EEIG ERTMS Users Group
123-133 Rue Froissart, 1040 Brussels, Belgium
Tel: +32 (0)2 673.99.33 - TVA BE0455.935.830
Website: www.ertms.be E-mail: info@ertms.be

GNSS Augmentation for ERTMS/ETCS

System Functional Hazard Analysis

EUG Solution for Enhanced Onboard Localisation Change Request (CR1368) – GNSS Augmentation for ERTMS/ETCS

Ref: 20E086
Version: 0g
Date: 06/10/2023

Modification History

Version	Date	Modification / Description	Editor
0a	01/05/2020	Initial version (incomplete draft)	C. Wullems (ESA)
0b	05/06/2020	Initial version (incomplete draft) – major update including update of basic functions	C. Wullems (ESA)
0c	08/07/2020	Initial draft release	C. Wullems (ESA)
0d	05/05/2022	Major update and revision to implement comments from JWG review (EUG, Shift2Rail X2Rail5-WP5: Alstom, Hitachi Rail STS, AŽD, CAF, NSL)	C. Wullems (ESA)
0e	19/05/2022	Update after internal review (C. Neville, S. Porfili, J. Ostolaza, EUSPA)	
0e	21/05/2022	Update after internal review (G. Fernandez, ESSP)	
0e	23/05/2022	Update after review by X2Rail5-WP5 (A. Lucidi, K. Ali, Alstom)	
0e	01/06/2022	Update after review by X2Rail5-WP5 (L. Freda Albanese, Hitachi Rail STS)	
0f	10/06/2022	Draft release for EURAIL System Pillar	C. Wullems (ESA)
0g	16/06/2023	Update after JWG workshop 29/09/2022 • Updated system description and reference architecture considering simplification of trackside functions; • Updated FMEA considering simplification of trackside functions, and alignment with updated SRS; and • Updated preliminary THR allocations considering simplification of trackside functions.	C. Wullems (ESA)
0g	28/09/2023	Document update: • Updated hazard identification considering three on-board localisation architecture types; and • Removed trace of minimal cut set (GATE58) from SUBSET-88-2 Part 1 in annex; • Editorial updates improving readability, correction of typographic errors.	C. Wullems (ESA)
0g	06/10/2023	Minor updates after JWG workshop 02/10/2023. Draft release for input to ERJU work packages on GNSS Augmentation for Rail based on EGNOS.	C. Wullems (ESA)

Table of Contents

1 Introduction

1.1 Scope and Purpose

1.1.1.1 GNSS Augmentation (GA) for ERTMS/ETCS aims to provide a framework to support the use supported GNSS Augmentation Systems such as EGNOS (the European Geostationary Navigation Overlay Service) to enable the use of Global Navigation Satellite Systems (GNSS) within enhanced on-board localisation in a technology-neutral manner.

1.1.1.2 The **scope** of this document is to define a preliminary set of high-level quantitative safety requirements that must be fulfilled to provide interoperable GA for ERTMS/ETCS. This document addresses the specificities of GNSS Augmentation based on hypothetical EGNOS L1 and DFMC railway safety of life (SoL) services.

1.1.1.3 The **purpose** of this document is to define high-level quantitative safety requirements needed for technical interoperability[1] of the GA for ERTMS/ETCS. This document provides:

- GA system description including functional architecture and interfaces defined to the level required to support interoperability and the safety analyses
- GA hazard identification and linking of GA system hazards to hazards in subsystem and system boundaries
- GA hazard analysis (causal analysis conducted with a transmission channel and functional FMEA)
- Safety requirements (given as tolerable hazard rates and tolerable functional failure rates)

1.1.1.4 The annexes of this document provide the following analyses and additional support information:

- Annex A: Preliminary THR apportionment
- Annex B: Open points to be addressed in future iterations of the analysis

1.1.1.5 This document is part of a package of documents on the GS for ERTMS/ETCS in support of Change Request (CR1368). The package is comprised of the following documents:

- GNSS Augmentation for ERTMS/ETCS – System Requirement Specification [EUG-20E085] (this document)
- GNSS Augmentation for ERTMS/ETCS – Interface Control Document for GA-OB / GA-TS (Airgap) [EUG-20E087]
- GNSS Augmentation for ERTMS/ETCS – System Functional Hazard Analysis [EUG-20E086]

[1] Technical interoperability is defined as the set of harmonised technical requirements that enable interoperability.

1.2 References

1.2.1.1 The following documents are references in this document.

PERSPECTIVE	ERA, “Report on ERTMS Longer Term Perspective,” 18/12/2015.
[SS041]	UNISIG, “ERTMS/ETCS – Performance Requirements for Interoperability – SUBSET-041 Issue 3.2.0.” 2015.
[SS077]	UNISIG, “ERTMS/ETCS – UNISIG Causal Analysis Process – SUBSET-077 Issue 3.0.0.” 2016.
[SS088-2 Part 1]	UNISIG, “ERTMS/ETCS – ETCS Application Level 2 – Safety Analysis: Part 1 – Functional Fault Tree – SUBSET-088-2 Part 1 Issue 3.6.0.” 2016.
[SS088-2 Part 2]	UNISIG, “ERTMS/ETCS – ETCS Application Level 2 – Safety Analysis: Part 2 – Functional Analysis – SUBSET-088-2 Part 2 Issue 3.6.0.” 2016.
[SS088 Part 3]	UNISIG, “ERTMS/ETCS – ETCS Application Level 2 – Safety Analysis: Part 3 – THR Apportionment – SUBSET-088 Part 3 Issue 3.6.0.” 2016.
[SS091]	UNISIG, “ERTMS/ETCS – Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2 – SUBSET-091 Issue 3.6.0.” 2016.
[EUG-20E087]	EUG, “GNSS Augmentation for ERTMS/ETCS – Interface Control Document for GA-OB / GA-TS (Airgap). Version 0g.” 2023.
[EUG-20E085]	EUG, “GNSS Augmentation for ERTMS/ETCS – System Requirement Specification. Version 0g.” 2023.
[EN50126-1]	CENELEC, “Railway applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process – EN 50126-1.” CENELEC, Brussels, Belgium, 2017.
[EN50129]	CENELEC, “Railway applications – Communication, signalling and processing systems – Safety-related electronic systems for signalling – EN 50129.” CENELEC, Brussels, Belgium, 2018.
[EN50159]	CENELEC, “Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems – EN 50159.” CENELEC, Brussels, Belgium, 2010.
[DO-229]	RTCA, “DO-229F – Minimum Operational Performance Standards for Global Positioning System/Satellite Based Augmentation System Airborne Equipment.” RTCA Inc., Washington D.C., USA, 2020.
[DO-235]	Radio Technical Commission for Aeronautics, “Assessment of Radio Frequency Interference to the GNSS L1 Frequency Band”, Ref: DO-235B; 13/03/2008.
[ED-259]	EUROCAE, “ED-259A (v0.17) – Minimum Operational Performance Standard for Galileo / Global Positioning System / Satellite-based Augmentation System Airborne Equipment.” Saint-Denis, France, 2023.

[IS-GPS-200]	GPS Directorate, “Interface Specification – NAVSTAR GPS Space Segment / Navigation User Segment User Interfaces – IS-GPS-200. Rev. N.” 2022.
[IS-GPS-705]	GPS Directorate, “Interface Specification – NAVSTAR GPS Space Segment / User Segment L5 Interfaces – IS-GPS-705. Rev. J.” 2022.
[GAL-OS-SIS-ICD]	European Commission, “European GNSS (Galileo) Open Service – Signal-in-Space Interface Control Document. Issue 2.0.” 2021.
[X2Rail2-D3.9]	CAF, Siemens Mobility and Thales Transportation. “Deliverable D3.9 – System Architecture Specification and System Functional Hazard Analysis for Stand Alone Fail-Safe Train Positioning”; 06/04/2021

1.3 Terms and Abbreviations

1.3.1.1 The following terms and abbreviations are used in this document:

ATPE	Along-Track Position Error
ATPL	Along-Track Protection Level
CCS	Control-Command and Signalling
CCS-OB	CCS On-board
CCS-TS	CCS Trackside
CED	Clock and Ephemeris Data
CPF	Central Processing Facility
CRC	Cyclic Redundancy Check
DFC	Dual Frequency Correction
DFMC	Dual Frequency Multiple Constellation
DFRE	Dual Frequency Range Error (dual frequency UDRE)
DFRECI	Dual Frequency Range Error Change Indicator
DFREI	Dual Frequency Range Error Indicator
DNU	Do Not Use
ECAC	European Civil Aviation Conference
EEIG	European Economic Interest Group
EGNOS	European Geostationary Navigation Overlay Service (SBAS developed by the European Union)
ERA	European Union Agency for Railways (formerly European Railway Agency)
ERJU	Europe’s Rail Joint Undertaking
ERTMS	European Rail Traffic Management System
ESA	European Space Agency
ESSP	European Satellite Services Provider
ETCS	European Train Control System
EUG	EEIG ERTMS Users Group
EUSPA	European Union Agency for the Space Programme (formerly European GNSS Agency)

FDE	Fault Detection and Exclusion
FE	Feared Event
FEC	Forward Error Correction
FFFIS	Form-Fit Functional Interface Specification
FIS	Functional Interface Specification
FMEA	Failure Modes and Effects Analysis
FRMCS	Future Railway Mobile Communication System
FTA	Fault Tree Analysis
GA	GNSS Augmentation
GAC	GNSS Augmentation Channel
GAD	GNSS Augmentation Dissemination
GA-OB	GNSS Augmentation On-board
GAP	GNSS Augmentation Processing
GA-TS	GNSS Augmentation Trackside
GEO	Geostationary Earth Orbit
GIVE	Grid Ionospheric Vertical Error
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM-R	Global System for Mobile Communications – Railway
HMI	Hazardous Misleading Information
HPL	Horizontal Protection Level
HR	Hazard Rate
IOD	Issue of Data
IODC	Issue of Data Clock
IODE	Issue of Data Ephemeris
LOC-OB	On-board Localisation
LPV	Localizer Performance with Vertical Guidance
MCC	Mission Control Centre
MI	Misleading Information
MOPS	Minimum Operation Performance Standard

MT	Message Type
NLES	Navigation Land Earth Station
NLOS	Non-Line-Of-Sight
OBU	On-Board Unit
OS	Open Service
PDM	Position Domain Monitor
PRN	Pseudo-Random Noise
PR	PseudoRange
RIMS	Ranging and Integrity Monitoring Station
RTCA	Radio Technical Commission for Aeronautics
SARPs	Standards and Recommended Practices
SBAS	Satellite Based Augmentation System
SDD	Service Definition Document
SFHA	System Functional Hazard Analysis
SIL	Safety Integrity Level
SIS	Signal in Space
SNT	SBAS Network Time
SoL	Safety of Life
SoM	Start of Mission
SRS	System Requirements Specification
SV	Satellite Vehicle
TBC	To Be Confirmed
TBD	To Be Defined
TFFR	Tolerable Function Failure Rate
THR	Tolerable Hazard Rate
TSI	Technical Specification for Interoperability
TTA	Time To Alert
UDRE	User Differential Range Error
UDREI	User Differential Range Error Indicator
UIRE	User Ionospheric Range Error

UTC	Universal Time Coordinate
VLF	Vehicle Localisation Function
VLS	Vehicle Localisation Sensor

2 Approach for the Preliminary Safety Analyses

2.1.1.1 The table below summarises the approach taken for the safety analyses in this document, taking into consideration the relevant phases and activities from EN 50126 [EN50126].

Phase	How phase is addressed in this document	Document section
1. System definition	Functions and interoperability-relevant interfaces are defined for the GA for ERTMS/ETCS, supported by the definition of a high-level functional reference architecture.	Section 3 provides the GA dissemination framework for ERTMS/ETCS system description.
2: Risk analysis and evaluation	In this preliminary analysis, risk analysis and evaluation focus on the identification and classification of hazards associated with the system, and the assessment of risk. The selected risk acceptance principle is *explicit risk estimation*, due the introduction of GNSS augmentation and GNSS-based localisation being considered a significant change with the introduction of entirely new elements in ERTMS/ETCS. A LOC-OB implementation would need to satisfy safety and performance requirements that ensure suitability of its use with ETCS; however, as the specific approach to integration with ETCS is not currently agreed, there are limitations to the level of analysis that can be performed. At a system level, it can be assumed that ETCS with enhanced localisation using GNSS and GA would comply with the THR for the ETCS Core Hazard and at subsystem level, with the THRs for on-board and trackside subsystems (i.e., incorporating the LOC-OB, and supporting elements including GNSS Augmentation). The risk analysis includes: • Identification of hazards at the boundary of GNSS Augmentation Processing (GAP) in the Vehicle Localisation Function (VLF) and at the boundaries of on-board localisation (LOC-OB) and ETCS. Links are established between VLF<GAP> hazards and the ETCS Core Hazard considering three on-board localisation architecture types. • Identification of the causes of VLF<GAP> hazards though an FMEA assessing transmission channel and functional hazards based on the GA reference functional architecture.	Section 4 addresses identification of hazards; Sections 5, 6, and 7 address identification of causes; and Section 8 provides the list of hazardous events from the FMEA.

3: Specification of system requirements	In this preliminary analysis, this phase focuses on the specification of safety requirements related to functions and interoperability-relevant interfaces, as well as the associated safety targets. This includes: • Safety requirements and exported conditions from the FMEA. • A preliminary THR apportionment based on a fault-tree analysis that considers hazardous events identified in the FMEA. • Specification of quantitative safety targets.	Section 9 provides the list of safety requirements and exported conditions from the FMEA; Section 10 provides preliminary quantitative safety targets; and Annex A provides the preliminary THR apportionment used to derive the preliminary safety targets.

3 GNSS Augmentation Dissemination Framework for ERTMS/ETCS System Description

3.1 High-level EGNOS-based Functional Architecture for Safety Analyses

3.1.1.1 Figure 3-1 illustrates the reference functional architecture for EGNOS-based GNSS augmentation in ERTMS/ETCS with internal and external interfaces for the purpose of conducting the safety analyses.

3.1.1.2 The architecture addresses EGNOS L1 and DFMC services, focusing on the essential interfaces with an impact on interoperability for delivering GNSS augmentation functionality, maintaining neutrality from a technology perspective regarding integration of GNSS and augmentation within the onboard localisation equipment.

3.1.1.3 Future EGNOS services including the possible use of terrestrial dissemination means are not addressed in this release of the SFHA.

3.1.1.4 The reference functional architecture is comprised of the GNSS Augmentation On-board (GA-OB) and GNSS Augmentation Trackside (GA-TS):

- The GA-OB includes GNSS receiver(s), one several types of Vehicle Localisation Sensors (VLSs) used by the Vehicle Localisation Function (VLF), and GNSS Augmentation Processing within the VLF.
- The GA-TS includes the GNSS Augmentation Dissemination Function (GADF) and the trackside interfaces to the GNSS Augmentation System (GAS) and GNSS.

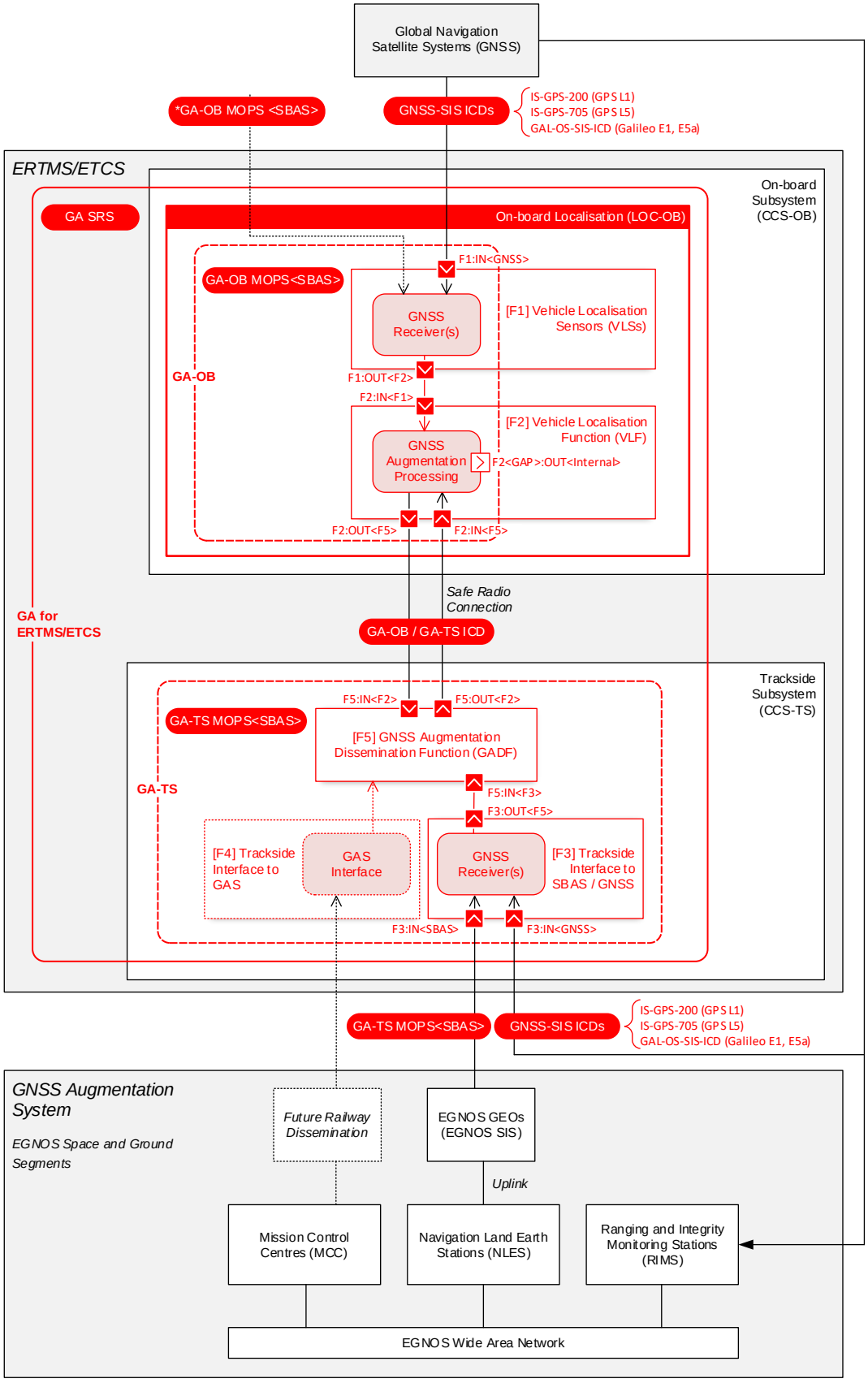


Figure 3-1. EGNOS-based GNSS Augmentation Reference Functional Architecture for ERTMS/ETCS (Interfaces)

3.1.1.5 The Vehicle Localisation Function (VLF) utilises GNSS augmentation to improve position accuracy and derive a statistical bounding on residual orbit, clock, and ionosphere errors through the application of corrections and residual pseudorange error models. In the case of EGNOS, the on-board GNSS receiver(s) would be required to conform to the Minimum Operational Performance Standards (MOPS) of the EGNOS Railway SoL service (GA-OB MOPS<SBAS>)

3.1.1.6 The GA-OB MOPS<SBAS> would define essential requirements on the GNSS receiver including (not limited to):

- Assumptions on GNSS receiver constraints including receiver pre-correlation filtering (bandwidth, roll-off, and central frequency), receiver differential group delay, and requirements on correlator spacing and code tracking loop;
- GNSS signal and message processing;
- SBAS message processing; and
- Computation of pseudorange error bounds.

3.1.1.7 In addition to reception of SBAS messages via the trackside, the GA-OB may support direct reception of SBAS messages via the SBAS GEO SIS; however, principles for use of this interface are not currently defined in the SRS[2] and therefore not addressed in this SFHA. It should be noted that information from EGNOS received by the VLF via the GA-TS and via the SBAS GEO SIS cannot be mixed in a single GNSS processing channel.

3.1.1.8 The GA-TS is responsible for the interface to the GNSS Augmentation System (GAS), and specifically to EGNOS via the SBAS SIS for EGNOS L1 and DFMC services. The GNSS Augmentation Dissemination Function (GADF) is responsible for the dissemination of SBAS messages containing correction and integrity information to the GA-OB. The GADF timestamps and encapsulates SBAS messages in GAM packets, leaving the in-built message protections (e.g., CRC) intact. While the GADF performs some message processing (e.g., in support of maintaining active data sets), by encapsulating SBAS messages, the complexity of the function is greatly reduced, and assumptions related to inbuilt defences against message-level hazards that are assumed by EGNOS and its respective integrity commitments are maintained. The GADF can also provide GNSS navigation data to the GA-OB to support faster start-up time, especially in difficult start-up environments (e.g., where there is significant obscuration of GNSS satellites).

3.1.1.9 The GA-TS also is responsible for obtaining navigation data from the Global Navigation Satellite System (GNSS), where subframes / pages / messages containing navigation data are encapsulated and provided to the GA-OB for the constellations supported by EGNOS (i.e., GPS LNAV and Galileo F/NAV).

3.1.1.10 It is assumed the trackside would support a mandatory set of EGNOS-based services linked with a future baseline (ETCS version) for Europe. Markets outside of Europe are not constrained by the CCS TSI.

[2] It was agreed at the EUG/EUSPA/ESA/X2Rail5 Joint Working Group workshop held on the 02/10/2023 that the interface be left open for further assessment. It was deemed valuable for regional line solutions (with reference to the ERJU FUTURE project, in which a demonstrator considering direct reception of EGNOS messages at the GA-OB via the EGNOS SIS is planned). Refer to Open Items in Annex B.

3.1.1.11 The ICD for GA-OB / GA-TS [EUG-20E087] defines interoperability-relevant messages, packets and variables exchanged between the GA-OB and GA-TS.

3.1.1.12 The Safe Radio Connection between the GA-OB and GA-TS is intentionally left undefined; for example, it could potentially be the EURORADIO channel between the on-board and trackside or a dedicated GNSS augmentation radio channel between the GA-OB and GA-TS provided by the FRMCS.

3.1.2 GA Functions

3.1.2.1 The *GNSS Augmentation (GA) dissemination framework for ERTMS/ETCS* is comprised of the functions listed in Table 3-1, which additionally indicates the documents where requirements are defined.

3.1.2.2 A functional decomposition has been performed on macro functions of the *GA dissemination framework for ERTMS/ETCS* to determine the sub functions that comprise the macro functions and the basic functions that comprise the sub functions. Table 3-1 lists the macro functions and identified sub functions (refer to Section 5.3 for the complete functional decomposition).

Table 3-1. Functions of GNSS Augmentation for ERTMS/ETCS

Macro Function / Sub Function		GA Dissemination Framework Requirements (SRS)	On-board GA-Specific Requirements (GA-OB MOPS)	Trackside GA-Specific Requirements (GA-TS MOPS)	GNSS-Specific Signal-in-Space ICD (GNSS-SIS-ICD)	Messages, packets and variables exchanged over airgap for GA (GA-OB / GA-TS ICD)
F1	**Vehicle Localisation Sensors (VLSs) <GNSS Receiver>[3]**					
F1.1	Process GNSS signal		X		X	
F2	**Vehicle Localisation Function (VLF) <GNSS Augmentation Processing>**					
F2.1	Process GNSS navigation data (received from GNSS receiver and GA-TS)	X	X		X	X
F2.2	Process GA messages (received from GA-TS)	X	X			X
F2.3	GNSS pseudorange determination and use		X			
F2.4	Compute and apply GNSS pseudorange error models (GA-provided integrity)		X			
F2.5	Supervise GA message content timeout	X	X			
F2.6	Supervise and manage TTA	X	X			
F2.7	Manage GA session	X				X

[3] Note: Functionality related to reception of SBAS messages by the on-board GNSS receiver(s) from the SBAS GEO SIS is not currently addressed in the SRS or SFHA. It will be addressed in a future release of the documents.

