UNISIG

ERTMS/ETCS - Class 1

Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2

REF : SUBSET-091
ISSUE : 2.5.0
DATE : 05-05-09

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. 24-08-01	All	Document Creation	WLH
0.0.2 21-09-01	All		GM
0.0.3 04-10-01	All	Further additions and amendments following the transfer of some sections to other parts of Subset 088-2	WLH / GM
0.0.4. 11-10-01	All	Amendments as requested by Ansaldo and the addition of the agreed system THR	WLH
0.0.5 2002-04-29	All	Updates based on v200 of the rest of Subset-088.	DARI
0.0.6 2002-05-21	All	Various updated after comments from Invensys, Siemens and Ansaldo. Document changed name from Subset-088 Part 4 to Subset-091.	DARI
0.0.7 2002-05-23	All	Online editing during RAMS-group meeting	RAMS-meeting
0.0.8 2002-05-31	All	Follow-up of remaining is-sues after RAMS-group meeting	DARI
0.0.9 2002-06-12	All	Various updated after comments from Invensys, Siemens and Ansaldo.	DARI
0.0.10 2002-06-14	8.3	Minor correction	DARI
0.0.11 2002-06-25	6, 8, 10	Clarifications after review by UNISIG Super Group	DARI
2.0.0. 28-06-02	None	Raised in issue for release to the Users Group	WLH
2.0.1. 11-11-02		Editorial Changes	WLH

2.0.2 10-12-02		Editorial changes in line with review comments from Ansaldo, Bombardier and Siemens	WLH
2.0.3. 28-01-03		Further changes to ensure correspondence with Sub-set 088 Part 3.	WLH
2.1.0 31-01-03		Raised in issue for release to the Users Group	WLH
2.2.2 20-03-03		Final release after amend-ment to reflect the com-ments in the final report from the ISA's version 1.1 dated 07-03-03 as pro-posed via the Unisig con-solidated review comments on the ISA report v 0.0.2 March 03.	WLH
2.2.3 28-06-04		• prEN50129 changed to EN50129 • KERNEL-33 and -34 added • All references to "high-speed" removed • Ch 5.3 rewritten • Note B in sect 10.2 added • References to SUBSET-041 added in Annex A • Various small correc-tions	DARI
2.2.4 05-09-04		Various updated after comments from Siemens and Ansaldo.	DARI
2.2.5 04-10-04		Various updated after comments at RAMS-meeting 2004-09-09 and comments from Ansaldo.	DARI
2.2.6		Mission profile for conven-	DARI

26-11-04		tional rail added	
2.2.7 22-12-04		Mission profile for conventional rail modified after comments from Siemens and Alcatel	DARI
2.2.8 20-06-05		• LO-H4 added in paragraph 8.2.1.2 • Ch 10.3.3 (% of time in modes) deleted • Frequency of radio messages for CR altered in section 10.3.2.	DARI
2.2.9 06-07-05		Updates after RAMS-meeting 2005-06-28	DARI
2.2.10 08-07-05		Raised in issue for release to the Users Group.	DARI
2.2.11 10-10-05		Note on ETCS_OB07 added.	DARI
2.2.12 14-06-07		• Updated versions of references SUBSET-026, -040, -041, -078 and -088 to match baseline 2.3.0 • Text about train type adaptation components added in sect 4.3.1.4 • EXT_SR04 added • New chapter about hazard analysis added	DARI
2.2.13 20-06-07		Updated during RAMS-meeting	DARI
2.2.14 25-06-07		Minor corrections	DARI
2.2.15 04-09-07		Updates during RAMS-meeting	DARI
2.2.16 09-10-07		Updated reference versions during RAMS-meeting	DARI
2.3.0		Text in section 4.3.1.4	DARI

12-05-08		changed. Administrative updates for baseline 2.3.0.	
2.3.1 17-12-08		Updates after comments from ERA, agreed during RAMS-meeting.	DARI
2.3.2 18-02-09		Updated during RAMS-meeting	DARI
2.3.3 12-03-09		ERA comments implemented: • Reference to Subset-113 removed. • Merger of 4.1.1.11 and 4.1.1.12 Released for ERA Control Group approval.	DARI
2.4.0 19-03-09		Version number updated for release.	DARI
2.5.0 05-05-09		Updated during RAMS-meeting: • Version nr of Subset-039, -040 and -078 updated for consistency with baseline 2.3.0d.	DARI

2. TABLE OF CONTENTS

3. REFERENCES

3.1.1.1 This document has been elaborated making reference to other publications and therefore incorporates some provisions from these other publications. The incorporated provisions are cited at the appropriate places in the text, and the publications are listed hereafter for information:

- EN 50126; Railway applications, The specification and demonstration of Reliability, Availability, Maintainability and Safety (September 1999)
- EN 50128; Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems (March 2001)
- EN 50129; Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signalling (February 2003)
- EN 50159-1; Railway applications - Communications, signalling and processing systems - Part 1: Safety-related communication in closed transmission systems (March 2001)
- EN 50159-2; Railway applications - Communications, signalling and processing systems - Part 2: Safety-related communication in open transmission systems (March 2001)

3.1.1.2 The following documents were consulted in the development in this document:

	Version
• UNISIG System Requirements Specification - Subset 026	2.3.0
• Subset-037	2.3.0
• Subset-039	2.3.0
• Subset-040	2.3.0
• Subset-041	2.1.0
• RBC / RBC Handover FMEA - Subset 078	2.4.0
• MMI FMEA (L1) - Subset 079 - 1	2.2.2
• MMI FMEA (L2) - Subset 079 - 2	2.2.2
• TIU FMEA (L1) - Subset 080 - 1	2.2.2
• TIU FMEA (L2) - Subset 080 - 2	2.2.2
• Transmission Path FMEA (L1) - Subset 081 - 1	2.3.0

- Transmission Path FMEA (L2) - Subset 081 - 2 — 2.3.0
- Safety Analysis, Functional Fault Tree (L1) - Subset-088 - 1 Part 1 — 2.3.0
- Safety Analysis, Functional Fault Tree (L2) - Subset-088 - 2 Part 1 — 2.3.0
- Safety Analysis, Functional Analysis (L1) - Subset-088 - 1 Part 2 — 2.3.0
- Safety Analysis, Functional Analysis (L2) - Subset-088 - 2 Part 2 — 2.3.0
- Safety Analysis, THR Apportionment - Subset-088 Part 3 — 2.3.0
- Subset-098 — 1.0.0
- Subset-108 — 1.2.0

3.1.1.3 Subset 026 was the subject of the safety analysis and was used as a statement of the UNISIG design intent.

3.1.1.4 The FMEA documents identified hazardous events that could exist at the mandatory boundaries to the ETCS reference architecture. These events are used as the base events of the fault tree developed in Subset-088 Part 1.

4. INTRODUCTION

4.1 Scope

4.1.1.1 This document defines the generic high-level quantitative safety requirements for ETCS operating in either Level 1 or Level 2. The figures given relate to the UNISIG groupings of constituents operating in a defined context and make no presumption on system implementation. The figures given are the minimum that must be reached in order to ensure that Technical Interoperability is achieved safely. The technical interoperability supports the operational interoperability that in its turn enables the interlinking of national railway networks.

