U-N-I-S-I-G

ERTMS/ETCS

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

REF : SUBSET 080-1/2
ISSUE : 3.0.12
DATE : 2014-05-08

Company	Technical Approval	Management approval
ALSTOM		
ANSALDO		
AZD		
BOMBARDIER		
CAF		
SIEMENS		
THALES		

© This document has been developed and released by UNISIG

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,	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)

© This document has been developed and released by UNISIG

	5.3.7.1, 5.3.8.1. - Chapter 7. - 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	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	C. Latorre (MERMEC)

	5.6.3 - update FMEA id 5.6.5 - update FMEA id 5.6.6 - updated chapter 6 for S-034 references - updated chapter 7	The FMEA row of Train Integrity input has been removed since according to S-034 the input has to be harmonized. 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 2014-05-08		Baseline 3 1st maintenance release version	DARI

2. TABLE OF CONTENTS

© This document has been developed and released by UNISIG

© This document has been developed and released by UNISIG

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]	UNISIG: Subset 026, UNISIG SRS, issue 3.4.0
[Ref. 2]	UNISIG: Subset 034, FIS for the Train Interface, issue 3.1.0
[Ref. 3]	ERA: ETCS Driver Machine Interface - ERA_ERTMS_015560, issue 3.4.0
[Ref. 4]	UNISIG: Subset 035, Specific Transmission Module FFFIS, issue 3.1.0
[Ref. 5]	UNISIG: Subset 077, Causal Analysis Process; issue 2.3.2.

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

Failures in Level NTC (e.g. regarding output 'Special Brake inhibit / Pantograph / Air tightness / Main Power Switch – STM Order' and input 'National System Isolation') are excluded from this analysis since it is only applicable to Level 1 and Level 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.

© This document has been developed and released by UNISIG

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		

© 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				
5.1.1.2		**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		RAM issue		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).

© This document has been developed and released by UNISIG

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, LS, SR, OS	"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, LS, SR OS,	"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

© This document has been developed and released by UNISIG

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).

© This document has been developed and released by UNISIG

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.”

© 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	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		

© This document has been developed and released by UNISIG

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.

© This document has been developed and released by UNISIG

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				
5.2.3.1.1	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	
5.2.3.1.2		**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		

© This document has been developed and released by UNISIG

5.2.4 Special Brake Inhibit – Trackside Orders

The interface of the special brake inhibition is not standardized in [Ref. 2]. The below analysis must therefore be considered preliminary because it makes assumptions on the interface.

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 Inhibit – Trackside Order (NOT INHIBITED/INHIBITED)	**Absent** **Incorrect** Failure to 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 (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				
5.2.4.2		**Insertion** 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 (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		

© This document has been developed and released by UNISIG

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	**Same analysis as described in Ref. ID 5.2.4.1 and 5.2.4.2**									

© This document has been developed and released by UNISIG

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,LS,SR, OS,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,LS,SR, OS,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.	*Evaluation of potential effect on safe speed and distance supervised is project specific*	Application Constraint: If using Special Brake as available and affecting the Emergency Brake curve, the failure of the input 'Special Brake status' could have catastrophic safety severity. A project specific safety analysis is required.	*Hint: Evaluation not in this Subset*		

© This document has been developed and released by UNISIG

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**									

© This document has been developed and released by UNISIG

5.3 Control of Train

5.3.1 Change of Traction System (CTS)

The interface of the change of traction system is not standardized in [Ref. 2]. The below analysis must therefore be considered preliminary because it makes assumptions on the interface.

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 is not properly transmitted to the vehicle so that the vehicle will not execute the change of traction when required	Traction System do not change when required or change 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)

© This document has been developed and released by UNISIG

5.3.2 Pantograph – Trackside orders (powerless section – lower pantograph)

The interface of the pantograph is not standardized in [Ref. 2]. The below analysis must therefore be considered preliminary because it makes assumptions on the interface.

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	Pantograph – 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 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)

© This document has been developed and released by UNISIG

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	**Same analysis as described in Ref. ID 5.3.2.1**									

© This document has been developed and released by UNISIG

5.3.4 Air tightness – Trackside orders

The interface of the change of air tightness is not standardized in [Ref. 2]. The below analysis must therefore be considered preliminary because it makes assumptions on the interface.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operat ional Mode	Failure Effects			ETCS external Protection /Mitigation/ barriers	Severity	EVENT ID	Internal barriers
					Local	Intermediate	Initial End Effect				
5.3.4.1	Air Tightness – 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 stay open 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 not close the flaps when required	Air Conditioning intake not closed whenrequired	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.	Insignificant		Air tightness area is announced and indicated to the driver on the DMI (S-026 §5.18.6).

© 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				
5.3.4.2		**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 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	**Same analysis as described in Ref. ID 5.3.4.1 and 5.3.4.2**									

5.3.6 Passenger Door

The interface of the passenger door is not standardized in [Ref. 2]. The below analysis must therefore be considered preliminary because it makes assumptions on the interface.