Macro Function / Sub Function		GA Dissemination Framework Requirements (SRS)	On-board GA-Specific Requirements (GA-OB MOPS)	Trackside GA-Specific Requirements (GA-TS MOPS)	GNSS-Specific Signal-in-Space ICD (GNSS-SIS-ICD)	Messages, packets and variables exchanged over airgap for GA (GA-OB / GA-TS ICD)
F3	**Trackside Interface to SBAS / GNSS <GNSS Receiver>**					
F3.1	Process SBAS signal			X		
F3.2	Process GNSS signal			X	X	
F4	**Trackside Interface to GAS <TBD> (future placeholder)**					
F5	**GNSS Augmentation Dissemination Function (GADF)**					
F5.1	Select GACs	X		X		
F5.2	Process GA messages for selected GACs (received from trackside interface to SBAS / GAS)	X		X		
F5.3	Provide GA message stream(s)	X				
F5.4	Provide GA active data for selected GACs	X				
F5.5	Provide GA active alerts for selected GACs	X				
F5.6	Process GNSS navigation data (received from trackside interface to GNSS)	X		X	X	
F5.7	Provide GNSS navigation data sets	X			X	
F5.8	Manage GA session	X				X

3.1.3 Macro Function Interfaces and Sub Function Outputs

3.1.3.1 The macro function interfaces and sub function outputs relevant for conducting the safety analyses are detailed in this subsection (illustrated in Figure 3-1).

3.1.3.2 External (standardised) macro function interfaces:

These interfaces are standardised to support technical interoperability.

Interface ‘F1:IN<GNSS>’ Interface between the GNSS Receiver(s) in the GA-OB and the Global Navigation Satellite System (GNSS) via the SIS. This includes the GNSS constellations supported by EGNOS (i.e., GPS L1, L5; Galileo E1-B/C, E5a).

Interface ‘F3:IN<SBAS>’ Interface between the GNSS Receiver(s) in the GA-TS and EGNOS via the SBAS SIS.

Interface ‘F3:IN<GNSS>’ Interface between the GNSS Receiver(s) in the GA-TS and GNSS via the SIS. This includes the GNSS constellations supported by EGNOS (i.e., GPS L1, L5; Galileo E1-B/C, E5a).

Interface ‘F2 ↔ F5’ Interface between the GA-OB and GA-TS. The ICD for GA-OB / GA-TS [EUG-20E087] defines interoperability-relevant messages, packets and variables exchanged over the Safe Radio Connection (airgap).

3.1.3.3 Internal (non-standardised) macro function interfaces:

Interface ‘F1 → F2’ Functional interface between the GNSS Receiver(s) and VLF in the GA-OB.

Interface ‘F3 → F5’ Functional interface between the GNSS Receiver(s) and GADF in the GA-TS.

3.1.3.4 Sub function outputs (internal of macro function):

This level of abstraction is necessary to support safety analyses for the GNSS augmentation processing part of the VLF, as other subfunctions for PVT processing / hybridisation with sensors, etc. are not defined and are specific to the supplier LOC-OB implementation.

‘F2<GAP> → F2<Int>’ Output of GNSS Augmentation Processing (GAP) sub function of the VLF macro function (F2).

4 Hazard Identification

4.1 Methodology

4.1.1.1 To support the preliminary hazard analyses, a structured hierarchical approach is taken for the identification of hazards at different boundaries:

- Boundary of the European Train Control System (ETCS);
- Boundary of On-board Localisation (LOC-OB); and
- Boundary of GNSS Augmentation Processing of the Vehicle Localisation Function (VLF<GAP>).

4.1.1.2 As there is currently no defined reference architecture for ERTMS/ETCS with On-board Localisation (LOC-OB), for the scope of the analysis:

- Hazards identified at the boundary of the GA dissemination framework for ERTMS/ETCS (VLF<GAP>) are linked to hazards at the LOC-OB boundary with assumptions on the probability a hazardous event at the VLF<GAP> boundary would propagate to the boundary of the LOC-OB.
- Hazards identified at the LOC-OB boundary are linked to ETCS hazardous events considering three generalised functional architectures integrating on-board localisation with ETCS. The scope of these functional architectures is only to establish causal links for supporting the FMEA.
- The ETCS functional fault tree from SUBSET-088 [SS088-2 Part 1] is used to establish the link between relevant ETCS hazardous events and ETCS system hazards.

4.1.1.3 The GA reference functional architecture (Figure 3-1) illustrates a system of systems, with the GA dissemination framework for ERTMS/ETCS interfacing to EGNOS and GNSS systems. Identification of hazards within these systems is not in the scope of this analysis as they are external to the defined system.

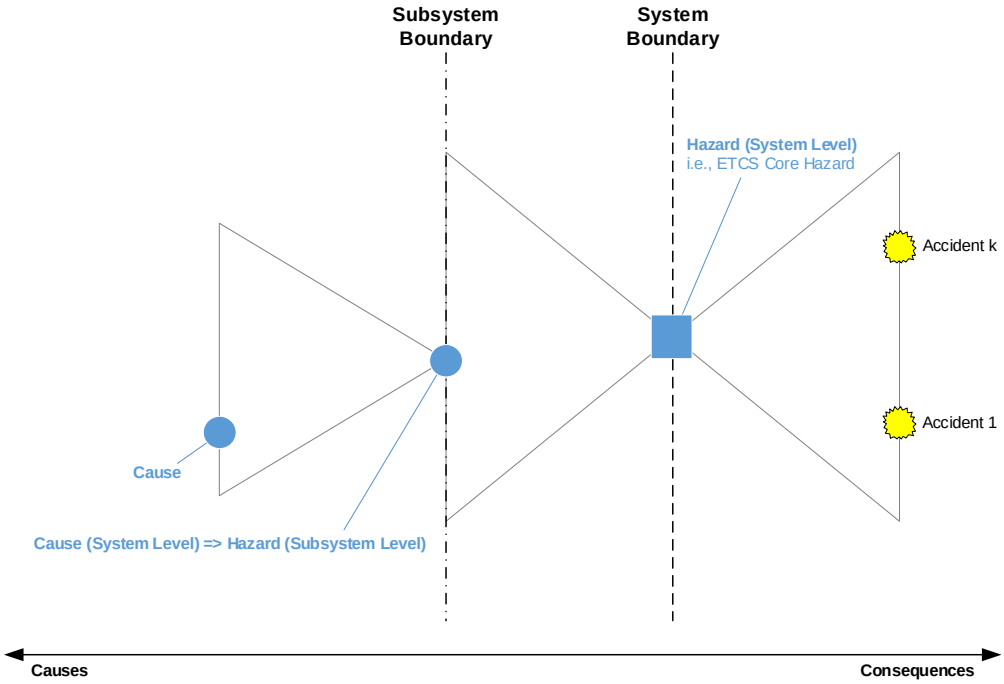


Figure 4-1. Identification of hazards at different boundaries [EN50129]

4.2 Identified Hazards

4.2.1.1 This section summarises the results of the preliminary hazard analysis. The identified hazards at the GNSS augmentation processing and on-board localisation boundaries are used to determine how failure modes of GNSS augmentation processing, identified by the FMEA in Section 6, can propagate to the ETCS system level hazards (i.e., ETCS Core Hazard).

4.2.2 Hazards at ETCS System Boundary

4.2.2.1 The following two system-level hazards at the ETCS system boundary are defined in SUBSET-091 [SS091]:

ID	ETCS Core Hazard
Hazard	Failure to provide on-board supervision and protection according to the information advised to the ETCS on-board from external entities
Remarks	This hazard covers the case where ETCS has information on safe speed and distance.

ID	ETCS Auxiliary Hazard
Hazard	Failure to interact correctly with the driver regarding information not supervised by ETCS
Remarks	This hazard covers the case where ETCS does not have information on safe speed and distance.

4.2.2.2 The allocation of responsibility between ETCS and the driver varies depending on the ETCS mode (as specified in SUBSET-026). For example, in Full Supervision (FS), a larger responsibility is placed on ETCS compared to Staff Responsible (SR), in which only a limited amount of information about train safety is handled via ETCS [SS091]. Important information such as train speed is provided to the driver to enable safe driving. The ETCS Auxiliary Hazard covers the cases related to interaction with the driver via the DMI where ETCS does not have information on safe speed and distance.

4.2.2.3 Hazards associated with the DMI functions independent of the ETCS Core Hazard are not addressed in this analysis.

4.2.3 Hazards at On-board Localisation (LOC-OB) Boundary

4.2.3.1 The On-board Localisation (LOC-OB) functions considered in this analysis are detailed in Table 4-1. Note that non-safety related positioning functions have not been included (e.g., provision of 3D train position for passenger services, etc.)

Table 4-1. On-board localisation (LOC-OB) functions

LOC-OB Function ID	Description
LOC-OB_FN-001	Provide safe train front end 1D position
LOC-OB_FN-002	Provide safe train speed
LOC-OB_FN-003	Provide safe train acceleration
LOC-OB_FN-004	Provide safe distance travelled

4.2.3.2 The hazards identified with respect to the above functions are detailed in Table 4-2.

Table 4-2. On-board localisation (LOC-OB) hazards

LOC-OB Hazard ID	Description
LOC-OB_HAZ-001	Confidence interval does not include actual 1D position of train front end
LOC-OB_HAZ-002	Train speed underestimates the actual speed of the train (speed confidence interval does not include actual speed of the train)
LOC-OB_HAZ-003	Incorrect actual physical speed direction
LOC-OB_HAZ-004	Acceleration confidence interval does not include the actual acceleration of the train
LOC-OB_HAZ-005	Confidence interval of distance travelled does not include actual position of train front end

4.2.3.3 The above hazards at the boundary of On-board Localisation (LOC-OB) are linked to ETCS hazardous events considering three generalised functional architectures integrating on-board localisation with ETCS based on a generalisation of architectural concepts from Shift2Rail X2Rail5 Stream 1 and Stream 2, and OCORA release 3. These functional architectures are illustrated in Table 4-3 with the associated allocation of on-board functions based on the subsets from ETCS Baseline 3 Release 2.

Note that the allocation of functions is hypothetical and not considered complete; however, for the scope of this analysis, it is considered reasonable in the absence of agreed architectures, interfaces, and respective specifications describing integration of on-board localisation in ETCS. The figures are not intended to illustrate physical architectures or interfaces; rather high-level functional blocks and information flows (with a focus on information output of the On-board Localisation (LOC-OB) and functions consuming the output information – indicated in red).

4.2.3.4 The functional architectures are as follows:

- *Type A – On-board localisation for virtual balise detection.* This architecture type is based on a generalisation of the X2Rail5 Stream 1 architecture.
- *Type B – On-board localisation for ETCS odometry and virtual balise detection.* This architecture type is based on a generalisation of the X2Rail5 Stream 2 architecture.
- *Type C – On-board localisation for train positioning, speed, acceleration and virtual ETCS transponder detection*. This is a generalisation of the OCORA release 3 logical architecture.

4.2.3.5 Assumptions:

a) It is assumed for all architecture types that the following functions are not allocated to On-board Localisation (LOC-OB):
   - Determination of train standstill (2.2.3); and
   - Determination of current on-board LRBG (2.3).

b) A virtual balise detection / Virtual ETCS Transponder Service (VETS) function is assumed for all architecture types; however, it is not considered part of the On-board Localisation (LOC-OB) as it is a consumer of information from the LOC-OB. The allocation of this function is outside the scope of the analysis and therefore designated to “Other” in Table 4-3.

c) The function of reporting the train position to the RBC remains allocated to the ETCS on-board (i.e., an ETCS kernel function).

d) Functions to check of odometer accuracy thresholds and storage of accumulated underestimation / overestimation in measuring the movements over a defined total distance are introduced in Baseline 4; however, these are not addressed in this preliminary analysis.

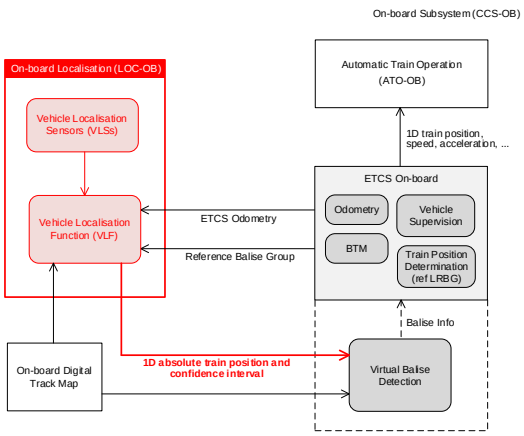
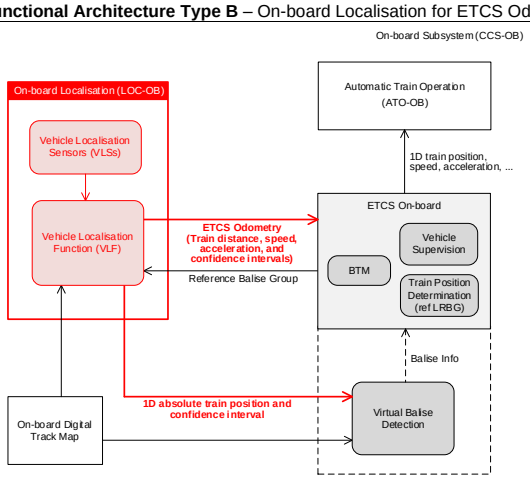
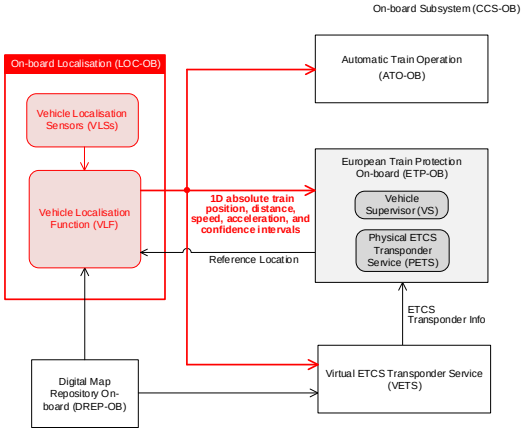
e) Hazardous events related to Cold Movement Detection (CMD) are introduced in Baseline 4. It is assumed for all architecture types that CMD is not a function of On-board Localisation (LOC-OB), although it could be a potential consumer of information from the LOC-OB.

f) On-board train integrity proving functions are outside the scope of this preliminary analysis. While this function could be a potential consumer of information from the LOC-OB, it is assumed that it is not a function of the LOC-OB.

g) Inputs to the On-board Localisation including digital track map, information provided by ETCS on-board / ETP-OB (e.g., reference balise group / reference location) are assumed to be fault-free.

h) Geographical position reporting function of ETCS (display of the geographical position of the estimated front end of the train in relation to the track kilometre) is not addressed in this preliminary analysis.

Table 4-3. Functional architectures, hypothetical allocation of on-board functions, and related ETCS FTA gates

	Hypothetical Allocation of On-board Functions		Related Fault Tree Gates	ETCS On-board / European Train Protection On-board (ETP-OB)	On-board Localisation (LOC-OB)	Other (see assumptions)
Functional Architecture Type A – On-board Localisation for Virtual Balise Detection						
	2	Determine train speed and position	Gate "CH33"			
	2.1.1	Determine train position referenced to LRBG	Gate 58	X		
	2.1.2	Determine distance travelled	Gate 147	X		
	2.1.3	Determine train orientation (cab status / TIU)	Event KER-15	X		
	2.1.4	Detection of cold movement	Event ODO-5	X		
	2.2.1	Determine train speed	Gate 48	X		
	2.2.2	Determine physical speed direction	Event ODO-3	X		
	2.2.3	Determine train standstill	Gate 61	X		
	2.3	Determine current on-board LRBG	Event KER-7	X		
	8	Other functions				
	8.X	Virtual Balise Detection / Virtual ETCS Transponder Detection	Gate 55			X
Functional Architecture Type B – On-board Localisation for ETCS Odometry and Virtual Balise Detection						
	2	Determine train speed and position	Gate "CH33"			
	2.1.1	Determine train position referenced to LRBG	Gate 58	X		
	2.1.2	Determine distance travelled	Gate 147		X	
	2.1.3	Determine train orientation (cab status / TIU)	Event KER-15	X		
	2.1.4	Detection of cold movement	Event ODO-5	X		
	2.2.1	Determine train speed	Gate 48		X	
	2.2.2	Determine physical speed direction	Event ODO-3		X	
	2.2.3	Determine train standstill	Gate 61	X		
	2.3	Determine current on-board LRBG	Event KER-7	X		
	8	Other functions				
	8.X	Virtual Balise Detection / Virtual ETCS Transponder Detection	Gate 55			X
Functional Architecture Type C – On-board Localisation for Train Positioning, Speed, Acceleration and Virtual ETCS Transponder Detection						
	2	Determine train speed and position	Gate "CH33"			
	2.1.1	Determine train position referenced to LRBG	Gate 58		X	
	2.1.2	Determine distance travelled	Gate 147		X	
	2.1.3	Determine train orientation (cab status / TIU)	Event KER-15		X	
	2.1.4	Detection of cold movement	Event ODO-5	X		
	2.2.1	Determine train speed	Gate 48		X	
	2.2.2	Determine physical speed direction	Event ODO-3		X	
	2.2.3	Determine train standstill	Gate 61	X		
	2.3	Determine current on-board LRBG	Event KER-7	X		
	8	Other functions				
	8.X	Virtual Balise Detection / Virtual ETCS Transponder Detection	Gate 55			X

4.2.3.6 Table 4-4 details the links between the identified LOC-OB hazards and hazardous events in the ETCS functional fault-tree analysis (FTA).

Table 4-4. On-board Localisation (LOC-OB) hazards and links to ETCS functional FTA

<table>
<tr><th>LOC-OB Function</th><th>LOC-OB Hazards</th><th>Link to ETCS Functional FTA</th></tr>
<tr><td>LOC-OB_FN-001: Provide safe train front end 1D position</td><td>LOC-OB_HAZ-001: Confidence interval does not include actual 1D position of train front end</td><td>
<table>
<tr><td>LOC-OB Output:</td><td>Safe train front end 1D position</td></tr>
<tr><td>Consumer:</td><td>ETCS On-board / European Train Protection On-board (ETP-OB)</td></tr>
<tr><td>Applicable Functional Architecture Types:</td><td>Type C</td></tr>
</table>
<table>
<tr><th>LOC-OB Hazard</th><th>Link to ETCS Functional FTA</th><th>Remarks</th></tr>
<tr><td>LOC-OB_HAZ-001</td><td>GATE58: Incorrect determination of train position ref to LRBG.</td><td></td></tr>
</table>
<table>
<tr><td>LOC-OB Output:</td><td>Safe train front end 1D position</td></tr>
<tr><td>Consumer:</td><td>Virtual Balise Detection / Virtual ETCS Transponder Service (VETS)</td></tr>
<tr><td>Applicable Functional Architecture Types:</td><td>Type A, B, C</td></tr>
</table>
<table>
<tr><th>LOC-OB Hazard</th><th>Link to ETCS Functional FTA</th><th>Remarks</th></tr>
<tr><td>LOC-OB_HAZ-001</td><td>GATE55: Wrong/No data transmitted to on-board from balise via the TRANS-BALISE-3 hazardous event at the Balise Transmission System (BTS) boundary</td><td>TRANS-BALISE-3 is caused by hazardous events of the BTM (BTM-H7, BTM-H8, BTM-H9) and Eurobalise (EUB-H7, EUB-H8, EUB-H9). Considering detection of a virtual balise / virtual ETCS transponder using train 1D position from the LOC-OB, H7, H8 and H9 are linked to LOC-OB_HAZ-001.</td></tr>
</table>
Definitions of H7, H8, H9:
H7: Erroneous localisation of a Balise Group, with reception of valid telegrams
H8: The order of reported Balises, with reception of valid telegrams
H9: Erroneous reporting of a Balise Group in a different track, with reception of valid telegrams
</td></tr>
<tr><td>LOC-OB_FN-002: Provide safe train speed</td><td>LOC-OB_HAZ-002: Train speed underestimates the actual speed of the train (speed confidence interval does not include actual speed of the train)
LOC-OB_HAZ-003: Incorrect actual physical speed direction</td><td>
<table>
<tr><td>LOC-OB Output:</td><td>Safe train speed</td></tr>
<tr><td>Consumer:</td><td>ETCS On-board / European Train Protection On-board (ETP-OB)</td></tr>
<tr><td>Applicable Functional Architecture Types:</td><td>Type B, C</td></tr>
</table>
<table>
<tr><th>LOC-OB Hazard</th><th>Link to ETCS Functional FTA</th><th>Remarks</th></tr>
<tr><td>LOC-OB_HAZ-002</td><td>GATE48: Train Speed underestimated.</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td>
<table>
<tr><td>LOC-OB_HAZ-003</td><td>ODO-3: Incorrect actual physical speed direction.</td><td></td></tr>
</table>
</td></tr>
<tr><td>LOC-OB_FN-003: Provide safe train acceleration</td><td>LOC-OB_HAZ-004: Acceleration confidence interval does not include the actual acceleration of the train</td><td>
<table>
<tr><td>LOC-OB Output:</td><td colspan="2">Safe train acceleration</td></tr>
<tr><td>Consumer:</td><td colspan="2">ETCS On-board / European Train Protection On-board (ETP-OB)</td></tr>
<tr><td>Applicable Functional Architecture Types:</td><td colspan="2">Type B, C</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>LOC-OB Hazard</td><td>Link to ETCS Functional FTA</td><td>Remarks</td></tr>
<tr><td>LOC-OB_HAZ-004</td><td>GATE22: Incorrect supervision of actual train speed.</td><td>The link to GATE22 assumes acceleration information is used in traction/braking model (KERNEL-25).</td></tr>
</table>
</td></tr>
<tr><td>LOC-OB_FN-004: Provide estimated distance travelled</td><td>LOC-OB_HAZ-005: Confidence interval of distance travelled does not include actual position of train front end</td><td>
<table>
<tr><td>LOC-OB Output:</td><td colspan="2">Estimated distance travelled</td></tr>
<tr><td>Consumer:</td><td colspan="2">ETCS On-board / European Train Protection On-board (ETP-OB)</td></tr>
<tr><td>Applicable Functional Architecture Types:</td><td colspan="2">Type B, C</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>LOC-OB Hazard</td><td>Link to ETCS Functional FTA</td><td>Remarks</td></tr>
<tr><td>LOC-OB_HAZ-005</td><td>GATE147: Incorrect determination of distance travelled.</td><td></td></tr>
<tr><td colspan="3">For functional architecture type B, the estimated distance travelled is used by ETCS On-board to determine train position referenced to LRBG (i.e., GATE147: Incorrect determination of distance travelled is a cause of GATE58: Incorrect determination of train position ref to LRBG).
For both functional architecture types B and C, estimated distance travelled (since power-on) is used by the ETCS on-board / ETP-OB for supervision of distances not referred to a balise group (e.g., monitoring allowed distance to run in SR mode).
GATE147: Incorrect determination of distance travelled is a cause of GATE14: Incorrect speed monitoring (supervision against unsafe speed), which addresses both speed and distance monitoring.</td></tr>
</table>
</td></tr>
</table>

4.2.4 Hazards at Boundary of GNSS Augmentation Processing of the Vehicle Localisation Function (VLF<GAP>)

4.2.4.1 The GNSS Augmentation Processing (GAP) functions considered in this analysis are detailed in Table 4-5. This refers to the boundary considering output from the GAP sub function of the VLF (refer to Figure 3-1).

