ERTMS on SATELLITE Galileo Game Changer

Deliverable D3.1

Safety Analysis of ERSAT ERTMS Application over GNSS

Due date of deliverable: 31/05/2018

Actual submission date: 21/09/2018

Leader/Responsible of this Deliverable: RINA-C

Reviewed: Y

Document status		
Revision	Date	Description
00	05/06/2018	First Release
01	28/06/2018	Second Release
02	20/09/2018	Third Release, implementing reviewer comments.

Project funded from the European Union's Horizon 2020 research and innovation programme		
Dissemination Level		
PU	Public	
CO	Confidential, restricted under conditions set out in Model Grant Agreement	X
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

Start date of project: 01/12/2017 Duration: 24 months

This deliverable was prepared as part of the project ERSAT GGC, receiving funding from the European GNSS Agency (GSA) under the European Union's Horizon 2020 research and innovation programme, under grant agreement No 776039.

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
SPERANDIO Francesco	RINA-C	Author
STURARO Silvia	RINA-C	Author
BASSO Marzia	RINA-C	Reviewer
FELICETTI Andrea	RINA-C	Reviewer
SABINA Salvatore	ASTS	Reviewer
POGNANTE Fabio	ASTS	Contributor
CASALINUOVO Giuseppe	ASTS	Contributor
GUERRUCCI Luigi	RFI	Contributor
PARIS Daniela	RFI	Reviewer
BEUGIN Julie	IFSTTAR	Reviewer
BASILI Alessandro	BVI	Reviewer
EVANGELISTI Claudio	ITCF	Reviewer
STALLO Cosimo	RDL	Reviewer
BARRE Antoine	SNCF	Reviewer
SIERRA Beatriz	INECO	Reviewer

DOCUMENT APPROVAL

Document Code	Rev.	Approved	Authorised	Date
ERSAT-GGC_WP3_D3.1_Safety Analysis of ERSAT ERTMS Application over GNSS_V01	01	TMT	Massimiliano Ciaffi	2018/06/28
ERSAT-GGC_WP3_D3.1_ Safety Analysis of ERSAT ERTMS Application over GNSS_V02	02	TMT	Massimiliano Ciaffi	2018/09/20

EXECUTIVE SUMMARY

In order to apply the Enhanced ERTMS/ETCS Functional Architecture, capable of using GNSS and Public Radio TLC Technologies, the safety aspects of the ERTMS/ETCS system upon the future application of the abovementioned positioning and communication technologies have to be investigated.

This document describes the Qualitative Safety and Hazard Analysis carried out in ERSAT GGC WP3 - Task 3.1 and reports the relative results.

TABLE OF CONTENTS

LIST OF FIGURES

ACRONYMS AND DEFINITIONS

Acronym	Description
BG	Balise Group
BTM	Balise Transmission Module
COP	Code Of Practice
CSM	Common Safety Method
DB	Database
ERE	Explicit Risk Estimation
ERSAT-GGC	ERTMS on SATellite – Galileo Game Changer
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
FMECA	Failure Mode, Effects, and Criticality Analysis
GAD/TV	GNSS Augmentation Dissemination/ Trackside Verification
GNSS	Global Navigation Satellite System
HW	Hardware
MA	Movement Authority
MLCP	Multi-Link Communication Platform
MoM	Minute of meeting
MTCP	Multipath TCP
PVT	Position, Velocity, Time
QoS	Quality of Service
RAIM	Receiver Autonomous Integrity Monitoring
RBC	Radio Block Center
SIL	Safety Integrity Level
SIS	Signal In Space
SoM	Start Of Mission
SOW	Scope of work
STI	Standard for Technical Interoperability
SW	Software
TLC	Telecommunication
TMS	Traffic Management System
VB	Virtual Balise
VBD	Virtual Balise Detection
VBR	Virtual Balise Reader
VBTS	Virtual Balise Transmission System
WP	Work Package

Table 1 – Acronyms

Term	Description
Q_STATUS	status of SoM position report (UNISIG SUBSET-026 [R3])

Table 2 - Definitions

1. BACKGROUND

ERSAT GGC (Grant Agreement No 776039) is a follow up of ERSAT program launched in 2012 for integrating satellite technology on ERTMS platform. The primary goals of ERSAT GGC is to launch an operational line by 2020 and accelerate the standardization process at European level for including the satellite technology in the new ERTMS Standard for Technical Interoperability (STI).

In the framework of the Project ERSAT GGC, the WP3 is related to Safety and Hazard Analysis of the Enhanced ERTMS Functional Architecture, defined through the WP2 activities and previous related research projects, for the introduction of the GNSS technology, and consequently derived Virtual Balise concept, and Public Radio TLC Communication Network.
It is noteworthy that the Enhanced ERTMS Functional Architecture has been defined aiming:

- A minimum impact on current specifications;
- A functional retrofit UNISIG Compliant;
- The achievement of an acceptable safety level.

The Safety and Hazard Analyses of the ERSAT GCC system, considering the specific architecture, mission profile and operational scenarios, are object of WP3 activities, which are split into two main tasks:

- Task 3.1, aims at ensuring that the hazardous failures - potentially arisen after the integration of the Virtual Balise concept and Public Radio TLC related functional blocks within the current ERTMS architecture - are identified and qualitatively assessed;
- Task 3.2, aims at addressing the quantitative aspects of the risk analysis and deriving the Tolerable Hazard Rates to be fulfilled to ensure a safe use of the architecture and the compliance with reference regulations.

The present report, referred as deliverable D3.1, is the output of the Task 3.1.

The Failure Mode, Effects, and Criticality Analysis (FMECA) developed in this deliverable retains a functional block approach (refer also to WP3 SOW and WP3 Kick-Off MoM.
Furthermore, for the same purpose, the relevance of the interface and collaboration with WP2 has been pointed out and agreed.

2. OBJECTIVE

The aim of this document is to systematically carry out a qualitative Safety and Hazard Analysis focused on the introduction of the Virtual Balise Concept and of the IP-Based Public Mobile Radio Networks (Land and/or Satellite) in the Standard ERTMS/ETCS Reference Architecture. According with Risk Management approach applicable to Railway field (i.e. CSM and EN 50126), this hazard analysis has identified the hazard that could affect the system, defined the suitable safety requirements and identified the compliant Codes of Practice ensuring the residual risk acceptance.

3. INTRODUCTION

The Safety and Hazard Analysis object of this Deliverable is structured as detailed below.

Section § 1 provides the ERSAT GGC project background and the WP3 role description.

Section § 2 presents the objective of the present analysis.

Section § 4 provides an overview of the Enhanced ERTMS/ETCS Functional Architecture.

Section § 5 outlines the Safety Analysis scope and assumptions.

In Section § 6 the methodology on which the Safety and Hazard Analysis have been developed is presented.

Section § 7 presents the Hazard identified through the Safety Analysis (attached in Appendix B – The FMECA) and the proposed risk control strategy.

Section § 7.6 highlights the Safety Analysis output.

Appendix A - Guide Words integrates the description of the Failure Mode identification approach and process.

Appendix B – The FMECA, entirely reports the developed FMECA Analysis.

4. THE ENHANCED ERTMS FUNCTIONAL ARCHITECTURE

The Enhanced ERTMS/ETCS functional architecture is foreseen to integrate:

- The GNSS technology, to enable the Virtual Balise Concept for the ERTMS Train Position function;
- The IP-Based Public Mobile Radio Networks (Land and/or Satellite), to enhance the ERTMS On-board-Trackside communication.

The project Enhanced ERTMS/ETCS functional architecture, reported in Figure 1, has been defined within Task 2.1 activities of ERSAT-GGC WP 2 [R1] with the following approach:

- Identifying the interaction with the current ERTMS/ETCS functions;
- Minimizing the impact on the current ERTMS/ETCS specification;
- Avoiding unnecessary constraints in order to let each supplier designing its own new functional blocks.

The following subsections list and briefly describe the enhanced functional blocks relative to the Virtual Balise Concept (§ 4.1) and the IP-Based Radio communication (§4.2).
For major details, please refer to [R1].

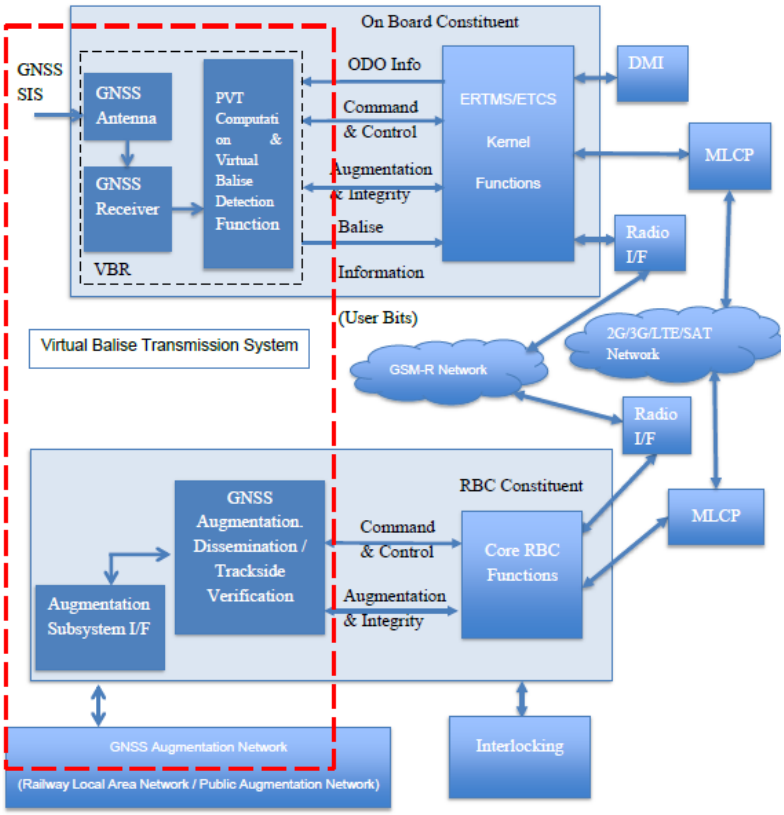

Figure 1 – The ERSAT-GGC Enhanced ERTMS/ETCS Functional Architecture [R1]

4.1 The Virtual Balise Transmission System Functional Architecture

The enhanced functional architecture subject of this analysis is based on the ERTMS/ETCS reference functional architecture, including the existing Eurobalise Transmission System, Euroloop Transmission System and Radio Transmission System, which integrates the Virtual Balise Transmission System (VBTS), highlighted in Figure 1 (within the Red dashed line).

