ERTMS/ETCS

Failure Modes and Effects Analysis for TIU in Application Level 1 and Level 2

REF : SUBSET-080
ISSUE : 3.3.0
DATE : 09-05-24

Company	Technical Approval	Management approval
ALSTOM		
AZD		
CAF		
HITACHI RAIL STS		
MERMEC		
SIEMENS		
THALES		

1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.0.1. 16/03/01	ALL	Creation	S. Chassard
0.0.2 26/02/02	5	Revised after comments and to achieve consistency with subset 88	SCH
2.0.0.	3.1.1.2.	Raised in issue for release to the EEIG.	WLH
2.2.2.		Final release after amendment to reflect the comments in the final report from the ISA's version 1.1 dated 07-03-03 as proposed via the Unisig consolidated review comments on the ISA report v 0.0.2 March 03.	WLH
3.0.0	ALL	Update to SRS Baseline 3.3.0	C. Latorre (MERMEC)
3.0.1	ALL	Update followed to RAMS WG meeting of 03-04 July 2012 (Stockholm)	C. Latorre (MERMEC)
3.0.2	ALL	Update followed to RAMS WG comments	C. Latorre (MERMEC)
3.0.3	ALL	Update followed to RAMS WG conf call meeting of 09 October 2012 (see MoM 'RAMS Meeting nr 2012:10 – telecon 2012-10-09').	C. Latorre (MERMEC)
3.0.4	- Footer of the first section. - 5.4.1.4. - Chapter 8. - 5.4.1.1.	Some editorial changes. Comments from NK and JPG have been considered in 5.4.1.1.	C. Latorre (MERMEC)
3.0.5	- FMEA ref. Id. 5.6.1, 5.6.2, 5.4.1.4, 5.3.1.1, 5.3.2.1, 5.3.3.1, 5.3.4.1, 5.3.5.1, 5.3.7.1, 5.3.8.1. - Chapter 7.	Update followed to TIU Safety Group's comments reported in MoM 'RAMS Meeting nr 2012:11 – Madrid 2012-10-25/26' v002.	C. Latorre (MERMEC)

	- Section 5.2.6. - Table 4.		
3.0.6	- FMEA ref. Id. 5.4.2.8 - 5.2.6.1 - FMEA ref. Id. 5.3.6.2 - FMEA ref. Id. 5.4.1.7 - FMEA ref. Id. 5.4.2.8 - FMEA ref. Id. 5.6.5 - FMEA ref. Id. 5.6.10 - section 7.1.2	Comments on S-080 v3.0.5 from JPG have been considered.	C. Latorre (MERMEC)
3.0.7	- FMEA ref. Id. 5.1.1.2 - section 5.2.3.2 - FMEA ref. Id. 5.3.9.1 (TCO) - section 7.1.3 (Assumption for TCO) - FMEA ref. Id. 5.1.2.1 - FMEA ref. Id. 5.1.3.2 - FMEA ref. Id. 5.6.1 - FMEA ref. Id. 5.6.2	Comments on S-080 v3.0.6 from TIU Safety Group.	C. Latorre (MERMEC)
3.0.8	- FMEA ref. Id. 5.2.2.2 - Added section 7.1.4 'Brake Pressure'	Analysis modified as consequence of SG's answer about Service Brake application's feedback.	C. Latorre (MERMEC)
3.0.9	- 5.2.3.2 - 5.2.3.3 - section 5.2.6 - section 5.2.7 - Section 5.3.6 - Section 5.4.3 - Inserted new row in FMEA for 'Train data – Other International Train Categories' (section 5.6) - inserted FMEA Id 5.6.3 - update FMEA id 5.6.5	Emergency Brake Command Feedback and Status noted as to be deleted from the analysis since not more considered in current S-034 version. Updated Special Brake Status Analysis and Additional Brake Status due to S-034 modification. Passenger Door output has been renamed to Station Platforms according to current S-034 version The FMEA row of Train Integrity input has been removed since according to S-034 the input has to be harmonized.	C. Latorre (MERMEC)

	- update FMEA id 5.6.6 - updated chapter 6 for S-034 references - updated chapter 7	Inserted Analysis for Train data – Other International Train Categories. Updated analysis for Train data – traction/brake parameters (consistency with S-120) Updated analysis for Train data – maximum train speed (consistency with S-120) Added application constraints in Conclusion Chapter for: • Special Brake Status Input • Station Platforms Input • Train Data – Maximum Train Speed • Train Data – Traction/Brake parameters	
3.0.10	ALL	Update to SRS Baseline 3.3.1	C. Latorre (MERMEC)
3.0.11		Updated during RAMS-meeting	DARI
3.0.12 2014-10-27		Baseline 3 1st maintenance release version	DARI, F. Bitsch
3.1.0		Modifications due to CR239, CR539, CR1163, CR1258 Rejection	C. Latorre (MERMEC)
3.1.1		Chnges from Unisig_RAMSWG_COM_SS-080v3.1.0_v1.0 review and comments from CAF (AV)	C. Latorre (MERMEC)
3.1.2	5.5 Editorial change to FMEA Ref Id 7.1.1	Editorial change to FMEA Ref Id Added a clause to section 'Conclusion – Application Constraint' 7.1.1	C. Latorre (MERMEC)
3.1.3	FMEA 5.5.2.1 and 5.5.2.2 FMEA 5.5.2.9 Clause 7.1.1.8	After RAMS meeting (2016:02) discussion, the analysis have been updated in: - Train Data - Train Category (Cant Deficiency)	C. Latorre (MERMEC)

		- Train Data - Traction system(s) accepted by the engine -> change in Mode Field - Internal Barrier -> Driver validation according specific project	
3.1.4	FMEA 5.2.6.1 FMEA 5.4.1.3 FMEA 5.5.2.2 FMEA 5.5.2.4 FMEA 5.5.2.9 FMEA 5.5.2.10 Table 1 FMEA 5.3.4.1 FMEA 5.4.1.4 Clause 7.1.1.6 Chapter 8	- Change following comments received from CAF. - Change following comments received from THALES. - Severity in 5.4.1.4 changed to catastrophic after CAF comment - Clause 7.1.1.6 reports new assumption of FMEA 5.4.1.4 - Chapter 8: TI-6a deleted from the item list of the note	C. Latorre (MERMEC)
3.1.5	FMEA 5.4.1.4 Clause 7.1.1.6 Chapter 8	- Severity in 5.4.1.4 changed to RAM Issue after RAMS Meeting discussion - Clause 7.1.1.6 reports assumption of FMEA 5.4.1.4 - Chapter 8: TI-6a deleted	C. Latorre (MERMEC)
3.1.6	Chapter 8	- Minor change due to RAMS WG comments	C. Latorre (MERMEC)
3.2.0 2016-06-20	No change	Baseline 3 2nd release version	RAMS WP
3.2.1	FMEA 5.1.3.4	- New row 5.1.3.4 added in FMEA §5.1.3 Non-Leading	C. Latorre (MERMEC)
3.2.2	General Update for TSI 2022	Modification for CR1346 (output Remote Shunting) Modification for CR 940 (Train Integrity Input).	C. Latorre (MERMEC)

		Modification for CR1238 (ATO function, AD output) New row 5.3.3.1 Modification For CR1290 (Train Running Number Input) Editorial Change For CR1341 (Unauthorised Direction Movement Protection) Modification For CR 1367 (SUPERVISED MANOEUVRE, Overall Consist length Input) Modification for CR 1342 (L2/L3 -> LR)	
3.2.3	§5.3.11 ‘Engine Orientation in Supervised Manoeuvre’. General updated after comment from RAMS WG review.	- New Output Engine Orientation in Supervised Manoeuvre. - General updated after comment from RAMS WG review	
3.2.4	FMEA Table §7.1.1 ‘Application Constraint’	- AD mode added where missing in FMEA Table. - Row 5.1.6.2 ‘Remote Shunting’ split using additional row 5.1.6.3 for managing different ETCS mode. - Row 5.4.3.3 and 5.4.3.4 ‘Train Integrity’ ‘ETCS external barrier’ and ‘Internal barrier’ columns updated. - Editorial, ‘Safe Consist Length’ renamed as ‘Overall Consist Length’ - 7.1.1.3 Application Constraint added for ‘Special Brake Status’	

		- 7.1.1.10 Application Constraint added for ‘Train Data Train Length’. - 7.1.1.15 Application Constraint added for ‘Train Data Train Length’ during intentional train splitting.	
3.2.5	FMEA 5.4.3.3, 5.4.3.4 Train integrity Application Constrain 7.1.1.15 ‘train integrity’	- Internal barrier update claiming clause S-034 §2.3.5.2.2 - Update of Application constraint claiming clause S-034 §2.3.5.2.2	
3.2.6	FMEA 5.4.1.10, 5.4.1.11 Cab Status and related Application Constrain 7.1.1.7 ‘Cab Status’. Annex A.	- Failure Mode related to opposite cab status considered as valid.	
3.2.7	FMEA 5.4.1.10 Cab Status for mode SM	- General: LR changed in L2 - Analysis for mode SM has been changed.	
3.2.8	FMEA 5.4.3.3, 5.4.3.4 Train integrity Application Constrain 7.1.1.15 ‘train integrity’	- S-034 reference clause amended.	
3.2.9	General review, FMEA 5.4.2.8	- Quality review after SG comments - Row 5.4.2.8 removed since Direction Controller not relevant in NL	
3.3.0 09-05-24	No change	Baseline 4 release version	RAMS WP

2. TABLE OF CONTENTS

3. INTRODUCTION

The purpose of this document is to provide an FMEA (Failure Modes Effects Analysis) for the ERTMS onboard interface with train in ERTMS application level 1 and in level 2.

The inputs documents used as a basis for this study are:

[Ref. 1] SUBSET-026, UNISIG SRS

[Ref. 2] SUBSET-034, FIS for the Train Interface

[Ref. 3] ETCS Driver Machine Interface - ERA_ERTMS_015560

[Ref. 4] SUBSET-035, Specific Transmission Module FFFIS

[Ref. 5] SUBSET-077, Causal Analysis Process.

