ERTMS/ETCS
ETCS Application Level 1 - Safety Analysis **Part 2 - Functional Analysis**
REF : SUBSET-088-1 Part 2 ISSUE : 3.8.0 DATE : 07-05-24

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

1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.0.1. 14-05-01	All	Document Creation based on level 2	SC
0.0.2 14-02-02	All	Document completely rebuilt based on level part 2 v0.3.0	SC
0.0.3	All	Revised according to revision of part 1 v003	SC
0.0.4 26-02-02	6, 7, 8	Revised according to comments	SC
2.0.0. 27-02-02		Raised in issue for release to the EEIG	WLH
2.0.1. 27-10-02	Document Title 4.1.1.1	Report number deleted Minor amendments to tables Section 7 & 8 moved to part 3 0f Subset 088	WLH
2.0.2. 19-12-02	4.1.1.2 expanded	Update with review comments from Ans & Sie. Improve links to the fault tree and clarification of events	WLH
2.0.3. 15-01-03	4.1.1.2. amended ODO 4 definition amended TRANS events rationalised Other events clarified.	Update following review meeting on 14-01-03	WLH
2.0.4 27-01-03	Event 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 18-10-04	Section 6	Section 6.- Mode Column reviewed and updated with applicable modes Section 6.- Changed affected functions of events Kernel-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 08-04-10	Section 6	Update with new/changed MMI-x events	KN
2.3.2 14-09-10		Notes taken during RAMS-meeting, as proposal to Karin to continue work.	DARI
2.3.3 15-10-10	Section 6	Include new mode Limited Supervision Insert new column "mitigation conditions" in FMEA and update according to methodology concluded in RAMS group	KN

2.3.4 15-03-11		“MMI” changed to “DMI” except for "MMI-x" events	KN
		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)	
2.3.5 17-06-2011	Section 6	Update according to Subset-079: MMI-4 removed	KN
2.3.6		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 and MMI-2k 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		• 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	TIU-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 2nd release version	RAMS WP
3.7.0	No change	Release version	RAMS WP

3.7.1	Section 6	ODO-4: description was changed to clarify that this base event also covers relocation function. This issue is related to CR782/870 ODO-5: this new base event is introduced in connection with analysis of CR1345 for cold movement functionality	KN
3.7.2	Section 6	Formal correction	KN
		New template	KN
3.7.3	No change	Internal RAMS Baseline	RAMS WP
3.7.4	Section 6	Formal changes	KN
3.7.5	Section 6	Kernel-13, Kernel-14 (CR1341), MMI-1j and MMI-2m added	KN
3.7.6	Section 6	ODO-4 changed after discussion with EECT New events Kernle-35 and -36 added	KN
3.7.7		Editorial changes Note: A previous edition was used to update and finalise SUBSET-091 (ed. 4.0.0). In the meantime, this document was also completed and the updated edition of this document does not affect the content of SUBSET-091	RAMS WP
3.8.0 07-05-24	Cover page, footer, 4.1.1, 6.1.3	Application of quality checks proposed by SG Baseline 4 release version	KN

2. TABLE OF CONTENTS

3. INTRODUCTION

3.1.1.1 This document is Part 2 of the ETCS analysis. It provides the Application Level 1 functional analysis. This is undertaken 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 ERTMS/ETCS UNISIG reference architecture (as captured in the FMEA's listed in Part 0) and also within ETCS. The second objective is to determine the claims that can be made to prevent or reduce the probability of the ETCS Core Hazard defined in Part 1, following these failures.

3.1.1.3 The analysis includes consideration of each of the main operational modes of the system applicable to level 1 in a manner whereby all assumptions are clearly visible.

4. DESCRIPTION

4.1.1.1 The 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 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 ERTMS/ETCS 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.

Note: The entities considered for level 1 are Balise, Radio (on-board or trackside) and Loop 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. Therefore the TRACK-X events are listed in the following table but are not used in 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 main functions of ETCS that can fail as a result of the base event and can be 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 form external entities, estimating the position of trains, elaborating and sending information between on-board 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 balise telegrams, 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 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

Assigned Criticality of Base Event	***Interpretation of the Assignment***
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 ERTMS/ETCS UNISIG 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 on-board 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 on-board 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 on-board system is able to respect train separation, speed profile and topography, reliance is placed upon;

- Receipt of a correct Movement Authority and track conditions from the balises and infill media (balise, loop, RIU)
- Integrity of displayed information and acknowledgement of these information by driver (e.g. mode profiles or track conditions)

