



ERTMS/ETCS - Class 1

ETCS Application Levels 1 & 2 - Safety Analysis

Part 3 - THR Apportionment

REF : SUBSET-088 Part 3

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 2	WLH
0.1.3. 20-08-01	All	Draft Issue	S. Adomeit
0.1.4. 24-08-01	All	Revised after discussion and/or comments	S. Adomeit
0.1.5. 07-09-01	All	Revised after comments	S. Adomeit
0.1.6. 14-09-01	All	Revised after RAMS meeting	S. Adomeit
0.1.7. 27-09-01	All	Revised during meeting	S. Adomeit
0.1.8. 29-09-01	All	Revised after meeting Chapter 5, 6 7	S. Adomeit
0.2.0. 01-10-01	All	Raised in issue for release to Esrog	WLH
0.2.1. 27-10-01	All	Value Apportionment Revise Mission Profile Comments	S.Adomeit WLH G. McGuire
0.2.2. 02-11-01	All	Revised after Comments	S.Adomeit
0.2.3. 14-01-02	All	Restructured	W L H
0.2.4	All	Prepared for online revising at	S. Adomeit

18-01-02		RAMS meeting	
0.2.5 20-01-02	All	Revised at RAMS meeting	S. Adomeit
0.2.6 26-01-02	All	Prepared for online revising at RAMS meeting	S. Adomeit
0.2.7 31-01-02	All	Revised at RAMS meeting	S. Adomeit
0.2.8 05-02-02	All	Revised according comments	S. Adomeit
0.2.9 07-02-02	All	Revised at RAMS meeting	S. Adomeit
0.3.0 12-02-02	All	Revised according comments	S. Adomeit
0.3.1 19-02-02	All	Rationalisation. Comments added at 4.1, 4.2, 4.5,	WLH
2.0.0. 26-02-02		Comments from Ansaldo and Siemens. Raised in issue for release to the EEIG	WLH
2.0.1 06-11-02		Summary of Hazardous events from Part 2 added at section 4. Update of system mitigations at section 5.4	WLH
2.0.2 10-12-02		Updated in line with review comments from Alcatel, Ansaldo, Bombardier and Siemens	WLH
2.0.3. 15-01-03		Updated in line comments from review meeting of 14-01-03 TRANS events rationalised Implications of 2 balise groups for TSRs examined	WLH
2.0.4 26-01-03		Editorial changes following comments from Ansaldo, Bombardier and Siemens	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	WLH



		report from the ISA's version 1.1 dated 07-03-03 as proposed via the Unisig consolidated review comments on the ISA report v0.0.2 March 03.	
2.2.3 07-07-05		Changes due to consolidation of SUBSET-091	S. Adomeit
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	7
4. SUMMARY OF HAZARDOUS EVENTS	8
5. MISSION PROFILE AND RELATED ASSUMPTIONS	11
5.1 Format of the Mission Profile	11
5.2 The Reference Infrastructure	11
5.3 Operational Parameters	13
5.4 System Mitigations	14
5.5 Operational Assumptions	16
5.6 Special Functions	18
6. APPORTIONMENT	19
6.1 Principles of Apportionment	19
6.2 Transmission Considerations	21
7. SAFETY REQUIREMENTS FOR THE ON-BOARD FUNCTIONS	26
7.1 Allocations to the ETCS Onboard Constituent	26
7.2 Considerations for Elements External to the On-board	26
7.3 Apportioned Target	30
8. SAFETY REQUIREMENTS FOR THE ETCS TRACKSIDE FUNCTIONS	31
8.1 Allocations to ETCS Trackside Constituents	31
8.2 Considerations for Elements External to the Trackside ETCS	31
8.3 Apportioned Target	33
9. SAFETY REQUIREMENTS FOR THE TRANSMISSION FUNCTIONS	34
9.1 Apportionment between the On-board and Trackside for the Radio, the Balise and Loop Subsystems	34
9.2 Assessment of the Radio Transmission Subsystem	35
9.3 General Considerations Relating to the Radio Transmission System	36
9.4 Summary of Hazardous Events	38
10. CONCLUSIONS	42
10.1 General Conclusions	42
10.2 Conclusions Relating to the Derived Balise Targets	43
11. SENSITIVITY ANALYSIS	46
11.1 Scope of the Sensitivity Analysis	46
11.2 Review of operational Scenarios	46



11.3	Insertion (TRANS-BALISE-3)	49
12.	SUMMARY OF THE SAFETY REQUIREMENTS FOR ETCS.....	50
12.1	Introduction.....	50
12.2	General Design Requirements	50
12.3	Safety Requirements for the On-board Subsystem	50
12.4	Safety Requirements for the Trackside Subsystem	51
12.5	Safety requirements for the Transmission Subsystems	52
12.6	Safety Requirements for External Entities	53
13.	ANNEX A.....	55

3. INTRODUCTION

- 3.1.1.1 Part 3 of this set of documents apportions the approved Tolerable Hazard Rate for technical failures of ETCS (THR_{ETCS}) to the grouping of constituents permitted by the Control Command technical standard for Interoperability.
- 3.1.1.2 This apportionment is undertaken against a mission profile that has been agreed with representatives of the European Railway Authorities. This done in order to determine realistic exposure times that a passenger on a train might experience in the defined one-hour journey.
- 3.1.1.3 The apportionment is taken to a point define the maximum tolerable hazard rates required to ensure technical interoperability whilst leaving freedom for an implementation that best suits a suppliers expertise and technology base.
- 3.1.1.4 The requirement for each constituent grouping is considered in isolation on the assumption that other constituent groupings are working correctly, that ETCS is deployed in accordance with the Unisig Dimensioning and Engineering Rules (subset 040, version 2.0.0.) and that all external inputs to ETCS are correct.
- 3.1.1.5 The requirements for each constituent grouping are completed by specific considerations for better understanding and further analysis.
- 3.1.1.6 As targets for the design of equipment are derived from the Mission Profile and therefore, the mission profile itself is considered as a safety requirement of ETCS. The mission profile adopted is related to a high-speed application as well as conventional applications.
- 3.1.1.7 Application specific mission profile parameters that are outside of the defined reference mission profile will require additional safety analysis to ensure that the application of equipment that is designed to meet the targets derived herein will not compromise the safety of the travelling public.
- 3.1.1.8 As this is the final document in the analysis of ETCS, it concludes with a summary of the preliminary safety requirements as derived in all parts of Subset 088. These requirements are preliminary, as the European Railways Users Group has not verified the operational assumptions.

4. SUMMARY OF HAZARDOUS EVENTS

4.1.1.1 In the functional analyses for level 1 and level 2 contained in Subset 088 Level 1, Part 2 and Subset 088 Level 2, part 2 a series of ETCS hazardous events that may occur within the previously defined boundary for ETCS have been defined. They are summarised here for convenience.

Event Id.	Event Description
MMI-1a	False acknowledgement of mode change from Full Supervision
MMI-1b	False command to enter Non-leading mode
MMI-1c	False command of Override EoA request
MMI-1d	False acknowledgement of Level Transition
MMI-1e	False acknowledgement of Train Trip
MMI-1f	False acknowledgement of Track Ahead Free
MMI-2a	False presentation of speed or distance on the MMI
MMI-2b	False presentation of mode on the MMI
MMI-3	Falsification of driver's train data input
MMI-4	Frozen or delayed MMI display
ODO-1	Incorrect standstill indication
ODO-2	Speed measurement underestimates trains actual speed
ODO-3	Incorrect actual physical speed direction
ODO-4	Distance measurement is incorrect
KERNEL-1	Balise linking consistency checking failure
KERNEL-2	Balise group message consistency checking failure
KERNEL-3	Failure of radio message consistency check
KERNEL-4	Radio sequencing checking failure
KERNEL-5	Radio link supervision function failure
KERNEL-6	Manage communication session failure
KERNEL-7	Incorrect LRBG
KERNEL-8	Emergency Message Acknowledgement Failure
KERNEL-9	Speed calculation underestimates train speed
KERNEL-10	Functional failure of standstill detection
KERNEL-11	Incorrect traction/braking model (e.g. brake use restrictions)
KERNEL-12	Failure of standstill supervision
KERNEL-13	Failure of backward distance monitoring
KERNEL-14	Failure of reverse movement protection
KERNEL-15	Incorrect cab status (TIU failure)



Event Id.	Event Description
KERNEL-16	Incorrect train status TIU sleeping/cab status
KERNEL-17	Wrong Acceptance of MA
KERNEL-18	Failure to manage RBC/RBC handover
KERNEL-19	Failure of train trip supervision in OS and FS
KERNEL-20	Failure of train trip supervision, shunting and SR
KERNEL-21	Incorrect supervision of stop in SR
KERNEL-22	Incorrect current EoA
KERNEL-23	Incorrect train position / train data sent from on-board to trackside
KERNEL-24	Failure of message acknowledgement
KERNEL-25	Incorrect traction/braking model (Acceleration only)
KERNEL-26	Deleted
KERNEL-27	Incorrect System Data (e.g. current level)
KERNEL-28	Incorrect confidence interval
KERNEL-29	Failure to shorten MA
KERNEL-30	Incorrect shortening of MA
KERNEL-31	Deleted
KERNEL-32	Failure of loop message consistency checking
KERNEL-33	Wrong processing of MA information
KERNEL-34	Incorrect supervision of MA time-outs (sections and overlaps)
TI-1	Service brake / emergency brake not commanded when required
TI-2	Service brake / emergency brake release commanded when not required
TI-3	Inappropriate sleeping request
TI-4	Incorrect brake status (TIU failure)
TI-5	Incorrect direction controller position report (TIU failure)
TI-6a	Loss of Cabin Active signal
TI-6b	Wrong Cabin considered as Active
TRANS-BALISE-1	Incorrect balise group message received by the on-board kernel functions as consistent
TRANS-BALISE-2	Balise group not detected by on-board kernel functions (deletion)
TRANS-BALISE-3	Inserted balise group message received the on-board kernel functions as consistent
TRANS-OB/RADIO-1	Incorrect radio message received by the on-board kernel functions as consistent
TRANS-OB/RADIO-2	Radio message not received by the on-board kernel functions
TRANS-TS/RADIO-1	Incorrect on-board radio message received by RBC kernel functions as consistent



Event Id.	Event Description
TRANS-LOOP-1	Incorrect loop message received by the on-board kernel functions as consistent.
TRANS-LOOP-3	Inserted loop message received by the on-board kernel functions as consistent
LEU-H4	Transmission of an erroneous telegram / telegrams interpretable as correct, due to failure within the LEU function
RIU-2	Incorrect RIU radio message received by the on-board kernel functions as consistent (Same hazardous event as TRANS-OB/RADIO-1)
RBC-1	Radio message deleted in the RBC kernel in an undetectable way
RBC-2	Incorrect RBC radio message sent from the RBC kernel functions, such that the message appears consistent.
RBC-3	Incorrect adjacent RBC message sent or received by the RBC kernel functions as correct, causing an incorrect message to be sent to the ETCS on-board.

5. MISSION PROFILE AND RELATED ASSUMPTIONS

5.1 Format of the Mission Profile

- 5.1.1.1 The term “mission profile” is defined in EN 50126.
- 5.1.1.2 For the apportionment of the THR_{ETCS} it is necessary to define a complete mission profile against which the exposure of a passenger to defined hazards can be assessed.
- 5.1.1.3 The mission profile consists of two parts as follows
- The Reference Infrastructure
 - The Operational Parameters
- 5.1.1.4 The details are based on the experience gained from the several pilot lines underway in Europe whilst taking into account the application of ETCS to a conventional railway.

5.2 The Reference Infrastructure

- 5.2.1.1 This section defines a reference infrastructure, representing average physical and operational characteristics of the railway network, to which the interoperability Directive applies.
- 5.2.1.2 Not all parameters are used in the apportionment process. An asterisk (*) denotes those parameters that are used.
- 5.2.1.3 Note A: The technical procedure “Start of Mission” is initiated by the 3 different operational scenarios with their respective frequency as indicated below. These are assumed to equate to 2 Start of Mission / hour, see Annex A 6.6.1.2.

Reference Number	Parameter description	Value	
		For (*) see paragraph 5.2.1.2	
		High-speed Rail	Conventional Rail
5.2.1.4	Length of the line	260 km	80 km
5.2.1.5	Number of Radio Block Centres	3 h ⁻¹	1 h ⁻¹

Reference Number	Parameter description	Value	
		For (*) see paragraph 5.2.1.2	
		High-speed Rail	Conventional Rail
5.2.1.6	Number of station (general) and/or stopping points, see Note B	25 h ⁻¹	25 h ⁻¹
5.2.1.7	Number of stations (stations where Start of Mission is implied due to awakening of the train), see Note A.	1 h ⁻¹ (*)	2 h ⁻¹ (*)
5.2.1.8	Number of changes in direction of travel (where Start of Mission is implied), see Note A.	1 h ⁻¹ (*)	2 h ⁻¹ (*)
5.2.1.9	Number of tunnels	10 h ⁻¹	3 h ⁻¹
5.2.1.10	Number of trains on the line	15 h ⁻¹	15 h ⁻¹
5.2.1.11	Number of Signals (0 possible for level 2)	0-200 h ⁻¹	0-50 h ⁻¹
5.2.1.12	Maximum distances between Balise groups	2.5 km	2.5 km
5.2.1.13	% of journey with the maximum distance between Balise groups	~ 10 %	~ 10 %
5.2.1.14	Number of Unlinked Balise groups (marked as Unlinked)	1 in 1000 (*)	4 in 1000 (*)
5.2.1.15	Number of Repositioning Balise groups (only Level 1)	1 in 100	1 in 100
5.2.1.16	Number of Level transitions (including STM X - STM Y transitions)	2 h ⁻¹ (*)	2 h ⁻¹ (*)
5.2.1.17	Number of temporary Shunting areas with number of border Balises	1 / 66	1 / 66
5.2.1.18	Number of fixed Shunting areas (after which Start of mission is implied), see Note A	1 h ⁻¹ (*)	1 h ⁻¹ (*)
5.2.1.19	Number of National Border transitions	1 h ⁻¹	1 h ⁻¹

5.3 Operational Parameters

5.3.1.1 This section defines operational parameter, representing average physical and operational characteristics of the railway network, to which the interoperability Directive applies.

Reference Number	Parameter description	Value	
		For (*) see paragraph 5.2.1.2	
		High-speed Rail	Conventional Rail
5.3.2	General		
5.3.2.1	Average speed of trains of the line	260 km/h	80 km/h
5.3.2.2	Max. speed of trains of the line	350 km/h	250 km/h
5.3.2.3	Frequency of balise messages	150 - 650 h ⁻¹ (*)	50 - 150 h ⁻¹ (*)
5.3.2.4	Frequency of balise messages used only for reset of confidence interval (%), thus having a link reaction marked as No Reaction.	~ 90 % (L2) (*) ~ 50 % (L1) (*)	~ 90 % (L2) (*) ~ 50 % (L1) (*)
5.3.2.5	Frequency of radio messages Track to Train	100 - 360 h ⁻¹	25 - 360 h ⁻¹
5.3.2.6	Frequency of radio messages Train to Track	100 - 650 h ⁻¹	50 - 650 h ⁻¹
5.3.2.7	Frequency of Emergency Messages (only level 2)	4*10 ⁻⁴ h ⁻¹	4*10 ⁻⁴ h ⁻¹
5.3.2.8	Number of train data entry procedure, see Note A	2 h ⁻¹ (*)	4 h ⁻¹ (*)
5.3.2.9	Number of RBC/RBC Transitions	3 h ⁻¹	1 h ⁻¹
5.3.2.10	Max. expected loss of train integrity	N/A	N/A
5.3.2.11	Mean Down time of a failed ETCS onboard balise receiver in an unfitted area	1 hour (*)	1 hour (*)
5.3.2.12	Mean down time of a non-detectable balise group. See Note C below.	24 hours (*)	24 hours (*)

5.4 System Mitigations

- 5.4.1.1 The target Tolerable Hazard rate is for Technical Failures only and therefore only a limited number of mitigations can be claimed in the derivation of the tolerable hazard rate for individual constituents.
- 5.4.1.2 Part 2 of this suite of documents derived a complete set of mitigations that would reduce either the frequency or severity of a hazard. The following table indicates those that can be claimed as mitigation against technical failures.
- 5.4.1.3 It is important in trying to achieve a balance between the technical safety of ETCS and an overall operational safety, the effect of the external events and their relationship to ETCS in minimising the effect of a hazard is discussed as part of this analysis.

