

ERTMS/ETCS

ETCS Application Level 2 - Safety Analysis

Part 2 - Functional Analysis

REF : SUBSET-088-2 Part 2

ISSUE : 3.7.0

DATE : 2019-12-16

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



1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.0.1. 14-05-01	All	Document Creation	WLH
0.0.2 25-05-01	4	Key to the fault tree symbols added	WLH
0.1.0 14-06-01	3.1.1.2 & 5.2.1.2	Inclusion of Ansaldo comments. Release for general Unisig review	WLH
0.1.1. 25-06-01	Section 8 Appendix B	Initial comments added Fault tree raised to issue 005.	WLH
0.1.2. 06-08-01	All	Document restructured into 4 parts. This part becoming part 3	WLH
0.1.2. Draft 06-08-01	All	Draft Issue	GM
0.1.3. 22-08-01	All	Updated following review in Stuttgart.	GM
0.1.4 24-08-01	Part Number	Part Number changed from Part 3 to Part 2	GM
0.1.5. 03-09-01	All	Updated following UNISIG RAMS group review.	GM
0.1.6. 18-09-01	All	Minor modification following UNISIG RAMS review meeting	GM
0.1.7. 31-09-01	All	Minor modification following UNISIG Supergroup / RAMS Group meeting	GM
0.2.0. 01-10-01	Sections 3 & 4	Minor modifications and raised in issue for release to Esrog	WLH
0.2.1. 01-11-16	All	Modifications suggested by Bombardier	DARI

© This document has been developed and released by UNISIG



0.2.2 01-11-21	5.1.1.5	Comments on Emergency Message	RAMS meeting 2001-11-21
0.2.3 01-11-28	All	Comments by BTS	DARI
0.2.4 01-11-30	All	consistency check with Part 1	Ado
0.2.5 01-12-13	All	Updates after RAMS-meeting 2001-12-06	DARI
0.3.0 02-01-15	All	Minor updates after comments from ANS, CSEE, SIE and comments at RAMS-meeting 02-01-10	DARI
2.0.0. 26-02-02	Minor changes to 3.1.1.1 & 3.1.1.2.	Raised in issue for release to the EEIG	WLH
2.0.1 26-10-02	Document title 4.1.1.2. Added as new paragraph. Analysis work sheets MMI-2, TI-6 and TRACK	Report Number deleted Notes re MMI-2 and TI-6 breakout added to the analysis sheets. Note regarding analysis of TRACK events clarified. Sections 7 & 8 moved to Part 3 of Subset 088	WLH
2.0.2. 10-12-02	4.1.1.2 rewritten Minor modifications to section 6	Address review comments from Ans and Sie. Improve links to the Fault tree and clarification of events	WLH
2.0.3 15-01-03	4.1.1.2 ODO 4 amended Some event descriptions improved. TRANS events rationalised	Comments raised at the review meeting of 14-01-03	WLH
2.0.4 27-01-03	Diagram added		WLH
2.1.0. 31-01-03		Raised in issue for release to the Users Group	WLH

2.2.2 21-03-03		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
2.2.3 25-05-04	All	Updated with new events added to Fault Tree: Kernel-33 Kernel-34	IS
2.2.4 19-10-04	Section 6	Section 6.- Mode Column reviewed and updated with applicable modes Section 6.- Changed affected functions of events Kernel-23, 33 & 34	IS
2.2.10 08-07-05		Raised in issue for release to the Users Group. Version number to be consistent with SUBSET-091.	DARI
2.2.11 20-09-07		Formal changes, corrections of grammar and spelling	KN
2.3.0 02-04-08		Administrative updates for baseline 2.3.0	DARI
2.3.1 15-03-11	Section 6	Include new mode Limited Supervision Insert new column "mitigation conditions" in FMEA and update according to methodology concluded in RAMS group	KN
		"MMI" changed to "DMI" except for "MMI-x" events	
		Change "location" to "position" where applicable according to CR808	

		Adaptation to Subset.026, 3.2.0 Update with new/changed MMI-x events according to final version of Subset-079 (updated to 2.3.0)	
2.3.2	Section 6	Update according to Subset-079: MMI-4 removed	KN
2.3.3		Update according to Subset-079: MMI-2j and MMI-4 added, MMI-2i removed	KN
3.0.0		Update according to Subset-079: MMI- 2j, MMI-2k and MMI-5 added, MMI-2a split into MMI-2a.1 and MMI-2a.2	KN
3.0.1	Section 6	Update according to Subset-079: Event description changed, MMI-1g added, modes added	KN
3.0.2		Update after internal RAMS WP review	KN
3.0.3		Minor updates during RAMS-meeting	DR
3.1.0		CR1106 considered. Administrative changes for release to ERA.	DR
3.2.0		<ul style="list-style-type: none"> • Use ETCS Core Hazard. as standardized term • Override EoA is renamed to Override • MMI-6 added • MMI-2d: LS mode removed • MMI-2a.2: First Line of Intervention added 	KN

3.3.0		Update after internal RAMS WP review	KN
3.4.0		Minor updates during RAMS-meeting	DR
3.5.0		Baseline 3 release version	DR
3.5.1 2013-01-31		Updated relevant modes for TI-1	KN
3.5.2		Update for B3 MR1 based on changes in Subset-079 (event description changed) and in Subset-080 (new events added)	KN
3.5.3		Updated during RAMS-meeting	DARI
3.5.4	Section 6	Renaming of MMI-2F	KN
3.5.5	TI-10	Update according to SUBSET-080	KN
3.5.6	Section 6	TI-6a deleted according to SUBSET-080 Formal Updates	KN
3.5.7	Section 6	TI-4 updated according to SUBSET-080	KN
3.6.0 2016-06-20	No change	Baseline 3 2 nd release version	RAMS WP
3.7.0	No change	Release version	RAMS WP



2. TABLE OF CONTENTS

1. MODIFICATION HISTORY	2
2. TABLE OF CONTENTS.....	7
3. INTRODUCTION.....	8
4. DESCRIPTION.....	9
5. INTEROPERABILITY CONSIDERATIONS FOR ETCS.....	11
6. FUNCTIONAL ANALYSIS.....	13
7. TRANSMISSION CHANNEL EVENTS.....	60
8. GRAPHICAL REPRESENTATION OF HAZARDOUS EVENTS	61



3. INTRODUCTION

- 3.1.1.1 This document is Part 2 of the ETCS analysis. It contains the Application Level 2 analysis and provides the functional analysis of a Level 2 system in order to identify issues that are key to achieving technical interoperability.
- 3.1.1.2 The first objective of this analysis is to analyse the effect of potentially catastrophic failures at the mandatory boundaries to the Unisig reference architecture (as captured in the FMEA's listed in Part 0) and also within ETCS. The second objective is to determine all claims that could be made to prevent or reduce the probability of the ETCS Core Hazard defined in Part 1 occurring as a result of these failures.
- 3.1.1.3 The analysis includes consideration of each of the main operational modes of the system applicable to level 2 in a manner whereby all assumptions are clearly visible.

