

ERTMS/ETCS

ETCS Application Levels 1 & 2 - Safety Analysis

Part 0 - Document Overview

REF : SUBSET-088 Part 0

ISSUE : 3.7.0

DATE : 2019-12-16

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. 14-05-01	All	Document Creation	WLH
0.0.2 25-05-01	4	Key to the fault tree symbols added	WLH
0.1.0 14-06-01	3.1.1.2 & 5.2.1.2	Inclusion of Ansaldo comments. Release for general Unisig review	WLH
0.1.1. 25-06-01	Section 8 Appendix B	Initial comments added Fault tree raised to issue 005.	WLH
0.1.2. 06-08-01	All	Document restructured into 4 parts. This part becoming part 0	WLH
0.1.3 17-08-01	4	References added	WLH
0.1.4 23-08-01	All	Restructured into 5 parts with parts 2 & 3 reversed. Configuration management facility added at section 4.	WLH
0.1.5.	All	Erroneous copy of 0.1.4. incorrectly circulated. Document up-issued to avoid confusion	WLH
0.1.6	All	Updated to reflect comments from the Super Group regarding the overall suite of documents	WLH
0.2.0. 01-10-01	3 & 6	Minor amendments and raised in issue for release to Esrog.	WLH
0.2.1. 10-10-01	4	Clarifications added as a result of a meeting with DB & SNCF	WLH
0.2.2. 10-10-01	4	Minor amendment incorporating RAMS Group review comments	WLH

02.3. 11-10-01	4 & 6	Incorporation of SNCF comments and extended definition of System Data	WLH
0.2.4. 18-10-01	4	Further clarification on the system context as requested by the Railways and Ansaldo.	WLH
0.2.5. 08-11-01	4 & 6	Comments from Ansaldo & Bombardier	WLH
0.3.0 28-01-02	3.1.1.3. 4.1.1.4. 4.1.1.7. 4.1.1.9.	Comments from Siemens and raised for issue within Unisig	WLH
0.3.1. 21-02-02		Tidying up prior to release to take account of revised structure of Report 2	WLH
2.0.0. 26-02-02		Raised in issue for release to the EEIG	WLH
2.0.1 10-10-02	3.1.1.3. 4.1.1.6. Title of section 7 Table in section 7	Amended to assist the ISAs	WLH
2.0.2. 04-12-02	3.1.1.3, 4.1.1.7, 6.1.1.3 Table in section 7	Amended in response to review comments from Ansaldo and Siemens	WLH
2.0.3. 12-01-0	4.1.1.7 Section 7 Table	Amendment to the format of the ETCS THR target following review meeting on 14-01-03. Update of document issue status table.	WLH
2.1.0. 31-01-03	Section 7 Table	Raised in issue for release to the users Group.	WLH
2.2.2. 21-03-03		Final release after amendment to reflect the comments in the final report from the ISA's version 1.1 dated 07-03-03 as proposed	WLH

		via the Unisig consolidated review comments on the ISA report v 0.0.2 March 03.	
2.2.3	4.1.1.1, 4.1.1.5, 4.1.1.8, 4.1.1.11	References to High-Speed removed.	IS
2.2.4	4.1.1.1, 4.1.1.5, 4.1.1.8, 4.1.1.11, 6.1.1.3	References to High-Speed removed Ch.4 – Added reference to Conventional Rail directive Ch.6 Specific National Values moved from “Session Control Data” section to “National Values/Default Values” section Ch 6. Added <i>Radio Network Identity</i> to Session Control Data	IS
2.2.5	5.1.1.1	Reference to SRS updated.	DARI
2.2.10		Raised in issue for release to the Users Group. Version number to be consistent with SUBSET-091.	DARI
2.2.11 20-09-07		<ul style="list-style-type: none"> Updated version of reference SUBSET-026 to match baseline 2.3.0 Versions added to other referenced subsets 	KN
2.3.0 02-04-08		Administrative updates for baseline 2.3.0	DARI
2.3.1 15-03-11		Updates for baseline 3.2	KN
2.3.2	5	Update versions of referenced documents and issue status of Subset-088	KN
3.0.0		<ul style="list-style-type: none"> Update versions of referenced documents and issue status of Subset-088 CR1102 considered 	