[Ref. 6] Extract from Deliverable D6.1 "Results of feasibility studies and laboratory tests for candidate technologies selection and adaptation of existing solutions", X2Rail-4

This analysis is based on the reference architecture provided in SUBSET-026 Chapter 2.

4. ASSUMPTIONS

4.1.1.1 The functions analysed in this document are those specified in the FIS TIU [Ref. 2] and listed in chapter 2 of the same document.

4.1.1.2 Failures identified as leading to a RAM issue are not developed further.

4.1.1.3 Special Braking orders and status are handled as a whole no matter which type of brake is applied (eddy current brake, regenerative brake, magnetic shoe brake, etc.).

4.1.1.4 The Traction Status input has been excluded from this analysis since the effects related to its failures depend by the use made of Traction Status information by STM in level NTC.

5. FMEA

This FMEA study has been conducted according to FMEA process defined in SUBSET-077 [Ref. 5].

Deviating from the FMEA definition in SUBSET-077, the column 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-XX hazardous events in SUBSET-091 (ETCS Core Hazard coverage).

5.1 Mode Control

5.1.1 Sleeping

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	**Intermediate**	**Initial End Effect**				
5.1.1.1	Sleeping Command information (SLEEPING REQUESTED/SLEEPING NOT REQUESTED)	**Absent** **Incorrect** Failure to report “sleeping requested”	- TIU Failure - ETCS onboard failure other than TIU	SB, PS	“Sleeping requested” state is not provided to board	On-board ETCS does not know if it has to go to sleeping	On-board remains in SB, PS mode		RAM Issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.1.1.2		**Incorrect Insertion** Inappropriate selection of "Sleeping requested"	- TIU Failure - ETCS onboard failure other than TIU	SB	"Sleeping requested" state unduly selected during normal operation	Loss of Standstill protection	Exceedance of safe speed or distance as advised to ETCS	Operational rule: Driver has to ensure the standstill before closing the cab.	Catastrophic	TI-3	
5.1.1.3		**Incorrect Insertion** Inappropriate selection of "Sleeping requested"	- TIU Failure - ETCS onboard failure other than TIU	PS	Sleeping unduly selected during normal operation	-	On-board transits in SL mode		RAM issue		Vehicle must be at "standstill"
5.1.1.4		**Incorrect Insertion** Failure to maintain "Sleeping requested" state	- TIU Failure - ETCS onboard failure other than TIU	SL	"Sleeping requested" state deactivated prematurely	ETCS OB switches to SB mode	Leading Engine cannot proceed. 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.		marginal	TI-3	Transition to SB mode is not possible if vehicle is not at standstill. The engine is remote controlled by the leading engine (Subset-026, 4.4.6.1.3).

5.1.2 Passive Shunting

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.1.2.1	Passive shunting information (PASSIVE SHUNTING PERMITTED/PASSIVE SHUNTING NOT PERMITTED)	**Incorrect Insertion** Inappropriate selection of "Passive shunting permitted"	- TIU Failure - ETCS onboard failure other than TIU	SH	"Passive shunting permitted" information is provided to On-board ETCS when not required	At desk closure, On-Board ETCS switches in PS Mode instead of SB. Standstill supervision function no more provided.	Exceedance of safe speed or distance as advised to ETCS	Driver has to ensure the standstill (e.g. by applying the parking brake before leaving the cab).	Catastrophic	TI-7	"Continue Shunting on desk closure" function is active.

© This document has been developed and released by UNISIG

5.1.3 Non-Leading

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.1.3.1	Non-Leading information (NON LEADING PERMITTED – NON LEADING NOT PERMITTED)	**Absent Incorrect** Failure to report "Non Leading permitted"	- TIU Failure - ETCS onboard failure other than TIU	SB, SH, FS, AD, LS, SR, OS,SM	"Non Leading permitted" information is not provided to On-board ETCS	On-board ETCS is not allowed to switch in NL mode and remains in the current mode. Train supervision functions active according to the current mode.	ETCS On-board equipped on non leading engine can command EB during Non-Leading Engine movement.	Driver shall expect the transition to NL mode before moving Non Leading Engine.	RAM issue		
5.1.3.2		**Incorrect Insertion** Inappropriate selection of "Non Leading permitted"	- TIU Failure - ETCS onboard failure other than TIU	SB, SH, FS, AD, LS, SR OS, SM	"Non Leading permitted" information is provided to On-board ETCS when not required	On-board ETCS switches to NL mode after driver selection when not required. Loss of supervision.	Exceedance of safe speed or distance as advised to ETCS.	New mode is displayed on the DMI. Driver is not going to leave the cab.	Catastrophic	TI-8	Driver selects NON LEADING on DMI and Vehicle is at standstill
5.1.3.3		**Incorrect Insertion** Failure to maintain "Non Leading permitted"	- TIU Failure - ETCS onboard failure other than TIU	NL	"Non Leading not permitted" information provided to On-board ETCS when not required	On-board ETCS switches to SB mode when not required activating standstill supervision	Vehicle cannot proceed		RAM issue		Vehicle is at standstill

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.1.3.4		**Absent** **Incorrect** Report "Non Leading permitted" which is not correct	- TIU Failure - ETCS onboard failure other than TIU	NL	"Non Leading permitted" information is provided to On-board ETCS when not required	When at standstill the ETCS on-board stays in NL mode instead of switching to SB mode.		NL mode is displayed on the DMI. Driver is not leaving the cab as long as the on-board is in NL mode.	RAM issue		Driver is only able to go to SB, NP or IS mode.

5.1.4 Isolation

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.1.4.1	Isolation output (ETCS ISOLATED/ETCS NOT ISOLATED)	**Absent incorrect** Failure to transmit ETCS ISOLATED state to the vehicle	- TIU Failure - ETCS onboard failure other than TIU	IS	Information received by vehicle is “ETCS OBU not isolated” but ETCS OBU is isolated	Related to the function for which the output information is used for. No effect on ETCS supervision	-		RAM Issue		
5.1.4.2		**Incorrect Insertion** Faulty Transition to ETCS ISOLATED state	- TIU Failure - ETCS onboard failure other than TIU	All Modes	Information received by vehicle is “ETCS OBU isolated” but ETCS OBU is not isolated.	DMI continues displaying current mode information.	-	The driver knows when the OBU is isolated and will be informed of the isolation mode.	RAM Issue		Isolation status must be shown to the driver (Subset 026 4.4.3.1.2).

5.1.5 Automatic Driving

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.1.5.1	Automatic Driving	**Absent / Incorrect**: Failure to transmit AD Mode State	- TIU Failure - ETCS onboard failure other than TIU	AD	Information AD mode is not given to Rolling Stock	The Rolling Stock ignores any traction/brake command coming from the ATO-OB which is not intended.	Performance impact: No traction / braking is possible by ATO. No direct safety impact: ETCS on-board activates the EB if needed.	Driver reacts by changing the mode	RAM Issue		
5.1.5.2	Automatic Driving	**Incorrect / Insertion**: Faulty trasmission of AD Mode State	- TIU Failure - ETCS onboard failure other than TIU	SH, FS, SM, LS, SR, OS, NL, UN, PT, RV	Information AD mode is given to Rolling Stock although the ETCS on-board is not in AD mode	The Rolling Stock disables the traction command from the driver (but not the braking commands) and enables the traction/braking and door commands from the ATO on-board.	Performance impact: No traction command can be given by the driver. The only hazardous situation could be when the train is blocked in a location from where it needs to escape.	ATO on-board gives driving commands only if ATO is in the state EG (Engaged) so that ATO is not active in this case.	Marginal		

5.1.6 Remote Shunting

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.1.6.1	Remote Shunting output (ETCS on-board is in a mode permitting remote shunting/ETCS on-board is not in a mode permitting remote shunting)	**Absent incorrect** Failure to transmit to the vehicle transmit that ETCS on-board state is in a mode permitting remote shunting	- TIU Failure - ETCS onboard failure other than TIU	SH	Information “ERTMS/ETCS on-board is in a mode permitting remote shunting” is not given to Rolling Stock	A radio remote control device, that is operated by the train driver in near distance (visual range) to the vehicle cannot be active.	No remote shunting possible	-	RAM Issue	-	
5.1.6.2		**Incorrect Insertion** Faulty information to the vehicle that ETCS on-board is not in a mode permitting remote shunting	- TIU Failure - ETCS onboard failure other than TIU	FS, AD, LS, OS, SM	Information “ERTMS/ETCS on-board is in a mode permitting remote shunting” is given to Rolling Stock erroneously	ETCS on-board unit is not in SH mode only whilst the radio remote control is active	Safe speed and distance is supervised by ETCS and driver can be assumed at the train desk.	Driver is at the train desk since SOM is needed to transit in given modes.	RAM Issue	-	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.1.6.3		**Incorrect Insertion** Faulty information to the vehicle that ETCS on-board is not in a mode permitting remote shunting	- TIU Failure - ETCS onboard failure other than TIU	SR, UN, PT, RV, NL	Information “ERTMS/ETCS on-board is in a mode permitting remote shunting” is given to Rolling Stock erroneously	ETCS on-board unit is not in SH mode only whilst the radio remote control is active	Driver can be assumed at the train desk.	Driver is at the train desk since SOM is needed to transit in given modes.	RAM Issue	-	
5.1.6.4		**Incorrect Insertion** Faulty information to the vehicle that ETCS on-board is not in a mode permitting remote shunting	- TIU Failure - ETCS onboard failure other than TIU	PS, SL	Information “ERTMS/ETCS on-board is in a mode permitting remote shunting” is given to Rolling Stock erroneously.	The desk of a Passive Shunting/Sleeping engine is closed and the engine is coupled to a leading engine who is in charge with the train movement supervision.	Leading engine takes responsibility of the train.	Leading engine takes responsibility of the train.	RAM issue	-	-

5.2 Control of Brakes

5.2.1 Service Brake Command

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Enent-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.2.1.1	Service Brake command (SERVICE BRAKE COMMANDED / SERVICE BRAKE NOT COMMANDED)	**Absent** **Incorrect** Failure to Command Brake Application when required	- TIU Failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS	SB application command (SERVICE BRAKE COMMANDED state) not transmitted to the vehicle	SB Not activated when required. Emergency Brake application when passing the EBI limits or before any other critical situation in all cases where EBI limits protect the train. In situations where EBI limits are not active (e.g. Protection against undesirable movements Subset-026, 3.14) EB is applied as consequence of the SB application failure (Subset-026, 3.14.1.2).	Vehicle at standstill after EB has been applied	Application Constraints: If the ETCS Onboard is implemented using Service Brake to protect the train against undesirable movements, then a project specific safety analysis is needed in order to show that the failure of this signal is recognized and the EB is applied as safeguarding.	RAM Issue		Subset-026, 3.14.1.2: "In case only the application of (the non-vital) service brake has been commanded and the service brake fails to be applied, the emergency brake command shall be given."

