ERTMS/ETCS
Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2
REF : SUBSET-091 ISSUE : 3.4.0 DATE : 2015-12-01

Company	Technical Approval	Management approval
ALSTOM		
ANSALDO		
AZD		
BOMBARDIER		
CAF		
SIEMENS		
THALES		

1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.0.1 (2001-08-24) - 2.4.0 (2009-03-19)		See version history in previous versions	
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
2.5.1 2010-11-24		• CR 103, 594, 656, 731, 802, 881, 1004: Various adjustments in the Train Data and Additional Data definitions according to Subset-026 v3.1.1 chapter 3.18 • CR 413: LX added as example in ETCS_TR07 • CR 637: Limited Supervision added • CR 753: acc to CR (except in base event id) • CR 808: 'Location' changed to 'position' in a few locations • EXT_SR03 completed with an 'and input' as a result of the update of Subset-079 to better cover the function Train Data input from sources other than the Driver	DARI
2.5.2 2011-01-26		• Version history before 2.5.0 collapsed. • Versions of EN standards removed.	DARI

		• Change on EXT_SR03 undone in v2.5.1 undone; covered by change proposal for CR 1039 • List of Train Data and Additional Data in §11.1.1.4 replaced by pointer to SRS • CR 637: further changes • CR 753: further changes in Figure 2, 3 and 4 • CR 802: acc to CR • CR 927: acc to CR • CR 1020: Footnote 14 in §14.1.1.2 expanded	
2.5.3 2011-04-26		• Definition of MMI-events coordinated with Subset-079 • CR 802: Note added that the “other solution” is not further studied	DARI
3.0.0 2011-09-30		Updated during RAMS-meeting: • CR1102: acc to CR • Subset-041 v3.0.4 considered • New versions of Subset-079 considered • New versions of Subset-088 considered • Rest list defined in chapter 4 • A few other minor clarifications	DARI
3.0.1 2012-01-04		• MMI-events and reference list updated due to new versions of Subset-	DARI

		079 (v3.6.0) and -088 (v3.1.0). • Reference list updated with new version of Subset-040 (v3.0.7) • CR752: acc to CR • CR1039: acc to CR • CR1106: acc to CR	
3.0.2 2012-01-19		Updated during RAMS-meeting: • Review comments from UNISIG SG implemented according to "Unisig_SG_COM_SS-091v300_v2.0.doc" • Changes in latest version of justification for CR1105 "Additional notes for S-091 update_v3.docx" implemented	DARI
3.1.0 2012-01-27		New version of Subset-088 considered	DARI
3.1.1 2012-02-02		Updated due to ERA comments on v3.1.0	DARI
3.1.2 2012-02-24		Synchronisation with the latest available versions of referenced documents during RAMS-meeting	DARI
3.2.0 2012-03-12		Baseline 3 release version	DARI
3.2.1 2014-04-22		Draft Baseline 3 First Maintenance pre-release version for review	DARI
3.2.2 2014-04-25		Baseline 3 1st Maintenance pre-release version	DARI
3.3.0 2014-05-08		Baseline 3 1st Maintenance release version	DARI

3.4.0 2015-12-01	7.2.1.5	Updated due to ERA/OPI/2014-8	Martin Vlcek

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 EN 50128; Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems
- EN 50129; Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signalling
- EN 50159; Railway applications - Communications, signalling and processing systems - Safety-related communication in transmission systems

3.1.1.2 The following documents, part of TSI Annex A, were consulted in the development in this document:

- System Requirements Specification - Subset 026
- Subset-036
- Subset-037
- Subset-039
- Subset-040
- Subset-041
- Subset-098

3.1.1.3 The following documents, not part of TSI Annex A, were consulted in the development in this document:

• RBC / RBC Handover FMEA - Subset 078	3.3.2
• DMI FMEA (L1) - Subset 079 - 1	3.13.0
• DMI FMEA (L2) - Subset 079 - 2	3.13.0
• TIU FMEA (L1/L2) - Subset 080 - 1/2	3.0.12
• Transmission Path FMEA (L1) - Subset 081 - 1	3.4.3
• Transmission Path FMEA (L2) - Subset 081 - 2	3.4.3
• Safety Analysis, Functional Fault Tree (L1) - Subset-088 - 1 Part 1	3.5.4
• Safety Analysis, Functional Fault Tree (L2) - Subset-088 - 2 Part 1	3.5.4
• Safety Analysis, Functional Analysis (L1) - Subset-088 - 1 Part 2	3.5.4
• Safety Analysis, Functional Analysis (L2) - Subset-088 - 2 Part 2	3.5.4
• Safety Analysis, THR Apportionment - Subset-088 Part 3	3.5.4
• ETCS DMI Safety Analysis – Subset-118	1.2.6

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

3.1.1.5 The FMEA documents identified hazardous events connected to the ETCS Core Hazard (see definition in section 4.2) that could exist at the mandatory boundaries to the ERTMS/ETCS Reference Architecture. These events are used as the base events of the fault tree developed in Subset-088 Part 1.

3.1.1.6 Subset-118 identified hazardous events connected to the ETCS Auxiliary Hazard (see definition in section 4.2) and specified the Tolerable Hazard Rates for these. The results of Subset-118 are not incorporated in Subset-088 but referenced directly in the present document, see ETCS_OB10 in section 7.2.

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[1]. 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 achieved in order to ensure that ETCS may be safely integrated in any interoperable railway system.