5.1.1.6 Brake Command;

To ensure that the ETCS on-board 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 data, 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 helps **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-1a	Incorrect data to trackside constituents from engineering process	Balise Data, System Data, MA Data, Linking data	Balises are positioned incorrectly in relation to its content/embedded information, the on-board confidence interval and / or co-ordinate data	All		Safety Critical	Engineering data processing and installation procedures need to be of a SIL4 quality
ENG-1b	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

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
ENG-1b (Continued)	Incorrect engineering data processing	MA Data, System Data, Linking data from the trackside	Radio infill message not referring to the good LRBG (infill only accepted in FS and LS)	FS, LS		Safety Critical	Engineering data processing need to be of a SIL4 quality
ENG-2	Incorrect data to on-board 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 the 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

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
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	
			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). 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. In SR, the train is tripped by a	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
					balise containing MA information with V_MAIN=0		
				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.
DRV-2	Incorrect Driver input of SR	MRSP, DSP leading to	Driver inputs unsafe SR speed.	SR	Prevailing conditions are	Safety Critical	Data entry procedures.

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
	speed, Override	incorrect supervision			such that the driver can drive safely at the excessive speed. SR mode is not the main mode of operation		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 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 DMI.	All	Validation of train data required	Criticality depends on the data	
DRV-3 (Continued)			Category - Tilting / non-tilting, if incorrect it is possible that the ETCS could allow	All	Driver vigilance can be claimed in noticing that the train is failing to	Safety Critical	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
			excessive train speed on bends not suitable for non-tilting trains.		tilt on bends.		
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.
						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.

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
DRV-3 (Continued)			Traction/Brake parameters - The supervision function will be incorrect and the train will fail to apply safe braking 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..
DRV-3 (Continued)			Maximum Train 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, or Adhesion Factor.	All	Acknowledgement of data required.	Criticality depends on the data	Data entry procedure should protect against basic human error.
			Driver ID - System acquires an incorrect ID, operational	All		Not a Safety Function	

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
			data only, not safety related				
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
DRV-4 (Continued)			Train Running Number - Operational data only, not safety related.	All		Not a Safety Function	
DRV-4			Adhesion Factor -	All		Safety	Data entry procedure should protect against

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
(Continued)			Driver fails to perceive that adhesion is, or might be lower and that adhesion factor should be reduced. System acquires an adhesion factor that is greater than achievable under prevailing conditions. Adhesion factor affects braking curve.			Critical	basic human error. Driver vigilance is presumed
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.
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, AD, OS, LS, SB, PT, 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

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
					Kernel accepts the ack only when it is inside the "rectangle"		
			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
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 are isolated and DMI screen still displays many items of FS/OS modes.	SB, SH, FS, LS, SR,AD, OS	Only possible to select Non-leading during standstill.	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		The DMI issues the command requesting	FS, LS, OS, SR,	Procedures for Override must be	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
	request		passing of signal at danger without driver intending to do so.	SB, SH, UN, PT, SN	fulfilled, kernel accepts the ack only when inside the "rectangle" (SRS ch. 5.8)		
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, AD, SN	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.
			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 acknowledgement 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-1g	False request for SH mode	Current Mode of Operation	Shunting initiated at an inappropriate location	SB, FS, LS, SR, OS, AD,	Shunting Request is only possible at	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
				UN, PT, SN	standstill.		Product specific safeguarding of SH entry procedure
MMI-1h	False acknowledgement of undesired train movement (RAM, RMP, UDMP, 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-1j	False command to inhibit BTM alarm reaction	Safe speed and distance as known by ETCS	No reaction is applied when BTM alarm is activated. BG with safety information can be missed.	SB, SH, SR	Inhibition can only be performed when train is in standstill. Inhibition will be revoked when the maximum allowed distance is reached, or if OBU transits to another mode.	Safety Related	Driver is aware of inhibition due to icon displayed on DMI, so Driver vigilance is presumed.
MMI-2a.1	False presentation of	Information to driver	False presentation of the data on the DMI, relative	FS	Protected by On-board	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
	train speed		to the data understood by the Kernel - Display of too low actual speed		Supervision and monitoring		
				Other modes than FS	See DRV-1	See DRV-1	See DRV-1
MMI-2a.2	False presentation of speed (except train speed) or distance, including supervision status	Information to driver	False presentation of the data on the DMI, relative to the data understood by the Kernel - 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	FS	Protected by On-board Supervision and monitoring	Safety Related	Driver vigilance is presumed
				Other modes than FS	See DRV-1	See DRV-1	See DRV-1
MMI-2b	False presentation of mode	Information to driver	False presentation of the data on the DMI, relative to the data understood by the Kernel - Display of mode that is of higher level of ETCS responsibility than is	Mode Specific	Protected by train speed supervision	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
			actually in operation.				
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.
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, AD, 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	SB, SH, FS, AD, LS, SR, OS, UN, PT, SN	Protected by On-board Supervision	Safety Related	Operational rules for driver
			Override is activated, but active status is not displayed		Kernel supervision of : - SR speed and distance	Safety Critical	Entry procedure to override Operational rules for driver

