



ERTMS/ETCS - Class 1

ETCS Application Level 2 - Safety Analysis

Part 2 - Functional Analysis

REF : SUBSET-088-2 Part 2

ISSUE : 2.3.0

DATE : 02-04-08

Company	Technical Approval	Management approval
ALSTOM		
ANSALDO		
BOMBARDIER		
INVENSYS		
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. TABLE OF CONTENTS

1. MODIFICATION HISTORY.....	2
2. TABLE OF CONTENTS.....	5
3. INTRODUCTION.....	6
4. DESCRIPTION.....	7
5. INTEROPERABILITY CONSIDERATIONS FOR ETCS	9
6. FUNCTIONAL ANALYSIS.....	11
7. TRANSMISSION CHANNEL EVENTS.....	40
7.1 General.....	40
8. SUMMARY OF EVENTS CONSIDERED.....	41



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 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 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 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 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 location 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.

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

4.1.1.9

<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 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 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 core hazard.

4.1.1.10 The criticality is assigned prior to claiming mitigating conditions.

4.1.1.11 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 Location Determination:

To ensure that the ETCS onboard system is able to determine its speed and location, 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 location 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)
- MMI (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

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating 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	Failure of the engineering data processing and installation procedures are outside the scope of this study
ENG 1 b	Incorrect data to trackside constituents from engineering process	<u>Radio Data.</u> MA Data, System Data, Linking data from trackside	Incorrect data preparation for a specific scheme	All	Safety Critical	Failure of the engineering data processing is outside the scope of this study
ENG-2	Incorrect data to onboard from engineering process for a mission	Train Data	Incorrect data preparation for a specific scheme	All	Safety Critical	Failure of the engineering data processing is outside the scope of this study
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 Failure of the engineering data processing is outside the scope of this study
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

© 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	Criticality	Mitigating Conditions
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	Failure of the engineering data processing is outside the scope of this study.
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 occur only in case of emergency, 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	Safety Related	Driver must go against indicated safe limits. Protected by supervision function of both speed and distance.
			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	Safety Critical	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.
DRV-1 Continued				OS	Safety Critical	In OS there is reduced protection, however the train speed and limited distance are supervised by the Dynamic Speed Profile.

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
DRV-2	Incorrect Driver input of SR speed, override EoA	MRSP, DSP leading to incorrect supervision	Driver inputs unsafe SR speed or distance. Driver overrides EOA when not allowed	SR	Safety Related	Prevailing conditions are such that the driver can drive safely at the excessive speed. SR mode is not the main mode of operation. Data entry procedures
					Safety Critical	For override EOA, specific conditions must exist for the facility to be invoked. Use of EOA is usually subject to Authorisation by trackside personnel, however if the driver decides to select the function, ETCS provides no protection Train speed must be below the National limit for Override EOA
DRV-3	Incorrect train data entered by driver	Train Data	The driver inputs incorrect train data into the MMI.	All	Criticality depends on the data.	Potentially dangerous train data input into ETCS must be accepted as valid.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating 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	Safety Critical	Driver vigilance can be claimed in noticing that the train is failing to tilt on bends. The data entry procedure protects 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	Safety Related	Due to acceleration performance of trains only a significant error in length would cause rear end overspeeding. The data entry procedure protects 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) protects against the clearing of points, and collision hazards.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
DRV-3 (Continued)			Deceleration rate - The supervision function will be incorrect and the train will fail to apply safe breaking curves	All	Safety Critical	The parameter entered must be an overestimate of the trains braking capability. Driver vigilance. Data entry procedure.
DRV-3 (Continued)			Maximum Permitted Speed - The driver inputs a maximum train speed in excess of that permitted for the train.	All	Safety Related	Driver vigilance Data entry procedure Needs to be significant error to result in hazard Unlikely to be a problem for high speed trains Line speed profile in FS
			Loading Gauge and Axle Load - Entry of incorrect parameters for the High speed network	All	Safety Critical	Data entry procedure
			Power Supply	All	Not a Safety Function	Data entry procedure
			Train Running Number - Operational data only, not safety related.	All	Not a Safety Function	Driver vigilance Data entry procedure In addition, the ETCS has its own unique identification number