4.1.1.2 The safety requirements defined in this document supplement those contained in the SRS and other subsets referenced by the TSI. Any specific application of ETCS will need risk assessment to be undertaken in accordance with the CCS TSI and other applicable relevant European Regulations; this process will be supported by the safety requirements defined herein. To achieve interoperability any on-board ETCS application shall respect the requirements stated in this specification (chapter 7). The requirements apportioned to track-side ETCS (chapter 8) shall be considered as a reference (e.g., for the development of trackside equipment suitable for general use also in demanding implementations), but less stringent safety requirements for trackside are allowed, if the risk assessment proves that they are sufficient to meet the safety objective for the service without exporting to any other subsystem requirements in addition to the ones specified in the corresponding TSIs.

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 on-board 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 9.4.

4.1.1.7 The safety requirements are related to a safety function for the entity under consideration. For the ETCS Core Hazard, this specific safety function is defined in Subset-088

[1] Although the scope of this specification is generally restricted to Level 1 and 2, scenarios from Level 0 was also considered when analysing the ETCS Auxiliary Hazard in Subset-118. The reason is that it was identified that the potentially most restrictive scenarios with regards to the DMI input/output could actually be derived from operation in Level 0. The safety target used for operation in Level 0 is explained in paragraph 4.2.1.10.

Part 3 along with its associated hazard. The defined hazard is repeated in this part. For the ETCS Auxiliary Hazard, Subset-118 analyses hazards associated with the DMI functions that are at the same level as, and independent of, the ETCS Core Hazard.

4.1.1.8 The safety requirements are given as Tolerable hazard rates (THRs) in section 4.2 and the apportionment to on-board and track-side ETCS equipment is done in chapter 6, taking into account the considerations on the communication between ETCS on-board and trackside made in chapter 5.

4.1.1.9 Intentionally deleted.

4.1.1.10 Subset-088 Parts 1 & 2 provided details on the various claims made which would mitigate against the emergence of the ETCS 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 9.4.

4.1.1.12 Note 1: The THR does not include failures due to causes external to the Architecture in Figure 4, such as operational errors, dragging equipment etc.

4.1.1.13 Note 2: When the term of “the Architecture in Figure 4” is used in this document, it is always meant the architecture which originally comes from the ERTMS/ETCS Reference Architecture (as it is introduced in chapter 2 of Subset-026), but because of its different purpose, it differs in some details. See chapter 13 for the purpose of the Architecture in Figure 4.

4.2 System Context

4.2.1.1 All of the analyses are undertaken against the representation shown below. This puts the ETCS functionality as defined by the ERTMS/ETCS Reference Architecture, in its operational environment of an interoperable railway as mandated by the European Directives on the Interoperability of the rail system.

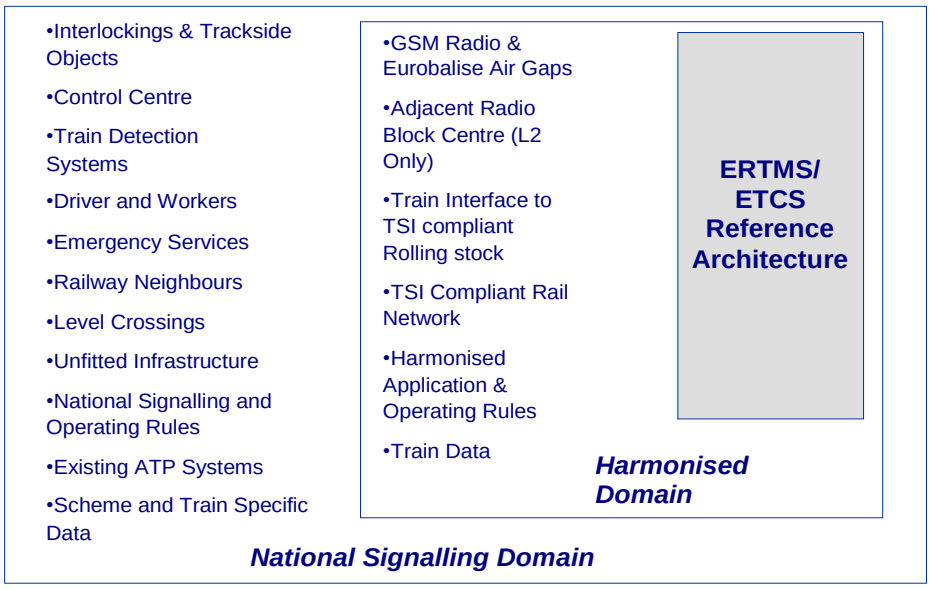


Figure 1: The ERTMS/ETCS Reference Architecture in its Context

4.2.1.2 With “ERTMS/ETCS 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 ERTMS/ETCS 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 ERTMS/ETCS 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 ERTMS/ETCS 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 This specification refers to the role of ETCS as

To provide the driver with information to allow him to drive the train safely and to enforce respect of this information, to the extent advised to ETCS.

4.2.1.7 The following shall be noted:

4.2.1.7.1 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).

4.2.1.7.2 The extent to which information about safe train operation is advised to ETCS varies in different modes. For example, in SR and LS mode only a limited amount of information about train safety is handled via ETCS, thus placing a larger responsibility on the driver. The distribution of responsibility between ETCS and driver is specified in Subset-026, chapter 4. Still, in these modes, important information such as train speed is provided to the driver to allow him to drive the train safely, and must be done so correctly in order not to create a possible hazard.

4.2.1.8 Thus it is necessary to define two different hazards of ETCS to distinguish between these two situations:

- For the case that ETCS has information on safe speed and distance (hazard is denoted “ETCS Core Hazard”):

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

- For the case that ETCS does not have information on safe speed and distance (hazard is denoted “ETCS Auxiliary Hazard”):

  ETCS interacts erroneously with the driver so that safe train operation, not supervised by ETCS, is jeopardized.