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
					- Override time, distance and balise passage.		
			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	Operational rules for driver
MMI-2g	Failure to present acknowledge-ment 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	• kernel check of mode acknowl-edgement. Dependent on mode a) brake if no ack b) no mode change without ack • kernel monitoring of new mode	Safety Related	Driver vigilance is presumed.
MMI-2i	Failure to present LX “not protected”	Information to driver	LX “not protected” information is not shown to the driver. Driver could	FS, OS, LS, AD	Protected by On-board Supervision	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
	information		fail to reduce train speed				
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, AD	Protected by On-board Supervision (UDMP)	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, AD	Kernel Monitoring	Safety Related	Driver vigilance is presumed.
MMI-2m	Failure to indicate BTM alarm reaction inhibition	Information to driver	Missing indication of BTM alarm reaction inhibition misleads the driver. OBU is still allowed to move over BMM without track condition stored. In case of real BTM failure, BG with safety	SB, SR, SH	Inhibition will be revoked when the maximum allowed distance is reached, or if OBU transits to another mode.	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
			information can be missed				
MMI-3	Falsification of driver's train data/additional data input stored on-board	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-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.

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 to LRBG Position reporting (only in FS when infill radio is used), 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	When going forward: ETCS on-board will think the train is reversing and apply UDMP. This is not hazardous, but restrictive. If the	Safety Related	

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
					forward movement is unintended, the RAP will be disabled. When going backwards: ETCS on-board will think the train is running forward and disable the UDMP/RMP. The error could be discovered when the first expected balise group is not detected, if linking is used.		
ODO-4	The confidence interval for distance measurement does not include the real position of the train	Incorrect determination of speed and position. Position Report (only in FS when infill radio is	Over-estimation of position could result in a premature acceleration from a speed restriction	All	If linking is used, on passing the next balise group outside its expected window, the balise group will not be accepted and the	Safety Critical	The interlocking should prevent trains from 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
	c)	used), Information to driver.			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		
				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.
ODO-5	Cold Movement not detected	Unsafe train position Undetected passing of BG	On-board uses wrong information for train run stored information • EOLM	NP, SB	Application specific permissible maximum	Safety Critical	Project specific analysis for maximum distance which vehicle is permitted to move

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
		Exceedance of safe distance Erroneously valid information	information, • train position, • ETCS Level, • RBC ID, • table of trackside supported events which is set to invalid when NP is entered is set to valid when cold movement is not detected		distance to move in NP is not exceeded. Tolerated non-zero movement will be added to the confidence Interval. In NP EB is permanently commanded.		while being considered “not moved”
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 on-board (balise message)	Balise group message consistency checking is a protective function against the receipt of inconsistent messages	All (except NP, 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	Provision of Data	Radio message	All		Safety	

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
	message correctness check	to on-board (MA etc.) with radio infill	correctness check is a protective function against the receipt of inconsistent messages	(except NP,SF, IS)		Related	
KERNEL-4	Radio sequencing checking failure	Provision of Data to on-board (MA etc) with radio infill	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 on-board (MA etc) with radio infill	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 on-board (MA etc) with radio infill	Failure to correctly manage a communication session results in the loss of communications and a failure to receive more restrictive route	FS, OS. LS	This function is an inherent protective function of ETCS (Linking reaction, T_NVCONTACT)	Safety Related	

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
			information.				
KERNEL-7	Incorrect LRBG	Determination of train position to LRBG	All position reports are based upon the LRBG. If the on-board reports an incorrect LRBG to the RIU, the train would appear to be at another position e.g. the previous LRBG	All (except NP ,SF,IS)	This is an inherent core function of ETCS.	Safety Critical	
KERNEL-9	Speed calculation underestimates train speed	Determination of speed	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 on-board 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, OS, LS	This is an inherent core function of ETCS.	Safety Critical	
KERNEL-12	Failure of standstill supervision	Protection against undesired movements	This is a protective function performed by ETCS	SB		Safety Critical	