Claim	ETCS Claimable Feature	Hazards
Quality of Engineering data	No	ENG-1a, 1b,, 2 & 3 EXT 2
Supervision by ETCS Onboard	Yes	DRV 1, MMI 2a (incorrect speed displayed) MMI 4 (frozen display)
Data Entry Procedure	No	DRV 2, DRV 3 (category, length, deceleration, max permitted speed, loading gauge & axle load, train running number) DRV 4
Driver vigilance	No	DRV 3 (category, deceleration, train running number) DRV 4 (ETCS level, adhesion) MMI 1a, 1b, 1c, 1d, 1e, 1f (incorrect speed displayed, frozen display, incorrect data displayed, erroneous acknowledgement) MMI 2a, 2b, 4 ODO 1, 2, 4 TI 2, 3 ,4, 5, 6a KERNEL 10
Interlocking detection of route free	No	DRV 3 (length) ODO 4 KERNEL 15

Claim	ETCS Claimable Feature	Hazards
Start of Mission Procedure	Yes	DRV 4 (ETCS level)
Mode Transition Table	Yes	DRV 5 KERNEL 16 MMI 1a, 1b, 1d, 1e, 1f
Operating Rules	No	DRV 5 KERNEL 15
Balise Linking	Yes	ODO 3, 4. TRANS-BALISE-3

Claim	ETCS Claimable Feature	Hazards
Linking reaction	Yes	KERNEL 28 TRANS-BALISE- 2
Message Consistency Checks	Yes	TRANS-BALISE-1, -2, -3 TRANS-OB/RADIO-1, -TS/RADIO-1 LEU-H4 TRANS-LOOP-1, -3 RBC 2, 3 RIU 2
Maximum distance between Balise Groups	Yes	ODO 4 KERNEL 28
Balise Groups contain at least two Balises for safety data.	Yes	TRANS-BALISE- 2
Provision of correct routes by the interlocking	No	EXT 1
Low demand for Emergency Messages	No	EXT 3
SR not the main operational	Yes	DRV 2

Claim	ETCS Claimable Feature	Hazards
mode		
Plausibility checks	Yes	DRV 3
Balise detection	Yes	ODO 1, 3
Radio message acknowledgement	Yes	KERNEL 4
Radio link time out	Yes	KERNEL 5, 18 TRANS-OB/RADIO-2 RBC 1
Supervision and protection	Yes	MMI 2a

5.4.1.4 The mitigation claims marked with Yes are based on the inherent protective features designed into ETCS and may be claimed mitigations in a supplier's specific analysis.

5.5 Operational Assumptions

5.5.1.1 This defines specific operational assumptions that are used in the subsequent analyses.

Reference Number	Parameter description	Value	
		For (*) see paragraph 5.2.1.2	
		High-speed Rail	Conventional Rail
5.5.1.2	Probability of driver failing to verify a level transition function at an ETCS border. See Rule A.	0,001 (*)	0,001 (*)
5.5.1.3	Probability of driver passing a safe authorisation when driving in SR mode. See Rule B.	0,001 (*)	0,001 (*)

5.5.1.4 Internal discussions within the analysis team revealed a wide range of possibilities for the above figures based on each member's own National experience. The figure adopted is therefore a compromise between these National views and a compromise between high speed and conventional applications



5.5.1.5 The analysis for the balise subsystem annexed to this document assumes that the following operational rules are in place. If these can not be fulfilled, the analysis must be re-evaluated:

- Rule A: It is assumed that entry of a train into a level 1 or level 2 equipped area will be controlled by a line side entry signal. It is further assumed that if there are no other optical signals in the ETCS area, this entry signal (or other suitable operational rules) is controlled to prevent an ETCS fitted train entering the area if the train is not able to successfully switch to the correct level.
- Rule B: It is assumed that in level 1 and 2 applications without line side signals that there is some external marker to indicate stopping points. Clearly such a marker will not display any aspect information. Therefore it is assumed that the driver will be authorised by operational procedures outside the scope of this document.

5.5.1.6 These assumptions cover the situations where, if the driver fails to obey information displayed by ETCS a hazardous situation could result. However, in the following analysis no assumptions are made about the vigilance of a driver acting in mitigation to technical failures.



5.6 Special Functions

- 5.6.1.1 Associated with the role of the ETCS system, there are specific additional hazards that could be identified which will not lead to an exceedance of safe speed or distance.
- 5.6.1.2 An example of such a function is handling of areas where stopping is not permitted. This does not contribute to the ETCS top hazard as it is currently defined because it is information advised to ETCS and therefore, it is not considered to be an open point and this situation is not analysed.

6. APPORTIONMENT

6.1 Principles of Apportionment

6.1.1.1 The role of the ETCS system has been defined in Part 0 as being

**To provide the driver with information to enable him to drive his train safely
and to enforce respect of this information**

Associated with this role is the top-level hazard, also defined in Part 0.

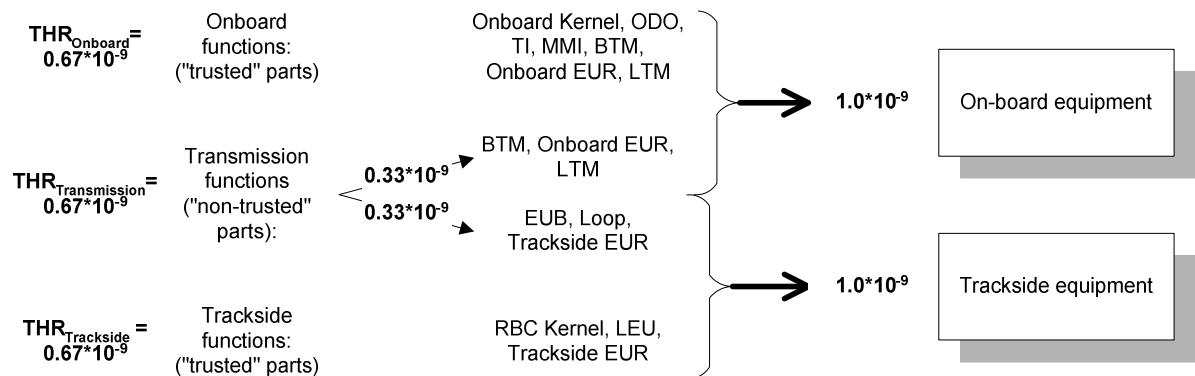
Exceedance of safe speed / distance limits as advised to ETCS

6.1.1.2 This hazard, due to technical failures, must not occur with a frequency greater than

$$2.0 * 10^{-9} \text{ hour}^{-1} \text{ train}^{-1}$$

This is known as the THR_{ETCS} .

6.1.1.3 The requirement according to the Technical Specifications for Interoperability is to allocate THR_{ETCS} equally between the on-board and the trackside equipment and allocate the system hazards as identified in Parts 1 and 2 of this document. These hazardous events are allocated as either 'on-board events', 'trackside events' or 'non-trusted transmission events', each initially obtaining 1/3 each of the THR_{ETCS} . The functions corresponding to the 'transmission events' are actually carried out by either the on-board or trackside equipment. Therefore, half of the target for the transmission events is allocated to the on-board equipment and the other half to the trackside equipment. The result is the required equal splitting between on-board and trackside equipment as shown in the figure below. The figure introduces the terms $\text{THR}_{\text{Onboard}}$ and $\text{THR}_{\text{Trackside}}$ denoting the numerical safety requirement for the purely on-board and trackside functions. Note that the infill functions are associated with the balise:



- 6.1.1.4 Apportionment of the overall THR to the constituent groupings is undertaken against a definition of the role of that constituent and its related safety hazard. The apportionment is then assessed against the exposure of a passenger to that hazard in a representative one-hour journey.
- 6.1.1.5 Occurrence of any one of the defined hazards should not lead to ETCS exceeding the THR_{ETCS}
- 6.1.1.6 In all cases, the target allocated to equipment and specific functions in order to achieve Technical Interoperability takes into consideration the operational aspects, the protective features inherent in the design of ETCS and the frequency of occurrence of operational events as dictated by the Mission Profile.

6.2 Transmission Considerations

6.2.1 Corruption of Messages

- 6.2.1.1 According to EN 50159-1¹ and -2², it is possible to protect data communications with measures that mitigate against errors inside a transmission channel whose characteristics are not completely known (non-trusted).
- 6.2.1.2 As identified in the analysis of the transmission channels, (e.g. Subset-081 - Transmission Path FMEA), it is useful to consider part of the sender and receiver functionality as belonging to the non-trusted transmission channel, according to EN 50159 indications.
- 6.2.1.3 It has been chosen to adopt this concept both for Euroradio and Eurobalise transmission, for the case of corruption of messages and of masquerade (this latter is only applicable to radio communication). ETCS functionality considered as belonging to the non-trusted communication channel is inside “Euroradio”, “BTM”, “Eurobalise” and “Euroloop and Radio Infill units”.
- 6.2.1.4 Note: Euroradio, BTM and LTM also contain functions that belong to the on-board and trackside safety relevant functionality.
- 6.2.1.5 In the apportionment of the THR_{ETCS} , it is assumed that the failure modes inside the equipment that are considered to be part of the non-trusted communication channel are protected by the safety code with respect to the corruption of messages.

¹ Applied for the Balise / Loop transmission systems, which are regarded as a closed transmission system

² Applied for the Radio transmission system, which is regarded as an open transmission system



6.2.1.6 It is therefore permissible to define the “non-trusted part” of ETCS transmission equipment as that part of ETCS equipment fulfilling the above assumptions in relation to corruption. A supplier of onboard or trackside ETCS equipment will be allowed to define parts of his equipment as non-trusted, if it can be proved that the equipment and failure modes inside this part does not violate the protection capability of the safety code.

6.2.1.7 Note: It is also assumed that the characteristics of the air gaps for Euroradio, Eurobalise and Euroloop are according to the assumptions in the corresponding specifications, ensuring that the probability of undetected corruption is negligible, due to the performance of the safety codes.

6.2.2 Masquerade of messages

6.2.2.1 The quantitative safety targets derived in this document are valid for errors in the communication channels originated by random events (e.g., corruption due to electromagnetic interference, abnormal delays or repetitions in the non-trusted communication system).

6.2.2.2 Masqueraded messages, originated by intentional attacks to the radio transmission system, must be treated separately on the basis of qualitative considerations, because the rate of malicious attacks can not be estimated. The protection offered by the cryptographic safety code defined in the Euroradio specifications may be considered sufficient provided the organisation responsible for system operation can demonstrate the appropriateness of measures to ensure the confidentiality of the keys.

6.2.3 Apportionment of the TRANS Hazardous Events

6.2.3.1 Each TRANS-x-event summarised in section 4 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 of hazard rates to each constituent are listed below.

6.2.3.2 The assignment of events to functional elements within a constituent shall not be interpreted as a mandatory partitioning between sub-systems.

6.2.4 Balise Channel Events

6.2.4.1 TRANS-BALISE-1 (Corruption)

BTM-H4 Transmission to the on-board kernel of an erroneous telegram, interpretable as correct, due to failure within the on-board BTM function

EUB-H4 Transmission of an erroneous telegram, interpretable as correct, due to failure within a Balise.

Note: TRANS-BALISE-1 also includes the undetectable corruption of a message in the air gap. The occurrence of this event is considered to be negligible due to the characteristics of the safety code.

6.2.4.2 TRANS-BALISE-2 (Deletion)

BTM-H1 A Balise Group is not detected, due to failure within the on-board BTM function

EUB-H1 A Balise Group is not detected, due to failure of the Balise Group to transmit a detectable signal

6.2.4.3 TRANS-BALISE-3 (Insertion)

BTM-H7 Erroneous localisation of a Balise Group, with reception of valid telegrams, due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal)

EUB-H7 Erroneous localisation of a Balise Group, with the reception of valid telegrams, due to failure within Balises (too strong up-link signal)

BTM-H8 The order of reported Balise, with reception of valid telegrams, is erroneous due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal)

EUB-H8 The order of reported Balises, with reception of valid telegram, is erroneous due to failure within a Balise (too strong up-link signal)

BTM-H9 Erroneous reporting of a Balise Group in a different track, with reception of valid telegrams, due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal)

EUB-H9 Erroneous reporting of a Balise Group in a different track, with reception of valid telegrams, due to failures within Balises (too strong up-link signal)



6.2.5 Loop Channel Events

6.2.5.1 TRANS-LOOP-1 (Corruption)

LTM-H4 Transmission of an erroneous telegram / telegrams, interpretable as correct, due to failure within the on-board LTM function

LO-H4 Transmission of an erroneous telegram / telegrams interpretable as correct, due to failure within a Loop.

Note: TRANS-LOOP-1 also includes the undetectable corruption of a message in the air gap. The occurrence of this event is considered to be negligible due to the characteristics of the safety code.

6.2.5.2 TRANS-LOOP-3 (Insertion)

LTM-H9 Erroneous reporting of a Loop in a different track, with reception of valid telegrams, due to failure within the on-board LTM function

LO-H9 Erroneous reporting of a Loop in a different track, with reception of valid telegrams, due to failures within Loops

6.2.5.3 Note that the equivalent of deletion is not carried through for the loop, as this is not a hazard.



6.2.6 Radio Channel Events

6.2.6.1 For the radio channel events, the same numbering for corruption, insertion and deletion is used, as for the balise channel events. Note that this implies that the number series will not be complete for the radio channel, as insertion is not a hazard.

6.2.6.2 TRANS-OB/RADIO-1 (Corruption)

TR-EUR-H4, Radio message corrupted in the trackside Euroradio, such that the message appears as consistent.

OB-EUR-H4, Radio message corrupted in the on-board Euroradio, such that the message appears as consistent.

Note: TRANS-OB/RADIO-1 also includes the undetectable corruption of a message in the air gap. The occurrence of this event is considered to be negligible due to the characteristics of the safety code.

6.2.6.3 TRANS-OB/RADIO-2 (Deletion)

TR-EUR-H1, Radio message deleted in the trackside in an undetectable way

OB-EUR-H1, Radio message deleted in the on-board in an undetectable way

6.2.6.4 TRANS-TS/RADIO-1 (Corruption)

TR-EUR-H4, Radio message corrupted in the trackside Euroradio, such that the message appears as consistent.

OB-EUR-H4, Radio message corrupted in the on-board Euroradio, such that the message appears as consistent.

Note: TRANS-TS/RADIO-1 also includes the undetectable corruption of a message in the air gap. The occurrence of this event is considered to be negligible due to the characteristics of the safety code.

6.2.6.5 The TRANS-xx/RADIO-1 allocation reflects the bi-directional nature of the radio link and that the potential for corruption is present in either direction (Trackside to Onboard or Onboard to Trackside).

7. SAFETY REQUIREMENTS FOR THE ON-BOARD FUNCTIONS

7.1 Allocations to the ETCS Onboard Constituent

7.1.1.1 The purpose of this section is to define the role of the on-board system (less those parts related to the transmission functions) and to derive the maximum tolerable hazard rate against which this equipment will be assessed.

7.1.1.2 From the trial apportionment, the ETCS On-board (i.e. excluding the non-trusted transmission functions) must not contribute to the ETCS hazard with a failure rate greater than $THR_{On-board} = 1/3 * THR_{ETCS}$.

$$THR_{On-board} = 0.67 * 10^{-9} \text{ dangerous failures hour}^{-1}.$$

7.1.1.3 Each supplier shall prove the attainment of the $THR_{On-board}$, considering, in its specific analysis (e.g., fault tree) for the equipment, at least the following hazardous events, as defined in Part 2:

- KERNEL - 1-34
- ODO - 1-4
- TI - 1-6
- MMI - 1-4
- BTM-H4 (the parts of the hazard that arise due to failures inside the trusted part of the transmission channel)
- LTM-H4 (the parts of the hazard that arise due to failures inside the trusted part of the transmission channel)
- OB-EUR-H4 (the parts of the hazard that arise due to failures inside the trusted part of the on-board transmission channel)

7.1.1.4 The proof shall consider the Mission Profile defined in section 5.3 and may take account of the protective features inherent in ETCS as also identified in section 5.4.

7.2 Considerations for Elements External to the On-board

7.2.1 Introduction

7.2.1.1 This section considers the external hazardous events ENG, EXT and DRV as developed in part 2. These events do not contribute to the ETCS-THR but they do have an effect on overall system safety as experienced by a passenger on the train.



7.2.1.2 External elements providing incorrect data could lead to an accident even if the ETCS is working correctly. Examples of this are,

- Wrong engineering data used in the preparation of a scheme
- Incorrect installation of equipment
- Incorrect data entered by the Driver
- Incorrect information at the train interface.

7.2.1.3 These represent a “probability of error” that is fed into ETCS by external factors and is therefore outside the responsibility of ETCS. However, it is appropriate to consider their impact and any possible measures to minimise this impact in order to ensure that the operational safety as perceived by a passenger is maximised.

7.2.1.4 A hazard caused by Onboard functions depends on a failure of the driver together with function failures by the onboard equipment, but the relationship between Driver errors and Onboard functions depends on mode. For example, when the train is in OS mode, ETCS supervises a speed limit, but does not supervise the stop before an obstacle on the track such a rock fall for example, as the obstacle is not known to ETCS.

7.2.2 Engineering Data

7.2.2.1 This is ENG 3 where specific pre loaded engineering data for fixed train data and / or ETCS identity is stored in the on-board.

7.2.2.2 The creation of engineering data and its loading into the on-board must achieve a quality level commensurate with a SIL 4 system. This is interpreted as meaning that the process for the obtaining of the raw data through to its loading into ETCS must be analysed to identify possible threats to the correctness of the data and putting in place actions which minimise the scope for error.

7.2.2.3 Standardisation of such procedures is not necessary for interoperability.

7.2.3 Installation

7.2.3.1 The quality of the installation process for the train will affect the safety level achieved both in the country of origin and in any other country that train might enter.

7.2.3.2 The Data Preparation and Installation Engineering must be considered as a part of the design of a specific ETCS application. Therefore, it will be managed with quality procedures commensurate with the SIL 4 allocation to the technical system. As above, this is interpreted as meaning that the whole process must be analysed to identify possible sources of error and putting in place measures to counter such errors.

7.2.3.3 Standardisation of such procedures is not necessary for interoperability.

7.2.4 Interaction with the Driver

7.2.4.1 Data Entry

7.2.4.1.1 This section refers to the events DRV2, 3, 4 & 5 as developed in Part 2 of this suite of documents. These events cover the entry of safety critical data by the driver at the start of a mission or during a mission.