The VBTS is intended as a safe spot transmission system that aims at conveying balise information from the trackside infrastructure to the on-board equipment.

The on-board and trackside functional blocks, which constitute the VBTS, are described in the following sub-sections (§ 4.1.1 and § 4.1.2).

Please note that, according to the project strategy the modifications to the ERTMS/ETCS reference architecture should be reduced at minimum. For this reason, it has been assumed that the ERTMS/ETCS Kernel and the Core RBC module shall ensure:

- the compliance with the SUBSET-026 [R3] ERTMS/ETCS functions;
- the gateway function between the VBTS On-board and Trackside components by means the Euroradio channel.

4.1.1 On-board VBTS functions

According to [R1], the on-board VBTS equipment, Virtual Balise Reader (VBR) in the following, is comprised of the functional blocks represented in Figure 2 and described in the following:

- The **GNSS Antenna**, the device that receives the radio GNSS Signal In Space (SIS);
- The **GNSS Receiver (RX) Function**, fed by the Antenna module, periodically provides the code and the carrier phase measurements relative to the input GNSS SIS;
- The **PVT Computation Function,** fed with the computed code and carrier phase measurement (i.e. pseudorange information), mainly computes the Position, Velocity, Time (PVT) solution on the basis of GNSS information, Augmentation and other on-board information;
- The **Virtual Balise Detection Function,** fed with the computed PVT solution:
    - Compares the computed PVT information with the pre-known virtual balise positions stored in the on-board Track Database (DB), to enable the Virtual Balise detection;
    - In case of Virtual Balise detection, it communicates the following information to the ETCS on-board Kernel:
        - Time / odometer stamp (according to the Odometry data received from ERTMS/ETCS Kernel) of the detected virtual balise centre;
        - The detection error associated with the virtual balise detection accuracy;
        - Balise information for the detected virtual balise according to the on-board track Database.

- The **Railways RAIM**, the on-board functional block that, executing the Receiver Autonomous Integrity Monitoring (RAIM) algorithms, ensures an integrity check to cope with GNSS system and local feared events that may have impact on the PVT solution to be used for detecting the virtual balise.

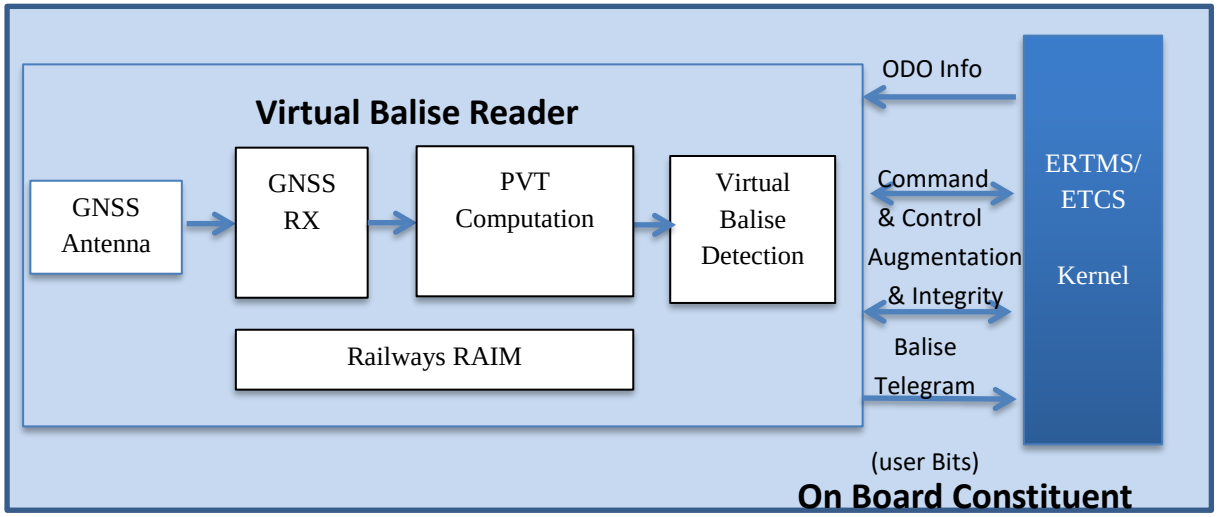

Figure 2 – The VBTS On-board functional blocks

Referring to the Standard ERTMS/ETCS Functional Architecture, the VBR functional block should be added to the existing BTM in order to ensure the communication of both Virtual and Physical Balise information to the ERTMS Kernel.

4.1.2 The Trackside VBTS functions

According to [R1], the Trackside VBTS equipment is comprised of:

- The **GNSS Augmentation Dissemination** functional block, responsible for:
  - disseminating the GNSS augmentation information;
  - timely computing and disseminating warning or alarms based on the information received from the "Core RBC Functions" block and the GNSS Augmentation system.
- The **Trackside Verification Function** responsible for carrying out additional railway verification checks on the Train Position by the combination of multiple information.

The whole of the two abovementioned functions are referred as the GAD/TV functional block. Regarding the GNSS Augmentation information, which is disseminated by the GAD/TV to the on-board by means of the existing Euroradio link, the interface between VBTS and an adequate Augmentation System (i.e. Railways compliant in terms of safety and performance) is foreseen.

4.1.3 The VBTS interfaces

As inferred from Figure 1, the project ERTMS Functional architecture foresees that VBTS is interfaced to the exiting ERTMS/ETCS On-board and Trackside functional blocks by means of the following logical interfaces:

The VBTS –ERTMS/ETCS Kernel Interfaces:

- **Command and Control:** this bidirectional interface addresses the management of the VBR equipment (e.g. equipment configuration, auto-test etc.)
- **Augmentation & Integrity:** this bidirectional interface is involved in the dissemination of the GNSS augmentation information forwarded from the Trackside GAD/TV block;
- **ODO Info:** this interface carries the ERTMS/ETCS Odometry information for time and odometer stamping of Virtual Balises (as per BTM, see Subset-036) as well as for crosscheck purposes;
- **Balise Information:** analogously to BTM for a Physical Balise, this interface carries the
  - User Bits,
  - The odometer time or space stamping,
  - The dynamic calculation of the accuracy (the only difference with respect the Physical Balise).

The VBTS –ERTMS/ETCS RBC Interfaces:

- **Command and Control:** this bidirectional interface addresses the management of the GNSS Augmentation Dissemination/Trackside Verification (GAD/TV) module within the RBC constituent;
- **Augmentation & Integrity:** this bidirectional interface enables the dissemination of the GNSS augmentation information received from the interfaced GNSS Augmentation System and optionally selected on the basis of the VBR estimated position, and the reception of VBR information / warnings.

4.2 THE IP-BASED PUBLIC MOBILE RADIO NETWORKS

Beside the Virtual Balise Concept, the future ERTMS/ETCS system includes the IP-based Radio Communication concept addressing the enhancement of the RBC-On-board communication (already investigated within NGTC project).

A Radio Communication System based on a Multi-bearer public network (terrestrial and satellite communication) as represented in Figure 3, is foreseen from rail stakeholders and ERA as ERTMS radio communication evolution.

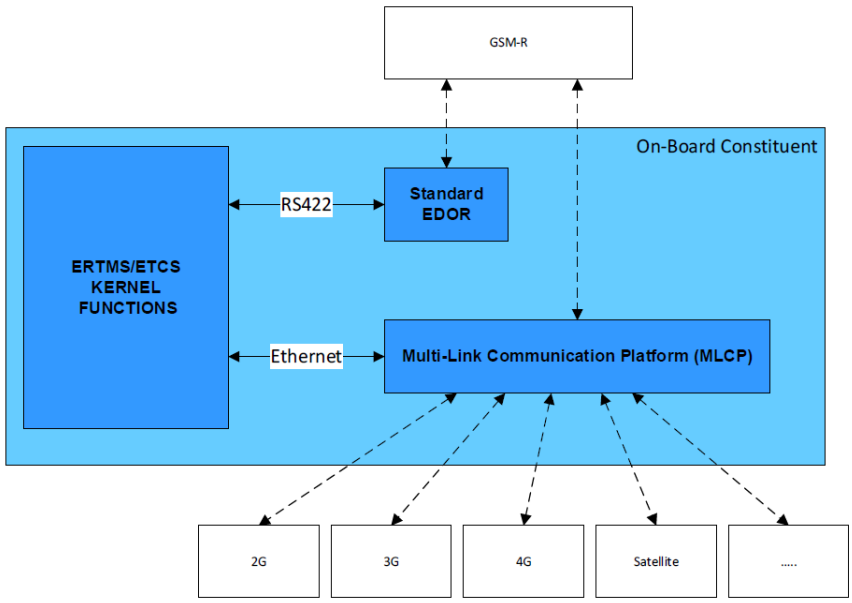

Figure 3 - Multi-Bearer IP based Communication Network System

The combination of intelligent routing algorithms and the IP-based solution enable the use of multiple technologies instead of a single one, thus the interoperability with the legacy GSM-R network will be guaranteed. Furthermore, the interoperability of multiple communication technologies will be supported by Multipath TCP (MP-TCP) protocol, which extend the traditional TCP protocol.