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
KERNEL-13	Failure of reverse movement distance monitoring	Protection against undesired movements	This is a protective function performed by ETCS	PT, RV		Safety Critical	
KERNEL-14	Failure of unauthorised direction 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 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 on-board (MA etc)	On-board accepts incomplete MA information from trackside	All(except NP ,SF,IS)	This is an 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-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-24	Failure of message acknowledge-ment	Provision of Data to on-board	Message acknowledgement is a protective feature and is used to ensure that the on-board has correctly received transmitted information RIU receives acknowledgement in error, ATP or driver is not aware (of restrictive MA)	FS, LS	Inherent protective function of ETCS	Safety Critical	
KERNEL-25	Incorrect traction/braking model (Acceleration only)	Braking Intervention Maximum train speed calculation	On traction cut-off, there is a delay until when the train stops accelerating Brake intervention times will be incorrect	SH,FS, LS,OS, SR,UN, RV	Inherent safety 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-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	
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-32	Failure of Loop message consistency checking	Provision of Data to on-board (loop message)	Loop group message consistency checking is a protective function against the receipt of inconsistent messages	FS, LS	There has to be another coincident failure for this to result in the ETCS Core Hazard.	Safety Related	Safety related loop transmission function.

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
KERNEL-33	Wrong processing of MA information	Supervision of EOA/LOA Supervision of train speed	Although the information received from trackside is correct, the on-board fails to establish the correct distance and/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	On-board 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	
KERNEL-35	Incorrect supervision of odometry errors for distance measurement	Check of odometer accuracy thresholds. Storage of accumulated underestimation / overestimation in measuring the movements over	The on-board does not apply safe reaction in case the accumulated underestimation/overestimation in measuring the movements over the defined total distance travelled exceeds the safety threshold.	All (except NP, IS, SF)	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
		a defined total distance					
KERNEL-36	Incorrect relocation of location based information	Determine EoA/LoA. Determine MRSP (based on location based information)	On-board fails to relocate location data in case no linking is available. Wrong distance calculated to EoA/start and end location of MRSP.	All (except NP, SB, PS, SL, NL, TR, PT, SF, IS)	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	
TI-2	Service brake / emergency brake release commanded when not required	Brake control function	Brakes released too early.	All (except IS)		Safety Critical	Driver vigilance is presumed 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	Any	Service Brake indicated ON when OFF	All (except		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
	failure)			NP, SL, NL,SF, IS)			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
TI-5	Incorrect direction controller position report (TIU failure)	Rollaway protection, protection against undesired movements, backwards distance monitoring	In case Dir Ctrl position changes direction: • Rollaway protection changes direction. In case Dir Ctrl position reported as forward/backward instead of neutral: Loss of Rollaway protection in one direction.	All		Safety Critical	Driver vigilance is presumed
TI-6b	Wrong Cabin	See KERNEL-15	See KERNEL-15	All		See	See KERNEL-15

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
	considered as Active					KERNEL-15	
TI-7	Inappropriate passive shunting request	Standstill protection	At desk closure on-board 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	Driver vigilance is presumed. Driver has to ensure the standstill (e.g. by applying the parking brake) before leaving the cab
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	• False Cant Deficiency Information (lower than real) • False Other International Train Categories • False train length • False loading gauge	All (except IS, SL, NL, PS, RV)	Driver must confirm changed train data via DMI (project specific)	Safety related	Infrastructure planning has to prevent that tilting infringes the allowed gauging. Product specific safe-guarding Operational rules for the driver

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
			• False axle load available on-board Results in supervision of wrong SSP or entering of a track which is not suitable for the train				
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 on-board 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	Mode	Mitigation Condition	Criticality	Exported Conditions
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	Note: 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. 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 the transmission channel (Balise, Loop or Radio) that could be responsible for the failure. 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.			
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				
TRACK-4	Incorrect MA data	MRSP DSP	Engineering Data Incorrect from RIU Trackside equipment failure				
TRACK-5	Incorrect system	MRSP DSP	Engineering Data				