7.2.4.1.2 The provision of incorrect data to the engineering process in relation to the characteristics of the train will affect achieved levels of system safety both in the country of origin and in any other country that the train might enter. (EXT 2)

7.2.4.1.3 For train data entry performed by the driver, any of the following errors may occur:

The driver is provided with an incorrect value (ENG 2) due either to EXT 2 or failures in a subsequent process - this event cannot be mitigated by ETCS and safety is therefore dependent upon the correctness of the complete process.

The driver is provided with the correct values but makes “typing errors” (events DRV 2, 3, 4 & 5). These events may mitigated may be mitigated with procedures e.g. double entry, read back and request for confirmation.

7.2.4.1.4 Thus it will be necessary to demonstrate that the selected national data entry procedure achieves a quality commensurate with a SIL 4 system taking into account the whole process from data gathering through to confirmation that the correct data has been stored in ETCS.

7.2.4.1.5 The number of driver interactions with the On-board equipment, driver failure rates and the possible consequence of a failure of such data - as indicated in Part 2 - shall be taken into account to assessing the data entry procedures.

7.2.4.2 The Reaction of the Driver to Misinformation on the MMI

7.2.4.2.1 This section refers to the events developed in part 2, MMI-2 (incorrect display with respect to the supervision) and MMI-4 (frozen display) and their contribution to THR_{ETCS} .

7.2.4.2.2 The ETCS hazards have been developed for the MMI failures where the driver is misinformed. In this situation there is a relationship between the driver and the supervision and protection provided by the ETCS equipment.

7.2.4.2.3 If a failure is initiated by Driver (DRV 1) or by an MMI error of display (MMI 2) it is combined as an AND function with the supervision and protection provided by ETCS. In this case ETCS is seen to act as mitigation for both Driver and MMI failures.

7.2.4.2.4 If a failure is initiated by the on-board kernel resulting in the display of incorrect information on the MMI and also supervision against this incorrect information, the only protection in this case is driver vigilance. If the driver is not aware of such an ETCS failure and the displayed values are reasonable, the AND between the driver and ETCS is no longer valid.

7.2.4.2.5 If the display functions of the MMI are used when the supervision and protection provided by ETCS is not available in whole or part, then a greater reliance will be placed on the integrity of the displayed data on the MMI. In such cases the integrity of the MMI should not be less than that achieved by the existing electromechanical devices used to display actual speed.

7.2.4.3 MMI Acknowledgements and Commands by the Driver

7.2.4.3.1 This section refers to the event MMI-1 developed in part 2 and its contribution to THR_{ETCS} .

7.2.4.3.2 This document does not mandate specific solutions for required safety: for example, in the case of acknowledgements, it is the responsibility of the supplier to prove that the THR for the on-board is achieved by whatever method is selected.

7.2.4.3.3 Such an analysis shall consider the frequency of occurrence of the scenarios where the function is used.

7.2.5 Interface to the Train

7.2.5.1 The dependency on correct information regarding brake status, direction control and cabin active which may originate from items which do not have the same level of integrity as ETCS.

7.2.5.2 The application of the train brakes when commanded by ETCS may rely on items that do not have the same level of integrity as ETCS.

7.3 Apportioned Target

- 7.3.1.1 The tolerable hazard rate target for the on-board system, less those parts forming the non-trusted part of the transmission system, is confirmed as,

$$\text{THR}_{\text{On-board}} = 0.67 * 10^{-9} \text{ dangerous failures hour}^{-1}.$$

- 7.3.1.2 Given that the function of the on-board system is supervise the movement of the train and protect against exceeding the speed and / or distance parameters as advised to the on-board. The THR relates to,

Failure to provide on-board supervision and protection in accordance with the information advised to the on-board from external entities.

Note: Included the concept of external entities is the trackside providing correct information to the on-board.

8. SAFETY REQUIREMENTS FOR THE ETCS TRACKSIDE FUNCTIONS

8.1 Allocations to ETCS Trackside Constituents

8.1.1.1 The purpose of this section is to define the role of the Trackside system (less those parts allocated to the non-trusted transmission functions), and to derive the maximum tolerable hazard rate against which this equipment will be assessed.

8.1.1.2 It is assumed that the LEU- and RBC-events are mutually exclusive, occurring in either Level 1 for the LEU or in Level 2 for the RBC.

Note: If LEUs are used for safety relevant information in level 2, this must be analysed separately to demonstrate that the THR_{ETCS} is not exceeded.

8.1.1.3 From the trial apportionment, the ETCS Trackside (i.e. excluding the non trusted transmission functions) must not contribute to the ETCS hazard with a failure rate greater than $THR_{trackside} = 1/3 * THR_{ETCS}$:

$$THR_{trackside} = 0.67 * 10^{-9} \text{ dangerous failures hour}^{-1}.$$

8.1.1.4 Each supplier shall prove the attainment of the $THR_{trackside}$, considering, in its specific analysis (e.g., fault tree) for the equipment taking into account the following events, as defined in Part 2

- RBC-2 and RBC-3 (Level 2 only)
- TR-EUR-H4 (Level 2 only) for the parts of the hazard that arise due to failures inside the trusted part of the trackside transmission channel

Or

- LEU-H4 (Level 1 only)
- TR-EUR-H4 (Level 1 if Radio infill is used) for the parts of the hazard that arise due to failures inside the trusted part of the trackside transmission channel.

8.1.1.5 The proof shall consider the Mission Profile in section 5.3 and can take account of the protective features inherent in ETCS as identified in section 5.4.

8.2 Considerations for Elements External to the Trackside ETCS

8.2.1 Introduction

8.2.1.1 This section considers the external events ENG EXT as identified in part 2 of this suite if documents that will have an effect on overall system safety as experienced by a passenger on the train.



8.2.1.2 External elements which form part of the consideration for a harmonised ETCS which if they provided incorrect data, could lead to an accident even if the ETCS is working correctly are,

- Wrong engineering data used in the preparation of a scheme
- Incorrect installation of equipment
- System maintenance

8.2.1.3 Other external entities upon whose operation ETCS is dependent but whose integrity cannot be harmonised are,

- Interlockings

8.2.1.4 These represent an “probability of error” that is fed into ETCS by external factors but are outside the responsibility of ETCS. However, it is appropriate to consider their impact and possible measures to minimise this impact in order to ensure that the operational safety as perceived by a passenger is maximised.

8.2.2 Engineering Data

8.2.2.1 Engineering data relates to the capture, description and the preparation of the network topography data for inclusion in the trackside equipment.

8.2.2.2 Errors in this data could lead to a hazard

8.2.2.3 Therefore, the complete process will be managed with quality procedures commensurate with the SIL 4 allocation to the technical system. This means the process must be analysed to identify potential areas of weakness that could lead to incorrect data and to put measures in place to minimise the threat created by these areas of weakness

8.2.2.4 It is not considered necessary to harmonise the processes.

8.2.3 Installation of Equipment

8.2.3.1 The quality of the installation process inclusive of testing, must be managed with quality procedures commensurate with the SIL 4 allocation to the technical system

8.2.4 Interlockings

8.2.4.1 Interlockings provide a vital role in identifying if the route ahead of a train is clear and it is safe to proceed

8.2.4.2 The probability of a Hazard caused by on wrong route information from an interlocking depends on equipment that is outside the scope of ETCS.

- 8.2.4.3 Hazards created by interlockings will be specific to the country in which the interlocking is sited.

8.3 Apportioned Target

- 8.3.1.1 The tolerable hazard rate for the trackside system, less those parts forming part of the non-trusted transmission system, is confirmed as

$$\text{THR}_{\text{trackside}} = 0.67 * 10^{-9} \text{ dangerous failures hour}^{-1}$$

- 8.3.1.2 The $\text{THR}_{\text{trackside}}$ is applicable to the LEU in level 1 or the RBC in level 2

- 8.3.1.3 Given that the role of the trackside is to advise the on-board of its safe movement limits and to provide the topography information to allow the on-board to calculate the correct intervention point. Then the THR relates to

Failure to provide information to the on-board supervision in accordance with the data advised to the trackside from external entities.

Note: Included the concept of external entities for Level 2 is the on-board providing correct information to the RBC.

9. SAFETY REQUIREMENTS FOR THE TRANSMISSION FUNCTIONS

9.1 Apportionment between the On-board and Trackside for the Radio, the Balise and Loop Subsystems

9.1.1.1 As the transmission system is not a referenced interoperable grouping, the purpose of this section is to derive the maximum tolerable hazard rates for the On-board and Trackside parts of the ETCS non-trusted transmission systems. The derived targets are required to ensure technical interoperability and therefore the system will be assessed against the targets.

9.1.1.2 Initially, $\frac{1}{3}$ of THR_{ETCS} is apportioned to the transmission functions and this equates to a dangerous failure rate of,

$$THR_{TX} = 6.7 * 10^{-10} \text{ hour}^{-1} \text{ train}^{-1}.$$

9.1.1.3 The transmission parts of ETCS are the GSM-Radio sub system, Balise sub system and the Loop subsystem. The apportionment of the tolerable failure rate to these separate transmission media is dependent on the ETCS level.

Note: The RBC to RBC link is a private link but its requirements are considered as part of the trackside THR with event RBC-3.

9.1.1.4 In level 1 there is only a limited amount of radio transmission with the use of the Radio Infill feature.

9.1.1.5 In level 2 the THR_{TX} is initially, shared equally between the balise system and the radio system as THR_{BTX} and THR_{RTX} respectively. This same apportionment will therefore be applied to level 1 as detailed in 9.1.1.4.

9.1.1.6 The hazards identified in Part 2 that relate to the balise system are

- TRANS-BALISE-1 - Corruption
- TRANS-BALISE-2 - Deletion
- TRANS-BALISE-3 - Insertion

The balise system and its associated hazards are analysed in Annex A. This separate analysis is necessary because of the complexity of the analysis resulting from the many uses of the balise sub system within ETCS.

9.1.1.7 The hazards identified in Part 2 that relate to the radio transmission system are

- TRANS-OB/RADIO-1 - Incorrect radio message received by the on-board kernel functions as consistent
- TRANS-OB/RADIO-2 -Radio message not received by the on-board kernel functions. Note: Deletion as experienced by the RBC has been determined as not being a hazard.
- TRANS-TS/RADIO-1 -Incorrect on-board radio message received by the RBC kernel functions as consistent

The radio system and its associated hazards are considered in the following sections where the tolerable failure rate of $1/6 * THR_{ETCS}$ is,

$$THR_{RTX} = 3.3 * 10^{-10} \text{ hour}^{-1}.$$

9.2 Assessment of the Radio Transmission Subsystem

9.2.1 Apportionment to the Corruption of Radio Messages

9.2.1.1 Undetected corruption of messages in the radio transmission system shall have a negligible probability with respect to THR_{RTX} . This means that the following events as defined in Part 2 must not have a failure rate of more than

$$THR_{RTX\text{corruption}} = 1.0 * 10^{-11} \text{ hour}^{-1}.$$

When taking into account the following events from Part 2

- TRANS-OB/RADIO-1
- TRANS-TS/RADIO-1

9.2.1.2 This is considered a valid approach due to the powerful message coding strategies employed in the radio sub system but it must take into account the non trusted parts of the transmission system both on-board and trackside.

9.2.1.3 The above considerations apply to the following radio paths,

RBC to On-board

On-board to RBC

RIU to On-board (Note: TRANS-TS/RADIO-1 is not applicable to the infill function.)

9.2.2 Apportionment to the Deletion of Radio Messages

9.2.2.1 Critical Messages sent via the GSM-R are subject to acknowledgement rendering undetected deletion as having a very low probability.



- 9.2.2.2 In the case of in-fill, deletion of a message will result in ETCS maintaining its existing braking profile.
- 9.2.2.3 No target hazard rate is allocated to this event in accordance with the considerations in the following section. Thus TRANS-OB/RADIO-2 is not classed as a hazard.

9.3 General Considerations Relating to the Radio Transmission System

9.3.1 General

- 9.3.1.1 The coding and message structure used in the radio transmission has been specifically designed to counter the hazards identified in EN 50159-1 Part 2: Safety-related communication in open transmission systems.

9.3.2 Corruption in the Radio Channel

- 9.3.2.1 The radio transmission system utilises a bi-directional data path over a non-trusted bearer.
- 9.3.2.2 The rate of occurrence of a hazard resulting from a failure of a non-trusted bearer depends on the number of incorrect safety related messages sent and on the capability of the safety coding / decoding procedure to detect the incorrect message.
- 9.3.2.3 The safety coding / decoding procedure adopted is based on wide experience and is designed to provide a very high level of protection.
- 9.3.2.4 Based on this safety coding/decoding procedure, it follows that a stringent target can be required in respect of the corruption hazards TRANS-OB/RADIO-1 and TRANS-TS/RADIO-1 with respect to TRANS-OB/RADIO-2.

9.3.3 Deletion in the Radio Channel

- 9.3.3.1 As indicated in 9.2.2.1, the data exchange between track and train is defined in the ETCS specifications such that normally the deletion of a message does not result in a hazard. Moreover, deletion of critical messages is mitigated by means of acknowledgement procedures. The only case where deletion may lead to a hazardous situation is in the case of Emergency messages and this situation is considered in the following section. On the basis of these further considerations the possibility of undetected deletion of messages is not carried forward as a provable / testable target.
- 9.3.3.2 Additionally to all the measures indicated above, deletion of a radio infill message is not considered a hazard contribution to the ETCS THR.

9.3.4 Emergency Messages via Radio

- 9.3.4.1 The transport of Emergency Messages is a service provided by ETCS. It is probably used to reduce the risks of accidents resulting from hazards such as avalanches, road vehicles on the track etc.
- 9.3.4.2 It is noted in the SRS that the Emergency Message shall use the high priority channel. Therefore it is not protected with the same safety features as the normal priority channel against corruption and / or deletion. The ETCS Emergency function is designed for the shortest possible response time, not for high integrity.
- 9.3.4.3 Thus the integrity of the Emergency Message is dependent upon the quality and availability of the radio network, and as such 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 performance that can be achieved by the emergency message function. If very stringent performances are required, it is possible that an additional independent emergency management service will be needed.
- 9.3.4.4 From an ETCS perspective, the use of Emergency Messages Service shall not detract from the safety of the technical system.

9.3.5 Final Apportionment to the Radio Transmission System

- 9.3.5.1 The initial apportionment has been modified to take account of the negligible contribution to the core hazard from the Radio transmission system. The resulting allocations are,

$\text{THR}_{\text{RTXcorruption}} = 1.0 * 10^{-11}$ Dangerous Failures hour⁻¹ train⁻¹ due to the corruption of messages sufficient to be interpreted as consistent by the on-board kernel or the RBC kernel, resulting in ETCS exceeding its known speed and distance limits.

Note: The attainment of this figure must take into account the non trusted parts of the communication channel in both the on-board and trackside systems.