4. DESCRIPTION

4.1.1.1 This functional analysis considers each fault tree base event from the functional fault tree in turn. The fault tree base events represent the low-level functions and data items of ETCS.

4.1.1.2 The fault tree in Part 1 of SUBSET-088 is oriented to system functionality. For the quantitative apportionment of the ETCS THR to constituents to be undertaken in Part 3 of SUBSET-088, some events indicated in the fault tree have been decomposed to a lower level in order to clearly align as on-board, air gap or trackside. This has been undertaken in accordance with the allocation defined in the Unisig reference architecture. More precisely:

The TRANS-ENTITY-X events in the following table refer only to errors occurring in the communication channel including the non trusted parts of transmitting and receiving entities. As a consequence, events corresponding to errors in the on-board and trackside kernel functionality that were not explicitly identified in the fault tree have been added. This has required the changing of some names from the fault tree.

Note the entities considered for Level 2 are Balise and Radio (onboard or trackside) where X is allocated as,

1 for Corruption

2 for Deletion

3 for insertion

These being the hazardous events identified in the transmission FMEAs.

TRACK-X events identified in the fault tree included errors in the engineering process in order to identify data errors that could affect functionality, both in the ETCS equipment and in the communication channel. They therefore represent a combination of events already identified. Thus, the TRACK-X events are listed in the following table but are not used in the apportionment process undertaken in Part 3 of SUBSET-088.

4.1.1.3 For each base event, the fault tree gates or hierarchical functions that the base event can affect are identified. This identifies the core functionality of ETCS that could fail as a result of the base event failure. This is used to trace the failure progression of each base event through the fault tree.

4.1.1.4 For each base event a brief explanation is provided to explain the context and content of the base event in relation to the ETCS Core Hazard. This describes the effects of the base event failure on the function of ETCS and how this relates to the ETCS Core Hazard. Base events that cannot be classed as initiating events, for example failures of



inherent protective functions (see further 4.1.1.6) of ETCS, are identified as such in the Explanation column.

4.1.1.5 If the relationship of the base event to the ETCS Core Hazard is dependent on the ETCS mode of operation then this is identified within the analysis and the relevant modes assessed. If the base event is applicable through all modes of operation then this is identified as such.

4.1.1.6 The role of ETCS is to display to the driver and to enforce the respect of a safe speed and distance. This mitigates against a large number of technical and operational hazards that can occur in the railway environment. ETCS achieves this role by reading information from external entities, estimating the position of trains, elaborating and sending information between onboard and trackside, displaying information and supervising train braking. These are considered the core functions of ETCS.

Moreover, in order to mitigate the possible failures in the core functions, ETCS also implements a set of protective functions, such as supervision of balise group linking, safety coding of messages, etc.

4.1.1.7 Finally, a criticality is assigned to each base event, without taking into consideration any mitigating conditions, based upon whether the event can be classed as Safety Critical, Safety Related or Not Safety Related. These classifications - set by expert judgement - have been used as a guideline for the analysis performed in Part 3 in order to establish the safety requirements for interoperability. The Part 2 classifications are not themselves the requirements.

The following table presents the base event criticality categorisation together with a brief definition of each category as used within the analysis.

4.1.1.8

<i>Assigned Criticality of Base Event</i>	<i>Interpretation of the Assignment</i>
Safety Critical Function/Data	A function or data item of ETCS which, if it failed would lead directly to the ETCS Core Hazard.
Safety Related Function/Data	A function or data item of ETCS which if failed in addition with other independent functions or conditions could result in the ETCS Core Hazard.
Not Safety Related	A function or data item of ETCS which if failed in addition with other independent safety related functions or conditions would not result in the ETCS Core Hazard.

4.1.1.9 In assessing mitigating conditions, all possible sources are considered.

5. INTEROPERABILITY CONSIDERATIONS FOR ETCS

5.1.1.1 The following ETCS interoperability considerations have been identified from the analysis in section 6 where dependencies and mitigating conditions that ensure the safe functionality of ETCS are defined. These dependencies are both internal and external relative to the ETCS reference architecture.

5.1.1.2 The following ETCS interoperability considerations are grouped into four distinct categories that reflect the core functions of ETCS.

5.1.1.3 Speed and Position Determination:

To ensure that the ETCS onboard system is able to determine its speed and position, reliance is placed upon;

- Eurobalise integrity (reliability and deployment)
- Eurobalise separation (maximum distance between Eurobalise)
- The use of linking information
- Odometry integrity (both reliability and accuracy)

5.1.1.4 Train Speed:

To ensure that the ETCS onboard system is able to respect the maximum permitted train speed and the true speed profile of the track, reliance is placed upon;

- Speed and position determination (as above)
- Driver (respect of indicated information and driver operating procedures)
- Train data (the data entry process, handling of train speed related data and the integrity of this data)
- DMI (integrity of displayed information)
- Receipt of correct information from Trackside (MA Data)

5.1.1.5 Movement Authority Data:

To ensure that the ETCS onboard system is able to respect train separation, location of obstructions/restrictions, speed profile and topography, reliance is placed upon;

- Receipt of a correct Movement Authority from the RBC, including optionally Mode Profile.
- Generation of a correct location report by the onboard system, (speed and location determination, as above)
- Integrity of displayed information and acknowledgement of these information by driver (e.g. mode profiles or track conditions)

5.1.1.5.1 Note: The Emergency Message is a service that is provided by ETCS to reduce the risk due to hazards coming from outside such as avalanches, road vehicles on track etc.