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Enent-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.2.1.2		**Incorrect Insertion** Faulty Transition to SERVICE BRAKE COMMANDED state	- TIU Failure - ETCS onboard failure other than TIU	All modes	SB application command (SERVICE BRAKE COMMANDED state) transmitted to the vehicle while not required	SB activated when not required	Vehicle unduly braked		RAM Issue		

5.2.2 Brake Pressure

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.2.2.1	Brake Pressure	**Absent Incorrect Insertion** Failure to report Brake Pressure information	- TIU Failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, RV, SH, SN	Wrong Brake Pressure information sent on-board	1) Erroneous Brake Pressure state used in the service brake feedback model by ETCS-OBU. T_bs1 and T_bs2 (service brake build up time) misjudged due to erroneous input.Calculated T_bs less than expected implies wrong calculation of SBI location. 2) In case Brake Pressure input is used as Service Brake feedback, erroneous brake pressure could lead to consider the service brake erroneously applied. 3) In case Brake Pressure input s not used as Service Brake feedback, no effect	1) and 2) Service Brake will be applied later than required. Emergency Brake application when passing the EBI limits or before any other critical situation. Vehicle at standstill after EB has been applied in all cases where EBI limits protect the train. In situations where EBI limits are not active (e.g. Protection against undesirable movements Subset-026, 3.14) if OBU uses service brake to stop the train and brake pressure as brake feedback, the loss of train undesirable movement protection occurs in case of failure to service brake.	Application Constraint: If the ETCS Onboard 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 analysis is needed in order to show that the failure of the signal has acceptable safety consequences.	RAM Issue		Independent failure to service brake output.

5.2.3 Emergency Brake Command

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.2.3.1	Emergency Brake command (EMERGENCY BRAKE COMMANDED / EMERGENCY BRAKE NOT COMMANDED)	**Absent Incorrect** Failure to Command Emergency Brake Application when required	- TIU Failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS	EB application command (EMERGENCY BRAKE COMMANDED state) not transmitted to the vehicle	EB Not activated when required	Exceedance of safe speed or distance as advised to ETCS	Product specific safeguarding	Catastrophic	TI-1	
5.2.3.2		**Insertion Incorrect** Brakes Application Commanded when not required	- TIU Failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS	EB application command (EMERGENCY BRAKE COMMANDED state) transmitted to the vehicle while not required	EB activated when not required	Vehicle incorrectly brought to stand-still		RAM Issue		

5.2.4 Special Brake Inhibition Area – Trackside Orders

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.2.4.1	Special Brake Inhibition Area – Trackside Order • the remaining distance from the max safe front end of the train to the start location of this special brake inhibition area • the remaining distance from the min safe rear end of the train to the end location of this special brake inhibition area	**Absent Incorrect** Failure to the information output leading to not request Special Brake inhibition when required	- TIU Failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS	Special Brake inhibition request not transmitted to the vehicle when required	Special Brake not inhibited although required by trackside. Special Brake Status informs OBU that Special Brake is not inhibited.	Special Brake are erroneously applied when EB/SB are requested, in a section where they should not be used. Possible damages to trackside infrastructure (e.g. to the tracks).		RAM Issue		

© This document has been developed and released by UNISIG

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.2.4.2		**Insertion** **Incorrect** Failure to the information output leading to request Special Brake inhibition when not required	- TIU Failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, SH, SB, RV	Special Brake inhibition request transmitted to the vehicle when not required	Special Brake inhibited although not required by trackside. Special Brake Status informs OBU that Special Brake is inhibited. OBU updates SB/EB braking curves according to current special brake status.	Emergency Brake applied by the vehicle before than expected by ETCS-OBU		RAM Issue		

5.2.5 Special Brake Inhibit – STM Orders

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.2.5.1	Special Brake Inhibit – STM Order (NOT INHIBITED/INHIBITED)	**Absent Incorrect** Failure to Request Special Brake inhibition when required	- TIU Failure - ETCS onboard failure other than TIU	SN	Special Brake inhibition request (INHIBITED state) not transmitted to the vehicle when required	Special Brake not inhibited although required by trackside. Special Brake Status informs OBU that Special Brake is not inhibited.	Special Brake are erroneously applied when EB/SB are requested, in a section where they should not be used. Possible damages to trackside infrastructure (e.g. to the tracks).		RAM Issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.2.5.2		**Insertion** Request Special Brake inhibition when not required	- TIU Failure - ETCS onboard failure other than TIU	SN	Special Brake inhibition request (INHIBITED state) transmitted to the vehicle when not required	Special Brake inhibited although not required by trackside. Special Brake Status informs OBU that Special Brake is inhibited. OBU updates SB/EB braking curves according to current special brake status.	Emergency Brake applied by the vehicle before than expected by ETCS-OBU		RAM Issue		

5.2.6 Special Brake Status

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.2.6.1	Special Brake Status (SPECIAL BRAKE ACTIVE/SPECIAL BRAKE NOT ACTIVE)	**Absent Incorrect Insertion** The input wrongly reports to ETCS-OBU that Special Brake is not active when actually it is	- TIU Failure - ETCS onboard failure other than TIU	FS, AD, LS, SR,OS, SM, UN	Status Information of SPECIAL BRAKE ACTIVE is not transmitted to ETCS-OBU when required or delayed	The braking curve used by ETCS-OBU assumes an Emergency Brake Capability lower than the actual. Wrong status on the DMI.	Emergency Brake applied by ETCS-OBU before than expected.	Driver knows the real status of Special Brake	RAM Issue		
5.2.6.2		**Incorrect Insertion** The input wrongly reports to ETCS-OBU that Special Brake is active when actually it is not	- TIU Failure - ETCS onboard failure other than TIU	FS, AD, LS, SR, OS, SM, UN	Special Brake Status is inappropriately reported as active to ETCS-OBU when actually it is not	Emergency Brake Capability less than assumed by ETCS Brake model, wrong curve calculation. Failure to display brake status to driver.	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.

5.2.7 Additional Brake Status

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.2.7.1	Additional Brake Status (ADDITIONAL BRAKE ACTIVE/ADDITIONAL BRAKE NOT ACTIVE)	**Same analysis as described in 5.2.6**									

5.3 Control of Train

5.3.1 Change of Traction System (CTS)

ef ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.1.1	Change Of Traction System	**Deletion** **Corruption** **Delay** **Repetition** **Insertion** The output information used to change the Traction System is erroneous or missing or delayed so that the traction system will not be changed when required	- TIU Failure - ETCS onboard failure other than TIU	All modes	The Change of Traction System output information OR Engine orientation in Supervised Manoeuvre is not properly transmitted to the vehicle so that the vehicle will not execute the change of traction when required	Traction System does not change when required or changes when not required.	Vehicle is fed with a non-appropriate traction system. Possible damage to infrastructure	Vehicle should be equipped with protection systems. Driver should be able to control the pantograph manually.	RAM Issue		Change of traction system is announced and indicated to the driver on the DMI (S-026 §5.18.10)

5.3.2 Powerless section with pantograph to be lowered – Trackside orders

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.2.1	Powerless section with pantograph to be lowered – Trackside orders	**Deletion** **Corruption** **Delay** **Repetition** **Insertion** The output information used to lower the pantograph is erroneous or missing or delayed so that the pantograph will be not in the lowered/raised status when required	- TIU Failure - ETCS onboard failure other than TIU	All modes	The Pantograph – Trackside output orders used to lower the pantograph OR Engine orientation in Supervised Manoeuvre is not properly transmitted to the vehicle so that the vehicle will not lower/raise the pantograph when required	Pantograph lowered/raised when not required	No Power to traction unit	Driver should be able to control the pantograph manually.	RAM Issue		Powerless section with pantograph to be lowered is announced and indicated to the driver on the DMI (S-026 §5.18.2)

5.3.3 Pantograph – STM Order

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.3.1	Pantograph – STM Order	**Deletion** **Corruption** **Delay** **Repetition** **Insertion** The output information used to lower the pantograph is erroneous or missing or delayed so that the pantograph will be not in the lowered/raised status when required	- TIU Failure - ETCS onboard failure other than TIU	SN	The Pantograph – Trackside output orders used to lower the pantograph is not properly transmitted to the vehicle so that the vehicle will not lower/raise the pantograph when required	Pantograph lowered/raised when not required	No Power to traction unit	Driver should be able to control the pantograph manually.	RAM Issue		Assumption for STM: Powerless section with pantograph to be lowered is announced and indicated to the driver on the DMI (compare S-026 §5.18.2)

© This document has been developed and released by UNISIG

5.3.4 Air tightness area– Trackside orders

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.4.1	Air Tightness area – Trackside Order	**Deletion** **Corruption** **Delay** The output information used for commanding the flaps closure is erroneous or missing or delayed so that the Air Conditioning intake will be open when not required	- TIU Failure - ETCS onboard failure other than TIU	All modes	The output information used for commanding the flaps closure OR Engine orientation in Supervised Manoeuvre is not properly transmitted to the vehicle so that the vehicle will not close the flaps when required	Air Conditioning intake not closed when required.	Passenger could be affected by sudden change of pressure or noxious air coming inside train	Driver should be able to control the air conditioning intakes manually.	Critical	No relation to ETCS Core hazard	Air tightness area is announced and indicated to the driver on the DMI (S-026 §5.18.6).

