	ERTMS/ETCS	
	Failure Modes and Effects Analysis for Transmission System in Application Level 2	

REF : SUBSET-081-2

ISSUE : 3.6.0

DATE : 08-05-24

Company	Technical Approval	Management approval
ALSTOM		
AZD		
CAF		
HITACHI RAIL STS		
MERMEC		
SIEMENS		
THALES		

© This document has been developed and released by UNISIG

1. MODIFICATION HISTORY

Issue Number Date	Section Number	Modification / Description	Author
0.0.1 - 19-Jan-01	all	Creation	S. Adomeit
0.0.2 - 23-Jan-01	all	Discussion with SAB (SG member)	S. Adomeit
0.0.3 – 26-Jan-01	all	Revised after comments	S. Adomeit
0.0.4 – 08-Feb-01	5.2; 6; 7	Revised after comments Creation	S. Adomeit
0.1.0 – 28-Feb-01	4; 5	Revised after comments	S. Adomeit
0.1.1 – 27-Aug-01	4; 5	Revised after comments Level 1 specific reminder now deleted in the table removed to Subset-081-1	S. Adomeit
0.2.0 – 05-Feb-02	all	Revised to achieve consistency to other documents	S. Adomeit
2.0.0 – 05-Feb-02	version number	revised for delivery	S. Adomeit
2.2.2. 21-03-03		Final release after amendment to reflect the comments in the final report from the ISA's version 1.1 dated 07-03-03 as proposed via the Unisig consolidated review comments on the ISA report v 0.0.2 March 03.	WLH
2.2.3 17-09-07	all	Document updated for SRS 2.3.0 baseline.	I. Sáez
2.2.4 11-10-07		Administrative updates according to agreement in RAMS-meeting 2007:6	DARI
2.3.0 02-04-08		Administrative updates for baseline 2.3.0	DARI
2.3.1		Updates for baseline 3:	DARI

2011-05-31		- New version of references - CR637	
2.3.2 2011-07-01		- Subset-030/-031/-032/-091 removed as references - Conclusions reformulated	DARI
3.0.0 2011-09-30		Administrative updates for baseline 3	DARI
3.1.0 2012-01-19		Coordinated with Subset-026 v3.2.1, Subset-036 v2.5.7 and Subset-037 v2.3.6. EN 50159-1 and -2 changed to EN 50159	DARI
3.2.0 2012-02-24		Updates agreed during RAMS-meeting	DARI
3.3.0 2012-03-12		Baseline 3 release version	DARI

3.4.0
2014-03-26
		Corrections:
		  - 5.2.3.1 "loop infill" clarified
		  - 5.2.3.2 "SR distance information from loop" added
		  - 5.2.3.3 "Default loop information" added
		Updates for B3 MR1:
		  - 5.2.3.4 "Data to be used by applications outside ERTMS/ETCS" added due to CR1155
			DARI

3.4.1 2014-04-15		Updated according to comments from Siemens	DARI
3.4.2 2014-04-16		Formal updates during RAMS-meeting	DARI
3.4.3 2014-05-08		Baseline 3 1st maintenance release version	DARI
3.4.4 2015-05-25		Updates:	KLMO

		- 5.2.3.5 "LSSMA display toggle order" added Due to CR 1223	
3.4.5 2015-06-23		No updates. Document version increased to align with SUBSET-081-1	KLMO
3.4.6 2015-10-19		Updates: - 4.1.1.7 "GSM-R" updated to "radio transmission channel"	KLMO
3.4.7 2016-05-03		No updates. Document version increased to align with SUBSET-081-1.	Martin Vlcek
3.4.8 2016-06-14	3.1.1.5	Update of references to SUBSET-026, 036, 040 and 077.	Martin Vlcek
3.5.0 2016-06-20	No change	Baseline 3 2nd release version	RAMS WP
3.5.1 2022-11-08		Editorial changes Checked according to TSI 2022 publication, no changes necessary because of CR1304, CR1307, CR1341, CR1342	Mathias Wagner
3.5.2 2023-09-19		Editorial changes to 3.1.1.5.	RAMS WP
3.6.0 08-05-24		Update due to SG quality check Baseline 4 release version	RAMS WP