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
	data. V_NVREL		Incorrect. Trackside equipment failure				
TRACK-6	Incorrect track description (level transition orders)	Determination of Current Level	Engineering Data Incorrect. Trackside equipment failure				
TRANS-BALISE-1 (was TRANS-1)	Incorrect balise group message received by the on-board Kernel functions as consistent	Provision of Data to on-board (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	Provision of Data to on-board	On-board 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

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
							are not appropriate.
TRANS-BALISE-3 (was TRANS-3)	Inserted balise group message received by the on-board Kernel functions as consistent	Provision of Data to on-board (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	Provision of Data to on-board (MA data etc.) with infill radio	Incorrect data includes corruption, late, repeated, etc.	FS, LS	Message consistency check. Messages are key coded to ensure authenticity and contain a Timestamp to check sequencing and delay.	Safety Critical	
LEU-H4	Transmission of an erroneous telegram / telegrams interpretable as correct, due to failure within the	Provision of Data to on-board (balise message)	Corruption of balise group message	All	Message consistency check.	Safety Critical	

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
	LEU function						
RIU-2	Incorrect RIU radio message received by the on-board kernel functions as consistent.	Provision of Data to on-board (MA data etc.)	Incorrect data includes corruption, late, repeated, etc.	FS, LS	Message consistency check Messages are key coded to ensure authenticity. Sequencing and Timestamp	Safety Critical	.
TRANS-LOOP-1	Incorrect loop message received by the on-board kernel functions as consistent.	Provision of Data to on-board	Corrupted loop message received as consistent	FS, LS	Message consistency check	Safety Critical	
TRANS-LOOP-3	Inserted Loop message received by the on-board kernel functions as	Provision of Data to on-board (infill message)	Cross-talk of loop group message resulting in a false release of braking	FS, LS	Message consistency check. Balise group linking.	Safety Critical	

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Mitigation Condition	Criticality	Exported Conditions
	consistent						
TRANS-LOOP-4	Non-infill Loop message deleted	Provision of Data to on-board (non-infill message)	Loop message does not reach ETCS on-board	Any		Safety Related	Regarding “SR distance information from loop” it is assumed that operational safety does not rely on this message. Regarding “Data to be used by applications outside ERTMS/ETCS” the criticality is application dependent.

6.1 Functional Analysis of Virtual Balise Cover Function

6.1.1 Introduction

6.1.1.1 The purpose of this FMEA is to derive proposed Engineering Rules (ENG RULE) and Operational Rules (OP RULE) in relation to the Virtual Balise Marker function defined in section §3.15.9 of SUBSET-026 v3.4.0, v3.6.0 and 4.0.0. It is assumed that the infrastructure owner derives and implements these rules.

6.1.1.2 It is furthermore assumed that the infrastructure owner defines correct Virtual Balise Cover orders and supplies the driver with these orders in a process that guarantees the correctness and timeliness of the order.

6.1.1.3 Normally, the FMEAs in UNISIG only concern the information at the interoperable interfaces of ETCS. In order to fulfil the above purpose, however, this FMEA also analyses some ERTMS/ETCS on-board internal failure modes and some operational situations. The analysis is then still performed for the information flowing on the interfaces; however, this shall then be understood as the handling of this information inside ERTMS/ETCS on-board all the way into the execution of the function using it.

6.1.1.4 DMI failures modes are included, using SUBSET-079 as input. Driver failures are however not analysed here.

6.1.1.5 This FMEA analyses the two information packets “VBC marker” and “VBC order”. They are given the ERTMS/ETCS on-board in different ways:

- The VBC marker analysed in chapter 6.2.1 can only be given from a balise, as Packet 0 from trackside with version X=2 and Packet 200 from trackside with version X=1, Y=1.
- The VBC order analysed in chapter 6.2.2 can either be given from a balise, as Packet 6, or from the driver as DMI input.

6.1.1.6 The analysis in cases 6.2.2.2.3.x uses the failure cause “The T_VBC is set to a value which doesn’t exceed the maximum time of train operation inside the LUC”. Therefore, it is here assumed that T_VBC is rather set too long instead of too short, and that the driver will systematically have to manually check all applicable VBCs once at SoM[1] inside this area. The assumption is further elaborated and defined in the FMEA, see OP RULE 1 and OP RULE 2.

6.1.1.7 Compatibility with baseline 2: a B2 ERTMS/ETCS on-board equipment will be stopped due to system version check if entering a LUC B3 X=2 area; in a B3 X=1 LUC area a B2 ERTMS/ETCS on-board equipment will not be protected by version check and will not consider VBC information included in balise groups. So external protections are necessary to avoid a B2 ERTMS/ETCS on-board equipment entering such area.

