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: 0f
Date: 10/06/2022

Modification History

Revision	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)

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 System 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 generic 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 an EGNOS railway safety of life (SoL) service.

1.1.1.3 The **purpose** of this document is to define generic 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 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:

- Functional fault-tree linking the failure modes identified in the causal analysis to the GA system hazard
- THR apportionment
- Safety target for system hazards
- Open points to be addressed in future iterations
- Trace of GATE58 minimal cut set SUBSET-88-2 Part 1

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]
- SBAS L1 Receiver Guidelines – On-board [ESSP-TN-25931]
- SBAS L1 Receiver Guidelines – Trackside [ESSP-TN-26038]
- SBAS DFMC Receiver Guidelines – On-board [ESSP-TN-26136]
- SBAS DFMC Receiver Guidelines – Trackside [ESSP-TN-26137]

[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 0d.” 2022.
[EUG-20E085]	EUG, “GNSS Augmentation for ERTMS/ETCS – System Requirement Specification. Version 0d.” 2022.
[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.
[ESSP-TN-25931]	ESSP, “SBAS L1 Receiver Guidelines for Railway – On-board Unit. Issue 01-00.” 2020.
[ESSP-TN-26038]	ESSP, “SBAS L1 Receiver Guidelines for Railway – Trackside Unit. Issue 01-00.” 2020.
[ESSP-TN-26136]	ESSP, “SBAS DFMC Receiver Guidelines for Railway – On-board Unit. Issue 01-00.” 2020.

[ESSP-TN-26137]	ESSP, “SBAS DFMC Receiver Guidelines for Railway – Trackside Unit. Issue 01-00.” 2020.
[DO229]	RTCA, “DO-229F – Minimum Operational Performance Standards for Global Positioning System/Satellite Based Augmentation System Airborne Equipment.” RTCA Inc., Washington D.C., USA, 2020.
[DO235]	Radio Technical Commission for Aeronautics, “Assessment of Radio Frequency Interference to the GNSS L1 Frequency Band”, Ref: DO-235B; 13/03/2008.
[ED259]	EUROCAE, “ED-259A (v0.12) – Minimum Operational Performance Standard for Galileo / Global Positioning System / Satellite-based Augmentation System Airborne Equipment.” Saint-Denis, France, 2022.
[IS-GPS-200]	GPS Directorate, “Interface Specification – NAVSTAR GPS Space Segment / Navigation User Segment User Interfaces – IS-GPS-200. Rev. M.” 2021.
[IS-GPS-705]	GPS Directorate, “Interface Specification – NAVSTAR GPS Space Segment / User Segment L5 Interfaces – IS-GPS-705. Rev. H.” 2021.
[GAL-OS-SIS-ICD]	European Commission, “European GNSS (Galileo) Open Service – Signal-in-Space Interface Control Document. Issue 2.0.” 2021.

1.3 Terms and Abbreviations

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

APDU	Application Protocol Data Unit
ATPE	Along-Track Position Error
ATPL	Along-Track Protection Level
CDF	Cumulative Distribution Function
CED	Clock and Ephemeris Data
CEI	Clock, Ephemeris, Integrity (data set)
CONOPS	Concept of Operations
CPF	Central Processing Facility
CRC	Cyclic Redundancy Check
CS	Circuit Switched
CSD	Circuit Switched Data
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)
EIRP	Effective Isotropic Radiated Power
ENT	EGNOS Network Time
ERA	European Union Agency for Railways (formerly European Railway Agency)
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
FFFIS	Form-Fit Functional Interface Specification
FDE	Fault Detection and Exclusion
FE	Feared Event
FIS	Functional Interface Specification
FMEA	Failure Modes and Effects Analysis
FRMCS	Future Railway Mobile Communication System
FTA	Fault Tree Analysis
GAD	GNSS Augmentation Dissemination
GEO	Geostationary Earth Orbit
GIVE	Grid Ionospheric Vertical Error
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSA	European GNSS Agency
GSM-R	Global System for Mobile Communications – Railway
HAL	Horizontal Alert Limit
HLDC	High Level Data Link Control
HMI	Hazardous Misleading Information
HPL	Horizontal Protection Level
HR	Hazard Rate
IC	Interoperability Constituent
IOD	Issue of Data
IODC	Issue of Data Clock
IODE	Issue of Data Ephemeris
IODF	Issue of Data Fast Corrections
IODG	Issue of Data used for matching MT39/40 pair in DFMC service
IODI	Issue of Data Ionospheric
IODN	Issue of Data Navigation Data (Galileo E1 I/NAV and E5a F/NAV)
IODM	Issue of Data Mask

IODP	Issue of Data PRN Mask
IODS	Issue of Data Service
IP	Internet Protocol
LPV	Localizer Performance with Vertical Guidance
MAC	Message Authentication Code
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
NPDU	Network Protocol Data Unit
NSDU	Network Service Data Unit
OBAD	Old But Active Data
OBU	On-Board Unit
OS	Open Service
PDM	Position Domain Monitor
PRN	Pseudo-Random Noise
PR	PseudoRange
PS	Packet Switched
PSD	Packet Switched Data
RAIM	Receiver Autonomous Integrity Monitoring
RBC	Radio Block Centre
RIMS	Range and Integrity Monitoring Stations
RSS	Root-Sum-Square
RTCA	Radio Technical Commission for Aeronautics
SaPDU	Safety Protocol Data Unit
SARPs	Standards and Recommended Practices
SBAS	Satellite Based Augmentation System

SDCM	System for Differential Corrections and Monitoring (SBAS developed by Russian Federation)
SDD	Service Definition Document
SIL	Safety Integrity Level
SIS	Signal in Space
SoL	Safety of Life
SoM	Start of Mission
SV	Satellite Vehicle
TBC	To Be Confirmed
TCP	Transmission Control Protocol
TEC	Total Electron Content
TFFR	Tolerable Function Failure Rate
THR	Tolerable Hazard Rate
TPDU	Transport Protocol Data Unit
TTA	Time To Alert
UDRE	User Differential Range Error
UDREI	User Differential Range Error Indicator
UIRE	User Ionospheric Range Error
UIC	Union Internationale des Chemins de fer (international union of railways)
UNIFE	Union des Industriels Ferroviaires Européennes (union of European railway industries)
UTC	Universal Time Coordinate
VAL	Vertical Alert Limit
VPL	Vertical Protection Level
WAAS	Wide Area Augmentation System (SBAS developed by the USA)
xAL	Horizontal or Vertical Alert Limit
xPL	Horizontal or Vertical Protection Level

2 Approach for the 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 from CENELEC EN 50126 and EN 50129 [EN50126, EN50129].

Phase	How phase is addressed in this document	Document section
RISK ASSESSMENT		
1. System definition	Including the functions and interfaces defined for the GA for ERTMS/ETCS	Section 3
2. Risk Analysis		
2.1. Hazard identification	Identification of hazards at GA system level	Section 0
2.2. Consequence analysis (analysis of the consequences, losses)	Linking of hazards at GA boundary to ETCS subsystem level hazardous events. The linking of subsystem level hazardous events to ETCS system level hazards is defined in SUBSET-088, which is used to establish the link between GA system level hazards and the ETCS Core Hazard.	Section 4.3
3. Risk evaluation	This phase involves derivation of THRs for GA system hazards. Determination of THRs is based the achievable performance of GNSS augmentation systems (i.e., SBAS) given that the intention is to leverage existing GNSS augmentation assets (e.g., the use of EGNOS in Europe). Furthermore, it is not possible to determine THRs with a top-down approach given that requirements for the EVLF and its integration in ETCS are not defined. Risk tolerability is not addressed directly; however, it is assumed that any EVLF implementation would need to meet application-level requirements for integration in ETCS, which would implicitly need to ensure the resulting risk of the ETCS Core Hazard does not exceed the defined THR.	Section 4.4
HAZARD CONTROL		
4. Hazard analysis (causal analysis)	Evaluation of the possible causes of hazards (technical failures) through the application of a functional FMEA and linking identified hazardous events to the GA top-level hazards through fault-tree analysis.	Section 5, Annex A
5. Determination of TFFRs and SILs	Apportionment of THRs for GA top-level hazards down to the determination of TFFRs and allocation of SILs.	Annex B
6. Safety requirements	Specification of safety requirements for technical interoperability of GA for ERTMS/ETCS	Section 7

3 GNSS Augmentation System Description

3.1 High-level Architecture for Safety Analyses

3.1.1.1 Figure 3-1 illustrates the reference functional architecture for GNSS augmentation in ERTMS/ETCS for the purpose of conducting the safety analyses. The architecture only focuses 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 enhanced onboard localisation equipment.