2.   TABLE OF CONTENTS

3. INTRODUCTION

3.1.1.1 The purpose of this study is to systematically evaluate and document the potential impact of a failure of each of the mandatory Interfaces of the Transmission System that occur at the boundary of the reference architecture. Each defined functional failure is assessed for its effects on the ETCS system and on train operation assuming that there are no other failures. The effects of each failure on train operation are assigned a severity category based upon the impact of such a failure on the safety of a passenger on the train.

3.1.1.2 Note that if some failures are noted as being a RAM issue only they are not developed further.

3.1.1.3 Note that there will be a separate document for each analysis and each Application Level. This will allow the level specific fault tree to refer to a unique set of FMEA's easing the problem of future modifications.

3.1.1.4 The analysis of the Transmission System interfaces has been carried out herein for Application Level 2.

3.1.1.5 The input documents used as a basis for this study are:
- UNISIG: SUBSET-077(Causal Analysis Process);
- UNISIG: SUBSET-026 (System Requirements Specification);
- UNISIG: SUBSET-036 (Eurobalise FFFIS);
- UNISIG: SUBSET-037 (Euroradio FIS);
- UNISIG: SUBSET-040 (Dimensioning and Engineering Rules);
- UNISIG: SUBSET-041 (Performance Requirements);
- UNISIG: SUBSET-044 (Euroloop FFFIS);
- CENELEC: EN 50159:2010.

4. SCOPE OF THE WORK

4.1.1.1 This FMEA considers a Transmission System defined according to EN 50159:

Safety related Transmission System

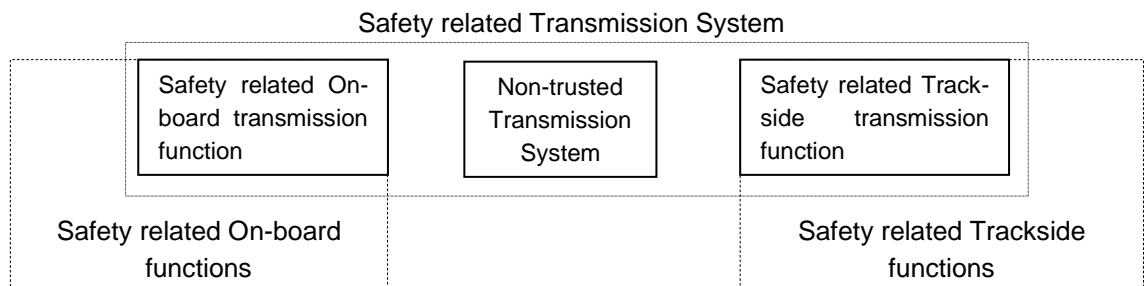| Safety related On-board transmission function	Non-trusted Transmission System	Safety related Track-side transmission function
Safety related On-board functions		Safety related Trackside functions

Figure 1: Overview

4.1.1.2 Note: Definition of Transmission System according to EN 50159: A service used by the application to communicate message streams between a number of participants, who may be sources or sinks of information.

4.1.1.3 The reference architecture therefore consists of:
- the non-trusted transmission system
- the safety related transmission functions (transmission and access protection) and
- the safety related application functions.

4.1.1.4 Three physical transmission systems will be considered: Euroradio, Eurobalise and Euroloop.

4.1.1.5 The non-trusted transmission system for Eurobalise consists of:
- Eurobalise[1]
- Airgap
- Passive onboard antenna

Excluded are:
- LEU / telegram generation
- BTM functionality (onboard receiver, decoding etc.)

4.1.1.6 The non-trusted transmission system for Euroloop consists of:
- Loop modem and cable
- Airgap
- Passive onboard antenna

Excluded are:
- LEU / telegram generation
- BTM functionality (onboard receiver, decoding etc.)