4.1.1.2 The safety requirements defined in this document supplement those contained in the SRS and other Unisig subsets referenced by the TSI. Any specific implementation and application will need its own hazard identification and safety analysis process to be undertaken in accordance with the applicable European standards and this process will be supplemented and supported by the generic safety requirements defined herein. The requirements in this document being the minimum to ensure Technical Interoperability.

4.1.1.3 The supporting documents cited in the text are to aid the tracing of the origin of the safety requirement. However, it is only this document that is considered to be mandatory.

4.1.1.4 It is the responsibility of the supplier to demonstrate the compliance of a particular implementation of ETCS equipment with the safety requirements defined herein, according to the procedures indicated in the applicable Technical Specification for Interoperability.

4.1.1.5 The Safety Requirements are structured as;

- Safety Requirements for the ETCS onboard System
- Safety Requirements for the ETCS trackside System
- Safety Requirements placed on External Entities where these are ETCS specific and need to be harmonised

4.1.1.6 The validity of the quantified safety requirements indicated in this document depends on several factors, i.e. assumptions on the characteristics of transmission systems, mission profile, operational issues, that are indicated in chapters 5 and 9.5.

4.1.1.7 The safety requirements are related to a safety function for the entity under consideration. This specific safety function is defined in Subset-088 Part 3 along with its associated hazard. The defined hazard is repeated in this part.

4.1.1.8 Safety Requirements are given as Tolerable Hazard Rates (THRs) which, if complied with, will meet the overall THR for ETCS as defined and agreed by the European Railways. Associated with the hazard rates are the critical functions necessary to ensure technical interoperability.

4.1.1.9 The Hazard Rates have come from the apportionment of the given THR in Subset-088 Part 3. The principle of this is briefly outlined in chapter 6.

4.1.1.10 Subset-088 Parts 1 & 2 provided details on the various claims made which would mitigate against the emergence of the core hazard in the event of the critical base event failure. See Annex C. These mitigations need to be harmonised to ensure that technical interoperability is achieved as well as system safety.

4.1.1.11 The format for the safety requirements as described complies with the Normative Annex A of EN 50129. The allocation of the THR between random and systematic failures is to be undertaken in accordance with EN 50129. The THR refers to the equipment installed on a single train and in the ETCS equipped area visited by the train during a reference mission defined in chapter 9.5. Note: The THR_{ETCS} does not include failures due to causes external to the ETCS reference architecture, such as operational errors, dragging equipment etc.

4.2 System Context

4.2.1.1 All of the analyses are undertaken against the representation shown below. This puts the ETCS class 1 functionality as defined by the ETCS reference architecture, in its operational environment of an interoperable railway as mandated by the European Directives 96/48 and 2001/16 in conjunction with the corresponding Technical Specifications for Interoperability.

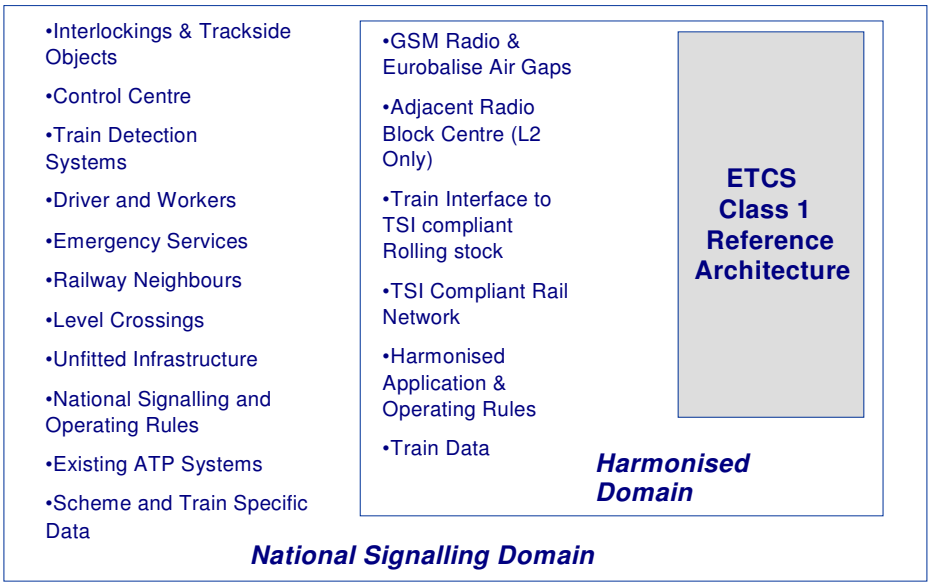

Figure 1: The ETCS Reference Architecture in its Context

4.2.1.2 With “ETCS Class 1 Reference Architecture” it is meant the ETCS part of ERTMS. This means that when adding new constituents within ERTMS, such as Euro-interlocking, this will not affect the scope of the Reference Architecture for ETCS.

4.2.1.3 The operational environment requires that the on-board part of the reference architecture must interface with defined entities throughout Europe in order to achieve technical and operational interoperability. These are denoted by the items within the Harmonised Domain. Due to the mobility of the on-board part, these items will influence the achieved level of safety across Europe.

4.2.1.4 The reference architecture and the harmonised items are required to work in conjunction with national signalling systems. These items are shown within the National Signalling Domain in the above figure. It is noted that these items will influence the achieved level of safety in a particular country.

4.2.1.5 The scope of the UNISIG work is the analysis of the reference architecture, see further section 4.3. However where the achieved system safety is critically dependent on the harmonised items, any assumptions or requirements are documented. Assumptions regarding the performance of a National signalling system are outside the scope of this work.

4.2.1.6 The role of ETCS as it is defined by the ETCS reference architecture in the railway environment, has been defined as

To provide the Driver with information to allow him to drive the train safely and to enforce respect of this information.

4.2.1.7 Note: Because ETCS does not include the braking system, the enforcement of respect of this information means issuing of appropriate commands to entities external to ETCS (e.g., braking systems).

4.2.1.8 Thus the Core Hazard for the reference architecture is defined as

Exceedance of the safe speed / distance as advised to ETCS.

4.2.1.9 The maximum allowed rate of occurrence for the core hazard has been defined by the Railways - and approved by the National Safety Authorities[1] - as being $2.0*10^{-9}$ / hour / train. This is the maximum Tolerable Hazard Rate (THR) for ETCS, denoted as THR_{ETCS}.

4.2.1.10 The THR has been derived from consideration of the consequences that an occurrence of the ETCS core hazard would have on a passenger travelling on a train.

4.2.1.11 The core hazard and its associated THR relate to the failure to perform the function of ETCS as defined in 4.2.1.6. This function is achieved with the ETCS reference architecture as defined in the SRS. Thus, failures due to operators (e.g. Driver, signalman

[1] Referring to the National Safety Authorities in France, Germany, Italy and United Kingdom

and maintenance staff) and operational rules are not included in this core hazard or its THR.

4.2.1.12 The THR is given as a rate per hour for a typical passenger journey where many of the ETCS operational modes may be used. Apportionment of the THR for the top-level hazard to the hazard rates of the UNISIG grouping of constituents is undertaken in Subset-088 Part 3. This apportionment is based on a defined Mission Profile.

4.2.1.13 In order to arrive at a numerical limit for the constituent hazard rates, sensitivity analysis has been undertaken on the Mission Profile covering, for example different percentage times for operational modes. This is intended to ensure that the resulting targets are applicable to a wide range of real life applications.