Concerning the Quality of Service (QoS), the Multi-Link Communication Platform (MLCP) integrating cognitive algorithms will follow the Euroradio protocol according to SUBSET-037 and SUBSET-093 to ensure the QoS requirement fulfilment.

5. THE SAFETY FOCUS

The Safety and Hazard Analysis presented herein is based on the Functional Architecture of Section § 4.

The scope of this Safety and Hazard Analysis is limited to the Virtual Balise Concept and the integration of the GNSS Technology within the ERTMS/ETCS Standard Reference Architecture (i.e. the functional blocks within the Red rectangle in Figure 1).
The Public Mobile Radio channel (described in § 4.2) is not object of these studies, since the interface with Multi-bearer public network will be ensured by the safe Euroradio protocol.
Concerning the Augmentation, the Safety analysis scope is limited to the interface with the GNSS Augmentation System, since the System itself is not object of the project.

Each functional block described at § 4.1, for the purpose of this analysis, has to be considered as a “black-box”. The communication channels between these blocks have been regarded with respect to CENELEC EN 50159 approach: the safety-related transmission is ensured exclusively demanding that the connected safety-related equipment fulfil the suitable requirements.

With reference to [R1], the VBTS transmission system has been classified as:

- Trusted (safe) parts:
  - Virtual Balise Reader safety related Functions;
  - GNSS Augmentation Dissemination / Trackside Verification;
- Non trusted parts:
  - Global Navigation Satellite total System, the combined ground and airborne subsystems, referring to its role as a source of positioning errors (i.e. feared events originating from satellite failures, such as ephemeris errors, pseudorange / clock errors; and feared events related to failures within the augmentation system);
  - GNSS Signal in Space, referring to its role as a source of positioning errors (i.e. feared events originating from the propagation environment including);
  - On-board GNSS antenna.

In particular, the VBR safety related functions, for the purpose of this preliminary analysis, have been assumed comparable with BTM SIL4 functions in terms of performance.
Additional considerations concerning the BTM / VBR performance as required in SUBSET-036 (and in particular in terms of accuracy and availability) can be investigated once the related specifications will be available.
.

6. THE SAFETY ANALYSIS METHODOLOGY

This section describes the methodology pursued in this first phase of the Safety Analysis that aims at:

- identifying the Virtual Balise Transmission System hazardous failures affecting the ERTMS/ETCS system;
- defining the technical and procedural safety measures at the Railway System level;
- assessing the risk of the hazardous scenarios according with Common Safety Method Risk Acceptance Principles.

6.1 REFERENCES AND GENERALITIES

The activities described herein have been developed on the basis of Railway best practices for the Risk Management, such as the Common Safety Method (CSM) [R6], [R7] and the CENELEC EN 50126 [R8], both addressing the safety-related changes being proposed to the existing railway system.
According to the project purpose, this safety analysis has adopted a delta approach with respect to the Standard ERTMS/ETCS Reference architecture, which has already experienced the safety acceptance and approval processes and it is in commercial service all over Europe since ten years.
Therefore, the safety analysis has been:

- guided by the best practices and;
- fed by both:
    - ERSAT GGC_WP2 D2.1, “Enhanced Functional ERTMS Architecture Capable of using GNSS and Public Radio TLC Technologies” and
    - UNISIG ERTMS/ETCS L2 System [R3].

6.2 FMECA: ASSUMPTIONS AND FRAMEWORK

This Qualitative Safety Analysis has adopted the *Failure Mode, Effects, and Criticality Analysis* (FMECA) approach, in general accordance with the “MIL-STD-1629A:1980 – Procedures for performing a failure mode, effects and criticality analysis”, has been adopted. The FMECA enables a systematic “*functional or hardware failures*” identification and evaluation process of their potential impact on “*mission success, personnel and system safety, system performance, maintainability*”[4].
The reasons for undertaking the FMECA methodology have been:

- the initial need to identify and assess each potential hazardous failure in a systematic manner;
- the need to identify those failures affecting the safety;
- the need to identify areas of improvements for the enhanced ERTMS Functional Architecture’ safety;
- the preference for a process extensively used throughout the industries, since the project has an application-oriented approach.

Specifically, the FMECA has been carried out at the block or interface level that are the lowest indenture level described in [R1], resulting in an *architectural* FMECA - the object of each FMECA table's row is the failure mode of a new architectural block or interface. A FMECA extract is provided in Table 4.

6.2.1 The Systematic Failure Mode Identification

To perform the failure identification process in a systematic way, each architectural component, including the interfaces (both internal and external), of the VBTS system have been inspected. As suggested in the CAP 760, "Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases", December 2010 the analysis has applied a list of guide-words per each studied architectural item in order to explore and reveal the component potential deviations from the designed intention. The adopted generic guide-word list is provided in Table 3.

Guide-word	Generic Description
NO	No part of the design intention is achieved e.g. No Power
MORE	An increase above the design intention is present e.g. Too much power
LESS	A decrease below the design intention is present e.g. Too little power
AS WELL AS	The design intention is achieved, but something else is present e.g. electrical noise on the power
PART OF	Only some of the design intention is achieved e.g. intermittent power
REVERSE	The design intention is the opposite of what happens e.g. no power, but shorted to earth or current reversed
OTHER THAN	The design intention is substituted by something different e.g. DC Power expected, but AC Power presented instead
EARLY	Something happens earlier in time than expected
LATE	Something happens later in time than expected
BEFORE	Relating to a sequence or order, something happens before it is expected
AFTER	Relating to a sequence or order, something happens after it is expected

Table 3 - The generic guide-word list [R12]

Starting from this generic list, a properly applicable and more specific sub-set of guide-words has been derived. The Appendix A - Guide Words reports the specific sub-lists of guide-words defined and applied to the VBTS blocks and interfaces (distinguishing if it carries an analogue or digital information), respectively.

It is noteworthy that, according to the applicable CENELEC Standards, the object of the analysis are the effects of random or systematic hardware/software failures that can affect the system safety. Consequently, the hardware/software failures due to malicious tampering of the block or action over the communication interface are not contemplated, since concerning the security scope instead of the safety one. On contrary, the analysis has considered the VBTS functional (e.g. software 1) faults due to the surrounding environment effects (e.g. multipath, Doppler,

[1] Please note that the referred VBTS software failure shall be considered as caused by external aspects (i.e. not associated to VBTS function fault), which shall be avoided or mitigated within the GNSS layer. Although, this analysis has partially addressed these failures at the Railway level, refer to § 7.5.

interference, etc.) on the GNSS SIS. These have been referred as bad SIS and/or SIS unavailability.

Table 4 provides an extract of the FMECA analysis applied on the GNSS Receiver functional block as example of the pursued approach.

FMECA ID	Architectural Block	Guide Word	Failure Mode	Failure Cause	Directl Failure Mode Effects
FB-K 1.2.1	**GNSS Receiver**	**NO**	The Block does not execute its function	Internal HW/SW failure	The block does not output any code/phase measurement upon the RF input
FB-K 1.2.2		**MORE**	The Block executes its functions more times then needed.	Internal HW/SW failure	The block outputs more than once the pseudorange measurement for the same RF signal
FB-K 1.2.3		**LESS**	The Block executes its functions less times then needed	Internal HW/SW failure	see NO
FB-K 1.2.4		**OTHER THAN**	Case 1) The Block's output information is other than expected: Valid Data, but different from the effective one	Internal HW/SW failure Environment Configuration	The block outputs a formally valid pseudorange measurement, but undue (i.e. wrong)
FB-K 1.2.5			Case 2) The Block's output information is other than expected: Non-Valid Data.	Internal HW/SW failure Environment Configuration	The block outputs a non-usable pseudorange information
FB-K 1.2.6		**EARLY**	The Block executes its function before than expected	Internal HW/SW failure	Case 1) - the device has no memory The receiver outputs a non-usable pseudorange measurement before the data processing completion
FB-K 1.2.7					Case 2) - the device has an internal memory The receiver outputs an undue (i.e. old) pseudorange measurement before the computing of the instantaneous one is completed
FB-K 1.2.8		**LATE**	The Block executes its function later than expected	Internal HW/SW failure Environment Configuration	The pseudorange measurement is issued later than expected

Table 4 – A FMECA Extract

6.2.2 The Operational Scenarios

Furthermore, the systematic approach foresees the study of each relevant operational scenarios within which the VBTS functional blocks are expected to interact with the existing ERTMS/ETCS system functions. In Table 5 are listed the Operational Scenarios analysed herein and described in ERSAT_GGC_WP2, "ERTMS Operational Scenarios", Technical Note, Rev. 0.2 [R2]. For the sake of tractability, a "Scenario ID" has been associated to each operational scenario; the traceability versus [R2] is reported in Table 5.