Table 4-5. GNSS Augmentation Processing (GAP) functions

VLF<GAP> Function ID	Description
VLF<GAP>_FN-001	Provide SBAS corrected pseudoranges, SBAS corrected satellite locations, model variance for differential correction residual error and model variance for residual ionospheric error
VLF<GAP>_FN-002	Provide alert within end-to-end TTA when an alert condition occurs. An alert condition occurs when SBAS has erroneously broadcast integrity data not bounding the residual errors at the specified confidence level, for any valid combination of active data.

4.2.4.2 The hazards identified with respect to the above functions are detailed in Table 4-6.

Table 4-6. GNSS Augmentation Processing (GAP) hazards

VLF<GAP> Hazard ID	Description
VLF<GAP>_HAZ-001	Residual errors (clock, orbit, and ionosphere) are not bounded at the required level of confidence and no alert is given within the end-to-end TTA

4.2.4.3 Table 4-7 details the links between the identified GAP hazards of the VLF and On-board Localisation (LOC-OB) hazards.

Table 4-7. Vehicle Localisation Function (VLF) hazards and links to On-board Localisation (LOC-OB) hazards

<table>
<tr><th>VLF Function</th><th>VLF Hazards</th><th>Link to LOC-OB Hazards</th></tr>
<tr><td>VLF<GAP>_FN-001: Provide SBAS corrected pseudoranges, SBAS corrected satellite locations, model variance for differential correction residual error and model variance for residual ionospheric error</td><td>VLF<GAP>_HAZ-001: Residual errors (clock, orbit, and ionosphere) are not bounded at the required level of confidence and no alert given within the end-to-end TTA</td><td>
<table>
<tr><td>VLF Output:</td><td colspan="2">SBAS corrected pseudoranges, SBAS corrected satellite locations, model variance for differential correction residual error and model variance for residual ionospheric error</td></tr>
<tr><td>Consumer:</td><td colspan="2">On-board Localisation (LOC-OB)</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>VLF Hazard</td><td>Link to LOC-OB Hazards</td><td>Remarks</td></tr>
<tr><td rowspan="2">VLF<GAP>_HAZ-001</td><td>LOC-OB_HAZ-001: Confidence interval does not include actual 1D position of train front end</td><td>It is assumed that determination of a 1D position and confidence interval of the train front end utilises SBAS corrected pseudoranges and residual error variances in the VLF PVT engine. See Note 1.</td></tr>
<tr><td>LOC-OB_HAZ-002: Train speed underestimates the actual speed of the train (speed confidence interval does not include actual speed of the train)</td><td>It is assumed that determination of train speed utilises SBAS corrected pseudoranges and residual error variances in the VLF PVT engine. See Note 2.</td></tr>
</table>
</td></tr>
</table>

	LOC-OB_HAZ-004: Acceleration confidence interval does not include the actual acceleration of the train	It is assumed that determination of train acceleration utilises SBAS corrected pseudoranges and residual error variances in the VLF PVT engine. See Note 2.
	LOC-OB_HAZ-005: Confidence interval of distance travelled does not include actual position of train front end	It is assumed that determination of distance travelled and confidence interval utilises SBAS corrected pseudoranges and residual error variances in the VLF PVT engine. See Note 1.

Additional Remarks

It is assumed that GNSS is not used in providing the physical speed direction; therefore, the VLF<GAP>_HAZ-001 hazard does not contribute to *LOC-OB_HAZ-003: Incorrect actual physical speed direction*.

Notes

Note 1**:** To meet application-level performances, hybridisation of GNSS with sensors (rotational, inertial, etc.) will be necessary; however, the details of the hybridisation approach are left to the supplier. Therefore, a conservative assumption is made that this hazard will propagate to the On-board Localisation (LOC-OB) boundary with a probability of 1.

Note 2: If GNSS pseudoranges are used for determining train speed and confidence interval, it should be noted that SBAS currently does not provide commitments in the pseudorange-rate domain (this is being investigated in the scope of EGNOS Next). Therefore, it is assumed that Doppler bounds are computed by the PVT engine based on the SBAS pseudorange bounds (e.g., approach proposed in R&D activities such as CLUG and GREET).

4.2.5 Summary

4.2.5.1 Table 4-8 details how GNSS Augmentation Processing (GAP) hazards of the Vehicle Localisation Function (VLF) propagate to the ETCS Core Hazard via On-board Localisation (LOC-OB) considering the three architecture types analysed.

4.2.5.2 The FMEA in the Sections 6 and 7 identify the failure modes that can cause the hazard VLF<GAP>_HAZ-001.

Table 4-8. Summary of identified hazards and links to the ETCS Core Hazard

VLF Hazard	LOC-OB Hazard	Link to ETCS Functional FTA [Architecture Type]	ETCS System Hazard
VLF<GAP>_HAZ-001 Residual errors (clock, orbit, and ionosphere) are not bounded at the required level of confidence and no alert given within the end-to-end TTA	**LOC-OB_HAZ-001** Confidence interval does not include actual 1D position of train front end	**GATE58 [Type C]** Incorrect determination of train position ref to LRBG	**ETCS CORE HAZARD** Exceedance of the safe speed or distance as advised to ETCS
		GATE55 [Types A, B and C] Wrong/No data transmitted to on-board from balise	
	LOC-OB_HAZ-002 Train speed underestimates the actual speed of the train	**GATE48 [Types B and C]** Train Speed underestimated	
	LOC-OB_HAZ-004 Acceleration confidence interval does not include the actual acceleration of the train	**GATE22 [Types B and C]** Incorrect supervision of actual train speed	
	LOC-OB_HAZ-005 Confidence interval of distance travelled does not include actual position of train front end	**GATE147 [Types B and C]** Incorrect determination of distance travelled	

5 Hazard Analysis (Causal Analysis) Approach

5.1.1.1 The objective of this hazard analysis is to evaluate the possible failure modes of GNSS Augmentation (causes of the VLF<GAP>_HAZ-001 hazard) at the GNSS Augmentation Processing (GAP) boundary of the Vehicle Localisation Function (VLF).

5.1.1.2 An FMEA has been conducted to assess transmission channel and functional hazards based on the GA reference functional architecture. This section provides an overview of the approach taken including identification of macro function data items, basic functions of the GA reference functional architecture, assumptions, FMEA columns, guidewords used for the analysis and end effect hazard severity level.

5.2 Identification of Macro Function Data Items

5.2.1.1 The table below details the macro function data items in support of the transmission channel hazard analysis.

Macro Function	Interface [Direction]	Macro Function Data Items	Details / Remarks
[F1] Vehicle Localisation Sensor<GNSS Receiver>	F1:IN<GNSS> [GNSS → F1]	GNSS SIS	GPS L1, L5; Galileo E1-B/C, E5a
	F1:OUT<F2> [F1 → F2]	GNSS ID, SVID	
		Raw pseudorange measurements	
		Carrier phase measurements	
		C/N0 measurements	
		Loss of lock indicator	Indication of loss of lock, cycle slip, half-cycle ambiguity
		GNSS navigation data bits	Demodulated and FEC decoded GNSS navigation data bits
[F2] Vehicle Localisation Function<GNSS Augmentation Processing>	F2:IN<F1> [F1 → F2]	Refer to F1:OUT<F2>	
	F2:IN<F5> [F5 → F2]	Refer to F5:OUT<F2>	
	F2:OUT<F5> [F2 → F5]	Acknowledgement	[EUG-20E087, p14]
		Allocate GA Message Stream	[EUG-20E087, p15]
		Initiate GA Session	[EUG-20E087, p16]
		GA Active Data Request	[EUG-20E087, p17]
		GNSS Navigation Data Request	[EUG-20E087, p18]
		Resume GA Message Stream	[EUG-20E087, p19]
		Suspend GA Message Stream	[EUG-20E087, p20]
		Terminate GA Session	[EUG-20E087, p21]
	F2<GAP>:OUT<Internal> [F2 Internal]	SBAS corrected pseudoranges	Carrier smoothed pseudoranges (L1 or ionosphere-free combination L1/L5) with SBAS corrections (incl. SBAS ionospheric correction for L1 users) and tropospheric correction applied.
		SBAS corrected satellite locations	
		Model variance for differential correction residual error	Model variance for satellite clock and ephemeris errors (σ_{flt} for SBAS L1 and σ_{DFC} for SBAS DFMC)

Macro Function	Interface [Direction]	Macro Function Data Items	Details / Remarks
		Model variance for residual ionospheric error	Model variance for residual ionospheric error (σ_{UIRE}) after application of SBAS ionospheric correction for SBAS L1 users or for ionosphere-free dual frequency measurements for DFMC users
		Model variance for residual tropospheric error	Model variance for residual error, over bounding extremely rare tropospheric delays after application of tropospheric correction
		Model variance for ionospheric divergence errors	Model variance for residual ionospheric errors caused by the difference between the implemented smoothing filter and the reference smoothing filter given an ionospheric code-carrier divergence during the transient phase (i.e., before filter reaches steady-state) for L1 single frequency measurements smoothed with the time variant reference smoothing filter, applying SBAS L1 ionospheric corrections
[F3] Trackside Interface to SBAS / GNSS <GNSS Receiver>	F3:IN<SBAS/GNSS> [SBAS/GNSS → F3]	SBAS / GNSS SIS	SBAS L1; SBAS L5; GPS L1, L5; Galileo E1-B/C, E5a
	F3:OUT<F5> [F3 → F5]	SBAS PRN	
		SBAS message data bits	Demodulated and FEC decoded SBAS messages
		GNSS ID, SVID	
		Raw pseudorange measurements	
		Carrier phase measurements	
		C/N0 measurements	
		Loss of lock indicator	Indication of loss of lock, cycle slip, half-cycle ambiguity
		GNSS navigation data bits	Demodulated and FEC decoded GNSS navigation data bits
[F4] Trackside Interface to GAS<TBD> (future)			Intentionally Omitted
[F5] GNSS Augmentation Dissemination Function	F5:IN<F3>	Refer to F3:OUT<F5>	
	F5:IN<F2> [F2 → F5]	Refer to F2:OUT<F5>	
	F5:OUT<F2> [F5 → F2]	GA Active Data Set	[EUG-20E087, p22]
		GA Message	[EUG-20E087, p23]
		GA Message Stream Allocated / Resumed	[EUG-20E087, p24]
		GA Message Stream Suspended	[EUG-20E087, p25]
		GA Session Error	[EUG-20E087, p26]
		GA Session Established	[EUG-20E087, p27]
		GA Session Terminated	[EUG-20E087, p28]
		GNSS Navigation Data Set	[EUG-20E087, p29]

5.3 Identification of Basic Functions

5.3.1.1 The table below details the functional decomposition in support of the functional hazard analysis.

Macro Function	Sub Functions	Basic Functions	Details / Remarks
[F1] Vehicle Localisation Sensor<GNSS Receiver>	[F1.1] Process GNSS signal	[F1.1.1] GNSS pre-correlation signal processing	
		[F1.1.2] Acquisition and tracking of GNSS signals	
		[F1.1.3] GNSS navigation data demodulation, FEC decoding and frame synchronisation	
[F2] Vehicle Localisation Function<GNSS Augmentation Processing>	[F2.1] Process GNSS navigation data (received from GNSS receiver and GA-TS)	[F2.1.1] GNSS navigation data CRC / parity checks	
		[F2.1.2] Decoding navigation message parameters	
		[F2.1.3] Message consistency checks	Consistency of IODs (e.g., IODC/IODE), reference times, etc. as per MOPS
	[F2.2] Processing of GA messages received from GA-TS (including alert messages and GA messages with DNU GA message stream indication)	[F2.2.1] Timestamp GA messages received from GA-TS	Including determination of reference time (SNT)
		[F2.2.2] GA message content CRC checks	Check CRC of encapsulated SBAS message
		[F2.2.3] Process GA message content	Processing data from encapsulated SBAS MTs
	[F2.3] GNSS pseudorange determination and use	[F2.3.1] Carrier smoothing on pseudorange measurements	
		[F2.3.2] Measurement quality monitoring	Detection of cycle slips and other measurement faults
		[F2.3.3] Pseudorange determination	SBAS corrected pseudorange determination considering application of SBAS corrections (incl. SBAS ionospheric correction for L1 users) and tropospheric correction to carrier smoothed pseudorange
		[F2.3.4] GNSS satellite selection (use criteria)	Conditions for use as per MOPS (e.g., validity of correction and integrity data, satellite elevation mask, active UDREI < 14 or DFREI < 15 (also if incremented by DFRECI = 2))
	[F2.4] Compute and apply pseudorange error models (SBAS-provided integrity)[4]	[F2.4.1] Compute and apply model for differential correction residual error	Model variance for satellite clock and ephemeris errors (σ_{flt} for SBAS L1 and σ_{DFC} for SBAS DFMC)
		[F2.4.2] Compute and apply model for residual ionospheric error	Model variance for residual ionospheric error (σ_{UIRE}) after application of SBAS ionospheric correction for SBAS L1 users or for ionosphere-free dual frequency measurements for DFMC users
		[F2.4.3] Compute and apply model of tropospheric residual uncertainty	Model variance for residual error, over bounding extremely rare tropospheric delays after application of tropospheric correction

[4] Error models related to the receiver in the local environment including receiver errors (including receiver noise, thermal noise, interference, inter-channel biases, extrapolation, time since smoothing filter initialisation, and processing errors for smoothed pseudoranges), multipath and antenna group delay variation are not included as they are outside the boundary of the proposed Railway SoL pseudorange service commitments.

Macro Function	Sub Functions	Basic Functions	Details / Remarks
		[F2.4.4] Compute model of ionospheric divergence for SBAS L1 users	Model variance for residual ionospheric errors caused by the difference between the implemented smoothing filter and the reference smoothing filter given an ionospheric code-carrier divergence during the transient phase (i.e., before filter reaches steady-state) for L1 single frequency measurements smoothed with the time variant reference smoothing filter, applying SBAS L1 ionospheric corrections
	[F2.5] Supervise GA message content timeout	[F2.5]	Supervision of SBAS message content timeout
	[F2.6] Supervise and manage TTA	[F2.6]	
	[F2.7] Manage GA session	[F2.7]	
[F3] Trackside Interface to SBAS / GNSS<GNSS Receiver>	[F3.1] Process SBAS signal	[F3.1.1] Acquisition and tracking of SBAS signals	
		[F3.1.2] SBAS data demodulation, FEC decoding and frame synchronisation	
	[F3.2] Process GNSS signal	[F3.2.1] GNSS pre-correlation signal processing	
		[F3.2.2] Acquisition and tracking of GNSS signals	
		[F3.2.3] GNSS navigation data demodulation, FEC decoding and frame synchronisation	
[F4] Trackside Interface to GAS <TBD>			Intentionally omitted
[F5] GNSS Augmentation Dissemination Function	[F5.1] Select GACs	[F5.1]	GNSS augmentation channel selection
	[F5.2] Processing of SBAS messages for selected GACs (received from trackside interface to SBAS)	[F5.2.1] Timestamping reception of messages from SBAS	Including determination of reference time (SNT)
		[F5.2.2] SBAS message CRC checks	
		[F5.2.3] Encapsulation of SBAS messages in GAM packets	
		[F5.2.4] Process SBAS messages	Processing of SBAS MTs to support GA dissemination functions
	[F5.3] Provide GA message stream(s)	[F5.3.1] Allocate GA message stream	
		[F5.3.2] Suspend GA message stream	
		[F5.3.3] Resume GA message stream	
	[F5.4] Provide GA active data for selected GACs	[F5.4]	
	[F5.5] Provide GA active alerts for selected GACs	[F5.5]	
	[F5.6] Process GNSS navigation data (received from trackside interface to GNSS)	[F5.6.1] GNSS navigation data CRC / parity checks	
		[F5.6.2] Decoding navigation message parameters	
		[F5.6.3] Message consistency checks	E.g., consistency of IODs (IODC/IODE), reference times, etc. as per MOPS
	[F5.7] Provide GNSS navigation data sets	[F5.7]	
	[F5.8] Manage GA session	[F5.8]	

5.4 Assumptions

5.4.1.1 The following assumptions have been made in performing the functional FMEA:

- The external GNSS Augmentation System (GAS) considered in this analysis is SBAS/EGNOS. Safety analyses would need to be performed for other GAS if they are to be considered.
- EGNOS is considered fault-free (i.e., the FMEA does not cover hazards internal to EGNOS).
- Impact from the local environment on GNSS ranging by the VLF is outside the scope of the FMEA, which focuses only on GA-relevant failure modes.
- Unbounded errors in the pseudorange domain leads to unbounded errors in the position domain with a probability of 1.
- Cyber-attacks are identified but not developed further in this issue of the SFHA. The next issue will address cyber-security aspects of the system.
- Failures identified as leading to a RAM issue are not developed further.

5.4.1.2 Note: references to requirements [DMS:XX] made in the Internal Barriers column refer to requirements from the aviation DFMC MOPS [ED-259A]. The SBAS-OB-MOPS / SBAS-TS-MOPS for Railway SoL Service are expected to include these requirements.

5.5 FMEA Columns

5.5.1.1 The columns in the FMEA worksheet are described in the table below (adapted from [SS077]):

FMEA Column	Description
RefID	A unique reference is allocated to the failure mode for the purpose of traceability.
Macro Function Data Item	For each macro interface function, its inputs and outputs will be identified. These inputs and outputs are the macro function data items or basic functions, for which the failure modes are to be determined.
Failure Mode	For each macro function data item / basic function considered, the failure modes will be determined by examining the function and its stated requirements. Guidewords described in Sections 5.6 and 5.7 are used to aid in the identification of failure modes.
Failure Causes	For each failure mode, failure causes that relate to the cause of the failure will be identified.
Failure Effects – Local	These are effects of the failure on the function assuming no other failure is present. The consequences of the assumed failure on the function shall be described including any resulting second order effects. It is possible for the local effect to be the failure mode.
Failure Effects – Initial End Effect	Initial End Effect will define the total effect of the assumed single failure. Its evaluation does not take into consideration any mitigations or protections inherent within the reference architecture that may reduce the impact of failure or prevent it from occurring.
Severity	The severity of the initial end effect assigned based on severity level provided in Section 5.8.
Internal Barriers / Mitigation	Barriers of the reference architecture that are known to mitigate against the identified risk will be noted in this column along with identified mitigations (requirements).

5.6 Guidewords for Data Transmission

5.6.1.1 Guidewords used for message level failure modes are detailed in the table below [SS077]:

Guideword	Definition
Corruption	Type of message error in which data corruption occurs (alteration of data)
Deletion	Type of message error in which a message is removed from the message stream
Delay	Type of message error in which message is received at a later time than intended
Repetition	Type of message error in which message is received also at a later time than intended
Insertion	Type of message error in which an additional message is implanted in the message stream
Re-sequence	Type of message error in which the order of the messages in the message steam is changed
Masquerade	Type of inserted message in which a non-authentic message is designed to appear authentic

5.7 Guidewords for Functional Failure Modes

5.7.1.1 Guidewords used for functional failure modes:

Guideword	Definition
As well as	Function executes when it should not
No or Not	Function does not execute when it should
Early	Function executes earlier than it should
Late	Function executes later than it should
Partial	Function only partially executes
Erroneous	Function executes in an incorrect way

5.8 End Effect / Hazard Severity Level

5.8.1.1 The severity levels detailed in the table below are used in the FMEA:

Severity Level	Consequence
Catastrophic	Incapacitation of driver; potential for multiple fatalities
Critical	Large reduction in functional capabilities or safety margins; excessive workload (driver / traffic controller) impairs ability to perform tasks; potential for serious or fatal injury
Marginal	Significant reduction in functional capabilities or safety margins; significant increase in workload (driver / traffic controller)
Insignificant	Slight reduction in functional capabilities or safety margins; slight increase in workload (driver / traffic controller) / use of operational procedures for degraded operating or emergency
RAM Issue	Service impact, not safety related
No effect	None

6 Transmission Channel Hazard Analysis – FMEA

6.1 GNSS SIS to GA-OB Transmission Channel

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
6.1.1.1	GNSS SIS	**Corruption** Reception of navigation data with corruption	• Interference environment (degraded C/N0, increased BER) • Erroneous frame sync • GNSS receiver HW/SW fault	• Erroneous navigation data • Erroneous reference time (SNT)	VLF<GAP>_HAZ-001	Critical	Internal barriers: • Corruption in GPS LNAV detected by 6-bit parity for each 24-bit word. LNAV subframes have an 8-bit preamble for frame sync. To ensure residual risk of undetected corruption is acceptable for GPS LNAV, the GA-OB shall comply with [DMS:249] • Corruption in GPS CNAV detected by 24-bit CRC in each message. 8-bit preamble provided in each CNAV for sync to message boundary • Corruption in GAL I/NAV detected by 24-bit CRC in each page. 10-bit sync pattern provided in each page for sync to page boundary • Corruption in GAL F/NAV detected by 24-bit CRC in each word. 12-bit sync pattern in each F/NAV page for sync to page boundary Requirements: • [SR_GNSS-GA-OB_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
6.1.1.2	GNSS SIS	**Deletion** Unable to acquire / track GNSS signals	• Radiofrequency interference • Cyber-attack (intentional jamming) • GNSS receiver HW/SW fault	• Degraded C/N0, below acquisition and tracking thresholds	GNSS measurements unavailable	RAM Issue	
6.1.1.3	GNSS SIS	**Delay / Repetition** Delayed, or record & replayed GNSS signals	• Cyber-attack targeting GNSS signals (e.g., GNSS meaconing, reradiation, record & replay) • GNSS receiver HW/SW fault	• Erroneous GNSS measurements (code and carrier phase) • Erroneous reference time (SNT)	VLF<GAP>_HAZ-001	Critical	Exported conditions: • [SC_GNSS-GA-OB_1] Detection of cyber-attacks targeting GNSS signals at the GA-OB is outside the scope of GA for ERTMS/ETCS. Implementation of barriers against spoofing threats would be needed. Requirements: • [SR_GNSS-GA-OB_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
6.1.1.4	GNSS SIS	**Insertion / Masquerade** Acquisition and tracking of non-authentic GNSS signals	• Cyber-attack targeting GNSS signals (e.g., GNSS spoofing, meaconing, reradiation, record & replay)	• Erroneous GNSS measurements (code and carrier phase) • Erroneous navigation data bits • Erroneous reference time (SNT)	VLF<GAP>_HAZ-001	Critical	Exported conditions: • [SC_GNSS-GA-OB_1] Detection of cyber-attacks targeting GNSS signals at the GA-OB is outside the scope of GA for ERTMS/ETCS. Implementation of barriers against spoofing threats would be needed.