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
DRV-4	Incorrect additional data as part of driver input	Train Data	The driver inputs incorrect additional data into the MMI. Driver ID, ETCS Level, RBC ID/ Telephone No or Adhesion Factor.	All	Criticality depends on the data	In all cases, Driver acknowledgement of data. Driver vigilance in operational conditions Data entry procedures
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	Safety Related	Driver vigilance and start-up procedures. 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. In degrade situations mitigation is that the driver does not have to input the level.
			ETCS Level - During cold start-up the location will not be known and therefore conflict could exist	All	Safety Related	Driver vigilance, ETCS start-up procedures On passing the first balise group the location will be known



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
			RBC ID/Telephone Number - System acquires an incorrect RBC Number	All	<p>Safety Related</p> <p>Safety Related</p>	<p>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.</p> <p>During a cold start-up, the onboard does not know its location or RBC area. An incorrect RBC could be contacted.</p> <p>For an MA to be provided to the train, the train has to provide a position report.</p>
DRV-4 (Continued)			<p>Adhesion Factor - 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	Driver vigilance



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
DRV-5	Incorrect driver input (Override or non-leading, Override route suitability etc.)	Current Mode of Operation	Driver inputs unsafe information	Mode Specific	Safety Critical	Operating Rules Transition table conditions have to be fulfilled in order to allow some mode changes
MMI-1a	False acknowledgement of mode change from Full Supervision	Current Mode of Operation	The MMI erroneously gives acknowledgement to Kernel with the consequence of entry to SR, SH or OS modes without driver knowledge	FS, OS	Safety Critical	Driver vigilance. ETCS mode transition table must be fulfilled (SRS ch 4.6.2)
MMI-1b	False command to enter Non-leading mode	Current Mode of Operation	At standstill, MMI erroneously issues command for entry to Non-leading. Rollaway protection is removed, brakes isolated and MMI screen still displays many items of FS/OS modes.	SB, SH, FS, SR, OS	Safety Critical	Driver vigilance. Note that display is active to permit driving in Non-leading. Only possible to select Non-leading during standstill.
MMI-1c	False command of Override EoA request		The MMI issues the command requesting passing of signal at danger without driver intending to do so.	FS, OS, SR	Safety Related	Driver vigilance. Procedures for Override EoA must be fulfilled (SRS ch 5.8)
MMI-1d	False acknowledgement of Level Transition	Current Level of Operation	The MMI erroneously gives acknowledgement to Kernel with the consequence avoid or release service brake	FS, OS	Safety Related	Driver vigilance. Procedures for Level Transitions must be fulfilled (SRS ch 5.10) ETCS mode transition table must be fulfilled (SRS ch 4.6.2)

© 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	Criticality	Mitigating Conditions
MMI-1e	False acknowledgement of Train Trip	Safe speed and distance as known by ETCS		TR	Safety Related	Driver vigilance. ETCS mode transition table must be fulfilled (SRS ch 4.6.2).
MMI-1f	False acknowledgement 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 MMI sends a false track ahead free to the on-board kernel	SB, SR, OS, PT	Safety Critical	Driver vigilance. There needs to be an obstacle in front of the train for the situation to be dangerous.
MMI-2a (Break out from MMI-2)	False presentation of speed or distance on the MMI	Information to driver	False presentation of the data on the MMI, relative to the data understood by the Kernel - Display of too low actual speed - Display of too long distance to go - Display of too high permitted speed	FS	Safety Related	Driver vigilance. Very specific MMI failure modes required providing consistently dangerous but seemingly correct data. Fully Protected by Onboard Supervision and monitoring
				Other modes than FS	See DRV-1	See DRV-1