- 5.1.1.5.2 Note: The integrity of the Emergency Message is dependent upon the quality and availability of the radio network, which is outside the scope of ETCS. The operator must take into account the probability of delay, deletion or corruption of Emergency messages when estimating the performances that can be achieved by ETCS emergency messages. If very stringent performances are required, it is possible that an additional independent emergency management is needed.
- 5.1.1.5.3 Note: According to the SRS, the Emergency Message shall use the high priority channel, and thus not be equipped with the safety mechanisms of the normal priority channel. The ETCS Emergency Message function is designed for the shortest possible response time, not for high integrity.
- 5.1.1.6 Brake Command;
To ensure that the ETCS onboard system is able to enforce respect of all speed and distance limits, reliance is placed upon;
- Correct and timely braking application and execution
 - The train braking system
 - Train data (the data entry process, handling of train brake assurance and performance related data and the integrity of this data)
 - Track data (topography and track conditions)
 - The driver (driver vigilance and operating procedures)
- 5.1.1.7 The safety requirements associated with these ETCS interoperability considerations are developed in Part 3 of this document.

6. FUNCTIONAL ANALYSIS

While executing the FMEA below mitigation conditions are taken into account before assigning the criticality.

A mitigation condition is a barrier or circumstance (either internal or external to ETCS) which help **decreasing the probability** of the Base Event reaching the ETCS Core Hazard. The condition can either be specified in the TSI Annex A or be a commonly accepted property of a railway system (e.g. train acceleration rate).

In the last column of the FMEA conditions can be exported to application or external entity, whereas

- a barrier which has not been judged possible to use as a Mitigation Condition on generic specification level, but that should be further studied in the safety analysis of an application is exported to **application** and
- a derived safety requirement for an external entity (interfacing system or process) is exported to the **external entity**.

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
ENG-1 a	Incorrect data to trackside constituents from engineering process	<u>Balise Data</u> . System Data, MA Data, Linking data	Balises are positioned incorrectly in relation to its content/embedded information, the onboard confidence interval and / or co-ordinate data.	All		Safety Critical	Engineering data processing and installation procedures need to be of a SIL4 quality



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
ENG 1 b	Incorrect data to trackside constituents from engineering process	Radio Data, MA Data, System Data, Linking data from trackside	Incorrect data preparation for a specific scheme	All		Safety Critical	Engineering data processing need to be of a SIL4 quality
ENG-2	Incorrect data to onboard from engineering process for a mission	Train Data	Incorrect data preparation for a specific scheme	All		Safety Critical	Engineering data processing need to be of a SIL4 quality
ENG-3	Incorrect train data from engineering process for permanent storage	Fixed Train Data, ETCS ID	Provision of incorrect train data to the data entry process	All		Safety Critical	Scheme Specific Process External to ETCS Engineering data processing need to be of a SIL4 quality
EXT-1	Wrong route or aspect transmitted by interlocking function	Route information linked to MA Data, System Data, Linking data	Error in the interlocking function resulting in incorrect information to ETCS	All		Safety Critical	Interlocking required to provide proper routes
EXT-2	Incorrect train data given to engineering process	Train Data, as for ENG-3	Incorrect data preparation for a specific scheme	All		Safety Critical	Engineering data processing need to be of a SIL4 quality

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
EXT-3	Failure to command Emergency Message (external system)	Provision of Emergency Messages	Emergency action not requested when prevailing conditions require emergency action	All		Safety Critical	Outside the control of ETCS Emergency situations does not occur on a regular basis, therefore time at risk will be low.
DRV-1	Driver attempts to exceed indicated speed or distance	Safe speed and distance as known by ETCS	Driver attempts to exceed indicated safe speed or distance.	FS	Protected by supervision function of both speed and distance.	Safety Related	



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
			In OS, SR and SH more responsibility is on the driver to ensure safety. In these modes ETCS does not have all the information about the line, for example unknown obstacles.	SR, SH	In SR and SH modes there is reduced protection. However the train is supervised to a maximum speed (both for SR and SH) and a maximum distance (only for SR and Level 2). Also, in SR or SH, the train is tripped on passing balises containing "Danger for SH", "Stop if in SR" or balises not in the list given to the train.	Safety Critical	National procedures need to direct driving in SR and SH mode.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
DRV-1 Continued				OS	In OS there is reduced protection; however the train speed and limited distance are supervised by the Dynamic Speed Profile.	Safety Critical	National procedures need to direct driving in OS mode.
			In LS the ETCS on-board equipment is responsible for the background supervision of the train movement to the extent permitted by the information provided by trackside. The driver must observe the existing line-side information (signals, speed boards etc.) and National operating rules.	LS	In LS there is reduced protection; however the train speed and limited distance are supervised by the Dynamic Speed Profile.	Safety Critical	National procedures need to direct driving in LS mode.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
DRV-2	Incorrect Driver input of SR speed, Override	MRSP, DSP leading to incorrect supervision	Driver inputs unsafe SR speed or distance.	SR	Prevailing conditions are such that the driver can drive safely at the excessive speed.	Safety Critical	Data entry procedures To have a hazardous situation, also DRV-1 needs to happen. This should be evaluation for an application.
			Driver overrides an EOA when not allowed		For override an EOA specific conditions must exist for the facility to be invoked; in particular train speed must be below the National limit for Override.	Safety Critical	Use of EOA is usually subject to Authorisation by trackside personnel, however if the driver decides to select the function, ETCS provides no protection Needs to be covered by national procedures.
DRV-3	Incorrect train data entered by driver	Train Data	The driver inputs incorrect train data into the MMI.	All	Validation of train data required	Criticality depends on the data.	



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
DRV-3 (Continued)			Category - Tilting / non-tilting, if incorrect it is possible that the ETCS could allow excessive train speed on bends not suitable for non-tilting trains.	All	Driver vigilance can be claimed in noticing that the train is failing to tilt on bends.	Safety Critical	Data entry procedure should protect against basic human error..
DRV-3 (Continued)			Length - Potential for acceleration out of a change of speed profile too early if the length is understated. Potential derailment possibility on clearing a set of points There could be stopping location issues if train too long for platform.	All	Due to acceleration performance of trains only a significant error in length would cause rear end overspeeding	Safety Related	Data entry procedure should protect against basic human error.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
						Safety Critical (NB, train length is safety critical for level 3 operation in reporting of min safe rear position)	Interlocking (track occupancy) required to protect against the clearing of points, and collision hazards.
DRV-3 (Continued)			Deceleration rate - The supervision function will be incorrect and the train will fail to apply safe breaking curves	All	The parameter entered must be an overestimate of the trains braking capability.	Safety Critical	Data entry procedure should protect against basic human error Driver vigilance is presumed.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
DRV-3 (Continued)			Maximum Permitted Speed - The driver inputs a maximum train speed in excess of that permitted for the train.	All	Needs to be significant error to result in hazard Line speed profile in FS	Safety Critical	Data entry procedure should protect against basic human error. Driver vigilance is presumed
			Loading Gauge and Axle Load - Entry of incorrect parameters for the High speed network	All		Safety Critical	Data entry procedure should protect against basic human error.
DRV-4	Incorrect additional data as part of driver input	Train Data	The driver inputs incorrect additional data into the DMI. Driver ID, ETCS Level, RBC ID/ Telephone No or Adhesion Factor.	All	Acknowledgement of data required.	Criticality depends on the data	Data entry procedure should protect against basic human error.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
DRV-4 (Continued)			Driver ID - System acquires an incorrect ID, operational data only, not safety related	All		Not a Safety Function	
DRV-4 (Continued)			ETCS Level - System in incorrect level	All	The majority of the time the system will undergo a warm start-up and ETCS will only allow valid levels to be entered in accordance with the level transition tables. ETCS start-up procedures	Safety Related	Data entry procedure should protect against basic human error. Driver vigilance is presumed
			ETCS Level - During cold start-up the position will not be known and therefore conflict could exist	All	ETCS start-up procedures On passing the first balise group the position will be known	Safety Related	Driver vigilance is presumed,