Note: it is not the purpose of this architecture to indicate a physical architecture or pre-determine where functions are allocated.

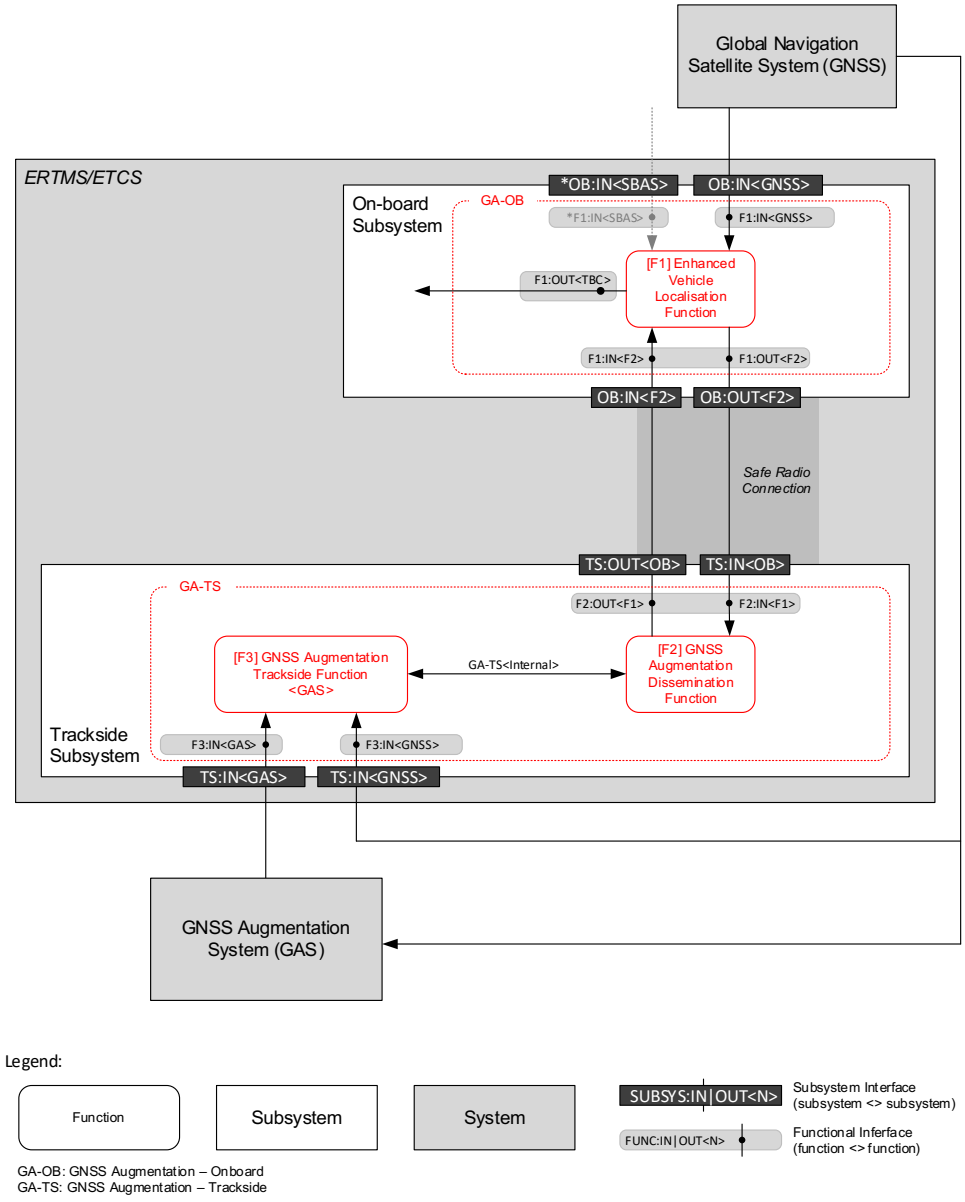


Figure 3-1. GNSS Augmentation Reference Functional Architecture for ERTMS/ETCS (Interfaces)

3.1.1.2 The Enhanced Vehicle Localisation Function (EVLF) utilises GNSS augmentation to improve position accuracy and derive a statistical bounding (at the required level of confidence) on position errors

through the application of corrections and residual pseudorange error models. The GNSS receiver implemented within the EVLF shall implement the specific Minimum Operational Performance Standards (MOPS) of the GNSS augmentation service, which addresses requirements on GNSS signal and message processing, the specificities of GAS message processing and computation of pseudorange error bounds for the specific GNSS augmentation type and service (e.g., EGNOS Legacy and DFMC Railway SoL Services[2]). In addition to reception of GNSS augmentation information via the trackside, the EVLF may have an interface supporting direct reception of SBAS messages via the SBAS GEO SIS; however, principles for use of this interface are not currently defined in the current SRS (version 0f) and will be addressed in a future release. It should be noted that information from EGNOS received by the EVLF via the GADF and via the SBAS GEO SIS cannot be mixed in a single GNSS processing channel.

3.1.1.3 The GNSS Augmentation Dissemination Function (GADF) is responsible for the dissemination of GA messages containing correction and integrity information to the EVLF. The GADF can also provide GNSS navigation data to the EVLF to support faster start-up time, especially in difficult start-up environments (e.g., where there is significant obscuration of GNSS satellites).

3.1.1.4 The GNSS Augmentation Trackside Function (GATF) is responsible for the interface between the GNSS Augmentation Trackside (GA-TS) and the GNSS Augmentation System (GAS). The GATF timestamps and encapsulates GA messages in GAM packets, leaving the in-built message protections (e.g., CRC) intact. While the GA-TS performs some message processing (e.g., in support of maintaining active data sets), by encapsulating GA messages, the complexity of the function is greatly reduced, and assumptions related to inbuilt defences against message-level hazards that are assumed by the GNSS augmentation service and its respective integrity commitments are maintained.

Some additional GA message processing may also be allocated to the GATF to reduce the amount of data to be transferred to the GA-OB without impacting its ability to apply models for degradation of data. For example, in the case of the SBAS Legacy service, the GATF could reduce the quantity of information related to ionospheric corrections to be transferred to the GA-OB by only providing the vertical delays and errors (GIVEs) for relevant Ionospheric Grid Points (IGPs).

The GATF is also responsible for obtaining navigation data from the Global Navigation Satellite System (GNSS), which is repackaged in packets optimised to provide essential CED parameters to the EVLF. This includes GNSS navigation data for constellations supported by the GAS (e.g., for EGNOS: GPS L1, L5; Galileo E1-B/C, E5a).

3.1.2 Basic Functions

3.1.2.1 Enhanced Vehicle Localisation Function (EVLF) [GA-relevant functionality only]

- Reception of GA messages from GADF
- Reception of GA active data sets[3] from GADF
- Reception of GNSS navigation data from GADF
- Transmission and reception of GA session management messages and acknowledgements

[2] For MOPS addressing EGNOS legacy and DFMC railway SoL services for the EVLF, refer to [ESSP-TN-25931] and [ESSP-TN-26136].