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.4.2		**Corruption** **Repetition** **Insertion** The output information used for commanding the flaps closure is erroneous so that the Air Conditioning intake will be closed when not required	- TIU Failure - ETCS onboard failure other than TIU	All modes	The output information used for commanding the flaps closure OR Engine orientation in Supervised Manoeuvre is not properly transmitted to the vehicle so that the vehicle will close the flaps when not required	Air Conditioning intake closed when not required	Unfavourable climate condition inside the train	Driver should be able to control the air conditioning intakes manually.	RAM Issue		

5.3.5 Air tightness – STM Order

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.5.1	Air tightness – STM Order	**Deletion** **Corruption** **Delay** The output information used for commanding the flaps closure is erroneous or missing or delayed so that the Air Conditioning intake will be stay open when not required	- TIU Failure - ETCS onboard failure other than TIU	SN	The output information used for commanding the flaps closure is not properly transmitted to the vehicle so that the vehicle will not close the flaps when required	Air Conditioning intake not closed when required	Passenger could be affected by sudden change of pressure or noxious air coming inside train	Driver should be able to control the air conditioning intakes manually.	Critical	No relation to ETCS Core hazard	Assumption for STM: Air tightness area is announced and indicated to the driver on the DMI (compare S-026 §5.18.6).

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.5.2		**Corruption** **Repetition** **Insertion** The output information used for commanding the flaps closure is erroneous so that the Air Conditioning intake will be closed when not required	- TIU Failure - ETCS onboard failure other than TIU	All modes	The output information used for commanding the flaps closure is not properly transmitted to the vehicle so that the vehicle will close the flaps when not required	Air Conditioning intake closed when not required	Unfavourable climate condition inside the train	Driver should be able to control the air conditioning intakes manually.	RAM Issue		

5.3.6 Station Platform

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.6.1	Station Platform	**Deletion** **Corruption** **Delay** The output information 'Station Platform' used for enabling the passenger door is erroneous or missing or delayed so that the passenger door will not be open when required	- TIU Failure - ETCS onboard failure other than TIU	All modes	The output information used for enabling the passenger door OR Engine orientation in Supervised Manoeuvre is not properly transmitted to the vehicle so that the vehicle will not open the passenger door when requested by the driver	Passenger door opening disabled when not required	Passenger door does not open when externally required	Assumption: The ETCS door opening enabling function is not for safety reasons, e.g. in cases of evacuation. There is an emergency procedure to open the doors.	RAM Issue		

© This document has been developed and released by UNISIG

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.6.2		**Corruption** **Repetition** **Insertion** The output information of Station Platform used for passenger door enabling is erroneous so that the passenger door opening will be enabled when not allowed	- TIU Failure - ETCS onboard failure other than TIU	All modes	The output information used for enabling is not OR Engine orientation in Supervised Manoeuvre properly transmitted to the vehicle so that the passenger door opening will be enabled when not allowed	ETCS OBU does not inhibit the opening of passenger door when required	Passengers could be injured / run over when leaving the train.	Doors should be controlled manually by the driver (e.g. independent switches which control each side doors).	Critical	No relation to ETCS Core hazard	

.

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

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.7.1	Powerless section with main power switch to be switched off – Trackside orders	**Deletion** **Corruption** **Delay** The output information used to switch off the main power switch is erroneous or missing or delayed so that the main power will not be switched off when required	- TIU Failure - ETCS onboard failure other than TIU	All modes	The output information used to switch off the main power OR Engine orientation in Supervised Manoeuvre is not properly transmitted to the vehicle so that the vehicle will not switch off the main power when required	Main power switch is not opened where necessary.	Main power switch is not opened in powerless section	Driver should be able to control the main power switch manually.	RAM Issue		Powerless section with main power switch to be switched off is announced and indicated to the driver on the DMI (S-026 §5.18.3).
5.3.7.2		**Corruption** **Repetition** **Insertion** The output information used to Switch Off the main power switch is erroneous so that the main power will be switched off when not required	- TIU Failure - ETCS onboard failure other than TIU	All modes	The output information used to switch off the main power OR Engine orientation in Supervised Manoeuvre is not properly transmitted to the vehicle so that the vehicle will switched off the main power when not required	Main power switch is opened where not necessary.	Main power switch is opened before or after a powerless section	Driver should be able to control the main power switch manually.	RAM Issue		

5.3.8 Main Power Switch – STM Order

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.8.1	Main Power Switch – STM Order	**Deletion** **Corruption** **Delay** The output information used to Switch Off the main power switch is erroneous or missing or delayed so that the main power will not be switched off when required	- TIU Failure - ETCS onboard failure other than TIU	SN	The output information used to switch off the main power is not properly transmitted to the vehicle so that the vehicle will not switch off the main power when required	Main power switch is not opened where necessary.	Main power switch is not opened in powerless section	Driver should be able to control the main power switch manually.	RAM Issue		Assumption for STM: Powerless section with main power switch to be switched off is announced and indicated to the driver on the DMI (compare S-026 §5.18.3).

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.8.2		**Corruption** **Repetition** **Insertion** The output information used to Switch Off the main power switch is erroneous so that the main power will be switched off when not required	- TIU Failure - ETCS onboard failure other than TIU	All modes	The output information used to switch off the main power OR Engine orientation in Supervised Manoeuvre is not properly transmitted to the vehicle so that the vehicle will switch off the main power when not required	Main power switch is opened where not necessary.	Main power switch is opened before or after a powerless section	Driver should be able to control the main power switch manually.	RAM Issue		

5.3.9 Traction Cut Off

Note that [Ref. 2] mentions the possibility for a TCO command being issued by an STM. This is not considered here.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.9.1	Traction Cut-off (TCO) application command (DO NOT CUT OFF TRACTION/CUT OFF TRACTION)	**Absent** **Incorrect** Failure to Command TCO when required	- TIU Failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, SH, SN, RV	TCO application command (CUT OFF TRACTION state) not transmitted to the vehicle when required.	Unable to cut the traction at warning limit	EBI limits are calculated considering incorrect braking / traction model assuming that residual traction has impact on braking distance. Exceedance of safe speed or distance as advised to ETCS.	If the ETCS/ERTMS on-board equipment is configured to T_traction = MAX((T_traction_cut_off - (T_warning + T_bs2)) ; 0) (see Subset-026, section 3.13.9.3.2.3) the failure of this output shall be considered as having a catastrophic safety severity and product specific safeguarding have to be considered. If the ETCS/ERTMS on-board equipment is configured to T_traction = T_traction_cut_off the failure of this output is to be considered as having a RAM severity.	Catastrophic	TI-11	

© This document has been developed and released by UNISIG

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.9.2		**Insertion Incorrect** Request TCO when not required	- TIU Failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS	TCO application command (CUT OFF TRACTION state) transmitted to the vehicle while not required	TCO activated when not required	Vehicle incorrectly held without traction		RAM Issue		

© This document has been developed and released by UNISIG

5.3.10 Change of allowed current consumption

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.10.1	Change Of Allowed Current Consumption	**Deletion** **Corruption** **Delay** **Repetition** **Insertion** The output information used to change the Allowed Current Consumption is erroneous or missing or delayed so that the Allowed Current Consumption will not be changed when required	- TIU Failure - ETCS onboard failure other than TIU	All modes	The output information used to change the Allowed Current Consumption OR Engine orientation in Supervised Manoeuvre is not properly transmitted to the vehicle so that the vehicle will not execute the change when required	Allowed Current Consumption do not change when required	Vehicle performs higher current consumption that permitted. Trackside equipment is shut down.		RAM Issue		

.

5.3.11 Engine orientation in Supervised Manoeuvre

As stated in the note 2.4.11.2 of [Ref. 2], this output is generated by the ERTMS/ETCS on-board in Supervised Manoeuvre mode to indicate to the train how to interpret the outputs “Change of traction system”, “Powerless section with pantograph to be lowered – Trackside orders”, “Air tightness area – Trackside orders”, “Station platform”, “Powerless section with main power switch to be switched off – Trackside orders” and

“Change of allowed current consumption”. The failure effect to ‘Engine orientation in Supervised Manoeuvre’ output is analysed into FMEA row related to outputs:

- “Change of traction system” (§5.3.1);
- “Powerless section with pantograph to be lowered – Trackside orders” (§5.3.2);
- “Air tightness area – Trackside orders” (§5.3.4);
- “Station platform” (§5.3.6);
- “Powerless section with main power switch to be switched off – Trackside orders” (§5.3.7);
- “Change of allowed current consumption” (§5.3.10);