9.3.6 Impact on the Balise / Loop Transmission Systems

9.3.6.1 As a result of demanding that the contribution of the Radio system to the core hazard is negligible, the initial one sixth apportionment to the balise transmission system is amended to $1/3 * THR_{ETCS}$ thus,

$THR_{BTX} = 6.7 * 10^{-10}$ Dangerous Failures / hour when taking into account the hazards,

- TRANS-BALISE-1 - Corruption
- TRANS-BALISE-2 - Deletion
- TRANS-BALISE-3 - Insertion
- TRANS-LOOP-1
- TRANS-LOOP-3

9.3.6.2 The detailed analysis and apportionment of this revised target is undertaken in Annex A of this document.

9.4 Summary of Hazardous Events

9.4.1.1 The following list summarises the hazardous events.

Event Id.	Event Description
MMI-1a	False acknowledgement of mode change from Full Supervision
MMI-1b	False command to enter Non-leading mode
MMI-1c	False command of Override EoA request
MMI-1d	False acknowledgement of Level Transition
MMI-1e	False acknowledgement of Train Trip
MMI-1f	False acknowledgement of Track Ahead Free
MMI-2a	False presentation of speed or distance on the MMI
MMI-2b	False presentation of mode on the MMI
MMI-3	Falsification of driver's train data input
MMI-4	Frozen or delayed MMI display
ODO-1	Incorrect standstill indication
ODO-2	Speed measurement underestimates trains actual speed
ODO-3	Incorrect actual physical speed direction
ODO-4	Distance measurement is incorrect

Event Id.	Event Description
KERNEL-1	Balise linking consistency checking failure
KERNEL-2	Balise group message consistency checking failure
KERNEL-3	Failure of radio message correctness check
KERNEL-4	Radio sequencing checking failure
KERNEL-5	Radio link supervision function failure
KERNEL-6	Manage communication session failure
KERNEL-7	Incorrect LRBG
KERNEL-8	Emergency Message Acknowledgement Failure
KERNEL-9	Speed calculation underestimates train speed
KERNEL-10	Functional failure of standstill detection
KERNEL-11	Incorrect traction/braking model (e.g. brake use restrictions)
KERNEL-12	Failure of standstill supervision
KERNEL-13	Failure of backward distance monitoring
KERNEL-14	Failure of reverse movement protection
KERNEL-15	Incorrect cab status (TIU failure)
KERNEL-16	Incorrect train status TIU sleeping/cab status
KERNEL-17	Wrong Acceptance of MA
KERNEL-18	Failure to manage RBC/RBC
KERNEL-19	Failure of train trip supervision in OS and FS
KERNEL-20	Failure of train trip supervision, shunting and SR
KERNEL-21	Incorrect supervision of stop in SR
KERNEL-22	Incorrect current EoA
KERNEL-23	Incorrect train position / train data sent from on-board to trackside
KERNEL-24	Failure of message acknowledgement
KERNEL-25	Incorrect traction/braking model (Acceleration only)
KERNEL-26	Deleted
KERNEL-27	Incorrect System Data (e.g. current level)
KERNEL-28	Incorrect confidence interval
KERNEL-29	Failure to shorten MA

Event Id.	Event Description
KERNEL-30	Incorrect shortening of MA
KERNEL-31	Deleted
KERNEL 32	Failure of loop message consistency checking
KERNEL-33	Wrong processing of MA information
KERNEL-34	Incorrect supervision of MA time-outs (sections and overlaps)
TI-1	Service brake / emergency brake not commanded when required
TI-2	Service brake / emergency brake release commanded when not required
TI-3	Inappropriate sleeping request
TI-4	Incorrect brake status (TIU failure)
TI-5	Incorrect direction controller position report (TIU failure)
TI-6a	Loss of Cabin Active signal
TI-6b	Wrong Cabin considered as Active
EUB-H1	A balise group is not detected, due to failure of a balise group to transmit a detectable signal
EUB-H4	Transmission of an erroneous telegram interpretable as correct, due to failure within a Balise
EUB-H7	Erroneous localisation of a Balise Group, with reception of valid telegrams, due to failure within Balises (too strong up-link signal)
EUB-H8	The order of reported Balises, with reception of valid telegram, is erroneous due to failure within a Balise (too strong up-link signal)
EUB-H9	Erroneous reporting of a Balise Group in a different track, with reception of valid telegrams, due to failures within Balises (too strong up-link signal)
BTM-H1	A balise group is not detected, due to failure within the onboard BTM function
BTM-H4	Transmission to the on-board kernel of an erroneous telegram, interpretable as correct, due to failure within the onboard BTM function
BTM-H7	Erroneous localisation of a Balise Group, with reception of valid telegrams, due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal)
BTM-H8	The order of reported Balises, with reception of valid telegrams, is erroneous due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal)

Event Id.	Event Description
BTM-H9	Erroneous reporting of a Balise Group in a different track, with reception of valid telegrams, due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal)
OB-EUR-H4	Radio message corrupted in onboard Euroradio, such that the message appears as consistent
TR-EUR-H4	Radio message corrupted in trackside Euroradio, such that the message appears as consistent
LEU-H4	Transmission of an erroneous telegram / telegrams interpretable as correct, due to failure within the LEU function
LO-H4	Transmission of an erroneous telegram / telegrams interpretable as correct, due to failure within a Loop
LTM-H4	Transmission of an erroneous telegram / telegrams, interpretable as correct, due to failure within the on-board LTM function
RBC-2	Incorrect radio message sent from RBC Kernel, such that the message appears as consistent
RBC-3	Incorrect radio message from an adjacent RBC, causing incorrect message to ETCS onboard

10. CONCLUSIONS

10.1 General Conclusions

10.1.1 Overview

10.1.1.1 ETCS is a system that forces the driver to respect the information that it is aware of. Thus, in relation to achieving a safe railway operation,

- The information that ETCS receives from external sources must be correct else ETCS could enforce respect of unsafe commands.
- The information sent over the interoperable interfaces of ETCS must be both acquired and correct; else ETCS could enforce respect of unsafe commands.
- The degree of protection that ETCS can provide for the driver is dependent upon the operational mode of the on-board system.

10.1.1.2 In 10.2.2 and 10.2.3 recommendations are made to minimise the effect of these potential weaknesses. In addition,

- Qualitative requirements are placed on external information where that information affects interoperability by limiting the achieved safety on another network.
- ETCS ensures that wherever possible, information that is not acquired (deletion) is not more restrictive. Where this basic signalling principle is not achievable, the use of system level mitigations such as an acknowledgement procedure is required.
- Maximum use of Full Supervision is required as part of the mission profile as this provides the maximum protection against Driver error.

10.1.2 Mission Profile Dependency

10.1.2.1 Apportionment of the THR_{ETCS} over the approved grouping of constituents has created demanding failure rate targets for the equipment.

10.1.2.2 The derivation of the hazards is a clear and unambiguous process whilst the derivation of the numerical targets is crucially dependent on the mission profile and the assumed rate of occurrence of operational scenarios.

10.1.2.3 Associated with the mission profile, are the assumptions made about the rate at which the driver can create a hazard that ETCS should then try to prevent. Again, the derivation of the numerical failure rate targets is dependent on these assumptions.



10.1.3 Relevance of the Numerical Targets

- 10.1.3.1 The numerical targets are derived from a probability of a random ETCS failure of,
 $2.0 * 10^{-9}$ hours.
- 10.1.3.2 The figures derived from the above target may form the basis for conformity assessment but there is no direct link between the figures and the safety of a travelling passenger.
- 10.1.3.3 The overall safety achieved on an operational railway is dependent on issues out side of ETCS. ETCS however, is primarily designed to protect against human (driver) error and in order to relate the failure rate of ETCS to the safety of an operational railway requires a much better understanding of how the driver interacts with the equipment.
- 10.1.3.4 Considerations on the use of un-linked balises to relay vital data result in targets that are not readily achievable. However, the elaboration of additional engineering rules such as the use of 2 balise groups to announce a speed restriction, allow the ETCS THR to be achieved.
- 10.1.3.5 Of particular concern are modes other than Full Supervision where the driver has increased levels of responsibility. The responsibility placed on the driver must carefully specified such that each of these modes equates to a uniform level of responsibility in each country visited by a driver.

10.2 Conclusions Relating to the Derived Balise Targets

10.2.1 General

- 10.2.1.1 The linking of Balise information points is a very powerful protection mechanism in combating both deletion and cross talk. Thus, the ratio of 1000 to 1 for linked information points to information points that are not linked is regarded as a desirable average.
- 10.2.1.2 The failure rate targets derived are related to cases where linking is not used as this represents the worst case.
- 10.2.1.3 The warning of Temporary Speed Restrictions by placing total reliance on the detection of un-linked balises led to requirements on the failure rate for an information point that is not feasible. This resulted in the requirement for the use of 2 separate balise groups each with a minimum of 2 balises. This requirement eased the target failure rates on both the onboard and trackside to figures that are feasible.

- 10.2.1.4 As consequence of the need to have minimum of two balise transponders forming a safety related information point, there must be a fault detection and reporting process to resolve the problem of one balise in the pair failing. Such a process is required for both level 1 and level 2 and needs harmonising in terms of the information to be recorded and how access is provided to the information so as to minimise down times.
- 10.2.1.5 As a consequence of the 2 separate balise group requirement the Start of Mission criteria led to the most onerous failure rate for an information point. The figure derived remained within the bounds of feasibility.
- 10.2.1.6 In the case of situations where linking is not established or is not used, particular scrutiny of the common operational rules is required to ensure a minimum risk to the travelling passenger is achieved. An example that is noted is that a procedure for entry into an ETCS area from an unfitted area that prevents entry of unfitted trains or of trains where the on-board is not fully functional in cases where mixed traffic is not allowed (e.g. Level 2 without optical signals)
- 10.2.1.7 The possibility of cross talk cannot be covered by quantified safety analysis, therefore the top level requirement is passed to the balise working groups to establish quantitative requirements and application rules designed to minimise the possibility of cross talk.
- 10.2.1.8 An ETCS scheme designer needs to be aware when positioning information points that if a linked information point with an associated linking reaction is not detected, the train may be brought to a stand at a point beyond the information point. This position will be dictated in ETCS by the accumulated odometer errors in the on-board kernel plus the extreme end of the information point expectation window.
- 10.2.1.9 The figures derived in Annex A relate to a defined mission profile, the frequency of non-linked information points, the frequency of scenarios and are based on assumptions about fault detection times. Thus equipment designed to meet these targets must be deployed carefully to ensure that the assumptions are not invalidated in a way that reduces the overall THR_{ETCS} or invalidates technical interoperability.
- 10.2.1.10 In undertaking the analysis several areas have been identified where it is both possible and desirable to extend the inherent protective features of ETCS. These issues are covered in the next section.



10.2.2 Proposals for Additions to the Inherent Protective Features of ETCS

10.2.2.1 The following are proposals to reduce the frequency of occurrence the TRANS-BALISE-2 Hazard

In order to minimise the possibility of missing restrictive information in a linked information point the following rule is proposed,

The 'No Reaction' option is not permissible in the case of linked balises containing data, which if missed, could lead to the ETCS core hazard.

Reference, Annex A - Paragraph 5.1.2.4

10.2.2.2 In order to minimise the distance a train can travel with linking active and a failed on-board receiver the following rule is defined,

If two expected consecutive linked balise groups announced by linking are not detected (regardless of their defined linking reaction), the on-board shall consider the linking command of the second balise group as a command to apply the service brake.

The driver shall be informed of this specific linking reaction.

Reference, Annex A - Paragraph 5.1.2.5

10.2.2.3 The following is taken into account to reduce the frequency of occurrence the TRANS 3 Hazard

In order to minimise the possibility of cross talk in repositioning moves the following rule is considered,

If two consecutive repositioning information points are found, this shall result in the activation of the service brake by the on-board until the train is at standstill. The EoA shall be withdrawn to the current head of the train and the driver informed.

Reference, Annex A - Section 7.3.1.4.

10.2.3 Proposals for Additions to the Engineering Rules for ETCS

10.2.3.1 Methods to reduce the frequency of occurrence of the TRANS-BALISE-3 hazards are given in Subset 036 (the Eurobalise FFFIS).

11. SENSITIVITY ANALYSIS

11.1 Scope of the Sensitivity Analysis

- 11.1.1.1 The apportionment undertaken in this document has demonstrated that ETCS meets the THR_{ETCS} . The resulting detailed requirements for the ETCS grouping of constituents are summarised in section 12. This sensitivity analysis identifies the major dependencies in achieving the THRs and the level of freedom that there may be in meeting or improving the hazard rates. This section is however, purely indicative of what maybe possible and therefore, is not mandatory.
- 11.1.1.2 The sensitivity analysis revisits each of the operational scenarios to consider their sensitivity to the derived THR requirements and the mission profile parameters used in the calculation of the THRs. This further analysis supplements the preliminary sensitivity analyses that were undertaken in Annex A which were undertaken to decide if formulae being taken forward were robust.
- 11.1.1.3 The THRs that have been shown to be dependent upon the operational parameters are those derived for the balise in defending against the transmission hazards of deletion and insertion. The THR figures for the on-board and trackside subsystems are not affected by the operational parameters.

11.2 Review of operational Scenarios

11.2.1 Deletion (TRANS-BALISE-2)

- 11.2.1.1 This revisits section 6.4.2 of Annex A and the preliminary sensitivity analysis at section 6.8 in Annex A.
- 11.2.1.2 The derivation of the THR for TRANS-BALISE-2 in this scenario is based on the formula,

$$R_{NL} = r_{NL} * P_{DR} * ((\lambda_{IP} * 24h) + (\lambda_{ONB} * T_{NL}))$$

where the THR (R_{NL}) was $3.3 * 10^{-10}$ Dangerous Failures hour⁻¹.

- 11.2.1.3 Looking at ETCS dependent figures for the failure rate of the balise group (λ_{IP}) and the failure rate for the on-board balise detection (λ_{ONB}), the figures that have been derived are considered to be at the bound of feasibility. These being,

$$\lambda_{IP} = 1.0 * 10^{-9} \text{ Dangerous Failures hour}^{-1}.$$

$$\lambda_{ONB} = 1.0 * 10^{-7} \text{ Dangerous Failures hour}^{-1}.$$

Where, ignoring the frequency of occurrence modifiers $r_{NL} * P_{DR}$, the ETCS dependencies are dominated by the $(\lambda_{ONB} * T_{NL})$ term. In order to bring this in line with $(\lambda_{IP} * 24h)$ then the undetected duration of an on-board failure T_{NL} needs to be reduced by a factor of 10.

- 11.2.1.4 Even without amending T_{NL} or the mission parameters, the achieved hazard rate is $1.24 * 10^{-10}$ dangerous failures hour⁻¹. This would allow for two entry scenarios per hour without breaching the THR_{ETCS} . However, as the number of entries (r_{NL}) will also double thus, the achieved hazard rate for 2 scenarios will be $2.48 * 10^{-10}$ dangerous failures hour⁻¹.
- 11.2.1.5 A more uncertain parameter in the mission profile is the probability of driver error, which is the dominant feature in the external parameters. Figures for driver error are heavily dependent on individual layouts and further comment on this is outside of the experience of Unisig.
- 11.2.1.6 In the analysis, it is recommended to link the clearance of a signal controlling entry to the ETCS area to proof that the onboard balise detection is working. This overcomes the problem of a train gaining entry without having read the entry balise but does not help when a failed train passes the entry signal displaying danger. In the context of this second case, it is clear that, as soon as a failure of the on-board balise detect function is detected, the ETCS on-board equipment must be considered non-operational. This detection may be done either by,

A self test feature. The failure to pass such a self test resulting in the on-board switching to the System Failure (SF) mode thus co-operating in the attainment of λ_{ONB} .

External events (e.g. linking errors). This case would need to be managed by operational rules.

- 11.2.1.7 If the ETCS area is a Level 1 area open to mixed traffic (ETCS fitted trains and trains without ETCS (unfitted)) then the performance of the failed ETCS train will be the same as the unfitted in terms passing the entry signal at danger. In this instance there is a dependency on the driver in noticing that an expected level change has not occurred.

- 11.2.1.8 In conclusion, it is possible to tolerate a factor of 2 increase in either the rate of scenario occurrence, probability of driver errors or the mean down time of the on-board equipment without exceeding the allowed THR.

11.2.2 Train authorised to Start in Staff Responsible

- 11.2.2.1 This revisits section 6.4.3 of Annex A and the preliminary sensitivity analysis at section 6.8 in Annex A.
- 11.2.2.2 In Level 1 we have the same considerations as for entry into an ETCS area. Thus an improvement in rate of detection of on-board failures would be a means of improving the actual hazard rate. However, based on the THR requirement figures with all existing assumptions the actual failure rate is again $1.24 * 10^{-10}$ dangerous failures hour⁻¹.
- 11.2.2.3 The major assumption is the rate of occurrence of the scenario and comments made at 11.2.1.5 are applicable.
- 11.2.2.4 Similar arguments apply for Level 2 regarding the ETCS parameters and again the frequency of occurrence of the erroneous Staff Responsible authorisation is outside the domain of Unisig. However as above, the achieved failure rate with the existing assumptions is $1.24 * 10^{-10}$ dangerous failures hour⁻¹.
- 11.2.2.5 In conclusion, it is possible to tolerate a factor of 2 increase in either the rate of scenario occurrence, probability of driver errors or the mean down time of the on-board equipment without exceeding the allowed THR.

11.2.3 Temporary Speed Restrictions

- 11.2.3.1 This revisits section 6.5.2 of Annex A and the preliminary sensitivity analysis at section 6.8 in Annex A.
- 11.2.3.2 Based on the announcement of TSRs from 2 independent balise groups and the adoption of the additional linking reaction rule, it was shown in section 8.2 of Annex A that the achieved failure rate is $5.0 * 10^{-10}$ dangerous failure hour⁻¹. This clearly satisfies the THR of $8.25 * 10^{-10}$ dangerous failure hour⁻¹.
- 11.2.3.3 The limiting factor from an ETCS perspective is λ_{ONB} with a failure rate of 10^{-7} hour⁻¹. This cannot be improved upon as it is at the limit of feasibility.
- 11.2.3.4 The other limiting factor that governs the additional linking rule is the time taken to traverse 2 linked information points. From the mission profile this is based on 400 balise groups being interrogated in 1 hour giving a time of 0.005 hours. Clearly the rate at which balises are interrogated depends upon the train speed and the spacing of balises.

- 11.2.3.5 In conclusion, it is not possible to tolerate any increase in the governing parameters discussed above without exceeding the allowed THR.

11.2.4 Shunting

- 11.2.4.1 This revisits section 6.5.3 of Annex A and the preliminary sensitivity analysis at section 6.8 in Annex A.
- 11.2.4.2 The likelihood of a failure in an ETCS defined shunting area leading to an incident on an adjacent ETCS line is considered very remote and is not considered further.
- 11.2.4.3 Issues of loose wagons are outside of the Unisig domain.

11.2.5 Start of Mission

- 11.2.5.1 This revisits section 6.6.1 of Annex A and the preliminary sensitivity analysis at section 6.8 in Annex A.
- 11.2.5.2 The resulting formula for the THR gave,

$$1.6 * 10^{-7} = 24\lambda_{IP} + \lambda_{ONB}$$

When we substitute for the 2 defined balise detection failure rates, this results in an achieved hazard rate of $1.24 * 10^{-7}$ dangerous failures hour⁻¹ with λ_{ONB} being the limiting ETCS parameter.

- 11.2.5.3 In conclusion, it is not possible to tolerate any increase in either the rate of scenario occurrence, probability of driver errors or mean down time of the on-board equipment without exceeding the allowed THR.