6.2 GA-OB to GA-TS Transmission Channel

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
6.2.1.1	GA Messages exchanged between GA-ON and GA-TS	**Corruption** Reception of GA messages with corruption	• Interference environment (degraded SNR, increased BER) • GA-OB HW/SW fault (safety-related transmission function) • GA-TS HW/SW fault (safety-related transmission function)	• Erroneous GA alerts • Erroneous GA active data (timestamps, SBAS message content) • Erroneous GA message (timestamp, SBAS message content) • Erroneous GNSS navigation data • Missed GA alerts • Erroneous acknowledgement • Erroneous national values (GA service assumptions) • Erroneous reference time (SNT)	VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_GA-OB-GA-TS_1] Safe radio channel for exchange of GA messages between GA-OB and GA-TS shall comply with EN 50159 implementing CRC for detection of message corruption • [SR_GA-OB-GA-TS_2] For GA-OB safety-related transmission function, the HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance) • [SR_GA-OB-GA-TS_3] For GA-TS safety-related transmission function, the HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
6.2.1.2	GA Messages exchanged between GA-ON and GA-TS	**Deletion** Deletion of GA messages	• Radiofrequency interference • GA-OB HW/SW fault (safety-related transmission function) • GA-TS HW/SW fault (safety-related transmission function) • Cyber-attack targeting safe radio channel between GA-OB and GA-TS	• Missed GA alerts • Timeout of SBAS message content	VLF<GAP>_HAZ-001	Critical	Internal barriers: • SBAS broadcasts a valid message every second to provide a continuity of signal • Acknowledgement and retry mechanism for critical GA messages (i.e., those containing alerts) [EUG-20E085] Requirements: • [SR_GA-OB-GA-TS_4] Safe radio channel for exchange of GA messages between GA-OB and GA-TS shall comply with EN 50159 implementing sequence numbers for detection of deleted GA messages • [SR_GA-OB-GA-TS_2] For GA-OB safety-related transmission function, the HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance) • [SR_GA-OB-GA-TS_3] For GA-TS safety-related transmission function, the HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
6.2.1.3	GA Messages exchanged between GA-ON and GA-TS	**Delay** Delayed GA messages	• GA-OB HW/SW fault (safety-related transmission function) • GA-TS HW/SW fault (safety-related transmission function) • Cyber-attack targeting safe radio channel between GA-OB and GA-TS	• Delayed GA alerts • Timeout of SBAS message content	VLF<GAP>_HAZ-001	Critical	Internal barriers: • Timestamp of reception of SBAS messages by GA-TS and timestamp of reception of GA messages (encapsulating SBAS messages) by GA-OB, facilitating detection of delayed GA messages Requirements: • [SR_GA-OB-GA-TS_2] For GA-OB safety-related transmission function, the HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance) • [SR_GA-OB-GA-TS_3] For GA-TS safety-related transmission function, the HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
6.2.1.4	GA Messages exchanged between GA-ON and GA-TS	**Repetition / Re-sequence** Repeated or re-sequenced GA messages	• GA-OB HW/SW fault (safety-related transmission function) • GA-TS HW/SW fault (safety-related transmission function) • Cyber-attack targeting safe radio channel between GA-OB and GA-TS	• Missed GA alerts • Timeout of SBAS message content	VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_GA-OB-GA-TS_4] Safe radio channel for exchange of GA messages between GA-OB and GA-TS shall comply with EN 50159 implementing sequence numbers for detection of deleted GA messages • [SR_GA-OB-GA-TS_2] For GA-OB safety-related transmission function, the HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance) • [SR_GA-OB-GA-TS_3] For GA-TS safety-related transmission function, the HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
6.2.1.5	GA Messages exchanged between GA-ON and GA-TS	**Insertion / Masquerade**	• GA-OB HW/SW fault (safety-related transmission function) • GA-TS HW/SW fault (safety-related transmission function) • Cyber-attack targeting safe radio channel between GA-OB and GA-TS	• Erroneous GA alerts • Erroneous GA active data (timestamps, SBAS message content) • Erroneous GA message (timestamp, SBAS message content) • Erroneous GNSS navigation data • Missed GA alerts • Erroneous acknowledgement • Erroneous national values (GA service assumptions) • Erroneous reference time (SNT)	VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_GA-OB-GA-TS_4] Safe radio channel for exchange of GA messages between GA-OB and GA-TS shall comply with EN 50159 implementing sequence numbers for detection of deleted GA messages • [SR_GA-OB-TS_5] Safe radio channel for exchange of GA messages between GA-OB and GA-TS shall comply with EN 50159 implementing cryptographic techniques to detect masqueraded GA messages (authentication and cryptographic message integrity) • [SR_GA-OB-GA-TS_2] For GA-OB safety-related transmission function, the HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance) • [SR_GA-OB-GA-TS_3] For GA-TS safety-related transmission function, the HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

6.3 GNSS SIS to GA-TS Transmission Channel

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
6.3.1.1	GNSS SIS	**Corruption** Reception of navigation data with corruption	• Interference environment (degraded C/N0, increased BER) • Erroneous frame sync • GNSS receiver HW/SW fault	• Erroneous navigation data • Erroneous reference time (SNT)	Erroneous navigation data provided to GA-OB; erroneous timestamping of GA messages; VLF<GAP>_HAZ-001	Critical	Internal barriers: • Corruption in GPS LNAV detected by 6-bit parity for each 24-bit word. LNAV subframes have an 8-bit preamble for frame sync. To ensure residual risk of undetected corruption is acceptable for GPS LNAV, the GA-OB shall comply with [DMS:249] • Corruption in GPS CNAV detected by 24-bit CRC in each message. 8-bit preamble provided in each CNAV for sync to message boundary • Corruption in GAL I/NAV detected by 24-bit CRC in each page. 10-bit sync pattern provided in each page for sync to page boundary • Corruption in GAL F/NAV detected by 24-bit CRC in each word. 12-bit sync pattern in each F/NAV page for sync to page boundary Requirements: • [SR_GNSS-GA-TS_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
6.3.1.2	GNSS SIS	**Deletion** Unable to acquire / track GNSS signals	• Radiofrequency interference • Cyber-attack (intentional jamming) • GNSS receiver HW/SW fault	• Degraded C/N0, below acquisition and tracking thresholds • GNSS measurements unavailable	Unavailability of navigation data; unavailability of SNT for timestamping	RAM Issue	

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
6.3.1.3	GNSS SIS	**Delay / Repetition** Delayed, or record & replayed GNSS signals	• Cyber-attack targeting GNSS signals (e.g., GNSS meaconing, reradiation, record & replay) • GNSS receiver HW/SW fault	• Erroneous GNSS measurements (code and carrier phase) • Erroneous reference time (SNT)	Erroneous timestamping of GA messages; VLF<GAP>_HAZ-001	Critical	Requirements: • [SR-GNSS-GA-TS_2] Barriers against cyber-attacks resulting in delayed / replayed GNSS signals shall be implemented. • [SR_GNSS-GA-TS_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
6.3.1.4	GNSS SIS	**Insertion / Masquerade** Acquisition and tracking of non-authentic GNSS signals	• Cyber-attack targeting GNSS signals (e.g., GNSS spoofing, meaconing, reradiation, record & replay)	• Erroneous GNSS measurements (code and carrier phase) • Erroneous navigation data bits • Erroneous reference time (SNT)	Erroneous navigation data provided to GA-OB; erroneous timestamping of GA messages; VLF<GAP>_HAZ-001	Critical	Requirements: • [SR-GNSS-GA-TS_2] Barriers against cyber-attacks resulting in spoofed GNSS signals shall be implemented.

6.4 SBAS SIS to GA-TS Transmission Channel

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
6.4.1.1	SBAS SIS	**Corruption** Reception of SBAS messages with corruption	• Interference environment (degraded C/N0, increased BER) • Erroneous frame sync • GNSS receiver HW/SW fault	• Erroneous SBAS messages	Erroneous SBAS messages provided to GA-OB; VLF<GAP>_HAZ-001	Critical	Internal barriers: • Corruption in SBAS L1 detected by 24-bit CRC for each SBAS message. Frame synch provided by correlation with 24-bit preamble (distributed over 3 successive 8-bit blocks) • Corruption in SBAS L5 detected by 24-bit CRC for each SBAS message. Frame sync provided by correlation with 24-bit preamble (distributed over 6 successive 4-bit blocks) Requirements: • [SR_SBAS-GA-TS_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
6.4.1.2	SBAS SIS	**Deletion** Deletion of SBAS messages	• Radiofrequency interference (C/N0 degraded below demodulation threshold) • Cyber-attack (intentional jamming) • GNSS receiver HW/SW fault	• One or more SBAS messages not received • Missed alert	Alert not provided to GA-OB; VLF<GAP>_HAZ-001	Critical	Internal barriers: • SBAS broadcasts a valid message every second to provide a continuity of signal • Communication link failure is indicated for SBAS L1 or SBAS L5 when no valid SBAS message has been received for 4 seconds [DMS:299, DMS:113]. Communication link failure is considered a very low occurrence event assuming reliable reception of SBAS messages at the trackside. • In the case of communication link failure, the GA-TS shall send a GA Message with GA message type Q_GAMT = 2 (DNU GA message stream) to the GA-OB, requiring acknowledgement, indicating that the GA-OB shall no longer use the GA message stream Requirements: • [SR_SBAS-GA-TS_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
6.4.1.3	SBAS SIS	**Delay / Repetition** Delayed, or record & replayed SBAS signals	• Cyber-attack targeting GNSS signals (e.g., GNSS meaconing, reradiation, record & replay) • GNSS receiver HW/SW fault	• Delayed SBAS messages • Delayed alert / missed alert • Erroneous SBAS message content • Undetected timeout of SBAS message content	Delayed / erroneous SBAS messages provided to GA-OB; erroneous SBAS message content timeout; violation of T_NVGAMAXTTA; VLF<GAP>_HAZ-001	Critical	Internal barriers: • For SBAS L5, the equipment shall drop (stop tracking) an SBAS L5 signal and discard all previously received data from that signal when the GNSS second of week is determined and an SBAS message is received that passes CRC but whose 4 second preamble block does not match the expected block corresponding to the GNSS second of the week [DMS:235] • If a cyber-attack is detected, the GA-TS shall send a GA Message with GA message type Q_GAMT = 2 (DNU GA message stream) to the GA-OB, requiring acknowledgement, indicating that the GA-OB shall no longer use the GA message stream Requirements: • [SR-SBAS-GA-TS_2] Barriers against cyber-attacks resulting in delayed / replayed SBAS signals shall be implemented. • [SR_SBAS-GA-TS_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
6.4.1.4	SBAS SIS	**Insertion / Masquerade** Acquisition and tracking of non-authentic SBAS signals	• Cyber-attack targeting GNSS signals (e.g., GNSS spoofing, meaconing, reradiation, record & replay)	• Erroneous SBAS messages	Erroneous SBAS messages provided to GA-OB; VLF<GAP>_HAZ-001	Critical	Requirements: • [SR-SBAS-GA-TS_3] Barriers against cyber-attacks resulting in spoofed SBAS signals shall be implemented.

7 Functional Hazard Analysis – FMEA

7.1 F1: Vehicle Localisation Sensor<GNSS Receiver>

Ref ID	Basic Function	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.1.1.1	[F1.1.1] GNSS pre-correlation signal processing	**Erroneous** Pre-correlation bandwidth not within permitted range; differential group delay exceeds allowed maximum; pre-correlation filter not compliant with requirements on roll-off or central frequency	• Non-compliance with receiver design constraints [DMS:052]	• SBAS does not protect user from impact of signal distortions / EWF feared events • Impact on receiver measurements (error in corrected smoothed pseudorange) exceeds that of a compliant receiver	VLF<GAP>_HAZ-001	Critical	Internal barriers: • Compliance with [DMS:052] Exported conditions: • [SC_F1_1] If not compliant with [DMS:052], SBAS does not protect user against EWF feared events. Implementation of barrier against EWF feared events in on-board receiver perimeter would therefore be required.
7.1.1.2	[F1.1.2] Acquisition and tracking of GNSS signals	**No or Not** GNSS signals not acquired or tracked	• GNSS receiver HW/SW fault	• GNSS measurements unavailable	GNSS measurements unavailable	RAM Issue	
7.1.1.3	[F1.1.2] Acquisition and tracking of GNSS signals	**Erroneous** Use of incorrect signals for code and carrier phase measurements	• Non-compliance with [DMS:237] and [DMS:238] • Use of GPS signals other than L1 C/A- code and L5-Q5 signals for code and carrier phase measurements • Use of GAL signals other than E1-C and E5a-Q signals for code and carrier phase measurements, E1-C signals being processed with BOC(1,1) replicas only, and E5a- Q signals, with BPSK(10) replicas only	• Performances of measurements made using other signals not committable by SBAS	VLF<GAP>_HAZ-001	Critical	Internal barriers: • Compliance with [DMS:237] for GPS • Compliance with [DMS:238] for GAL

Ref ID	Basic Function	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.1.1.4	[F1.1.2] Acquisition and tracking of GNSS signals	**Erroneous** Use of incompatible tracking loop	• Non-compliance with constraints on tracking loop implementation [DMS:155] and [DMS:239]	• SBAS does not protect user from impact of signal distortions / EWF feared events • Impact on receiver measurements (error in corrected smoothed pseudorange) exceeds that of a compliant receiver	VLF<GAP>_HAZ-001	Critical	Internal barriers: • Compliance with [DMS:155] for GPS code tracking loops • Compliance with [DMS:239] for GAL code tracking loops Exported conditions: • [SC_F1_2] If not compliant with [DMS:155] and [DMS:239], SBAS does not protect user against EWF feared events. Implementation of barrier against EWF feared events in on-board receiver perimeter would therefore be required.
7.1.1.5	[F1.1.2] Acquisition and tracking of GNSS signals	**Erroneous** Mistaking one GPS L1 C/A code signal with another; one GPS L5 signal with another; one GAL E1 signal with another; or one GAL E5a signal with another	• Cross-correlation effects during acquisition or reacquisition	• GPS L1 C/A ranging data does not correspond to PRN code number used for signal tracking • GPS L5 ranging data does not correspond to PRN code number used for signal tracking • Galileo E1 ranging data does not correspond to primary code number used for signal tracking • Galileo E5a ranging data does not correspond to primary code number used for signal tracking	VLF<GAP>_HAZ-001	Critical	Internal barriers: • Compliance with [DMS:247] and [DMS:770] for GPS L1 C/A • Compliance with [DMS:015] and [DMS:777] for GPS L5 • Compliance with [DMS:023] and [DMS:778] for GAL E1 • Compliance with [DMS:024] and [DMS:779] for GAL E5a

Ref ID	Basic Function	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.1.1.6	[F1.1.2] Acquisition and tracking of GNSS signals	**Erroneous** Overshoot exceeds theoretical bias error (ionosphere-free pseudorange)	• Simultaneous code step errors on L1/E1 and L5/E5a signals with the same magnitude of up to 10 meters but opposite signs	• Smoothed ionosphere-free pseudorange error exceed theoretical bias error	VLF<GAP>_HAZ-001	Critical	Internal barriers: • Compliance by use of first-order code tracking loops (no overshoot) Exported conditions: • [SC_F1_3] If use of first-order tracking loops is not guaranteed, an analysis is required to demonstrate that the overshoot does not exceed a specified threshold (TBC) or to support bounding of the overshoot following the occurrence of the code step errors.
7.1.1.7	[F1.1.2] Acquisition and tracking of GNSS signals	**Erroneous / Early / Late / Partial** Erroneous acquisition or tracking of GNSS signals	• GNSS receiver HW/SW fault	• Erroneous GNSS measurements (GNSS ID, SVID, code and carrier phase measurements, C/N0, LLI)	VLF<GAP>_HAZ-001	Critical	Requirements • [SR_F1_1] GNSS receiver HW and SW / firmware shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.1.1.8	[F1.1.2] Acquisition and tracking of GNSS signals	**Erroneous** Acquisition and tracking of signals with interference exceeding nominal interference environment	• Radiofrequency interference • Cyber-attack (intentional jamming)	• Degraded C/N0, increased pseudorange noise	Standard deviation of distribution that bounds errors in the tails associated with GNSS receiver (*including receiver noise, thermal noise, interference, inter-channel biases, extrapolation, time since smoothing filter initialisation and processing errors*) may not bound the respective pseudorange errors at the required level of confidence	Critical	Exported conditions: • [SC_F1_4] Bounding of pseudorange errors related to the GNSS receiver including interference is outside scope of GA for ERTMS/ETCS but shall be addressed in the on-board receiver perimeter. If RF interference exceeds the nominal interference environment (TBC), the GNSS receiver shall guarantee the increased pseudorange errors due to the RF interference are bound (i.e., no increase in risk of misleading information). Impact on availability / continuity is expected.

Ref ID	Basic Function	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.1.1.9	[F1.1.3] GNSS navigation data demodulation, FEC decoding and frame synchronisation	**Erroneous** Erroneous navigation data demodulation, FEC decoding and frame synchronisation	• High BER • GNSS receiver HW/SW fault	• Erroneous navigation data	VLF<GAP>_HAZ-001	Critical	Internal barriers: • Errors in navigation data detected by CRC / parity checks

7.2 F2: Vehicle Localisation Function<GNSS Augmentation Processing>

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.2.1.1	[F2.1.1] GNSS navigation data CRC / parity checks	**Erroneous** Erroneous GNSS navigation data CRC / parity check	• GA-OB HW/SW fault	• Undetected navigation message corruption • Erroneous navigation data	VLF<GAP>_HAZ-001	Critical	Requirements • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.2	[F2.1.2] Decoding navigation message parameters	**Erroneous** Erroneous decoding of navigation message parameters	• GA-OB HW/SW fault	• Erroneous navigation data	VLF<GAP>_HAZ-001	Critical	Requirements • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.3	[F2.1.3] Message consistency checks	**Erroneous** Erroneous message consistency checks (e.g., consistency of IODs, reference times, etc.)	• GA-OB HW/SW fault	• Inconsistent navigation data is used (e.g., navigation message parameters with the wrong IOD)	VLF<GAP>_HAZ-001	Critical	Requirements • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.4	[F2.2.1] Timestamp GA messages received from GA-TS	**No or Not** Reception of GA message from GA-TS not timestamped	• GA-OB HW/SW fault • Reference time (SNT) unavailable	• SBAS message content timeout supervision unavailable; • TTA supervision unavailable	GNSS channel unavailable; no pseudoranges available for use by VLF	RAM Issue	
7.2.1.5	[F2.2.1] Timestamp GA messages received from GA-TS	**Erroneous / Late** Erroneous or late timestamping of GA message received from GA-TS	• GA-OB HW/SW fault • Erroneous time reference (SNT)	• Incorrect supervision of SBAS message content timeouts • Incorrect supervision of TTA	VLF<GAP>_HAZ-001	Critical	Requirements • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.2.1.6	[F2.2.1] Timestamp GA messages received from GA-TS	**Early** GA message received from GA-TS timestamped with earlier timestamp	• GA-OB HW/SW fault • Erroneous time reference (SNT)	• SBAS message content times out early • Pseudoranges become unavailable or degradation parameters applied	Impact on bounding of errors (larger due to degradation parameters) or fewer pseudoranges available for use by VLF	RAM Issue	
7.2.1.7	[F2.2.2] GA message content CRC checks	**Erroneous** Erroneous verification of CRC of GA message content (encapsulated SBAS message CRC)	• GA-OB HW/SW fault	• Erroneous SBAS message	VLF<GAP>_HAZ-001	Critical	Requirements • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.8	[F2.2.3] Process GA message content	**Erroneous** Erroneous processing of GA message content (SBAS message)	• GA-OB HW/SW fault	• Erroneous SBAS message content / parameters	VLF<GAP>_HAZ-001	Critical	Requirements • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.9	[F2.3.1] Carrier smoothing on pseudorange measurements	**Erroneous** Erroneous carrier smoothing on pseudorange measurements	• GA-OB HW/SW fault • Undetected cycle slip (MQM) • Smoothing filter does not comply with [DMS:322] or [DMS:156]	• Unbounded error in smoothed pseudorange • Feared event propagates into user measurements faster due to use of a smoothing filter with a faster response than filter defined in [DMS:322] or [DMS:156] (i.e., weighting function time constant < 100s) • For SBAS L1 users, broadcast GIVE does not guarantee bounding of error due to ionospheric divergence with a	VLF<GAP>_HAZ-001	Critical	Internal barriers: • Compliance with [DMS:322] for SBAS L1 provided integrity monitoring • Compliance with [DMS:156] for SBAS L5 provided integrity monitoring Exported conditions: • [SC_F2_1] If not compliant with [DMS:322] and [DMS:156], additional barriers may need to be defined in the receiver to address the faster response of the smoothing filter with a shorter weighting function time constant. In addition, the impact of a shorter weighting function time constant needs

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
				smoothing filter weighting function time constant greater than reference filter [DMS:322] (> 100 s)			to be considered in the bounding of pseudorange errors related to receiver noise, multipath, and for single frequency users, the difference between the implemented smoothing filter and the reference smoothing filter given an ionospheric code-carrier divergence. Requirements • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.10	[F2.3.2] Measurement quality monitoring	**Erroneous** Erroneous measurement quality monitoring	• GA-OB HW/SW fault • Excessive interference	• Undetected cycle slip or other undetected measurement fault • Impact on smoothed pseudorange	VLF<GAP>_HAZ-001	Critical	Requirements • [SR_F2_2] Signal tracking quality shall be monitored such that the allocated integrity risk due to undetected cycle slip or other undetected measurement fault is within the manufacturer's allocation [DMS:323] • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.11	[F2.3.3] Pseudorange determination	**Erroneous** Erroneous pseudorange determination	• GA-OB HW/SW fault • Erroneous application of SBAS corrections (incl. SBAS ionospheric correction for L1 users) and tropospheric correction to carrier smoothed pseudorange	• Unbounded error in smoothed pseudorange	VLF<GAP>_HAZ-001	Critical	Requirements • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.2.1.12	[F2.3.4] GNSS satellite selection (use criteria)	**No or Not / Partial** Valid GNSS satellites not selected	• GA-OB HW/SW fault	• Fewer satellites available	Impact on number of pseudoranges that can be used by VLF	RAM Issue	
7.2.1.13	[F2.3.4] GNSS satellite selection (use criteria)	**Erroneous** Erroneous selection of GNSS satellites	• GA-OB HW/SW fault	• Selection of satellites that do not meet the use criteria (TBC) (e.g., validity of correction and integrity data, satellite elevation mask, active UDREI < 14 or DFREI < 15 (also if incremented by DFRECI = 2))	VLF<GAP>_HAZ-001	Critical	Requirements • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.14	[F2.4.1] Compute and apply model for differential correction residual error	**Erroneous** Erroneous computation and application of model for differential correction residual	• GA-OB HW/SW fault • Erroneous model parameters (model variance for satellite clock and ephemeris errors (σ_{flt} for SBAS L1 and σ_{DFC} for SBAS DFMC))	• Unbounded error in smoothed pseudorange	VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.15	[F2.4.2] Compute and apply model for residual ionospheric error	**Erroneous** Erroneous computation and application of model for residual ionospheric error	• GA-OB HW/SW fault • Erroneous model parameters (model variance for residual ionospheric error (σ_{UIRE}) after application of SBAS ionospheric correction for SBAS L1 users or for ionosphere-free dual frequency measurements for DFMC users)	• Unbounded error in smoothed pseudorange	VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.16	[F2.4.3] Compute and apply model of tropospheric residual uncertainty	**Erroneous** Erroneous computation and application of model of tropospheric uncertainty	• GA-OB HW/SW fault • Erroneous model parameters (model variance for residual error does not over-bound extremely rare	• Unbounded error in smoothed pseudorange	VLF<GAP>_HAZ-001	Critical	Exported conditions: • [SC_F2_2] Tropospheric model needs to be validated for railway Requirements:

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
			tropospheric delays after application of tropospheric correction)				• [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.17	[F2.4.4] Compute model of ionospheric divergence for SBAS L1 users	**Erroneous** Erroneous computation of model of ionospheric divergence for SBAS L1 user	• GA-OB HW/SW fault • Erroneous model parameters (model variance for residual ionospheric errors caused by the difference between the implemented smoothing filter and the reference smoothing filter given an ionospheric code-carrier divergence during the transient phase (i.e., before filter reaches steady-state) for L1 single frequency measurements smoothed with the time variant reference smoothing filter, applying SBAS L1 ionospheric corrections)	• Unbounded error in smoothed pseudorange	VLF<GAP>_HAZ-001	Critical	Exported conditions: • [SC_F2_3] The value of σ_{divg} for SBAS L1 users needs to be set accounting for the difference between the implemented smoothing filter and the reference smoothing filter for a given ionospheric divergence – i.e., during the transient phase if the implemented smoothing filter is the filter defined in [DMS:322]. For this filter, $\sigma_{divg} = 0$ after steady state is reached. Requirements: • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.18	[F2.5] Supervise GA message content timeout	**Erroneous / Late / No or Not** Erroneous, late or no timeout SBAS message content	• GA-OB HW/SW fault • Erroneous timestamp in GA message • Incorrect time reference (SNT)	• Use of SBAS message content that has timed out • Unbounded error in smoothed pseudoranges	VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.2.1.19	[F2.5] Supervise GA message content timeout	**Early** Early timeout of SBAS message content	• GA-OB HW/SW fault • Erroneous timestamp in GA message • Incorrect time reference (SNT)	• SBAS message content times out early • Pseudoranges become unavailable or degradation parameters applied	Impact on bounding of errors (larger due to degradation parameters) or fewer pseudoranges available for use by VLF	RAM Issue	
7.2.1.20	[F2.6] Supervise and manage TTA	**Erroneous / Late /** Supervision function transitions GNSS channel into a safe state erroneously or later than it should	• GA-OB HW/SW fault • Erroneous timestamp of reception of GA message from GA-TS • Erroneous timestamp in GA message (reception from SBAS SIS) • Incorrect time reference (SNT) GA-OB or GA-TS	• Unbounded errors	VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.2.1.21	[F2.6] Supervise and manage TTA	**Early** Supervision function transitions GNSS channel to safe state earlier than it should	• GA-OB HW/SW fault • Erroneous timestamp of reception of GA message from GA-TS • Erroneous timestamp in GA message (reception from SBAS SIS) • Incorrect time reference (SNT) GA-OB or GA-TS	• GNSS channel becomes unavailable	Availability impact on pseudoranges available for use by VLF	RAM Issue	
7.2.1.22	[F2.7] Manage GA session	**Erroneous** Erroneous acknowledgement	• GA-OB HW/SW fault	• Missed alert	VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F2_1] GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

7.3 F3: Trackside Interface to SBAS/GNSS<GNSS Receiver>

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.3.1.1	[F3.1.1] Acquisition and tracking of SBAS signals	**No or Not** SBAS signals not acquired or tracked	• GNSS receiver HW/SW fault	• SBAS messages unavailable	SBAS messages unavailable	RAM Issue	
7.3.1.2	[F3.1.1] Acquisition and tracking of SBAS signals	**Erroneous** Mistaking one SBAS L1 signal with another; one SBAS L5 signal with another	• Cross-correlation effects during acquisition or reacquisition	• SBAS correction and integrity data does not correspond to PRN code number used for signal tracking (wrong PRN); incorrect message stream provided for PRN. • Unsupported / unauthorised SBAS provider erroneously used (i.e., not providing railway SoL service, commitments on pseudorange domain integrity)	Provision of SBAS corrections from the wrong SBAS signal to GA-OB; VLF<GAP>_HAZ-001	Critical	Internal barriers: • For SBAS L1, service provider ID verified by MT27 ensuring authorised service provider is used • For SBAS L5, service provider ID verified by MT47 ensuring authorised service provider is used
7.3.1.3	[F3.1.2] SBAS data demodulation, FEC decoding and frame synchronisation	**Erroneous** Erroneous SBAS message demodulation, FEC decoding and message synchronisation	• High BER • GNSS receiver HW/SW fault	• Erroneous SBAS messages	Provision of erroneous SBAS messages to GA-OB; VLF<GAP>_HAZ-001	Critical	Internal barriers: • Errors in SBAS messages detected by CRC check
7.3.1.4	[F3.2.1] GNSS pre-correlation signal processing	**Erroneous** Pre-correlation bandwidth not within permitted range; differential group delay exceeds allowed maximum; pre-correlation filter not compliant with requirements on roll-off or central frequency	• Non-compliance with receiver design constraints [DMS:052]	• SBAS does not protect user from impact of signal distortions / EWF feared events • Impact on receiver measurements (error in corrected smoothed pseudorange) exceeds that of a compliant receiver	Impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Internal barriers: • Compliance with [DMS:052] Exported conditions: • [SC_F3_1] If not compliant with [DMS:052], SBAS does not protect user against EWF feared events. Implementation of barrier against EWF feared events in on-board receiver perimeter would therefore be required.

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.3.1.5	[F3.2.2] Acquisition and tracking of GNSS signals	**No or Not** GNSS signals not acquired or tracked	• GNSS receiver HW/SW fault	• GNSS measurements unavailable	Reference time (SNT) and timestamping unavailable; diagnostic functions dependent on GNSS positioning unavailable (i.e., cyber security defences TBC)	RAM Issue	
7.3.1.6	[F3.2.2] Acquisition and tracking of GNSS signals	**Erroneous** Use of incorrect signals for code and carrier phase measurements	• Non-compliance with [DMS:237] and [DMS:238] • Use of GPS signals other than L1 C/A- code and L5-Q5 signals for code and carrier phase measurements • Use of GAL signals other than E1-C and E5a-Q signals for code and carrier phase measurements, E1-C signals being processed with BOC(1,1) replicas only, and E5a- Q signals, with BPSK(10) replicas only	• Performances of measurements made using other signals not committable by SBAS	Impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Internal barriers: • Compliance with [DMS:237] for GPS • Compliance with [DMS:238] for GAL
7.3.1.7	[F3.2.2] Acquisition and tracking of GNSS signals	**Erroneous** Use of incompatible tracking loop	• Non-compliance with constraints on tracking loop implementation [DMS:155] and [DMS:239]	• SBAS does not protect user from impact of signal distortions / EWF feared events • Impact on receiver measurements (error in corrected smoothed pseudorange) exceeds that of a compliant receiver	Impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Internal barriers: • Compliance with [DMS:155] for GPS code tracking loops • Compliance with [DMS:239] for GAL code tracking loops Exported conditions: • [SC_F3_2] If not compliant with [DMS:155] and [DMS:239], SBAS does not protect user against EWF feared events. Implementation of barrier against EWF feared events in on-board receiver perimeter would therefore be required.

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.3.1.8	[F3.2.2] Acquisition and tracking of GNSS signals	**Erroneous** Mistaking one GPS L1 C/A code signal with another; one GPS L5 signal with another; one GAL E1 signal with another; or one GAL E5a signal with another	• Cross-correlation effects during acquisition or reacquisition	• GPS L1 C/A ranging data does not correspond to PRN code number used for signal tracking • GPS L5 ranging data does not correspond to PRN code number used for signal tracking • Galileo E1 ranging data does not correspond to primary code number used for signal tracking • Galileo E5a ranging data does not correspond to primary code number used for signal tracking	Impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Internal barriers: • Compliance with [DMS:247] and [DMS:770] for GPS L1 C/A • Compliance with [DMS:015] and [DMS:777] for GPS L5 • Compliance with [DMS:023] and [DMS:778] for GAL E1 • Compliance with [DMS:024] and [DMS:779] for GAL E5a
7.3.1.9	[F3.2.2] Acquisition and tracking of GNSS signals	**Erroneous** Overshoot exceeds theoretical bias error (ionosphere-free pseudorange)	• Simultaneous code step errors on L1/E1 and L5/E5a signals with the same magnitude of up to 10 meters but opposite signs	• Smoothed ionosphere-free pseudorange error exceed theoretical bias error	Impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Internal barriers: • Compliance by use of first-order code tracking loops (no overshoot) Exported conditions: • [SC_F3_3] If use of first-order tracking loops is not guaranteed, an analysis is required to demonstrate that the overshoot does not exceed a specified threshold (TBC) or to support bounding of the overshoot following the occurrence of the code step errors.
7.3.1.10	[F3.2.2] Acquisition and tracking of GNSS signals	**Erroneous / Early / Late / Partial** Erroneous acquisition or tracking of GNSS signals	• GNSS receiver HW/SW fault	• Erroneous GNSS measurements (GNSS ID, SVID, code and carrier phase measurements, C/N0, LLI)	Impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Requirements • [SR_F3_1] GNSS receiver HW and SW / firmware shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.3.1.11	[F3.2.2] Acquisition and tracking of GNSS signals	**Erroneous** Acquisition and tracking of signals with interference exceeding nominal interference environment	• Radiofrequency interference • Cyber-attack (intentional jamming)	• Degraded C/N0, increased pseudorange noise •	Standard deviation of distribution that bounds errors in the tails associated with GNSS receiver (*including receiver noise, thermal noise, interference, inter-channel biases, extrapolation, time since smoothing filter initialisation and processing errors*) may not bound the respective pseudorange errors at the required level of confidence; Impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F3_2] If RF interference exceeds the nominal interference environment (TBC), the GNSS receiver shall guarantee the increased pseudorange errors due to the RF interference are bounded (i.e., no increase in risk of misleading information). Impact on availability / continuity is expected.
7.3.1.12	[F3.2.3] GNSS navigation data demodulation, FEC decoding and frame synchronisation	**Erroneous** Erroneous navigation data demodulation, FEC decoding and frame synchronisation	• High BER • GNSS receiver HW/SW fault	• Erroneous navigation data	Impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Internal barriers: • Errors in navigation data detected by CRC / parity checks

7.4 F5: GNSS Augmentation Dissemination Function

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.4.1.1	[F5.1] Select GACs	**No or Not** Available GNSS augmentation channel not selected (SBAS PRN)	• GA-TS HW/SW fault	• Authorised SBAS PRN not selected	SBAS messages from authorised SBAS signal are unavailable	RAM Issue	
7.4.1.2	[F5.1] Select GACs	**Erroneous** Erroneous selection of GNSS augmentation channel (SBAS PRN)	• GA-TS HW/SW fault • Mistaking one SBAS PRN for another	• Unsupported / unauthorised SBAS provider erroneously used (i.e., not providing railway SoL service, commitments on pseudorange domain integrity)	Provision of SBAS corrections from the wrong SBAS signal to GA-OB; VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.4.1.3	[F5.2.1] Timestamp reception of messages from SBAS	**No or Not** Reception of SBAS message not timestamped	• GA-TS HW/SW fault • Reference time (SNT) unavailable	• Timestamp of SBAS message reception not available	SBAS message content timeout supervision unavailable; TTA supervision unavailable; GNSS channel unavailable	RAM Issue	
7.4.1.4	[F5.2.1] Timestamp reception of messages from SBAS	**Early** Reception of SBAS message timestamped with earlier timestamp	• GA-TS HW/SW fault • Erroneous reference time (SNT)	• Timestamp applied in GA message is earlier than reception of SBAS message	SBAS message content times out early; pseudoranges become unavailable or degradation parameters applied	RAM Issue	
7.4.1.5	[F5.2.1] Timestamp reception of messages from SBAS	**Erroneous / Late** Erroneous or late timestamping of reception of SBAS message	• GA-TS HW/SW fault • Erroneous reference time (SNT)	• Incorrect timestamp or timestamp later than reception of SBAS messages applied in GA message	Incorrect supervision of SBAS message content timeouts; incorrect supervision of TTA; VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.4.1.6	[F5.2.2] SBAS message CRC checks	**Erroneous** Erroneous SBAS message CRC check	• GA-TS HW/SW fault	• Undetected SBAS message corruption • Erroneous SBAS message	Erroneous SBAS message used for GA-TS functions (providing active GA data, alerts, etc. to GA-OB); provision of erroneous data to GA-OB; impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.4.1.7	[F5.2.3] Encapsulation of SBAS messages in GAM packets	**No or Not** SBAS message not encapsulated	• GA-TS HW/SW fault	• Invalid GA message sent to GA-OB	SBAS message content times out early; pseudoranges become unavailable or degradation parameters applied; impact on bounding of errors (larger due to degradation parameters) or fewer pseudoranges available for use by VLF	RAM Issue	

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.4.1.8	[F5.2.3] Encapsulation of SBAS messages in GAM packets	**Erroneous** Erroneous encapsulation of SBAS message	• GA-TS HW/SW fault	• Acknowledgement not requested for critical message (e.g., SBAS alert) • Invalid GA message sent to GA-OB	Missed alerts; VLF<GAP>_HAZ-001	Critical	Internal barriers: • CRC of SBAS message encapsulated in GA message verified by GA-OB • GA-OB shall supervise when no valid GA message has been received for T_GATIMEOUT seconds. If Timer T_GATIMEOUT expires, the GA-OB shall ensure all GA integrity data for the GA message stream become unavailable Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.4.1.9	[F5.2.4] Process SBAS messages	**Erroneous** Erroneous processing of SBAS messages	• GA-TS HW/SW fault • Undetected message corruption	• Erroneous SBAS message content / parameters	Erroneous SBAS message content / parameters used for GA-TS functions (providing active GA data, alerts, etc. to GA-OB); provision of erroneous data to GA-OB; impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.4.1.10	[F5.3.1] Allocate GA message stream	No or Not / Partial / Erroneous Erroneous allocation of GA message stream	• GA-TS HW/SW fault	• Allocation of two GA message streams from the same GAC (i.e., same SBAS PRN) • Allocation of incompatible GA message stream (e.g., SBAS DFMC instead of SBAS L1) • GA message stream not allocated	Impact on availability from allocation of two streams with the same GAC; unavailability of GNSS channel due to incompatible GA message stream or no GA message stream allocated	RAM Issue	Internal barriers: • GA-OB detects incompatible message stream through SBAS message type numbers.
7.4.1.11	[F5.3.2] Suspend GA message stream	**As well as** GA-TS suspends GA message stream when it should not	• GA-TS HW/SW fault	• GA-TS unnecessarily suspends message stream	Integrity information for GA message stream becomes unavailable / times out; GA-OB GNSS channel becomes unavailable	RAM Issue	

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.4.1.12	[F5.3.2] Suspend GA message stream	**No or Not / Late / Erroneous** GA message stream not suspended when GA-TS sends GA alert or DNU message stream	• GA-TS HW/SW fault	• GA-TS fails to suspend GA message stream when GA alert or DNU message stream sent to GA-OB	GA alert or DNU message stream not acknowledged by GA-OB; Integrity information of GA message stream does not become unavailable / time out; VLF<GAP>_HAZ-001	Critical	Internal barriers: • GA-TS suspends the relevant GA message stream when “GA alert” or “DNU message stream” is sent to GA-OB. This ensures integrity information times out if GA alert or DNU is not acknowledged. • For GA alert, once acknowledged by GA-OB, message stream is resumed after ensuring any additional alert messages (different alert sequences) have been received and acknowledged. • For DNU message stream, the GA-OB ceases using and discards any ranging data and GA data obtained from the relevant GA message stream Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.4.1.13	[F5.3.3] Resume GA message stream	**No or Not** GA message stream not resumed by GA-TS	• GA-TS HW/SW fault • Failed reception of acknowledgement / “resume GA message stream” message	• GA-TS fails to resume GA message stream after acknowledgement of GA alert (and no additional alerts) or reception of “resume GA message stream” message (and no alerts to acknowledge)	Integrity information for GA message stream becomes unavailable / times out; GA-OB GNSS channel becomes unavailable	RAM Issue	

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.4.1.14	[F5.3.3] Resume GA message stream	**As well as / Erroneous** GA message stream resumed when it should not	• GA-TS HW/SW fault • Undetected message corruption	• GA-TS resumes GA message stream before GA alert is acknowledged • GA-TS resumes GA message stream after "DNU message stream" sent to GA-OB	GA alert or DNU message stream not acknowledged by GA-OB; Integrity information of GA message stream does not become unavailable / time out; VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.4.1.15	[F5.4] Provide GA active data for selected GACs	**No or Not** GA active data not provided	• GA-TS HW/SW fault • Failed reception of SBAS messages (e.g., higher BER due to interference environment)	• Incomplete set of GA active data available to send to GA-OB	GA-OB waits until complete active data set can be obtained (at SBAS broadcast update rate of 1 Hz); delay for GA-OB GNSS channel to become available with integrity	RAM Issue	
7.4.1.16	[F5.4] Provide GA active data for selected GACs	**Erroneous** Provision of erroneous GA active data	• GA-TS HW/SW fault • Undetected message corruption	• Erroneous SBAS messages	Erroneous SBAS message content sent to GA-OB; VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.4.1.17	[F5.5] Provide GA active alerts for selected GACs	**No or Not** GA active alerts not provided	• GA-TS HW/SW fault • Failed reception of SBAS messages (e.g., higher BER due to interference environment)	• SBAS alerts not provided to GA-OB when resuming GA message stream	Missed alerts; VLF<GAP>_HAZ-001	Critical	Internal barriers: • SBAS broadcasts a valid message every second to provide a continuity of signal • Communication link failure is indicated for SBAS L1 or SBAS L5 when no valid SBAS message has been received for 4 seconds [DMS:299, DMS:113]. Communication link failure is considered a very low occurrence event assuming reliable reception of SBAS messages at the trackside. • In the case of communication link failure, the GA-TS shall send a GA Message with GA message type Q_GAMT = 2 (DNU GA message stream) to the GA-OB, requiring acknowledgement, indicating that the GA-OB shall no longer use the GA message stream Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.4.1.18	[F5.5] Provide GA active alerts for selected GACs	**Erroneous** Provision of erroneous GA active alerts	• GA-TS HW/SW fault • Undetected message corruption	• Erroneous SBAS alerts provided to GA-OB when resuming GA message stream	Missed alerts; erroneous SBAS integrity data; VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.4.1.19	[F5.6.1] GNSS navigation data CRC / parity checks	**Erroneous** Erroneous GNSS navigation data CRC / parity check	• GA-TS HW/SW fault	• Undetected navigation message corruption • Erroneous navigation data	Erroneous navigation data provided to GA-OB; impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Internal barriers: • GA-OB verifies CRC / parity of encapsulated GNSS navigation data Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.4.1.20	[F5.6.2] Decoding navigation message parameters	**Erroneous** Erroneous decoding of navigation message parameters	• GA-TS HW/SW fault	• Erroneous navigation message content / parameters	Erroneous navigation message content / parameters used for GA-TS functions; impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.4.1.21	[F5.6.3] Message consistency checks	**Erroneous** Erroneous message consistency checks (e.g., consistency of IODs, reference times, etc.)	• GA-TS HW/SW fault	• Inconsistent navigation data is used (e.g., navigation message parameters with the wrong IOD)	Erroneous navigation message content / parameters used for GA-TS functions; impact on reference time (SNT) and timestamping; impact on diagnostic functions dependent on GNSS positioning (i.e., cyber security defences TBC); VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

Ref ID	Basic Function	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects		Severity	Internal Barriers / Mitigation
				Local Effect	Initial End Effect		
7.4.1.22	[F5.7] Provide GNSS navigation data sets	**No or Not / Late** GNSS navigation data sets not provided	• GA-TS HW/SW fault • Failed reception of GNSS navigation message (e.g., higher BER due to interference environment)	• GNSS navigation data unavailable • Last 3 different sets of LNAV clock / ephemeris parameters for GPS unavailable • Last 4 different sets of F/NAV clock / ephemeris parameters for Galileo unavailable	GNSS navigation data not provided to GA-OB or GNSS navigation data IODs do not match the current broadcast SBAS corrections	RAM Issue	
7.4.1.23	[F5.7] Provide GNSS navigation data sets	**Erroneous** Provision of erroneous navigation data sets	• GA-TS HW/SW fault • Undetected message corruption	• Erroneous navigation data set	Erroneous navigation data sent to GA-OB; VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)
7.4.1.24	[F5.8] Manage GA session	**Erroneous** Erroneous acknowledgment	• GA-TS HW/SW fault	• Missed alert	VLF<GAP>_HAZ-001	Critical	Requirements: • [SR_F5_1] GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)

8 List of Hazardous Events from FMEA

Event Id.	Event Description	GA Function Reference	FMEA Reference
OB-GRX-1	Erroneous GNSS pre-correlation signal processing	F1.1.1	7.1.1.1
OB-GRX-2	Erroneous acquisition or tracking of GNSS signals	F1.1.2	7.1.1.2; 7.1.1.3; 7.1.1.4; 7.1.1.5; 7.1.1.6; 7.1.1.7; 7.1.1.8
OB-GRX-3	Erroneous GNSS navigation data demodulation, FEC decoding or frame synchronisation	F1.1.3	7.1.1.9
OB-GAP-1	Failure of GNSS navigation data CRC / parity checks (GA-OB)	F2.1.1	7.2.1.1
OB-GAP-2	Erroneous decoding of navigation message parameters (GA-OB)	F2.1.2	7.2.1.2
OB-GAP-3	Failure of message consistency checks (IODs, reference times, etc.) (GA-OB)	F2.1.3	7.2.1.3
OB-GAP-4	Erroneous timestamping of GA messages received from GA-TS	F2.2.1	7.2.1.4; 7.2.1.5; 7.2.1.6
OB-GAP-5	Failure of SBAS message CRC checks (encapsulated in GA message)	F2.2.2	7.2.1.7
OB-GAP-6	Erroneous processing of SBAS message content (encapsulated in GA message)	F2.2.3	7.2.1.8
OB-GAP-7	Erroneous carrier smoothing on pseudorange measurements	F2.3.1	7.2.1.9
OB-GAP-8	Failure of measurement quality monitoring	F2.3.2	7.2.1.10
OB-GAP-9	Erroneous pseudorange determination	F2.3.3	7.2.1.11
OB-GAP-10	Erroneous GNSS satellite selection (use criteria)	F2.3.4	7.2.1.12; 7.2.1.13
OB-GAP-11	Erroneous computation or application of model for differential correction residual error	F2.4.1	7.2.1.14
OB-GAP-12	Erroneous computation or application of model for residual ionospheric error	F2.4.2	7.2.1.15
OB-GAP-13	Erroneous computation or application of model of tropospheric residual uncertainty	F2.4.3	7.2.1.16
OB-GAP-14	Erroneous computation of model of ionospheric divergence for SBAS L1 users	F2.4.4	7.2.1.17
OB-GAP-15	Erroneous supervision of SBAS message content timeout (encapsulated in GA message)	F2.5	7.2.1.18; 7.2.1.19
OB-GAP-16	Erroneous supervision and management of TTA	F2.6	7.2.1.20; 7.2.1.21
OB-GAP-17	Erroneous management of GA session	F2.7	7.2.1.22
TS-GRX-1	Erroneous acquisition or tracking of SBAS signals (GA-TS)	F3.1.1	7.3.1.1; 7.3.1.2
TS-GRX-2	Erroneous SBAS data demodulation, FEC decoding or frame sync (GA-TS)	F3.1.2	7.3.1.3
TS-GRX-3	Erroneous GNSS pre-correlation signal processing (GA-TS)	F3.2.1	7.3.1.4
TS-GRX-4	Erroneous acquisition or tracking of GNSS signals (GA-TS)	F3.2.2	7.3.1.5; 7.3.1.6; 7.3.1.7; 7.3.1.8; 7.3.1.9; 7.3.1.10; 7.3.1.11

TS-GRX-5	Erroneous GNSS navigation data demodulation, FEC decoding or frame sync (GA-TS)	F3.2.3	7.3.1.12
TS-GAD-1	Erroneous GAC selection	F5.1.1	7.4.1.1; 7.4.1.2
TS-GAD-2	Erroneous timestamping of reception of messages from SBAS	F5.2.1	7.4.1.3; 7.4.1.4; 7.4.1.5
TS-GAD-3	Failure of SBAS message CRC checks	F5.2.2	7.4.1.6
TS-GAD-4	Erroneous encapsulation of SBAS messages in GAM packets	F5.2.3	7.4.1.7; 7.4.1.8
TS-GAD-5	Erroneous processing of SBAS message content	F5.2.4	7.4.1.9
TS-GAD-6	Erroneous allocation of GA message stream	F5.3.1	7.4.1.10
TS-GAD-7	Failure in suspending GA message stream	F5.3.2	7.4.1.11; 7.4.1.12
TS-GAD-8	Failure in resuming GA message stream	F5.3.3	7.4.1.13; 7.4.1.14
TS-GAD-9	Provision of erroneous GA active data for selected GACs	F5.4	7.4.1.15; 7.4.1.16
TS-GAD-10	Provision of erroneous GA active alerts for selected GACs	F5.5	7.4.1.17; 7.4.1.18
TS-GAD-11	Failure of GNSS navigation data CRC / parity checks (GA-TS)	F5.6.1	7.4.1.19
TS-GAD-12	Erroneous decoding of navigation message parameters (GA-TS)	F5.6.2	7.4.1.20
TS-GAD-13	Failure of message consistency checks (IODs, reference times, etc.) (GA-TS)	F5.6.3	7.4.1.21
TS-GAD-14	Provision of erroneous GNSS navigation data sets	F5.7	7.4.1.22; 7.4.1.23
TS-GAD-15	Erroneous management of GA session	F5.8	7.4.1.24