[3] Active data sets are sets of GA messages containing data that is valid (i.e., has not yet timed out). Reception of an active data set consisting of last received valid GA messages by the trackside reduces the amount of time needed before a valid combination of active data is available to the EVLF.

- Timestamping of GA messages received from GADF[4]
- Supervision and management of TTA
- Supervision of GA message content timeout
- GA message processing
- GNSS signal processing
- GNSS pseudorange determination and use
- Computation and application of GA corrections to smoothed pseudorange
- Computation and application of GNSS pseudorange error models

Note: EVLF functionality related to reception of SBAS messages from the SBAS GEO SIS via OB:IN<SBAS> is not addressed in this document and will be addressed in a future release.

3.1.2.2 GNSS Augmentation Dissemination Function (GADF)

- Transmission of GA message steams to EVLF
- Transmission of GA active data sets to EVLF
- Transmission of GA active alerts to EVLF
- Transmission of GNSS navigation data sets to EVLF
- Transmission and reception of GA session management messages and acknowledgements
- Reception of GA messages from GATF
- Reception of GA active data sets from GATF
- Reception of GA active alerts from GATF
- Reception of GNSS navigation data sets from GATF
- Transmission and reception of GADF-GATF session management messages and acknowledgements
- Selection of GA service and channel compatible with services supported by EVLF
- Resumption of suspended GA message streams

3.1.2.3 GNSS Augmentation Trackside Function (GATF)

- Reception of GA messages from GAS
- Transmission of GA messages to GADF for each service / GAC
- Transmission of requested GA active data sets to GADF
- Transmission of requested GNSS navigation data sets to GADF
- Transmission and reception of GADF-GATF session management messages and acknowledgements

[4] Note that is the timestamping of GA messages received at the EVLF from the GADF. This timestamp is in the same reference time indicated by the qualifier Q_GAT within the GAM Packet [EUG-20E087], In the case of SBAS, the reference time would be SBAS Network Time (SNT). It should be noted that this timestamp is different from T_TRAIN (time according to trainborne clock at which message is sent) provided in messages exchanged between the GA-OB and GA-TS, where T_TRAIN is used for message consistency checks.

- Selection of GACs
- Maintain GA active data set for each GAC
- Maintain GA active alerts for each GAC
- Timestamping reception of messages from GAS[5]
- Encapsulation of messages received from GAS in GAM packets
- Maintain GNSS navigation data sets
- GNSS signal processing
- Processing of GAS messages to support GATF functions

3.1.3 Interfaces

3.1.3.1 Functional interfaces:

Interface 'F1 ↔ F2'	Functional interface between the EVLF and GADF. The ICD for GA-OB / GA-TS [EUG-20E087] defines interoperability-relevant messages, packets and variables exchanged over the Safe Radio Connection (airgap).
Interface 'F2 ↔ F3'	Functional interface between the GADF and GATF. A standardized interface has not been deemed necessary as this interface is not considered relevant for interoperability.

3.1.3.2 External standardised interfaces:

Interface 'OB:IN<GNSS>'	Interface between the GA-OB (EVLF) and the Global Navigation Satellite System (GNSS) via the SIS. This includes GNSS constellations supported by the GNSS Augmentation System (e.g., for EGNOS; GPS L1, L5; Galileo E1-B/C, E5a).
Interface 'TS:IN<GAS>'	Interface between the GA-TS (GATF) and the GNSS Augmentation System (GAS).
Interface 'TS:IN<GNSS>'	Interface between the GA-TS (GATF) and GNSS. This includes GNSS constellations supported by the GAS (e.g., for EGNOS; GPS L1, L5; Galileo E1-B/C, E5a).

3.1.3.3 External interfaces for EGNOS-based GA:

Interface 'OB:IN<SBAS>'	**[Not currently defined]** interface between GA-OB (EVLF) and the SBAS SIS (L1 Legacy and L5 DFMC). To be addressed in a future release.
Interface 'TS:IN<SBAS>'	Interface between the GA-TS (GATF) and EGNOS via the SBAS SIS.

[5] This is the timestamping of messages received at the GATF from the GAS encapsulated within a GAM Packet (Packet 212) [EUG-20E087], where the timestamp (T_GAM) is in the reference time indicated by the qualifier Q_GAT within the GAM Packet. In the case of SBAS, the reference time would be SBAS Network Time (SNT). It should be noted that this timestamp is different from T_TRAIN (time according to trainborne clock at which message is sent) provided in messages exchanged between the GA-OB and GA-TS, where T_TRAIN is used for message consistency checks. For this reason, it is possible for the EVLF to receive a GA message that passes message consistency checks without a valid T_GAM.

3.1.3.4 This document provides safety analyses for the EGNOS-specific GNSS Augmentation Trackside Function (GATF) in addition to generic functions. Figure 3-2 illustrates the reference functional architecture with GNSS augmentation based on EGNOS (reception via the SBAS SIS).

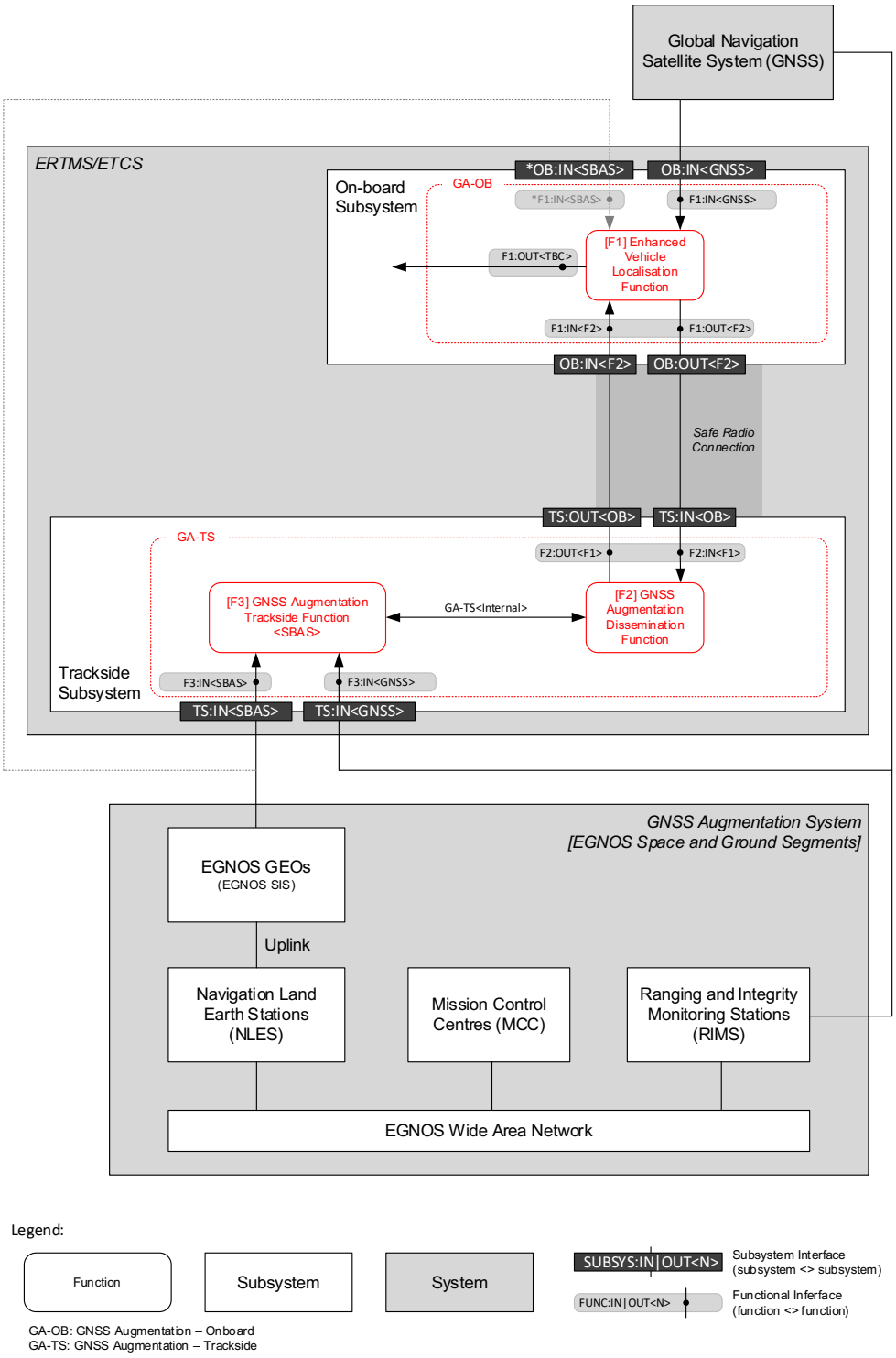


Figure 3-2. GNSS Augmentation Functional Reference Architecture with EGNOS-based GA