11.2.6 General Conclusion on Deletion

- 11.2.6.1 In section 5.1.2.3, Note A, the assumption is made that Start of Mission can be initiated by Entry into an ETCS area or Starting in Staff Responsible as well as by Start of Mission itself. The assumption made is that only 1 these event events will take place in an hour. From the considerations in 11.2.1, 11.2.2 and 11.2.5 it is shown that 2 events are permissible within the hour without exceeding the overall THR_{ETCS}.

11.3 Insertion (TRANS-BALISE-3)

- 11.3.1.1 The general rules to avoid cross talk problems are covered in the Balise FFFIS (Subset 036) and therefore no further comment is made here.
- 11.3.1.2 With the establishment of the repositioning rule detailed at 7.3.1.4 in Annex A repositioning ceases to be an issue for insertion however the rules developed in the Balise FFFIS will still be applicable.



12. SUMMARY OF THE SAFETY REQUIREMENTS FOR ETCS

12.1 Introduction

- 12.1.1.1 These are derived safety requirements prior to the introduction of the system enhancements described in section 10.2.2 and improvements in the operational processes, they are therefore preliminary as the adoption of any or all of the proposals could affect the derived targets.

12.2 General Design Requirements

- 12.2.1.1 The ETCS System shall be designed in accordance with the practices for Safety Related Electronic Signalling Systems. The safety integrity level will be derived from the different tolerable hazard rates

For Hazard Rates of $< 10^{-9}$ a SIL 4 process will be applicable

- 12.2.1.2 The defined targets shall be achieved in a specified environment (Temperature, vibration, EMI etc)

12.3 Safety Requirements for the On-board Subsystem

- 12.3.1.1 The hazard rate for the on-board system, less those parts forming part of the non trusted transmission paths, must be shown not to exceed,

$$\text{THR}_{\text{On-board}} = 0.67 * 10^{-9} \text{ dangerous failures hour}^{-1}.$$

- 12.3.1.2 Where the dangerous failure is defined as,

Failure to provide on-board supervision and protection according to the information advised to the on-board from external entities.

Note: External entities include the assumption that the trackside provides correct information to the on-board.

- 12.3.1.3 Each supplier shall prove the attainment of the $\text{THR}_{\text{On-board}}$, considering, in its specific analysis for the equipment, at least the following events, as defined in Part 2:

- KERNEL - 1-34
- ODO - 1-4
- TI - 1-6
- MMI - 1-4
- BTM-H4 (the parts of the hazard that arise due to failures inside the trusted part of the channel)



- LTM-H4 (the parts of the hazard that arise due to failures inside the trusted part of the channel)
 - OB-EUR-H4 (the parts of the hazard that arise due to failures inside the trusted part of the channel)
- 12.3.1.4 The proof shall consider the Mission Profile defined in section 4 and may take account of the protective features inherent in ETCS as also identified in section 4.

12.4 Safety Requirements for the Trackside Subsystem

- 12.4.1.1 The hazard rate for the trackside system visited by a train in the reference mission, less those items forming the non trusted parts of the transmission system, must be shown not to exceed,

$$THR_{\text{trackside}} = 0.67 * 10^{-9} \text{ dangerous failures hour}^{-1}.$$

- 12.4.1.2 Where the dangerous failure is defined as,

Failure to provide information to the on-board supervision in accordance with the data advised to the trackside from external entities.

Note: External entities include the assumption that the on-board provides correct information to the RBC in level 2. If this is not the case, it shall be considered as part of the on-board hazard detailed in 12.3.1.2.

- 12.4.1.3 Each supplier shall prove the attainment of the $THR_{\text{trackside}}$, considering, in its specific analysis (e.g., fault tree) for the equipment taking into account the following events, as defined in Part 2
- RBC-2 and RBC-3 (Level 2 only)
- Or
- LEU-H4 (Level 1 only)
 - TR-EUR-H4 (Level 2 only) for the parts of the hazard that arise due to failures inside the trusted part of the transmission channel.
- 12.4.1.4 The proof shall consider the Mission Profile in section 5.3 and may take account of the protective features inherent in ETCS as identified in section 5.4.

12.5 Safety requirements for the Transmission Subsystems

12.5.1 Radio Transmission

12.5.1.1 The rate of occurrence of data corruption must be shown not to exceed,

$THR_{RTXcorruption} = 1 \cdot 10^{-11}$ Dangerous Failures hour⁻¹ due to the corruption of messages sufficient to be interpreted as consistent by the on-board kernel or the RBC kernel, resulting in ETCS exceeding its known speed and distance limits.

12.5.1.2 When taking into account the following events from Part 2

- TRANS-OB/RADIO-1
- TRANS-TS/RADIO-1

12.5.1.3 This figure includes the influence of the non-trusted parts of the transmission system in both the on-board and trackside. Therefore the same target applies to both the onboard and trackside non-trusted equipment as defined in section 6.2.1.

12.5.2 Balise Transmission

12.5.2.1 The rate of occurrence of data corruption must be shown not to exceed,

$THR_{BTXcorruption} = 1 \cdot 10^{-11}$ Dangerous Failures hour⁻¹ due to the corruption of messages sufficient to be interpreted as consistent by the on-board kernel resulting in ETCS exceeding its speed and distance limits

12.5.2.2 This figure includes the influence of the non-trusted parts of the transmission system in both the on-board and trackside. Therefore the same target applies to both the onboard and trackside non-trusted equipment as defined in section 6.2.1.

12.5.2.3 This same figure is deemed to be applicable to the loop.

12.5.2.4 In regard of message deletion, the rate of failure for a balise information point to become undetectable must be shown not to exceed,

$$\lambda_{IP} = 1.0 \cdot 10^{-9} \text{ Dangerous Failures hour}^{-1}.$$

In addition, the rate of failure for the on-board to fail to irradiate an information point or to detect the transmission from the information point must be shown not to exceed,

$$\lambda_{ONB} = 1.0 \cdot 10^{-7} \text{ Dangerous Failures hour}^{-1}.$$

Annex A - 8.2.1.8.

12.5.2.5 For cross talk in both the loop and the balise the derived figure is,

$$1.0 \cdot 10^{-9} \text{ Dangerous Failures hour}^{-1}.$$

12.6 Safety Requirements for External Entities

12.6.1 ETCS Dependencies

12.6.1.1 In the analyses, it has been identified that safety performance of the system where ETCS is applied from the perspective of a travelling passenger is crucially dependent upon the integrity of the information it receives from external entities.

12.6.1.2 The external entities can be considered in 2 parts

Those entities which form part of a harmonised ETCS system

Existing Entities that ETCS is required to interface with.

12.6.1.3 The external entities which form part of a harmonised ETCS identified in the analyses are

- Data Preparation
- System Deployment
- Train Data Engineering

12.6.1.4 The overall safety performance of ETCS is critically dependent on the Train Data entered and therefore the creation and entry process for such data must be commensurate with a SIL 4 system.

12.6.2 Integrity Requirements for Data Preparation

12.6.2.1 The collection, interpretation and allocation of data relating to the network must be undertaken to a quality level commensurate with the SIL 4 allocation to the ETCS equipment.

12.6.3 Integrity Requirements for System Deployment

12.6.3.1 The overall safety performance of ETCS is critically dependent on the Engineering and therefore the complete Engineering process must be of a quality commensurate with a SIL 4 system.

12.6.4 Integrity Requirements for the Data Engineering

12.6.4.1 The overall safety performance of ETCS is critically dependent on the Train Data that is entered. Therefore the complete Data Entry process from the creation of the train data through to confirmation that the data is correctly stored on-board must be of a quality commensurate with a SIL 4 system.



- 12.6.4.2 Thus for ETCS, the process of confirming that data is correctly stored on-board must be of a quality level commensurate with a SIL-4 system.



13. ANNEX A

Assessment of the Eurobalise & Euroloop Transmission Subsystems



1. TABLE OF CONTENTS

1. TABLE OF CONTENTS.....	56
2. SCOPE OF THE APPENDIX	58
3. INTRODUCTION.....	60
3.1 Application of the Balise Transponder.....	60
3.1.1 General Principles	60
3.2 The Balise as a Constituent	60
3.3 Probability of an Information Point becoming Undetectable	61
4. BALISE INFORMATION POINT HAZARDS	63
4.1 General.....	63
4.2 Initial Apportionment to TRANS-BALISE-1, -2 & -3.....	64
5. INHERENT PROTECTION AGAINST THE MIGRATION OF HAZARDS TRANS-BALISE-2 & -3.....	66
5.1 TRANS-BALISE-2 (Deletion).....	66
5.1.1 Background	66
5.1.2 TRANS-BALISE-2 with Linking.....	66
5.1.3 TRANS-BALISE-2 without Linking	67
5.1.4 Amended Apportionment to TRANS-BALISE-2	68
5.2 TRANS-BALISE-3 (Cross Talk).....	68
5.2.1 Background	68
5.2.2 TRANS-BALISE-3 with Linking.....	69
5.2.3 TRANS-BALISE-3 without Linking	70
5.2.4 Amended Apportionment to TRANS-BALISE-3	70
6. OPERATIONAL CONSIDERATIONS FOR TRANS-BALISE-2	72
6.1 General.....	72
6.2 The Probability of the On-Board Detecting an Information Point.....	73
6.3 Tolerable Rate for the Deletion of an Information Point.....	74
6.3.1 General	74
6.3.2 Deletion of Un-Linked Information Points when the On-Board Linking Checks are Active	74
6.3.3 Deletion of Information Points when the On-Board Linking Checks are not Active	74
6.4 Operational Moves Prior to the Establishment of Linking	75
6.4.1 General	75
6.4.2 Entry into an ETCS Area from an Unfitted Area.....	75
6.4.3 Train Authorised to Start in Staff Responsible	77



6.5	Non-linked Applications in Linked Areas	78
6.5.1	General Considerations	78
6.5.2	Temporary Speed Restrictions (TSR)	78
6.5.3	Shunting	79
6.6	Moves that Negate Linking	81
6.6.1	Start of Mission	81
6.7	Most Onerous Target for TRANS-BALISE-2	81
6.8	Preliminary Sensitivity Analysis	81
7.	OPERATIONAL CONSIDERATIONS FOR TRANS-BALISE-3	83
7.1	General	83
7.2	Start of Mission and Entry into ETCS Areas	83
7.3	Repositioning in Level 1	84
7.4	Worst Case Target	84
7.5	Sensitivity Analysis	84
7.5.1	Current Mission Profile	84
7.5.2	Other Mission Profiles	85
8.	APPORTIONMENT TRACKSIDE / ON-BOARD	86
8.1	Fault Tree for TRANS-BALISE-1 (Corruption)	86
8.2	Fault Tree for TRANS-BALISE-2 (Deletion)	87
8.3	Fault Tree for TRANS-BALISE-3 (Cross Talk)	90

2. SCOPE OF THE APPENDIX

2.1.1.1 This analysis is undertaken to derive the balise and loop subsystem targets for parameters that impact on the technical safety of ETCS. This analysis is based on clear assumptions to derive the maximum permissible rates for the following three balise subsystem transmission hazards as identified in parts 1 and 2 of this suite of documents. These are paraphrased as follows,

- Incorrect balise group or loop message received by the on-board kernel functions as consistent - (Corruption)
- Balise group not detected by the on-board kernel functions - (Deletion)
- Cross talk from an adjacent balise group or loop of a message received by the on-board kernel functions as consistent - (Insertion).

2.1.1.2 These three hazards are, where appropriate, apportioned between the on-board and trackside parts of the balise subsystem as tolerable failure rates for equipment that is sufficient to ensure technical interoperability.

2.1.1.3 The loop is included in this annex as its transmission characteristics are based on those of the balise.

2.1.1.4 The process adopted for the analysis is a step by step, top down apportionment from the THR_{BTX} as derived in the main body of the document, to the three hazards indicated. These figures are then put into the context of a balise group and the on-board part of the balise subsystem.

2.1.1.5 In undertaking this work it has become necessary to define the parts of the Eurobalise system more specifically. Thus the following terms are used in this report

Balise Transponder - The device mounted in the track

Balise Channel - The non-trusted part of the communication path established between the LEU or the fixed data in non variable balises, and the on-board kernel.

Information Point - A group of balise transponders numbering between 1 and 8. These together form a source of data to be transmitted to the on-board kernel.

Note: In this study the minimum number of balises forming a group is taken as 2. This is the minimum number recommended in the SRS where deletion could lead to a hazardous consequence.



Balise Subsystem - A global term to cover both the onboard and trackside parts inclusive of the air gap



3. INTRODUCTION

3.1 Application of the Balise Transponder

3.1.1 General Principles

- 3.1.1.1 The balise transponder is a versatile constituent within the ETCS as it can be used to perform many functions. In performing these functions the balise may be used either as a fixed data device or when used in conjunction with a Lineside Electronic Unit (LEU), the data can be varied. Balises may also be used singly or in groups of up to eight.
- 3.1.1.2 In this document a balise group is referred to as an Information Point. This is irrespective of the number of balises in the group. It is also irrespective of whether the balises have stored and fixed data or they are supplied from a LEU with variable data.
- 3.1.1.3 Information points may be deployed in a manner where they are marked internally as linked and when the on-board system checks this linking data it is able to anticipate an information point at a predefined position. This allows the on-board system to take a predetermined action (linking reaction) should it determine that it has not encountered the anticipated information point at the expected location.
- 3.1.1.4 When the on-board is using linking data it will also accept data from information points that are not marked as linked
- 3.1.1.5 Information points that are not marked as linked (un-linked) or when the on-board is not using the linking information, in both of these cases reliance is placed on the on-board system to detect the presence of an information point without any indication that such a point is expected.
- 3.1.1.6 The safety requirement for an information point will depend on the function that it is expected to perform in a specific application and whether linking is used or not. Safety requirements may also be influenced by which ETCS application level is being used.

3.2 The Balise as a Constituent

- 3.2.1.1 The track mounted balise transponder is the basic element in an information point. It is unidirectional device that transmits its telegrams 'on demand' as a train passes over it. There is no real time acknowledgement capability to determine if the telegrams transmitted have been received correctly.



- 3.2.1.2 The Eurobalise transmission forms a sub-system in its own right. In this study, events occurring in the non-trusted parts in both the balise and the on-board are considered.
- 3.2.1.3 The data in a balise is either, pre-programmed and fixed or is varied depending upon external conditions. On-board the received data is passed to the onboard kernel where a full message can be assembled from the totality of telegrams sent from a group of balises forming an information point. The on-board kernel makes checks on the consistency of the received message before utilising the information.
- 3.2.1.4 The balise channel forms a closed communications channel as covered by Cenelec EN50159 - 1.
- 3.2.1.5 In establishing the safety requirements for technical interoperability for a balise channel it is necessary to take the following sequential steps
- Identify the hazards related to an information point.
 - Develop a constituent based fault tree to link the information point hazards to link to the core hazard
 - Undertake a preliminary apportionment to the information point hazards
 - Make allowance for any inherent protection afforded ETCS that limits the migration of the information point hazards towards the core hazard and to amend the preliminary apportionment accordingly.
 - Undertake an operational analysis based on the agreed mission profile to determine worst case scenarios and their frequency of occurrence
 - Apportion tolerable failure rates between the trackside and on-board parts of the balise subsystem. In this respect the trackside part is the information point with apportionment to a single balise being undertaken by the Unisig Balise working Group for inclusion in Subset-036.