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
			Train Running Number - Operational data only, not safety related.	All		Not a Safety Function	
			RBC ID/Telephone Number - System acquires an incorrect RBC Number	All	Upon start-up the Onboard will contact the last known RBC, If unable to contact the RBC there will be a loss or no communication with RBC and the train will remain under the responsibility of the driver.	Safety Related	



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
					During a cold start-up, the onboard does not know its position or RBC area. An incorrect RBC could be contacted. For a MA to be provided to the train, the train has to provide a position report.	Safety Related	



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
DRV-4 (Continued)			<p>Adhesion Factor -</p> <p>Driver fails to perceive that adhesion is, or might be lower and that adhesion factor should be reduced.</p> <p>System acquires an adhesion factor that is greater than achievable under prevailing conditions.</p> <p>Adhesion factor affects braking curve.</p>	All		Safety Critical	<p>Data entry procedure should protect against basic human error.</p> <p>Driver vigilance is presumed</p>
DRV-5	Incorrect driver input (Override or non-leading, Override route suitability etc.)	Current Mode of Operation	Driver inputs unsafe information	Mode Specific	Transition table conditions have to be fulfilled in order to allow some mode changes	Safety Critical	Operating Rules should protect against human errors.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
MMI-1a	False acknowledgement of mode change to less restrictive mode	Current Mode of Operation	The DMI erroneously gives acknowledgement to Kernel with the consequence of entry to UN, RV, SN, SR, SH, LS or OS modes without driver knowledge	FS, PT, OS, LS, SB, SH	A request to enter the less restrictive mode is needed. Also, ETCS mode transition table must be fulfilled (SRS ch. 4.6.2).	Safety Related	Driver vigilance is presumed
			The DMI fails to transmit the acknowledgment with the consequence that the driver is not prepared to take more responsibility		Service Brake is applied after 5 seconds		
			The DMI erroneously gives acknowledgement to Kernel with the consequence of entry to IS	all	Isolation status is shown to the driver	Safety Related	Driver vigilance is presumed Use of external switch to enter Isolation mode



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
MMI-1b	False command to enter NL mode	Current Mode of Operation	DMI erroneously issues command for entry to Non-leading. Rollaway protection is removed, brakes isolated and DMI screen still displays many items of FS/OS modes.	SB, SH, FS, LS SR, OS	Only possible to select Non-leading during standstill (see ETCS mode transition table).	Safety Critical	Driver vigilance. is presumes. Operating Rules should protect against human errors. Product specific safe-guarding of NL entry procedure
MMI-1c	False command of Override request		The DMI issues the command requesting passing of signal at danger without driver intending to do so.	FS, LS OS, SR, SB, SH, UN, PT, SN	Procedures for Override must be fulfilled, kernel accepts the ack only when inside the "rectangle" (SRS ch. 5.8)	Safety Critical	Driver vigilance is presumed
MMI-1d	False acknowledgement of Level Transition	Current Level of Operation	The DMI erroneously gives acknowledgement to Kernel with the consequence avoid or release service brake	FS, LS OS, SR, SB, UN, TR	Procedures for Level Transitions must be fulfilled (SRS ch 5.10) ETCS mode transition table must be fulfilled (SRS ch 4.6.2)	Safety Related	Driver vigilance is presumed.

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
			The DMI fails to transmit the acknowledgment with the consequence that the driver is not prepared to take more responsibility		Service brake is applied after 5 seconds (SRS 5.10.4)		
MMI-1e	False acknowledgment of Train Trip	Safe speed and distance as known by ETCS		TR	ETCS mode transition table must be fulfilled (SRS ch 4.6.2).	Safety Related	Driver vigilance is presumed.
MMI-1f	False acknowledgment of Track Ahead Free	Safe speed and distance as known by ETCS The train can go into FS and receive new MA while section is occupied	The DMI sends a false track ahead free to the on-board kernel	SB, SR, OS, PT, LS	There needs to be an obstacle in front of the train for the situation to be dangerous.	Safety Critical	Driver vigilance is presumed Product specific safeguarding of TAF procedure.
MMI-1g	False request for SH mode	Current Mode of Operation	Shunting initiated at an inappropriate location	SB, FS, LS, SR, OS, UN, PT, SN	Shunting Request is only possible at standstill.	Safety Related	Driver vigilance is presumed. Product specific safeguarding of SH entry procedure



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
MMI-1h	False acknowledgement of undesired train movement (RAM, RMP, SSS, PT distance and reversing distance)	Safe speed and distance as known by ETCS	The DMI erroneously gives acknowledgement to Kernel. Train Brakes are released unintentionally.	SH, FS, LS, SR, OS, UN, PT, RV, SB	Reinitializing of supervision function using new train position	Safety Related	Driver vigilance is presumed
MMI-2a.1	False presentation of train speed	Information to driver	False presentation of the data on the DMI, relative to the data understood by the Kernel - Display of too low actual speed	FS	Protected by Onboard Supervision and monitoring	Safety Related	Driver vigilance is presumed
				Other modes than FS	See DRV-1	See DRV-1	See DRV-1
MMI-2a.2	False presentation of speed (except train speed) or	Information to driver	False presentation of the data on the DMI, relative to the data understood by the Kernel	FS	Protected by Onboard Supervision and monitoring	Safety Related	Driver vigilance is presumed