4.2.1.8.1 Note: Normally, the speed and distance jointly define the safe limits which are exceeded in the ETCS Core Hazard. The ETCS Core Hazard is formulated with the “or” to cover also the cases where a certain speed is not obviously connected to the distance supervision, e.g. train trip, standstill supervision, SR distance etc.

4.2.1.9 According to the principles explained in section 4.1 and the provisions of the CCS TSI, the maximum allowed rate of occurrence of the ETCS Core Hazard is $1.0*10^{-9}$ / hour for ETCS on-board and 10^{-9} / hour for ETCS trackside installed in an area visited by a train during a reference mission defined in section 9.4.

4.2.1.10 For the ETCS Auxiliary Hazard (including Level 0), the risk acceptance criterion in Common Safety Methods for Risk Assessment (EC 2009/352) is used, together with an extension described in section 5.4 of Subset-118. Note however that this criterion is broken down to THR values of the technical equipment in the present document. Thus, fulfilment of the risk acceptance criteria for the ETCS Auxiliary Hazard is fully covered by fulfilling the detailed requirements in ETCS_OB10.

4.2.1.11 The hazards and their 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 ERTMS/ETCS Reference

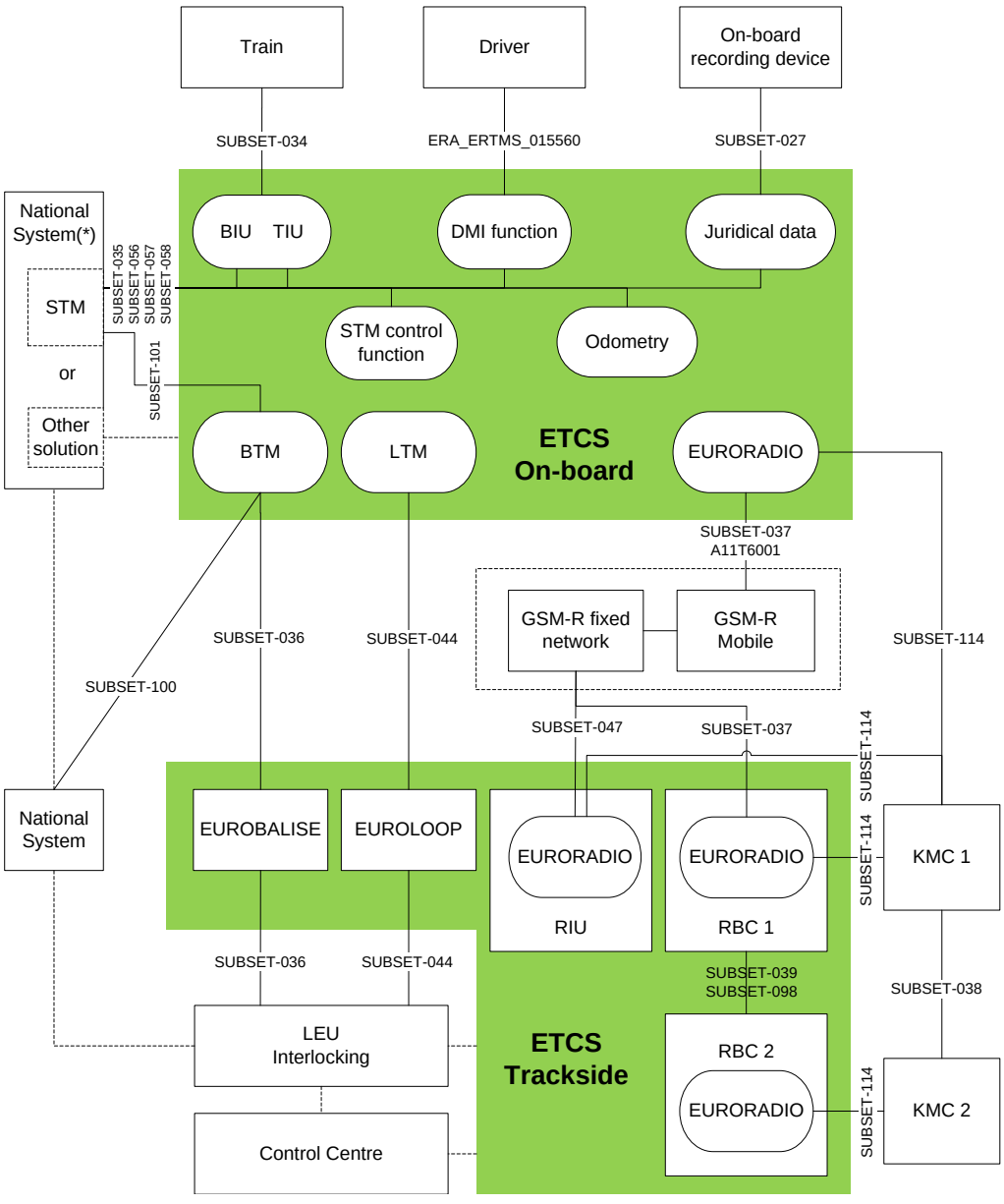
Architecture as defined in the SRS. Thus, failures due to operators (e.g. Driver, signalman and maintenance staff) and operational rules are not included in these hazards or their THR.

4.2.1.12 The THR is given as a rate per hour for a typical journey (see further section 9.4) where many of the ETCS operational modes may be used. Apportionment of the THR for the ETCS Core 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 ERTMS/ETCS Reference Architecture

4.3.1.1 The part denoted as “ERTMS/ETCS Reference Architecture” in paragraph 4.2.1.1 is a functional architecture as depicted below.