---

[1] The Eurobalise is here regarded as a part of the non-trusted transmission channel. This refers to its role in the Corruption of messages.

4.1.1.7 The non-trusted transmission system for Euroradio consists of:

- Fixed data network (e.g. ISDN)
- Radio transmission channel (base stations etc.)
- Airgap
- Onboard mobile and antenna

Excluded are:

- Cryptography and telegram generation
- RBC

4.1.1.8 The safety related functions (both transmission and protection related) will be carried out by the safety related ETCS onboard and trackside equipment (RBC, LEU) and the engineering process.

4.1.1.9 Threats to the safety related equipment (e.g. ETCS trackside and ETCS onboard) and thus to the safety related transmission functions are not considered here.

4.1.1.10 Only failure causes within the non-trusted transmission channel (equipment and air gap) and the corresponding threats (Please refer to 5.1.1.8) are therefore considered.

4.1.1.11 Note: The failure causes external to the non-trusted transmission system will not be detailed in the table but still apply to all messages and will be indicated here only (see 5.2.1.2 to 5.2.1.5)

4.1.1.12 This analysis considers a non-trusted transmission system which is not fully specified, since the real interface between safety related equipment, which fulfils the safety related transmission functions, and the non-trusted transmission system depends on the implementation chosen by each manufacturer. The airgap however is considered as clearly defined.

5. FMEA

5.1 Assumptions

5.1.1.1 To simplify the FMEA it is assumed that each message during one hour shall contain all possible data ("track to train" or "train to track"), so that the necessary failure rate for each message is the same and independent from the application.

5.1.1.2 The failure effect of each data item is analysed separately, always considering the worst case scenario (typically catastrophic failure effect). No further analysis of specific data items and their failure effects is therefore necessary (Refer to example in the table).

5.1.1.3 Because the architecture and size of the non-trusted transmission system is not fully specified, the possible failure causes are more or less unknown, therefore the corresponding threats are considered.

5.1.1.4 Note: The real failure causes are more or less meaningless therefore in the table often "any failure of the non-trusted transmission system" is used.

5.1.1.5 The following threats will be considered: Repetition, Deletion, Insertion, Re-sequencing, Corruption, Delay and Masquerade (refer to EN 50159).

5.1.1.6 The identified severity is defined/assessed without System Protection or if the System Protection fails.

5.1.1.7 Most cases of threats to transmitted data are handled within the safety related transmission system which therefore prevents in most cases the transmission of incorrect data to the application.

5.1.1.8 Only in case where the safety related transmission functions are insufficient (e.g. regarding Deletion), further detailed analysis of causes and effects within the application is necessary.

5.1.1.9 The following safety services shall be considered: Message authenticity, Message integrity, Message timeliness and Message sequence (refer to EN 50159).

© This document has been developed and released by UNISIG

5.2 FMEA Table

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.1.1	Balise message (1 to 8 balise telegrams), Loop message, Radio message (Track to Train and Train to Track)	Track Description, Linking Information, MA data, Emergency messages, System data, Location data, Specific answers	Repetition, Deletion, Insertion, Resequence, Corruption, Delay, Masquerade	any failure of the non-trusted transmission system	level 2, all modes	t.b.d see below	t.b.d see below	t.b.d see below		catastrophic	t.b.d see below

© This document has been developed and released by UNISIG

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.1.2				any failure of safety related On-board transmission functions at source or sink of information (e.g. inside onboard kernel)						catastrophic	Design and Implementation process (Project or Product specific)

© This document has been developed and released by UNISIG

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.1.3				any failure of safety related Trackside transmission functions at source or sink of information (e.g. RBC kernel; inside LEU; or during Balise programming)						catastrophic	Design and Implementation process (Project or Product specific)
5.2.1.4				wrong Engineering data or wrong installation					Additional Engineering and Installation processes for project specific applications	catastrophic	Related Engineering and/or installation rules for Eurobalise transmission system must be respected (See Subset-040, Subset-036)
5.2.1.5				wrong route information at external interface (e.g. interlocking)					Project specific analysis	catastrophic	