Scenario ID	Scenario Description	Scenario Reference
Scenario A	Registration and Start Up	§ 2 in [R2]
Scenario B	Start Of Mission in Level 2 with Q_STATUS "Known", at Terminal Railway Station	§ 3.2 in [R2]
Scenario C	Start Of Mission in Level 2 with Q_STATUS "Known", at Intermediate Railway Station	§ 3.3 in [R2]
Scenario D	Start Of Mission in Level 2 with Q_STATUS "Known", in Line	§ 3.4 in [R2]
Scenario E	Start of Mission in Level 2 with Q_STATUS "Unknown", at Terminal Railway Station, with "Approximation" of the Train Position	§ 4.1.1 in [R2]
Scenario F	Start of Mission in Level 2 with Q_STATUS "Unknown", at Terminal Railway Station, with TMS-RBC connection available	§ 4.1.2 in [R2]
Scenario G	Start of Mission in Level 2 with Q_STATUS "Unknown", at Terminal Railway Station, with TMS-RBC connection is not available	§ 4.1.3 in [R2]
Scenario H	Start of Mission in Level 2 with Q_STATUS "Unknown", at Intermediate Railway Station, with "Approximation" of the Train Position	§ 4.2 and § 4.1.1 in [R2]
Scenario I	Start of Mission in Level 2 with Q_STATUS "Unknown", at Intermediate Railway Station, with TMS-RBC connection available	§ 4.2 and § 4.1.2 in [R2]
Scenario J	Start of Mission in Level 2 with Q_STATUS "Unknown", at Intermediate Railway Station, with TMS-RBC connection is not available	§ 4.2 and § 4.1.3 in [R2]
Scenario K	Start of Mission in Level 2 with Q_STATUS "Unknown", in Line, with "Approximation" of the Train Position	§ 4.3 and § 4.1.1 in [R2]
Scenario L	Start of Mission in Level 2 with Q_STATUS "Unknown", in Line, with TMS-RBC connection available	§ 4.3 and § 4.1.2 in [R2]
Scenario M	Start of Mission in Level 2 with Q_STATUS "Unknown", in Line, with TMS-RBC connection not available	§ 4.3 and § 4.1.3 in [R2]

Table 5 – ERSAT GGC Operational Scenarios and their traceability

Although the large set of scenarios, some common aspects can be identified and the main cases of VBTS functions involvement are three:

1. The Track Database version validation, expected to be completed during the Registration and Start-Up (Scenario A);
2. The VBR initialization upon the information concerning the Train occupied track (Scenarios B – M);
3. The Virtual Balise Group detection (Scenarios K-M).

The FMECA methodology has been applied to each abovementioned operational scenario.

6.3 THE RISK ASSESSMENT

As per the EU Regulation 402/2013 [R6] and relative amendment of 13 July 2015 [R7] on the Common Safety Methods (CSM) for risk assessment, the hazards systematically identified through the Risk Management can be analysed and evaluated on the basis of one or more of the following Risk Acceptance Principles (RAPs):

- **The application of Acknowledged Codes of Practice (COP)**, where the hazard is addressed by accepted standards that define the way in which the associated risk is controlled. The evidence of compliance with the selected COP is sufficient to reduce as acceptable the residual risk level;
- **A comparison with similar systems (Reference Systems)**, where a system already assessed and sufficiently similar in scope, application and environment exists, the corresponding hazard analysis and mitigations can be applied. The comparison allow to similarly control the risk and reduce as acceptable the residual risk level;
- **An Explicit Risk Estimation (ERE)**, where the hazard cannot be addressed by a relevant Code of Practice or Reference System, or deviations are required from these, this principle may be required. In most cases the ERE is qualitatively performed using hazard severity categories, frequency categories, the risk matrix and risk categories.

The present analysis has defined a set of safety measures (reported in §§ 7.2 - 7.5) to be respected in order to ensure an acceptable risk level (according to CENELEC) and avoid safety level reduction for the affected ERTMS/ETCS function.
The acceptance of the residual risk has been derived by the identification of compliant applicative conditions defined within already in force Codes of Practice. The specific applied COPs, addressing the desired safety-related behaviour of each VBTS functional block and interface of Figure 1, are listed and explained in Section § 7.6.
For the sake of completeness, in the following are reported the CENELEC definitions (please refer to EN 50126 Standard [R8]) addressing the hazard risk level assessment, herein taken as reference.
Table 6 reports the EN 50126 [R8] categories for the frequency of occurrence of the hazardous event and the relative description.

Category	Frequency description
Frequent	The hazardous event is likely to occur frequently. The hazard will be continually experienced
Probable	The hazardous event will occur several times. The hazard can be expected to occur often
Occasional	The hazardous event is likely to occur several times. The hazard can be expected to occur several times
Remote	The hazardous event is likely to occur sometime in the system life cycle. The hazard can reasonably expected to occur
Improbable	The hazardous event is unlikely to occur, but possible. It can be assumed that the hazard may exceptionally occur
Incredible	The hazardous event is extremely unlikely to occur. It can be assumed that the hazard may not occur

Table 6 - Frequency of occurrence of hazardous events

Table 7 reports the EN50126 [R8] definition of the hazard severity level and the description of the associated consequences.

Severity Level	Consequences to Persons or Environment	Consequence to Service
Catastrophic	Fatalities and/or multiple severe injuries and/or major damage to the environment.	-
Critical	Single fatality and/or severe injury and/or significant damage to the environment	Loss of a major system
Marginal	Minor injury and/or significant threat to the environment	Severe system(s) damage
Insignificant	Possible minor injury	Minor system damage

Table 7 - Hazard Severity Level and consequences

Table 8 reports the definition of the EN 50126 Risk Categories and the actions to be performed against each one.

Risk Category	Action to be applied
Intolerable (R1)	The risk shall be eliminated
Undesirable (R2)	The risk shall only be accepted when risk reduction is impracticable and with the agreement of the Railway Authority or the Safety Regulatory Authority, as appropriate
Tolerable (R3)	Acceptable with adequate control and with the agreement of the Railway Authority
Negligible (R4)	Acceptable with/without the agreement of the Railway Authority

Table 8 - The Qualitative Risk Categories

The present Risk Assessment has adopted the Risk-Matrix reported in Table 9 and compliant with EN 50126 [R8].

Frequency of occurrence of a hazardous event	Risk Levels			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Undesirable
Remote	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Tolerable
Incredible	Negligible	Negligible	Negligible	Negligible
	Insignificant	Marginal	Critical	Catastrophic
	Severity Levels of Hazard Consequences			

Table 9 - The ERSAT-GGC Project Risk-Matrix

6.4 THE FMECA FIELDS

Table 10 and Table 11 detail the fields of FMECA worksheet adopted for each scenario.

FMECA Field	Field Description
ID	A unique FMECA internal reference number (e.g. FB-XX xx.yy.zz) assigned for traceability purposes, which cannot be changed: • FB-XX: identifies the Block's level FMECA for Scenario XX; • xx: identifies the System of the architecture; • yy: identifies the item of the System xx; • zz: identifies the failure mode of the item yy within the System xx.
Input from Design	
System	The studied architecture's system
System Description	Description of the system functionalities/ aim

FMECA Field	Field Description
Architectural Item	The item of the referred system, object of analysis
Functional Description - Generic	The description for the item's functions in a generic case
Functional Description - Scenario specific	The description for the item's functions in the scenario specific case
Safety Analysis	
Guide Word	The Guide Word upon which the Failure Mode is declined
Failure Mode	The manner by which the failure, affecting the analysed Architectural Item, is observed
Failure Cause	The generic cause for the observed Failure Mode
Direct Effects	The direct consequence(s) that the failure mode has on the function or output of the specific item analysed in the specific scenario
Local Effects	The effects of the item's failure on the related/connected items, for the specific scenario
Final Effect	The consequence(s) that the failure mode has at the architecture level, in the specific scenario
Safety Impact	Yes: the failure's effects are safety critical; No: the failure's effects are not safety critical; r
Associated Hazard	Description of the associated faulty situation
Risk Assessment	
Safety Measures	The description of the technical safety measures required to ensure an acceptable risk level and avoid safety level reduction for the affected ERTMS/ETCS function upon the identified failure mode
Risk Acceptance Principle (RAP)	The risk acceptance principle(s) adopted among COP, Reference System and ERE, according to CSM RA [R6] and [R7]
Acceptance Criteria Specification	Description of how the adopted RAP can accept the hazard associated risk level

Table 10 - The FMECA Template for the architectural blocks

FMECA Field	Field Description
ID	A unique FMECA internal reference number (e.g. FI-XX xx.yy.zz.ww) assigned for traceability purposes, which cannot be changed: • FI-XX: identifies the Interface's level FMECA for Scenario XX; • xx: identifies the Interface; • yy: identifies the Data Flow within the Interface xx; • zz: identifies the communication direction for the Data Flow yy, of the Intrerface xx; • ww: identifies the failure mode of the communication zz, for the Data Flow yy within the Interface xx.