3.0.1		Update versions of referenced documents and issue status of Subset-088	KN
3.0.2		Update after internal RAMS WP review	KN
3.0.3		Minor updates during RAMS-meeting	DR
3.1.0		Administrative changes for release to ERA.	DR
3.2.0		<ul style="list-style-type: none"> Update of referenced documents 'Out of date message received' deleted ETCS Core Hazard used as standardized term 	KN
3.3.0		Update of issue status of Subset-088	KN
3.4.0		Updates agreed during RAMS-meeting	DR
3.5.0		Baseline 3 release version	DR
3.5.1	5.1.1.1, 7.1.1.1	Update of subset versions	KN
3.5.2	5.1.1.1, 7.1.1.1	Update for B3 MR1	KN
3.5.3		Formal updates during RAMS-meeting	DARI
3.5.4	5.1.1.1, 7.1.1.1	Update of subset versions. Baseline 3 1 st maintenance release version.	KN, DARI
3.5.5	5.1.1.1, 7.1.1.1	Update of subset versions	KN
3.5.6	5.1.1.1, 7.1.1.1	Update of subset versions	KN
3.5.7	5.1.1.1, 7.1.1.1	Update of subset versions	KN
3.6.0 2016-06-20	No change	Baseline 3 2 nd release version	RAMS WP
3.6.1	7.1.1.1	Update of subset versions	KN
3.7.0	No change	Release version	RAMS WP



2. TABLE OF CONTENTS

1. MODIFICATION HISTORY	2
2. TABLE OF CONTENTS.....	6
3. INTRODUCTION.....	7
4. SYSTEM CONTEXT.....	8
5. REFERENCE DOCUMENTS	10
6. GLOSSARY.....	11
Train Data	11
Additional Data.....	11
National Values / Default Values	11
Specific System Data	11
Transmission Status (Balise / Loop)	12
7. ISSUE STATUS OF SUBSET-088.....	13



3. INTRODUCTION

3.1.1.1 This suite of documents captures the safety analysis of the Unisig ETCS Reference Architecture when used in Application Levels 1 and 2.

3.1.1.2 The analysis has the objective of deriving the Safety Requirements for ETCS Application Levels 1 & 2. These are the requirements that must be satisfied in order to achieve Technical Interoperability and therefore, cover both, the Unisig reference architecture and those functions external to the reference architecture that must be harmonised in order to enable interoperability.

3.1.1.3 The document is split into 4 distinct parts as follows

- Part 0 - this part. This part provides an overview of the contents of each of the subsequent four parts. It also defines the context of the analysis and provides the configuration management for the overall set of documents.
- Part 1 - Contains a system wide, generic, non mandatory fault tree for ETCS based on the failure modes of a set of macro functions for ETCS that have been derived from the Unisig System Requirements Specification.

There are separate fault trees for Level 1 (SUBSET-088 - 1 Part 1) and for Level 2 (SUBSET-088 - 2 Part 1)

- Part 2 - Uses the fault tree in part 1 to analyse ETCS in a bottom up manner to establish by analysis, all the mitigating events, including the macro functions that can limit the migration of the base events of the fault tree.

There are separate analyses for Level 1 (SUBSET-088 - 1 Part 2) and for Level 2 (SUBSET-088 - 2 Part 2)

- Part 3 - Covers the top down apportionment of a Tolerable Hazard Rate for the Unisig reference architecture as defined by the European Railways. The analysis is based around a grouping of constituents and is taken to point where targets need to be defined for technical interoperability. The apportionment is done against an agreed Mission Profile (included in part 3), assuming that all items external to the constituent under examination are working correctly.

Part 3 contains the conclusions from the analysis process and has a summary of the safety requirements.

4. SYSTEM CONTEXT

4.1.1.1 All of the analyses are undertaken against the representation shown below. This puts the ETCS functionality as defined by the Unisig reference architecture, in its operational environment of a interoperable railway as mandated by the European Directives on the Interoperability of the rail system.

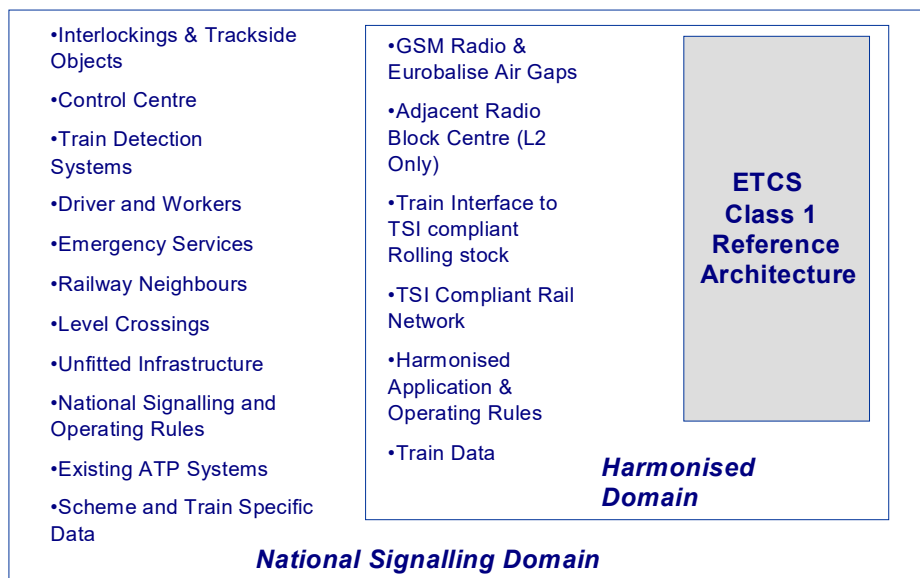
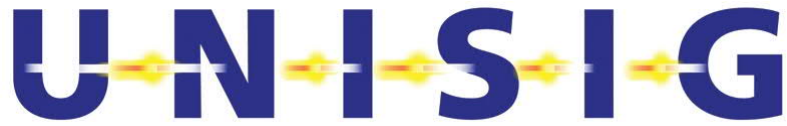