(*) Depending on its functionality and the desired configuration, the national system can be addressed either via an STM using the standard interface or via another national solution

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

4.3.1.2 Note: In the ETCS specifications, the interface to the “other solution” addressing the national system is not specified. Therefore, it is not further studied here.

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 $THR_{On\text{-}board}$ 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 Rolling Stock subsystem, as more appropriate for the specific case, anyway it has to be ensured that the safety requirements of both subsystems are not prejudiced.

4.3.1.5 Also the physical border between the ERTMS/ETCS trackside interoperability constituent (especially between the RBC or LEU) and the interlocking is not standardized; the supplier of the ERTMS/ETCS trackside shall clearly identify the borders of the equipment put on the market, i.e. the limits of the system to which the $THR_{Trackside}$ applies.

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 and Subset-118 as events that could lead to the ETCS Core Hazard and ETCS Auxiliary Hazard, respectively. 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 on-board equipment and similarly, TR refers to a requirement on the ETCS trackside equipment.

4.6 Process Requirements

4.6.1.1 The safety performance of the system where ETCS is applied is crucially dependent not only upon the performance of ETCS itself, but also upon the quality of data from sources external to ETCS, transferred to ETCS. Therefore requirements are placed on the corresponding processes where necessary. These requirements demand that the process being adopted shall be of a quality level that is appropriate to the required safety level. This should be interpreted to mean that

- the criticality of the data need to be determined from an overall railway system safety perspective

- 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 to the required safety level, taking into account the functional properties of ETCS and the safety integrity requirements specified in the present document

4.6.1.2 The above does not imply that processes need harmonising; in fact the definition of the processes is outside the scope of this document.

5. ETCS SYSTEM PERSPECTIVE ON TRANSMISSION SUBSYSTEMS

5.1 Corruption of messages

5.1.1.1 According to EN 50159[2], 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 THRs, 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 on-board 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 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

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

has been broken down to the grouping of constituents (ETCS on-board 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 on-board, 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 infill 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 infill Eurobalise. In summary, no safety target is given for the deletion of any infill messages[3].

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 cannot be estimated. The protection offered by the cryptographic safety code defined in Euroradio specifications may be considered sufficient,

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

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 ETCS Core Hazard

6.1.1.1 The ETCS Core Hazard and the associated THRs has been defined in paragraphs 4.2.1.8 and 4.2.1.9.

6.1.1.2 Intentionally deleted.

6.1.1.3 This specification allocates 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'. The functions corresponding to the 'transmission events' are actually carried out by either the on-board or trackside equipment. To respect the equal values of THR for on-board and track-side ETCS, the allocation according to Figure 3 is performed. Figure 3 also introduces the terms $THR_{On\text{-}board}$ and $THR_{Trackside}$ denoting the numerical safety requirement for the purely on-board and trackside functions. These are further elaborated in sections 7.2 and 8.2, respectively. The THR figures apportioned to the transmission functions are further elaborated in Subset-088 and the resulting requirements are presented in 7.3 and 8.3.

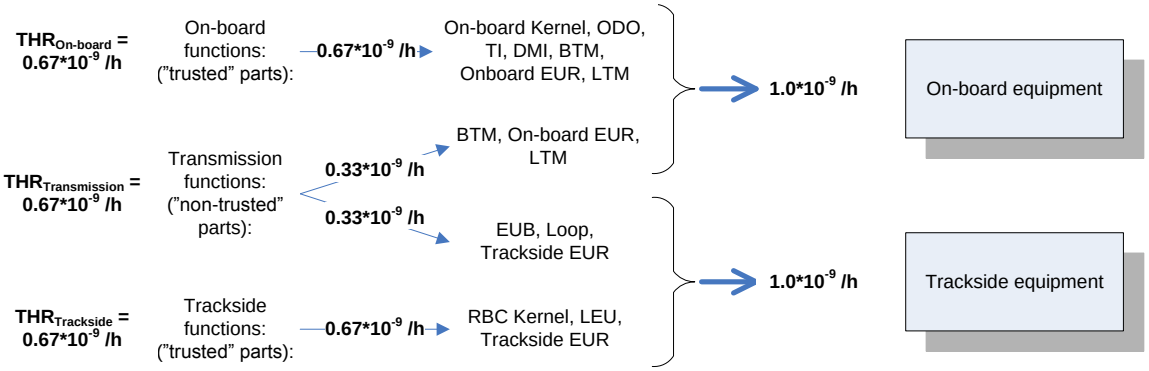


Figure 3: Principles for apportionment of THRs to ETCS equipment.

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.

6.2 ETCS Auxiliary Hazard

6.2.1.1 The ETCS Auxiliary Hazard and the associated THRs have been defined in paragraphs 4.2.1.8 and 4.2.1.10.

6.2.1.2 The whole risk acceptance criterion for the ETCS Auxiliary Hazard is allocated to the on-board equipment, since the contributions coming from the trackside equipment are considered negligible.

7. SAFETY REQUIREMENTS FOR THE ETCS ON-BOARD 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, electromagnetic interference etc) according to the indications in the applicable Technical Specification for Interoperability.

7.1.1.3 The dangerous failure for the ETCS on-board equipment, connected to the ETCS Core Hazard, is defined as,

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

7.1.1.3.1 The dangerous failure for the ETCS on-board equipment, connected to the ETCS Auxiliary Hazard, is defined as,

Failure to interact correctly with the driver regarding information not supervised by ETCS.