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
MMI-2b (Break out from MMI-2)	False presentation of mode on the MMI	Information to driver	False presentation of the data on the MMI, relative to the data understood by the Kernel - Display of mode that is of higher level of ETCS responsibility than is actually in operation.	Mode Specific	Safety Critical	Driver vigilance
MMI-3	Falsification of driver's train data input	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 input of data procedure, being supplier specific.
MMI-4	Frozen or delayed MMI display	Information to driver	MMI fails to update information in a timely manner due to a frozen or delayed display.	All	Safety Related	Driver vigilance A frozen display would only be an issue in SR & OS. However the train maximum speed is limited and supervised by the onboard Acknowledgement by the driver is required every time there is a change of mode.
ODO-1	Incorrect standstill indication	Standstill Indication	Indicates Standstill when in motion	All	Safety Critical	Driver Vigilance Detected upon passing a balise.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
ODO-2	Speed measurement underestimates trains actual speed	Determination of distance travelled, determination of train location relative to LRBG Position reporting, Provision of MA. Common mode error as it affects both the supervision and the display to the driver	If the speed is underestimated then the distance travelled will also be underestimated.	All	Safety Critical	In SR the train speed will be low (fixed national value) thus allowing time for driver vigilance. Driver is responsible for the movements of the train, therefore should be able to maintain it within a safe speed.
ODO-3	Incorrect actual physical speed direction	Determination of train location relative to LRBG	Incorrect train location leading to violation of MA	All	Safety Related	When going in the wrong direction, the given MA direction will give no protection if ODO-3 happens. However, the error will be discovered when the first expected balise group is not detected, if linking is used.

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
ODO-4	Distance measurement is incorrect	Position Reports, Information to driver. Incorrect determination of speed and location.	<p>Incorrect determination of location resulting in erroneous position reports to the trackside such that the RBC provides a dangerous MA.</p> <p>Underestimated location could result in a train exceeding its MA or failing to reduce speed for a speed restriction.</p> <p>Over-estimation of location could result in a premature acceleration from a speed restriction</p> <p>In level 3 over estimation of location determination is an issue.</p>	All	Safety Critical	<p>If linking is used, on passing the 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)</p> <p>There is a time at risk when, 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. Although safety requirements for odometry errors are defined, no maximum distance between balise groups is defined.</p> <p>NB The interlocking should prevent trains occupying the same block.</p>
				SR		<p>In SR the train speed will be low (fixed national value) thus allowing time for driver vigilance.</p> <p>Driver is responsible for the movements of the train, therefore should be able to maintain it within safe distance.</p>



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
KERNEL-1	Balise linking consistency checking failure	Linking reaction	Balise linking consistency is a protective function against linking rules violation.	FS, OS	Safety Related	There has to be another coincident failure for this to result in the core hazard. There will be a time at risk when linking reaction is required.
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)	Safety Related	There has to be another coincident failure for this to result in the core hazard. Safety related balise transmission function.
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	
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)	Safety Related	This function is an inherent protective function of ETCS Message acknowledgement



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
KERNEL-5	Radio link supervision function failure	Provision of Data to onboard (MA etc)	<p>Radio link supervision is a protective function against receiving the latest valid message later than a specified time.</p> <p>Failure to correctly manage a communication session could result in the loss of communications and a failure to receive more restrictive route information.</p> <p>Driver could switch to a lower level (1, STM)</p>	FS, OS	Safety Related	This function is an inherent protective function of ETCS (Linking reaction, T_NVCONTACT)
KERNEL-6	Manage communication session failure	Provision of Data to onboard (MA etc)	<p>Failure to correctly manage a communication session results in the loss of communications and a failure to receive more restrictive route information.</p> <p>Driver could switch to a lower level (1, STM)</p>	FS, OS	Safety Related	