Figure 1: The ETCS Reference Architecture in its Context

- 4.1.1.2 The operational environment requires that the on-board part of the reference architecture must interface with defined entities throughout Europe in order to achieve technical and operational interoperability. These are denoted by the items within the Harmonised Domain. Due to the mobility of the on-board part, these items will influence the achieved level of safety across Europe.
- 4.1.1.3 The reference architecture and the harmonised items are required to work in conjunction with national signalling systems. These items are shown within the National Signalling Domain in the above figure. It is noted that these items will influence the achieved level of safety in a particular country.
- 4.1.1.4 The scope of the Unisig work is the analysis of the reference architecture. 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.

- 4.1.1.5 This analysis refers to the role of ETCS as train protection, i.e.
- 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.
- 4.1.1.6 Thus the ETCS Core Hazard for the reference architecture is defined as
- Exceedance of the safe speed or distance as advised to ETCS.
- 4.1.1.7 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.
- 4.1.1.8 According to the principles explained in Part 3 and the provisions of the CCS TSI, the maximum allowed rate of occurrence of the ETCS Core Hazard is $1.0 \cdot 10^{-9}$ / hour for ETCS onboard installed on a train and 10^{-9} / hour for ETCS trackside installed in an area visited by a train during a reference mission defined in Part 3.
- 4.1.1.9 Intentionally deleted.
- 4.1.1.10 The ETCS Core Hazard and its associated THR relate to the failure to perform the function of ETCS as defined in 4.1.1.5. This function is achieved with the Unisig reference architecture as defined in the SRS. It is inclusive of both random equipment failures and any systematic failures that could be introduced as a result of the design process.
- 4.1.1.11 Failures due to operators (e.g. Driver, signaller, maintenance staff) and operational rules are not included in this ETCS Core Hazard or THR.
- 4.1.1.12 The THR is given as a rate per hour for a typical journey where many of the ETCS operational modes may be used. Apportionment of the THR for the ETCS Core Hazard to the hazard rates for the Unisig grouping of constituents is undertaken in Part 3. This apportionment is based on a defined Mission Profile.
- 4.1.1.13 In order to arrive at a reasoned value for the constituent hazard rates, a sensitivity analysis is 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.



5. REFERENCE DOCUMENTS

5.1.1.1 The following documents were consulted in the development in this document

Unisig System Requirements Specification – SUBSET-026 v3.6.0

RBC / RBC Handover FMEA – SUBSET-078 v3.4.0

DMI FMEA (L1) – SUBSET-079-1 v3.14.0

DMI FMEA (L2) – SUBSET-079-2 v3.14.0

TIU FMEA (L1/L2) – SUBSET-080 v3.2.0

Transmission Path FMEA (L1) – SUBSET-081 - 1 v3.5.0

Transmission Path FMEA (L2) – SUBSET-081 – 2 v3.5.0

5.1.1.2 SUBSET-026 was the subject of the safety analysis and was used as a statement of the ETCS design intent.

5.1.1.3 The FMEA documents identified potentially catastrophic events that could exist at the mandatory boundaries to the Unisig reference architecture. These events are used as the base events of the fault tree developed in Part 1.

6. GLOSSARY

- 6.1.1.1 In addition to the general Unisig glossary, there are two terms which are used in the following parts that benefit from defining as follows
- 6.1.1.2 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.
- 6.1.1.3 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.
- 6.1.1.4 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.:

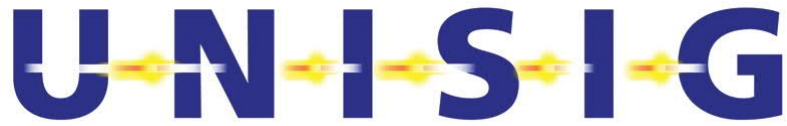
- Radio link supervision data (M_NVCONTACT, T_NVCONTACT)

Specific System Data

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

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

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



The following information is used to monitor radio sessions:

Session Control Data:

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

Session Status:

- Session established
- Session terminated
- No connection established
- Connection lost
- 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.

7. ISSUE STATUS OF SUBSET-088

7.1.1.1 The current issue status of the four parts of this document is as follows. Note that the issue status of this part (Part 0) is incremented whenever there is an up issue of one of the other four parts.

Part Number	Current Issue Status
Part 1- Level 1	3.7.0
Part 1 - Level 2	3.7.0
Part 2 - Level 1	3.7.0
Part 2 - Level 2	3.7.0
Part 3	3.7.0