5.4 Train Status

5.4.1 Cab Status

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.4.1.1	Cab status (NOT ACTIVE/ ACTIVE)	**Absent** **Incorrect** Failure or delay to report Cab status **(cases:** **1. CAB A ‘ACTIVE’ / CAB B ‘NOT ACTIVE’ fails to CAB A ‘NOT ACTIVE’ / CAB B ‘NOT ACTIVE’** **2. CAB A ‘NOT ACTIVE’ / CAB B ‘ACTIVE’ fails to CAB A ‘NOT ACTIVE’ / CAB B ‘NOT ACTIVE’)**	- TIU Failure - ETCS onboard failure other than TIU	FS, AD, LS, SR, PT OS, NL, UN, SN, RV, SM	No Cab Status information or delayed sent on-board (although one cab is open it is wrongly assumed that no cab is activated) .	ETCS OB goes directly to SB mode	Vehicle brakes applied due to standstill supervision.	Driver realises that DMI is off.	RAM Issue		Standstill supervision applies brakes if movement exceeds specified national distance.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.4.1.2		**Absent** **Incorrect** Failure or delay to report Cab status **(cases:** **1. CAB A ‘ACTIVE’ / CAB B ‘NOT ACTIVE’ fails to CAB A ‘NOT ACTIVE’ / CAB B ‘NOT ACTIVE’** **2. CAB A ‘NOT ACTIVE’ / CAB B ‘ACTIVE’ fails to CAB A ‘NOT ACTIVE’ / CAB B ‘NOT ACTIVE’)**	- TIU Failure - ETCS onboard failure other than TIU	SH	No Cab Status information or delayed sent on-board (although one cab is open it is wrongly assumed that no cab is activated) .	Inappropriate transition to SB if the function “continue shunting on desk closure” is not active or if passive shunting signal is not received	Vehicle brakes applied due to standstill supervision.	Driver realises that DMI is off.	RAM Issue		
5.4.1.3		**Absent** **Incorrect** Failure or delay to report Cab status **(cases:** **1. CAB A ‘ACTIVE’ / CAB B ‘NOT ACTIVE’ fails to CAB A ‘NOT ACTIVE’ / CAB B ‘NOT ACTIVE’** **2. CAB A ‘NOT ACTIVE’ / CAB B ‘ACTIVE’ fails to CAB A ‘NOT ACTIVE’ / CAB B ‘NOT ACTIVE’)**	- TIU Failure - ETCS onboard failure other than TIU	SH	No Cab Status information or delayed sent on-board (although one cab is open it is wrongly assumed that no	Inappropriate transition to PS mode if the function “continue shunting on desk closure” is active AND Passive Shunting input signal is received;	Although the PS mode is less restrictive than SH, vehicle will not perform any undesired movement since the passive shunting input shall have the value "Passive shunting permitted" only if a brake is applied	Driver realises that DMI is off and ensures the standstill if necessary (e.g. by applying the parking brake before leaving the cab)	RAM Issue		Passive Shunting signal received and “continue shunting on desk closure” has been selected by Driver from the DMI.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
					cab is activated).		(Subset 034 §2.2.2.3.1).				
5.4.1.4		**Absent** **Incorrect** Failure or delay to report Cab status **(cases:** **1. CAB A 'ACTIVE' / CAB B 'NOT ACTIVE' fails to CAB A 'NOT ACTIVE' / CAB B 'NOT ACTIVE'** **2. CAB A 'NOT ACTIVE' / CAB B 'ACTIVE' fails to CAB A 'NOT ACTIVE' / CAB B 'NOT ACTIVE')**	- TIU Failure - ETCS onboard failure other than TIU	SB	No Cab Status information or delayed sent on-board (although one cab is open it is wrongly assumed that no cab is activated).	Transition to SL mode if "sleeping" input signal is received and vehicle is at standstill. No more movement protection, unable to apply brakes. Same situation can apply also in SB if both cabs are normally closed (no failure) and sleeping signal	Vehicle is coupled electrically to a leading engine and will not perform any undesired movement. If it is not coupled no sleeping signal can be transmitted in SB mode. No transition to SL mode is possible under the exported constraint that the vehicle has to ensure that sleeping input is received only if another cab in the	Driver realises that DMI is off although he has not closed the desk. Exported Constraint: The vehicle shall ensure that sleeping input is received only if another cab in the train is active (i.e. another train control system (ETCS or national) provides the supervision of the train movement).	RAM Issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
						is unduly reported to ‘Sleeping Requested’ (refer to 5.1.1.2 TI-3).	train is active (i.e. another train control system (ETCS or national) provides the supervision of the train movement).				
5.4.1.5		**Insertion Incorrect** Cab Status Information is received inappropriately as ACTIVE instead of ‘NOT ACTIVE’ **(cases:** **1. CAB A ‘NOT ACTIVE’ / CAB B ‘ACTIVE’ fails to CAB A ‘ACTIVE’ / CAB B ‘ACTIVE’** **2. CAB A ‘ACTIVE’ / CAB B ‘NOT ACTIVE’ fails to CAB A ‘ACTIVE’ / CAB B ‘ACTIVE’)**	- TIU Failure - ETCS onboard failure other than TIU	SH, FS, AD, LS, SR, PT OS, NL, UN, RV, SM	Incorrect Cab Status transmitted to ETCS OBU so that, both cabs are erroneously assumed to be “activated” (Not admitted condition)	No harmonized reaction if two cabs are reported active at the same time. Assumption for a possible behaviour: Transition to System Failure mode and EB applied.	Vehicle will be at standstill.		RAM Issue		Note: If the assumption for the intermediate reaction is not fulfilled then a project specific analysis is necessary.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.4.1.6		**Incorrect Insertion** Cab Status Information is received inappropriately as ACTIVE instead of 'NOT ACTIVE' **(cases:** **1. CAB A 'NOT ACTIVE' / CAB B 'NOT ACTIVE' fails to CAB A 'ACTIVE' / CAB B 'NOT ACTIVE'** **2. CAB A 'NOT ACTIVE' / CAB B 'NOT ACTIVE' fails to CAB A 'NOT ACTIVE' / CAB B 'ACTIVE')**	- TIU Failure - ETCS onboard failure other than TIU	SB	Incorrect Cab Status transmitted to ETCS OBU (closed desk is erroneously assumed to be open by the OBU).	The DMI is on.	Vehicle remains at standstill. Start of Mission can proceed. Driver to revalidate or enter Driver ID.		RAM Issue		ETCS standstill protection.
5.4.1.7		**Incorrect Insertion** Cab Status Information is received inappropriately as ACTIVE instead of 'NOT ACTIVE' **(cases:** **1. CAB A 'NOT ACTIVE' / CAB B 'NOT ACTIVE' fails to CAB A 'ACTIVE' / CAB B 'NOT ACTIVE'** **2. CAB A 'NOT ACTIVE' / CAB B 'NOT ACTIVE' fails to CAB A 'NOT ACTIVE' / CAB B 'ACTIVE')**	- TIU Failure - ETCS onboard failure other than TIU	SL	Incorrect Cab Status transmitted to ETCS OBU (closed desk is erroneously assumed to be open by	Transition to SB. Standstill supervision is activated.	Standstill supervision can lead to inappropriate vehicle braking, Leading Engine cannot proceed. Start of Mission can proceed. Driver to revalidate or enter Driver ID.		RAM Issue		.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
					the OBU).						
5.4.1.8		**Incorrect Insertion** Cab Status Information is received inappropriately as ACTIVE instead of 'NOT ACTIVE' **(cases:** **1. CAB A 'NOT ACTIVE' / CAB B 'NOT ACTIVE' fails to CAB A 'ACTIVE' / CAB B 'NOT ACTIVE'** **2. CAB A 'NOT ACTIVE' / CAB B 'NOT ACTIVE' fails to CAB A 'NOT ACTIVE' / CAB B 'ACTIVE')**	- TIU Failure - ETCS onboard failure other than TIU	PS	Incorrect Cab Status transmitted to ETCS OBU (closed desk is erroneously assumed to be open by the OBU).	Undesired transition to SH mode If "Stop Shunting on desk opening" is not stored on-board.	Train Supervision Functions applicable in SH mode can brake the vehicle.		RAM Issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.4.1.9		**Incorrect Insertion** Cab Status Information is received inappropriately as ACTIVE instead of 'NOT ACTIVE' **(cases:** **1. CAB A 'NOT ACTIVE' / CAB B 'NOT ACTIVE' fails to CAB A 'ACTIVE' / CAB B 'NOT ACTIVE'** **2. CAB A 'NOT ACTIVE' / CAB B 'NOT ACTIVE' fails to CAB A 'NOT ACTIVE' / CAB B 'ACTIVE')**	- TIU Failure - ETCS onboard failure other than TIU	PS	Incorrect Cab Status transmitted to ETCS OBU (closed desk is erroneously assumed to be open by the OBU).	Inappropriate transition to SB mode if "Stop Shunting on desk opening" is stored on-board.	Vehicle brakes applied due to standstill supervision; inappropriate vehicle braking.		RAM Issue		
5.4.1.10		**Incorrect Insertion** Cab Status Information is received inappropriately so that ACTIVE CABIN is reported as the opposite **(cases:** **1. CAB A 'ACTIVE' / CAB B 'NOT ACTIVE' fails to CAB A 'NOT ACTIVE' / CAB B 'ACTIVE'** **2. CAB A 'NOT ACTIVE' / CAB B 'ACTIVE' fails to CAB A 'ACTIVE' / CAB B 'NOT ACTIVE')**	- TIU Failure - ETCS onboard failure other than TIU	SM	Opposite Cab Status transmitted as active to ETCS OBU	Level 2 if train separation by cooperation on board/RBC: - Train Orientation is misjudged by OBU lead to train position (FE, Max/Min Front End wrongly calculated on-	- RBC uses wrong train position so that the train distancing function may turn unsafe and unsafe MA is provided to the train. - Also in the case the MA is still safe OBU may supervise it using wrong Train	Due to Subset 034 2.5.1.3 each cab will be connected to its individual input on vehicle side. It is assumed that CAB A and CAB B information are reciprocally fully independent and a double independent fault is needed in order to make the	Catastrophic	TI-6b	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
						board and transmitted by OBU to RBC - Wrong Train position is assumed by RBC. - Wrong confidence interval used onboard.	Position Confidence Interval (Exceedance of safe speed or distance as advised to ETCS)	event possible.			
5.4.1.11		**Incorrect Insertion** Cab Status Information is received inappropriately so that ACTIVE CABIN is reported as the opposite **(cases:** **1. CAB A ‘ACTIVE’ / CAB B ‘NOT ACTIVE’ fails to CAB A ‘NOT ACTIVE’ / CAB B ‘ACTIVE’** **2. CAB A ‘NOT ACTIVE’ / CAB B ‘ACTIVE’ fails to CAB A ‘ACTIVE’ / CAB B ‘NOT ACTIVE’)**	- TIU Failure - ETCS onboard failure other than TIU	All mode except SL, PS	Opposite Cab Status transmitted as active to ETCS OBU	Level 2: - Wrong desk reported open resulting in incorrect train position being reported to Trackside - Wrong Train position assumed by the RBC lead to calculate wrong MA.	- MA used on-board not coherent with effective train orientation. - RBC uses wrong train position so that the train distancing function may turn unsafe and unsafe MA is provided to other train.	Due to Subset 034 2.5.1.3 each cab will be connected to its individual input on vehicle side. It is assumed that CAB A and CAB B information are reciprocally fully independent and a double independent fault is needed in order to make the event possible.	Catastrophic	TI-6b	