7.1.1.3.2 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 specifications in §3.1.1.2 must be fulfilled. .

7.2 ETCS on-board equipment except transmission system

ETCS_OB01	ETCS Core Hazard THR The hazard rate for the ETCS on-board 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 (background information is provided by 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 $THR_{On\text{-}board}$ taking into account at least the following events, as defined in Annex A:

- KERNEL-1 - KERNEL-34
- ODO-1 - ODO-4
- TI-1 - TI-11
- MMI-1 - MMI-6

- 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 on-board equipment. Therefore, the following requirement for ETCS is formulated:

ETCS_OB02	The ETCS On-board Data entry process must be of a quality level that is appropriate to the required safety level. See further section 4.6.1.1.. (background information is provided by Subset-088 Part 3, paragraph 12.6.3.1)

7.2.1.5 Intentionally deleted.

ETCS_OB03	Intentionally deleted.
ETCS_OB04	Intentionally deleted.

ETCS_OB10

ETCS Auxiliary Hazard THR

The ETCS on-board system shall be shown not to exceed the following tolerable hazard rates:

Hazardous Situation		THR (failures per hour)
DMI-01a	Failure to provide Warning indication	$1.0*10^{-4}$
DMI-01b	Valid ETCS on-board output via DMI obscured by erroneous output (audio or visual)	$2.0*10^{-4}$
DMI-01c	Failure to display request for acknowledgement	$2.0*10^{-5}$
MMI-2f	Failure to display Override status (failure mode deletion), including false enabling of override selection	$2.0*10^{-5}$
DMI-01f	Failure to display ACK for RV request	$2.0*10^{-4}$
DMI-01g	Failure to display Air Tightness Control	$2.0*10^{-5}$
DMI-02a	False presentation of Warning	$2.0*10^{-5}$
DMI-02b	False presentation of IS mode (shown as IS mode when not)	$2.0*10^{-2}$

DMI-02c	False presentation of brake indication	$1.0*10^{-3}$
MMI-2f	Failure to display Override status (failure mode insertion), including false enabling of override selection	$1.0*10^{-3}$
DMI-02g	False presentation of “LX not protected”	$2.0*10^{-5}$
MMI-2c	False presentation of track adhesion factor (shown as applied when not)	$1.3*10^{-5}$
DMI-03e	Wrong fixed text message displayed	$2.0*10^{-6}$
DMI-03f	“Tunnel stopping area” displayed at the wrong geographical place	$2.0*10^{-4}$
MMI-2a.1	False presentation of train speed	$7.4*10^{-7}$
MMI-2b	False presentation of mode	$1.0*10^{-6}$
DMI-04a	False command to exit shunting	$4.0*10^{-3}$
DMI-04c	False START command	$2.0*10^{-2}$
MMI-1g	False request for SH mode	$8.0*10^{-5}$
DMI-04g	Spurious request to change to another ETCS Level	$4.0*10^{-5}$
DMI-04h	Spurious acknowledgement of intervention leading to release of emergency or service brake	$2.0*10^{-6}$
DMI-04j	False Isolation command	$2.0*10^{-7}$
MMI-1a	False acknowledgement of mode change to less restrictive mode	$4.0*10^{-6}$
MMI-1b	False Command to enter NL mode	$2.0*10^{-2}$
MMI-1d	False acknowledgement of Level Transition	$4.0*10^{-5}$
MMI-6	Falsification of Virtual Balise Cover (failure mode corruption)	$4.0*10^{-7}$
MMI-6	Falsification of Virtual Balise Cover (failure mode insertion)	$3.0*10^{-6}$
DMI-05a	Deleted Level transition acknowledgement	$1.0*10^{-5}$
DMI-05b	Deleted acknowledgement	$1.0*10^{-5}$
DMI-05e	Deleted driver request to apply Track Adhesion Factor	$2.0*10^{-5}$
DMI-05f	Deleted Reversing mode acknowledgement	$2.0*10^{-4}$

(background information is provided by Subset-118)

7.3 ETCS on-board transmission system

7.3.1 Radio channel

ETCS_OB05	Corruption of radio messages The requirement for the non-trusted part of OB-EUR-H4[4] is that the non-trusted ETCS on-board 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 / hour (background information is provided by Subset-088 Part 3, paragraph 12.5.1.1)

[4] For trusted part, see paragraph 7.2.1.2.

7.3.2 Balise Channel

ETCS_OB06	Corruption of balise group message The requirement for the non-trusted part of BTM-H4[5] is that the non-trusted ETCS on-board 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 / hour (background information is provided by Subset-088 Part 3, paragraph 12.5.2.1)
ETCS_OB07	Failure of balise group detection The rate of failure for the ETCS on-board to fail to detect a balise group shall be shown not to exceed $1.0 * 10^{-7}$ dangerous failures / hour (background information is provided by 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 / hour In Subset-036 this requirement is distributed between ETCS on-board and track-side equipment. This yields the requirement for the ETCS on-board equipment to have a maximum unavailability of $1.0 * 10^{-6}$ with regards to each of the following failure modes: • The ETCS on-board equipment is more sensitive than expected. • The ETCS on-board equipment is transmitting more Tele-powering field than specified. See subset 036, Annex F for details of potential failure modes and possible solutions. (background information is provided by Subset-088 Part 3, paragraph 12.5.2.5 and subset-036 paragraph 6.4.5.2)

[5] 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[6] is that the non-trusted ETCS on-board 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 / hour (background information is provided by Subset-088 Part 3, paragraphs 12.5.2.1 & 12.5.2.3)

[6] 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, electromagnetic interference 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 on-board supervision in accordance with the data advised to the ETCS trackside from external entities.