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
	distance, including supervision status		<ul style="list-style-type: none"> - Display of too high permitted speed/target speed/release speed/ First Line of Intervention - Display of too long target distance . Display of wrong supervision status 	Other modes than FS	See DRV-1	See DRV-1	See DRV-1
MMI-2b	False presentation of mode	Information to driver	<p>False presentation of the data on the DMI, relative to the data understood by the Kernel</p> <ul style="list-style-type: none"> - Display of mode that is of higher level of ETCS responsibility than is actually in operation. 	Mode Specific	Protected by Onboard Supervision and monitoring	Safety Critical	Driver vigilance is presumed
MMI-2c	False presentation of track adhesion factor	Information to driver	False presentation of track adhesion on the DMI misleads the driver.	Mode Specific	Braking curve calculation by kernel	Safety Critical	Driver vigilance is presumed.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
MMI-2d	Failure to present Entry in FS/OS information	Information to driver	Driver does not know that he has to observe speed limitation, because during entry FS/OS track description is not available for whole train length.	FS, OS		Safety Critical	Operational rules for driver
MMI-2e	False presentation of train data/ additional data	Information to driver	Train data are incorrectly displayed or driver is not / incorrectly informed about train data change from an external source	SB, FS, SR, LS, OS, UN, TR, SN, PT, RV	Depending on train data, see further Subset-079	Safety Critical	Operational rules for driver Depending on train data: Product specific safe-guarding
MMI-2f	Failure to display Override status including false enabling of override selection	Information to driver	Override is not activated, but active status is displayed	FS, OS, UN, SR, SN	Protected by Onboard Supervision	Safety Related	Operational rules for driver
			Override is activated, but active status is not displayed		Kernel supervision of : - SR speed and distance - Override time, distance and balise passage.	Safety Critical	



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
			enabled override selection: shown when not expected		kernel accepts the request only when inside the "rectangle"(see conditions in SRS 5.8.2.1)	Safety Related	
MMI-2g	Failure to present acknowledgement message to a less restrictive mode	Information to driver	Failure to presentation an acknowledgement message on the DMI with the consequence that a transition to a less restrictive mode can happen without the driver being prepared to take over more responsibility.	Mode Specific	<ul style="list-style-type: none"> kernel check of mode acknowledgement. Dependent on mode <ul style="list-style-type: none"> a)brake if no ack b)no mode change without ack kernel monitoring of new mode 	Safety Related	Driver vigilance is presumed.
MMI-2h	False presentation of TAF request	Information to driver	Movement authority may be erroneously updated by RBC after driver input	SB, SR, OS, LS, PT		Safety Critical	Operational rules for driver Product specific safeguarding of TAF procedure

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
MMI-2i	Failure to present LX "not protected" information	Information to driver	LX "not protected" information is not shown to the driver. Driver could fail to reduce train speed	FS, OS, LS	Protected by Onboard Supervision	Safety Related	Driver vigilance is presumed.
MMI-2j	False presentation of reversing allowed	Information to driver	"Reversing allowed" information is shown to the driver. Driver could try reversing against valid MA	FS, LS, OS	Protected by Onboard Supervision (RMP)	Safety Related	Driver vigilance is presumed.
MMI-2k	False presentation of level transition announcement	Information to driver	Missing Level transition announcement prevents the driver from taking over more responsibility in time in case of transition to lower level or National System	FS, LS, SR, OS, NL, UN, TR, PT, SN	Acknowledgment within 5 seconds at level transition point	Safety Related	Driver vigilance is presumed..
			Unexpected Level transition announcement misleads the driver.	FS, LS, SR, OS, NL, UN, TR, PT, SN	Kernel Monitoring	Safety Related	Driver vigilance is presumed.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
MMI-3	Falsification of driver's train data/ additional data input stored onboard	Train data	Falsification of the driver's train data input to Kernel, without a possibility for the driver to realise this	All		Safety Critical	Driver vigilance is presumed. MMI-3 can be further developed in a product specific fault tree to obtain a less demanding tolerable failure rate for an individual MMI failure.
MMI-4	Falsification of SR speed/ distance data	exceedance of safe speed or distance	Wrong supervision of maximum staff responsible speed or distance due to falsified input.	SR		Safety Critical	Operational rules for driver
MMI-5	Falsification of train integrity confirmation input	Safe speed and distance as known by ETCS	RBC sends a train to an erroneous track due to wrong integrity information	SB, FS, LS, SR, OS, PT	Company specific protection measures	Safety Critical	Operational rules for driver External equipment to detect train integrity (e.g. axle counters)
MMI-6	Falsification of Virtual Balise Cover	exceedance of safe speed or distance	Wrong processing of balise groups due to falsified input.	SB		Safety Critical	Operational rules for driver
ODO-1	Incorrect standstill indication	Standstill Indication	Indicates Standstill when in motion	All	Detected upon passing a balise.	Safety Critical	Driver vigilance is presumed

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
ODO-2	Speed measurement underestimates trains actual speed	Determination of distance travelled, determination of train position relative to LRBG Position reporting, Provision of MA. Common mode error as it affects both the supervision and the display to the driver	Accuracy of speed known on-board, in ceiling speed monitoring, release speed monitoring and in target speed monitoring in case the compensation of the speed measurement inaccuracy is inhibited	All	In SR the train speed will be low (fixed national value) thus allowing time for driver vigilance.	Safety Critical	Driver vigilance is presumed



ODO-3	Incorrect actual physical speed direction	Determination of train position relative to LRBG	Incorrect train position leading to violation of MA	All	<p><u>When going forward:</u> ETCS-onboard will think the train is reversing and apply RMP. This is not hazardous, but restrictive. If the forward movement is unintended, the RAP will be disabled.</p> <p><u>When going backwards:</u> ETCS-onboard will think the train is running forward and disable the RMP.</p> <p>The error could be discovered when the first expected balise group is not detected, if linking is used.</p>	Safety Related	
ODO-4	The confidence interval for	Position Reports, Information to	Incorrect determination of position resulting in	All	If linking is used, on passing the	Safety Critical	The interlocking should prevent trains from