Input from Design	
Interface	The studied architecture's Interface
Data Flow - Generic	Description of the Data Flow generally carried through the Interface
Data Flow - Scenario Specific	Description of the specific Data Flow carried through the Interface within the analysed scenario case
Data Type	The type (i.e. format) of the data, e.g. Analogue/ RF signal or Digital signal (at packet or bit level)
TX	The transmitter from which the Data Flow departs
RX	The receiver at which the Data Flow arrives
Safety Analysis	
Guide Word	The Guide Word upon which the Failure Mode is declined
Failure Mode	The manner by which the failure, affecting the analysed Architectural Item, is observed
Failure Cause	The generic cause for the observed Failure Mode
Direct Effects	The direct consequence(s) of the interface failure mode at the receiver side, in the specific scenario
Local Effects	The effects that the interface failure causes locally, for the specific scenario
Final Effect	The consequence(s) that the failure mode has at the architecture level, in the specific scenario
Safety Impact	Yes: the failure's effects are safety critical; No: the failure's effects are not safety critical; r
Associated Hazard	Description of the associated faulty situation
Risk Assessment	
Safety Measures	The description of the technical safety measures required to ensure an acceptable risk level and avoid safety level reduction for the affected ERTMS/ETCS function upon the identified failure mode
Risk Acceptance Principle (RAP)	The risk acceptance principle(s) adopted among COP, Reference System and ERE, according to CSM RA [R6] and [R7]
Acceptance Criteria Specification	Description of how the adopted RAP can accept the hazard associated risk level

Table 11 - The FMECA Template for the architecture's interfaces

7. THE SAFETY ANALYSIS RESULTS

This Section reports the results of the Qualitative Safety and Hazard Analysis (reported in Appendix B – The FMECA) performed on the ERTMS/ETCS Functional Architecture as described in § 4 and according to the methodology described in § 6.

7.1 IDENTIFIED HAZARDS

The systematic Safety Analysis - guided by the failure identification process and applied on each new functional block and interface for each operational scenario - in correspondence of a safety-relevant failure effect, has identified the following Top Hazard:

"Possible Incorrect Train Positioning leading to train collision/derailment"

The severity of the abovementioned Hazard, due to the potential level of damages on persons, environment and system has been evaluated as "Catastrophic", according to EN 50126 [R8].

The following sub-sections provide the technical safety measures required to control the risk associated to the identified hazard.

7.2 SAFETY REQUIREMENTS FOR TRACK DATABASE VERSION VERIFICATION FAILURES

According to the "*Registration and Start Up"* operational scenarios described in [R2], once the communication session between RBC and EVC has been established the compatibility of the Track Database (DB) version between Trackside and On-board is verified.

The safety analysis has regarded as safety-relevant the failure modes affecting:

- the GAD/TV functions;
- the VBR functions;
- the bi-directional communication over the GAD/TV – RBC interface;
- the bi-directional communication over the VBR-EVC interface.

Whose effects can

- avoid or delay the Track DB validation;
- unduly admit a positive Track DB version validation.

Table 12 below lists the required technical safety measures that shall be respected in order to avoid the specific failure modes or reduce as acceptable the consequent hazard risk level.

REQ. ID	REQ. Description
REQ. 001	GAD/TV shall cyclically forward the Track DB verification request till it receives an answer from the on-board
REQ. 002	The ERTMS/ETCS system shall not provide any MA till the Track DB version has not been verified with a positive result
REQ. 003	VBR shall communicate to GAD/TV the result of the Track DB version verification only if: - the Track DB has been correctly and completely downloaded; - the verification of Track DB version has been completed.
REQ. 004	Once the RBC-EVC communication session is established the Track DB version shall be verified
REQ. 005	VBR shall avoid the communication of undue (i.e. wrong/ unforeseen) messages
REQ. 006	The VBR design shall foresee auto-test functionality to detect internal failures and in case lead VBR to a fail-safe state
REQ. 007	The ERTMS/ETCS shall treat the VBR unavailability as a safety affecting fault
REQ. 008	GAD/TV shall avoid the communication of undue (i.e. wrong/ unforeseen) messages
REQ. 010	GAD/TV design shall foresee auto-test functionality to detect internal failures and in case lead GAD/TV to a fail-safe state
REQ. 011	The ERTMS/ETCS shall transmit an Emergency Message in case of GAD/TV unavailability
REQ. 012	The ERTMS/ETCS EVC-VBR interface shall be a closed safety-related transmission system compliant to the EN 50159 standard. Therefore the following mitigation measures shall be taken into account: - Safety reaction shall be applied in case of misoperation; - Message integrity shall be provided by including a safety code (e.g. CRC); - The receiver shall apply an error detection mechanism; - Authenticity shall be provided by adding a source identifier to the message data; - The message shall identify the receiver; - The timeliness of the message shall be provided.
REQ. 015	The GAD/TV-RBC interface shall be a closed safety-related transmission system compliant to the EN 50159 standard. Therefore the following mitigation measures shall be taken into account: - Safety reaction shall be applied in case of misoperation; - Message integrity shall be provided by including a safety code (e.g. CRC); - The receiver shall apply an error detection mechanism; - Authenticity shall be provided by adding a source identifier to the message data; - The message shall identify the receiver; - The timeliness of the message shall be provided.

Table 12 – Required Safety measures for the Track DB version verification failures

Please refer the FMECA included in Appendix B section 9.2.1 for the specific association between failure modes and required safety measures.

7.3 SAFETY REQUIREMENTS FOR THE TRACK NOTIFICATION AND VBR INITIALIZATION FAILURES

According to [R2], regardless the Q_STATUS value and scenario location (i.e. Terminal or Intermediate Railway Station and Line), during the SoM the VBR shall be initialized through a trackside communication or a Physical Balise detection to allow it to safely discriminate the correct track on which the train is located.

The safety analysis has regarded as safety-relevant the failure modes affecting:

- the VBR functions;
- the bi-directional communication over the GAD/TV – RBC interface;
- the bi-directional communication over the VBR-EVC interface.

Whose effects can

- avoid or delay the platform discrimination and consequent VBR initialization;
- unduly admit a positive VBR initialization.

Table 13 below lists the required technical safety measures that shall be respected in order to avoid the specific failure modes or reduce as acceptable the consequent hazard risk level.

REQ. ID	REQ. Description
REQ. 017	The ERTMS/ETCS Trackside subsystem shall not provide any MA till the positive VBR initialization has not been performed and communicated
REQ. 018	VBR shall be set "initialized" only if all the information necessary to enable the VB detection functionality have been correctly received and processed
REQ. 005	VBR shall avoid the communication of undue (i.e. wrong/ unforeseen) messages
REQ. 006	The VBR design shall foresee auto-test functionality to detect internal failures and in case lead VBR to a fail-safe state
REQ. 007	The ERTMS/ETCS shall treat the VBR unavailability as a safety affecting fault
REQ. 012	The ERTMS/ETCS EVC-VBR interface shall be a closed safety-related transmission system compliant to the EN 50159 standard. Therefore the following mitigation measures shall be taken into account: - Safety reaction shall be applied in case of misoperation; - Message integrity shall be provided by including a safety code (e.g. CRC); - The receiver shall apply an error detection mechanism; - Authenticity shall be provided by adding a source identifier to the message data; - The message shall identify the receiver; - The timeliness of the message shall be provided.
REQ. 015	The GAD/TV-RBC interface shall be a closed safety-related transmission system compliant to the EN 50159 standard. Therefore the following mitigation measures shall be taken into account: - Safety reaction shall be applied in case of misoperation; - Message integrity shall be provided by including a safety code (e.g. CRC); - The receiver shall apply an error detection mechanism; - Authenticity shall be provided by adding a source identifier to the message data; - The message shall identify the receiver; - The timeliness of the message shall be provided.

Table 13 – Required Safety measures for the Track discrimination and VBR initialization failures

Please refer the FMECA included in Appendix B sections 9.2.2 - 9.2.7 for the specific association between failure modes and required safety measures.

7.4 SAFETY REQUIREMENTS FOR VIRTUAL BALISE DETECTION FAILURES

Concerning the Degraded Operation scenario relative to the SoM in line, due to a fault, with Q_STATUS = “Unknown”, [R2] foresees the train localization upon the first Virtual Balise detection in Staff Responsible (SR) mode.
This scenario demands the existing ERTMS/ETCS system to interact with the whole VBTS functional blocks and interfaces.

The safety analysis has regarded as safety-relevant the failure modes affecting:

- The GNSS Signal In Space (SIS) quality and/or availability;
- The Pseudorange computation consistency and/or availability;
- The PVT solution computation consistency and/or availability;
- The Virtual Balise detection consistency and/or availability;
- The Balise User bit delivery consistency and/or availability;
- The RAIM integrity validation check consistency and/or availability;
- The GNSS Augmentation Dissemination consistency and/or availability;
- The bi-directional communication over the VBR-EVC the external interface;
- The bi-directional communication over the GAD/TV-RBC external interface;
- The uni-directional communication over the GNSS Antenna- GNSS Receiver internal interface;
- The uni-directional communication over the GNSS Receiver – PVT Computation Block internal interface;
- The uni-directional communication over the PVT Computation Block – Virtual Balise Detector internal interface;
- The uni-directional communication over the GNSS Augmentation external interface.

Whose effects can

- avoid or delay the VB detection;
- unduly claim the expected VB detection.

Table 14 below lists the required technical safety measures that shall be respected in order to avoid the specific failure modes or reduced as acceptable the consequent hazard risk level.