4.3 The Reference Architecture

4.3.1.1 The part denoted as “UNISIG Class 1 Reference Architecture” in paragraph 4.2.1.1 is a functional architecture as depicted below.

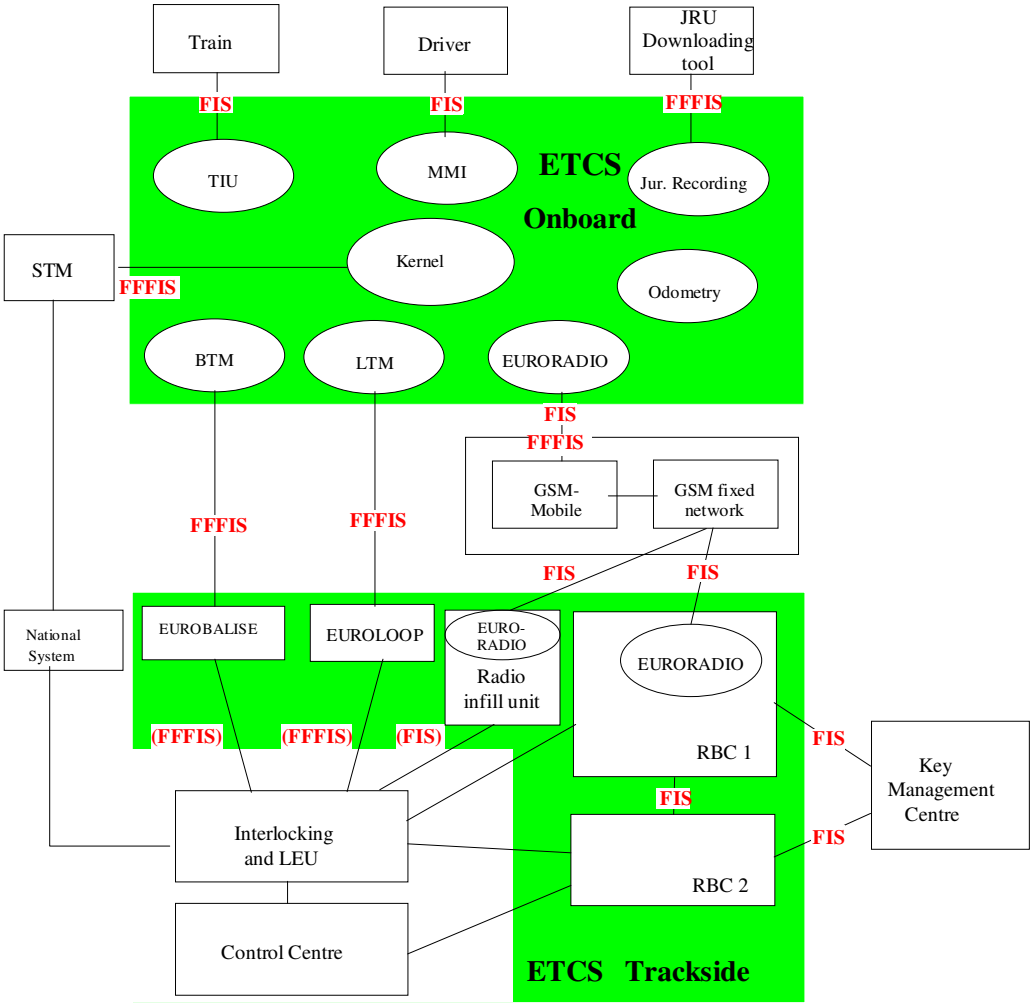

Figure 2: ERTMS/ETCS system referred to as “ETCS Reference Architecture”

4.3.1.2 Note: Interfaces in brackets are not required for interoperability.

4.3.1.3 The physical border between the ERTMS/ETCS on-board interoperability constituent and the rolling stock is not standardized; the supplier of the ERTMS/ETCS on-board shall clearly identify the borders of the equipment put on the market, i.e. the limits of the system to which the $THR_{ETCS\ Onboard}$ applies.

4.3.1.4 The effects of possibly required adaptation components to interface the ETCS on-board to a specific rolling stock shall be considered in the context of the verifications of Control Command and Signaling and Rolling Stock subsystems; such adaptation components may be considered part of the CCS or of the RS subsystem, as more appro-

priate for the specific case, anyway it has to be ensured that the safety requirements of both subsystems are not prejudiced.

4.4 Hazardous events

4.4.1.1 Associated with each THR requirement is a list of events which were identified in the functional analysis in Subset-088 as events that could lead to the hazard associated with the given THR. The list can be found in Annex A. Other, additional hazardous events may be derived according to specific implementations of ETCS equipment. It is the responsibility of the supplier to demonstrate how the events listed in Annex A, and also how the implementation specific events, are controlled.

4.5 Requirements Numbering

4.5.1.1 A numbering system for the quantified requirements has been introduced; ETCS_OB/TRxx, where OB refers to a requirement on the ETCS onboard equipment and similarly, TR refers to a requirement on the ETCS trackside equipment.

4.6 Process Requirements

4.6.1.1 ETCS is crucially dependent upon the quality of data from external sources and requirements are placed on such external entities where necessary. These requirements demand that the process being adopted shall be commensurate to a SIL 4 system. This is interpreted to mean that the process in question must be examined in detail to identify where there are potential threats to the accuracy of the process and that measures are put in place to minimise these threats.

4.6.1.2 The data referred to in this document includes both, data that might need to be entered by a train driver and data used by system designers to calculate parameters such as speed restrictions and stopping distances.

4.6.1.3 The above does not imply that processes need harmonising.

5. ETCS SYSTEM PERSPECTIVE ON TRANSMISSION SUBSYSTEMS

5.1 Corruption of messages

5.1.1.1 According to EN 50159-1[2] and -2[3], it is possible to protect data communication with measures that mitigate errors inside a transmission channel whose characteristics are not completely known.

5.1.1.2 In the analysis of such a transmission channel, see e.g. Subset-081 - Transmission Path FMEA, it is sometimes useful to consider part of the sender and receiver functionality as belonging to the non-trusted transmission channel, according to EN 50159 indications.

5.1.1.3 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). In Annex B, ETCS functionality considered as belonging to the non-trusted communication channel is inside “Euroradio”, “BTM”, “Eurobalise” and “Euroloop and Radio Infill unit”.

5.1.1.4 Note: Euroradio, BTM and LTM also contain functions that belong to on-board and, respectively, trackside safety relevant functionality.

5.1.1.5 In the apportionment of the THR_{ETCS}, it is assumed that the failure modes inside the equipment considered part of the non-trusted communication channel are protected by the safety code with respect to the corruption of messages. The target for the level of protection required is given in section 7.3.1.

5.1.1.6 It is therefore possible 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 is then allowed to define parts of his equipment as non-trusted, if he can prove that the equipment and failure modes inside this part does not violate the protection capability of the safety code.

5.1.1.7 The analysis of ETCS has assumed that the characteristics of the air gaps for Euroradio, Eurobalise and Euroloop are according to the corresponding specifications, with the probability of undetected corruption being negligible, due to the performance of the safety codes. Proof that the safety codes achieve the level of protection as defined in this document will be the responsibility of each supplier. Note: The air gaps refer to the

[2] Applied for the Balise transmission system, which is regarded as a closed transmission system

[3] Applied for the Radio transmission system, which is regarded as an open transmission system

non-trusted parts of the communication channel that are not part of the ETCS equipment.