9 List of Safety Requirements and Exported Conditions from FMEA

9.1 Transmission Channel Hazard Analysis

9.1.1 List of Safety Requirements from FMEA

ID	Description	FMEA Reference
SR_GNSS-GA-OB_1	GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)	6.1.1.1; 6.1.1.3
SR_GA-OB-GA-TS_1	Safe radio channel for exchange of GA messages between GA-OB and GA-TS shall comply with EN 50159 implementing CRC for detection of message corruption	6.2.1.1
SR_GA-OB-GA-TS_2	For GA-OB safety-related transmission function, the HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)	6.2.1.1; 6.2.1.2; 6.2.1.3; 6.2.1.4; 6.2.1.5
SR_GA-OB-GA-TS_3	For GA-TS safety-related transmission function, the HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)	6.2.1.1; 6.2.1.2; 6.2.1.3; 6.2.1.4; 6.2.1.5
SR_GA-OB-GA-TS_4	Safe radio channel for exchange of GA messages between GA-OB and GA-TS shall comply with EN 50159 implementing sequence numbers for detection of deleted GA messages	6.2.1.2; 6.2.1.4; 6.2.1.5
SR_GA-OB-GA-TS_5	Safe radio channel for exchange of GA messages between GA-OB and GA-TS shall comply with EN 50159 implementing cryptographic techniques to detect masqueraded GA messages (authentication and cryptographic message integrity)	6.2.1.5
SR_GNSS-GA-TS_1	GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)	6.3.1.1; 6.3.1.3
SR_GNSS-GA-TS_2	Barriers against cyber-attacks resulting in delayed / replayed GNSS signals shall be implemented (details TBC in future SFHA release; note that ground truth at trackside should enable the definition of an effective diagnostic).	6.3.1.3
SR_GNSS-GA-TS_3	Barriers against cyber-attacks resulting in spoofed GNSS signals shall be implemented (details TBC in future SFHA release; note that ground truth at trackside should enable the definition of an effective diagnostic).	6.3.1.4
SR_SBAS-GA-TS_1	GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)	6.4.1.1; 6.4.1.2; 6.4.1.3
SR_SBAS-GA-TS_2	Barriers against cyber-attacks resulting in delayed / replayed SBAS signals shall be implemented (details TBC in future SFHA release; note that ground truth at trackside should enable the definition of an effective diagnostic).	6.4.1.3
SR_SBAS-GA-TS_3	Barriers against cyber-attacks resulting in spoofed SBAS signals shall be implemented (details TBC in future SFHA release; note that ground truth at trackside should enable the definition of an effective diagnostic).	6.4.1.4

9.1.2 List of Exported Conditions from FMEA

ID	Description	FMEA Reference
SC_GNSS-GA-OB_1	Detection of cyber-attacks targeting GNSS signals at the GA-OB is outside the scope of GA for ERTMS/ETCS. The LOC-OB shall implement barriers against spoofing threats.	6.1.1.3; 6.1.1.4

9.2 Functional Hazard Analysis

9.2.1 List of Safety Requirements from FMEA

ID	Description	FMEA Reference
SR_F1 _1	GNSS receiver HW and SW / firmware shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)	7.1.1.7
SR_F2_1	GA-OB HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)	7.2.1.1; 7.2.1.2; 7.2.1.3; 7.2.1.5; 7.2.1.7; 7.2.1.8; 7.2.1.9; 7.2.1.10; 7.2.1.11; 7.2.1.13; 7.2.1.14; 7.2.1.15; 7.2.1.16; 7.2.1.17; 7.2.1.18; 7.2.1.20; 7.2.1.22
SR_F2_2	Signal tracking quality shall be monitored such that the allocated integrity risk due to undetected cycle slip or other undetected measurement fault is within the manufacturer's allocation [DMS:323]	7.2.1.9
SR_F3_1	GNSS receiver HW and SW / firmware shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)	7.3.1.10
SR_F3_2	If RF interference exceeds the nominal interference environment (TBC), the GNSS receiver shall guarantee the increased pseudorange errors due to the RF interference are bounded (i.e., no increase in risk of misleading information). Impact on availability / continuity is expected.	7.3.1.11
SR_F5_1	GA-TS HW and SW shall be designed such that probability of providing misleading information is acceptable with respect to system integrity requirements (where EN50129 and EN50128 provide acceptable means for compliance)	7.4.1.2; 7.4.1.5; 7.4.1.6; 7.4.1.8; 7.4.1.9; 7.4.1.12; 7.4.1.14; 7.4.1.16; 7.4.1.17; 7.4.1.18; 7.4.1.19; 7.4.1.20; 7.4.1.21; 7.4.1.23; 7.4.1.24

9.2.2 List of Exported Conditions from FMEA

ID	Description	FMEA Reference
SC_F1_1	If not compliant with [DMS:052], SBAS does not protect user against EWF feared events. Implementation of barrier against EWF feared events in on-board receiver perimeter would therefore be required.	7.1.1.1
SC_F1_2	If not compliant with [DMS:155] and [DMS:239], SBAS does not protect user against EWF feared events. Implementation of barrier against EWF feared events in on-board receiver perimeter would therefore be required.	7.1.1.4
SC_F1_3	If use of first-order tracking loops is not guaranteed, an analysis is required to demonstrate that the overshoot does not exceed a specified threshold (TBC) or to support bounding of the overshoot following the occurrence of the code step errors.	7.1.1.6
SC_F1_4	Bounding of pseudorange errors related to the GNSS receiver including interference is outside scope of GA for ERTMS/ETCS but shall be addressed in the on-board receiver perimeter. If RF interference exceeds the nominal interference environment (TBC), the GNSS receiver shall guarantee the increased pseudorange errors due to the RF interference are bound (i.e., no increase in risk of misleading information). Impact on availability / continuity is expected.	7.1.1.8
SC_F2_1	If not compliant with [DMS:322] and [DMS:156], additional barriers may need to be defined in the receiver to address the faster response of the smoothing filter with a shorter weighting function time constant. In addition, the impact of a shorter weighting function time constant needs to be considered in the bounding of pseudorange errors related to receiver noise, multipath, and for single frequency users, the difference between the implemented smoothing filter and the reference smoothing filter given an ionospheric code-carrier divergence. In the case of a non-compliant smoothing filter, justification would be needed to demonstrate integrity assumptions are not violated considering differences of the implemented smoothing filter with respect to the response of the reference smoothing filter, addressing: a) The transient function of the error during convergence time of the filter (i.e., elapsed time since smoothing filter re-initialisation until in the steady state); b) Inflation of residual error variances in the case of a smoothing filter with a weighting function time constant < 100 seconds (i.e., in the steady state); and c) For single frequency users, residual ionospheric error caused by the difference between the implemented filter and the reference filter caused by ionospheric divergence during the transient phase.	7.2.1.9
SC_F2_2	Tropospheric model needs to be validated for railway (e.g., considering application of masking angle to reduce mapping function anomalies from blind model, validation in extreme conditions)	7.2.1.16
SC_F2_3	The value of σ_{divg} for SBAS L1 users needs to be set accounting for the difference between the implemented smoothing filter and the reference smoothing filter for a given ionospheric divergence – i.e., during the transient phase if the implemented smoothing filter is the filter defined in [DMS:322]. For this filter, $\sigma_{divg} = 0$ after steady state is reached.	7.2.1.17
SC_F3_1	If not compliant with [DMS:052], SBAS does not protect user against EWF feared events. Implementation of barrier against EWF feared events in on-board receiver perimeter would therefore be required.	7.3.1.4
SC_F3_2	If not compliant with [DMS:155] and [DMS:239], SBAS does not protect user against EWF feared events. Implementation of barrier against EWF feared events in on-board receiver perimeter would therefore be required.	7.3.1.7
SC_F3_3	If use of first-order tracking loops is not guaranteed, an analysis is required to demonstrate that the overshoot does not exceed a specified threshold (TBC) or to support bounding of the overshoot following the occurrence of the code step errors.	7.3.1.9

10 Preliminary Quantitative Safety Targets

10.1.1.1 This section defines a preliminary set of high-level quantitative safety requirements needed for technical interoperability of the GA for ERTMS/ETCS. The top-level hazard at the boundary of the GNSS Augmentation Processing of the Vehicle Localisation function (VLF<GAP>) is allocated a preliminary target based on achievable pseudorange domain integrity performances considering the use of EGNOS.

10.1.1.2 It is assumed that an EGNOS Railway SoL Service would provide detection of fault conditions (i.e., presence in the system of any feared events or any events beyond the defined fault-free conditions) and bounding of residual errors in the pseudorange domain under fault-free conditions. Fault-free conditions refer to no extreme ionosphere / scintillation conditions; included in fault-free conditions is frequently observed events such as ground station nominal multipath / interference / cycle slips, interruptions in the ground segment, processing facility switches, etc.

10.1.1.3 How pseudoranges and respective error bounds are used in the VLF is outside the boundary of this analysis; however, integrity is guaranteed for solutions based on snapshot Weighted Least Squares when the pseudorange error is bounded for all measurements (including user segment errors such as related to receiver noise, multipath, etc.). If Kalman filters are used, the protection level is computed from the estimated covariance with the assumption that measurement error distribution is uncorrelated and zero-mean Gaussian. This assumption is not valid as errors (i.e., orbit, clock, and ionospheric errors) are correlated in time and are not Gaussian. For implementations of the VLF based on Kalman filtering, methods for handling temporal correlation on measurement errors and errors from biases of previous epochs within the Kalman filter need to be considered.

10.1.1.4 The maximum allowed rate of the occurrence of the top-level hazard, **VLF<GAP>_HAZ-001: Residual errors (clock, orbit, and ionosphere) are not bounded at the required level of confidence and no alert is given within the end-to-end TTA**, is allocated 5.0E-6 / hour.

10.1.1.5 This target has been apportioned between GA on-board (GA-OB), GA trackside (GA-TS) and the GA transmission channels based on the analysis performed in Annex A. Safety requirements are given as tolerable hazard rates (THRs) and for functions, tolerable functional failure rates (TFFRs). Safety integrity levels (SILs) are determined from the TFFRs.

10.2 GA On-board (GA-OB)

GA-OB	**GA-OB THR** The hazard rate for the GA on-board (excluding the non-trusted parts of the GA transmission channel) shall not exceed a THR of: 2.5E-8 dangerous failures / hour [UNSTABLE]

10.2.1.1 Attainment of $THR_{GA\text{-}OB}$ shall consider at least the following hazardous events:

- On-board interface to GNSS SIS
  - OB-GRX-1: Erroneous GNSS pre-correlation signal processing
  - OB-GRX-2: Erroneous acquisition of tracking of GNSS signals
  - OB-GRX-3: Erroneous GNSS navigation data demodulation, FEC decoding or frame synchronisation
- GNSS augmentation processing
  - OB-GAP-1: Failure of GNSS navigation data CRC / parity checks
  - OB-GAP-2: Erroneous decoding of navigation message parameters
  - OB-GAP-3: Failure of message consistency checks (IODs, reference times, etc.)
  - OB-GAP-4: Erroneous timestamping of GA messages received from GA-TS
  - OB-GAP-5: Failure of SBAS message CRC checks (encapsulated in GA message)
  - OB-GAP-6: Erroneous processing of SBAS message content (encapsulated in GA message)
  - OB-GAP-7: Erroneous carrier smoothing on pseudorange measurements
  - OB-GAP-8: Failure of measurement quality monitoring
  - OB-GAP-9: Erroneous pseudorange determination
  - OB-GAP-10: Erroneous GNSS satellite selection (use criteria)
  - OB-GAP-11: Erroneous computation of application of model for differential correction residual error
  - OB-GAP-12: Erroneous computation of application of model for residual ionospheric error
  - OB-GAP-13: Erroneous computation or application of model of tropospheric residual uncertainty
  - OB-GAP-14: Erroneous computation of model of ionospheric divergence for SBAS L1 users
  - OB-GAP-15: Erroneous supervision of SBAS message content timeout (encapsulated in GA message)
  - OB-GAP-16: Erroneous supervision and management of TTA
  - OB-GAP-17: Erroneous management of GA session
- Safety-related radio transmission function
  - GA-OB-RADIO-H1: Radio message corrupted in GA-OB such that message appears consistent
  - GA-OB-RADIO-H2: Radio message deleted in GA-OB in an undetectable way
  - GA-OB-RADIO-H3: Radio message inserted in GA-OB such that message appears as consistent

10.2.1.2 In the analysis in Annex A, an exploratory apportionment of the GA-OB THR is made, considering a TFFR of 1E-8 / hour (SIL3) for the *on-board GNSS measurement engine function* (which includes pre-correlation signal processing, acquisition and tracking of GNSS signals, FEC decoding, frame synchronisation, and navigation data demodulation).

Function	Allocation
On-board GNSS measurement engine function	TFFR: 1E-8 / hour (SIL2: 1E-8 / hour $\leq$ TFFR $<$ 1E-7 / hour)

10.3 GA Trackside (GA-TS)

GA-TS	**GA-TS THR** The hazard rate for the GA trackside (excluding the non-trusted parts of the GA transmission channel) shall not exceed a THR of: 2.5E-8 dangerous failures / hour [UNSTABLE]

10.3.1.1 Attainment of $THR_{GA\text{-}TS}$ shall consider at least the following hazardous events:

- Trackside interface to SBAS / GNSS SIS
  - TS-GRX-1: Erroneous acquisition or tracking of SBAS signals
  - TS-GRX-2: Erroneous SBAS data demodulation, FEC decoding or frame synchronization
  - TS-GRX-3: Erroneous GNSS pre-correlation signal processing
  - TS-GRX-4: Erroneous acquisition or tracking of GNSS signals
  - TS-GRX-5: Erroneous GNSS navigation data demodulation, FEC decoding or frame synchronization
- GNSS augmentation dissemination
  - TS-GAD-1: Erroneous GAC selection
  - TS-GAD-2: Erroneous timestamping of reception of messages from SBAS
  - TS-GAD-3: Failure of SBAS message CRC checks
  - TS-GAD-4: Erroneous encapsulation of SBAS messages in GAM packets
  - TS-GAD-5: Erroneous processing of SBAS message content
  - TS-GAD-6: Erroneous allocation of GA message stream
  - TS-GAD-7: Failure in suspending GA message stream
  - TS-GAD-8: Failure in resuming GA message stream
  - TS-GAD-9: Erroneous provision of GA active data for selected GACs
  - TS-GAD-10: Erroneous provision of GA active alerts for selected GACs
  - TS-GAD-11: Failure of GNSS navigation data CRC / parity checks
  - TS-GAD-12: Erroneous decoding of navigation message parameters
  - TS-GAD-13: Failure of message consistency checks (IODs, reference times, etc.)
  - TS-GAD-14: Erroneous provision of GNSS navigation data sets
  - TS-GAD-15: Erroneous management of GA session
- Safety-related radio transmission function
  - GA-TS-RADIO-H1: Radio message corrupted in GA-TS such that message appears consistent
  - GA-TS-RADIO-H2: Radio message deleted in GA-TS in an undetectable way
  - GA-TS-RADIO-H3: Radio message inserted in GA-TS such that message appears consistent

10.3.1.2 In the analysis in Annex A, an exploratory apportionment of the GA-TS THR is made, considering a TFFR of 1E-8 / hour (SIL3) for the *trackside GNSS measurement engine*

function (which includes pre-correlation signal processing, acquisition and tracking of GNSS signals, FEC decoding, frame synchronisation, and navigation data demodulation).

Function	Allocation
Trackside GNSS measurement engine function	TFFR: 1E-8 / hour (SIL3: 1E-8 / hour $\leq$ TFFR $<$ 1E-7 / hour)

10.4 GA Transmission Channel (Non-trusted Part)

TRANS-HAZ	**GA Transmission Channel THR** The hazard rate for the non-trusted parts of the GA transmission channel shall not exceed a THR of: 1.5E-7 dangerous failures / hour [UNSTABLE]

10.4.1.1 Attainment of $THR_{TRANS\text{-}HAZ}$ shall consider at least the following hazardous events:

- SBAS SIS to GA-TS transmission channel
  - SBAS-GA-TS/UCR: Undetected SBAS message corruption
  - SBAS-GA-TS/UIM: Undetected inserted / masqueraded SBAS message
  - SBAS-GA-TS/UDL: Undetected SBAS message delay
- GNSS SIS to GA-TS transmission channel
  - GNSS-GA-TS/UCR: Undetected GNSS message corruption
  - GNSS-GA-TS/UIM: Undetected inserted / masqueraded GNSS navigation message
  - GNSS-GA-TS/USD: Undetected delay of GNSS signals
  - GNSS-GA-TS/USI: Undetected insertion of GNSS signals
- GA-TS to GA-OB transmission channel
  - TRANS-GA-OB/RADIO-1: Undetectable corruption of a message in the airgap (GA-OB)
  - TRANS-GA-TS/RADIO-1: Undetectable corruption of a message in the airgap (GA-TS)
- GNSS SIS to GA-OB transmission channel*
  - GNSS-GA-OB/UCR: Undetected GNSS message corruption
  - GNSS-GA-OB/UIM: Undetected inserted / masqueraded GNSS navigation message

*Note: While undetected delay and insertion of GNSS signals (i.e., GNSS spoofing) is addressed at the trackside, the impact of these hazardous events at the on-board (i.e., on pseudorange measurements used for on-board localisation) is not addressed within the GA for ERTMS/ETCS boundary. Barriers against such hazardous events (cyber-security threats) would need to be addressed within the LOC-OB perimeter.

Annex A Preliminary THR Apportionment

A.1.1.1 This annex provides a preliminary apportionment of **VLF<GAP>_HAZ-001**, the top-level hazard at the boundary of the GNSS Augmentation Processing of the Vehicle Localisation function (VLF<GAP>).

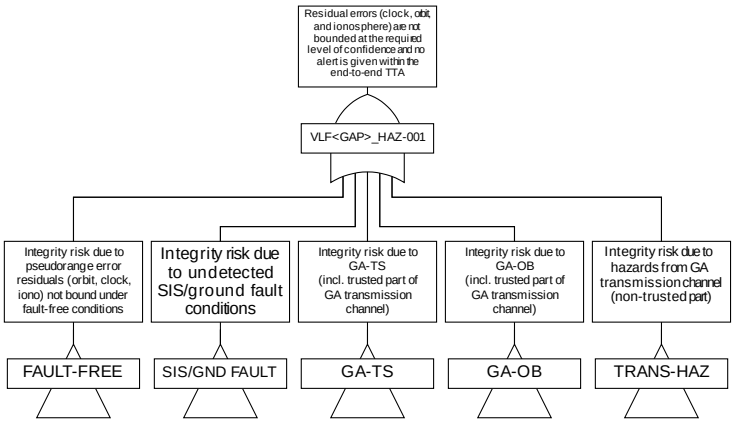
A.1.1.2 The allowed maximum rate of the occurrence of **VLF<GAP>_HAZ-001: Residual errors (clock, orbit, and ionosphere) are not bounded at the required level of confidence and no alert is given within the end-to-end TTA** is 5E-6 / hour, based on achievable pseudorange domain integrity performances considering the use of EGNOS.

A.1.1.3 The transmission channel is apportioned between trusted and non-trusted parts as described in [EN50159]. An initial allocation of 1% of the top-level hazard was made to non-trusted parts of the end-to-end GA transmission channel. After a first iteration with an estimation of hazardous failure rates, this was increased to 3%, such that:

$$THR_{VLF<GAP>\_HAZ-001} = 5.0E-6 \text{ / hour}$$

$$THR_{TRANS-HAZ} = 1.5E-7 \text{ / hour}$$

A.1.1.4 The preliminary apportionment is detailed below:



ID	Gate / Event	Description	Allocation (THR)
VLF<GAP>_HAZ-001	Residual errors (clock, orbit, and ionosphere) are not bounded at the required level of confidence and no alert is given within the end-to-end TTA	Top level GA hazard and THR allocation	5.0E-6 / hour
FAULT-FREE	Integrity risk due to pseudorange error residuals (orbit, clock, ionosphere) not bounded under fault-free conditions	Performance supported by SBAS*	2.4E-6 / hour
SIS/GND FAULT	Integrity risk due to undetected SIS / ground fault conditions	Performance supported by SBAS*	2.4E-6 / hour
GA-TS	Integrity risk due to GA trackside (including trusted part of the GA transmission channel)	Preliminary allocation	2.5E-8 / hour
GA-OB	Integrity risk due to GA on-board (including trusted part of the GA transmission channel)	Preliminary allocation	2.5E-8 / hour
TRANS-HAZ	Integrity risk due to hazards from GA transmission channel (non-trusted part)	Preliminary allocation	1.5E-7 / hour

A.1.1.5 A fault condition is the presence in the system (SBAS / GNSS) of any feared events or any events beyond the defined fault-free conditions.

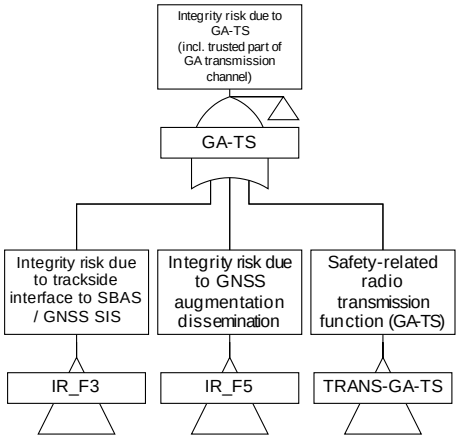
A.1.1.6 Fault-free conditions refer to no extreme ionosphere / scintillation conditions; included in fault-free conditions is frequently observed events such as ground station nominal multipath / interference / cycle slips, interruptions in the ground segment, processing facility switches, etc.

A.1.1.7 The other allocations for GA-TS, GA-OB and TRANS-HAZ are further elaborated in the following sections.

A.2 GA-TS: Integrity risk due to GNSS Augmentation Trackside

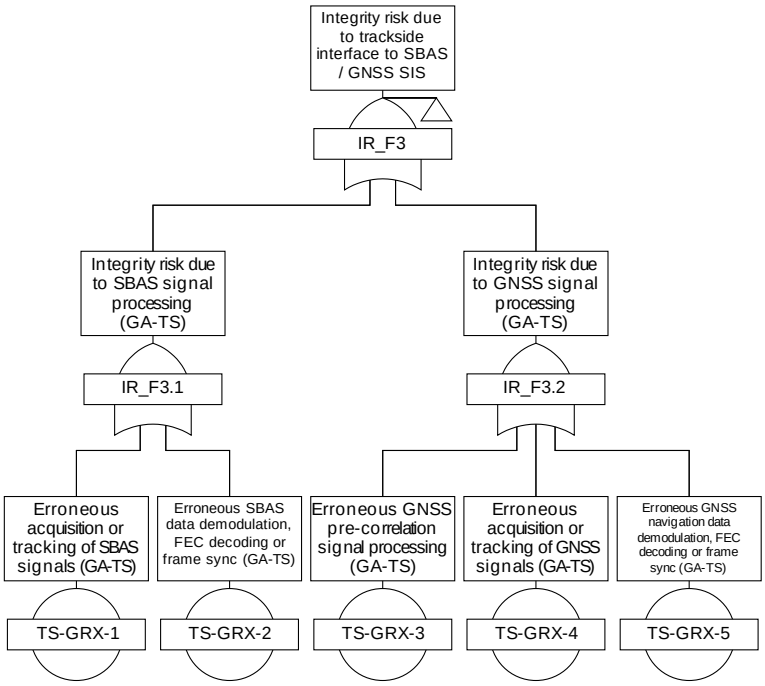
A.2.1.1 This allocation includes the trusted parts of the GA transmission channel in the trackside and considers a TFFR of 1E-8 / hour (SIL3) for the *trackside GNSS measurement engine function* (which includes pre-correlation signal processing, acquisition and tracking of GNSS signals, FEC decoding, frame synchronisation, and navigation data demodulation).