[1] It is further assumed that commissioning of the LUC is not done with trains operating in traffic inside it.

6.1.2 FMEA

6.1.2.1 Virtual Balise Cover Marker

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			Proposed External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
6.1.2.1.1-1----------	NID_VBCMK	**DELETION**	Engineering error in non-commissioned balises (e.g. VBC marker forgotten)	Any but NP	The ERTMS/ETCS on-board will not ignore the balise telegram in the LUC	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	ENG RULE 1: The setting of a VBC marker needs to follow a safe process	Catastrophic	-
6.1.2.1.1.2			Any failure of the non-trusted transmission system	Any but NP	As above	As above	As above	-	Catastrophic	The Eurobalise code protects against losing a packet inside a balise telegram. If the whole telegram is lost, there is no hazard.
6.1.2.1.2.1		**CORRUPTION**	Engineering error in non-commissioned balises (e.g. wrong NID_VBCMK programmed)	Any but NP	In case the balise telegram should have been ignored: The ERTMS/ETCS on-board will not ignore the balise telegram	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	ENG RULE 1: The setting of a VBC marker needs to follow a safe process	Catastrophic	

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			Proposed External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
6.1.2.1.2.2					In case the balise should not have been ignored: The ERTMS/ETCS on-board will ignore the balise telegram if there is a VBC order pointing to the new "wrong" NID_VBCMK	H2: Balise information (potentially restrictive) intended for traffic will be ignored	Exceedance of safe speed or distance	ENG RULE 1: The setting of a VBC marker needs to follow a safe process	Catastrophic	It is not certain that there is a VBC order pointing to the new "wrong" id. Ignoring all balise telegrams in a group can lead to a linking reaction.
6.1.2.1.2.3			Any failure of the non-trusted transmission system	Any but NP	As above (both cases)	As above (both cases)	As above (both cases)	As above (both cases)	Catastrophic	The Eurobalise code protects against corruption

6.1.2.1.3.1		**INSERTION**	Any failure of the non-trusted transmission system, i.e. cross-talk	Any but NP	If a VBC marker is cross-talked, the ERTMS/ETCS on-board will ignore the balise telegram according to rules in SUBSET-026 v3.4.0	None	None		'	

6.1.2.2 Virtual Balise Cover Order

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
6.1.2.2.1.1	Q_VBCO, NID_VBCMK, NID_C, T_VBC	**DELETION**	Any failure of the non-trusted transmission system	Any but NP	Intended setting of VBC order is not performed (in case Q_VBCO=1 was intended)	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	ENG RULE 2: A balise group giving a VBC order shall consist of at least two balises	Catastrophic	
6.1.2.2.1.2					Intended removal of VBC is not performed (in case Q_VBCO=0 was intended)	H2: Balise information (potentially restrictive) intended for traffic will be ignored	As above	As above	Catastrophic	As above

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
6.1.2.2.1.3			ERTMS/ETCS on-board internal failure	Any but NP	As above	As above	As above		Catastrophic	Product specific safeguarding to SIL4[2]
6.1.2.2.1.4			ERTMS/ETCS on-board memory buffer full	Any but NP	As above	As above	As above		Catastrophic	The number of memorised VBCs on-board is defined in SUBSET-040 v3.3.0 and v3.4.0 §4.3.2.1.1w (and must thereby be respected by trackside). For transitions between countries/regions, the previous VBCs are deleted when a balise group with a new country/region identifier (NID_C) is received, see SUBSET-026 v3.4.0 and v3.6.0 §3.15.9.5d.

[2] For DMI function failures, the SIL4 safety is expected to be built up by an entry+validation process, as in the case of e.g. train data entry.

Ref ID	Macro Function Data Item	Failure Mode	Failure Cause	Operation Mode	Failure Effects			External Protection / Mitigation Barriers	Severity	Internal Barriers
					Local	Intermediate	Initial End Effect			
6.1.2.2.1.5			The VBC order never reaches the ERTMS/ETCS on-board because the train has been moved into a LUC in a mode where balises are not read (NP, IS and SF)	Any but NP	As above	As above	As above	OP RULE 1: Driver needs to “re-enter and validate” or “remove” VBCs at each SoM inside a LUC to be sure the onboard uses the correct set of VBCs	Catastrophic	-