4 Hazard Identification

4.1.1.1 A structured hierarchical approach is taken for the identification of hazards at different boundaries:

- Boundary of the ERTMS/ETCS system;
- Boundary of the enhanced vehicle localisation function (EVLF); and
- Boundary of the GA framework for ERTMS/ETCS.

4.1.1.2 As there is currently no defined architecture for ERTMS/ETCS with the EVLF, for the scope of the analysis hazards identified at the boundary of the GA framework for ERTMS/ETCS are linked to relevant hazards at the ERTMS subsystem level, considering an enhanced vehicle localisation function using GNSS and the GA framework for ERTMS/ETCS for determination of the train position. The ERTMS safety analyses from [SS088-2 Part 1] are used to establish the link between relevant ERTMS/ETCS subsystem hazards and system hazards (specifically the ETCS Core Hazard).

4.1.1.3 The GA reference functional architecture (Figure 3-1) illustrates a system of systems, with the GA for ERTMS/ETCS interfacing to GAS and GNSS systems. Hazards of the GAS and GNSS systems are outside the defined system and therefore not within the scope of this analysis.

4.1.1.4 It should be noted the scope of this analysis is not to build a complete fault-tree, but rather support the preliminary safety analyses.

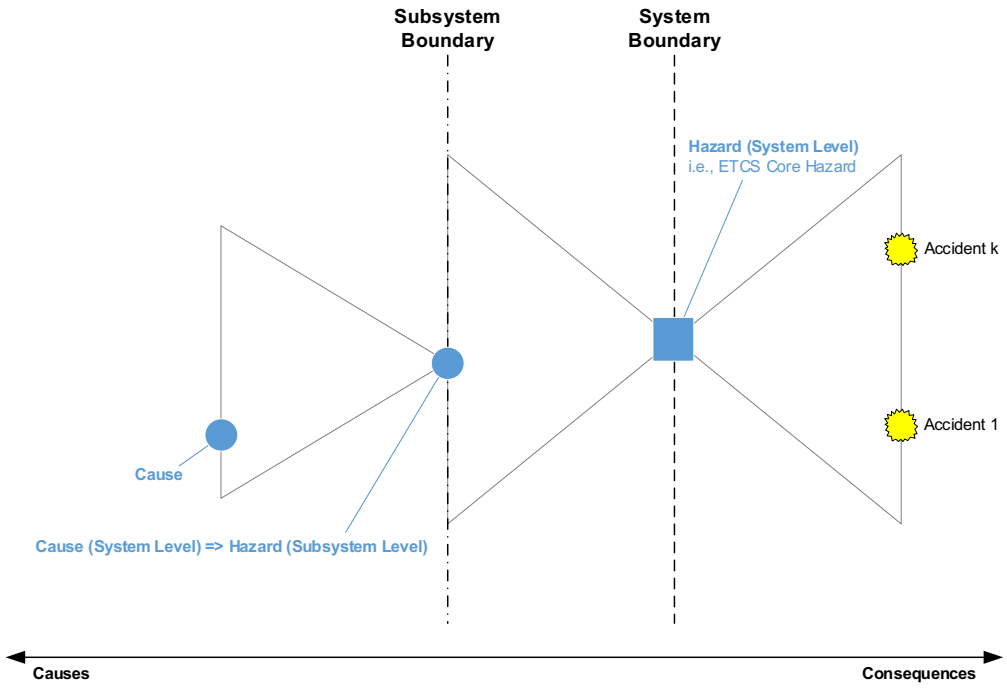


Figure 4-1. Identification of hazards at different boundaries [EN50129]

4.2 Identified Hazards

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 (ETCS Core Hazard)
System boundary	System level hazard at the boundary of the ERTMS/ETCS system
Remarks	ETCS system hazard is defined in [SS091]

ID	EVLF/IDTP
	Incorrect determination of train position
System boundary	Top-level hazard at the boundary of the enhanced vehicle localisation function (Interface F1:OUT<TBC>)
Remarks	Incorrect determination of train position includes train confidence interval not including the real position of the train.

ID	PRIR
Hazard	Pseudorange integrity risk (correction residual or ionospheric vertical error not bound and TTA > T_NVGAMAXTTA)
System boundary	Top-level hazard at the boundary of the GA for ERTMS/ETCS
Remarks	GA for ERTMS/ETCS is comprised of GA-OB and GA-TS

4.3 Hazardous Events at Subsystem Level and Link to ETCS Core Hazard

4.3.1.1 The GA for ERTMS/ETCS SRS addresses interoperability-relevant requirements that enable the use of GNSS augmentation in a technology-neutral manner. The EVLF is only defined to the extent needed for supporting GA-OB functions. Integration of the EVLF within ETCS is not defined, and as such, the specifications do not address the link between EVLF hazards and the ETCS Core Hazard.

4.3.1.2 The intermediate EVLF hazard, *IDPT: Incorrect determination of train position*, is considered equivalent to GATE58 in the ERTMS/ETCS functional fault tree [SS088-2 Part 1]. GATE58 can be considered sufficiently abstracted from the specificities of ETCS train positioning based on odometry and the balise transmission system, thus providing link from EVLF-based train position determination to the ETCS Core Hazard. Note: the link of EVLF/IDPT with GATE58 is limited to supporting the FMEA and assessment of the severity of failure effects. The link between GATE58 and the ETCS Core Hazard is illustrated in the trace of the GATE58 minimal cut set from the ERTMS/ETCS functional fault tree [SS088-2 Part 1], provided in Annex D. This illustrates the pathways for how hazardous events causing GATE58 can propagate to the ETCS Core Hazard.

4.3.1.3 It is assumed that the GA hazard PRIR: Pseudorange integrity risk (correction residual or ionospheric vertical error not bound and TTA > T_NVGAMAXTTA) is a cause for the hazard EVLF/IDPT (equivalent to GATE58). Although a very conservative assumption is made that a violation of integrity in the pseudorange domain would result in a violation of integrity in the position domain with a probability of 1, it should be emphasized that improvements to integrity performance at user level using sensor fusion, digital map integration (i.e., reducing to along-track errors only), etc. have not been taken into consideration in this analysis.

4.4 THR for GA Hazard *PRIR: Pseudorange integrity risk*

4.4.1.1 In the case of the GA for ERTMS/ETCS, it is not possible to apply a top-down approach for the derivation of safety requirements (i.e., THRs and SILs) as requirements for the enhanced vehicle localisation function (EVLF) and its integration within ETCS are not defined. Therefore, a bottom-up approach is considered.

4.4.1.2 Determination of THRs is based the achievable performance of GNSS augmentation systems (i.e., SBAS) given that the intention is to leverage existing GNSS augmentation assets (e.g., the use of EGNOS in Europe).