5.4.2 Direction Controller

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.4.2.1	Direction controller position (FORWARD/NEUTRAL/BACKWARD)	**Absent** **Incorrect** Direction Controller Position received inappropriately as NEUTRAL instead of 'FORWARD' or 'BACKWARD''	- TIU Failure - ETCS onboard failure other than TIU	SH, FS, AD, LS, SR, OS, UN, PT, RV, SM	Incorrect Direction Controller information sent to ETCS OBU (Direction Controller position is assumed to be 'NEUTRAL' instead of 'FORWARD' or 'BACKWARD')	The RAP shall prevent forward and reverse movements of the vehicle (Subset-026 3.14.2.3).	Movement of the vehicle inhibited by ETCS-OBU.		RAM Issue		
5.4.2.2		**Absent** **Incorrect** Direction Controller Position received inappropriately as NEUTRAL instead of 'BACKWARD'	- TIU Failure - ETCS onboard failure other than TIU	FS, AD, LS, OS	Incorrect Direction Controller information sent to ETCS OBU (Direction Controller position is assumed to be 'NEUTRAL' instead of 'BACKWARD')	Inhibition of RV mode switch if Reverse Position of direction controller cannot be reported to ETCS_OBU	Movement Backward inhibited by ETCS-OBU. If danger situation is ongoing, fast reversal movement of a train is not possible	Driver knows which direction is selected. Operational rules.	Marginal		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.4.2.3		**Incorrect Insertion** Direction Controller Position received inappropriately as FORWARD or 'BACKWARD' instead of 'NEUTRAL'	- TIU Failure - ETCS onboard failure other than TIU	SH, SR, OS, UN, PT, RV, FS, LS, SM	Incorrect Direction Controller information sent to ETCS OBU (Direction Controller position is assumed to be 'BACKWARD' or 'FORWARD' instead of 'NEUTRAL')	Rollaway protection is deactivated	Exceedance of the safe speed or distance as advised to ETCS	1.) Driver (knows which direction is selected) 2.) Safety-related function: Rollaway 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 rollaway protection systems 3.) The driver has to ensure the standstill before leaving the cab.	Catastrophic	TI-5	

© This document has been developed and released by UNISIG

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.4.2.4				SB	Incorrect Direction Controller information sent to ETCS OBU (Direction Controller position is assumed to be 'BACKWARD' or 'FORWARD' instead of 'NEUTRAL')	Standstill supervision is active.	-		No effect		
5.4.2.5		**Incorrect Insertion** Direction Controller Position received inappropriately as FORWARD instead of 'BACKWARD' or viceversa	TIU Failure - ETCS onboard failure other then TIU	SH, UN, FS, AD, LS, SR, OS, SM	Incorrect Direction Controller information sent to ETCS OBU (Direction Controller position is assumed to be 'FORWARD'/[BACKWARD] while the actual is 'BACKWARD'/[FORWARD])	roll away protection function will inhibit the backward/[FORWARD] movement instead of the forward/[BACKWARD] movement	Rolling in a slope is possible.	Driver knows which direction is selected.	Catastrophic	TI-5	Unauthorised Direction Movement Protection

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.4.2.6		**Incorrect Insertion** Direction Controller Position received inappropriately as BACKWARD instead of ‘FORWARD’	-TIU Failure - ETCS onboard failure other than TIU	PT, RV	Incorrect Direction Controller information sent to ETCS OBU (Direction Controller position is assumed to be ‘BACKWARD’ while the actual is ‘FORWARD’)	roll away protection function will inhibit the forward movement instead of the backward movement	Rolling in a backward slope is possible.	Driver knows which direction is selected.	Catastrophic	TI-5	

5.4.3 Train Integrity

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.4.3.1	Train Integrity (TRAIN INTEGRITY CONFIRMED/ TRAIN INTEGRITY LOST / TRAIN INTEGRITY STATUS UNKNOWN)	**Absent Incorrect Insertion** Train Integrity received inappropriately as LOST instead of 'CONFIRMED' or 'STATUS UNKNOWN'	- TIU Failure - ETCS onboard failure other than TIU	All	Train integrity status unduly taken as lost when train integrity information is different	RBC is informed of this state	Trackside's Train Separation Function not fully available under this failure.		RAM Issue in L2 operation		
5.4.3.2	Train Integrity (TRAIN INTEGRITY CONFIRMED/ TRAIN INTEGRITY	**Absent Incorrect Insertion** Train Integrity received inappropriately as UNKNOWN instead of 'CONFIRMED' or 'LOST'	- TIU Failure - ETCS onboard failure other than TIU	All	Train integrity status unduly taken as UNKNOWN when train integrity information is different	RBC is informed of this state	Trackside's Train Separation Function not fully available under this failure.		RAM Issue in L2 operation		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
	LOST / TRAIN INTEGRITY STATUS UNKNOWN)										
5.4.3.3	Train Integrity (TRAIN INTEGRITY CONFIRMED/ TRAIN INTEGRITY LOST / TRAIN INTEGRITY STATUS UNKNOWN)	**Absent Incorrect Insertion** Train Integrity received inappropriately as CONFIRMED instead of 'LOST' or 'STATUS UNKNOWN'	- TIU Failure - ETCS onboard failure other than TIU	All	Train integrity status unduly taken as confirmed when train integrity information is LOST or UNKNOWN during an unintentional train split.	False Confirmed Train Length into position report transmitted to RBC	RBC could be unaware that track might be occupied by an unexpected vehicle. RBC uses false Confirmed Train Length so that the train distancing function may turn unsafe and unsafe MA is provided to other train.	Driver shall notice the split and take safe action. For example, if there is a brake pipe, the lost wagon will cause the train to brake. Product Specific Safeguarding. Based on the Risk Analysis provided in [Ref. 6] the worst case for number of unintended train separations events in a year is 6,98 x 10-5 /h (per Freight train) and 2,61 x	Catastrophic	TI-12	Safety Related only in those applications that use the train integrity information to locate the train on the track. Based on clause S-034 §2.5.3.2.2 and related §2.6.3.2.1 and §2.6.2.4.2, the vehicle shall provide an updated train length following a change in the train composition. The train length change, based on clause S-026 §3.6.5.2.5, condition [7] triggers a 'No Integrity Information' report to RBC.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
								10-6 /h (per passengers train). These values can be used as barrier for the overall THR calculation. Two independent train integrity signals are necessary.			
5.4.3.4	Train Integrity (TRAIN INTEGRITY CONFIRMED/ TRAIN INTEGRITY LOST / TRAIN INTEGRITY STATUS UNKNOWN)	**Absent Incorrect Insertion** Train Integrity received inappropriately as CONFIRMED instead of 'LOST' or 'STATUS UNKNOWN'	- TIU Failure - ETCS onboard failure other than TIU	All	Train integrity status unduly taken as confirmed when train integrity information is LOST or UNKNOWN during an intentional train split.	False Confirmed Train Length into position report transmitted to RBC	RBC could be unaware that track might be occupied by an unexpected vehicle. RBC uses false Confirmed Train Length so that the train distancing function may turn unsafe and unsafe MA is provided to other train.	Two independent train integrity signals are necessary. Product specific safeguarding. During an intentional split It shall be assured that no valid Train Data (Train Length) is available or that trackside is informed about a change of the train length information. This information needs to be	Catastrophic	TI-12	Trackside is informed about a change of the train length information. Safety related only in those applications that use the train integrity information to locate the train on the track. Based on clause S-034 §2.5.3.2.2 and related §2.6.3.2.1 and §2.6.2.4.2, the vehicle shall provide an updated train length following a change in the train composition. The train length change, based on clause S-026 §3.6.5.2.5, condition [7]

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
								independent, possibly supported by means of driver validation or independent driver or shunter input.			triggers a ‘No Integrity Information’ report to RBC.

5.4.4 Traction Status

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.4.4.1		Traction Status (ON/OFF)	Level NTC only								

5.4.5 Set Speed

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.4.5.1	Set Speed	**Delay** **Deletion** **Corruption** **Insertion** Wrong input Set Speed (state and/or speed value)	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, PS	False Set Speed Information transmitted to ETCS OBU	ETCS DMI shows wrong 'Set Speed' information	No effect.	Driver knows the cruise speed he has already set at vehicle's traction control.	RAM Issue		

5.5 Train Data

5.5.1 Type of train data entry

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.5.1.1	Train data - Type of train data entry	**Absent** **Incorrect** Failure or delay to report Type of train data entry	- TIU Failure - ETCS onboard failure other than TIU	SB	Type of Train Data Entry change not sent or delayed on-board	At train data entry procedure ETCS DMI shows the incorrect Train Data window (see 11.3.9.6 [Ref. 3]).	No Effect	Driver shall be informed on the type of train when Train Data entry is selected.	RAM Issue		

5.5.2 Other Train data Information

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.5.2.1	Train data – Train category (Cant Deficiency)	**Delay** **Deletion** **Corruption** **Insertion** **Incorrect** Reception of Cant Deficiency information (lower than real)	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, RV	False Cant Deficiency Information transmitted to on board	Lower than real Cant Deficiency is assumed by ETCS OBU for evaluation of SSPs. This can result in more restrictive SSPs calculation (see S-026 3.11.3.2.3).	No effect.		RAM Issue		According to the specific project implementation: On-Board Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1])
5.5.2.2		**Corruption** **Insertion** **Incorrect** Reception of Cant Deficiency information (higher than real)	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, RV	False Cant Deficiency Information transmitted to on board	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 usafe wheel force condition and increase deterioration of track - Decreasing in load on inside wheel may	Driver must confirm Cant Deficiency information via DMI. Assumption: In a specific project, this failure mode can be regarded as having a ‘RAM Issue’ safety severity only if adequate safety	Catastrophic	TI-10	According to the specific project implementation: On-Board Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1]).