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	Passenger Door	**Deletion** **Corruption** **Delay** The output Passenger Door information used forenabling the passenger door is erroneous or missing or delayed so that the passenger door will be not be open when required	- TIU Failure - ETCS onboard failure other than TIU	All modes	The output information used for enabling the passenger door is not properly transmitted to the vehicle so that the vehicle will not open the passenger doorwhen 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 of Passenger Door information 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 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		

© This document has been developed and released by UNISIG

5.3.7 Main Power Switch – Trackside orders

The interface of the main power switch is not standardized in [Ref. 2]. The below analysis must therefore be considered preliminary because it makes assumptions on the interface.

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	Main Power Switch – 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 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).

© 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				
5.3.7.2		**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 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		

© This document has been developed and released by UNISIG

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	**Same analysis as described in Ref. ID 5.3.7.1 and 5.3.7.2**									

© This document has been developed and released by UNISIG

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	If the ETCS/ERTMS on-board equipment is configured to “traction cut-off at warning limit implemented” 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.	Assumption: If the ETCS/ERTMS on-board equipment is configured to “traction cut-off at warning limit implemented” (see Subset-026, section 3.13.9.3.2.3a) the failure of this output shall be considered as having a catastrophic safety severity. If the ETCS/ERTMS on-board equipment is configured to “traction cut-off at warning limit not implemented” 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

The interface of the change of allowed current consumption is not standardized in [Ref. 2]. The below analysis must therefore be considered preliminary because it makes assumptions on the interface.

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 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		

5.4 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, LS, SR, PT OS, NL, UN, SN, RV	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.
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		

© 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				
5.4.1.3		**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 cab is activated).	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 (Subset 034).	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				
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	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	Driver realises that DMI is off although he has not closed the desk. Exported Constraint: 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).	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				
5.4.1.5		**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, LS, SR, PT OS, NL, UN, RV	Incorrect Cab Status transmitted to ETCS OBU so that, both cabs are erroneously assumed to be "activated" (Not admitted condition)	Transition to System Failure mode and EB applied.	Vehicle will be at standstill.		RAM Issue		
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.

© 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				
5.4.1.7		**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 the OBU).	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		.
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		

© 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				
5.4.1.9		**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		

© This document has been developed and released by UNISIG

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, LS, SR, OS, UN, PT, RV	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, 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		

© 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				
5.4.2.3		**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,	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'	TIU Failure - ETCS onboard failure other then TIU	SH, UN, FS, LS, SR, OS, PT, RV	Incorrect Direction Controller information sent to ETCS OBU (Direction Controller position is assumed to be 'FORWARD' while the actual is 'BACKWARD')	roll away protection function will inhibit the backward movement instead of the forward movement	Rolling in a forward slope is possible.	Driver knows which direction is selected.	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				
5.4.2.6		**Incorrect Insertion** Direction Controller Position received inappropriately as BACKWARD instead of ‘FORWARD	-TIU Failure - ETCS onboard failure other than TIU	SH, UN, 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	
5.4.2.7		**Incorrect Insertion** Direction Controller Position received inappropriately as BACKWARD instead of ‘FORWARD	-TIU Failure - ETCS onboard failure other than TIU	FS, LS, SR, OS	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	The vehicle cannot move (forward movement is inhibited by RAP while backward movement is inhibited by RMP).	Driver knows which direction is selected.	RAM Issue		Reverse Movement Protection

© 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				
5.4.2.8		**Incorrect** **Insertion** Direction Controller Position received inappropriately as FORWARD or 'BACKWARD' instead of 'NEUTRAL'	- TIU Failure - ETCS onboard failure other than TIU	NL	Incorrect Direction Controller information sent to ETCS OBU (Direction Controller position is assumed to be 'BACKWARD' or 'FORWARD' instead of 'NEUTRAL')	Slave engine cannot proceed because it is coupled to a leading engine.	-	-	RAM issue		Leading vehicle controls the slave vehicle (S-026 §4.4.15.1.1.1)

© This document has been developed and released by UNISIG

5.4.3 Train Integrity

5.4.3.1 TBD

© This document has been developed and released by UNISIG

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								

© This document has been developed and released by UNISIG

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		

© This document has been developed and released by UNISIG

5.6 Train data Information

The interface of the train data information is not standardized in [Ref. 2]. The below analysis must therefore be considered preliminary because it makes assumptions on the interface.

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				

© 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				
5.6.1	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	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).	If gauging is not appropriate there can be a collision.	Assumption: This failure mode can be regarded as having a 'RAM Issue' safety severity only if it can be assumed that the activation of the tilting system does not affect the loading gauge. If this assumption is not fulfilled, the status of the tilting system shall be regarded as safety critical. Infrastructure planning has to prevent that tilting does not infringe the allowed gauging. Driver must confirm the Cant Deficiency information via DMI.	Catastrophic	TI-10	According to the specific train implementation, Onboard 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				
5.6.2		**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	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 and damage the infrastructure.	Driver must confirm the tilting condition via DMI.	Insignificant		According to the specific train implementation, Onboard Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1]).
5.6.3	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	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 train implementation, Onboard Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1]).