4.4.1.3 The proposed integrity requirements for the Railway SoL Service are consistent with integrity performances provided by SBAS to support aviation CAT-I precision approach (integrity risk = 2E-7 in any approach (150s), TTA = 6s).

4.4.1.4 Precision approach services are associated with the most stringent level of integrity performance that is provided by the current and next generation of SBAS (i.e., EGNOS V3). While non-precision approach (NPA) meets a higher level of integrity in the position domain (integrity risk = 1E-7 / hour, TTA = 10s, with an alert limit of 556m), NPA integrity is not committed by EGNOS in the pseudorange domain as all the barriers are designed against the Precision Approach services (i.e., for NPA service, the case of position domain impact analysis needs to be explicitly addressed[6]).

4.4.1.5 In EGNOS for Precision Approach services, although integrity commitments are made in the position domain, a conservative assumption is made that under fault-free conditions a violation of integrity in the pseudorange domain would result in a violation of integrity in the position domain with a probability of 1; therefore,

- an integrity risk allocation of 1E-7/150s is allocated to bounding of residual errors in the pseudorange domain under fault-free conditions (i.e., no extreme ionosphere / scintillation conditions; includes ground station nominal multipath, interference, cycle slips, etc.); and
- another allocation of 1E-7/150s is made for detection of fault conditions (i.e., presence in the system of any feared events or any events beyond the defined fault-free conditions).

4.4.1.6 As the railway SoL service would provide commitments in the pseudorange domain (i.e., pseudorange domain integrity service), pseudorange integrity risk is considered in terms of:

- *pseudorange error bound integrity risk*, i.e., bounded residual correction and vertical ionospheric errors; and
- *SIS / ground integrity risk*, i.e., detection and exclusion of fault conditions that are not bounded.

4.4.1.7 For railway applications, the integrity risk of 2E-7 / 150s is translated to a one-hour exposure time. The justification for this exposure period is related to safety analyses and the apportionment to constituents in the European Train Control System (ETCS), which is undertaken against a definition of the role of that constituent and its related hazards in a representative one-hour journey.

4.4.1.8 There are 24 × 150 second periods in one hour, resulting in an integrity requirement of 4.8E-6 / hour, equally allocated between pseudorange error bound integrity risk (fault-free) and SIS / ground integrity risk.

[6] In EGNOS V2, NPA was assessed using Monte Carlo simulation and extrapolation of a conservative value for the probability of a pseudorange error propagating to the position domain of 1/100. For EGNOS V3 a different approach is being considered.

4.4.2 Pseudorange error bound integrity risk for GA based on SBAS

4.4.2.1 The allocation of 2.4E-6 / hour to *pseudorange error bound integrity risk* relates to the level of confidence for bounding of residual clock / ephemeris and ionosphere errors (guaranteed in all feared event cases).

4.4.2.2 The residual errors for pseudorange measurements for fault-free satellites are modelled by root-sum-squaring the error components (under the assumption of zero-mean normal distributions).

$$\sigma_i = \sqrt{\sigma_{i,CRE}^2 + \sigma_{i,iono}^2}$$

Where:

$\sigma_{i,CRE}^2$ is the variance of the correction residual error for satellite i:

- For SBAS L1 Legacy service, $\sigma_{i,CRE}^2$ is the model variance for the residual error when SBAS corrections (long term, fast and range rate) are applied, and the degradation model is used (i.e., $\sigma_{i,CRE}^2 = \sigma_{i,flt}^2$).

$$\sigma_{i,flt}^2 = \begin{cases} \left[\left(\sigma_{i,UDRE}\right) \cdot (\delta UDRE) + \varepsilon_{fc} + \varepsilon_{rrc} + \varepsilon_{ltc} + \varepsilon_{er}\right]^2, & \text{if } RSS_{UDRE} = 0 \\ \left[\left(\sigma_{i,UDRE}\right) \cdot (\delta UDRE)\right]^2 + \varepsilon_{fc}^2 + \varepsilon_{rrc}^2 + \varepsilon_{ltc}^2 + \varepsilon_{er}^2, & \text{if } RSS_{UDRE} = 1 \end{cases}$$

  The system ensures that the UDRE it broadcasts bounds the ephemeris and clock residuals for a compliant user using any valid combination of active data broadcast by the system.

- For SBAS L5 DFMC service, $\sigma_{i,CRE}^2$ is the model variance for the residual error after application of SBAS dual-frequency corrections (i.e., $\sigma_{i,CRE}^2 = \sigma_{i,DFC}^2$).

$$\sigma_{i,DFC}^2 = \begin{cases} (\sigma_{DFRE} \cdot \delta_{DFRE})^2 + \varepsilon_{CORR}^2 + \varepsilon_{ER}^2, & \text{if } DES = 0 \\ (\sigma_{DFRE} + \varepsilon_{CORR} + \varepsilon_{ER})^2 \cdot \delta_{DFRE}^2, & \text{if } DES = 1 \end{cases}$$

  (Note that $\varepsilon_{ER}^2 = 0$ for LP/LPV operations, on which railway service is based)

  The system ensures that the DFRE it broadcasts bounds the ephemeris and clock residuals for a compliant user using any valid combination of active data broadcast by the system.

$\sigma_{i,iono}^2$ is the variance of the residual ionospheric error for satellite i:

- For SBAS L1, $\sigma_{i,iono}^2$ is the model variance for the slant range ionospheric error when applying SBAS L1 ionospheric corrections (i.e., $\sigma_{i,iono}^2 = \sigma_{i,UIRE}^2$).

  The system provides users with vertical delays (relative to an L1 signal) and their accuracy (σ_{GIVE}^2's) at geographically defined ionospheric grid points (IGPs). These vertical delays and the evaluated σ_{GIVE}^2's are interpolated by the user to the ionospheric pierce point (IPP) of the observed satellite. This computed vertical delay and the associated σ_{UIVE}^2 (model variance for user ionospheric vertical error computed from associated σ_{GIVE}^2's) must then be multiplied by the obliquity factor computed from the elevation angle to the satellite to obtain a slant range correction and the slant range correction error (σ_{UIRE}^2).

$$\sigma_{UIRE}^2 = F_{pp}^2 \cdot \sigma_{UIVE}^2$$

$$\sigma_{UIVE}^2 = \sum_{n=1}^{4\ or\ 3} W_n\left(x_{pp}, y_{pp}\right) \cdot \sigma_{n,ionogrid}^2$$

$$\sigma^2_{ionogrid} = \begin{cases} (\sigma_{GIVE} + \varepsilon_{iono})^2, & \text{if } RSS_{iono} = 0 \\ \sigma^2_{GIVE} + \varepsilon^2_{iono}, & \text{if } RSS_{iono} = 1 \end{cases}$$

The system ensures that the GIVE it broadcasts bounds the ionosphere residuals for a compliant user using any valid combination of active data broadcast by the system.

- For SBAS DFMC, $\sigma^2_{i,iono}$ is the model variance describing the residual ionospheric error (including ionospheric higher-order effects, ray bending and excess TEC) when applying the ionosphere-free dual-frequency L1/L5 combination (i.e., $\sigma^2_{i,iono} = \sigma^2_{i,UIRE}$).