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
							increase risk of vehicle overrun (especially of high wind present) - Suspension operating at performance limit reduces margin of safety associated with vehicle response to track geometry variation Risk of derailment.	margin against derailment can be demonstrated for the vehicle exceeding maximum authorized speed for its train category.			
5.5.2.3	Train data – Other International Train Categories	**Delay** **Deletion** **Corruption** **Insertion** **Incorrect** Reception of Other International Train Categories (Train Category with a SSP higher than real)	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, RV	False Other International Train Categories Information transmitted to on board	ERTMS/ETCS on-board system considers a wrong SSP category which it must obey.	Higher than real "Other International Train Categories" is assumed by ETCS OBU for evaluation of SSPs. This can result in less restrictive SSPs calculation (see S-026 3.11.3.2.3). Exceedance of the safe speed or distance as advised to ETCS	Driver must confirm Other International Train Category information via DMI. Product specific safeguarding	Catastrophic	TI-10	According to the specific project implementation: On-Board Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1]).

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.5.2.4	Train data – train length	**Delay** **Deletion** **Corruption** **Insertion** Wrong input for train length	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, RV	False Train length Information transmitted to ETCS OBU Wrong L_TRAIN used on board and related L_TRAININT variable calculated on board	Wrong supervision of SSPs and TSRs False Confirmed Train Length into position report transmitted to RBC	Exceedance of safe speed or distance as advised to ETCS. RBC uses false Confirmed Train Length so that the train distancing function may turn unsafe.	Operational rules for driver. Project Specific mitigation, e.g. driver must confirm train length information via DMI. Product specific safeguarding. Trackside evaluation for train distancing function is based on other external entities (e.g. Axel Counter, etc.) Project specific safety analysis is needed when OBU TI function for acquisition Train Length Information and related external source cannot be realized with the highest safety integrity level	Catastrophic	TI-10	According to the specific project implementation: On-Board Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1])

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.5.2.5	Train data – traction/brake parameters	**Delay** **Deletion** **Corruption** **Insertion** Wrong input for Traction/braking parameters higher than real	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, RV	False traction/brake parameters transmitted to ETCS OBU	wrong braking curve calculation	*Evaluation of potential effect on safe speed and distance supervised is project specific*	Application Constraint: If using Train Interface as external source for traction/brake parameter input the failure of this input could have catastrophic safety severity. A project specific safety analysis is required.	*Hint: Evaluation not in this Subset*		
5.5.2.6	Train data – maximum train speed	**Delay** **Deletion** **Corruption** **Insertion** *Assumption:* *Maximum train speed is not transmitted via TI. Under the above assumption failures have no safety-relevant effect in the system. If it is used during*									

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation al Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Even t-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
		operation a project specific safety analysis will be needed.									
5.5.2.7	Train data – loading gauge	**Delay** **Deletion** **Corruption** **Insertion** Wrong input for loading gauge	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, RV	False loading Gauge transmitted to ETCS OBU	vehicle enters a route although not suitable	collision with side barriers	Operational rules for driver Lineside indications and driver´s route knowledge product specific safeguarding traffic planning	Catastrophic	TI-10	According to the specific project implementation: On-Board Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1])
5.5.2.8	Train data – axle load category	**Delay** **Deletion** **Corruption** **Insertion** Wrong input for axle load	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, RV	False Axle Load Category transmitted to ETCS OBU	train enters a route although not suitable	derailment	operational rules for driver Lineside indications and driver´s route knowledge product specific safeguarding	Catastrophic	TI-10	According to the specific project implementation: On-Board Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1])

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.5.2.9	Train data – Train data information – Traction system(s) accepted by the engine	**Delay** **Deletion** **Corruption** **Insertion** Incorrect rinput reception of unaccepted traction system	- TIU failure - ETCS onboard failure other than TIU	All modes expect IS, SL, NL, PS, RV	Route unsuitability is not detected	Closest location corresponding to the unsuitability is not considered as EOA and SvL	The train is not tripped when overpassing the location of the route unsuitability. Damage of the engine		RAM issue		
5.5.2.10	Train Data - train fitted with airtight system	**Delay** **Deletion** **Corruption** **Insertion** Wrong input received on board so that the airtight system is assumed as available onboard when actually it is not	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, RV	Airtight system available received from external interface when it is not available. OBU informs driver.	ETCS OBU control of Air conditioning intake has no effect.	-		No Effect		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.5.2.11		**Delay** **Deletion** **Corruption** **Insertion** Wrong input received on board so that the airtight system is falsely assumed as not available	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, RV	Airtight system received falsely as not available from external interface. 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 Product specific safeguarding	Marginal		According to the specific project implementation: On-Board Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1])
5.5.2.12	Train Data - List of National Systems available on-board		Level NTC only								
5.5.2.13	Train Data - Axle number	**Delay** **Deletion** **Corruption** **Insertion** Wrong input for Axle number	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, RV	Wrong number of axles is used by external equipment/ETCS	Level 2 Only: Wrong number of axles transmitted to RBC.	-	Assumption: This failure mode can be regarded as having a 'RAM Issue' safety severity only if it can be assumed that axle number information is used for operational purpose and is not	RAM Issue		

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
								safety related. If this assumption is not fulfilled, a project specific analysis is needed.			

5.5.3 Overall Consist Length Information

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.5.3.1	Overall Consist Length Information	**Delay** **Deletion** **Corruption** **Insertion** Wrong input Overall Consist Length Information	- TIU failure - ETCS onboard failure other than TIU	SM	False Overall Consist Length Information transmitted to OBU	Level R Only: - False Safe Consist Length Information transmitted by OBU to RBC - Wrong Train Consist Front End assumed	- dangerous MA used on-board. - Also in the case the MA is still safe OBU may supervise it using wrong Train Position Confidence Interval (Exceedance of safe speed or distance as advised	Operational rules for driver. Product specific safeguarding. Project specific safety analysis is needed when OBU TI function for acquisition Overall Consist Length	Catastrophic	TI-13	Note: According to §3.18.3.2.2 the Driver shall never be involved in the modification of 'Train Data – Overall Consist Length'. Driver Train Data validation cannot be claimed as internal barrier against false Overall Consist Length.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
						by the RBC lead to calculate wrong MA. - Wrong confidence interval used onboard.	to ETCS)	Information and related external source cannot be realized with the highest safety integrity level.			
5.5.3.2	Overall Consist Length Information	**Delay** **Deletion** **Corruption** **Insertion** Wrong input Overall Consist Length Information	- TIU failure - ETCS onboard failure other than TIU	SM	False Safe Consist Length Information transmitted to ETCS OBU	Level R Only: False Safe Consist Length Information transmitted to RBC. Wrong Safe Consist Length and position can led the RBC to provide dangerous SM Authorization to other train.consist.	Collision	Trackside evaluation for train distancing function is based on other external entities (e.g. Axel Counter, etc.) Operational rules for driver. Product specific safeguarding. Project specific safety analysis is needed when OBU TI function for acquisition Overall Consist Length Information and	Catastrophic	TI-13	Note: According to §3.18.3.2.2 the Driver shall never be involved in the modification of 'Train Data – Overall Consist Length'. Driver Train Data validation cannot be claimed as internal barrier against false Overall Consist Length.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
								related external source cannot be realized with the highest safety integrity level.			
5.5.3.3	Train Data – Overall Consist Length Information	**Delay** **Deletion** **Corruption** **Insertion** Wrong input Overall Consist Length Information	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, SH, SM, NL, PS, RV	False Overall Consist Length Information transmitted to ETCS OBU Wrong L_TRAIN used on board and related L_TRAININT variable calculated on board	False Confirmed Train Length into position report transmitted to RBC False Train Length used onboard led to wrong supervision of SSPs and TSRs	RBC uses false Confirmed Train Length so that the train distancing function may turn unsafe. Exceedance of safe speed or distance as advised to ETCS	Trackside evaluation for train distancing function is based on other external entities (e.g. Axel Counter, etc.) Operational rules for driver. Product specific safeguarding. Project specific safety analysis is needed when OBU TI function for acquisition Overall Consist Length Information and related external	Catastrophic	TI-13	Note: According to §3.18.3.2.2 the Driver shall never be involved in the modification of 'Train Data – Overall Consist Length'. Driver Train Data validation cannot be claimed as internal barrier against false Overall Consist Length.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation al Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Even t-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
								source cannot be realized with the highest safety integrity level.			

5.6 Train Running Number

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation al Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Even t-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.6.1	Train Running Number	**Delay** **Deletion** **Corruption** **Insertion** **Incorrect** Wrong reception of Train Running Number	- TIU failure - ETCS onboard failure other than TIU	All modes except IS, SL, NL, PS, RV, SM	Wrong train running number is used in the ETCS on-board	Wrong train running number is sent to the RBC	Dispatcher is misleaded by TRN different from the expected.	Operational rules for driver	RAM issue		Not used inside ETCS for safety purposes

5.7 National System Isolation

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operational Mode	Failure Effects			ETCS External Protection/ Mitigation/ Barriers	Severity	Event-ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.7.1		National System Isolation (NTC isolated / NTC not isolated)	Level NTC only								

6. TRACEABILITY

This section lists the mandatory functions analysed and cross reference them to the SRS [Ref. 1] to the FIS TIU [Ref. 2], ERA DMI [Ref. 3] and STM FFFIS [Ref. 4].