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
KERNEL-7	Incorrect LRBG	Determination of train location 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)	Safety Critical	No mitigation afforded, this is an inherent core function of ETCS.
KERNEL-8	Emergency Message Acknowledgement Failure	Emergency stop failure	Onboard acknowledges receipt of message but does not take it into account	FS,OS, SR, PT	Safety Related	This is an inherent core function of ETCS
KERNEL-9	Speed calculation underestimates train speed	Determination of speed / location	As for ODO-2	All (except NP ,SF,IS)	Safety Critical	This is an inherent core function of ETCS
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)	Safety Related	Driver acknowledgement is required to release brakes.
KERNEL-11	Incorrect traction/braking model (e.g. brake use restrictions)	Dynamic Speed Profile	This is an inherent core function of ETCS	FS, OS, SE	Safety Critical	This is an inherent core function of ETCS
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	

© 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	Criticality	Mitigating Conditions
KERNEL-14	Failure of reverse movement protection	Protection against undesired movements	This is a protective function performed by ETCS	FS,SR, OS,PT, SE,RV	Safety Critical	
KERNEL-15	Incorrect cab status (TIU failure)	Determination of train location 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)	Safety Critical	Interlocking track occupancy protection Operational rules Reverse movement protection MA directionality points in the allowed direction
KERNEL-16	Incorrect train status TIU sleeping/cab status	Current Mode of Operation Standstill protection (KERNEL-12)	Detects sleeping	All	Safety Critical	ETCS mode transition table must be fulfilled (SRS ch 4.6.2)
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)	Safety Critical	This is an inherent core function of ETCS
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	Safety Related	Onboard has current valid MA Maximum time between radio communications, T_NVCONTACT



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
KERNEL-19	Failure of train trip supervision in OS and FS	Supervision of EoA / LoA	Failure of train trip monitoring, unable to trip on demand	FS, OS	Safety Critical	Inherent protective function of ETCS
KERNEL-20	Failure of train trip supervision, shunting and SR	Supervision of train trip.	Failure of train trip monitoring	SH, SR	Safety Critical	Inherent protective function of ETCS
KERNEL-21	Incorrect supervision of stop in SR	Supervision of EoA / LoA	Failure of train trip monitoring	SR	Safety Critical	Inherent protective function of ETCS
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, SE	Safety Critical	This is a safety critical function of ETCS that cannot be mitigated against



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating 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 location 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 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	In Level 2, protection will be provided by the interlocking and associated train detection methods
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	Safety Critical	Inherent protective function of ETCS

© 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	Criticality	Mitigating Conditions
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, OS,SR, UN,RV	Safety Critical	Inherent Safety function of ETCS
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	Safety Critical	Inherent core function of ETCS
KERNEL-28	Incorrect confidence interval	Determination of distance travelled Determination of train location 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)	Safety Critical	When passing a balise group, this will (if the error is sufficiently large) be found outside the expectation window, which will prompt activation of the link reaction.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
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	Safety Related	Core Function of ETCS
KERNEL-30	Incorrect shortening of MA	Supervision of EOA/LOA	Onboard applies insufficient shortening of MA	FS, OS	Safety Critical	Core Function of ETCS
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	Safety Critical	Core Function of ETCS
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	Safety Critical	Core Function of ETCS
TI-1	Service brake / emergency brake not commanded when required	Brake control function	Unable to apply brakes on demand.	All (except IS)	Safety Critical	None

© 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	Criticality	Mitigating 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 driver initiated
TI-3	Inappropriate sleeping request	Standstill protection	Inappropriate entry to Sleeping, with loss of Standstill protection as a consequence.	SB	Safety Critical	Cabin must be closed (see TI-6a) and the train must be at standstill. Driver vigilance
TI-4	Incorrect brake status (TIU failure)	Information to driver	Unsafe information to driver Brakes indicated ON when OFF	All	Safety Related	Driver vigilance
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: <ul style="list-style-type: none"> Rollaway protection changes direction. In case Dir Ctrl position reported as forward/backward instead of neutral: <ul style="list-style-type: none"> Loss of Rollaway protection in one direction. 	All	Safety Critical	Driver vigilance