5.2 Insertion of messages

5.2.1.1 In Subset-088 Part 3, it is stated that the rate of occurrence of balise group cross talk must be shown not to exceed 1.0 * 10^{-9} dangerous failures per hour. This requirement has been passed to the Eurobalise working group within UNISIG where the requirement has been broken down to the grouping of constituents (ETCS onboard equipment and balise) in Subset-036, where also the failure modes of this equipment are specified.

5.3 Deletion of Messages

5.3.1.1 In the case of radio transmission, the data exchange from track to train is defined in the ETCS specifications such that under normal conditions the deletion of a message does not result in a hazard. Anyway, degraded situations cannot in general be excluded, where the RBC sends a shorter MA than the one currently supervised onboard, although co-operative shortening should be used when possible. In such case, deletion of critical messages is dependent on the quality and availability of the radio system (which is outside the scope of these requirements) and can be mitigated by means of acknowledgement procedures and of radio link supervision.

5.3.1.2 Also, in the case of radio transmission from train to track, the system must be designed so that a loss or delay of a radio message does not cause an unacceptable risk. Note that the same mitigations are not defined in the SRS as for radio transmission from track to train. Therefore, additional mitigations outside the SRS might be necessary as a result of an application hazard analysis. However, in some specific cases, acknowledgement procedures are indeed defined in the SRS, e.g. acknowledgement of train data.

5.3.1.3 The same considerations as in section 5.3.1.1 apply to the deletion of Emergency messages. On this basis, the possibility of undetected deletion or delay of radio messages (in any direction) is not carried forward as provable / testable target in this specification. The mitigation (where necessary), by means of acknowledgement procedures and/or radio link supervision, is the responsibility of the specific trackside application of ETCS.

5.3.1.4 Additionally, the potential hazard of deletion of in-fill messages is also considered the responsibility of the specific trackside application of ETCS. If considered necessary, there is the linking mitigation that can be used for in-fill Eurobalise. In summary, no safety target is given for the deletion of any in-fill messages[4].

[4] However, for messages from Eurobalise, there is the safety target given in section 8.3, derived from scenarios other than in-fill messages.

5.4 Masquerade of messages

5.4.1.1 The quantitative safety targets mentioned 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 not trusted communication system).

5.4.1.2 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 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. PRINCIPLES OF APPORTIONMENT

6.1.1.1 The top hazard of the ETCS system and the associated THR_{ETCS} has been defined in paragraphs 4.2.1.7 and 4.2.1.9. This THR shall be broken down to the interoperable grouping of constituents, namely the onboard and trackside equipment. The result of this apportionment is reported in chapters 7 and 8, respectively.

6.1.1.2 The present chapter briefly summarises the principles of the apportionment process.

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 hazardous events as identified in Subset-088 Parts 1 and 2. The hazardous events are allocated as either 'on-board events', 'trackside events' or '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 desired equal splitting between onboard and trackside equipment. Figure 3 illustrates this. It also introduces the terms $THR_{Onboard}$ and $THR_{Trackside}$ denoting the numerical safety requirement for the purely onboard and trackside functions. These are further elaborated in sections 7.2 and 8.2, respectively.

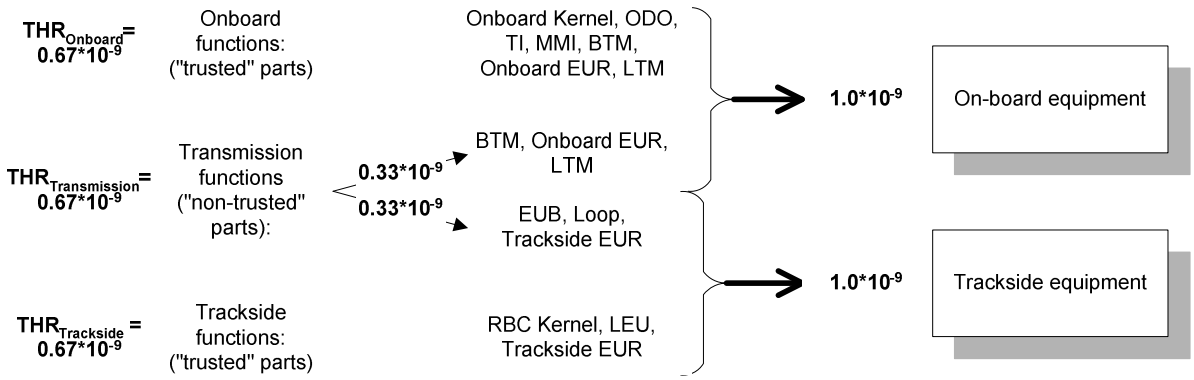

Figure 3: Principles for apportionment of THR_{ETCS} between onboard equipment and trackside equipment.

6.1.1.4 The apportionment to the constituent groupings is undertaken against a definition of the role of that constituent and its related hazard in a representative one-hour journey.

7. SAFETY REQUIREMENTS FOR THE ETCS ONBOARD EQUIPMENT

7.1 General

7.1.1.1 The safety integrity level will be derived from the different tolerable hazard rates. For Hazard Rates of < 10^{-9} f/h, a SIL 4 process will be applicable.

7.1.1.2 The defined targets shall be achieved in a specified environment (temperature, vibration, EMI etc) according to the indications in the applicable Technical Specification for Interoperability.

7.1.1.3 The dangerous failure for the ETCS onboard equipment is defined as,

Failure to provide onboard supervision and protection according to the information advised to the ETCS onboard from external entities.

Note: Only failures that cause the ETCS hazard, stated in paragraph 4.2.1.8, need to be considered. In this context, external entities include the trackside, which is assumed to provide the correct information to the on-board.

7.1.1.4 For the derived targets to be valid, the rules in Subset-026 “System Requirement Specification”, and Subset-108, must be implemented (see chapter 3 for versions).

7.2 ETCS onboard equipment except transmission system

ETCS_OB01	The hazard rate for the ETCS onboard system, less those parts forming part of the transmission paths, shall be shown not to exceed a THR of, $0.67*10^{-9}$ dangerous failures/hour (Ref. Subset-088 Part 3, paragraph 12.3.1.1)

7.2.1.1 Where the dangerous failure is defined according to 7.1.1.3.

7.2.1.2 Each supplier shall prove the attainment of the $THR_{Onboard}$ taking into account at least the following events, as defined in Annex A:

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

7.2.1.3 The proof shall consider the Mission Profile defined in sections 10.2 and 10.3, and the operational assumptions stated in section 10.4. Furthermore, the proof may take account of the protective features inherent in ETCS as identified in Annex C.

7.2.1.4 The overall safety performance of ETCS is critically dependent on the Train Data that is entered in the ETCS onboard equipment. Therefore, the following requirement for ETCS is formulated:

ETCS_OB02	The process of confirmation that the train data is correctly stored on-board must be of a quality commensurate with a SIL 4 system. (Ref. Subset-088 Part 3, paragraph 12.6.4.2)

7.2.1.5 Intentionally deleted. See CR88 and CR110 in SUBSET-108 (the SRS is updated accordingly).

ETCS_OB03	Intentionally deleted.
ETCS_OB04	Intentionally deleted.

