals for Train Status Information – Train integrity	To be harmonized									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
61.	5.4.4.2	Signals for Train Status Information – Traction Status	Not harmonized, since the signal is only related to STMs									
62.	5.4.5.2	Signals for Train Status Information – Set Speed	**Delay / Deletion / Corruption / Insertion:** Wrong input Set Speed (state and/or speed value) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
63.	5.5.1.3	Train data – Type of train data entry	**Deletion / Delay**: Loss of Type of train data entry signal (T_TT_S1 / T_TT_S2 unwantedly equal to Flexible) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
64.			**Corruption / Insertion:** Inappropriate reception of Type of train data entry signal (T_TT_S1 / T_TT_S2 unwantedly equal to Fixed) **Already analysed in Subset-080**									

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
65.	5.5.2.2.2	Train data – Train data information – Train category / Cant Deficiency	**Deletion/ Delay**: Incorrect reception of Cant Deficiency information (lower than real) **Already analysed in Subset-080**	Falsification of value which is transmitted via TI or incorrect reception of “train type”, “train composition ” or “tilting health status”								

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
66.			**Corruption/ Insertion:** Incorrect reception of Cant Deficiency information (higher than real)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components; falsification of value which is transmitted via TI or incorrect reception of “train type”, “train composition” or “tilting health status”	FS, LS, OS, UN, SN, SR, TR, SB, PT	Incorrect Cant deficiency information received from the vehicle side.	Higher than real Cant Deficiency is assumed on ETCS OBU. Error in on-board evaluation of SSPs.	Vehicle may exceed maximum authorized speed for its train category so that: - Increasing in lateral forces may result in unsafe wheel force condition and increase deterioration of track - Decreasing in load on inside wheel may increase risk of vehicle overrun (especially of high wind present)	Driver must confirm the cant deficiency information via DMI. Adequate safety margin against derailment can be demonstrated for the vehicle exceeding maximum authorized speed for its train category.	Catastrophic	TI_OB-CD, TI_VE-CD	On-board informs driver that change in Train Data needs to be validated by Driver (Subset-026, 3.18.3.3 and 5.17.2.2).

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
								- Suspension operating at performance limit reduces margin of safety associated with vehicle response to track geometry variation Risk of derailment. TI-10				

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
67.	5.5.2.3.2	Train data – Train data information – Train length	**Corruption/ Insertion:** Inappropriate reception of Train length variable	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components; falsification of value which is transmitted via TI or incorrect reception of “train type”, or “train composition”	FS, LS, OS, UN, SN, SR, TR, SB, PT	Inappropriate train length received from external interface. OBU informs driver.	Wrong minimum safe rear end. Wrong supervision of SSPs and TSRs AND wrong brake build up time could be calculated, see “brake build up time”	TI-10	Operational rules for driver.	Catastrophic	TI_OB-TL, TI_VE-TL	On-board informs driver that change in Train Data needs to be validated by driver (Subset-026, 3.18.3.3 and 5.17.2.2).

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
68.			**Deletion/ Delay**: Loss of Train length variable **Already analysed in Subset-080**	Falsification of value which is transmitted via TI or incorrect reception of “train type”, “train composition ” or “tilting health status”								
69.		Train data – Train data information – Traction model	**Re-sequence / Insertion / Corruption:** Inappropriate reception of Traction Model	Loss of Train composition information or loss of train type	FS, LS, OS, UN, SN, SR, TR, SB, PT	Incorrect determination of time delay T_traction_cut_off value	T_traction is incorrect..	Traction cut-off command is triggered untimely. TI-10		Catastrophic	TI_OB-TM, TI_VE-TM	On-board informs driver that change in Train Data needs to be validated by driver (Subset-026, 3.18.3.3 and 5.17.2.2).

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
70.		Train data – Train data information - Brake build up time model and speed dependent deceleration model	**Re-sequence / Insertion / Corruption:** Inappropriate reception of T_brake_emergency, T_brake_service values, A_brake_emergency(V), A_brake_service(V),	Falsification of value which is transmitted via TI or incorrect reception of “train type”, or “train composition ”	FS, LS, OS, UN, SN, SR, TR, SB, PT	Wrong kinematic behaviour of the train is assumed after a an emergency brake command has been initiated. Wrong values of A_brake_emergency(V) and T_brake_emergency are derived.	Wrong EB curve calculation. Conversion model is used although it is not suitable (see Subset-026, §3.13.3.2.1)	TI-10		Catastrophic	TI_OB-BMTI_VE-BM	On-board informs driver that change in Train Data needs to be validated by driver (Subset-026, 3.18.3.3 and 5.17.2.2).