REQ. ID	REQ. Description
REQ. 005	VBR shall avoid the communication of undue (i.e. wrong/ unforeseen) messages
REQ. 006	The VBR design shall foresee auto-test functionality to detect internal failures and in case lead VBR to a fail-safe state
REQ. 007	The ERTMS/ETCS shall treat the VBR unavailability as a safety affecting fault
REQ. 008	GAD/TV shall avoid the communication of undue ((i.e. wrong/ unforeseen) messages
REQ. 009	The on-board GNSS chain (i.e. from the GNSS antenna to the Balise delivery function) shall be redundant
REQ. 010	GAD/TV design shall foresee auto-test functionality to detect internal failures and in case lead GAD/TV to a fail-safe state
REQ. 011	The ERTMS/ETCS shall transmit an Emergency Message in case of GAD/TV unavailability
REQ. 012	The ERTMS/ETCS EVC-VBR interface shall be a closed safety-related transmission system compliant to the EN 50159 standard. Therefore the following mitigation measures shall be taken into account: - Safety reaction shall be applied in case of misoperation; - Message integrity shall be provided by including a safety code (e.g. CRC); - The receiver shall apply an error detection mechanism; - Authenticity shall be provided by adding a source identifier to the message data; - The message shall identify the receiver; - The timeliness of the message shall be provided.
REQ. 013	The PVT Computation Block -Virtual Balise Detector interface shall be a closed safety-related transmission system compliant to the EN 50159 standard. Therefore the following mitigation measures shall be taken into account: - Safety reaction shall be applied in case of misoperation; - Message integrity shall be provided by including a safety code (e.g. CRC); - The receiver shall apply an error detection mechanism; - Authenticity shall be provided by adding a source identifier to the message data; - The message shall identify the receiver; - The timeliness of the message shall be provided.
REQ. 014	The GNSS Receiver - PVT Computation Block interface shall be a closed transmission system between safety-related and non safety-related equipment compliant to the EN 50159 standard. Therefore, a safety reaction shall be applied in response to a transmission system failure (e.g. a GNSS receiver failure).
REQ. 015	The GAD/TV-RBC interface shall be a closed safety-related transmission system compliant to the EN 50159 standard. Therefore the following

REQ. ID	REQ. Description
	mitigation measures shall be taken into account: - Safety reaction shall be applied in case of misoperation; - Message integrity shall be provided by including a safety code (e.g. CRC); - The receiver shall apply an error detection mechanism; - Authenticiity shall be provided by adding a source identifier to the message data; - The message shall identify the receiver; - The timeliness of teh message shall be provided.
REQ. 016	The Augmentation System - GAD/TV interface shall be a closed safety-related transmission system compliant to the EN 50159 standard. Therefore the following mitigation measures shall be taken into account: - The GAD/TV shall apply a safety reaction in case of detected misoperation of the Augmentation System; - Message integrity shall be provided by including a safety code (e.g. CRC); - GAD/TV shall apply an error detection mechanism; - Authenticity shall be provided by adding a source identifier to the message data; - The message shall identify the receiver; - The timeliness of the message shall be provided.
REQ. 019	If the SIS unavailability exceeds a pre-defined time-threshold, VBR shall inform the ERTMS/ETCS. The ERTMS/ETCS shall manage this warning as a missed balise group and react in accordance to the applicable conditions.
REQ. 020	If the SIS SNR is below a pre-defined threshold, VBR shall inform the ERTMS/ETCS. The ERTMS/ETCS shall manage this warning as a missed balise group and react in accordance to the applicable conditions.
REQ. 021	The fresh pseudorange measurement shall be periodically provided after the receiver processing
REQ. 022	VBR shall detect the unavailability of the fresh and consistent pseudorange input
REQ. 023	In case of inconsistent input, VBR shall reject it and inform the ERTMS/ETCS. The ERTMS/ETCS shall manage this warning as a missed balise group and react in accordance to the applicable conditions.
REQ. 024	If the unavailability of the fresh and consistent pseudorange measurement exceeds a pre-defined time-threshold, VBR shall inform the ERTMS/ETCS. The ERTMS/ETCS shall manage this warning as a missed balise group and react in accordance to the applicable conditions.
REQ. 025	The fresh PVT solution shall be periodically provided after the processing of the input pseudorange data
REQ. 026	VBR shall detect the unavailability of the fresh and consistent PVT solution
REQ. 027	If the fresh and consistent PVT is missing, VBR shall inform the ERTMS/ETCS. The ERTMS/ETCS shall manage this warning as a missed balise

REQ. ID	REQ. Description
	group and react in accordance to the applicable conditions.
REQ. 028	VBR shall avoid the communication of undue (i.e. wrong/ unforeseen) PVT solutions
REQ. 029	The PVT solution shall be always crossed-check with other information
REQ. 030	The VBR auto-test shall detect and communicate the VB detection function unavailability to the ERTMS/ETCS, which shall manage this warning as a missed balise group and react in accordance to the applicable conditions.
REQ. 031	The ERTMS/ETCS shall manage the missed VB detection communication as a missed balise group and react in accordance to the applicable conditions.
REQ. 032	The VBR provided User bits/ time stamp / detection error shall be consistent with: - the actually detected VB - the validated Track DB
REQ. 033	The RAIM algorithm shall be periodically performed and the output correctly issued at the processing completion
REQ. 034	If the fresh and valid RAIM check is missing, VBR shall reject the PVT solution and inform the ERTMS/ETCS, which shall manage this warning as a missed balise group and react in accordance to the applicable conditions.
REQ. 035	VBR shall detect the RAIM validation check freshness and validity
REQ. 036	GAD/TV, which has in charge of the GNSS Augmentation dissemination responsibility, shall: - pre-process the Augmentation information; - manage the dissemination of the fresh and valid GNSS Augmentation data once the pre-processing is ended
REQ. 037	VBR shall verify the freshness of the received GNSS Augmentation information
REQ. 038	The fresh GNSS augmentation on-board unavailability shall be treated as a safety affecting fault
REQ. 039	VBR shall detect the fresh ODO message unavailability
REQ. 040	The fresh ODO information unavailability shall be treated as a safety affecting fault

Table 14 – Required Safety measures for the VB Detection failures

Please refer the FMECA included in Appendix B section 9.2.4 - 9.2.7 for the specific association between failure modes and required safety measures.

7.5 SAFETY REQUIREMENTS FOR VBTS NON-TRUSTED PARTS FAILURES

Concerning the VBTS Non-trusted parts identified in D 2.1 [R1], and recalled herein § 5, the safety analysis has regarded as safety-relevant the failure modes affecting:

- The GNSS Antenna input/output;
- The GNSS Receiver input/output;
- The GNSS Augmentation information.

Table 15 below lists the required technical safety measures that shall be respected in order to reduce as acceptable the consequent hazard risk level. Please note that as per the WP3 SoW the Safety Measures presented herein address the Railway domain, but these should be combined to a set of suitable mitigations addressing the GNSS signal and Augmentation information quality and availability.

REQ. ID	REQ. Description
REQ. 009	The on-board GNSS chain (i.e. from the GNSS antenna to the Balise delivery function) shall be redundant
REQ. 014	The GNSS Receiver - PVT Computation Block interface shall be a closed transmission system between safety-related and non safety-related equipment compliant to the EN 50159 standard. Therefore, a safety reaction shall be applied in response to a transmission system failure (e.g. a GNSS receiver failure).
REQ. 016	The Augmentation System - GAD/TV interface shall be a closed safety-related transmission system compliant to the EN 50159 standard. Therefore the following mitigation measures shall be taken into account: - The GAD/TV shall apply a safety reaction in case of detected misoperation of the Augmentation System; - Message integrity shall be provided by including a safety code (e.g. CRC); - GAD/TV shall apply an error detection mechanism; - Authenticity shall be provided by adding a source identifier to the message data; - The message shall identify the receiver; - The timeliness of the message shall be provided.
REQ. 019	If the SIS unavailability exceeds a pre-defined time-threshold, VBR shall inform the ERTMS/ETCS. The ERTMS/ETCS shall manage this warning as a missed balise group and react in accordance to the applicable conditions.
REQ. 020	If the SIS SNR is below a pre-defined threshold, VBR shall inform the ERTMS/ETCS. The ERTMS/ETCS shall manage this warning as a missed balise group and react in accordance to the applicable conditions.
REQ. 021	The fresh pseudorange measurement shall be periodically provided after the receiver processing
REQ. 022	VBR shall detect the unavailability of the fresh and consistent pseudorange input
REQ. 023	In case of inconsistent input, VBR shall reject it and inform the ERTMS/ETCS. The ERTMS/ETCS shall manage this warning as a missed balise group and react in accordance to the applicable conditions.
REQ. 024	If the unavailability of the fresh and consistent pseudorange measurement exceeds a pre-defined time-threshold, VBR shall inform the ERTMS/ETCS. The ERTMS/ETCS shall manage this warning as a missed balise group and react in accordance to the applicable conditions.
REQ. 029	The PVT solution shall be always crossed-check with other information
REQ. 033	The RAIM algorithm shall be periodically performed and the output correctly issued at the processing completion
REQ. 034	If the fresh and valid RAIM check is missing, VBR shall reject the PVT solution and inform the ERTMS/ETCS, which shall manage this warning as a missed balise group and react in accordance to the applicable conditions.
REQ. 035	VBR shall detect the RAIM validation check freshness and validity
REQ. 036	GAD/TV, which has in charge of the GNSS Augmentation dissemination responsibility, shall: - pre-process the Augmentation information; - manage the dissemination of the fresh and valid GNSS Augmentation data once the pre-processing is ended
REQ. 038	The fresh GNSS augmentation on-board unavailability shall be treated as a safety affecting fault

Table 15 - Required Safety measures for the VBTS Non-trusted parts failures

Please refer the FMECA included in Appendix B section 9.2.4 - 9.2.7 for the specific association between failure modes and required safety measures.