7.3 ETCS onboard transmission system

7.3.1 Radio channel

ETCS_OB05	Corruption of radio messages The requirement for the non-trusted part of OB-EUR-H4[5] is that the non-trusted ETCS onboard radio transmission equipment shall respect the definition of non-trusted as given in paragraph 5.1.1.6 and the THR of $1.0 * 10^{-11}$ Dangerous failures per hour (Ref. Subset-088 Part 3, paragraph 12.5.1.1)

[5] For trusted part, see paragraph 7.2.1.2.

7.3.2 Balise Channel

ETCS_OB06	Corruption of balise message The requirement for the non-trusted part of BTM-H4[6] is that the non-trusted ETCS onboard balise transmission equipment shall respect the definition of non-trusted given in paragraph 5.1.1.6. and the THR of $1.0 * 10^{-11}$ Dangerous failures per hour (Ref. Subset-088 Part 3, paragraph 12.5.2.1)
ETCS_OB07	Failure of balise group detection The rate of failure for the ETCS onboard to fail to detect a balise group shall be shown not to exceed $1.0 * 10^{-7}$ Dangerous failures per hour (Ref. Subset-088 Part 3, paragraph 12.5.2.4) Note: The ETCS_OB07 failure rate may be achieved by means of periodic self tests, during equipment operation. It is however possible to force the ETCS on-board to ignore the results of such tests, while passing over certain metal masses. In such cases, it is the responsibility of the infrastructure manager to prove that this disabling of the tests does not prejudice the achievement of the safety of the service.
ETCS_OB08	Cross-talk of balise group The overall THR for cross talk is, $1.0 * 10^{-9}$ dangerous failures per hour In Subset-036 this requirement is distributed between ETCS onboard and track-side equipment. This yields the requirement for the ETCS onboard equipment to have a maximum unavailability of $1.0 * 10^{-6}$ with regards to each of the following failure modes: • The ETCS onboard equipment is more sensitive than expected. • The ETCS onboard equipment is transmitting more Tele-powering field than specified. See subset 036, Annex F for details of potential failure modes and possible solutions. (Ref. Subset-088 Part 3, paragraph 12.5.2.5 and subset-036 paragraph 6.4.5.2)

[6] For trusted part, see paragraph 7.2.1.2.

7.3.3 Loop channel

ETCS_OB09	Corruption of Loop message The requirement for the non-trusted part of LTM-H4[7] is that the non-trusted ETCS onboard loop transmission equipment shall respect the definition of non-trusted given in paragraph 5.1.1.6. and the THR of $1.0 * 10^{-11}$ Dangerous failures per hour (Ref. Subset-088 Part 3, paragraphs 12.5.2.1 & 12.5.2.3)

[7] For trusted part, see paragraph 7.2.1.2.

8. SAFETY REQUIREMENTS FOR THE ETCS TRACKSIDE EQUIPMENT

8.1 General

8.1.1.1 The safety integrity level will be derived from the different tolerable hazard rates. For Hazard Rates of < 10^{-9} dangerous failures per hour, a SIL 4 process will be applicable.

8.1.1.2 The defined targets shall be achieved in a specified environment (temperature, vibration, EMI etc) according to the indications in the applicable Technical Specification for Interoperability.

8.1.1.3 The dangerous failure for the ETCS trackside equipment is defined as,

> Failure to provide information to the ETCS onboard supervision in accordance with the data advised to the ETCS trackside from external entities.

Note: Only failures which cause the ETCS hazard, stated in paragraph 4.2.1.8, has to be considered.

Note: External entities include the assumption that the ETCS onboard provides a correct train location report 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 7.1.1.3.

8.1.1.4 For the derived targets to be valid, the rules in Subset-026 “System Requirement Specification”, and Subset-040 “Dimensioning and Engineering Rules”, must be implemented. In addition, the change requests with IN-status in Subset-108 are considered as part of the implementation.

8.2 ETCS trackside equipment except transmission system

ETCS_TR01	The hazard rate for the ETCS trackside system, less those parts forming part of the transmission system, shall be shown not to exceed $THR_{Trackside}=0.67*10^{-9}$ dangerous failures/hour (Ref. Subset-088 Part 3, paragraph 12.4.1.1)

8.2.1.1 Where the dangerous failure is defined according to 8.1.1.3.

8.2.1.2 Each supplier shall prove the attainment of the $THR_{Trackside}$ taking into account at least the following events, as defined in Annex A:

- RBC-2 and RBC-3 (level 2 only)

- LEU-H4 (level 1 only)[8]
- TR-EUR-H4 (level 2 only) (the parts of the hazard that arise due to failures inside the trusted part of the transmission channel)

8.2.1.3 The proof shall consider the Mission Profile defined in sections 10.2 and 10.3, and the operational assumptions stated in section 10.4. Furthermore, the proof may take account of the protective features inherent in ETCS as also identified in Annex C.

8.2.1.4 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. However, if using LEUs for safety relevant information in Level 2, this must be analysed separately.

8.3 ETCS trackside transmission system

8.3.1 Radio channel

ETCS_TR02	Corruption of radio message The requirement for the non-trusted part of TR-EUR-H4[9] is that the non-trusted ETCS trackside radio transmission equipment shall respect the definition of non-trusted given in paragraph 5.1.1.6 and the THR of $1.0 * 10^{-11}$ Dangerous failures per hour (Ref. Subset-088 Part 3, paragraph 12.5.1.1)

8.3.2 Balise channel

ETCS_TR03	Corruption of balise message The requirement for the non-trusted part of EUB-H4 is that the non-trusted ETCS trackside balise transmission equipment shall respect the definition of non-trusted given in paragraph 5.1.1.6 with a THR of, $1.0 * 10^{-11}$ Dangerous failures per hour (Ref. Subset-088 Part 3, paragraph 12.5.2.1)
ETCS_TR04	Failure of balise group detection The rate of failure for a balise group with at least two balises to become undetectable, shall be shown not to exceed, $1.0 * 10^{-9}$ Dangerous failures per hour For an individual balise to be interoperable, it shall have an unavailability less than $2.0*10^{-5}$ with regards to hazard EUB-H1. This requirement has been derived

[8] Note that LEU-H4 contributes to failures both in the Eurobalise and the Euroloop channels.

[9] For trusted part, see paragraph 8.2.1.2.

	in Subset-036 from the above requirement on a balise group of two balises. (Ref. Subset-088 Part 3, paragraph 12.5.2.4 and Subset-036 paragraph 5.5.5.2)
ETCS_TR05	Cross-talk of balise group The overall THR for cross talk of, $1.0 * 10^{-9}$ dangerous failures per hour In Subset-036 this requirement is distributed between ETCS onboard and track-side equipment. This yields the requirement for the ETCS trackside equipment to meet the overall cross-talk THR of 10^{-9} f/h given in paragraph 8.3.1.2 of subset 088 Annex A, considering the ETCS onboard performance stated in ETCS_OB8 A methodology for this is suggested in Subset-036 Annex F, although the actual accomplishment of the analysis is supplier and application specific. (Ref. Subset-088 Part 3, paragraph 12.5.2.5 and Subset-036 paragraph 5.5.5.2)

8.3.2.1 Rules additional to those given in Subset-040 “Dimensioning and Engineering Rules”, have been derived as part of the analysis process. These additional rules are as follows.