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.1.6	Balise message (1 to 8 balise telegrams), Loop message, Radio message (Track to Train and Train to Track)	Telegrams (Data Items at lower level - means data items as a part of a message)	Repetition, Deletion, Insertion, Resequence, Corruption, Delay, Masquerade	any failure of the non-trusted transmission system	this is independent of level or mode	wrong information to onboard or to trackside	wrong speed or distance calculation	Exceedance of safe speed / distance by train		catastrophic	Definition of Telegrams, Messages and the Rules for Data Consistency and/or safety coding "Message integrity"

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.2.1	Balise message (1 to 8 balise telegrams)	Track Description, Linking Information, MA data, System data (possible content of all balise telegrams "track to train")	Repetition	any failure of the non-trusted transmission system, e.g. memory effects	level 2, all modes (in L2 some information is only accepted if transition to L1 is announ-ced.)	misuse of information onboard see below	wrong speed or distance calculation see below	Exceedance of safe speed / distance by train see below		catastrophic	Linking of Balise Groups "Message sequence"
5.2.2.1 a)	example:	MA Data e.g. MA			level 2 (level-transition to level 1)	using of wrong MA (old MA)	wrong speed and/or distance calculated	Exceedance of safe speed / distance by train		catastrophic	

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.2.2	Balise message (1 to 8 balise telegrams)	Track Description, Linking Information, MA data, System data	Deletion (Deletion of the message, independent if a balise group itself is found or not)	any failure of the non-trusted transmission system, e.g. no TSR, no Stop if in SR etc. an other failure cause is systematic e.g. message rejected due to Data Consistency problems (please refer to SRS 3.16.2)	level 2, all modes	data not updated to train	wrong speed or distance calculation	Exceedance of safe speed / distance by train		catastrophic	Linking of Balise Groups "Message sequence"
5.2.2.2 a)	example:	System Data e.g. - National Values / Default Values - Specific system data (e.g. EOLM; NID_C)				using of wrong national values	wrong speed and/or distance calculated	Exceedance of safe speed / distance by train	Specific trackside applications should check if their national values are more restrictive from default ones given in SRS. Any train must be aware of such a restrictive values A proper layout configuration is required (transferred to Subset-113 ETCS-H0005)	catastrophic	NID_C in case of inconsistencies default values will be used Linking of Balise Groups "Message sequence" Please refer to SRS 3.18.2.4/5

© This document has been developed and released by UNISIG

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.2.3				any failure of the non-trusted transmission system, e.g. no TSR, no Level transition, no Stop if in SR, train trip valid for one direction only (please refer to SRS 3.6.3.1.4.1 etc.	level 2: FS, OS, SR, LS;	data not updated to train or no reaction	wrong speed or distance calculation	Exceedance of safe speed / distance by train / missing level transition	high availability of Balise group messages (e.g. only balise groups with more than one balise) Driver responsibility under degraded modes such as SR, UN, SH, etc.	catastrophic	Duplication of unlinked balise groups (Subset026) Installation rules for: • Eurobalise on track (Subset040/Cp.4.1.1) • Passive antenna onboard (Subset040/Cp.4.1.1 & Subset036)
5.2.2.4	Balise message (1 to 8 balise telegrams)	Track Description, Linking Information, MA data, System data	Insertion, Resequence	any failure of the non-trusted transmission system (cross talk, memory effects) (regarding memory effects please refer to "Repetition")	level 2, all modes	misuse or wrong information onboard	wrong speed or distance calculation	Exceedance of safe speed / distance by train		catastrophic	memorising of complete telegrams or messages must be excluded within the non-trusted transmission system Linking of Balise Groups "Message sequence"