A.2.1.2 A SIL3 allocation is also equivalent to the level of safety offered by certified avionic GNSS receivers (i.e., certified to DAL B, equivalent to SIL3, based on aviation functional safety standards DO-178C / DO-254).

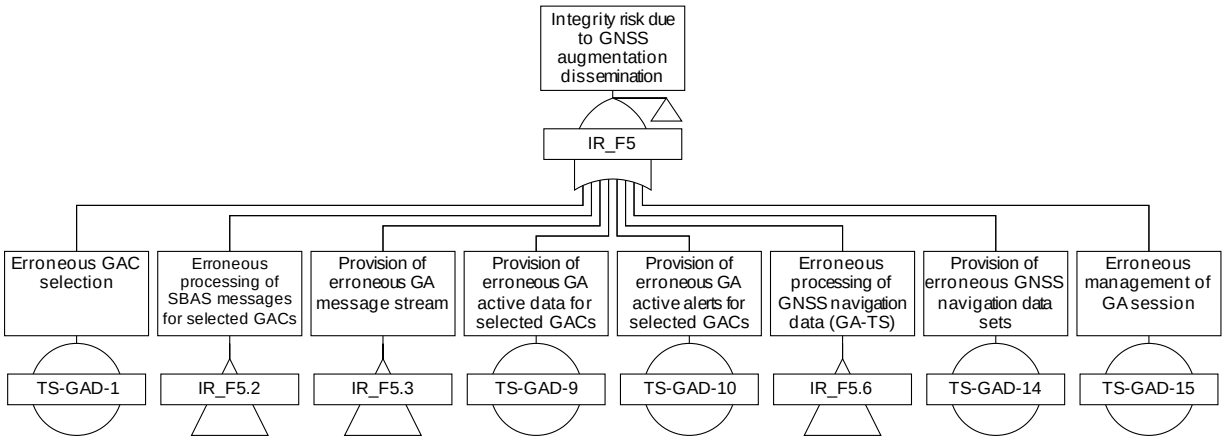


ID	Gate / Event	Description	Allocation (TFFR)	Estimated HR
IR_F3	Integrity risk due to trackside interface to SBAS / GNSS SIS	Preliminary allocation to trackside GNSS measurement engine function SIL3: 1E-8 / hour ≤ TFFR < 1E-7 / hour	2.0E-8 / hour	2.0E-8 / hour
IR_F5	Integrity risk due to GNSS augmentation dissemination	Preliminary allocation to trackside dissemination function SIL4: 1E-9 / hour ≤ TFFR < 1E-8 / hour	1.0E-9 / hour	1.0E-9 / hour
TRANS-GA-TS	Safety-related radio transmission function (GA-TS)	Preliminary allocation to trackside safety-related radio transmission function SIL4: 1E-9 / hour ≤ TFFR < 1E-8 / hour	1.0E-9 / hour	1.0E-9 / hour
		Margin in allocation	3.0E-9 / hour	
GA-TS			2.5E-8 / hour	2.2E-8 / hour
			Margin (HR, GA-TS allocation)	3.0E-9 / hour

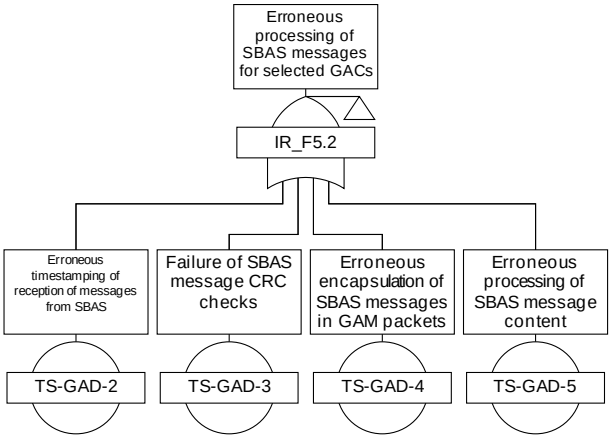
A.2.2 IR_F3: Integrity Risk Due to Trackside Interface to SBAS / GNSS SIS



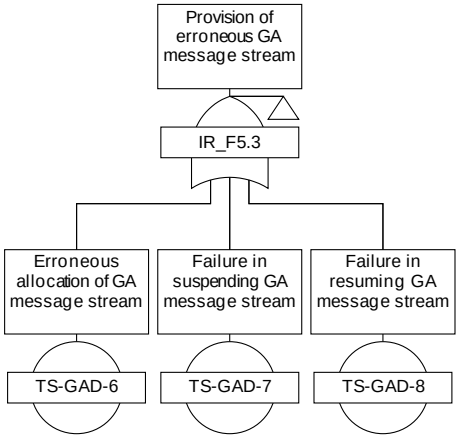
A.2.3 IR_F5: Integrity Risk Due to GNSS Augmentation Dissemination



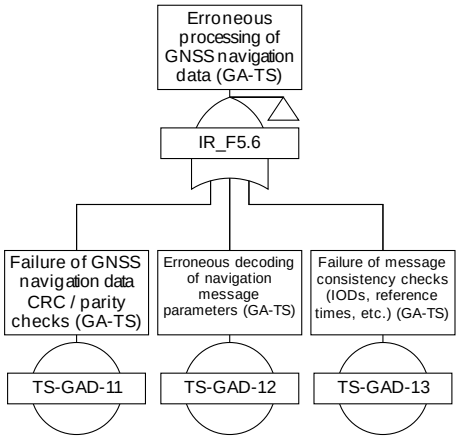
A.2.3.1 IR_F5.2: Erroneous processing of SBAS messages for selected GACs



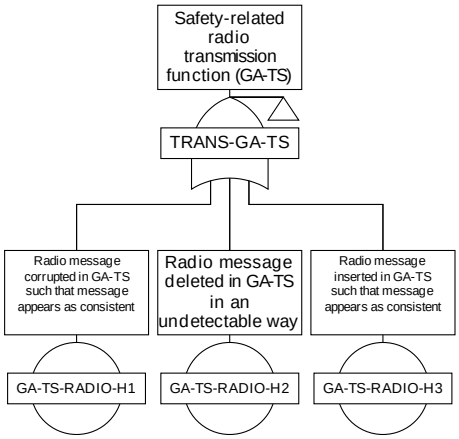
A.2.3.2 IR_F5.3: Erroneous provision of GA message stream



A.2.3.3 IR_F5.6: Erroneous processing of GNSS navigation data (GA-TS)



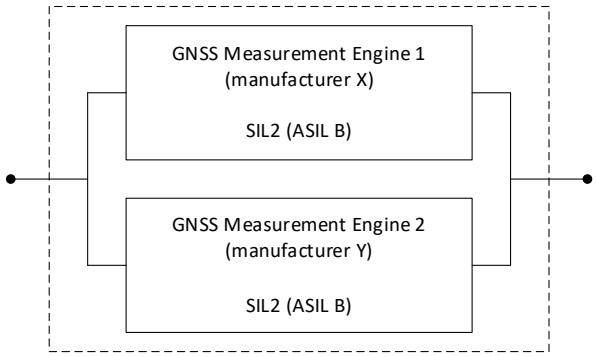
A.2.4 TRANS-GA-TS: Safety Related Radio Transmission Function (GA-TS)



A.3 GA-OB: Integrity risk due to GNSS Augmentation On-board

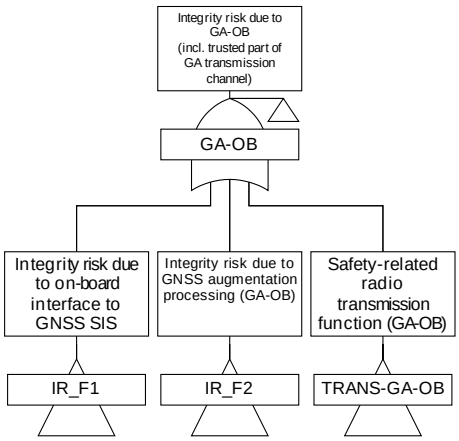
A.3.1.1 This allocation includes the trusted parts of the GA transmission channel in the on-board and considers a TFFR of 1E-8 / hour (SIL3) for the *on-board GNSS measurement engine function* (which includes pre-correlation signal processing, acquisition and tracking of GNSS signals, FEC decoding, frame synchronisation, and navigation data demodulation).

A.3.1.2 This is considered a feasible allocation of integrity budget to the on-board GNSS measurement engine, and potentially compatible with the use of COTS components to enable reduction of the cost of on-board GNSS elements as much as practicable (as per example below).



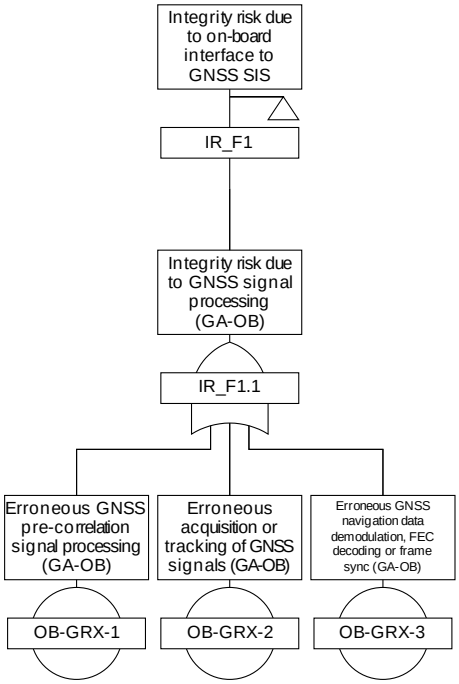
A.3.1.3 There are several safety-related COTS measurement engines on the market for automotive (i.e., certified to ASIL B, equivalent to SIL2), and these could be combined to meet the SIL3 target (for example, based on approaches described in IEC 61508). It should be noted however, that the impact of non-compliance to SBAS prescribed receiver constraints by the COTS measurement engines may require additional barriers to be implemented within the LOC-OB perimeter.

A.3.1.4 Further investigation is needed to assess options for use of COTS elements in a railway GNSS receiver chain, including the possibility of not relying on SBAS to protect the user against specific feared events linked with non-compliance of critical user receiver parameters.

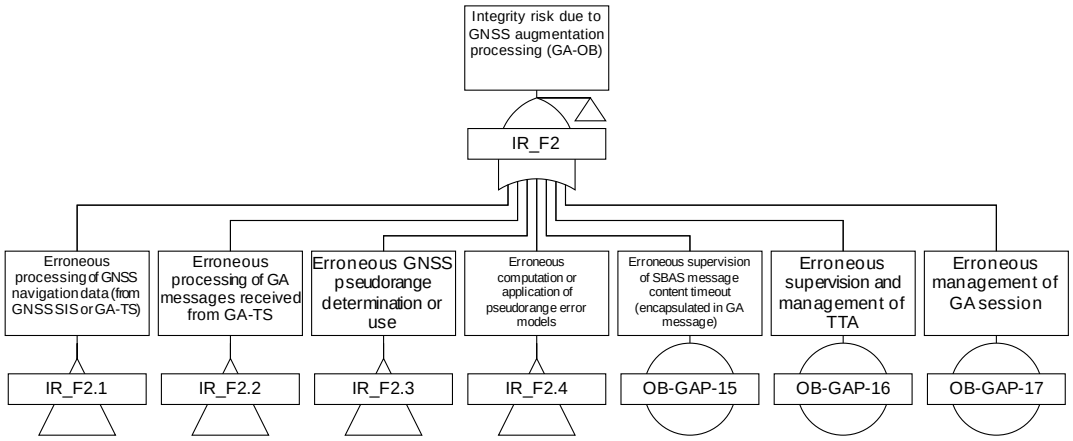


ID	Gate / Event	Description	Allocation (TFFR)	Estimated HR
IR_F1	Integrity risk due to on-board interface to GNSS SIS	Preliminary allocation to on-board GNSS measurement engine function SIL3: 1E-8 / hour ≤ TFFR < 1E-7 / hour	2.0E-8 / hour	2.0E-8 / hour
IR_F2	Integrity risk due to GNSS augmentation processing (GA-OB)	Preliminary allocation to GNSS augmentation processing function SIL4: 1E-9 / hour ≤ TFFR < 1E-8 / hour	1.0E-9 / hour	1.0E-9 / hour
TRANS-GA-OB	Safety-related radio transmission function (GA-OB)	Preliminary allocation to on-board safety-related radio transmission function SIL4: 1E-9 / hour ≤ TFFR < 1E-8 / hour	1.0E-9 / hour	1.0E-9 / hour
		Margin in allocation	3.0E-9 / hour	
GA-OB			2.5E-8 / hour	2.2E-8 / hour
		Margin (HR, GA-OB allocation)		3.0E-9 / hour

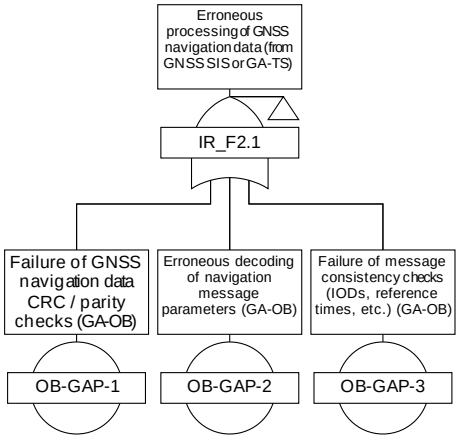
A.3.2 IR_F1: Integrity Risk Due to On-board Interface to GNSS SIS



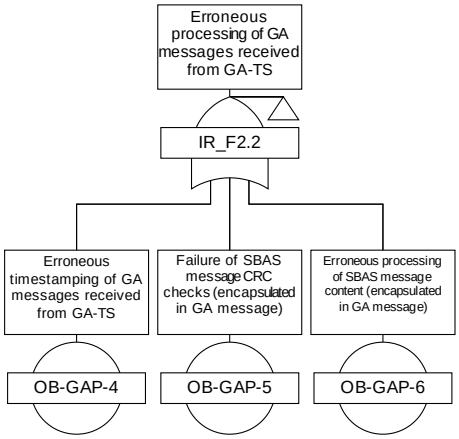
A.3.3 IR_F2: Integrity Risk Due to GNSS Augmentation Processing (GA-OB)



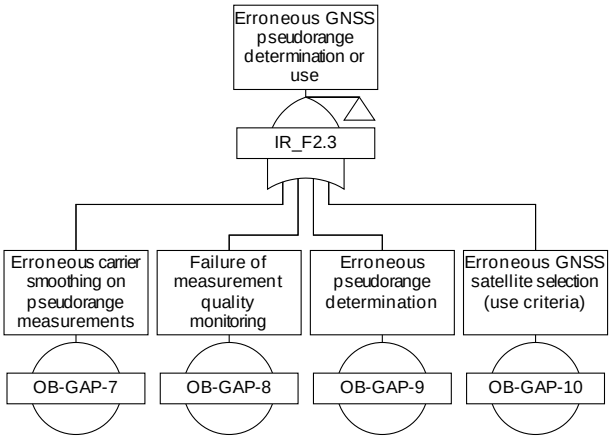
IR_F2.1: Erroneous processing of GNSS navigation data (from GNSS SIS or GA-TS)



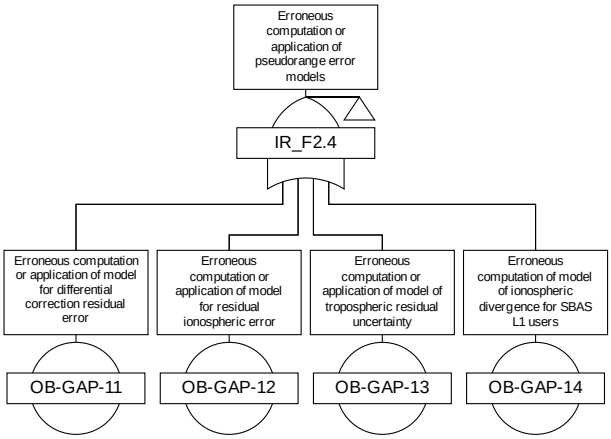
IR_F2.2: Erroneous processing of GA messages received from GA-TS



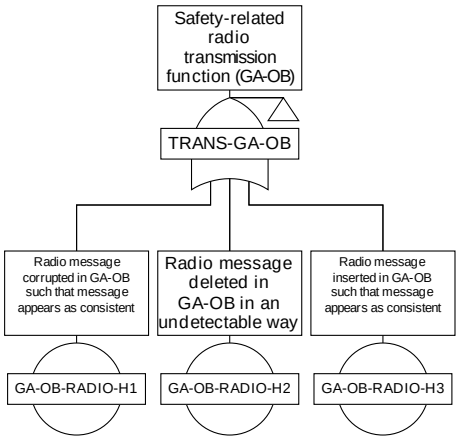
IR_F2.3: Erroneous GNSS pseudorange determination or use



IR_F2.4: Erroneous computation or application of pseudorange error models

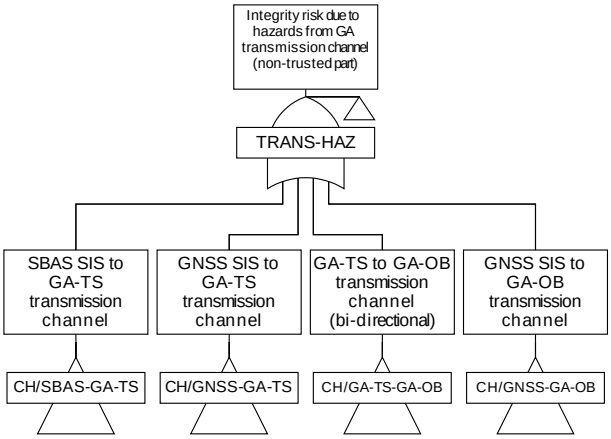


A.3.4 TRANS-GA-OB: Safety-related Radio Transmission Function (GA-OB)



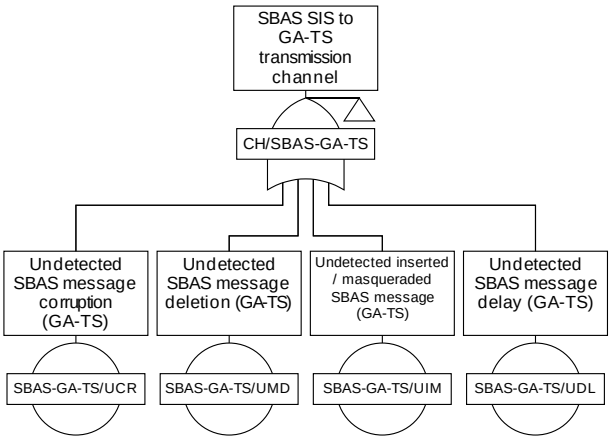
A.4 TRANS-HAZ: Integrity Risk due to Hazards from GNSS Augmentation Transmission Channel

A.4.1.1 This allocation addresses the non-trusted parts of the GA transmission channel.



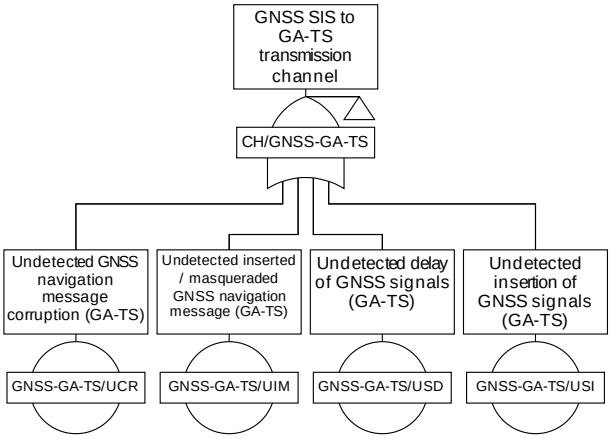
ID	Gate / Event	Description	Allocation (TFFR)	Estimated HR
CH/SBAS-GA-TS	SBAS SIS to GA-TS transmission channel	Preliminary allocation	6.0E-8 / hour	5.56E-8 / hour
CH/GNSS-GA-TS	GNSS SIS to GA-TS transmission channel	Preliminary allocation	1.0E-8 / hour	6.47E-9 / hour
CH/GA-TS-GA-OB	GA-TS to GA-OB transmission channel (bi-directional)	Preliminary allocation	2.0E-11 / hour	2.0E-11 / hour
CH/GNSS-GA-OB	GNSS SIS to GA-OB transmission channel	Preliminary allocation	8.0E-8 / hour	7.17E-8 / hour
		Margin in allocation	Nil	
TRANS-HAZ			1.5E-7 / hour	1.34E-7 / hour
		Margin (HR, TRANS-HAZ allocation)		1.62E-8 / hour

A.4.2 CH/SBAS-GA-TS: SBAS SIS to GA-TS Transmission Channel (non-trusted part)



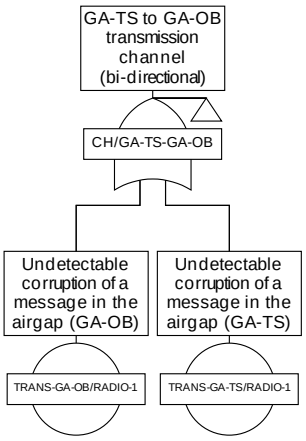
ID	Gate / Event	Description	Allocation (TFFR)	Estimated HR
SBAS-GA-TS/UCR	Undetected SBAS message corruption (GA-TS)	Preliminary allocation. Estimated hazard rates are based on the performance of error detection codes (e.g., CRCs). Refer to Section A.5.	5.5E-8 / hour	5.36E-8 / hour
SBAS-GA-TS/UMD	Undetected SBAS message deletion (GA-TS)	Deletion is detectable due to SBAS broadcasting a valid message every second to provide a continuity of signal	N/A	N/A
SBAS-GA-TS/UIM	Undetected inserted / masqueraded SBAS message (GA-TS)	Preliminary allocation to diagnostic function (considering availability of ground truth and no dynamics, TBC by analysis). Cyber-security barrier to be defined in next release of document.	1.0E-9 / hour	1.0E-9 / hour (TBC)
SBAS-GA-TS/UDL	Undetected SBAS message delay (GA-TS)	Preliminary allocation to diagnostic function (considering availability of ground truth and no dynamics, TBC by analysis). Cyber-security barrier to be defined in next release of document.	1.0E-9 / hour	1.0E-9 / hour (TBC)
		Margin in allocation	3.0E-9 / hour	
CH/SBAS-GA-TS			6.0E-8 / hour	5.56E-8 / hour
		Margin (HR, CH/SBAS-GA-TS allocation)		4.40E-9 / hour

A.4.3 CH/GNSS-GA-TS: GNSS SIS to GA-TS Transmission Channel (non-trusted part)