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
71.	5.5.2.4.3	Train data – Train data information – Brake percentage	**Re-sequence / Insertion / Corruption:** Inappropriate reception of Brake percentage	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components; falsification of value which is transmitted via TI or incorrect reception of “train type”, or “train composition”	FS, LS, OS, UN, SN, SR, TR, SB, PT	Wrong values of A_brake_emergency(V) and T_brake_emergency are derived.	Conversion model is used although it is not suitable (see Subset-026, §3.13.3.2.1). AND wrong speed dependent deceleration models could be calculated, see “speed dependent deceleration models”	Wrong EB curve calculation. TI-10		Catastrophic	TI_OB-BP, TI_VE-BP	On-board informs driver that change in Train Data needs to be validated by driver (Subset-026, 3.18.3.3 and 5.17.2.2).

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
72.			**Deletion / Delay**: Loss of Brake percentage	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components	FS, LS, OS, UN, SN, SR, TR, SB, PT	Wrong values of A_brake_emergency(V) and T_brake_emergency are derived (the lost values would have been lower than the stored ones)	Conversion model is used although it is not suitable (see Subset-026, §3.13.3.2.1).	Wrong EB curve calculation. TI-10		Catastrophic	TI_OB-BP, TI_VE-BP	On-board informs driver that change in Train Data needs to be validated by driver (Subset-026, 3.18.3.3 and 5.17.2.2).

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
73.		Train data – Train data information – Brake position	**Corruption:** Inappropriate reception of Brake position	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components; falsification of value which is transmitted via TI or incorrect reception of “train type”, or “train composition”	FS, LS, OS, UN, SN, SR, TR, SB, PT	Wrong kinematic behaviour of the train is assumed after a an emergency brake command has been initiated because wrong train type is assumed.	Wrong EB curve calculation. Conversion model is used although it is not suitable (see Subset-026, §3.13.3.2.1) AND wrong brake build up time could be calculated, see “brake build up time”	TI-10		Catastrophic	TI_OB-BPos-1.1, TI_OB-BPos-1.2, TI_VE-BPos-1.1, TI_VE-BPos-1.2	On-board informs driver that change in Train Data needs to be validated by driver (Subset-026, 3.18.3.3 and 5.17.2.2).

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
74.		Train data – Train data information – Nominal rotating mass	**Corruption / Insertion:** Incorrect reception of Nominal rotating mass	Falsification of train type	FS, LS, OS, UN, SN, SR, TR, SB, PT	M_rotating_nom could be greater than M_rotating_max or lower than M_rotating_min	Inappropriate safe deceleration A_safe(V,d)	Emergency Brake Deceleration curve is more restriced than needed (min, max value could be used instead)		RAM issue		SIL 4 software checks the correct value range.
75.		Train data – Train data information – Nominal rotating mass	**Deletion / Delay:** Loss of Nominal rotating mass	Loss of train type	FS, LS, OS, UN, SN, SR, TR, SB, PT	M_rotating_max and M_rotating_min are used to determine A_gradient Or a former M_rotating_nom is used	Safe deceleration A_safe(V,d) is more restrictive than needed.	Emergency Brake Deceleration curve is more restriced than needed.		RAM issue		

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
76.	5.5.2.5.2	Train data – Train data information – Maximum train speed	**Corruption/ Insertion:** Inappropriate reception of Maximum train speed	Falsification of “train type” or “train composition ”	FS, LS, OS, UN, SN, SR, TR, SB, PT	Maximum Train Speed is determined too high	Most Restrictive Speed Profile (MRSP) is wrongly determined (see SS-026 §3.13.7.2)	Wrong ceiling supervision limits. TI-10		Catastrophic	TI_OB-MTS, TI_VE-MTS	On-board informs driver that change in Train Data needs to be validated by driver (Subset-026, 3.18.3.3 and 5.17.2.2).
77.			**Deletion / Delay**: Loss of Maximum train speed	Loss of “train type” or “train composition ”	FS, LS, OS, UN, SN, SR, TR, SB, PT	Maximum Train Speed is determined too high (the lost values would have been lower than the stored ones)	Most Restrictive Speed Profile (MRSP) is wrongly determined (see SS-026 §3.13.7.2)	Wrong ceiling supervision limits. TI-10		Catastrophic	TI_OB-MTS, TI_VE-MTS	On-board informs driver that change in Train Data needs to be validated by driver (Subset-026, 3.18.3.3 and 5.17.2.2).