3.3 Probability of an Information Point becoming Undetectable

- 3.3.1.1 In the System Requirements Specification it is a requirement that an information point which contains information that if it is missed could lead to a hazardous consequence, must consist of a minimum of two balise transponders.
- 3.3.1.2 In this document it is always assumed that a critical information point consists of two transponders such that if one balise transponder fails then the remaining balise transponder is still available to be accessed by the on-board so that a safe reaction can be invoked.
- 3.3.1.3 The information point will fail when both balises are not detectable. The tolerable rate of this occurrence is denoted as λ_{IP}



- 3.3.1.4 The probability that an information point is not detectable (P_{IP}) when met by a train is the failure rate multiplied by the down time. This is valid when the down time is small with respect to the failure rate.
- 3.3.1.5 The mean down time for the group is T_D hours, where for the purposes of this analysis T_D is assumed to be on average 24 hours as noted in the Mission Profile. Thus,

$$P_{IP} = \lambda_{IP} * T_D h$$

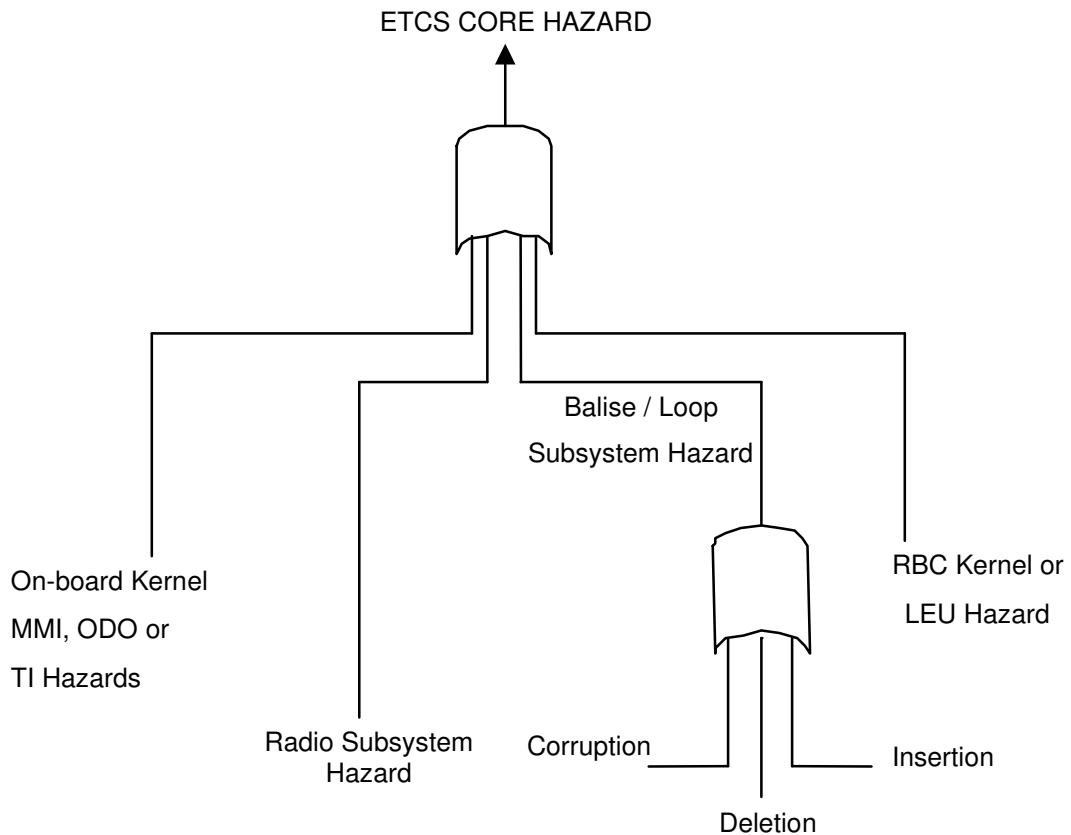
$$\underline{P_{IP} = \lambda_{IP} * 24h}$$

4. BALISE INFORMATION POINT HAZARDS

4.1 General

- 4.1.1.1 Three hazards have been identified as part of the Failure Modes and Effects Analysis (FMEA) on the transmission systems. These hazards are the base events of the functional fault tree in part 1 of Subset 088 where their influence in ETCS is shown. These hazards are now further analysed against specific ETCS modes utilising the work in part 2 of subset 088 where the protective features inherent in the current version of the ETCS system design were identified.
- 4.1.1.2 The identified system level transmission hazards that apportioning between the on-board and trackside are defined as,
- TRANS-BALISE-1 - Incorrect balise group message that is received by the on-board kernel functions as consistent - (Corruption)
 - TRANS-BALISE-2 - Balise group not detected by the on-board kernel functions - (Deletion)
 - TRANS-BALISE-3 - Inserted balise group message received by the on-board kernel functions as consistent - (Cross Talk).
- 4.1.1.3 For the loop the related transmission hazards are
- TRANS-LOOP-1- Incorrect loop message received by the on-board kernel functions as consistent - (Corruption)
 - TRANS-LOOP-3 - Inserted loop message received by the onboard kernel functions as consistent - (Cross Talk).
- 4.1.1.4 Note that the contribution from TRANS-BALISE-1 is required to be negligible with respect to TRANS-BALISE-2 & -3 due to the protection code applied to the transmitted telegrams.
- 4.1.1.5 The target for TRANS-BALISE-1 will be applicable to the corresponding loop hazard, TRANS-LOOP-1.
- 4.1.1.6 The case of the loop, deletion (an equivalent to TRANS-BALISE-2) is not considered as an issue as the loop is used to provide an infill function which, under certain conditions, will release the on-board equipment from a braking intervention. Thus as indicated in part 2 of this suite of documents, because the loop is used to transmit data that is less restrictive, deletion of a loop message will result in a failure on the safe side and therefore, is not considered to be a hazard.

4.1.1.7 Occurrence of any one of the hazards should not lead to ETCS exceeding the THR_{ETCS}



4.2 Initial Apportionment to TRANS-BALISE-1, -2 & -3

4.2.1.1 In the main body of the document it was determined that the contribution to the core hazard due to the radio system must be negligible. Thus, for both level 1 and level 2 the THR for the Balise / Loop subsystem becomes,

$$THR_{BTX} = 6.7 * 10^{-10} \text{ Dangerous Failures hour}^{-1}.$$

4.2.1.2 Initially this is split 50 / 50 between TRANS-BALISE-2 and TRANS-BALISE-3. This results in a THR to each hazard of,

$$\underline{TRANS-BALISE-2 = TRANS-BALISE-3 < 3.3 * 10^{-10} \text{ dangerous failures hour}^{-1} \text{ for level 1 \& level 2}}$$

This demands that TRANS 1 is negligible in relation to the target for TRANS 2 & 3. Thus the requirement is,

$$\underline{TRANS-BALISE-1 < 1.0 * 10^{-11} \text{ dangerous failures hour}^{-1} \text{ for level 1 \& level 2}}$$

4.2.1.3 Note that the apportionment between TRANS 2 & 3 is arbitrary at this stage and may be adjusted in the light of feasibility considerations.



- 4.2.1.4 Ongoing considerations only look at hazards TRANS-BALISE-2 & -3 on the basis that TRANS-BALISE-1 is required to be negligible with respect to TRANS-BALISE-2 & TRANS-BALISE-3. This is considered a valid requirement due to the powerful message coding strategy employed in the balise subsystem. Ultimately, it will be necessary to demonstrate that the selected and harmonised coding strategy is suitable for the defined noise environment.
- 4.2.1.5 In the case of the loop, the requirements as derived for the balise on corruption are deemed as applicable to the loop event.

5. INHERENT PROTECTION AGAINST THE MIGRATION OF HAZARDS TRANS-BALISE-2 & -3

5.1 TRANS-BALISE-2 (Deletion)

5.1.1 Background

- 5.1.1.1 This hazard can originate from either from the trackside or the on-board parts of the balise subsystem
- 5.1.1.2 The condition of the on-board kernel not being aware that it is passing over an information point is a potential hazard because of the lack of the acknowledgement path. This means that if an information point containing critical information is missed, the on-board kernel will remain in ignorance and the train will proceed using its existing information. If the missed data were more restrictive compared to that currently being supervised by ETCS e.g. Mode Change, then the core hazard could result
- 5.1.1.3 Thus it is necessary to consider the case when linking of information points is used and the on-board checks this linking. It is also necessary to consider when the linking is not used, either by the information points or when the on-board checking is not active.

5.1.2 TRANS-BALISE-2 with Linking

- 5.1.2.1 In the case of not detecting a linked information point with the on-board linking checks enabled, the on-board kernel linking reaction comes into play as mitigation when the on-board reaches the end of the expectation window.
- 5.1.2.2 If the information point is not missed but its presence is detected without being able to receive any valid data then the linking reaction will be applied. Thus detection of a linked information point allows the on-board kernel to take a defined action earlier than if the on-board kernel had allowed for all the odometer and positional tolerances before determining that an information point had been missed.
- 5.1.2.3 In the case where the information point is detected or completely missed and the option 'No Linking Reaction' is selected, the train will proceed until the on-board odometer indicates the end of a movement authority. In this case the on-board kernel would not have received more restrictive information contained in the linked information point and the core hazard would result.
- 5.1.2.4 Thus, the rule is proposed to protect against failures of the on-board,

The 'no reaction' option is not permissible in the case of linked balises containing data which if missed, could lead to the top hazard



5.1.2.5 A specific deployment could have many successive information points each with a 'no reaction' selection therefore the following rule is taken into account,

If two expected consecutive linked balise groups announced by linking are not detected (regardless of their defined linking reaction), the on-board shall consider the linking command of the second balise group as a command to apply the service brake.

The driver shall be informed of this specific linking reaction.

5.1.2.6 Subject to the distance between information points with an associated linking reaction and a corresponding danger point which makes allowance for the on-board tolerances due to the expectation window and odometer errors. There is no safety requirement in respect of not being able to detect an information point when linking is used.

5.1.2.7 Information points marked as un-linked will be read in this mode. If such an information point is detected but the data cannot be accessed, the service brake will be applied as required by the System Requirements Specification.

5.1.2.8 If the information point marked as un-linked is not detected there is no mitigation inherent in the ETCS equipment.

5.1.2.9 It is also clear that detecting an information point but being unable to decode the telegrams is not a safety hazard.

5.1.3 TRANS-BALISE-2 without Linking

5.1.3.1 In this instance with the on-board linking checks disabled, the on-board kernel has no expectation of meeting an information point irrespective if it is marked as linked or not, so a linking reaction is not possible. However the detection of an information point even if the data cannot be read does allow mitigating action, with an application of the service brake, to be invoked by the on-board kernel.

5.1.3.2 There is no inherent mitigation within ETCS if an information point is not detected in this situation.

5.1.3.3 Again, detection of an information point without being able to decode the telegrams is not a safety hazard as indicated in 5.1.2.7 and 5.1.2.9.

5.1.4 Amended Apportionment to TRANS-BALISE-2

5.1.4.1 The function of detecting the presence of an information point is a critical function and this function is most critical when information points are in applications where linking is not used.

As no mitigation is provided by the on-board kernel, the apportionment to TRANS-BALISE-2 based on the need to allow for applications where linking is not used remains as,

$3.3 * 10^{-10}$ dangerous failures hour⁻¹ due to deletion in both Level 1 and 2

5.1.4.2 It is clear that the occurrence of TRANS-BALISE-2 is dependent on the ability to detect information points in certain operational scenarios and the frequency that these scenarios are experienced.

5.2 TRANS-BALISE-3 (Cross Talk)

5.2.1 Background

5.2.1.1 The origin of this hazard is data being accepted by the on-board kernel that originates information points that are not relevant to the on-board kernel at the time of accepting the data. This could be because the data comes at the wrong time or because it comes from an unrelated location.

5.2.1.2 In order to be hazardous, the complete message from the erroneous information point must be received as a consistent message that, in turn results in a less restrictive train movement.

5.2.1.3 There are very specific failure modes where cross talk from an unrelated location can be generated. These modes are summarised as,

- A train on a track receiving data from an information point sited in an adjacent track due to either, increased on-board receiver sensitivity or increased transmission levels from the adjacent information point. This known as the single antenna case
- A train on a track that receives data from an adjacent track due to a train on the adjacent track powering the information point such that the first train reads the erroneous data. Again this could be due to either increased on-board receiver sensitivity or increased transmission levels from the adjacent information point. This is known as the double antennae case.

5.2.1.4 In some instances the likelihood of cross talk will be exacerbated and then carried over significant distances by cabling that conducts the interference and runs between several tracks. The cabling giving rise to this transversal cross talk is not necessarily



part of the balise subsystem deployment of the information points but could be associated with other trackside infrastructure items.

- 5.2.1.5 There is also potential for longitudinal cross talk when cables are laid in parallel with the track such that data from an irradiated information point is induced into the cable. This could result in data being transmitted along the cable such that a train not positioned over the information point reads the data at an inappropriate time and acts on the data. This is known as the 'mirage effect'.
- 5.2.1.6 Again the one or two antennae situations apply as a single antenna could, in theory transmit the transponder irradiating frequency along the cable to activate the transponders prematurely.
- 5.2.1.7 The conducted cross talk problems as outlined in 5.2.1.4 and 5.2.1.5 are both a safety hazard and a threat to operational reliability over wide area. It is exacerbated by the difficulty in detecting increased transmission levels from balise transponders
- 5.2.1.8 With the difficulty of defending against cross talk it is recommended that,

All possible precautions should be taken. Thus, where possible, information points must be positioned at a distance from the cable so that even with a maximum transmission level under failure conditions, cross talk cannot be induced into the cable.
- 5.2.1.9 In order to create the core hazard, data received from the erroneous information point by the on-board kernel must accepted as correct and when acted upon, must be such as to lead to the safe speed / distance profile as known by ETCS being exceeded.
- 5.2.1.10 The process adopted by the on-board kernel for determining the acceptability of a message depends whether on whether linking is being used and information points are anticipated or linking is not being used and therefore information points are not anticipated.
- 5.2.1.11 If the train merely detects the presence of information in the adjacent track without receiving valid data then the on-board will invoke a safe reaction and therefore this situation is not a safety hazard but it is an issue of operational reliability.
- 5.2.1.12 In the case of the loop, a loop message will not be accepted by the on-board unless a matching End of Loop Marker (EOLM) balise group as part of a linked chain is encountered first and duly accepted by the on-board. Thus, in the case of cross talk, to create a hazard will require valid messages to be received from both the EOLM and the loop itself which conspire to falsely release the train from a braking action. Thus cross talk in respect of the loop (TRANS-LOOP-3) is not considered to be a hazard due to the mitigation provided by the EOLM being deemed sufficient.

5.2.2 TRANS-BALISE-3 with Linking

- 5.2.2.1 When linking is being used the on-board kernel will not accept the data delivered from an information point until,



- The linking checks are passed (these include, the location of the information point being interrogated, its identity and the direction which the train should expect to pass over the information point) and,
- The telegrams received from the set of balise transponders forming the information point pass the message consistency checks.

5.2.2.2 Even if linking is active, the onboard kernel will still accept data from erroneous information points that are marked as not being linked. In order to be dangerous the telegrams need to pass the message consistency checks and be less restrictive.

5.2.2.3 This hazard rate would be reduced by the adoption of the rule, information points marked as non-linked must not contain a Movement Authority or other permissive data.

5.2.2.4 If the erroneous information point is itself part of a separate linked chain of information points and the on-board is checking linking information, then in order to be acted upon, both the linking and consistency checks must be passed. In this situation, the probability of cross talk resulting in a valid data leading to the core hazard is reduced relative to 5.2.2.2.

5.2.2.5 There are no inherent protective features which prevent ETCS acting on incorrect data resulting from cross talk once it has passed all the message consistency and linking checks

5.2.3 TRANS-BALISE-3 without Linking

5.2.3.1 In this instance, then clearly, there are no linking checks that will be applied by the on-board kernel. However the checking of message consistency by the on-board kernel is still possible across balise transponders forming an information point.

5.2.3.2 In this case, the system is at its most vulnerable to cross talk.

5.2.4 Amended Apportionment to TRANS-BALISE-3

5.2.4.1 The consideration regarding TRANS-BALISE-3 is that the inserted message passes all of the on-board tests outlined above therefore, in this case no mitigation from the on-board kernel can be claimed.

5.2.4.2 Since the on-board kernel is expected to respond to non-linked information points even when linking is active, no extra mitigation can be claimed due to the linking of information points that the train legitimately traverses.

5.2.4.3 Thus the maximum tolerable rate for cross talk leading to the core hazard from adjacent information points encountered in 1 hour.

TRANS-BALISE-3 < 3.3 * 10⁻¹⁰ dangerous failures hour⁻¹ for Cross Talk in both level 1 and 2



- 5.2.4.4 This figure therefore becomes the preliminary THR for TRANS-BALISE-3 relative to the information points encountered in a 1-hour journey.
- 5.2.4.5 The occurrence of TRANS-BALISE-3 is modified by the frequency of operational scenarios where linking checks are not used, the specific situations given in section 7 and by the number of adjacent information points susceptible to creating a cross talk hazard in certain operational modes.
- 5.2.4.6 The modes to be considered in section 7 of this annex are identified as,

When operating in Staff Responsible where the on-board linking checks are disabled

When operating in level 1 under Full Supervision and where information points are used for repositioning.



6. OPERATIONAL CONSIDERATIONS FOR TRANS-BALISE-2

6.1 General

- 6.1.1.1 It has been identified that ETCS is at a greater risk of creating the hazard TRANS-BALISE-2 in situations where it has to rely on non-linked information points.
- 6.1.1.2 In order to understand the frequency of occurrence of the hazard it is necessary to review the usage of non-linked information points to identify if they pose a safety-related hazard and if they do, how often will this hazard be experienced in a typical 1-hour journey.
- 6.1.1.3 This analysis assumes each event considered leads inevitably to the core hazard. Thus the analysis is very conservative.
- 6.1.1.4 Thus the following scenarios are examined
- Operational moves prior to the establishment of linking
 - Non-linked information points in a generally linked network
 - Moves which negate linking
- 6.1.1.5 The calculations herein are based on a mission profile for a one-hour journey. This mission profile is detailed in the main body of the document.
- 6.1.1.6 Key parameters utilised in the analysis are,
- Ratio of linked information points to non-linked - 1000 to 1
 - Average number of information points passed in a 1 hour journey - ~400.
 - Average time to travel between information points - 1/400 hours.
 - Number of non-linked information points encountered in 1 hour - 0.4
- 6.1.1.7 In addition, there is the existing Unisig imposed constraint that an information point will consist of a minimum of two balise transponders where a failure to detect that information point would lead to a hazardous condition.

6.2 The Probability of the On-Board Detecting an Information Point

6.2.1.1 Denoting the rate of occurrence of the on-board receiver being unable to detect an information point as λ_{ONB} .

6.2.1.2 If linking is assessed by the on-board, the duration of the on-board failure is limited to the time between 2 consecutive information points marked as linked, such as a safe reaction is activated if the second is missed (see 7.2.1.4). Thus if the average speed of the train is V km/h and the distance between such linked information points is D_L kilometres, the fault duration time becomes

$$D_L/V = T_L \text{ hours}$$

6.2.1.3 Thus the probability of the on-board failing to detect a working and linked information point is,

$$P_D = \lambda_{ONB} * (D_L/V)$$

6.2.1.4 Normally in assessing the distance between linked information points it will be necessary to take account of the on-board linking reaction. In level 2 only 10% of information points will have a 'brake intervention if not detected' instruction associated with them. In level 1 this percentage is assumed to rise to 50%. However an 'additional linking reaction' rule is used (see 5.1.2.5) such that if 2 consecutive linked information points are missed the on board applies the service brake. Thus D_L becomes twice the average distance between linked balise groups, namely 1km.