6.1.2.2.1	**CORRUPTION**	Any failure of the non-trusted transmission system	Any but NP	Intended setting of VBC order is not performed (in case Q_VBCO=1 was intended)	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	None needed	Catastrophic	The Eurobalise code protects against corruption in the transmission channel
6.1.2.2.2				Intended removal of VBC order is not performed (in case Q_VBCO=0 was intended)	H2: Balise information (potentially restrictive) intended for traffic will be ignored	As above	As above	Catastrophic	As above
6.1.2.2.3		ERTMS/ETCS on-board internal failure	Any but NP	As above (both cases)	As above (both cases)	As above (both cases)		Catastrophic	Product specific safeguarding to SIL4[3]. Specifically for corruption of T_VBC, special considerations are needed, and the case is analysed separately below, see B.2.2.2.3.x.

[3] For DMI function failures, the SIL4 safety is expected to be built up by an entry+validation process, as in the case of e.g. train data entry.

6.1.2.2.3.1	T_VBC	**CORRUPTION**	Train is **outside** LUC 1. The T_VBC is set to a value which doesn't exceed the maximum time of train operation inside the LUC. 2. ERTMS/ETCS on-board internal failure (e.g. clock) 3. External failure (e.g. UTC)	All	Timer expires and VBC order removed earlier than intended (hazardous case is only if it happens before commissioning of LUC).	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	ENG RULE 3: Balise group giving VBC order shall be placed at all entries to a LUC and need to correctly reflect the status of the LUC at all times, both setting valid VBCs and removing non-valid[4] VBCs and to define adequate T_VBC (long enough)	Catastrophic	
6.1.2.2.3.2					Timer expires and VBC order removed later than intended.	H2: Balise information (potentially restrictive) intended for traffic will be ignored	As above	As above	Catastrophic	

[4] The remove VBC order should be enforced until the need for using the same VBC code again arises.

6.1.2.2.3.3			Train is **inside** LUC with ERTMS/ETCS on-board **powered off** 1. The T_VBC is set to a value which doesn't exceed the maximum time of train operation inside the LUC. 2. ERTMS/ETCS on-board internal failure (e.g. clock) 3. External failure (e.g. UTC)	NP	Timer expires and VBC order removed earlier than intended (hazardous case is only if it happens before commissioning of LUC).	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	OP RULE 1 Driver needs to "re-enter and validate" or "remove" VBCs at each SoM inside a LUC to be sure the onboard uses the correct set of VBCs	Catastrophic	

6.1.2.2.3.4					Timer expires and VBC order removed later than intended.	H2: Balise information (potentially restrictive) intended for traffic will be ignored	As above	OP RULE 2: For every vehicle, driver needs to remove the VBC orders at the first SoM inside a LUC after the commis-sioning of the LUC [5]	Catastrophic	

[5] To cover the case of erroneously too long T_VBC, the manual removal needs to be done once per vehicle after the commissioning:. thus it is not enough to enforce this procedure only up to commissioning date + T_VBC days

6.1.2.2.3.5			Train is **parked inside** LUC with ERTMS/ETCS on-board **powered on** [6] 1. The T_VBC is set to a value which doesn't exceed the maximum time of train operation inside the LUC. 2. ERTMS/ETCS on-board internal failure (e.g. clock) 3. External failure (e.g. UTC)	Any but NP	Timer expires and VBC order removed earlier than intended (hazardous case is only if it happens before commissioning of LUC).	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	As ENG RULE 3 above. In addition: the balise groups need to be placed also where trains are normally parked with ERTMS/ETCS on-board powered. If this is not possible, OP RULE 1 and 2 can be applied also in other situations than SoM [7].	Catastrophic	
6.1.2.2.3.6					Timer expires and VBC order removed later than intended.	H2: Balise information (potentially restrictive) intended for traffic will be ignore	As above	As above	Catastrophic	

[6] Since the ERTMS/ETCS On-board is powered on the whole time, the Start of Mission procedure is not executed and therefore barrier OP RULE 1 is not effective.

[7] If this barrier is pursued, situations to be considered shall include using a vehicle that has been parked with ERTMS/ETCS On-board in SL mode, since it could be hazardous to receive e.g. erroneous National Values and Level Transition Orders, which will be used later when the vehicle becomes the leading vehicle.