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
TI-6a (Break out from TI-6)	Loss of Cabin Active signal	Standstill protection	The active Cabin is deactivated by a TI-failure resulting in an inappropriate entry to Sleeping, with a loss of Standstill protection as a consequence.	SB	Safety Critical	Sleeping must be requested (see TI-3) and the train must be at standstill. Driver vigilance.
TI-6b (Break out from TI-6)	Wrong Cabin considered as Active	See KERNEL-15	See KERNEL-15	All	See KERNEL-15	See KERNEL-15



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 the how erroneous data can lead to the 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 which 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 into that level of detail.</p>
TRACK- 2	Incorrect Adhesion Factor	DSP	Trackside functionality not currently implemented. 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	Criticality	Mitigating 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	Safety Critical	Message consistency check.
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	Safety Critical	<p>If only one balise is missed, consistency checking is mitigation.</p> <p>If all balises in a group are missed, linking is mitigation.</p> <p>The criticality of this failure is dependent upon the information missed within the unlinked balise group.</p> <p>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.</p>
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	Safety Critical	<p>Message consistency check.</p> <p>Balise group linking.</p>



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
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	Safety Critical	Message consistency check has to fail. Messages are key coded to ensure authenticity and contain a timestamp to check sequencing and delay. 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.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
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.)	Deletion in the communications channel resulting in the on-board being unable to receive a more restrictive MA	All	Safety Critical	<p>Train should still be within its current MA and can only be shortened via co-operative MA shortening. In addition an MA may be shortened by an emergency message, in this case, mitigation is provided by the link supervision.</p> <p>Radio Link supervision ensures messages are received no later than a specified time (T_NVCONTACT)</p> <p>T_NVCONTACT should be limited to a safe default value defined by each railway.</p> <p>Section timeouts will also provide mitigation.</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>
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	Safety critical	<p>Message sequencing, time stamping and addressing as recommended by Cenelec 50159-2 render this event as non hazardous</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	Criticality	Mitigating Conditions
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	Safety Critical	Message consistency check has to fail. Messages are key coded to ensure authenticity and time stamped as per Cenelec 50129-2 to check sequence and delay.
TRANS-TS/RADIO-2	Radio message not received by the RBC Kernel functions (Deletion)		Loss of train reports and / or message acknowledgements	All	Safety Critical	Train retains existing MA. Protection is afforded at the application level with transmission repeats. This event is not hazardous.
TRANS-TS/RADIO-3	Inserted radio message received by the RBC kernel functions as consistent. (Insertion)			All		Message sequencing, time stamping and addressing as recommended by Cenelec 50159-2 render this event as non hazardous
LEU-H4	Transmission of an erroneous telegram / telegrams interpretable as correct, due to failure within the LEU function	Provision of Data to onboard (balise message)	Corruption of balise group message	All	Safety Critical	Message consistency check.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
RBC-1	Radio message deleted in the RBC Kernel in an undetectable way	Provision of Data to onboard (MA data etc.)	Errors in the RBC kernel functions resulting in the on-board unable to receive a more restrictive MA	All	Safety Critical	<p>Train should still be within its current MA and can only be shortened via co-operative MA shortening. In addition an MA may be shortened by an emergency message, in this case, mitigation is provided by the link supervision.</p> <p>Radio Link supervision ensures messages are received no later than a specified time (T_NVCONTACT)</p> <p>T_NVCONTACT should be limited to a safe default value defined by each railway.</p> <p>Section timeouts will also provide mitigation.</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>



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating 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	Safety Critical	Message consistency check has to fail. Messages are key coded to ensure authenticity, Sequencing and Timestamp. 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.
RBC-3	Incorrect adjacent RBC message sent or received by the RBC kernel as consistent, causing an incorrect message to be sent to the onboard	Provision of Data to onboard (MA data etc.)	Errors in the in the kernel of the adjacent RBC kernel. Incorrect data includes corruption, late, repeated, etc.	All	Safety Critical	Message consistency check has to fail. Messages are key coded to ensure authenticity, Sequencing and Timestamp. 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.



7. TRANSMISSION CHANNEL EVENTS

7.1 General

- 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.

8. SUMMARY OF EVENTS CONSIDERED.