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.2.4 a)		Track Description, Linking Information, MA data, System data Repositioning information in particular (please refer to SRS 3.4.2.2.2)		any failure of the non-trusted transmission system (cross talk, memory effects)	level 2, start of mission SR --> FS (linking is not available or is not applied)	using of a wrong Balise Group for position Report;	leads to mode transition SR --> FS starting driving with an wrong allocated authority;	Exceedance of safe speed / distance by train	apply balise groups with more than one balise "Message authenticity"	catastrophic	Eurobalise transmission has been designed to feature intrinsic safety against cross talk. Installation rules for: • Eurobalise on track (Subset040/Cp.4.1.1) • Passive antenna onboard (Subset040/Cp.4.1.1) Cross-talk protection requirements. (Subset036/Cp4.2.5) Integrity requirements for cross-talk in Subset-091 (ETCS_TR05, ETCS_OB08).
5.2.2.5	Balise message (1 to 8 balise telegrams)	Track Description, Linking Information, MA data, System data	Corruption	any failure of the non-trusted transmission system	level 2, all modes	wrong information to onboard or to trackside	wrong speed or distance calculation	Exceedance of safe speed / distance by train		catastrophic	safety coding "Message integrity" Coding requirements in Subset036/Cp.4.3
5.2.2.5 a)	example:	Linking Information				using of wrong linking distances	wrong distance to EOA calculated	Exceedance of safe distance by train		catastrophic	

© This document has been developed and released by UNISIG

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.2.6	Balise message (1 to 8 balise telegrams)	Track Description, Linking Information, MA data, System data	Delay	any failure of the non-trusted transmission system (e.g. onboard delay)	level 2, all modes	wrong location reference	wrong speed or distance calculation	Exceedance of safe speed / distance by train		catastrophic	memorizing of complete telegrams or messages must be excluded within the non-trusted transmission system Linking of balise groups. Expectation window for the balise group may be reached before the message is received from non-trusted part System Performances (Subset_041/Requirement 5.2.1.1"response times", the non-trusted transmission part also contributes to this performance). (transferred to the definition of the applicable KERNEL-events in Subset-091 chapter 12)
5.2.2.7	Balise message (1 to 8 balise telegrams)	Track Description, Linking Information, MA data, System data	Masquerade								Not taken into account as balise transmission system is a closed transmission system

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.3.1	Loop message	Infill information: Track Description, Linking Information, MA data, System data	any	any failure of the non-trusted transmission system or usual information for mixed level	any	no operational impact	no operational impact	no operational impact		none	Infill information is rejected in Level 2 •

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.3.2		Non-infill information: - SR distance information from loop	any	any failure of the non-trusted transmission system or usual information for mixed level	any	no operational impact	no operational impact	no operational impact		none	pkt13 is rejected in Level 2

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.3.3		Non-infill information: - Default Loop information	any	any failure of the non-trusted transmission system	any	No operational impact	No operational impact	No operational impact		none	

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.3.4		Non-infill information: - Data to be used by applications outside ERTMS/ETCS	any	any failure of the non-trusted transmission system	any	application specific	application specific	application specific	application specific The consequences are not related tot he ETCS Core Hazard. As worst case, the severity ‚catastrohic' is assigned.	catastrophic	For Corruption, Repetition, Insertion and Resequence, there are safety measures; see e.g. Subest-081-1 paragraphs 5.2.3.5 and 5.2.3.6. For Deletion and Delay, there are no safety measures.

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.3.5		Non-infill information: - LSSMA display toggle order	any	any failure of the non-trusted transmission system		no operational impact	no operational impact	no operational impact		none	pkt180 is rejected in Level 2