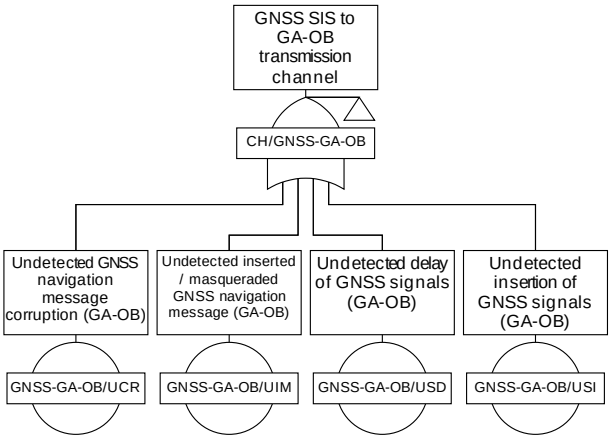
ID	Gate / Event	Description	Allocation (TFFR)	Estimated HR
GNSS-GA-TS/UCR	Undetected GNSS message corruption (GA-TS)	Preliminary allocation for undetected LNAV corruption for a maximum of 12 GPS satellites. Estimated hazard rates are based on the performance of error detection codes (e.g., CRCs). Refer to Section A.6.	2.5E-9 / hour	2.11E-9 / hour
		Preliminary allocation for undetected F/NAV corruption for a maximum of 12 Galileo satellites. Estimated hazard rates are based on the performance of error detection codes (e.g., CRCs). Refer to Section A.7.	2.5E-9 / hour	1.36E-9 / hour
GNSS-GA-TS/UIM	Undetected inserted / masqueraded GNSS navigation message (GA-TS)	Preliminary allocation to diagnostic function (considering availability of ground truth and no dynamics, TBC by analysis). Cyber-security barrier to be defined in next release of document.	1.0E-9 / hour	1.0E-9 / hour (TBC)
GNSS-GA-TS/USD	Undetected delay of GNSS signals (GA-TS)	Preliminary allocation to diagnostic function (considering availability of ground truth and no dynamics, TBC by analysis). Cyber-security barrier to be defined in next release of document.	1.0E-9 / hour	1.0E-9 / hour (TBC)
GNSS-GA-TS/USI	Undetected insertion of GNSS signals (GA-TS)	Preliminary allocation to diagnostic function (considering availability of ground truth and no dynamics, TBC by analysis). Cyber-security barrier to be defined in next release of document.	1.0E-9 / hour	1.0E-9 / hour (TBC)
		Margin in allocation	2.0E-9 / hour	
CH/GNSS-GA-TS			1.0E-8 / hour	6.47E-9 / hour
		Margin (HR, CH/GNSS-GA-TS allocation)		3.53E-9 / hour

A.4.4 CH/GA-TS-GA-OB: GA-TS to GA-OB Transmission Channel (non-trusted part)



ID	Gate / Event	Description	Allocation (TFFR)	Estimated HR
TRANS-GA-OB/RADIO-1	Undetectable corruption of a message in the airgap (GA-OB)	Preliminary allocation. Estimated hazard rates are based on the performance of error detection codes (e.g., CRCs). Refer to Section A.9.	1.0E-11 / hour	1.0E-11 / hour
TRANS-GA-TS/RADIO-1	Undetectable corruption of a message in the airgap (GA-TS)	Preliminary allocation. Estimated hazard rates are based on the performance of error detection codes (e.g., CRCs). Refer to Section A.9.	1.0E-11 / hour	1.0E-11 / hour
		Margin in allocation	Nil	
CH/GA-TS-GA-OB			2.0E-11 / hour	2.0E-11 / hour
		Margin (HR, CH/GA-TS-GA-OB allocation)		Nil

A.4.5 CH/GNSS-GA-OB: GNSS SIS to GA-OB Transmission Channel (non-trusted part)



ID	Gate / Event	Description	Allocation (THR)	Estimated HR
GNSS-GA-OB/UCR	Undetected GNSS message corruption (GA-OB)	Preliminary allocation for undetected LNAV corruption for a maximum of 12 GPS satellites. Estimated hazard rates are based on the performance of error detection codes (e.g., CRCs). Refer to Section A.6.	4.0E-8 / hour	3.80E-8 / hour
		Preliminary allocation for undetected F/NAV corruption for a maximum of 12 Galileo satellites. Estimated hazard rates are based on the performance of error detection codes (e.g., CRCs). Refer to Section A.7.	3.5E-8 / hour	3.27E-8 / hour
GNSS-GA-OB/UIM	Undetected inserted / masqueraded GNSS navigation message (GA-OB)	Preliminary allocation to diagnostic function (TBC by analysis). Cyber-security barrier to be defined in next release of document.	1.0E-9 / hour	1.0E-9 / hour (TBC)
GNSS-GA-OB/USD	Undetected delay of GNSS signals (GA-OB)	Outside boundary of pseudorange domain integrity commitments (GA for ERTMS/ETCS boundary) (i.e., cyber-security barrier to be addressed in LOC-OB perimeter)	N/A	N/A
GNSS-GA-OB/USI	Undetected insertion of GNSS signals (GA-OB)	Outside boundary of pseudorange domain integrity commitments (GA for ERTMS/ETCS boundary) (i.e., cyber-security barrier to be addressed in LOC-OB perimeter)	N/A	N/A
		Margin in allocation	4.0E-9 / hour	
CH/GNSS-GA-OB			8.0E-8 / hour	7.17E-8 / hour
		Margin (HR, CH/GNSS-GA-OB allocation)		8.30E-9 / hour

A.5 Quantification of Undetected SBAS Message Corruption

A.5.1.1 The following quantification is only an approximation as it assumes errors are independent, whereas errors are likely to occur in bursts due to the Viterbi detection of the convolutional code. While some of these assumptions may be reasonable for the trackside SBAS receiver, confirmation of BER with empirical data is highly recommended, especially for reception of SBAS messages by the GA-OB via the SBAS SIS (not currently defined but under consideration – to be addressed in a future revision of the SRS and SFHA).

A.5.1.2 A Bit Error Rate (BER) of 1E-6 is assumed for the trackside GNSS receiver considering a 500sps channel with ½ rate convolutional coding (250bps). SBAS messages are 250 bits, of which 24 bits are parity (CRC). Refer to Section A.8 for assumptions on the BER.

A.5.1.3 The probability of an error in an SBAS message (250 bits) given a BER of 1E-6 is:

$$1 - (1 - 1.00\text{E-}6)^{250} = 2.50\text{E-}4 \text{ per SBAS message}$$

A.5.1.4 Probability of erroneous SBAS message in an hour:

$$1 - (1 - 2.50\text{E-}4)^{3600} = 5.93\text{E-}1 \text{ / hour}$$

A.5.1.5 SBAS words are protected with a CRC-24Q, providing theoretical detection for single- and double-bit errors, any odd number of errors, and burst errors with length ≤ 24 bits per code word with a probability of 1. Large burst errors greater than parity length (b > 24) are detected with a probability of 2^{-24} if b > 25 bits or 2^{-23} if b = 25 bits. The assumed probability of undetected error ≤ 2^{-24} = 5.96E-8 for all channel bit error probabilities ≤ 0.5 [DO-229 A.4.3.3]

$$1 - (1 - (2.50\text{E-}4 \times 5.96\text{E-}8))^{3600} \approx 5.36\text{E-}8 \text{ / hour}$$

A.6 Quantification of GPS L1 LNAV Navigation Message Corruption

A.6.1.1 A Bit Error Rate (BER) of 1E-6 was considered a reasonable assumption for GPS L1 C/A considering demodulation performance of BPSK modulation without FEC and long symbols of 20ms (50bps data rate). Refer to Section A.8 for assumptions on the BER. While some of these assumptions may be reasonable for the trackside GNSS receiver, confirmation of BER with empirical data is highly recommended. As reception by GA-OB GNSS receivers is also foreseen, confirmation of BER with empirical data from representative railway environments is considered essential.

A.6.1.2 The GPS C/A frame is composed of 5 subframes of 300 bits; each subframe is composed of 10 words of 30 bits, of which 6 bits are parity.

A.6.1.3 The probability of an error in a word (30 bits) given a BER of 1E-6 is:

$$1 - (1 - 1.00E\text{-}6)^{30} = 3.00E\text{-}5 \text{ per word}$$

A.6.1.4 For SBAS provided integrity, only navigation data from subframes 1, 2 and 3 are used (i.e., GPS ionosphere model is not used). 20 words out of 50 in the frame are relevant, therefore probability of erroneous navigation data is calculated with respect to the 20 words.

A.6.1.5 The probability of erroneous navigation data (20 words) is:

$$1 - (1 - 3.00E\text{-}5)^{20} = 6.00E\text{-}4 \text{ per frame}$$

A.6.1.6 The GPS L1 C/A navigation message words are protected with an Extended Hamming Code (32,26), providing theoretical detection of up to 3 bits of error in a codeword with a probability of 1. The probability of errors not detected in a codeword = $2^{26}/2^{32}$ = 1.56E-2.

A.6.1.7 Therefore, the probability of an undetected error in a frame is:

$$1 - (1 - (3.00E\text{-}5 \times 1.56E\text{-}2))^{20} \approx 9.37E\text{-}6 \text{ per frame}$$

A.6.1.8 Considering that verified reception of a second frame is required prior to use of new data (requirement [DMS:249] in ED-259A), the residual risk of undetected error in frame data assuming uncorrelated errors between consecutive frames is:

$$(9.37E\text{-}6)^2 \approx 8.79E\text{-}11 \text{ per frame}$$

A.6.1.9 The following subsections consider two cases:

- LNAV data provided by the GA-TS at the Start of Mission (SoM); and
- LNAV clock and ephemeris data (CED) sets received from the GNSS SIS by the GA-OB / hour.

A.6.2 LNAV provided by GA-TS at Start of Mission

A.6.2.1 It is assumed that at Start of Mission (SoM) the GA-OB may request GNSS navigation data from the trackside to speed up the time to first fix (TTFF) if the GA-OB receiver is in cold start. It is assumed in the ETCS mission profile for conventional rail that there are two SoM procedures / hour [SS091] (note: for the high-speed rail profile, only one SoM procedure / hour is assumed).

A.6.2.2 A conservative assumption has been made that the GA-OB GNSS receiver does not have up to date GNSS navigation data on each train awakening. Therefore, GNSS navigation data is assumed to be provided by the trackside two times per hour. Considering the probability of an undetected error in a LNAV frame (with verified reception of a second frame), the navigation data corruption hazard rate / SV / hour is:

1.76E-10 / hour

A.6.2.3 Assuming one faulty measurement caused by navigation message corruption would lead to HMI in the PVT (i.e., not taking into consideration any additional barriers such as FD/FDE for detection of faulty measurements), the integrity risk due to undetected GPS LNAV corruption for at least one satellite in 12 GPS satellites is:

$$1 - (1 - 1.76E\text{-}10)^{12} \approx 2.11E\text{-}9 \text{ / hour}$$

A.6.3 LNAV CED sets received from the GNSS SIS by the GA-OB

A.6.3.1 DFMC SBAS MOPS assumes that there can be at most four F/NAV and at most three LNAV clock correction and ephemeris data sets for a single SV in any given interval of five minutes [ED-259A]. Therefore, in an hour it is assumed there can be at most 36 LNAV data sets for a single SV in an hour. Considering the probability of an undetected error in a LNAV frame (with verified reception of a second frame), the corruption hazard rate / SV is:

3.16E-9 / hour

A.6.3.2 A conservative assumption is made that one faulty measurement caused by navigation message corruption would lead to HMI in the PVT (i.e., not taking into consideration any additional barriers such as FD/FDE for detection of faulty measurements). Therefore, the integrity risk due to undetected GPS LNAV corruption for at least one satellite for a maximum of 12 GPS satellites is:

$$1 - (1 - 3.16E\text{-}9)^{12} \approx 3.80E\text{-}8 \text{ / hour}$$

A.7 Quantification of Galileo E5a F/NAV Navigation Message Corruption

A.7.1.1 The following quantification is only a preliminary approximation as it assumes errors are independent, whereas errors are likely to occur in bursts due to the Viterbi detection of the convolutional code. While some of these assumptions may be reasonable for the trackside GNSS receiver, confirmation of BER with empirical data is highly recommended. As reception by GA-OB GNSS receivers is also foreseen, confirmation of BER with empirical data from representative railway environments is considered essential.

A.7.1.2 A Bit Error Rate (BER) of 1E-6 is assumed considering a 50sps channel with ½ rate convolutional coding (25bps) and a block interleaver (61 $\times$ 8) on 488 symbols of the F/NAV page (500 symbols including 12-bit unencoded sync pattern) [GAL-OS-SIS-ICD]. F/NAV words are 238 bits (excluding 6-bit tail), of which 24 bits are parity (CRC). Note: assumptions on BER for F/NAV are to be confirmed in the next issue of this document.

A.7.1.3 The probability of an error in an F/NAV page (238 bits) given a BER of 1E-6 is:

$$1 - (1 - 1.00\text{E-}6)^{238} = 2.38\text{E-}4 \text{ per F/NAV page}$$

A.7.1.4 An F/NAV subframe consists of 5 pages; however, for SBAS provided integrity, only navigation data from page types 1, 2, 3 and 4 are relevant. Therefore, the probability of erroneous navigation data is calculated with respect to the 4 pages.

A.7.1.5 The probability of erroneous navigation data (4 pages) is:

$$1 - (1 - 2.38\text{E-}4)^{4} = 9.52\text{E-}4 \text{ per subframe}$$

A.7.1.6 F/NAV pages are protected with a CRC-24Q, providing protection against burst as well as random errors with a probability of undetected error $\leq 2^{-24} = 5.96\text{E-}8$ for all channel bit error probabilities ≤ 0.5.

A.7.1.7 Therefore, the probability of an undetected error in a subframe is:

$$1 - (1 - (2.38\text{E-}4 \times 5.96\text{E-}8))^{4} \approx 5.76\text{E-}11 \text{ per subframe}$$

A.7.1.8 The following subsections consider two cases:

- F/NAV data provided by the GA-TS at the Start of Mission (SoM); and
- F/NAV clock and ephemeris data (CED) sets received from the GNSS SIS by the GA-OB / hour.

A.7.2 F/NAV provided by GA-TS at Start of Mission

A.7.2.1 It is assumed that at Start of Mission (SoM) the GA-OB may request GNSS navigation data from the trackside to speed up the time to first fix (TTFF) if the GA-OB receiver is in cold start. It is assumed in the ETCS mission profile for conventional rail that there are two SoM procedures / hour [SS091] (note: for the high-speed rail profile, only one SoM procedure / hour is assumed).

A.7.2.2 A conservative assumption has been made that the GA-OB GNSS receiver does not have up to date GNSS navigation data on each train awakening. Therefore, GNSS navigation data is assumed to be provided by the trackside two times per hour. Considering the probability of an undetected error in an F/NAV subframe, the navigation data corruption hazard rate / SV / hour is:

$$1.13E\text{-}10 \text{ / hour}$$

A.7.2.3 Assuming one faulty measurement caused by navigation message corruption would lead to HMI in the PVT (i.e., not taking into consideration any additional barriers such as FD/FDE for detection of faulty measurements), the integrity risk due to undetected Galileo F/NAV corruption for at least one satellite in 12 Galileo satellites is:

$$1 - (1 - 1.13E\text{-}10)^{12} \approx 1.36E\text{-}9 \text{ / hour}$$

A.7.3 F/NAV CED sets received from GNSS SIS by the GA-OB

A.7.3.1 DFMC SBAS MOPS assumes that there can be at most four F/NAV and at most three LNAV clock correction and ephemeris data sets for a single SV in any given interval of five minutes [ED-259A]. Therefore, in an hour it is assumed there can be at most 48 F/NAV data sets for a single SV in an hour. Considering the probability of an undetected error in an F/NAV subframe, the navigation data corruption hazard rate / SV / hour is:

$$2.72E\text{-}9 \text{ / hour}$$

A.7.3.2 A conservative assumption is made that one faulty measurement caused by navigation message corruption would lead to HMI in the PVT (i.e., not taking into consideration any additional barriers such as FD/FDE for detection of faulty measurements). Therefore, the integrity risk due to undetected Galileo F/NAV corruption for at least one satellite in 12 Galileo satellites is:

$$1 - (1 - 2.72E\text{-}9)^{12} \approx 3.27E\text{-}8 \text{ / hour}$$

A.8 Assumptions on GNSS bit error rates (BER)

A.8.1.1 This section provides high-level initial justifications for assumptions on BER used in quantifying message corruption risk. This section will be improved in the next issue of the document and will include assumptions on Galileo E5a.

A.8.1.2 Table A-1 details minimum signal processing thresholds (C/N0 values that can be tolerated for aviation applications of GNSS) based on the minimum operational performance receiver signal processing model defined in Appendix D of DO235 [DO235, 2.5.2.2 & Appendix D].

Table A-1. GPS receiver minimum $C/N_{0,EFF}$ signal processing thresholds [DO235, Table 2-3]

Processing Mode	GPS	SBAS (WAAS)
Carrier tracking / data demodulation	29.93 dB-Hz	30 dB-Hz
1st satellite acquisition	32.4	N/A
2nd – 4th satellite acquisition	31.7	N/A

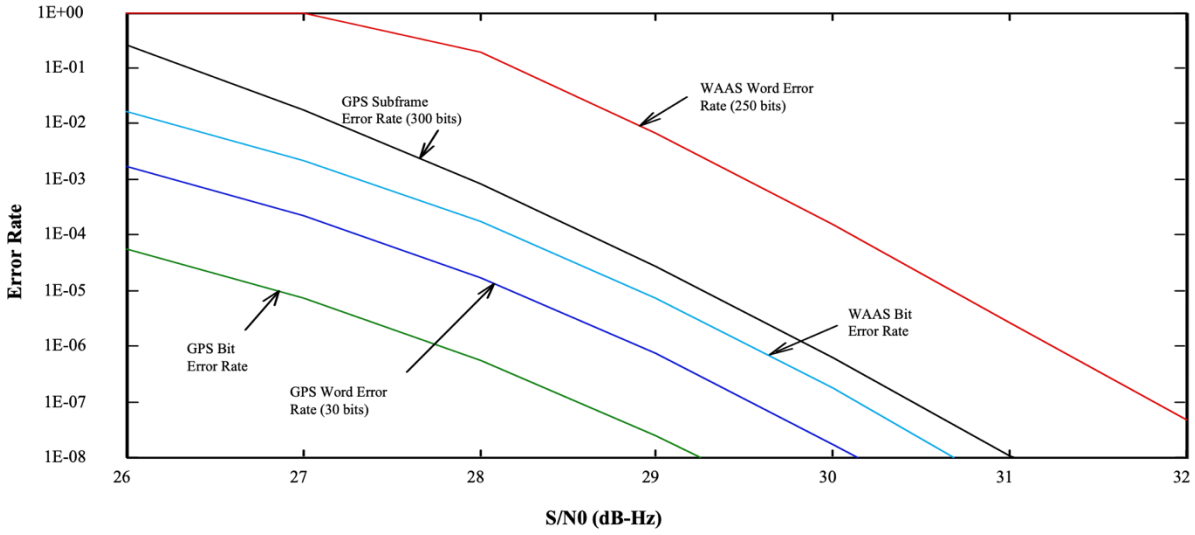


Figure A-1. GNSS bit and word error rates [DO235, Figure D-14]

A.8.1.3 Figure A-1 illustrates the probabilities of bit and word errors for GPS and SBAS as a function of $C/N_{0,EFF}$, where word error probabilities are approximated using:

$$P_w = 1 - (1 - P_b)^N$$

where N=32 for a GPS LNAV word,
N=300 for a GPS LNAV subframe, and
N=250 for a SBAS word

A.8.1.4 Note that the above approximation does not consider burst errors, which are likely to occur because of Viterbi detection of the convolutional code used in SBAS; the above approximation assumes bit errors are independent.

A.8.1.5 For GPS L1, based on the above plot and considering a minimum data demodulation signal processing threshold of 29.93 dB-Hz, a conservative BER of 1E-6 (corresponding to a C/N_0 of around 27.8 dB-Hz) is assumed with significant margin.

A.8.1.6 For SBAS L1, it is noted in [DO235, D.1.5] that to achieve an SBAS word error rate of 1E-3, a $C/N_{0,EFF}$ of around 29.5 dB-Hz is required. Based on the above plot and considering a minimum data demodulation signal processing threshold of 30 dB-Hz, a BER of 1E-6 (corresponding to a C/N_0 of around 29.5 dB-Hz, taking into account convolutional coding) is assumed with some margin.

A.9 Justification of safe radio connection message corruption hazard

A.9.1.1 It is assumed that the safe radio connection to be used for exchange of information between the GA-OB and GA-TS provides barriers against message level hazards that are at least as good as those specified for the EURORADIO protocol.

A.9.1.2 ETCS-OB05 – Corruption of radio messages [SS091]:

The requirement for the non-trusted part of OB-EUR-H4 is that the non-trusted ETCS on-board radio transmission equipment shall respect the definition of non-trusted as given in paragraph 5.1.1.6 and the THR of 1.0E-11 dangerous failures / hour.

A.9.1.3 ETCS-TR02 – Corruption of radio messages [SS091]:

The requirement for the non-trusted part of TR-EUR-H4 is that the non-trusted ETCS trackside radio transmission equipment shall respect the definition of non-trusted given in paragraph 5.1.1.6 and the THR of 1.0E-11 dangerous failures / hour.

A.9.1.4 In the apportionment of the THRs, it is assumed that the failure modes inside the equipment considered part of the non-trusted communication channel are protected by the safety code with respect to the corruption of messages.

Annex B Open Points to be Addressed in Future Iterations of the Analysis

B.1.1.1 The following table provides a list of open points related to the SFHA to be addressed in future iterations of the analysis. Many of these open points are to be addressed in work packages defined by ERJU/ERA/EUSPA/ESA/EUG addressing GNSS Augmentation for Rail based on EGNOS.

Table B-1. Open points list

Ref	Description	Solution / Workstream	Status / Notes
1	Cyber-attacks related to SBAS and GNSS signals received by the GA-TS are to be addressed in a future issue of the SFHA	To be confirmed	**Open.** Assessment of cybersecurity threats related to open SBAS transmission channel (SBAS SIS to GA-TS) and open GNSS transmission channel (GNSS SIS to GA-TS) to be performed.
2	Intentionally Removed		Combined with open point #3
3	Multi-disciplinary technical review of FMEA and FTA	To be confirmed	**Open.**
4	Assumptions on BER for computation of residual message corruption risk in Annex A	To be confirmed	**Open.** Activity to address confirmation of assumptions regarding BER, assumptions on bit error independence and burst errors, etc. for both trackside and on-board receivers. Possibly through analysis of empirical data from representative environments. As *residual risk of corruption* figures are based on assumptions including BER values, BER constraints need to be exported to MOPS once figures are consolidated.
5	Intentionally Removed		It was agreed not to define interfaces within GA-TS. Open point no longer applicable.
6	Intentionally Removed		It was agreed not to define interfaces within GA-TS. Open point no longer applicable.
7	Definition of requirements for Safe Radio Connection		**Closed.** Quantitative targets are no longer defined for non-trusted part of each transmission channel; a target is provided for the non-trusted part of the end-to-end transmission channel. In the preliminary THR apportionment, available margins for each transmission channel allocation are now made explicit. The allocation to the non-trusted part of GA-OB/GA-TS transmission channel for corruption risk is based on the performance of the CRC in Euroradio. This seems like a reasonable assumption; however, if a more relaxed allocation is sought, the available margin is known. Issue raised in review: In A.9 (justification of safe radio connection message corruption hazard) issue raised regarding assumption on Safe Radio Connection performance in terms of defences against message level hazards being at least as good as Euroradio. It was suggested that this was overly conservative, and requirements could be relaxed in the context of a relatively low top-level GA THR (i.e., ~ 5E-6 / hour).

8	Specification of requirements for trackside GNSS interference environment, guidelines for survey, etc.	To be confirmed	**Open.** To fulfil assumptions on BER for trackside, a standard interference environment will likely need to be defined with guidelines for conducting survey and ensuring compliance. If assessment on barriers for cyber-security threats demonstrates the need for a Position Domain Monitor (PDM), this may need to be extended to acceptance requirements for multipath environment in addition to in-band interference requirements (e.g., minimum effective C/N0 due to in-band interference for GNSS and SBAS signals) and out of band interference requirements (maximum interference level mask).

END OF DOCUMENT