ETCS_TR06	TSR balise groups When giving a Temporary Speed Restriction by means of unlinked balise groups, at least[10] two balise groups[11] shall be used to announce the TSR before the restricted area.
ETCS_TR07	Number of balises in each group A balise group, which contains information that if it is missed could lead to a hazardous consequence, shall consist of a minimum of two balises. This refers to a balise group that, for example, (1) gives a Temporary Speed Restriction, (2) gives the start of a linking chain, i.e. met in a Start of Mission or in a change from Level 0 to Level 1/2 or (3) constitutes a border balise group giving more restrictive National Values. (Ref. Subset-088 Part 3, Annex A, paragraph 3.3.1.1)

[10] For operational reasons, it might be necessary to use more than two groups.

[11] With two balises in each group, see requirement ETCS_TR07.

8.3.3 Loop channel

ETCS_TR08	Corruption of Loop message The requirement for the non-trusted part of LO-H4 is that the non-trusted ETCS trackside loop transmission equipment shall respect the definition of non-trusted given in paragraph 5.1.1.6. with a THR of, $1.0 * 10^{-11}$ Dangerous failures per hour (Ref. Subset-088 Part 3, paragraph 12.5.2.1 & 12.5.2.3)

9. SAFETY REQUIREMENTS FOR EXTERNAL ENTITIES

9.1 ETCS Dependencies

9.1.1.1 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.

9.1.1.2 The external entities can be considered in 3 parts

- Those entities which form part of a harmonised ETCS system, namely:
  - Data Preparation
  - System Deployment
  - Train Data Engineering
- Existing Entities which ETCS is required to interface to, such as the trackside systems:
  - Interlockings
  - Train detection systems

  The specification of requirements for such systems is outside scope of ETCS and this document.
- Other external conditions interfacing with ETCS:
  - Reference Infrastructure (see further chapter 10.2)
  - The behaviour of the driver (see further section 10.4)

9.2 Integrity Requirements for Data Preparation

EXT_SR01	The collection, interpretation, accuracy and allocation of data relating to the railway network shall be undertaken to a quality level commensurate with the SIL 4 allocation to the ETCS equipment. (Ref. Subset-088 Part 3, paragraph 12.6.2.1)

9.3 Integrity Requirements for System Deployment

EXT_SR02	The overall safety performance of ETCS is critically dependent on the Engineering and therefore the complete Engineering process shall be of a quality commensurate with a SIL 4 system. (Ref. Subset-088 Part 3, paragraph 12.6.3.1)

9.4 Integrity Requirements for the Data Engineering

EXT_SR03	The overall safety performance of ETCS is critically dependent on the Train Data that is prepared by the operator. Therefore the preparation of the Train Data shall be of a quality commensurate with a SIL 4 system. (Ref. Subset-088 Part 3, paragraph 12.6.4.1)

9.5 Mission Profile and Related Assumptions

EXT_SR04	Infrastructure installation and operational circumstances need to be considered as stated in chapter 10.

10. MISSION PROFILE AND RELATED ASSUMPTIONS

10.1 Introduction

10.1.1.1 To arrive at some of the requirements in the above sections, quite detailed analyses have been carried out. The analyses (as undertaken in Subset-088) make assumptions about various things in the environment of ETCS, such as interfacing systems and driver actions. In order for the resulting requirements to be relevant, these assumptions must be met. The assumptions are given in this chapter, and must be considered as a vital part of the safety study.

10.1.1.2 If the characteristics of an infrastructure installation or operational circumstances significantly differ from the assumptions stated in sections 10.2, 10.3 and 10.4 below, there is subsequently a risk that THR_{ETCS} will not be met, although ETCS equipment fulfils all requirements stated in the present document (chapter 7 and 8). An analysis of the impact of the deviating parameters must then be made, unless the parameters in question are classified as “not relevant” according to paragraph 10.1.1.4. Additional protective measures external to ETCS might be required

10.1.1.3 Also, when each supplier shall prove the safety of his equipment, it will be necessary in that analysis to make assumptions. These assumptions shall then consider the Mission Profile defined in sections 10.2 and 10.3 and the operational assumptions stated in section 10.3.2.13. The Mitigating Conditions in Subset-088 Part 2 can also be considered when doing this, according to the list in Annex C.

10.1.1.4 An (*) in the column “Value” of the table means that this specific parameter has been explicitly used in the purpose stated in paragraph 10.1.1.1. Therefore, a parameter can be regarded as “not relevant” if:

- there is no (*) for a parameter, and
- the parameter is also not used in the supplier specific safety analysis mentioned in paragraph 10.1.1.3.

10.1.1.5 Note: parameters that are relevant for the safety analysis, other than the ones marked with (*) in this specifications, shall be explicitly indicated in the safety case.

10.2 The Reference Infrastructure

10.2.1.1 This section defines a reference infrastructure, representing average physical and operational characteristics of the railway network, to which the interoperability Directive applies.

10.2.1.2 Not all parameters are used in the apportionment process.

10.2.1.3 Apart from the below quantified parameters, the assumptions stated in chapter 10.4.1.6 (Rule A and Rule B) are also relevant requirements on the infrastructure.

10.2.1.4 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 Subset-088 Part 3 Annex A 6.6.1.2.

10.2.1.5 Note B: If using the End-Section Timer, a stopping point could result in a Staff Responsible movement in level 1. This would affect the number of Staff Responsible movements in the analysis of the Balise Detect function in SUBSET-088 Part 3, Annex A. The effect of this has not been considered. Therefore, if using End Section Timers, the mentioned analysis must be re-considered.

Reference Number	Parameter description	Value For (*) see paragraph 10.1.1.4	
		High-speed Rail	**Conventional Rail**
10.2.1.6	Length of the line	260 km	80 km
10.2.1.7	Number of Radio Block Centres	3 h^{-1}	1 h^{-1}
10.2.1.8	Number of station (general) and/or stopping points, see Note B	25 h^{-1}	25 h^{-1}
10.2.1.9	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} (*)
10.2.1.10	Number of changes in direction of travel (where Start of Mission is implied), see Note A.	1 h^{-1} (*)	2 h^{-1} (*)
10.2.1.11	Number of tunnels	10 h^{-1}	3 h^{-1}
10.2.1.12	Number of trains on the line	15 h^{-1}	15 h^{-1}
10.2.1.13	Number of Signals (0 possible for level 2)	0-200 h^{-1}	0-50 h^{-1}
10.2.1.14	Maximum distances between Balise groups	2.5 km	2.5 km
10.2.1.15	% of journey with the maximum distance between Balise groups	~ 10 %	~ 10 %
10.2.1.16	Number of Unlinked Balise groups (marked as Unlinked)[12]	1 in 1000 (*)	4 in 1000 (*)
10.2.1.17	Number of Repositioning Balise groups (only Level 1)	1 in 100	1 in 100

[12] A Temporary Speed Restriction announced by unlinked balise groups counts as 1, although actually announced by 2 balise groups according to requirement ETCS_TR07.