6.2.1.5 When the on-board linking checks not active, the duration of an onboard failure, T_{NL} , needs to be estimated according to the prevailing operational conditions. It is the time since the on-board was last proved to be working and as this is operationally dependent, this may in some instances be an extended period.

6.2.1.6 The deletion of information points used to provide an infill function is not considered a hazard, as such an arrangement is not used to provide more restrictive information to the on-board.

6.2.1.7 When balises are used markers to advise of either a section of radio infill or loop infill, then deletion in this case would result in missing the infill information. Again, this is not a hazard due the infill systems not being used to transmit data that is more restrictive than that held by the onboard.



6.3 Tolerable Rate for the Deletion of an Information Point

6.3.1 General

- 6.3.1.1 An information point will not be detected and no linking reaction applied if,
- a) The information point is not linked AND (either, the un-linked information point has failed OR the on-board receiver is unable to detect balise transponders)
 - b) The on-board equipment does not use linking information AND (either, the information point has failed OR the on-board receiver is unable to detect balise transponders)

6.3.2 Deletion of Un-Linked Information Points when the On-Board Linking Checks are Active

- 6.3.2.1 This is the case indicated at a) in 6.3.1.1.
- 6.3.2.2 If the average train speed is V km/h. and the distance between un-linked information points is D_U kilometres, the rate of meeting un-linked information points is

$$V / D_U \text{ non-linked information points hour}^{-1}$$

- 6.3.2.3 The probability that the information point is not detectable, P_{IP} , is as derived in 3.3.1.5 based on the assumption that the mean down time for a balise group is 24 hours.

- 6.3.2.4 The probability that the on-board receiver is unable to detect balise transponders is

$$\lambda_{ONB} * D_L/V$$

As defined in 6.2.1.3.

- 6.3.2.5 Thus, the tolerable rate of occurrence of TRANS-BALISE-2 (R_L), the deletion of an unlinked information point when linking checks are active, is given by

$$R_L = (\text{Rate of meeting non-linked information points}) *$$

$$((\text{Probability of Balise Group Failure}) + (\text{Probability of the on-board failing to Detect}))$$

Giving,

$$\underline{R_L = V/D_U * ((\lambda_{IP} * 24h) + (\lambda_{ONB} * D_L/V))}$$

6.3.3 Deletion of Information Points when the On-Board Linking Checks are not Active

- 6.3.3.1 This corresponds to case b) in 6.3.1.1.

- 6.3.3.2 The rate of meeting information points when linking is not being used (r_{NL}) needs to be estimated in accordance with operational conditions (frequency of Start of Mission, frequency of Staff Responsible operations, frequency of entry into ETCS areas from unfitted areas, etc)
- 6.3.3.3 Operational conditions will need to be considered to estimate the probability that and the probability of driver errors (P_{DR}) influence the outcome.
- 6.3.3.4 The probability of that an information point is not detectable remains as P_{IP} as derived earlier and the rate that the on-board receiver fails to detect balise transponders is,

$$\lambda_{ONB} * T_{NL}$$

where T_{NL} is defined in 6.2.1.5 as the duration of an on-board failure when on-board linking checks are not active.

- 6.3.3.5 The result is that the rate of occurrence of the hazard TRANS-BALISE-2, deletion of a balise group when linking is not being checked is,

$$R_{NL} = (\text{Rate of meeting information points} * \text{Event frequency qualifiers}) *$$

$$((\text{Probability of Balise Group Failure}) + (\text{Probability of the on-board failing to Detect}))$$

Giving

$$R_{NL} = r_{NL} * P_{DR} * ((\lambda_{IP} * 24h) + (\lambda_{ONB} * T_{NL}))$$

6.4 Operational Moves Prior to the Establishment of Linking

6.4.1 General

- 6.4.1.1 For the scenarios considered in this section, the formula derived at 6.3.3.5 is applicable.

6.4.2 Entry into an ETCS Area from an Unfitted Area

- 6.4.2.1 For the purposes of this analysis it is assumed that the unfitted area has no ATP
- 6.4.2.2 In this case a train will have been operating in the unfitted area in the Unfitted mode of ETCS. In these modes the on-board kernel will supervise the driver to ensure that he does not exceed a predetermined speed.
- 6.4.2.3 Although not part of the Unisig considerations, it is assumed that entry of a train into a level 1 or level 2 equipped area will be controlled by a line side entry signal.
- 6.4.2.4 In both level 1 and level 2 the ETCS fitted train will need to read an initial information point when the linking checks on-board are disabled in order to get information regarding the ETCS application level, the route ahead and any linking information



relevant to subsequent information points. If the information is missed then the train will remain in 'Unfitted' mode and will respect the aspect of the entry signal.

- 6.4.2.5 If this entry information point has not been detected by the on-board kernel and the order to switch to an ETCS level or to contact a RBC has not been received, a potential hazard would result if the driver passes the signal whilst it remains at danger.
- 6.4.2.6 There is also the situation where entry into an ETCS area is authorised even though the entry information point has not been successfully interrogated. In this case, if the driver has not noticed the failure of the MMI to indicate the expected change of mode, the train will continue in 'Unfitted' mode.
- 6.4.2.7 For the authorisation to be given, the route must be clear up to the next signal even so, though the speed of the train maybe excessive. In level 1 without lineside signals and level 2 the train may continue for some considerable distance particularly if the problem is as a result of a permanent failure of the on-board system.
- 6.4.2.8 Thus there is a limit on the non availability of both the trackside and on-board parts of the balise subsystem in these scenarios dictated by the desire not to exceed the TRANS-BALISE-2 target for non-linked information points in level 2.
- 6.4.2.9 It is assumed that there is 1 entry into an ETCS area from an unfitted area once in a typical 1-hour journey and that 1 in 1000 times the driver will try and pass the unprotected entry signal at danger. Or, 1 in 1000 times the entry information point will be missed by the on-board when an authority is given to proceed coupled with a lack of driver observation in noting that a level transition has not been made.
- 6.4.2.10 It is noted that the on-board part may not have shown to be working for some considerable time. However an average figure of 1 hour is thought to be a reasonable assumption to make for this analysis.
- 6.4.2.11 Thus the following parameters are relevant,
- $T_{NL} = 1 \text{ hour}$
- $r_{NL} = 1 \text{ hour}^{-1}$
- $P_{DR} = 10^{-3}$
- 6.4.2.12 Thus, bearing in mind the two possible scenarios, in order to satisfy the TRANS 2 requirement on the balise sub system becomes,

$$3.3 * 10^{-10} \text{ hour}^{-1} = 1.0 * 10^{-3} ((\lambda_{IP} * 24h) + (\lambda_{ONB} * 1h))$$

$$3.3 * 10^{-7} \text{ hour}^{-1} = 24\lambda_{IP} + \lambda_{ONB}$$

Where the result is sensitive to the assumptions made about the time the since the on-board was last proved to be working and the rate of driver error.

- 6.4.2.13 It is noted that the scenarios could be improved with a procedure that prevented entry into an ETCS area where mixed traffic is not permitted, such as level 2 without optical signals. Such a procedure should prevent unfitted trains or trains with a failed on-board subsystem entering the ETCS area and only authorise entry to trains with a working on-board subsystem.

Note: For example the operational rules could allow the driver to pass a special indication, marking the entry in ETCS area, only if a Level Transition is indicated on the MMI.

6.4.3 Train Authorised to Start in Staff Responsible

- 6.4.3.1 Authorisation to move under Staff Responsible can be required as part of a journey possibly due to external system failures. Such authorisation is normally only given when the route ahead is believed to be free
- 6.4.3.2 In the Staff Responsible mode, the on-board does not check the linking of information points.
- 6.4.3.3 In level 1, the train relies on reading an information point to be able to be advised of a movement authority distance. This authority will provide the national value ceiling speed.
- 6.4.3.4 Thus in level 1, there is no protection provided by ETCS against a driver passing a signal at danger and the train will continue in Staff Responsible with a limit on the achievable ceiling speed being enforced by the on-board kernel. In addition there will be no expectation of subsequent information points, as any linking information contained in the first information point will have been missed.
- 6.4.3.5 It is assumed that in level 1 applications without line side signals that there is some external marker to indicate stopping points but clearly it will not display any aspect information. Therefore it is assumed that the driver will be authorised by operational procedures outside the scope of this document.
- 6.4.3.6 Assuming the event of entering Staff Responsible occurs once every hour and driver tries to pass a signal at danger once every 1000 times and that the rate of meeting information points, r_{NL} remains at 1 every hour. In addition, T_{NL} as the time of exposure to an on-board failure could be an extended period but 1-hour is assumed. Therefore, the tolerable rate for level 1 is,

$$3.3 * 10^{-10} \text{ hour}^{-1} = 1 * 10^{-3} * ((\lambda_{IP} * 24h) + (\lambda_{ONB} * 1h))$$

$$3.3 * 10^{-7} = (\lambda_{IP} * 24) + (\lambda_{ONB})$$

- 6.4.3.7 In level 2, entry into Staff Responsible will result in the train and supervising to the national ceiling speed and a given distance as supplied via the radio system. Thus the train will be trapped if it tries to exceed these limits as governed the odometry or it detects an information point instructing 'Stop if in Staff Responsible'. Although



operating at a reduced speed, failing to read an information point situated within the authorised distance to run that instructs the train to stop could be critical.

6.4.3.8 The train may also be provided with a list of information points that it can pass and the direction in which they may be traversed. When no such list is sent the train may pass over all information points to the limit of its movement authority.

6.4.3.9 Thus the critical situation in level 2 will be the frequency of entering Staff Responsible at 1.0 / hour modified by the frequency that the permitted distance is allocated beyond information points containing stop orders. The frequency of occurrence for this event is not clear since it is assumed that such an authorisation would be an error. However, it is assumed here to be 1 every 1000 times that Staff Responsible is entered.

6.4.3.10 This time the sum to be balanced becomes for level 2 is as before,

$$3.3 * 10^{-10} \text{ hour}^{-1} = 1 * 10^{-3} * ((\lambda_{IP} * 24h) + (\lambda_{ONB} * 1h))$$

6.4.3.11 Rearranging gives

$$3.3 * 10^{-7} \text{ hour}^{-1} = 24\lambda_{IP} + \lambda_{ONB}$$

6.4.3.12 This calculation is most sensitive to the rate of occurrence assumed. It is also sensitive to a lesser extent, to the assumption made about a reduced speed.

6.5 Non-linked Applications in Linked Areas

6.5.1 General Considerations

6.5.1.1 In the following analyses it is assumed that the train is working in a predominantly linked area and that the formula derived in 7.3.2.5 applies.

6.5.2 Temporary Speed Restrictions (TSR)

6.5.2.1 Temporary Speed Restrictions are applied to speed of traffic due to for example, the need to protect workers on an adjacent track or when some infrastructure damage has occurred.

6.5.2.2 Adherence to a TSR is clearly a safety issue, as missing the information will lead directly to the core hazard of ETCS.

6.5.2.3 In level 1 it is expected that un-linked information points will be used to announce the commencement of TSR's.

6.5.2.4 In level 2, TSR's will predominately, be issued as a movement authority from the Radio Block Centre. In this case it is possible to confirm successful receipt of the data with an acknowledgement from the on-board kernel.

6.5.2.5 It is permissible however to use un-linked information point based TSR's in level 2 and therefore it is the application of balise transponders in his role that creates the most demanding target.

6.5.2.6 The number of TSR's that a train might meet in a one-hour journey would vary with the type of railway and quite probably, the country. The initial assumption made here is that the 1 to 1000 ratio from the mission profile applies. This gives an hourly rate of occurrence of

$$400/1000 \sim 0.4 \text{ TSR's hour}^{-1} = r_{NL}$$

6.5.2.7 The exposure time to on-board failures is based on the time between linked balises with a linking reaction. It is assumed that only 10% of the information points i.e. 40 information points have such a reaction in level 2. Thus $T_L = 10/400 = 0.025$ hours.

6.5.2.8 Given the $3.3 * 10^{-10}$ / hour figure for TRANS 2, the requirement for a TSR becomes

$$3.3 * 10^{-10} \text{ hour}^{-1} = 0.4 (24h\lambda_{IP} + 0.025h \lambda_{ONB})$$

Rearranging gives

$$8.25 * 10^{-10} \text{ hour}^{-1} = 24\lambda_{IP} + 0.025 \lambda_{ONB}$$

Where the equation is sensitive to the number of TSR's experienced in one hour

6.5.2.9 If the additional linking reaction (see 5.1.2.5) is taken into account the equation to be balanced would assume every other information point had a linking reaction so T_L is the time to traverse 2 information points when it takes 1 hour to cover 400.

$$8.25 * 10^{-10} \text{ hour}^{-1} = 24\lambda_{IP} + 0.005 \lambda_{ONB}$$

6.5.3 Shunting

6.5.3.1 Shunting is a specific ETCS operational mode where the boundaries of shunting are delineated by unlinked information points. It must be noted that, in Shunting mode, the on-board does not use linking information.

6.5.3.2 The issue we are concerned with when a failure to detect the delineating information point by the shunting entity results in an accident involving a passing passenger train. This affects both levels 1 and 2.

6.5.3.3 This accident scenario depends the number times a passenger train would expect to pass a shunting zone in a 1 hour journey. This then takes account of the time taken to pass the shunting area, the likelihood of a shunting operation being underway at the time of passing and the likelihood of the shunting train trying to exceed the limit of shunt area under ETCS protection.

6.5.3.4 Assume there is 1 shunting area and it takes 6 minutes to pass it (1/10 hour). In addition there is a 1 in 10 chance of shunting being underway and of those shunting



operations, 1 in 100 results in the driver responsible for shunting exceeding his shunt limits. Coupled to this must be the probability of an ETCS failure of $2.0 * 10^{-9} \text{ hour}^{-1}$. Thus the TRANS-BALISE-2 limit applicable to shunting can be calculated on the level 1 preliminary apportionment,

$$(3.3 * 10^{-10} \text{ hour}^{-1}) * (10 * 10 * 100 * 2.0 * 10^{-9})$$

Becomes

$$6.6 * 10^{-19} \text{ hour}^{-1}$$

- 6.5.3.5 However, ETCS can only provide a limited protection against accident scenarios with loose wagons and therefore can only be considered to provide a small adjunct to other and more comprehensive protective operational measures.

6.6 Moves that Negate Linking

6.6.1 Start of Mission

- 6.6.1.1 If the train makes a change in the direction of travel between linked balises then the stored linking data becomes invalid and is erased from the on-board kernel.
- 6.6.1.2 The driver will be in Staff Responsible mode until reaching an initial and non-linked information point and therefore the analysis at 6.4.3 is applicable with the extended detection time for the on-board down time of 1 hour, however this makes the rate of occurrence as twice giving,

$$3.3 * 10^{-10} \text{ hour}^{-1} = 2.0 * 10^{-3} ((\lambda_{IP} * 24\text{h}) + (\lambda_{ONB} * 1\text{h}))$$

$$1.6 * 10^{-7} = 24\lambda_{IP} + \lambda_{ONB}$$

6.7 Most Onerous Target for TRANS-BALISE-2

- 6.7.1.1 The most onerous target to be taken forward is the one that gives the most challenging failure rate figures. At this stage, it is the figure derived from considering a Temporary Speed Restriction applied as an un-linked information point. This gives a tolerable target for the information point, given the range of application defined in the mission profile, as

$$\underline{8.25 * 10^{-10} \text{ dangerous failures hour}^{-1} = 24\lambda_{IP} + 0.005\lambda_{ONB}}$$

6.8 Preliminary Sensitivity Analysis

- 6.8.1.1 This preliminary sensitivity analysis is undertaken prior to the detailed THR calculations to determine if there are any further factors that need to be taken into account prior to deciding on the worst case to be taken forward.
- 6.8.1.2 Calculations on the tolerable failure rate for Entry into an ETCS Area are dependent on the assumptions made on the rate driver error. In the current analysis this is applied as a probability, which implies the effect is a random one, and can be averaged over a whole journey. However, it is only likely to be probabilistic against specific locations. Even this ignores emotional issues.
- 6.8.1.3 The overriding purpose of ETCS is to protect against Driver Error. In the case of Entry into an ETCS area there is room for a clarification of both operational and technical procedures to ensure that only fitted and operational trains are authorised to pass the entry point.

- 6.8.1.4 If the entry procedures are tightened up to eliminate the driver error element then the sensitivity is reduced to the number of times the scenario is enacted. In this respect once per hour seems entirely reasonable.
- 6.8.1.5 The other variables that can have an effect are those allocated to the down time for an information point and the down time of the onboard part of the balise sub-system. The greater implication is the need for a fault detection and reporting system.
- 6.8.1.6 In considering operation in Staff Responsible, it is again the assumed failure rate for the driver that dominates the calculation. There is room for clearly defining the responsibility allocated to driver when Staff Responsible and also providing strict limits on the distances that a Staff Responsible move is valid for.
- 6.8.1.7 The target for the Temporary Speed Restriction failure rate has been achieved based on 1 TSR being experienced every 2.5 hours of operation. This frequency of TSR may be appropriate for dedicated high-speed lines but does not take account of the many mixed traffic lines on older infrastructure where a rate of 1 TSR every hour maybe a more applicable figure.
- 6.8.1.8 In general the TSR is very sensitive to the rate of occurrence of the restriction and the on-board requirement is sensitive to the rate of detection of linked information points that have a defined safe reaction.
- 6.8.1.9 Assumptions made about the average down time for an information point seem entirely reasonable subject to an adequate fault reporting system and maintenance regime. Extended down times in critical areas will detract from the system safety.