Name	**Reference in FIS TIU** [Ref. 2]	**Reference in SRS** [Ref. 1]	**Input / Output**
Sleeping	2.2.1	4.4.6 / 4.6.3	Input
Passive shunting	2.2.2	4.4.20 / 4.6.3	Input
Non-Leading	2.2.3	4.4.15 / 4.6.3	Input
Isolation	2.2.4	4.4.3.1.1	Output
Automatic Driving	2.2.5	4.4.16	Output
Remote Shunting	2.2.6	4.4.8.1.4	Output
Service brake command	2.3.1	3.13.2.2.7 / 3.14.1	Output
Brake pressure	2.3.2	3.13.2.2.7 / A.3.10	Input
Emergency brake command	2.3.3.	3.13.10 / 3.14.1 / 4.4.4 / 4.4.5 / 4.4.13	Output
Special brake inhibition Area – Trackside Orders	2.3.4	3.12.1 / 3.13.2.2 / 5.20.5	Output
Special brake status	2.3.6	3.13	Input
Additional brake status	2.3.7	3.13	Input
Change of traction system	2.4.1	3.12.1	Output
Powerless section with pantograph to be lowered - Trackside orders	2.4.2	3.12.1	Output
Air tightness Area-Trackside orders	2.4.4	3.12.1	Output
Station platform	2.4.6	3.12.1	Output
Powerless section with main power switch to be switched off -Trackside orders	2.4.7	3.12.1	Output
Traction Cut Off	2.4.9	3.13.2.2.8	Output
Change of allowed current consumption	2.4.10	3.12.1	Output
Engine orientation in Supervised Manoeuvre	2.4.11	4.4.21.1.13	Output
Cab Status	2.5.1	4.6.3	Input
Direction Controller	2.5.2	3.14.2 / 5.13.1.4	Input
Train integrity	2.5.3	3.6.5.2.1/3.6.5.2.3	Input
Set Speed	2.5.5	4.7.2	Input
Overall Consist length information	2.6.2	3.18.3	Input
Other Train Data information	2.6.3	3.18.3 / 5.17	Input
Train running number	2.7.1	3.18.4.5	Input

Table 1 – SRS references

Name	**Reference in FIS TIU** [Ref. 2]	**Reference in DMI [Ref. 3]**	**Input / Output**
Set Speed	2.5.5	8.2.3.9	Input
Type of train data entry	2.6.1	11.3.9.6	Input
Other Train Data	2.6.3	11.3.9	Input
Train running number	2.7.1	11.3.1.3	Input

Table 2 – DMI references

Name	**Reference in FIS TIU** [Ref. 2]	**Reference in STM [Ref. 4]**	**Input / Output**
Service brake command	2.3.1	5.2.5	Output
Emergency brake command	2.3.3	5.2.5	Output
Special brake inhibit – STM Orders	2.3.5	5.2.4.3	Output
Pantograph-STM orders	2.4.3	5.2.4.3	Output
Air tightness-STM orders	2.45	5.2.4.3	Output
Main power switch-STM orders	2.4.8	5.2.4.3	Output
Traction Cut Off	2.4.9	5.2.4.3	Output
Cab Status	2.5.1	5.2.4.4	Input
Direction Controller	2.5.2	5.2.4.4	Input
Traction status	2.5.4	5.2.4.4	Input
National System isolation	2.7	10.3.3.5, 10.3.3.6 e), 10.14.1.2	Input

Table 3 – STM references

7. CONCLUSIONS

No inconsistencies and open points were found during the analysis. The following assumptions have been considered on the use of ETCS information:

7.1.1 Application Constraints

7.1.1.1 'Service Brake Command'. If the ETCS Onboard is implemented using Service Brake to protect the train against undesirable movements, then a project specific safety analysis is needed in order to show that the failure of this signal is recognized and the EB is applied as safeguarding.

7.1.1.2 'Brake Pressure'. If the ETCS Onboard 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 in order to show that the failure of the signal has acceptable safety consequences.

7.1.1.3 'Special Brake Status'. If using Special Brake as available and affecting the Emergency Brake curve, the failure of the input 'Special Brake status' can be considered as having insignificant safety severity only under the assumption that EB model (Kdry_rst) is calculated in such a way that EB distance is exceeded only according to the actual EBCL even in case of 'Special Brake Status' failure.

7.1.1.4 'Traction Cut Off''. The failure mode to this output can be regarded as having a 'RAM Issue' safety severity only if the ETCS/ERTMS on-board equipment is configured to T_traction = T_traction_cut_off (see Subset-026, section 3.13.9.3.2.3). If this assumption is not fulfilled, then failure to this output shall be held as having catastrophic safety consequences and product specific safeguarding has to be considered.

7.1.1.5 'Cab Status'. The failure mode of this input (see FMEA ref. Id. 5.4.1.5) can be regarded as having a 'RAM Issue' safety severity under the assumption that in case of two cabs are reported active at the same time the OBU reacts by transiting in System Failure Mode and applying EB. If this assumption is not fulfilled, then a project specific analysis is necessary.

7.1.1.6 'Cab Status'. It assumed that the vehicle has to ensure that sleeping input is received only if another cab in the train is active (i.e. another train control system (ETCS or national) provides the supervision of the train movement) (see FMEA ref. Id. 5.4.1.4).

7.1.1.7 'Cab Status'. It is assumed that CAB A and CAB B information are reciprocally fully independent, and a double independent fault is needed in order to make the event possible (see FMEA ref. Id. 5.4.1.10 and 5.4.1.11).

7.1.1.8 'Station Platform'. The failure of Station Platform input (see FMEA ref. Id. 5.3.6.1) can be regarded as having a 'RAM Issue' safety severity only if it can be assumed that the function related to the output of Station Platform for enabling the passenger door opening is not used for safety reasons (e.g. in cases of evacuation).

7.1.1.9 ‘Train Data – Train category (Cant Deficiency)’. A specific project can regard the failure mode of this input (see FMEA ref. Id. 5.5.2.2) as having a ‘RAM Issue’ safety severity only if adequate safety margin against derailment can be demonstrated for the vehicle exceeding maximum authorized speed for its train category. In that case a project specific analysis and safety case is necessary.

7.1.1.10 ‘Train Data – Traction/brake parameters’. If using Train Interface as external source for traction/brake parameter input the failure of this input could have catastrophic safety severity (see FMEA ref. Id. 5.5.2.5). A project specific safety analysis is required.

7.1.1.11 ‘Train Data – Train Length’ The failure mode of this input (see FMEA ref. Id. 5.5.2.4) may lead, under some condition, to potential 'catastrophic' safety consequence. Project specific safety analysis evaluating the contribution of this event to the related top Hazard is needed when OBU TI function for acquisition Train Data - Train Length Information and related external source cannot be realized with the highest safety integrity level.

7.1.1.12 ‘Train Data – Maximum train speed’. The analysis considers that ‘Maximum train speed’ is not transmitted via TI (see FMEA ref. Id. 5.5.2.6). Under this assumption failures have no safety-relevant effect in the system. If the above assumption is not valid a project specific safety analysis is needed in order to show that the failure of the signal has acceptable safety consequences.

7.1.1.13 ‘Train Data – Axle Number’. The failure mode of this input (see FMEA ref. Id. 5.5.2.13) can be regarded as having a ‘RAM Issue’ safety severity only if it can be assumed that axle number information is not used at RBC for safety-related purpose. If this assumption is not fulfilled, a project specific safety analysis is needed.

7.1.1.14 ‘Overall Consist Length Information’. The failure mode of this input (see FMEA ref. Id. 5.5.3.1, 5.5.3.2 and 5.5.3.3) may lead, under some condition, to potential ‘catastrophic’ safety consequence. Project specific safety analysis evaluating the contribution of this event to the related top Hazard is needed when OBU TI function for acquisition Overall Consist Length Information and related external source cannot be realized with the highest safety integrity level.

7.1.1.15 ‘Train Integrity’. The failure mode of this input has been recognized has a Hazardous Event (TI-12) having potential catastrophic effect. When evaluating the contribution of this event to the related top Hazard, it is possible to claim as external barrier the result of the Risk Analysis provided in [Ref. 6] where the worst case for number of unintended train separations events in a year is 6,98 x 10-5 /h (per Freight train) and 2,61 x 10-6 /h (per passengers train).

7.1.1.16 ‘Train Integrity’. During an intentional split, the failure mode of this input has been recognized has a Hazardous Event (TI-12) having potential catastrophic effect. As required by clause S-034 §2.5.3.2.2 and related §2.6.3.2.1 and §2.6.2.4.2, the vehicle shall provide to the OBU an updated train length following a change in the train composition.

8. ANNEX A – LIST OF TI-XX EVENTS IDENTIFIED

Event ID	Hazardous Event Description
TI-1	Service brake / emergency brake not commanded when required
TI-2 (*1)	Service brake / emergency brake release commanded when not required
TI-3	Inappropriate sleeping request
TI-4 (*1)	Incorrect brake status (TIU Failure)
TI-5	Incorrect direction controller position report (TIU Failure)
TI-6a(*1)	Intentionally deleted
TI-6b	Wrong Cabin considered as Active
TI-7	Inappropriate passive shunting request
TI-8	Inappropriate non leading permitted signal received
TI-9	Intentionally deleted
TI-10	Falsification of train data received by External Source
TI-11	Traction Cut-Off not commanded when required
TI-12	Inappropriate Train Integrity Confirmed Status received
TI-13	Falsification of Overall Consist Length Information received by External Source

Table 4 – List of TI-XX events identified

(*1) Note that the following events are currently unused in the FMEA reported in chapter 5:

- TI-2: Covered by TI-1.
- TI-4: This event is to be referred only to service brake. A project specific analysis is only necessary in case the brake pressure is used for safety purposes related to Service brake feedback (refer 7.1.1.2).