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
	distance measurement does not include the real position of the train	driver. Incorrect determination of speed and position.	<p>erroneous position reports to the trackside such that the RBC provides a dangerous MA.</p> <p>Underestimated position could result in a train exceeding its MA or failing to reduce speed for a speed restriction.</p> <p>Over-estimation of position could result in a premature acceleration from a speed restriction</p> <p>In level 3 over estimation of position determination is an issue.</p>		<p>next balise group outside its expected window, the balise group will not be accepted and the linking reaction will be invoked (dependent upon linking reaction). But if the error is large (develops quickly) before the next balise group the position of the train known by ETCS on-board is incorrect and potentially dangerous</p>		occupying the same block.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
				SR	In SR the train speed will be low (fixed national value) thus allowing time for driver vigilance.	Safety Related	Driver is responsible for the movements of the train according to national procedures, therefore should be able to maintain it within safe distance.
KERNEL-1	Balise linking consistency checking failure	Linking reaction	Balise linking consistency is a protective function against linking rules violation.	FS, OS, LS	There has to be another coincident failure for this to result in the ETCS Core Hazard.	Safety Related	
KERNEL-2	Balise group message consistency checking failure	Provision of Data to onboard (balise message)	Balise group message consistency checking is a protective function against the receipt of inconsistent messages	All (except NP,SL, SF,IS)	There has to be another coincident failure for this to result in the ETCS Core Hazard.	Safety Related	Safety related balise transmission function is required.
KERNEL-3	Failure of radio message correctness check	Provision of Data to onboard (MA etc.)	Radio message correctness check is a protective function against the receipt of inconsistent messages	All (except NP ,SF,IS)		Safety Related	

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
KERNEL-4	Radio sequencing checking failure	Provision of Data to onboard (MA etc)	Radio sequencing check is a protective function	All (except NP ,SF,IS)	This function is an inherent protective function of ETCS	Safety Related	Message acknowledgement
KERNEL-5	Radio link supervision function failure	Provision of Data to onboard (MA etc)	Radio link supervision is a protective function against receiving the latest valid message later than a specified time. Failure to correctly manage a communication session could result in the loss of communications and a failure to receive more restrictive route information.	FS, OS, LS	This function is an inherent protective function of ETCS (Linking reaction, T_NVCONTACT)	Safety Related	
KERNEL-6	Manage communication session failure	Provision of Data to onboard (MA etc)	Failure to correctly manage a communication session results in the loss of communications and a failure to receive more restrictive route information.	FS, OS, LS	This function is an inherent protective function of ETCS (Linking reaction, T_NVCONTACT)	Safety Related	

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
KERNEL-7	Incorrect LRBG	Determination of train position to LRBG	All position reports are based upon the LRBG. If the onboard reports an incorrect LRBG to the RBC, the train would appear to be at another location, e.g. the previous LRBG	All (except NP ,SF,IS)	This is an inherent core function of ETCS.	Safety Critical	
KERNEL-8	Emergency Message Acknowledgement Failure	Emergency stop failure	Onboard acknowledges receipt of message but does not take it into account	FS,OS, LS, SR, PT	This is an inherent core function of ETCS	Safety Related	
KERNEL-9	Speed calculation underestimates train speed	Determination of speed / location	As for ODO-2	All (except NP ,SF,IS)	This is an inherent core function of ETCS	Safety Critical	
KERNEL-10	Functional failure of standstill detection	Standstill indication and brake intervention	The onboard commands brake release prior to train being at standstill	All (except NP ,SF)	Driver acknowledgement is required to release brakes.	Safety Related	
KERNEL-11	Incorrect traction/braking model (e.g. brake use restrictions)	Dynamic Speed Profile	This is an inherent core function of ETCS	FS, LS, OS	This is an inherent core function of ETCS	Safety Critical	

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
KERNEL-12	Failure of standstill supervision	Protection against undesired movements	This is a protective function performed by ETCS	SB		Safety Critical	
KERNEL-13	Failure of backward distance monitoring	Protection against undesired movements	This is a protective function performed by ETCS	PT, RV		Safety Critical	
KERNEL-14	Failure of reverse movement protection	Protection against undesired movements	This is a protective function performed by ETCS	FS, LS; SR, OS, PT, RV		Safety Critical	
KERNEL-15	Incorrect cab status (TIU failure)	Determination of train position relative to LRBG	Wrong desk reported open resulting in incorrect train position being reported to Trackside. Potential level 3 issue	All (except NP, SF, IS)	MA points in the allowed direction	Safety Critical	Interlocking must protect against track occupancy Operational rules
KERNEL-16	Incorrect train status TIU sleeping/cab status	Current Mode of Operation Standstill protection (KERNEL-12)	Detects sleeping	All	ETCS mode transition table must be fulfilled (SRS ch 4.6.2)	Safety Critical	
KERNEL-17	Wrong Acceptance of MA	Provision of Data to onboard (MA etc)	Onboard accepts incomplete MA information from trackside	All (except NP, SF, IS)	This is an inherent core function of ETCS	Safety Critical	

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
KERNEL-18	Failure to manage RBC/RBC handover	Provision of Data to onboard (MA etc)	Failure to manage the RBC/RBC handover will result in a loss of communications and the on-board being unable to receive more restrictive route information.	All	Onboard has current valid MA Maximum time between radio communications, T_NVCONTACT	Safety Related	
KERNEL-19	Failure of train trip supervision in OS, LS and FS	Supervision of EoA / LoA	Failure of train trip monitoring, unable to trip on demand	FS, OS, LS	Inherent protective function of ETCS	Safety Critical	
KERNEL-20	Failure of train trip supervision, shunting and SR	Supervision of train trip.	Failure of train trip monitoring	SH, SR	Inherent protective function of ETCS	Safety Critical	
KERNEL-21	Incorrect supervision of stop in SR	Supervision of EoA / LoA	Failure of train trip monitoring	SR	Inherent protective function of ETCS	Safety Critical	
KERNEL-22	Incorrect current EoA	Supervision of EoA / LoA Provision and revocation of emergency messages	Incorrect internal data within onboard system leading to the erroneous assumption that the emergency stop position lies beyond the current EoA. Thus the train overruns the emergency stop location	FS, OS, LS		Safety Critical	

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
KERNEL-23	Incorrect train position / train data sent from on-board to trackside	Report train position Report train valid data	<p>The effect of incorrect train data is analysed at DRV 3.</p> <p>An incorrect train position report could result in the RBC formulating an incorrect MA or the erroneous establishment of an RBC / RBC handover process</p> <p>The event deals with the age of speed and location (timestamp) sent to RBC. The position report might include an “old” timestamp for the associated train location. This also implies the violation of clause 5.3.1.3 included in Subset-041</p>	All		Safety Critical	Protection must be provided by the interlocking and associated train detection methods