Reference Number	Parameter description	Value For (*) see paragraph 10.1.1.4	
		High-speed Rail	**Conventional Rail**
10.2.1.18	Number of Level transitions (including STM X - STM Y transitions)	2 h^{-1} (*)	2 h^{-1} (*)
10.2.1.19	Number of temporary Shunting areas with number of border Balises	1 / 66	1 / 66
10.2.1.20	Number of fixed Shunting areas (after which Start of mission is implied), see Note A	1 h^{-1} (*)	1 h^{-1} (*)
10.2.1.21	Number of National Border transitions	1 h^{-1}	1 h^{-1}

10.3 Operational Parameters

10.3.1.1 This section defines a reference infrastructure, representing average physical and operational characteristics of the railway network, to which the interoperability Directive applies.

10.3.1.2 In relation to the parameters in 10.3.3, it must be noted that SUBSET-091 deals only with performances of ETCS technical equipment. System safety depends also on other issues, such as operational rules. ETCS is able to guarantee a very good protection when trains are in FS mode, while in other modes the role of operational rules and human factors is greater. It is the responsibility of each application to show that operational rules, procedures, professional qualification of staff, etc., are sufficient to ensure the safety level required for service in all ETCS operational modes.

Reference Number	Parameter description	Value For (*) see paragraph 10.1.1.4	
		High-speed Rail	**Conventional Rail**
10.3.2	**General**		
10.3.2.1	Average speed of trains of the line	260 km/h	80 km/h
10.3.2.2	Max. speed of trains of the line	350 km/h	250 km/h
10.3.2.3	Frequency of balise messages	150 - 650 h^{-1} (*)	50 - 150 h^{-1} (*)
10.3.2.4	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) (*)
10.3.2.5	Frequency of radio messages Track to Train	100 - 360 h^{-1}	25 - 360 h^{-1}
10.3.2.6	Frequency of radio messages Train to Track	100 - 650 h^{-1}	50 - 650 h^{-1}
10.3.2.7	Frequency of Emergency Messages (only level 2)	$4*10^{-4}$ h^{-1}	$4*10^{-4}$ h^{-1}
10.3.2.8	Number of train data entry procedure, see Note A	2 h^{-1} (*)	4 h^{-1} (*)
10.3.2.9	Number of RBC/RBC Transitions	3 h^{-1}	1 h^{-1}
10.3.2.10	Max. expected loss of train integrity	N/A	N/A
10.3.2.11	Mean Down time of a failed ETCS onboard balise receiver in an unfitted area	1 hour (*)	1 hour (*)
10.3.2.12	Mean down time of a non-detectable balise group. See Note C below.	24 hours (*)	24 hours (*)

10.3.2.13 Note C: The balises used for Temporary Speed Restrictions does not need to be repaired or replaced within such a short time. This is because of rule ETCS_TR06. If the failures of these two groups are fully independent, the allowed Mean Down Time of one group is much longer than the normal use of a Temporary Speed Restriction. However, the wayside application must analyse the need for special rules for such balise group in order to accommodate for any potential failure dependence.

10.4 Operational Assumptions

10.4.1.1 This section defines the operational assumptions that were used as part of safety analysis process.

Reference Number	Parameter description	Value For (*) see paragraph 10.1.1.4	
		High-speed Rail	**Conventional Rail**
10.4.1.2	Probability of driver failing to verify a level transition function at an ETCS border. See Rule A.	0,001 (*)	0,001 (*)
10.4.1.3	Probability of driver passing a safe authorisation when driving in SR mode. See Rule B.	0,001 (*)	0,001 (*)

10.4.1.4 The figures adopted are a compromise between National views and a compromise between high-speed and conventional applications.

10.4.1.5 The derived targets for the Balise subsystem assume that the following operation rules are in place:

- 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.

10.4.1.6 These rules cover situations where, if a driver fails to obey information a hazardous situation could result. No assumptions about the vigilance of the driver acting in mitigation to ETCS failures have been made in the derivation of the safety targets.

11. GLOSSARY

11.1.1.1 In addition to the general UNISIG glossary, there are three terms which are used in the following parts that benefit from defining as follows

11.1.1.2 Driver Vigilance - The degree of reliance that can be placed on the driver and his ability to be aware of large errors in information displayed or system operation. Examples of such identifiable errors would be actual speed where the driver would, by virtue of his awareness, be able to identify a large error or failure of a tilting train to tilt.

11.1.1.3 Non-trusted transmission channels - see paragraph 5.1.1.6.

11.1.1.4 System Data - This term is used to encompass the following data.

Train Data

The following Train data as described within SRS chapter 3.18.3 is included.

This data is referred to as "Train data".

- Train categories
- Train length
- Traction / Braking model
- Maximum train speed
- Loading gauge
- Axle load
- Power supply
- Status of Airtight system
- Train running number

Additional Data

The following Additional data as described within SRS chapter 3.18.4 is included.

This data is referred to as "Additional data".

- Driver ID
- ERTMS/ETCS Level
- RBC ID / Telephone No.
- ETCS ID
- Adhesion factor

- Data used by applications outside ERTMS/ETCS (Train to Track)

National Values / Default Values

The National Values / Default values as described within SRS chapter A3.2 are included, e.g.:

- Radio link supervision data (M_NVCONTACT, T_NVCONTACT)

Specific System Data

The following data, which is needed by the system internally but which is not included in any other group of data is included.

This data is referred to as "Specific system data".

- Current mode
- EOLM Packet
- Radio in-fill area information
- Session control information (see below)
- In-fill location reference
- Balise ID (includes NID_C and NID_BG)
- MA request parameters
- Position report parameters

The following information is used to monitor radio sessions:

Session Control Data:

- Establish session (Session management, MA-, SH-, SR request, Radio Infill request)
- Terminate session (Session management, End of mission (Current mode))
- Activate / Deactivate T_NVCONTACT monitoring

Session Status:

- Session established
- Session terminated
- No connection established
- Connection lost
- Out of date message received

- Sequence error detected
- T_NVCONTACT violated
- Message inconsistency detected
- Radio Link reaction

Transmission Status (Balise / Loop)

- Switch on / off Balise Transmission
- Message inconsistency detected
- Linking reaction
- Braking reaction.

12. ANNEX A

12.1 List of Hazardous Events

12.1.1.1 The following is a list of the events inside ETCS that might cause the ETCS hazard to occur, either alone or in combination with other failures. The details of these events are presented in Subset-088 Part 2. The list is included here represents those hazardous events identified in Subset 088 Part 2 that have not been eliminated by the operational analysis in Subset 088 Part 3.

12.1.1.2 The third column below states what performance requirement in SUBSET-041 is connected to the respective base event. This means that a violation of the performance requirement shall be considered to cause the base event. Note that this does not mean that these are the only performance requirements that are needed to specify the base event; because the performances considered here are only the ones relevant for interoperability, as listed in SUBSET-041.