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

Note: External entities include the assumption that the ETCS On-board provides a correct train position 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 specifications in §3.1.1.2 must be fulfilled.

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 (background information is provided by 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, RBC-3 and RBC-4 (level 2 only)
- LEU-H4 (level 1 only)[7]
- TR-EUR-H4 (level 2 only) (the parts of the hazard that arise due to failures inside the trusted part of the transmission channel)

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

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[8] 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 / hour (background information is provided by Subset-088 Part 3, paragraph 12.5.1.1)

8.3.2 Balise channel

ETCS_TR03	Corruption of balise group 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 / hour (background information is provided by Subset-088 Part 3, paragraph 12.5.2.1)
ETCS_TR04	Failure of a balise group being detectable The rate of failure for a balise group with at least two balises to become undetectable (according to the definition in Subset-036), shall be shown not to exceed, $1.0 * 10^{-9}$ dangerous failures / 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 in Subset-036 from the above requirement on a balise group of two balises. (background information is provided by 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 is $1.0 * 10^{-9}$ dangerous failures / hour

[8] For trusted part, see paragraph 8.2.1.2.

	In Subset-036 this requirement is distributed between ETCS on-board 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 Part 3 Annex A, considering the ETCS on-board performance stated in ETCS_OB08 A methodology for this is suggested in Subset-036 Annex F, although the actual accomplishment of the analysis is supplier and application specific. (background information is provided by 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[9] two balise groups[10] 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, (3) constitutes a border balise group giving more restrictive National Values, (4) gives Level Crossing information or (5) gives Virtual Balise Cover order. (background information is provided by Subset-088 Part 3, Annex A, paragraph 3.3.1.1)

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

[10] 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 EUL-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 / hour (background information is provided by 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 ETCS system 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:
  - ETCS Trackside Data Preparation. This refers to the collection, interpretation, accuracy and allocation of data relating to the railway network and the engineering of it into ETCS Trackside Data (both installation and mission[11] specific).
  - ETCS On-board Data Preparation. This refers to the collection of train related data and the engineering of it into ETCS On-board Data, which is defined as Train Data, Additional Data and any application specific data needed (both installation and mission[12] specific).
  - ETCS Trackside System Deployment. This refers to the process of commissioning the prepared ETCS Trackside Data into the ETCS Trackside system.
  - ETCS On-board System Deployment. This refers to the process of commissioning the prepared ETCS On-board Data into the ETCS On-board system.
- 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)

[11] For example Temporary Speed Restrictions.

[12] For example Train Length.

9.2 Integrity Requirements for Trackside Data Preparation

EXT_SR01	The preparation of the ETCS Trackside Data is not part of ETCS, but shall be of a quality that is appropriate to the required safety level. See further paragraph 4.6.1.1. (background information is provided by Subset-088 Part 3, paragraph 12.6.2.1)

9.3 Integrity Requirements for the On-board Data Preparation

EXT_SR03	The preparation of the ETCS On-board Data is not part of ETCS, but shall be of a quality that is appropriate to the required safety level. See further paragraph 4.6.1.1. (background information is provided by Subset-088 Part 3, paragraph 12.6.3.1)

9.4 Integrity Requirements for ETCS Trackside System Deployment

EXT_SR02	The complete ETCS Trackside System Deployment process is not part of ETCS, but shall be of a quality that is appropriate to the required safety level. See further paragraph 4.6.1.1. (background information is provided by Subset-088 Part 3, paragraph 12.6.4.1)

9.5 Integrity Requirements for ETCS On-board System Deployment

EXT_SR05	The complete ETCS On-board System Deployment process is not part of ETCS (except what is defined in ETCS_OB02), but shall be of a quality that is appropriate to the required safety level. See further paragraph 4.6.1.1. (background information is provided by Subset-088 Part 3, paragraph 12.6.5.1)

9.6 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 THRs 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.

Example: A deviation which requires a special analysis would be the number of unlinked balise groups in a Limited Supervision application, which would most likely deviate significantly from the value stated in §12.2.1.16.

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 10.3.2.19. 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 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 travelled in one hour	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)[13]	1 in 1000 (*)	4 in 1000 (*)

[13] 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**
10.2.1.17	Number of Repositioning Balise groups (only Level 1)	1 in 100	1 in 100
10.2.1.18	Number of Level transitions (including NTC X - NTC 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 parameters, 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 group messages	150 - 650 h^{-1} (*)	50 - 150 h^{-1} (*)
10.3.2.4	Frequency of balise group 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}
10.3.2.1	Max. expected loss of train integrity	N/A	N/A
10.3.2.1	Mean Down time of a failed ETCS on-board balise receiver in an unfitted area	1 hour (*)	1 hour (*)
10.3.2.1	Mean down time of a non-detectable balise group. See Note C below.	24 hours (*)	24 hours (*)
10.3.2.1	Time spent with a need for reduced track adhesion factor in the brake curve calculations (slippery rail) (failure of event GOOD ADHESION in Subset-118)	< 5 % (*)	< 5 % (*)
10.3.2.1	Time spent on track with slope (risk of roll-away if no brakes applied) (failure of event GRADIENT in Subset-118)	< 10 % (*)	< 10 % (*)
10.3.2.1	Time spent in Level 0 (failure of event IN L0 in Subset-118)	< 10 % (*)	< 10 % (*)