7. OPERATIONAL CONSIDERATIONS FOR TRANS-BALISE-3

7.1 General

- 7.1.1.1 The operational scenarios vulnerable to cross talk have been identified in section 6.2 and these are now analysed in the context of the mission profile starting from the preliminary derivation of,

$$3.3 * 10^{-10} \text{ dangerous failures hour}^{-1}$$

7.2 Start of Mission and Entry into ETCS Areas

- 7.2.1.1 Start of Mission may commence in Staff Responsible. This is summarised in section 7.4.2.
- 7.2.1.2 When entering a level 1 area from an unfitted area the reading of an adjacent information point consisting of a minimum of 2 balises could result in the train obtaining a false proceed permission, a false speed profile or false distance, any or all of which leading to the core hazard.
- 7.2.1.3 The likelihood of this occurring could be as a result of the situations outlined in section 6.2.1. The occurrence of the double antennae case or the existence of cabling likely to conduct cross talk when the information point has an excessive transmit level will be very specific to a network.
- 7.2.1.4 In the Staff Responsible mode the on-board will accept any information as long as it passes the message consistency checks. Therefore the vulnerability of the system depends on the frequency on the duration that the system is in Staff Responsible and the likelihood that there is an adjacent information point during this period.
- 7.2.1.5 The situation of the two antennae problem is likely to be experienced in area where traffic density is high such as the approaches to large stations

From the Mission profile the time spent in Staff Responsible is 3% of the 1 hour journey time (~ 2 minutes)

The number of potentially hazardous adjacent information points encountered whilst in Staff Responsible is clearly application specific but is assumed to be 50% of the information points encountered because of the traffic density consideration. Thus the exposure is for 1.5% of the time

- 7.2.1.6 Thus a target can be derived as,

$$3.3 * 10^{-10} * 100/1.5, \text{ giving}$$

$$\underline{2.2 * 10^{-8} \text{ dangerous failures hour}^{-1} \text{ due to cross talk.}}$$

7.2.1.7 The exposure time to the resulting hazard will be dependent upon driver vigilance

7.3 Repositioning in Level 1

7.3.1.1 In level 1 when an information point marks the entry into several possible routes the information provided to the train defines the static speed as the lowest of all of the possible routes. This is coupled with the distance to the farthest repositioning information point. However, in order for the train to take the route that is actually set it will accept information from the first repositioning point it reads

7.3.1.2 In this case a hazard could result if an incorrect repositioning point was read that provided a less restrictive movement such as an excessive speed for the intended route

7.3.1.3 Again, the likelihood of this effect occurring could be as a result of the situations outlined in section 6.2.1. The occurrence of the double antennae case or the existence of cabling likely to conduct cross talk when the information point has an excessive transmit level will be very specific to a network and does not yield to a probabilistic approach.

7.3.1.4 Thus the requirement is derived taken into account that this hazard be mitigated by the additional rule,

If 2 consecutive repositioning information points are found, this shall result in activation of the service brake by the on-board until the train is at a standstill. When at standstill the EoA shall be withdrawn to the current head of the train and the Driver informed.

This rule eliminates the hazard.

7.4 Worst Case Target

7.4.1.1 The target taken forward is,

$1.0 * 10^{-8}$ dangerous failures hour⁻¹ due to cross talk.

7.5 Sensitivity Analysis

7.5.1 Current Mission Profile

7.5.1.1 This preliminary sensitivity analysis is undertaken prior to the detailed THR calculations to determine if there are any further factors that need to be taken into account prior to deciding on the worst case to be taken forward.

7.5.1.2 In theory the system is sensitive to cross talk

7.5.1.3 Since the risk of its occurrence cannot be quantified and the exposure times to failed ETCS components could be excessive due the problem of detecting the origin of the



failure. It is essential that great care be exercised in the placement of balise transponders by keeping as far away from conductive cables as much as possible.

7.5.2 Other Mission Profiles

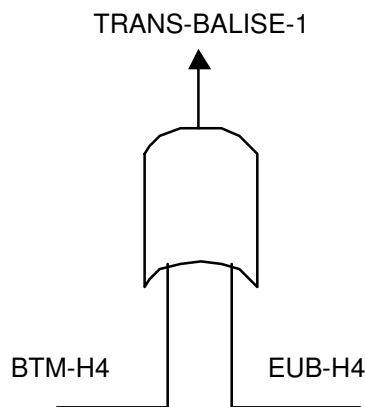
7.5.2.1 In a conventional railway with its greater traffic density and more complex layout, the opportunities for cross talk seem greater. Thus the final target is further amended to,

$1.0 * 10^{-9}$ dangerous failures hour⁻¹ due to cross talk.

8. APPORTIONMENT TRACKSIDE / ON-BOARD

8.1 Fault Tree for TRANS-BALISE-1 (Corruption)

8.1.1.1 The Fault Tree for TRANS-BALISE-1 is shown below where it breaks out into the on-board and trackside contributions to corruption.



8.1.1.2 The subordinate hazards to TRANS-BALISE-1 are defined as

BTM-H4: Transmission to the on-board kernel of an erroneous telegram, interpretable as correct, due to a failure within the on-board BTM function.

EUB-H4: Transmission of an erroneous telegram, interpretable as correct, due to a failure within the balise.

8.1.1.3 From previous assumptions were it was noted that the requirement on TRANS-BALISE-1 was for it to be negligible with respect TRANS-BALISE-2 & TRANS-BALISE-3 we derive the maximum tolerable rate for Corruption as,

$1.0 * 10^{-11}$ dangerous failures hour⁻¹ due to the corruption of messages sufficient to be interpreted as consistent by Kernel resulting in ETCS exceeding its known speed and distance limits.

8.1.1.4 The same target for corruption is applied to the loop where the subordinate events to TRANS-LOOP-1 (the loop equivalent of TRANS-BALISE-1) are,

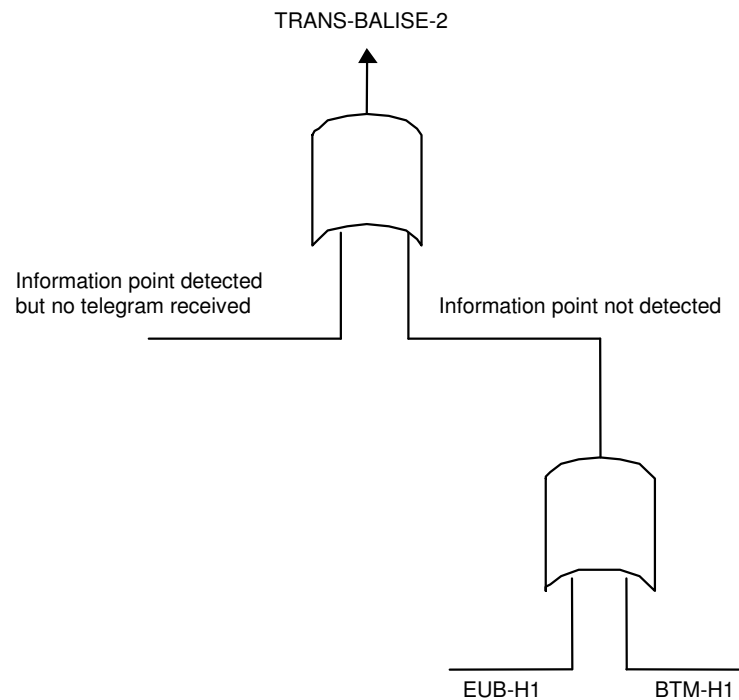
LTM-H4 Transmission to the on-board kernel of an erroneous telegram, interpretable as correct, due to failure within the on-board LTM function

LO-H4 Transmission of an erroneous telegram interpretable as correct, due to failure within a Loop

- 8.1.1.5 Note: For both the balise and the loop, the quality of the selected coding strategy for protection against interference in the air gap is believed sufficient to ensure that achievement of this degree of protection can be allocated equally to the non trusted parts of the on-board and balise / loop.

8.2 Fault Tree for TRANS-BALISE-2 (Deletion)

- 8.2.1.1 The Fault Tree for TRANS-BALISE-2 is shown below. The reference to on-board in the fault tree relates to that part of the balise channel that resides on the train.



- 8.2.1.2 It has been shown that detection of an information point without being able to interpret the telegram is not a hazard. Therefore no safety related target is apportioned to this part of the fault tree.
- 8.2.1.3 The subordinate events contributing to the failure to detect an information point are defined as,
- BTM-H1: A balise group is not detected, due to a failure within the on-board BTM function.
- EUB-H1: A balise group is not detected due to failure of a balise group to transmit a detectable signal.
- 8.2.1.4 Note: As indicated earlier, there is no hazard associated with deletion for the loop as it is used to transmit data that is less restrictive to the onboard.

- 8.2.1.5 In considering the part of the fault tree, 'information point not detected', the whole of the most onerous figure derived for TRANS-BALISE-2 is allocated to this hazard. Thus,

$$8.25 * 10^{-10} \text{ dangerous failures hour}^{-1} = 24\lambda_{IP} + 0.005\lambda_{ONB}$$

Thus,

$$4.2 * 10^{-10} = 24h\lambda_{IP} \quad \&$$

$$4.2 * 10^{-10} = 0.005\lambda_{ONB}$$

Which results in the two targets

- 8.2.1.6 The maximum Tolerable Failure Rate for an information point to be undetectable due to technical failures is

$$THR_{IP} = 1.75 * 10^{-11} \text{ Failures hour}^{-1}$$

- 8.2.1.7 The maximum tolerable rate for the on-board to fail to irradiate an information point or to detect the transmission from an information point is derived as,

$$THR_{ONB} = 0.84 * 10^{-7} \text{ Failures hour}^{-1} = THR_{BTM-H1}$$

- 8.2.1.8 The figures derived are not fully compatible with the feasibility of the interoperability targets for balise detection that have been concluded to be

$$\lambda_{BTM_H1} = 1.0 * 10^{-7} \text{ Failures hour}^{-1}$$

$$\lambda_{EUB_H1} = 1.0 * 10^{-9} \text{ Failures hour}^{-1}$$

- 8.2.1.9 For the onboard it is judged that the difference between the derived target and that which is feasible is negligible. Therefore, $\lambda_{BTM_H1} = 1.0 * 10^{-7} \text{ Failures hour}^{-1}$ is the requirement carried forward.

- 8.2.1.10 For the track mounted balise group it becomes necessary to use two separate balise groups in order to meet the target of $THR_{IP} = 1.75 * 10^{-11} \text{ Failures hour}^{-1}$ given in 8.1.2.6. Therefore the following requirement is derived.

When reliance is placed on the detection of unlinked balise groups for the announcement of Temporary Speed Restrictions, it is required that two separate balise groups are used each with a minimum of two balises.

- 8.2.1.11 This is motivated by the fact that the derived THR of $1,75 \cdot 10^{-11}$ Failures hour⁻¹ will then not be the requirement for a single balise group, but rather for the combination of failures in the two balise groups. Assuming independence between the two groups:

$$\text{THR}_{\text{IP}} = \text{THR}_{\text{EUB-H1}}^2 \cdot \text{MDT}_{\text{BG}}$$

$$1.75 \cdot 10^{-11} \text{ Failures / hour} = \text{THR}_{\text{EUB-H1}}^2 \cdot \text{MDT}_{\text{BG}}$$

where MDT_{BG} is the mean down time for the first failed balise group. So, even if having a very long MDT_{BG} , the resulting $\text{THR}_{\text{EUB-H1}}$ doesn't become very demanding. For example, with an MDT_{BG} of 4 weeks, the $\text{THR}_{\text{EUB-H1}}$ equates to $2 \cdot 10^{-7}$ Failures hour⁻¹, far less demanding than the feasible 10^{-9} Failures hour⁻¹.

- 8.2.1.12 As a consequence of the requirement 8.2.1.10 the TSR scenario ceases to be the most onerous target for a balise group. Instead, according to section 6.6.1.2, the Start of Mission scenario will be most onerous where,

$$1.6 \cdot 10^{-7} \text{ dangerous failures hour}^{-1} = 24\lambda_{\text{IP}} + \lambda_{\text{ONB}}$$

Substituting for λ_{ONB} with $1.0 \cdot 10^{-7}$ as the feasible limit, gives a maximum Tolerable Failure Rate for a balise group to be undetectable due to technical failures as

$$\text{THR}_{\text{EUB-H1}} = 2.5 \cdot 10^{-9} \text{ Failures hour}^{-1}$$

- 8.2.1.13 As this is only slightly less demanding than the feasible 10^{-9} Failures hour⁻¹ it has been decided to use as the requirement to carry forward

$$\text{THR}_{\text{EUB-H1}} = 1.0 \cdot 10^{-9} \text{ Failures hour}^{-1}$$

- 8.2.1.14 So, in summary, the following two requirements for technical interoperability are finally concluded as,

$$\underline{\text{THR}_{\text{BTM-H1}} = 1.0 \cdot 10^{-7} \text{ Failures hour}^{-1}}$$

$$\underline{\text{THR}_{\text{EUB-H1}} = 1.0 \cdot 10^{-9} \text{ Failures hour}^{-1}}$$

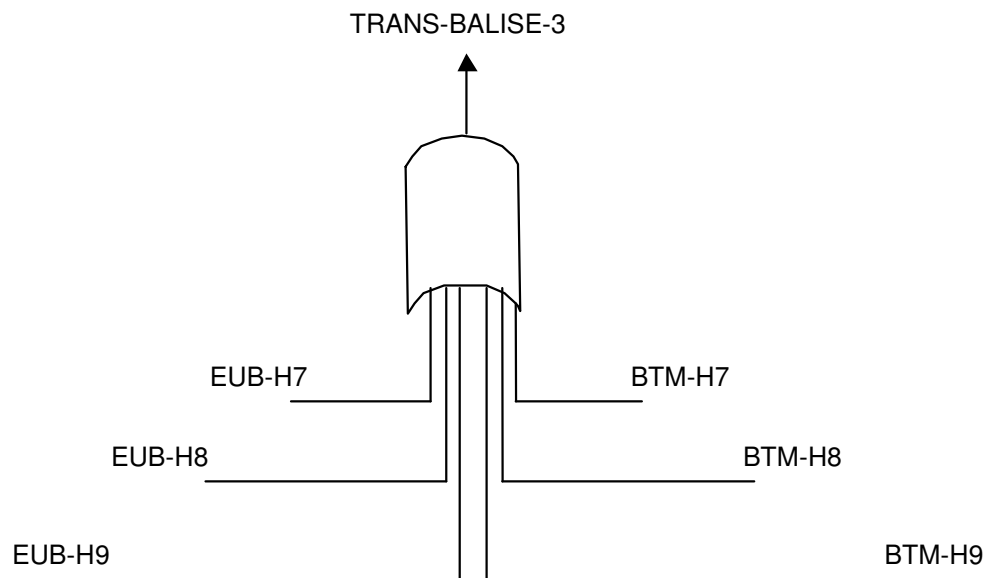
- 8.2.1.15 The effect of these figures on the TSR requirement is to make the dependence on information point failure negligible to effect of $0.005\lambda_{\text{ONB}}$. Thus the predicted failure rate for TSRs becomes.

$$\text{HR}_{\text{TSR}} = 0.005 \cdot 10^{-7} \text{ Failures hour}^{-1}$$

$$\underline{\text{HR}_{\text{TSR}} = 5.0 \cdot 10^{-10} \text{ Failures hour}^{-1}}$$

8.3 Fault Tree for TRANS-BALISE-3 (Cross Talk)

8.3.1.1 The fault tree for TRANS-BALISE-3 in respect of the balise is shown below



8.3.1.2 Thus the target for insertion due to cross talk resulting from technical failures as derived in this Annex at section 7.5.2 is

$$1.0 * 10^{-9} \text{ dangerous failures / hour due to cross talk.}$$

8.3.1.3 The subordinate balise events to TRANS-BALISE-3 are defined as,

- | | |
|--------|---|
| BTM-H7 | Erroneous localisation of a Balise Group, with reception of valid telegrams, due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal) |
| EUB-H7 | Erroneous localisation of a Balise Group, with reception of valid telegrams, due to failure within Balises (too strong up-link signal) |
| BTM-H8 | The order of reported Balise, with reception of valid telegrams, is erroneous due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal) |
| EUB-H8 | The order of reported Balises, with reception of valid telegram, is erroneous due to failure within a Balise (too strong up-link signal) |
| BTM-H9 | Erroneous reporting of a Balise Group in a different track, with reception of valid telegrams, due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal) |
| EUB-H9 | Erroneous reporting of a Balise Group in a different track, with reception of valid telegrams, due to failures within Balises (too strong up-link signal) |



- 8.3.1.4 The apportionment of TRANS-BALISE-3 over the subordinate balise events will be undertaken by the Unisig Working Group on the Eurobalise sub-system with the results being included in the mandatory document Subset 036 (The Eurobalise FFFIS).
- 8.3.1.5 Note that, as indicated in paragraph 5.2.1.12 of this annex, there is no corresponding hazard related to the loop due to the inherent protective measures in ETCS which provide for linking from the End of Loop Marker balise which also defines the identity and location of the expected loop.