Event Id.	Event Description	Corresponding performance requirement in SUBSET-041
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	5.3.1.2: Accuracy of speed known on-board
ODO-3	Incorrect actual physical speed direction	
ODO-4	Distance measurement is incorrect	

Event Id.	Event Description	Corresponding performance requirement in SUBSET-041
KERNEL-1	Balise linking consistency checking failure	5.2.1.1: Delay between receiving of a balise message and applying the emergency brake
KERNEL-2	Balise group message consistency checking failure	5.2.1.1: Delay between receiving of a balise message and applying the emergency brake
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	5.3.1.2: Accuracy of speed known on-board
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	5.2.1.1: Delay between receiving of a balise message and applying the emergency brake
KERNEL-20	Failure of train trip supervision, shunting and SR	5.2.1.1: Delay between receiving of a balise message and applying the emergency brake
KERNEL-21	Incorrect supervision of stop in SR	5.2.1.1: Delay between receiving of a balise message and applying the emergency brake

Event Id.	Event Description	Corresponding performance requirement in SUBSET-041
KERNEL-22	Incorrect current EoA	5.2.1.6: Delay between receiving of an emergency message and applying the reaction on-board
KERNEL-23	Incorrect train position / train data sent from on-board to trackside	5.3.1.3: Age of location measurement for position report to trackside 5.3.2.1: Safe clock drift
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	5.2.1.3: Delay between receiving of a balise message and reporting the resulting change of status on-board (5.2.1.4: Delay between receiving of a MA via radio and the update of EOA on-board). Note: Whether 5.2.1.4 is safety related must be evaluated in the specific application's hazard analysis, see further section 5.3.

Event Id.	Event Description	Corresponding performance requirement in SUBSET-041
KERNEL-34	Incorrect supervision of MA time-outs (sections and overlaps)	5.2.1.3: Delay between receiving of a balise message and reporting the resulting change of status on-board (5.2.1.4: Delay between receiving of a MA via radio and the update of EOA on-board). Note: Whether 5.2.1.4 is safety related must be evaluated in the specific application's hazard analysis, see further section 5.3.
TI-1	Service brake / emergency brake not commanded when required	5.2.1.1: Delay between receiving of a balise message and applying the emergency brake
TI-2	Service brake / emergency brake release commanded when not required	5.2.1.1: Delay between receiving of a balise message and applying the emergency brake
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)	

Event Id.	Event Description	Corresponding performance requirement in SUBSET-041
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	
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	

Event Id.	Event Description	Corresponding performance requirement in SUBSET-041
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	

13. ANNEX B

13.1 Graphical Representation (Informative)

13.1.1.1 The figure below illustrates the hazardous events in Annex A in relation to the UNISIG Reference Architecture.

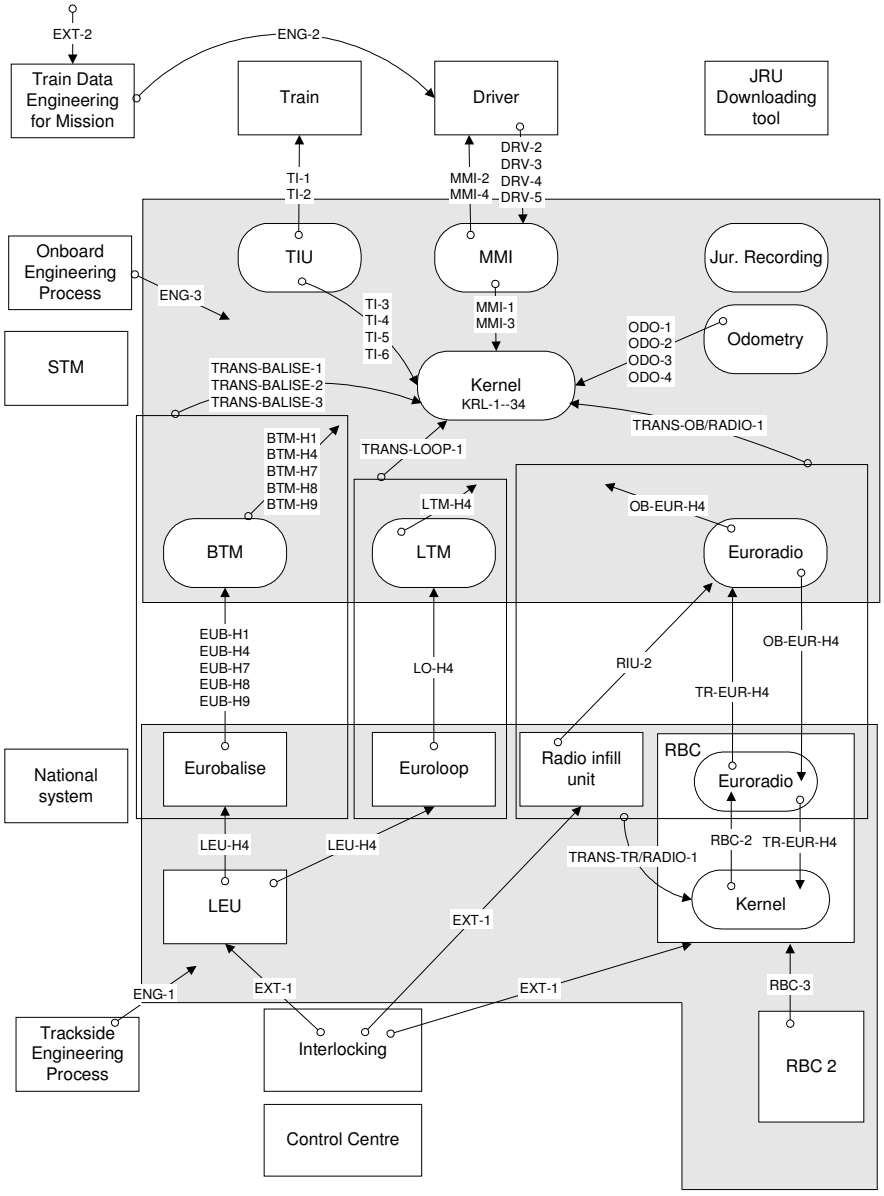

Figure 4: Graphical representation of the hazardous events within the UNISIG Reference Architecture.

14. ANNEX C

14.1 Protection Measures Inherent in ETCS

14.1.1.1 The hazardous events specified in Annex A do not necessarily directly lead to the top hazard as specified in paragraph 4.2.1.7. ETCS as specified in the SRS has several protective features built in at system level. These inherent protective features can act in preventing basic causal events migrating to create the core hazard. The following list indicates the protective features and the causal events that are affected by that feature.

14.1.1.2 The protective features listed below are based on the inherent features designed into ETCS and may be claimed as mitigations in a supplier's specific safety analysis

Inherent Protective Feature (from Subset-088 Part 2)	**ETCS Hazardous Event Affected (from Subset-088 Part 2)**
Supervision by ETCS Onboard	MMI-2a MMI-4
Mode Transition Table	KERNEL-16 MMI-1a, -1b, -1d, -1e, -1f
Balise Linking	ODO-3, 4
Linking reaction	KERNEL-28[13]
Message Consistency Checks	[14]
Maximum distance between Balise Groups	ODO-4 KERNEL-28
Balise Groups contain at least two Balises for safety data	[15]
Balise detection	ODO-1, -3
Radio message acknowledgement	KERNEL-4
Radio link time out	KERNEL-5, -18
Supervision and protection	MMI-2a

[13] Also, the linking reaction is a valid protective feature for BTM-H1 and EUB-H1. However, when deriving the targets for these events - as stated in the present document - this protection has already been credited.

[14] The message consistency check is a valid protective feature for BTM-H1, BTM-H4, EUB-H1, EUB-H4, OB-EUR-H4, TR-EUR-H4 and all balise cross-talk events. However, when deriving the targets for these events - as stated in the present document - this protection has already been credited.

[15] The two balises are a valid protective feature for BTM-H1 and EUB-H1. However, when deriving the targets for these events - as stated in the present document - this protection has already been credited.