6.1.2.2.3.7			Train is running **inside** LUC with ERTMS/ETCS on-board **powered on** 1. The T_VBC is set to a value which doesn't exceed the maximum time of train operation inside the LUC. 2. ERTMS/ETCS on-board internal failure (e.g. clock) 3. External failure (e.g. UTC)	Any but NP	Timer expires and VBC order removed earlier than intended (hazardous case is only if it happens before commissioning of LUC).	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	The time at risk is small. see further B2.3.1.3.	Catastrophic	
6.1.2.2.3.8					Timer expires and VBC order removed later than intended.	Not an applicable scenario. A LUC is not commissioned when there is traffic inside it.	n.a.	n.a.	None	n.a.

6.1.2.2.4.1		**INSERTION**	Any failure of the non-trusted transmission system; i.e. cross-talk	Any but NP	If a correct VBC order is cross-talked, the ERTMS/ETCS on-board will use it and - set the VBC (in case Q_VBCO=1) or - remove the VBC (in case Q_VBCO=0)	None, since the VBC order is correct	None		'	
6.1.2.2.4.2			ERTMS/ETCS on-board internal failure	Intended setting of VBC order is not performed (in case 'set VBC' is inserted)	H1: Balise information (potentially permissive) only intended for test purposes will be used in traffic	Exceedance of safe speed or distance	None needed	Catastrophic		Product specific safeguarding to SIL4[8].
6.1.2.2.4.3				Intended removal of VBC order is not performed (in case 'remove VBC' is inserted)	H2: Balise information (potentially restrictive) intended for traffic will be ignored	As above	As above	Catastrophic		As above

[8] For DMI function failures, the SIL4 safety is expected to be built up by an entry+validation process, as in the case of e.g. train data entry.

6.1.3 Notes

6.1.3.1 Notes of ENG RULE 1: The rule says that the setting of a VBC marker needs to follow a safe process. This could be perceived as redundant to the general rule in SUBSET-091 called EXT_SR01 that requires the preparation of the ETCS Trackside Data to be of a quality that is appropriate to the required safety level. However, in a construction area the data (e.g. balise telegrams) is not commissioned and can therefore not be expected to have gone through all safety processes. Even so, safety reliance is placed on balise telegrams in the construction area; therefore ENG RULE 1 is necessary.

6.1.3.2 Notes on OP RULE 1 and 2:

- The use of the VBC function requires the driver to validate that ERTMS/ETCS on-board has the correct set of VBCs in many operational situations, at least connected to the technical procedure Start of Mission inside a LUC. In some of these situations it is clear that the validation is not merely a double check of a list that should already be valid, but that the driver will be expected to actually correct the set of VBCs (if not using VBC orders from balises at all, the driver will need to enter the VBC codes even more frequently). The effect of a failure to do so correctly might have catastrophic consequences. Therefore, the operational procedure which shall guarantee that the driver can take this responsibility must be elaborated with great care, taking into account the aspects of human failures given the ergonomics of the VBC set and remove function specified in ERA_ERTMS_015560 “ERTMS/ETCS, ETCS Driver Machine Interface”.
- It needs to be made sure that the timer is restarted when the driver checks the VBC. Therefore, OP RULE 1 must contain the instruction to go through the set and validation procedure for each VBC that is required for operation in the LUC.

6.1.3.3 Notes on ERTMS/ETCS on-board timer function:

- The timer related to the VBC function shall be active also when ERTMS/ETCS on-board is powered off. This implies that ERTMS/ETCS on-board must make itself reliant upon external sources of time, most likely with unknown safety properties. The timer at power off shall therefore not be considered as a safety function but must be mitigated with external barriers; see further cases B.2.2.2.3.x.

6.1.3.4 For the case of erroneously releasing a VBC timer while running inside a LUC, there are no operational mitigations. The driver will not be given any warning on the DMI if a VBC timer expires, but the ERTMS/ETCS on-board will simply start processing the balise telegrams that should have been ignored in the LUC. However, it is believed that the time at risk for such an event will be limited since the train will at some point in time go outside the LUC. Therefore, any accuracy and safety requirements imposed by this scenario will highly likely be bounded by accuracy and safety requirements imposed by other scenarios involving the ERTMS/ETCS on-board clock with ERTMS/ETCS on-board powered, e.g. MA timer.

7. TRANSMISSION CHANNEL EVENTS

7.1.1.1 Each TRANS-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 Part 3.

8. GRAPHICAL REPRESENTATION OF HAZARDOUS EVENTS

8.1.1.1 The figure below illustrates the hazardous events of section 6 in relation to the ERTMS/ETCS UNISIG Reference Architecture.