  $\sigma_{\mathrm{UIRE}}[\mathrm{i}] = \frac{40.0}{261.0+\mathrm{El}^2_{\mathrm{deg}}[\mathrm{i}]} + 0.018$ and $\mathrm{El}_{\mathrm{deg}}[\mathrm{i}]$ is the elevation angle in degrees of satellite i

4.4.3 SIS / ground integrity risk for GA based on SBAS

4.4.3.1 The allocation of 2.4E-6 / hour to *SIS / ground integrity risk* relates to the detection of fault conditions (i.e., presence in the system of any feared events or any events beyond the defined fault-free conditions). An example of external feared events includes:

- Loss of SV SIS healthy status
- Signal distortion (evil waveform)
- SV code carrier incoherency
- Pseudorange step error
- Pseudorange drift error
- Pseudorange acceleration error
- SV hardware bias jump
- SV hardware bias drift
- Erroneous broadcast ephemeris (orbits)
- Erroneous broadcast clocks
- Erroneous navigation message
- IOD anomaly
- Degraded carrier phase
- Degraded EIRP

4.4.4 THR allocation

4.4.4.1 Based on the current achievable performances, a THR of 5.0E-6 / hour is allocated taking into consideration EGNOS railway SoL service integrity performance of 4.8E-6 / hour and an additional 2.0E-7 allocation to functions and transmission channel hazards related to the GA framework for ERTMS/ETCS.

PRIR	**Pseudorange integrity risk THR**

	The hazard rate for the GA top-level hazard, *pseudorange integrity risk (correction residual or ionospheric vertical error not bound and TTA > T_NVGAMAXTTA)*, shall not exceed a THR of: 5.0E-6 dangerous failures / hour

4.4.4.2 In the case of an alert condition, integrity is ensured with a reactive fail-safe design. An alert condition occurs when the GAS has erroneously broadcast integrity data not bounding the residuals (i.e., orbit and clock correction and ionosphere residual errors) at the required confidence level.

4.4.4.3 The THR includes the Time to Alert (TTA), which is the time elapsed from the onset of the alert condition to its detection and negation in the EVLF.

5 Hazard Analysis (Causal Analysis) Approach

5.1.1.1 The objective of the hazard analysis is to evaluate the possible causes (technical failures) of GA top-level hazards based on the GNSS augmentation reference functional architecture and application of a functional FMEA.

5.1.1.2 This section provides an overview of the approach taken including identification of macro function data items, 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 functional FMEA is carried out on the basic functions and data items of the macro functions of the reference GA system. Macro function data items are identified for functions relating to reception and transmission of messages.

#	Macro Function	Basic Function	Functional Interface	Direction	Data Item	Details / Remarks
F1.1	Enhanced Vehicle Localisation Function	Reception of GA messages from GADF	F1:IN<F2>	F2 → F1	GA messages (Q_GAMT = 0, Nominal GA messages)	Encapsulating Legacy and DFMC SBAS MTs
			F1:IN<F2>	F2 → F1	GA messages (Q_GAMT = 1, GA alert messages)	Encapsulating Legacy and DFMC SBAS alert sequence MTs
			F1:IN<F2>	F2 → F1	GA messages (Q_GAMT = 2, DNU GA message stream)	Includes SBAS MT0
F1.2	Enhanced Vehicle Localisation Function	Reception of GA active data sets from GADF	F1:IN<F2>	F2 → F1	GA messages (Q_GAMT = 0, Nominal GA messages)	Set of Legacy or DFMC SBAS MTs with message content that is valid (i.e., has not timed out)
F1.3	Enhanced Vehicle Localisation Function	Reception of GNSS navigation data from GADF	F1:IN<F2>	F2 → F1	GNSS navigation data sets	GPS L1 LNAV and Galileo E5a F/NAV. GPS L5 CNAV and Galileo E1B I/NAV for possible degraded modes of operation – currently an open point (not required for SBAS)
F.1.4	Enhanced Vehicle Localisation Function	Transmission and reception of GA session management messages and acknowledgements	F1:OUT<F2>	F1 → F2	Acknowledgement message	
			F1:OUT<F2>	F1 → F2	Initiate GA session message	
			F1:OUT<F2>	F1 → F2	GA active data request message	
			F1:OUT<F2>	F1 → F2	GNSS navigation data request message	
			F1:OUT<F2>	F1 → F2	Terminate GA session message	

#	Macro Function	Basic Function	Functional Interface	Direction	Data Item	Details / Remarks
			F1:OUT<F2>	F1 → F2	Allocate GA message stream message	
			F1:OUT<F2>	F1 → F2	Resume GA message stream message	
			F1:OUT<F2>	F1 → F2	Suspend GA message stream message	
			F1:IN<F2>	F2 → F1	GA session established message	
			F1:IN<F2>	F2 → F1	GA message stream allocated / resumed message	
			F1:IN<F2>	F2 → F1	GA session error message	
			F1:IN<F2>	F2 → F1	GA session terminated message	
			F1:IN<F2>	F2 → F1	GA message stream suspended message	
F1.5	Enhanced Vehicle Localisation Function	Timestamping of GA message received from GADF				Timestamp of GAM reception at EVLF
F1.6	Enhanced Vehicle Localisation Function	Supervision and management of TTA				Supervision of T_GATIMEOUT timer
F1.7	Enhanced Vehicle Localisation Function	Supervision of GA message content timeout				SBAS Legacy and DFMC message content timeout
F1.8	Enhanced Vehicle Localisation Function	GA message processing				Legacy and DFMC SBAS MTs
F1.9	Enhanced Vehicle Localisation Function	GNSS signal processing	F1:IN<GNSS>	GNSS → F1	GNSS pre-correlation signal processing	
			F1:IN<GNSS>	GNSS → F1	Acquisition and tracking of GNSS signals	
			F1:IN<GNSS>	GNSS → F1	Navigation data demodulation and FEC decoding	
			F1:IN<GNSS>	GNSS → F1	Navigation data processing	
F1.10	Enhanced Vehicle Localisation Function	GNSS pseudorange determination and use				
F1.11	Enhanced Vehicle Localisation Function	Computation and application of GA corrections to smoothed pseudorange				
F1.12	Enhanced Vehicle Localisation Function	Computation and application of GNSS pseudorange error models				
F2.1	GNSS Augmentation Dissemination Function	Transmission of GA message streams to EVLF	F2:OUT<F1>	F2 → F1	GA messages (Q_GAMT = 0, Nominal GA messages)	Encapsulating Legacy and DFMC SBAS MTs

#	Macro Function	Basic Function	Functional Interface	Direction	Data Item	Details / Remarks
			F2:OUT<F1>	F2 → F1	GA messages (Q_GAMT = 1, GA alert messages)	Encapsulating Legacy and DFMC SBAS alert sequence MTs
			F2:OUT<F1>	F2 → F1	GA messages (Q_GAMT = 2, DNU GA message stream)	Includes SBAS MT0
F2.2	GNSS Augmentation Dissemination Function	Transmission of GA active data sets to EVLF	F2:OUT<F1>	F2 → F1	GA messages (Q_GAMT = 0, Nominal GA messages)	Set of Legacy of DFMC SBAS MTs with message content that is valid (i.e., has not timed out)
F2.3	GNSS Augmentation Dissemination Function	Transmission of GA active alerts to EVLF	F2:OUT<F1>	F2 → F1	GA messages (Q_GAMT = 1, GA alert messages)	Encapsulating Legacy and DFMC SBAS alert sequence MTs
F2.4	GNSS Augmentation Dissemination Function	Transmission and reception of GA session management messages and acknowledgements	F2:IN<F1>	F1 → F2	Acknowledgement message	
			F2:IN<F1>	F1 → F2	Initiate GA session message	
			F2:IN<F1>	F1 → F2	GA active data request message	
			F2:IN<F1>	F1 → F2	GNSS navigation data request message	
			F2:IN<F1>	F1 → F2	Terminate GA session message	
			F2:IN<F1>	F1 → F2	Allocate GA message stream message	
			F2:IN<F1>	F1 → F2	Resume GA message stream message	
			F2:IN<F1>	F1 → F2	Suspend GA message stream message	
			F2:OUT<F1>	F2 → F1	GA session established message	
			F2:OUT<F1>	F2 → F1	GA message stream allocated / resumed message	
			F2:OUT<F1>	F2 → F1	GA session error message	
			F2:OUT<F1>	F2 → F1	GA session terminated message	
			F2:OUT<F1>	F2 → F1	GA message stream suspended message	
F2.5	GNSS Augmentation Dissemination Function	Reception of GA messages from GATF	GA-TS<Internal>	F3 → F2	GA messages (Q_GAMT = 0, Nominal GA messages)	Encapsulating Legacy and DFMC SBAS MTs
F2.6	GNSS Augmentation Dissemination Function	Reception of GA active data sets from GATF	GA-TS<Internal>	F3 → F2	GA messages (Q_GAMT = 0, Nominal GA messages)	Set of Legacy of DFMC SBAS MTs with message content that is valid (i.e., has not timed out)

