



**ERTMS/ETCS - Class 1**

**ETCS Application Level 1 - Safety Analysis**

**Part 2 - Functional Analysis**

REF : SUBSET-088-1 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 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 Of 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. TABLE OF CONTENTS

1. MODIFICATION HISTORY .....	2
2. TABLE OF CONTENTS .....	4
3. INTRODUCTION .....	5
4. DESCRIPTION .....	6
5. INTEROPERABILITY CONSIDERATIONS FOR ETCS .....	8
6. FUNCTIONAL ANALYSIS .....	10
7. TRANSMISSION CHANNEL EVENTS .....	32
8. SUMMARY OF EVENTS CONSIDERED .....	33



### **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 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 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 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 (onboard 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 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 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

<b><i>Assigned Criticality of Base Event</i></b>	<b><i>Interpretation of the Assignment</i></b>
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.

4.1.1.9 The criticality is assigned prior to claiming mitigating conditions.

4.1.1.10 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, 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 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 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

Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating 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 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-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	Failure of the engineering data processing is outside the scope of this study
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)	FS	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

© 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-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	Failure of the engineering data processing is outside the scope of this study.
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). 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 balise containing MA information with V_MAIN=0
				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.  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, or Adhesion Factor.	All	Criticality depends on the data	In all cases, Driver acknowledgement of data. Driver vigilance in operational conditions Data entry procedures
			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
DRV-4 (Continued)			Adhesion Factor - 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.	All	Safety Critical	Driver vigilance
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)





Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
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)
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).



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
MMI-2a (Break out of 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 <ul style="list-style-type: none"> <li>- Display of too low actual speed</li> <li>- Display of too long distance to go</li> <li>- Display of too high permitted speed</li> </ul>	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
MMI-2b (Break out of 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 <ul style="list-style-type: none"> <li>- Display of mode that is of higher level of ETCS responsibility than is actually in operation.</li> </ul>	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.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
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.
ODO-2	Speed measurement underestimates trains actual speed	Determination of distance travelled, determination of train location 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	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.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
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.
ODO-4	Distance measurement is incorrect	Position Report (only in FS when infill radio is used), Information to driver. Incorrect determination of speed and location. Underestimation of location result in the train exceeding its MA or failing to reduce speed for a speed restriction Over estimation of location could result in a premature acceleration from a speed restriction.	Location determination Position reporting underestimated resulting in train exceeding its MA  In level 3 over-estimation of location determination is an issue.	All	Safety Critical	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)  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 group is defined.  Nb The interlocking should prevent trains occupying the same block.



Fault Tree Base Event	Fault Tree Base Event Description	Affected ETCS Functions or Data	Explanation	Mode	Criticality	Mitigating Conditions
				SR		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 safe distance.
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.) with radio infill	Radio message correctness check is a protective function against the receipt of inconsistent messages	All (except NP,SF,I S)	Safety Related	None
KERNEL-4	Radio sequencing checking failure	Provision of Data to onboard (MA etc) with radio infill	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) 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	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) with radio infill	Failure to correctly manage a communication session results in the loss of communications and a failure to receive more restrictive route information.	FS, OS	Safety Related	
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 RIU, 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.

© 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-9	Speed calculation underestimates train speed	Determination of speed	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	
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 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 MA directionality points in the allowed direction

© 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-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-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-24	Failure of message acknowledgement	Provision of Data to onboard	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	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-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-32	Failure of Loop message consistency checking	Provision of Data to onboard (loop message)	Loop group message consistency checking is a protective function against the receipt of inconsistent messages	FS	Safety Related	There has to be another coincident failure for this to result in the core hazard. Safety related loop transmission function.
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 and/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



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 (except NP, SL, NL, SF, IS)	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"> <li>Rollaway protection changes direction.</li> </ul> In case Dir Ctrl position reported as forward/backward instead of neutral: 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 of 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 of TI-6)	Wrong Cabin considered as Active	See KERNEL-15	See KERNEL-15	All	See KERNEL-15	See KERNEL-15
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, Loop or Radio) that could be responsible for the failure.</p>		
TRACK- 2	Incorrect Adhesion Factor	DSP	Trackside functionality not currently implemented. Trackside equipment failure.	<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>		

© 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
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 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			
TRANS-BALISE-1  (was TRANS-1)	Incorrect balise group message received by the on-board Kernel functions as consistent	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
TRANS-BALISE-2 (was TRANS-2)	Balise group not detected by on-board Kernel functions	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 the on-board Kernel functions as consistent	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>
TRANS-OB/RADIO-1 (was TRANS-4)	Incorrect radio message received by the on-board Kernel functions as consistent	Provision of Data to onboard (MA data etc.) with infill radio	Incorrect data includes corruption, late, repeated, etc.	FS	Safety Critical	<p>Message consistency check has to fail.</p> <p>Messages are key coded to ensure authenticity and contain a Timestamp to check sequencing and delay.</p>



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

© This document has been developed and released by UNISIG



## **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. SUMMARY OF EVENTS CONSIDERED