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects Local	Failure Effects Intermediate	Failure Effects Initial End Effect	System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
5.2.4.1	Radio message (Track to Train)	Track Description, Linking Information, MA data, System data, Emergency messages	Repetition, Insertion, Resequence	any failure of the non-trusted transmission system, e.g. memory effects	level 2, all modes	wrong information to onboard	wrong speed or distance calculation	Exceedance of safe speed / distance by train		catastrophic	clear identification of messages (Time stamp) "Message sequence" message identity for some types of messages Safety Protocol in Subset037 Cp.7.2
5.2.4.2	Radio message (Track to Train)	Track Description, Linking Information, MA data, System data, Emergency messages	Deletion, Delay	any failure of the non-trusted transmission system	level 2, all modes	no complete information	wrong speed or distance calculation	Exceedance of safe speed / distance by train	Additional mitigations outside ETCS might be neccesary. Safety analysis must be performed for trackside specific applications. Impact of delayed/deleted messages send to train equipment must be checked (e.g. emergency messages, see below) (the issue is documented in Subset-091 §5.3)	catastrophic	clear identification of messages (Time stamp) and message acknowledgement "Message sequence" Please refer to SRS 3.7.2.2 Safety Protocol in Subset037 Cp.7.2
5.2.4.3		Emergency messages e.g. - Unconditional emergency stop - Revocation of emergency message			level 2, all modes; specific operation conditions	no Emergency information		Exceedance of safe speed / distance by train	Service External to ETCS (It is expected that using of Emergency Messages Service shall not deteriorate the safety of the system) (the issue is documented in Subset-091 §5.3)	catastrophic	using of high priority channel for conditional and unconditional emergency stop; supervision of radio link "Message timeliness"; acknowledgement of each message and/or inform the RBC separately

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.4.4	Radio message (Track to Train)	Track Description, Linking Information, MA data, System data, Emergency messages	Corruption	any failure of the non-trusted transmission system	level 2, all modes	wrong information to onboard	wrong speed or distance calculation	Exceedance of safe speed / distance by train		catastrophic	safety coding "Message integrity" Safety Protocol in Subset037 Cp.7.2
5.2.4.5	Radio message (Track to Train)	Track Description, Linking Information, MA data, System data, Emergency messages	Masquerade	any failure of the non-trusted transmission system	level 2, all modes	wrong information to onboard	wrong speed or distance calculation	Exceedance of safe speed / distance by train		catastrophic	Cryptographic techniques (Key management) "Message authenticity" Key Management system definition in Subset064

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects Local	Failure Effects Intermediate	Failure Effects Initial End Effect	System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
5.2.5.1	Radio message (Train to Track)	System data, Location data, Specific answers/re-quests (specific acknowledgements or requests)	Repetition, Insertion, Resequence	any failure of the non-trusted transmission system, e.g. memory effects	level 2, all modes	wrong information to trackside see below	generation of wrong messages "track to train"	Exceedance of safe speed / distance by train		catastrophic	clear identification of messages and its references (Time stamp; LRBG) "Message sequence" "Message authenticity" message identity for some types of messages Safety Protocol in Subset037 Cp.7.2
5.2.5.1 a)	example:	System data e.g. - Train Data - Additional data - Specific system data				wrong train data to trackside	generation of wrong messages "track to train"	onboard supervision reject information		RAM issue	
5.2.5.1 b)	example:	Specific answers / requests e.g. - Acknowledgement - Acknowledgement of Emergency Stop - Request to shorten MA is granted - Request to shorten MA is rejected - Request for SH - MA Request - Track Ahead Free Granted				wrong track ahead free information	generation of wrong messages "track to train"	Exceedance of safe speed		catastrophic	

© This document has been developed and released by UNISIG

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.5.2	Radio message (Train to Track)	System data, Location data, Specific answers/requests (specific acknowledge-ments or requests)	Deletion, Delay	any failure of the non-trusted transmission system	level 2, all modes	no information	generation of wrong messages "track to train	Exceedance of safe speed / distance by train		catastrophic	Subset026 provides internal mitigations such as acknowledgement procedures (e.g. train data)
5.2.5.2 a)	example:	System data e.g. - Train Data - Additional data - Specific system data				no update of train data for RBC	generation of wrong messages "track to train"	onboard supervision reject information		RAM issue	Train data acknowledgement by RBC
5.2.5.2 b)	example:	System data Specific system data			SR	no update of specific system data (e.g. current mode SR) for RBC	generation of wrong messages "track to train"	Exceedance of safe speed / distance by train	There is no ack from RBC to train for change mode to SR. The RBC should be responsible for generation of a safe MA to the train. (transferred to Subset-113 ETCS-H0002)	catastrophic	logical proving at application level principle "proceeding only if correct information are available"