© 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				
5.6.4	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	False Train length Information transmitted to ETCS OBU	Wrong supervision of SSPs and TSRs	Exceedance of safe speed or distance as advised to ETCS	Operational rules for driver. Product specific safeguarding.	catastrophic	TI-10	According to the specific train implementation, Onboard Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1])
5.6..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	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*		

© 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				
5.6.6	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 operation a project specific safety analysis will be needed.*									

© 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				
5.6..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	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 train implementation, Onboard Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1])
5.6..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	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 train implementation, Onboard Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1])

© 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				
5.6.9	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	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		According to the specific train implementation, Onboard Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1])
5.6.10		**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	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 onboard Product specific safeguarding	Marginal		According to the specific train implementation, Onboard Informs Driver that change in Train Data needs to be validated by Driver (3.18.3.3 and 5.17.2.2 [Ref. 1])

© 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				
5.6.11	Train Data - List of National Systems available on-board		Level NTC only								
5.6.12	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	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 safety related. If this assumption is not fulfilled, a project specific analysis is needed.	RAM Issue		

5.7 National System Isolation

© 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				
5.7.1		National System Isolation (NTC isolated / NTC not isolated)	Level NTC only								

© This document has been developed and released by UNISIG

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
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 inhibit – Trackside Orders	2.3.4	3.12.1 / 3.13.2.2	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
Pantograph-Trackside orders	2.4.2	3.12.1	Output
Air tightness-Trackside orders	2.4.4	3.12.1	Output
Passenger Door	2.4.6	3.12.1	Output
Main Power Switch-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
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	Input
Train Data information	2.6.2	3.18.3 / 5.17	Input

Table 1 – SRS references

Name	**Reference in FIS TIU** [Ref. 2]	**Reference in DMI [Ref. 3]**	**Input / Output**
Type of train data entry	2.6.1	10.3.9.6	Input

Table 2 – DMI references

Name	**Reference in FIS TIU** [Ref. 2]	**Reference in STM [Ref. 4]**	**Input / Output**

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 Train Data – Train category (Cant Deficiency)

The failure mode of this input (see FMEA ref. Id. 5.6.1) can be regarded as having a 'RAM Issue' safety severity only if the following assumptions can be assumed:

1. The activation/deactivation of the tilting system neither affects track forces nor the gravity centre significantly.
2. The tilting system does not affect the loading gauge.

If the above assumptions are not fulfilled, the activation / deactivation and therefore the status of the tilting system can be safety critical. In that case a project specific analysis and safety case is necessary.

7.1.2 Train Data – Axle Number

The failure mode of this input (see FMEA ref. Id. 5.6.11) 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.

7.1.3 Traction Cut-Off output

The failure of this output shall be considered as having a catastrophic safety severity only if the ETCS/ERTMS on-board equipment is configured to "traction cut-off at warning limit implemented" (see Subset-026, section 3.13.9.3.2.3a). In case the ETCS/ERTMS on-board equipment is configured to "traction cut-off at warning limit not implemented" the failure of this output can be considered as having a RAM severity.

7.1.3.1

7.1.4 Application Constraints

7.1.4.1 '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.

© This document has been developed and released by UNISIG

7.1.4.2 ‘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.

7.1.4.3 ‘Special Brake Status’. If using Special Brake as available and affecting the Emergency Brake curve, the failure of the input ‘Special Brake status’ could have catastrophic safety severity, then a project specific safety analysis is needed in order to show that the failure of the signal has acceptable safety consequences.

7.1.4.4 In this analysis it is assumed that the function related to the output of Passenger Door for enabling the passenger door opening is not used for safety reasons, e.g. in cases of evacuation.

7.1.4.5 Train Data – Maximum Train Speed. Under the assumption that Maximum Train Speed is not transmitted via TI, the failure of this input has 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.

7.1.4.6 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, then a project specific safety analysis is needed in order to show that the failure of the signal has acceptable safety consequences.

© This document has been developed and released by UNISIG

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 (*)	Service brake / emergency brake release commanded when not required
TI-3	Inappropriate sleeping request
TI-4 (*)	Incorrect brake status (TIU Failure)
TI-5	Incorrect direction controller position report (TIU Failure)
TI-6a(*)	Loss of Cabin Active Signal
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

Table 4 – List of TI-XX events identified

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

- TI-2: Covered by TI-1.
- TI-4: The event needs a project specific analysis in case the brake pressure is used for safety purposes.
- TI-6a: The analysis shows that the consequences are only RAM-related
- TI-6b: This requires a double fault and is outside the scope of this FMEA. However, the event would need to be considered in an implementation.