#	Macro Function	Basic Function	Functional Interface	Direction	Data Item	Details / Remarks
F2.7	GNSS Augmentation Dissemination Function	Reception of GA active alerts from GATF	GA-TS<Internal>	F3 → F2	GA messages (Q_GAMT = 1, GA alert messages)	Encapsulating Legacy and DFMC SBAS alert sequence MTs
F2.8	GNSS Augmentation Dissemination Function	Reception of GNSS navigation data sets from GATF	GA-TS<Internal>	F3 → F2	GNSS navigation data sets	GPS L1 LNAV and Galileo E5a F/NAV. GPS L5 CNAV and Galileo E1B I/NAV for possible degraded modes of operations – currently and open point (not required for SBAS)
F2.9	GNSS Augmentation Dissemination Function	Transmission and reception of GADF-GATF session management messages and acknowledgments	GA-TS<Internal>	F3 → F2	Not defined	Protocol not defined, not considered necessary for interoperability
			GA-TS<Internal>	F2 → F3	Not defined	Protocol not defined, not considered necessary for interoperability
F2.10	GNSS Augmentation Dissemination Function	Selection of GA service and channel compatible with services supported by EVLF				Selection of SBAS PRN
F2.11	GNSS Augmentation Dissemination Function	Resumption of suspended GA message streams				
F3.1	GNSS Augmentation Trackside Function	Reception of GA messages from GAS	F3:IN<SBAS>	SBAS → F3	Legacy and DFMC SBAS MTs	MTs received via SBAS SIS
F3.2	GNSS Augmentation Trackside Function	Transmission of GA messages to GADF for each service / GAC	GA-TS<Internal>	F3 → F2	GA messages (Q_GAMT = *)	Encapsulating Legacy and DFMC SBAS MTs
F3.3	GNSS Augmentation Trackside Function	Transmission of requested GA active data sets to GADF	GA-TS<Internal>	F3 → F2	GA messages	Set of Legacy or SBAS MTs with message content that is valid (i.e., has not timed out)
F3.4	GNSS Augmentation Trackside Function	Transmission of requested navigation data sets to GADF	GA-TS<Internal>	F3 → F2	GNSS navigation data sets	GPS L1 LNAV and Galileo E5a F/NAV. GPS L5 CNAV and Galileo E1B I/NAV for possible degraded modes of operations – currently an open point (not required for SBAS)
F3.5	GNSS Augmentation Trackside Function	Transmission and reception of GADF-GATF session management messages and acknowledgements	GA-TS<Internal>	F3 → F2	Not defined	Protocol not defined, not considered necessary for interoperability
			GA-TS<Internal>	F2 → F3	Not defined	Protocol not defined, not considered

#	Macro Function	Basic Function	Functional Interface	Direction	Data Item	Details / Remarks
						necessary for interoperability
F3.6	GNSS Augmentation Trackside Function	Selection of GACs				Selection of SBAS PRN
F3.7	GNSS Augmentation Trackside Function	Maintain GA active data set for each GAC				
F3.8	GNSS Augmentation Trackside Function	Maintain GA active alerts for each GAC				
F3.9	GNSS Augmentation Trackside Function	Timestamping reception of messages from GAS				
F3.10	GNSS Augmentation Trackside Function	Encapsulation of messages received from GAS in GAM packets				
F3.11	GNSS Augmentation Trackside Function	Maintain GNSS navigation data sets				
F3.12	GNSS Augmentation Trackside Function	GNSS signal processing	F3:IN<GNSS>	GNSS → F3	Acquisition and tracking of GNSS signals	
			F3:IN<GNSS>	GNSS → F3	Navigation data demodulation and FEC decoding	
			F3:IN<GNSS>	GNSS → F3	Navigation data processing	
F3.13	GNSS Augmentation Trackside Function	SBAS signal processing	F3:IN<SBAS>	SBAS → F3	Acquisition and tracking of SBAS signals (L1 and L5)	
			F3:IN<SBAS>	SBAS → F3	SBAS L1 data demodulation and FEC decoding	
			F3:IN<SBAS>	SBAS → F3	SBAS L5 data demodulation and FEC decoding	
			F3:IN<SBAS>	SBAS → F3	SBAS L1 message processing	
			F3:IN<SBAS>	SBAS → F3	SBAS L5 message processing	

5.3 Assumptions

5.3.1.1 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 EVLF 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 FMEA Columns

5.4.1.1 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 5.5, 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 – Intermediate	These are effects at intermediate level (e.g., subsystem level), assuming no other failures are present.
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 Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD	Define barriers of the reference architecture that protect are known to mitigate against the identified risk will be noted in this column. This information will be used in the development of functional fault trees.

5.5 Guidewords for Data Transmission

5.5.1.1 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 also 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 steam
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

5.6 Guidewords for Discrete Signals

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

Guideword	Definition
Incorrect	Signal is incorrect / in the wrong state
Absent	Signal is absent
Timing	Signal is delayed / appears later than required
Insertion	Another signal / a random change of state

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 Hazard Analysis (Causal Analysis) – FMEA

This section provides the Failure Modes and Effects Analysis (FMEA) conducted according to the process described in Section 5.

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

6.1 FMEA GNSS-EVLF Interface (F1:IN<GNSS>)

6.1.1 GNSS Pre-correlation Signal Processing

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.1.1.1	GNSS Pre-correlation Signal Processing	**Incorrect** Pre-correlation signal processing not compatible with GA assumptions	• GNSS receiver not compliant with critical parameters that comprise the user receiver configuration space for fault modes to be protected by GA	SBAS inadequately bounds pseudorange errors / does not provide protection against fault modes / degradations in GNSS signals for which the SBAS provider assumes a receiver operating within a compatible configuration space	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-OB-MOPS: • The equipment shall apply the following receiver design constraints [DMS:52].

6.1.2 Acquisition and Tracking of GNSS Signals

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.1.2.1	Acquisition and Tracking of GNSS Signals	**Incorrect** Mistaking one GPS L1 C/A code 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	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-OB-MOPS: • An acceptable means of compliance for acquisition is to reject L1 ranging data if there is a 3000 km separation between satellite positions computed from the L1 LNAV almanac and from the L1 LNAV ephemerides currently broadcast by the satellite [DMS:247].
6.1.2.2	Acquisition and Tracking of GNSS Signals	**Incorrect** Mistaking one GPS L5 signal with another	• Cross-correlation effects during acquisition or reacquisition	GPS L5 ranging data does not correspond to PRN code number used for signal tracking	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-OB-MOPS: • After acquisition, the equipment shall only use GPS L5 ranging data when the PRN code number used for signal tracking is confirmed at least once by the PRN parameter broadcast in L5 CNAV messages [DMS:015].
6.1.2.3	Acquisition and Tracking of GNSS Signals	**Incorrect** Mistaking one GAL E1 signal with another	• Cross-correlation effects during acquisition or reacquisition	Galileo E1 ranging data does not correspond to primary code number used for signal tracking	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-OB-MOPS: • The equipment shall decode continuously E5a F/NAV and E1 I/NAV navigation data streams for each tracked Galileo satellite [DMS:021]. • After acquisition, the equipment shall only use Galileo E1 ranging data when the primary code number used for signal tracking is confirmed at least once by the satellite ID provided in E1 I/NAV Word Type 4 [DMS:023].