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.5.2 c)	example:	Location data e.g. - LRBG - Distance from LRBG - Confidence Interval - Length of track covered by train possibly - The way train integrity was confirmed - Standstill detection - Direction of Movement			level 2, all modes; assignment of coordinate system	no update of changing of direction	generation of wrong messages "track to train"	onboard supervision reject information		catastrophic	Deletion of LRBG´s after changing of directions "Message authenticity" .
5.2.5.2 d)	example:	Location data "Position Report Packet"				no update of train position	generation of messages based on older information	using of information if possible		RAM issue	logical proving at application level principle "proceeding only if sufficient information are available"

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.5.2 e)	example:	Specific answers / requests e.g. - Acknowledgement - Acknowledgement of Emergency Stop - Request to shorten MA is granted - Request to shorten MA is rejected - Track Ahead Free Granted - Request for SH - MA Request				no update of information	generation of wrong messages "track to train"	onboard supervision reject information		RAM issue	logical proving at application level principle "proceeding only if correct information are available"
5.2.5.3	Radio message (Train to Track)	System data, Location data, Specific answers/requests (specific acknowledge-ments or requests)	Corruption	any failure of the non-trusted transmission system	level 2; all modes	wrong information to trackside	generation of wrong messages "track to train"	Exceedance of safe speed / distance by train		catastrophic	safety coding "Message integrity" Safety Protocol in Subset037 Cp.7.2

© This document has been developed and released by UNISIG

Ref. Id	ETCS Macro Function (Transmission function are defined here by transmitted message)	Macro Function Data Item	Failure Mode / Threats	Failure Cause	Operation Mode	Failure Effects			System Protection / Mitigation /Barriers (external)	Severity	System Protection / Mitigation /Barriers (internal)
						Local	Intermediate	Initial End Effect			
5.2.5.3 a)	example:	Location data e.g - LRBG - Distance from LRBG - Confidence Interfall - Direction of Movement - The way train integrity was confirmed - Standstill detection - Length of track covered by train possibly				wrong end position of the train to trackside	generation of wrong messages "track to train" to the following train	Exceedance of safe distance		catastrophic	
5.2.5.4	Radio message (Train to Track)	System data, Location data, Specific answers/requests (specific acknowledge-ments or requests)	Masquerade	any failure of the non-trusted transmission system or external attack	level 2; all modes	wrong information to trackside	generation of wrong messages "track to train"	Exceedance of safe speed / distance by train		catastrophic	Cryptographic techniques (Key management) "Message authenticity" Key Management system definition in Subset064

6. TRACEABILITY

6.1.1.1 This section lists the mandatory functions analysed from SUBSET-026.

6.1.1.2 Regarding the definition of a Transmission system according EN 50159 these functions therefore consists of safety related and non-safety related transmission functions.

6.1.1.3 The following level 2 main functions are analysed:
- Transmit movement authorities and track description data to the train (Please refer to SUBSET-026 2.6.6.2.2)
- The train receives a movement authority and track description via Euroradio relating to a balise (Please refer to SUBSET-026 2.6.6.2.4).

6.1.1.4 The following groups of transmission functions for level 2 are analysed:
- Radio transmission functions (Please refer to SUBSET-026 3.5; 3.16.3; 8.4.4)
- Balise transmission functions (Please refer to SUBSET-026 3.4; 3.6.3.1; 3.16.1/2; 3.17.3; 8.4.2)

6.1.1.5 The analysis of balise and Euroloop transmission functions is only based on the accepted/rejected information in ETCS Application Level 2 (as states 3.1.1.4), according to system requirements table in SUBSET-026 chapter 4.8.3.

7. CONCLUSIONS

7.1.1.1   Any issues found in this analysis have been transferred to the appropriate sections in SUBSET-091 and/or -113.