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
KERNEL-24	Failure of message acknowledgement	Provision of Data to onboard	<p>Message acknowledgement is a protective feature and is used to ensure that the on-board has correctly received transmitted information</p> <p>RBC receives acknowledgement in error, ATP or driver is not aware of the emergency.</p>	FS, LS	Inherent protective function of ETCS	Safety Critical	
KERNEL-25	Incorrect traction/braking model (Acceleration only)	<p>Braking Intervention</p> <p>Maximum train speed calculation</p>	<p>On traction cut-off, there is a delay until when the train stops accelerating</p> <p>Brake intervention times will be incorrect</p>	SH,FS, LS, OS, SR,UN, RV	Inherent safety function of ETCS	Safety Critical	
KERNEL-26	Deleted						
KERNEL-27	Incorrect System Data (e.g. current level)	Current mode of Operation	ETCS enters incorrect unsafe mode for conditions, i.e. less restrictive mode	All	Inherent core function of ETCS	Safety Critical	



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
KERNEL-28	Incorrect confidence interval	Determination of distance travelled Determination of train position to LRBG	Train is outside train calculated confidence interval. The confidence interval determines the max front/rear position of the train. The confidence interval increases in relation to the distance travelled from the last location reference depending on the accuracy of odometry equipment.	All (except NP, SF, IS)	When passing a balise group, which will (if the error is sufficiently large) be found outside the expectation window, this will prompt activation of the link reaction.	Safety Critical	
KERNEL-29	Failure to shorten MA	Supervision of EOA/LOA	Onboard fails to implement MA reduction following co-operative shortening. Only leads to a hazard if the RBC receives information that the on-board has agreed with the shortening.	FS, OS, LS	Inherent core function of ETCS	Safety Related	

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
KERNEL-30	Incorrect shortening of MA	Supervision of EOA/LOA	Onboard applies insufficient shortening of MA	FS, OS, LS	Inherent core function of ETCS	Safety Critical	
KERNEL-33	Wrong processing of MA information	Supervision of EOA/LOA Supervision of train speed	Although the information received from trackside is correct, the onboard fails to establish the correct distance or timers when processing the related MA information	FS, OS, LS	Inherent core function of ETCS	Safety Critical	
KERNEL-34	Incorrect supervision of MA time-outs (sections and overlaps)	Supervision of EOA/LOA Supervision of train speed	Onboard applies insufficient shortening of MA following timeout of any timer In case of this event leading to GATE RS, only overlaps time-outs shall be considered for release speed supervision	FS, OS, LS	Inherent core function of ETCS	Safety Critical	
TI-1	Service brake / emergency brake not commanded when required	Brake control function	Unable to apply brakes on demand.	All (except IS, SL, NL, PS)		Safety Critical	



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
TI-2	Service brake / emergency brake release commanded when not required	Brake control function	Brakes released too early.	All (except IS)		Safety Critical	Brake release is initiated by driver according operational rules.
TI-3	Inappropriate sleeping request	Standstill protection	Inappropriate entry to Sleeping, with loss of Standstill protection as a consequence.	SB	Cabin must be closed and the train must be at standstill.	Safety Critical	Driver vigilance is presumed.
TI-4	Incorrect brake status (TIU failure)	Any	Service Brake indicated ON when OFF	All		Safety Related	Driver vigilance is presumed. A project specific analysis is only necessary in case the brake pressure is used for safety purposes related to service brake feedback. Otherwise it is a RAM issue. It is not relevant for emergency brake, considering 2.3.2.2 from subset 034, v3.1.1

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
TI-5	Incorrect direction controller position report (TIU failure)	Rollaway protection, protection against undesired movements, backwards distance monitoring	<p>In case Dir Ctrl position changes direction:</p> <ul style="list-style-type: none"> Rollaway protection changes direction. <p>In case Dir Ctrl position reported as forward/backward instead of neutral:</p> <ul style="list-style-type: none"> Loss of Rollaway protection in one direction. 	All		Safety Critical	Driver vigilance is presumed.
TI-6b	Wrong Cabin considered as Active	See KERNEL-15	See KERNEL-15	All		See KERNEL-15	See KERNEL-15
TI-7	Inappropriate passive shunting request	Standstill protection	At desk closure On-Board ETCS switches in PS Mode instead of SB. Standstill protection is not provided in this mode.	SH	"Continue Shunting on desk closure" function must be active.	Safety Critical	<p>Driver vigilance is presumed.</p> <p>Driver has to ensure the standstill (e.g. by applying the parking brake) before leaving the cab</p>



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
TI-8	Inappropriate Non Leading permitted signal received	Supervision of EOA/LOA Supervision of train speed	On-board ETCS switches to NL mode after driver selection when not required with a loss of supervision as consequence.	SB, SH, FS, LS, SR OS	Train must be at standstill and Driver selects NON LEADING on DMI. NL mode is displayed on the DMI.	Safety Related	Driver vigilance is presumed.
TI-10	Falsification of train data received by External Source	Supervision of train speed	<ul style="list-style-type: none"> False Cant Deficiency Information (higher than real) False Other International Train Categories False train length False loading gauge False axle load available onboard <p>Results in supervision of wrong SSP or entering of a track which is not suitable for the train</p>	All (except IS, SL, NL, PS, RV)	Driver must confirm changed train data via DMI.	Safety related	<p>Infrastructure planning has to prevent that tilting infringes the allowed gauging.</p> <p>Product specific safe-guarding</p> <p>Operational rules for the driver</p>

© This document has been developed and released by UNISIG



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
TI-11	Traction Cut-Off not commanded when required	Supervision of EOA/LOA Supervision of train speed	Traction Cut-off command not transmitted to the train	All (except IS, SL, NL, PS, SH, SN, RV)	For traction cut-off at warning limit, the criticality could be safety critical.	Safety critical	Product specific safe-guarding
					If the ETCS onboard is not configured for "traction cut-off at warning limit" the criticality would be none.	None	



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Notes
TRACK-1	Incorrect gradient (track description)	Release Speed, DSP	Engineering Data incorrect. Incorrect gradient will result in an incorrect traction/braking model. Trackside equipment failure	<p>Note:</p> <p>In the functionally oriented perspective of the Fault Tree in Part 1, the TRACK events define how erroneous data can lead to the ETCS Core Hazard.</p> <p>Here in Part 2, we are less interested in the detail of the data but more interested in the failure modes of equipment that can create this erroneous data. This is necessary in order to be able to apportion hazard rates to equipment in Part 3. Therefore, the TRACK-events are not analysed further, but instead merged into the TRANS-events, defined to indicate the failure mode and also the transmission channel (Balise or Radio) that could be responsible for the failure.</p> <p>A further splitting of the TRANS-events into constituents and more fine-grained failure modes are done in Subset 088 part 3. However, the FMEA-tables here in Part 2 are not carried out to that level of detail.</p>
TRACK- 2	Incorrect Adhesion Factor “slippery rail”	DSP	Trackside equipment failure.	
TRACK-3	Incorrect Signalling related speed restriction	MRSP, DSP	Engineering Data Incorrect. Trackside equipment failure Level 1 issue only	
TRACK-4	Incorrect MA data	MRSP DSP	Engineering Data Incorrect from RBC Trackside equipment failure	
TRACK-5	Incorrect system data. V_NVREL	MRSP DSP	Engineering Data Incorrect. Trackside equipment failure	
TRACK-6	Incorrect track description (level transition orders)	Determination of Current Level	Engineering Data Incorrect. Trackside equipment failure	