Reference Number	Parameter description	Value (For (*) see paragraph 10.1.1.4)	
		High-speed Rail	**Conventional Rail**
10.3.2.1	Time spent in modes without ETCS supervision of safe speed and distance (e.g. UN and LS) (failure of event MODE SUPERVISED in Subset-118)	< 20 % (*)	< 20 % (*)
10.3.2.1	Time spent in SB mode (failure of events NO UN PROPOSAL, NOT IN SB in Subset-118)	< 5 % (*)	< 5 % (*)
10.3.2.1	Time spent in standstill (operational) (failure of event STANDSTILL in Subset-118)	< 5 % (*)	< 5 % (*)

10.3.2.19 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 way-side 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	Probability of failure For (*) see paragraph 10.1.1.4	
		High-speed Rail	**Conventional Rail**
10.4.1.2	The driver performs an action in a non-complex situation which is covered by training and procedures. For example: - Probability of driver failing to verify a level transition function at an ETCS border. See Rule A. - Probability of driver passing a safe authorisation when driving in SR mode. See Rule B.	0,001 (*)	0,001 (*)
10.4.1.3	The driver recognises that ETCS is behaving in a way that is clearly contrary to their expectations. To fall into this category, the contradiction must be obvious. OR The driver manages to operate the train safely, although a certain degree of ETCS support which is normally present, has failed. To fall into this category, the reliance on the failed ETCS support must be fairly low.	0.01 (*)	0.01 (*)
10.4.1.4	The driver recognises that ETCS is behaving in a way that is contrary to their expectations. The contradiction is not obvious as in 10.4.1.3, but still clear to a driver who is paying normal attention. OR The driver manages to operate the train safely, although a certain degree of ETCS support which is normally present, has failed. To fall into this category, the reliance on the failed ETCS support is higher than in 10.4.1.3.	0.1 (*)	0.1 (*)
10.4.1.5	The driver performs an action in a more or less complex / pressing situation which is not covered by training or procedures.	0.2 – 0.9 (*)	0.2 – 0.9 (*)

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

10.4.1.7 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.

10.4.1.8 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 Subset-023, 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

See SRS chapter 3.18.3.

Additional Data

See SRS chapter 3.18.4.

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 infill area information
- Session control information (see below)
- Infill 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
- 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.

11.1.1.5 In addition to the general Subset-023, the following abbreviations are used:

CCS	Control-Command and Signalling
DRV	Driver
EUB	Eurobalise
EUL	Euroloop
EUR	Euroradio
EXT	External to ETCS
KMC	Key Management Centre
OB-	On-board-
ODO	Odometry
SSS	Standstill Supervision
TAF	Track Ahead Free
THR	Tolerable Hazard Rate
TR-	Trackside-

TRANS	Transmission
TSI	Technical Specifications for Interoperability

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 Core 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.

12.1.1.3 Note: The events DMI-xx are denoted separately from the MMI-xx events to signify that they are not expected to lead to any failures related to the ETCS Core Hazard. They are relevant only in connection with the ETCS Auxiliary Hazard in ETCS_OB10.

Event Id.	Event Description	Corresponding performance requirement in Subset-041
DMI-03e	Wrong fixed text message displayed	
DMI-04h	Spurious acknowledgement of intervention leading to release of emergency or service brake	
DMI-04j	False Isolation command	
MMI-1a	False acknowledgement of mode change to less restrictive mode	
MMI-1b	False command to enter NL mode	
MMI-1c	False command of Override request	
MMI-1d	False acknowledgement of Level Transition	
MMI-1e	False acknowledgement of Train Trip	
MMI-1f	False acknowledgement of Track Ahead Free	
MMI-1g	False request for SH mode	

Event Id.	Event Description	Corresponding performance requirement in Subset-041
MMI-1h	False acknowledgement of undesired train movement (RAP, RMP, SSS, PT distance and reversing distance)	
MMI-2a.1	False presentation of train speed	
MMI-2a.2	False presentation of speed (except train speed) or distance, including supervision status	
MMI-2b	False presentation of mode	
MMI-2c	False presentation of track adhesion factor	
MMI-2d	Failure to present Entry in FS/OS information	
MMI-2e	False presentation of train data/additional data	
MMI-2f	Failure to display Override status, including false enabling of override selection	
MMI-2g	Failure to present acknowledgement message to a less restrictive mode	
MMI-2h	False presentation of TAF request	
MMI-2i	Failure to present LX “not protected” information	
MMI-2j	False presentation of reversing allowed	
MMI-2k	False presentation of level transition announcement	
MMI-3	Falsification of driver’s train data / additional data input stored on-board	
MMI-4	Falsification of SR speed/distance data	
MMI-5	Falsification of train integrity confirmation input	
MMI-6	Falsification of Virtual Balise Cover	
ODO-1	Incorrect standstill indication	

Event Id.	Event Description	Corresponding performance requirement in Subset-041
ODO-2	Speed measurement underestimates trains actual speed	5.3.1.2: Accuracy of speed known on-board, in ceiling speed monitoring, release speed monitoring and in target speed monitoring in case the compensation of the speed measurement inaccuracy is inhibited
ODO-3	Incorrect actual physical speed direction	
ODO-4	The confidence interval for distance measurement does not include the real position of the train	
KERNEL-1	Balise linking consistency checking failure	In case the message is received but the linking is not consistent: 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, in ceiling speed monitoring, release speed monitoring and in target speed monitoring in case the compensation of the speed measurement inaccuracy is inhibited
KERNEL-10	Functional failure of standstill detection	
KERNEL-11	Incorrect traction/braking model (e.g. brake use restrictions)	