7.6 THE COMPLIANT CODES OF PRACTICE

The safety requirements identified in order to control the various failure modes that can lead to the Top Hazard *"Possible Incorrect Train Positioning leading to train collision/derailment"* and listed across Sections §§ 7.2, 7.3,7.4 and 7.5 shall be fulfilled to ensure at least the function original safety level.

According to the CSM regulation [R6] and [R7], the residual risk level (i.e. after the safety measures application) can be accepted identifying a set of applicable Codes of Practice, already compliant with in force regulations, which includes some applicative conditions compliant with the required safety measures. Since the novelty of the Virtual Balise Concept a Code of Practice handling its peculiarities has not been identified, but some similarities can be identified (e.g. between BTM and VBR functions) among the COPs addressing the existing ERTMS/ETCS Functional Architecture.

Specifically, beside CENELEC EN 50126 [R8] and CSM [R6], [R7] approach, the following COPs have been considered as highlighted in Figure 4:

- CENELEC EN 50159 [R10] - compliant to the required safety measures addressing the functional VBTS interfaces, both external and internal, which are regarded as closed safety-related transmission system, where:
    - the risk of unauthorized access is considered negligible ;
    - the number of pieces of connectable equipment - either safety-related or not - to the transmission system is known and fixed;
    - the physical characteristics of the transmission system (e.g. transmission media, environment under worst case conditions, etc.) are fixed and unchanged during the life cycle of the system .

  According to this COP the referred interfaces are required to follow at least these fundamental safety-services:
    - message authenticity;
    - message integrity;
    - message timeliness;
    - message sequence.
- CENELEC EN 50129 [R9] – a set of its criteria is compliant to:
    - The VBR and GAD/TV operational and safety requirements ensuring the respective functions to correctly opera.te (e.g. the avoidance of undue messages, correct processing of safety-related information). The required design comply with some processes addressed in EN 50129, Annex B.2: "Assurance of correct functional operation";

- The VBR and GAD/TV required single fault detection capability (e.g. auto-test functionality, redundancy and independency) and subsequent reactions (e.g. fail-safe). The required design comply with some principles addressed in EN 50129, Annex B.3: " Effects of faults";

- UNISIG Subset-026 [R3] – a set of its System Requirements Specifications comply with some functional behaviour of the Enhanced ERTMS/ETCS Functional Architecture since required to address new problems (e.g. the Track DB version validation, Track notification, VBR initialization or Virtual Balise Group missed detection) in a way similar to already existing problems, please refer to
  - § 3.5.3 Establishing a communication session;
  - § 3.7 Completeness of data for safe train movement and § 3.7.2 Responsibility for completeness of information
  - § 3.4.4. Linking;
  - § System Failure.
- UNISIG Subset-088 [R5] – a set of the Fault Tree Base Event (e.g. TRANS-BALISE-1, TRANS-BALISE-2, TRANS-BALISE-3) analysed in Part 2 comply with some herein studied failure modes.

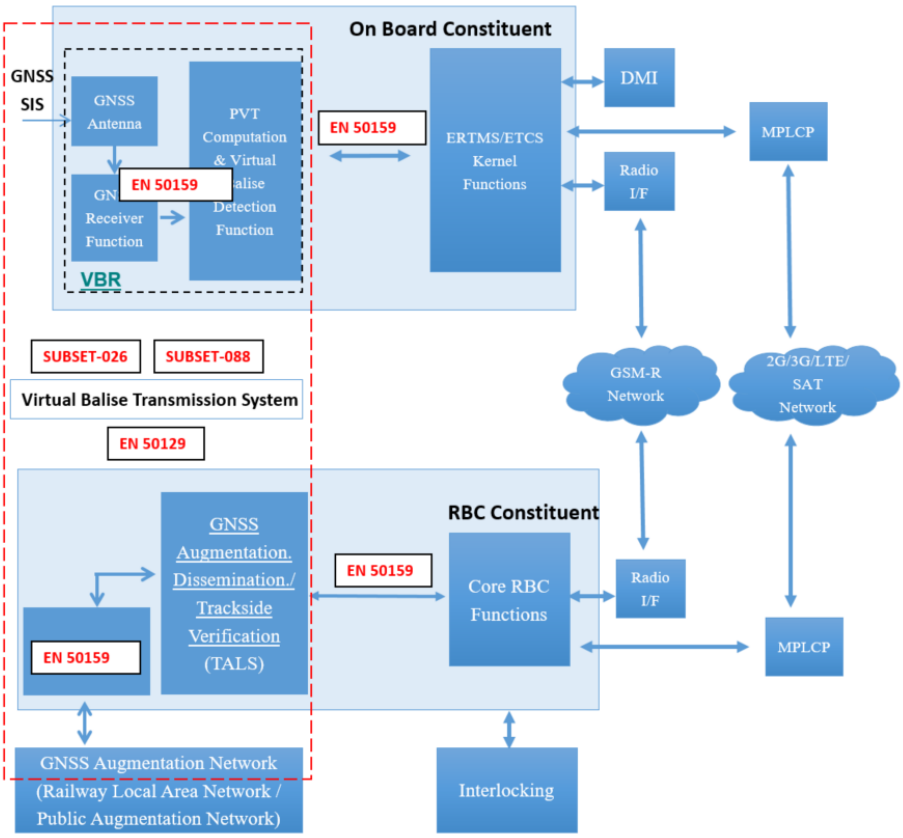

Figure 4 – The Codes of Practice applicable to VBTS

Please note that Figure 4 shows only the COPs compliant to the safety measures addressing the safety analysis scope of work, but it is assumed that the architecture studied in this report does not affect the interface with the remaining functional blocks.

Refer to the “Acceptance Criteria Specification” field of the FMECA (attached in Appendix B – The FMECA) for more detail on the safety measures and COPs applicative conditions compliance.

7.6.1 The Residual Risk Level

Since the identified compliance between the herein required Safety Measures and the set of criteria included within some applicable in force Codes of Practice, the residual risk level can be assessed Tolerable, as per the CENELEC definition (refer to Table 8). Therefore, according to the Risk-Matrix of Table 9 the frequency of occurrence of the specific hazardous event is minimized as Improbable. Please note that the latter shall be rigorously evaluated once the VBTS specifications will be available.

8. CONCLUSIONS

This deliverable constitutes the Safety and Hazard analysis carried out on the Enhanced ERTMS/ETCS functional architecture as currently defined in WP2, and described in § 4.

The analysis has been developed in compliance with the Risk Management defined in CSM [R6],[R7] and EN50126 [R8].

This document considers in input the Enhanced functional architecture as defined in WP2.

As a result, the proposed architecture is capable of managing the hazards emerged from the safety analysis of the operational scenarios defined by WP2 with an acceptable residual risk level provided that the safety measures defined in sections §§ 7.2, 7.3, 7.4 and 7.5 are fulfilled.

In particular it is confirmed the need of a VBR and GAD/TV compliant to SIL4 requirement, according to CENELEC EN 50126 [R8], EN 50129 [R9] and UNISIG SUBSET-088 [R5].

9. APPENDICES

9.1 APPENDIX A - GUIDE WORDS

This Annex describes the generic failure modes that has been associated to the CAP 760 list of Guide Words and reports the specific sub-lists of Guide Words actually applied for the identification of the failure modes affecting the VBTS blocks and interfaces.

The Architectural Blocks Failure Modes

The left side of Table 16 reports the potential failure modes affecting an architectural block and its functionalities declined upon the list of Guide Words provided in CAP 760. Since not each Guide Word might be associable to a block credible failure mode or multiple guide words lead to the same failure mode, a selection process has been applied on the Guide Word list. The right side Table 16 reports the resulting, actually applied, sub-list of guide words (highlighted in green colour).

Generic Guide Words from CAP 760	
Guide Word	**Corresponding Failure Mode**
NO	The block does not execute its functions. No output is available.
MORE	The block malfunctions and: 1. sends out more permissive (undue) information 2. executes its function more than needed
LESS	The block malfunctions and: 1. sends out less permissive (undue) information; 2. executes its function less than needed
AS WELL AS	The block malfunctions and sends out Non-Valid Data (e.g. old) as well as the Valid one.
PART OF	The block malfunctions: it provides only part of the expected information
REVERSE	The block malfunctions and sends out information in a

Selected Guide Words	
Guide Word	**Corresponding Failure Mode**
NO	The block does not execute its functions. No output is available.
MORE	The block malfunctions and: 1. Covered by OTHER THAN 2. executes its function more than needed
LESS	The block malfunctions and: 1. Covered by OTHER THAN 2. executes its function less than needed
AS WELL AS	Covered by OTHER THAN
PART OF	Covered by OTHER THAN
REVERSE	Covered by OTHER THAN

Generic Guide Words from CAP 760		Selected Guide Words	
Guide Word	**Corresponding Failure Mode**	**Guide Word**	**Corresponding Failure Mode**
	reverse way		
OTHER THAN	The block malfunctions and the information sent out is other than expected (i.e. corrupted): 1. Valid Data, but different from the effective one; 2. Non-Valida Data	**OTHER THAN**	The block malfunctions and the information sent out is other than expected (i.e. corrupted): 1. Valid Data, but different from the effective one (e.g. more/less permissive, old, reversed information): 2. Non-Valida Data (e.g. partial information, information of other interfaces).
EARLY	Due to a malfunction the block's output is anticipated	**EARLY**	Due to a malfunction the block's output is anticipated
LATE	Due to a malfunction the block enters in a loop, and delays the output	**LATE**	Due to a malfunction the block enters in a loop and delays the output
BEFORE	Due to a malfunction the block's output is sent before the expected condition(s) is verified	**BEFORE**	Covered by EARLY
AFTER	Due to a malfunction the block's output is delayed even if the expected condition(s) is verified	**AFTER**	Covered by LATE

Table 16: The CAP 760 Guide Words applied for the Architectural Block Safety Analysis

The Interfaces Failure Modes

Regarding the interfaces, a distinction should be made upon the nature of the information transmitted over them. Indeed, the information exchanged internally and externally the VBTS block could be a digital data packet (compliant with the specific communication protocol) or an analogue signal (e.g. the RF signal coming from the satellite antenna). The former is analysed in Table 17 while the second in the Table 18

The left side of both tables reports the potential failure modes affecting a communication interface (or the information get at the receiver side) declined upon the list of Guide Words provided in CAP 760. Since not each Guide Word might be associable to an interface credible failure mode or multiple guide words lead to the same failure mode, a selection process has been applied on the Guide Word list. The right side of both tables reports the resulting, actually applied, sub-list of guide words (highlighted in green colour).