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
78.	5.5.2.6.2	Train data – Train data information – Loading gauge	**Corruption / Insertion / Deletion:** Incorrect reception of loading gauge	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components; falsification of value which is transmitted via TI or incorrect reception of “train type”, “train composition” or “tilting health status”	SB, FS, LS, SR, OS, UN, TR, PT, SN	Incorrect loading gauge is stored on-board.	Train enters a route although not suitable.	Collision with side barriers.	Operational rules for driver. Lineside signs and driver´s route knowledge; traffic planning	Catastrophic	-	

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
79.	5.5.2.7.2	Train data – Train data information – Axle load category	**Corruption / Insertion / Deletion:** Incorrect reception of axle load	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components; falsification of value which is transmitted via TI or incorrect reception of “train type” or “train composition”	SB, FS, LS, SR, OS, UN, SN	Incorrect axle load is stored on-board.	Train enters a route although not suitable.	TI-10.	Operational rules for driver. Lineside signs and driver´s route knowledge. Traffic planning.	Critical	TI_OB-ALC, TI_VE-ALC	On-board informs driver that change in Train Data needs to be validated by driver (Subset-026, 3.18.3.3 and 5.17.2.2).

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
80.	5.5.2.8.2	Train data – Train data information – Traction system(s) accepted by the engine	**Corruption / Insertion / Deletion:** Incorrect reception of an accepted traction system **Already analysed in Subset-080**	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components; falsification of value which is transmitted via TI or incorrect reception of “train type” or “train composition”								

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
81.	5.5.2.9.2	Train data – Train data information – Train fitted with airtight system	**Deletion/ Delay**: Loss of Train fitted with airtight system signal (T_AT_S = 0 instead of 1)	Any single failure of the ERTMS/ETCS on-board system or/and of the vehicle components; falsification of value which is transmitted via TI or incorrect reception of “train type”, or “train composition”	FS, LS, OS, UN, SN, SR, TR, SB, PT	Airtight system not available received from external interface when it is available. OBU informs driver.	Air conditioning intake is not controlled automatically.	Passenger could be affected by sudden change of pressure or noxious air coming inside train.	Opening/Closing air conditioning intake can be manually controlled on-board.	Marginal		On-board informs driver that change in Train Data needs to be validated by Driver (Subset-026, 3.18.3.3 and 5.17.2.2).

Line No.	Ref ID	Macro Function: Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			External Protection / Mitigation / Barriers	Severity	Event-ID	Internal Barriers
						Local	Inter-mediate	Initial End Effect				
82.			**Corruption/ Insertion:** Inappropriate reception of Train fitted with airtight system signal (T_AT_S = 1 instead of 0) **Already analysed in Subset-080**	Falsification of value which is transmitted via TI or incorrect reception of “train type”, or “train composition ”								
83.	5.6.1.2	National System Isolation	Level NTC only, see Subset-080.									

6.2 Fault Trees

6.2.1.1 The fault tree tool adopted for the analysis work is Isograph Fault Tree+ in version 11.0. This tool allows the graphical modelling and the quantitative calculation of fault trees.

6.2.1.2 In FaultTree+ all compositions are calculated with the help of unavailability (Q, dimensionless) and the failure frequency (w, failure/h).

6.2.1.3 FaultTree+ uses the following terms which deviates from terminology of technical literature:

- r for failure rate λ,
- w for failure frequency ω, and
- tau for inspection interval τ

6.2.1.4 With Q << 1 as it is the case in practice w ≈ r is valid.

6.2.1.5 Normally the FTA fault model dormant has been used.


FTA_TI_2019-06.psa

FTA-2019-06.pdf