Event Id.	Event Description	Corresponding performance requirement in Subset-041
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, LS and FS	5.2.1.1: Delay between receiving of a balise message and applying the emergency brake 5.2.1.13: Delay between passing an EOA/LOA 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
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 position 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	

Event Id.	Event Description	Corresponding performance requirement in Subset-041
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.
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 5.2.1.13: Delay between passing an EOA/LOA and applying the emergency brake
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	

Event Id.	Event Description	Corresponding performance requirement in Subset-041
TI-6b	Wrong Cabin considered as Active	
TI-7	Inappropriate passive shunting request	
TI-8	Inappropriate Non Leading permitted signal received	
TI-10	Falsification of train data received by External Source	
TI-11	Traction Cut-Off not commanded when required	
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 on-board BTM function	
BTM-H4	Transmission to the on-board kernel of an erroneous telegram, interpretable as correct, due to failure within the on-board BTM function	

Event Id.	Event Description	Corresponding performance requirement in Subset-041
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 on-board 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	
EUL-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	The RBC misinterprets a message from an adjacent RBC, causing incorrect message to ETCS on-board	

Event Id.	Event Description	Corresponding performance requirement in Subset-041
RBC-4	The RBC gives an erroneous message to an adjacent RBC	

13. ANNEX B

13.1 Graphical Representation (Informative)

13.1.1.1 The figure below illustrates the hazardous events in Annex A. The architecture shown is based on the ERTMS/ETCS Reference Architecture defined in Subset-026, but differs in some details. The reason for this difference is that, in contrast to the ERTMS/ETCS Reference Architecture, the purpose of Figure 4 is to show the hazardous events in relation to the items to which THR is allocated.

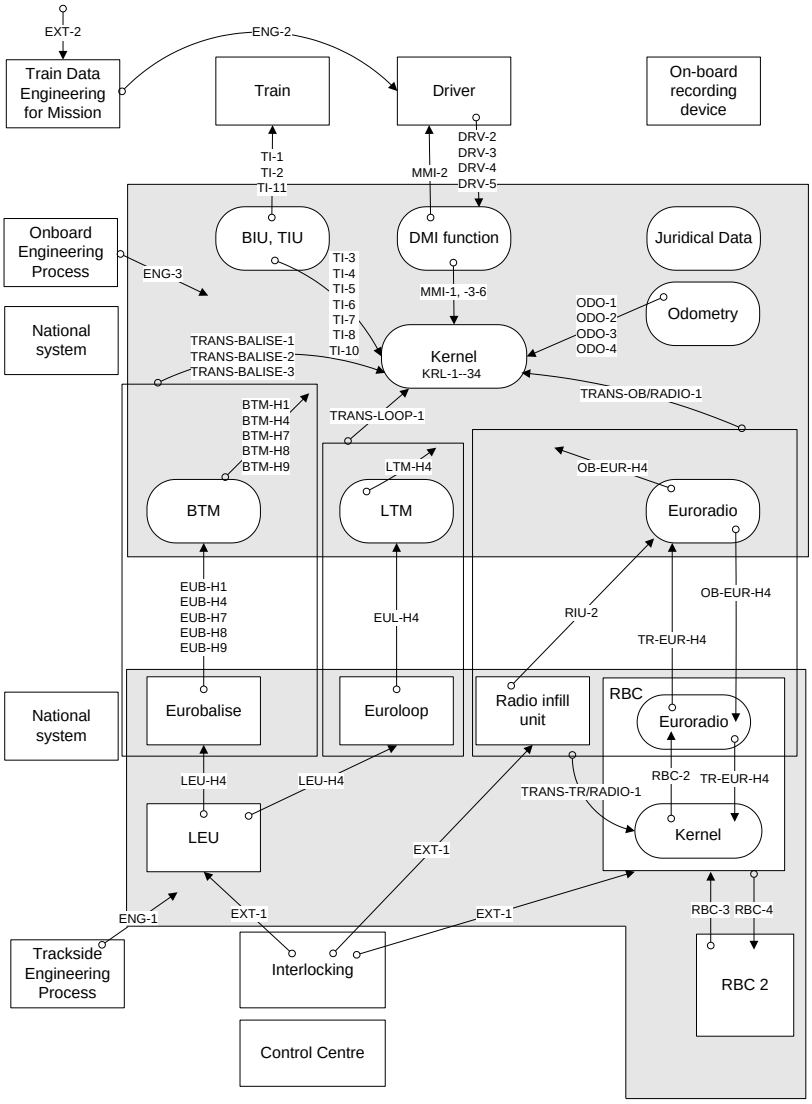


Figure 4: Graphical representation of the hazardous events within the ERTMS/ETCS Reference Architecture adapted for THR allocation.

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 ETCS Core Hazard as specified in paragraph 4.2.1.8. 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 ETCS 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 On-board	MMI-1h, -2a.1, 2a.2, -2f, -2i, -2j
Override procedure	MMI-1c
Mode Transition Table	KERNEL-16 MMI-1a, -1b, -1d, -1e
Balise Linking	ODO-3, 4
Linking reaction	KERNEL-28[14]
Message Consistency Checks	[15]
Maximum distance between Balise Groups	ODO-4 KERNEL-28
Balise Groups contain at least two Balises for safety data	[16]
Balise detection	ODO-1, -3
Radio message acknowledgement	KERNEL-4
Radio link time out	KERNEL-5, -6, -18

[14] 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.

[15] 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. When the balise group message consistency reaction is disabled via packet 145, no safety related data, that if missed could lead to the ETCS core hazard, is allowed to be placed in that balise group. This requirement is brought forward in Subset-040.

[16] 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.