Generic Guide Words from CAP 760	
Guide Word	**Corresponding Failure Mode**
NO	Packet loss
MORE	One or more packets have been inserted or repeated
LESS	One or more packets have been deleted
AS WELL AS	One or more external packets have been received as well as the expected ones
PART OF	Only part of the packet(s) is received (e.g. only some bytes/bit are received or only few packets out of the total packets)
REVERSE	The complementary message is received
OTHER THAN	"The received packet is other than expected (i.e. corrupted/affected by channel errors): 1. Valid Data, but different from the one actually transmitted 2. Non-Valid Data
EARLY	The packet is received earlier (in time)
LATE	The interface channel inserts a delay Δt on the packet travel time
BEFORE	The packet is received before (i.e. resequenced)
AFTER	The packet is received after (i.e. resequenced)

Selected Guide Words	
Guide Word	**Corresponding Failure Mode**
NO	Packet loss
MORE	N/A - It is a non-credible failure due to channel errors
LESS	Covered by NO
AS WELL AS	Covered by OTHER THAN
PART OF	Covered by OTHER THAN or NO, respectively
REVERSE	Covered by OTHER THAN
OTHER THAN	The received packet is other than expected (i.e. corrupted/affected by channel errors) 1. Valid Data, but different from the one actually transmitted/expected 2. Non-Valid Data
EARLY	N/A - It is a non-credible failure due to channel errors
LATE	The interface channel inserts a delay Δt on the packet transition time
BEFORE	Covered by OTHER THAN
AFTER	Covered by OTHER THAN

Table 17: The CAP 760 Guide Words applied for the Safety Analysis of the Interface carrying a Digital Data Packet

Generic Guide Words from CAP 760	
Guide Word	**Corresponding Failure Mode**
NO	No power is measured
MORE	More power than expected is measured
LESS	Less power than expected is measured
AS WELL AS	The noise and/or interference power levels are measured as well as the power of the expected signal
PART OF	The expected power is measured in an intermittent manner
REVERSE	N/A
OTHER THAN	A power level other than the expected one is measured (e.g. due to channel noise/ interference)
EARLY	N/A
LATE	N/A
BEFORE	N/A
AFTER	N/A

Selected Guide Words	
Guide Word	**Corresponding Failure Mode**
NO	No signal/power is measured
MORE	Covered by OTHER THAN
LESS	Covered by OTHER THAN
AS WELL AS	Covered by OTHER THAN
PART OF	The expected power is measured in an intermittent manner
REVERSE	N/A
OTHER THAN	A power level other than the expected one is measured (e.g. due to channel noise/ interference)
EARLY	N/A
LATE	N/A
BEFORE	N/A
AFTER	N/A

Table 18: The CAP 760 Guide Words applied for the Safety Analysis of the Interface carrying an Analogue Signal

9.2 APPENDIX B – THE FMECA

9.2.1 Registration and Start Up

The Functional FMECA for the "*Registration and Start Up"* scenario of § 2 in [R2], traced as *Scenario A* herein, is reported in the Excel file attached here below, including both the Block and Interface analyses.
For further detail on the scenario, please refer the § 2 of [R2].

Scenario A -
FMECA_Registration&

9.2.2 Start Of Mission In Level 2 with Q_STATUS "Known", at Terminal Railway Station

The Functional FMECA for the "*SoM in Level 2 with Q_STATUS "Known" at Terminal Railway Station"* scenario of §3.2 in [R2], traced as *Scenario B* herein, is reported in the Excel file attached here below, including both the Block and Interface analyses.
For further detail on the scenario, please refer the §3.2 of [R2].

Scenario B -
FMECA_SOM_Termina

9.2.3 Start Of Mission In Level 2 with Q_STATUS "Known", at Intermediate Railway Station

The Functional FMECA for the "*SoM in Level 2 with Q_STATUS "Known" at Intermediate Railway Station"* scenario of §3.3 in [R2], traced ad *Scenario C* herein, is reported in the Excel file attached here below, including both the Block and Interface analyses.
For further detail on the scenario, please refer the §3.3 of [R2].

Scenario C -
FMECA_SOM_Interme

9.2.4 Start Of Mission In Level 2 with Q_STATUS "Known", in Line

The Functional FMECA for the *"SoM in Level 2 with Q_STATUS "Known" in Line"* scenario of §3.4 in [R2], traced as *Scenario D* herein, is reported in the Excel file attached here below, including both the Block and Interface analyses.
For further detail on the scenario, please refer the §3.4 of [R2].

Scenario D -
FMECA_SOM_Line_Q_s

9.2.5 Start of Mission in Level 2 with Q_STATUS "Unknown", at Terminal Railway Station

The Functional FMECA relative to the "*SoM in Level 2 with Q_STATUS "Unknown" at Terminal Railway Station*" scenarios of § 4.1 in [R2] are reported in the Excel files attached here below, including both the Block and Interface analyses.

SOM WITH "APPROXIMATION" OF THE TRAIN POSITION

Referred as *Scenario E* herein. For further detail on the scenario, please refer the §4.1.1 of [R2]

Scenario E - FMECA_SOM_Termina

WITH THE TMS-RBC CONNECTION AVAILABLE

Referred as *Scenario F* herein. For further detail on the scenario, please refer the §4.1.2 of [R2]

Scenario F - FMECA_SOM_Termina

WITHOUT THE TMS-RBC CONNECTION

Referred as *Scenario G* herein. For further detail on the scenario, please refer the §4.1.3 of [R2]

Scenario G - FMECA_SOM_Termina

9.2.6 Start of Mission in Level 2 with Q_STATUS "Unknown", at Intermediate Railway Station

The Functional FMECA relative to the "*SoM in Level 2 with Q_STATUS "Unknown" at Intermediate Railway Station"* scenarios is reported in the Excel files attached here below, including both the Block and Interface analyses.

Analogously to § 9.2.5 three cases have been identified, herein referred as *Scenario H*, *Scenario I* and *Scenario J*, for further detail please refer the §4.2 of [R2].

Scenario H - FMECA_SOM_Interme

Scenario I - FMECA_SOM_Interme

Scenario J - FMECA_SOM_Interme

9.2.7 Start of Mission in Level 2 with Q_STATUS “Unknown” in Line

The Functional FMECA relative to the “*SoM in Level 2 with Q_STATUS “Unknown” in Line*” scenarios is reported in the Excel files attached here below, including both the Block and Interface analyses.
Analogously to § 9.2.5 and § 9.2.6 three cases have been identified, herein referred as *Scenario K*, *Scenario L* and *Scenario M*, for further detail please refer the §4.3 of [R2].


Scenario K - FMECA_SOM_ Line_ Q


Scenario L - FMECA_SOM_ Line_ Q


Scenario M- FMECA_SOM_ Line_ Q

REFERENCES

[R1] ERSAT GGC_WP2 D2.1, “Enhanced Functional ERTMS Architecture Capable of using GNSS and Public Radio TLC Technologies”, Rev 0.4.

[R2] ERSAT_GGC_WP2, “ERTMS Operational Scenarios”, Technical Note, Rev. 0.2.

[R3] UNISIG – “SUBSET-026 System Requirements Specification”, Ver. 3.6.0.

[R4] UNISIG – “SUBSET-036 FFFIS for Eurobalise”, Ver. 2.4.1.

[R5] UNISIG – “SUBSET-088 ETCS Application Levels 1 & 2 - Safety Analysis” Ver 3.5.4.

[R6] Commission Regulation (EC) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009.

[R7] Commission Regulation (EU) N°2015/1136 of 13 July 2015 amending implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment.

[R8] CENELEC EN 50126-1, “Railway Applications - The Specification And Demonstration Of Reliability, Availability, Maintainability And Safety (RAMS) - Part 1: Generic Rams Process”, 1999.

[R9] CENELEC EN 50129, “Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling”, 2003.

[R10] CENELEC EN 50159, “Railway Applications - Communication, Signalling and Processing Systems - Safety-Related Communication in Transmission Systems”, 2010.

[R11] MIL-STD-1629A:1980 – Procedures for performing a failure mode, effects and criticality analysis.

[R12] CAP 760, “Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases”, December 2010.