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
TRANS-BALISE-1 (was TRANS-1)	Incorrect balise group message received by on-board Kernel functions as consistent. (Corruption)	Provision of Data to onboard (balise message)	Corruption of balise group message	All	Message consistency check.	Safety Critical	
TRANS-BALISE-2 (was TRANS-2)	Balise group not detected by on-board Kernel functions (Deletion)	Provision of Data to onboard	Onboard fails to receive data from balise and failure to detect any of the balises in the group.	All	If only one balise is missed, consistency checking is mitigation. If all balises in a group are missed, linking is mitigation.	Safety Critical	The criticality of this failure is dependent upon the information missed within the unlinked balise group. Having two (or more) balises in the group can mitigate the hazard of deletion. In situations where deletion is critical, single balise groups are not appropriate.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
TRANS-BALISE-3 (was TRANS-3)	Inserted balise group message received by on-board Kernel functions as consistent. (Insertion)	Provision of Data to onboard (balise message)	Cross-talk of balise group message	All	Message consistency check. Balise group linking.	Safety Critical	
TRANS-OB/RADIO-1 (was TRANS-4)	Incorrect radio message received by the on-board Kernel functions as consistent. (Corruption)	Provision of Data to onboard (MA data etc.)	Incorrect data includes corruption, late, repeated, etc.	All	Message consistency check has to fail. Messages are key coded to ensure authenticity and contain a timestamp to check sequencing and delay.	Safety Critical	Emergency messages are not covered by the MAC code and therefore there is no mitigation. If the onboard can decode the message as an emergency message the message will be acknowledged by the onboard to the RBC



TRANS-OB/RADIO-2 (was TRANS-5)	Radio message not received by the on-board Kernel functions (Deletion)	Provision of Data to onboard (MA data etc.)	<p>Deletion in the communications channel resulting in the on-board being unable to receive a more restrictive MA.</p> <p>The onboard will be unable to receive emergency messages, no protection afforded against the loss of conditional emergency messages. However, this is conditional upon an emergency message being transmitted to the train.</p>	All	<p>Train should be shortened via co-operative MA shortening. For shortening by an emergency message mitigation is provided by the radio link supervision.</p> <p>This ensures messages are received no later than a specified time (T_NVCONTACT) which should be limited to a safe default value defined by each railway.</p> <p>Section timeouts will also provide mitigation.</p>	Safety Critical	
-----------------------------------	--	---	---	-----	---	-----------------	--



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
TRANS-OB/RADIO-3	Inserted radio message received by the on-board kernel functions as consistent. (Insertion)		Erroneous MA received by the on-board resulting in an exceedance of speed / distance	All	Message sequencing, time stamping and addressing as recommended by Cenelec 50159 render this event as non hazardous	Safety Critical	
TRANS-TS/RADIO-1 (was TRANS-6)	Incorrect radio message received by RBC Kernel functions as consistent. (Corruption)	Provision and revocation of emergency messages. Provision of data to the on-board		All	Message consistency check Messages are key coded to ensure authenticity and time stamped as per Cenelec 50129-2 to check sequence and delay.	Safety Critical	



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
TRANS-TS/RADIO-2	Radio message not received by the RBC Kernel functions (Deletion)		Loss of train reports and / or message acknowledgements	All	Train retains existing MA. Protection is afforded at the application level with transmission repeats	Safety Critical	.
TRANS-TS/RADIO-3	Inserted radio message received by the RBC kernel functions as consistent. (Insertion)				Message sequencing, time stamping and addressing as recommended by Cenelec 50159 render this event as non hazardous	Safety Critical	



RBC-1	Radio message deleted in the RBC Kernel in an undetectable way	Provision of Data to onboard (MA data etc.)	<p>Errors in the RBC kernel functions resulting in the on-board unable to receive a more restrictive MA.</p> <p>The onboard will be unable to receive emergency messages, no protection afforded against the loss of conditional emergency messages. However, this is conditional upon an emergency message being transmitted to the train.</p>	All	<p>Train should be shortened via co-operative MA shortening. For shortening by an emergency message mitigation is provided by the radio link supervision.</p> <p>This ensures messages are received no later than a specified time (T_NVCONTACT) which should be limited to a safe default value defined by each railway.</p> <p>Section timeouts will also provide mitigation.</p>	Safety Critical	
-------	--	---	---	-----	---	-----------------	--



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
RBC-2	Incorrect RBC radio message sent from the RBC kernel functions, such that the message appears consistent	Provision of Data to onboard (MA data etc.)	Errors in the RBC kernel resulting in erroneous messages to the Euroradio trackside function.	All	Message consistency check. Messages are key coded to ensure authenticity, Sequencing and Timestamp.	Safety Critical	Messages via the high-priority channel are not covered by the MAC code and therefore there is no mitigation. If the onboard can decode the message as an emergency message the message will be acknowledged by the onboard to the RBC.
RBC-3	RBC misinterprets a message from an adjacent RBC causing an incorrect message to be sent to the onboard	Provision of Data to onboard (MA data etc.)	Errors in the kernel of the RBC. Incorrect data includes corruption, late, repeated, etc.	All	Message consistency check. Messages are key coded to ensure authenticity, Sequencing and Timestamp.	Safety Critical	



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
RBC-4	Erroneous message sent from RBC to an adjacent RBC	Provision of Data to RBC	Errors in the kernel of the RBC. Incorrect data includes corruption, late, repeated, etc.	All	Message consistency check. Messages are key coded to ensure authenticity, Sequencing and Timestamp.	Safety Critical	



7. TRANSMISSION CHANNEL EVENTS

- 7.1.1.1 Each TRANS-ENTITY-X event in section 6 consists of several different transmission related events, each belonging to exactly one constituent and one functional element within that constituent. Identification of these events to allow proper allocation to each constituent will be undertaken in SUBSET-088 Part 3 as part of the process of apportioning the ETCS THR.