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.1.2.4	Acquisition and Tracking of GNSS Signals	**Incorrect** Mistaking one GAL E5a signal with another	• Cross-correlation effects during acquisition or reacquisition	Galileo E5a ranging data does not correspond to primary code number used for signal tracking	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-OB-MOPS: • The equipment shall decode continuously E5a F/NAV and E1 I/NAV navigation data streams for each tracked Galileo satellite [DMS:021]. • Use of I/NAV to verify satellite ID (TBC)
6.1.2.5	Acquisition and Tracking of GNSS Signals	**Incorrect** GPS L1/L5 iono-free pseudorange error overshoot exceeds theoretical bias error	• When tracking GPS satellite affected by up to +10m on L1 and up to -10m on L5, iono-free pseudorange error overshoot exceeds theoretical bias error	Pseudorange error bound does not include pseudorange error overshoot	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-OB-MOPS: • The overshoot exceeding the theoretical bias error by the carrier smoothed ionosphere-free pseudorange measurement shall be less than or equal to 0.05 meters 360 seconds and more after the occurrence of the simultaneous code step errors on L1 and L5 [DMS:379]. • Either generation of GPS L1 C/A-code and GPS L5 pseudorange measurements using first-order code tracking loops (as there will be no overshoot) or manufacturer to show by analysis that above requirement is satisfied. • Note: there is currently no requirement addressing bounding of the overshoot during the transient phase (time elapsed since smoothing filter reinitialization until steady state) following the occurrence of the code step errors.

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.1.2.6	Acquisition and Tracking of GNSS Signals	**Incorrect** Galileo E1/E5a iono-free pseudorange error overshoot exceeds theoretical bias error	• When tracking Galileo satellite affected by up to +10m on E1 and up to -10m on E5a, iono-free pseudorange error overshoot exceeds theoretical bias error	Pseudorange error bound does not include pseudorange error overshoot	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-OB-MOPS: • The overshoot exceeding the theoretical bias error by the carrier smoothed ionosphere-free pseudorange measurement shall be less than or equal to 0.05 meters 360 seconds and more after the occurrence of the simultaneous code step errors on E1 and E5a [DMS:380]. • Either generation of Galileo E1 and E5a pseudorange measurements using first-order code tracking loops (as there will be no overshoot) or manufacturer to show by analysis that above requirement is satisfied. • Note: there is currently no requirement addressing bounding of the overshoot during the transient phase (time elapsed since smoothing filter reinitialization until steady state) following the occurrence of the code step errors.
6.1.2.7	Acquisition and Tracking of GNSS Signals	**Absent** Unable to acquire / track GNSS signals	• Radiofrequency interference • Cyber-attack (intentional jamming)	Degraded C/N0, below acquisition and tracking threshold	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.1.2.8	Acquisition and Tracking of GNSS Signals	**Timing** Acquisition and tracking of delayed GNSS signals	• Cyber-attack targeting GNSS signals (e.g., GNSS meaconing, reradiation, record & replay)	Erroneous GNSS ranging data; erroneous EVLF time	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Cyber-attacks related to GNSS signals received by the EVLF are outside the scope of GA for ERTMS/ETCS.

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.1.2.9	Acquisition and Tracking of GNSS Signals	**Insertion** Acquisition and tracking of non-authentic GNSS signals	• Cyber-attack targeting GNSS signals (e.g., GNSS spoofing, meaconing, reradiation, record & replay)	Erroneous GNSS ranging data; erroneous EVLF time	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Cyber-attacks related to GNSS signals received by the EVLF are outside the scope of GA for ERTMS/ETCS.

6.1.3 Navigation Data Demodulation, FEC Decoding and Processing

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.1.3.1	GNSS Navigation Data	**Corruption** Reception of corrupted GPS LNAV navigation data	• Interference environment (C/N0 degraded, increased BER) • Erroneous frame sync • Receiver hardware fault • Receiver firmware / software fault	Reception of subframe with corrupted word(s) resulting in use of erroneous CED; erroneous GNSS ranging data; erroneous EVLF time	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	IS-GPS-200: • Corruption detected by parity 6-bit parity for each 24-bit LNAV word (300-bit LNAV subframe of 10 words), words failing parity check discarded • 8-bit preamble in each subframe for frame sync SBAS-OB-MOPS: • Except for L1 LNAV information leading to the exclusion of a GPS satellite, the equipment shall only use clock and ephemeris data when it is verified by reception of a second message (subframes 1, 2, and 3 of the GPS L1 LNAV navigation message) containing the same data, with a broadcast IODE that matches the 8 least-significant bits of the broadcast IODC [DMS:249].

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
								• Note: this requirement ensures residual risk of undetected corruption is acceptable.
6.1.3.2	GNSS Navigation Data	**Corruption** Reception of corrupted navigation data (GPS C/NAV, Galileo I/NAV, Galileo F/NAV)	• Interference environment (C/N0 degraded, increased BER) • Erroneous message/page sync • Receiver hardware fault • Receiver firmware / software fault	Reception of subframe with corrupted word(s) resulting in use of erroneous CED; erroneous GNSS ranging data; erroneous EVLF time	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	IS-GPS-705: • Corruption detected by 24-bit CRC in CNAV message • 8-bit preamble in each CNAV message for sync to message boundary GAL-OS-SIS-ICD: • Corruption detected by 24-bit CRC in I/NAV page • Corruption detected by 24-bit CRC in F/NAV word • 10-bit sync pattern in I/NAV page for sync to page boundary • 12-bit sync pattern in each F/NAV page for sync to page boundary
6.1.3.3	GNSS Navigation Data	**Deletion** Deleted GNSS navigation data	• Radiofrequency interference (C/N0 degraded below demodulation threshold) • Cyber-attack (intentional jamming) • Receiver hardware fault • Receiver firmware / software fault	GNSS navigation message not available for one or more satellites	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.1.3.4	GNSS Navigation Data	**Delay, Repetition** Delay of GNSS navigation data / repetition of old	• Cyber-attack targeting GNSS signals (e.g., GNSS spoofing, record & replay)	Reception of old navigation data (earlier IOD); applicable set of corrections (from SBAS messages) do not correspond to	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Cyber-attacks related to GNSS signals received by the EVLF are outside the scope of GA for ERTMS/ETCS.

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
		navigation data (earlier IOD)	• Receiver hardware fault • Receiver firmware / software fault	IODC/IODE or IODnav of GNSS navigation data; even if navigation data is still within curve fit interval, absence of GA corrections for IOD would result in unavailability				
6.1.3.5	GNSS Navigation Data	**Insertion, Masquerade** Reception of non-authentic navigation data designed to appear authentic	• Cyber-attack targeting GNSS signals (e.g., GNSS spoofing / record & replay)	Erroneous CED; erroneous GNSS ranging data; erroneous EVLF time	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Cyber-attacks related to GNSS signals received by the EVLF are outside the scope of GA for ERTMS/ETCS.
6.1.3.6	GNSS Navigation Data	**Re-sequence** Out of sequence (messages / subframes / pages)	• Cyber-attack targeting GNSS signals (e.g., GNSS spoofing) • Receiver hardware fault • Receiver firmware / software fault	Reception of GNSS navigation messages / subframes / pages out of sequence (i.e., with respect to frame / subframe layout in ICD)			No Effect	Cyber-attacks related to GNSS signals received by the EVLF are outside the scope of GA for ERTMS/ETCS.

6.2 FMEA SBAS-EVLF Interface (F1:IN<SBAS>)

6.2.1.1 This interface is reserved for supporting reception of SBAS SIS by the EVLF. The analysis will address this interface once principles have been defined in a future release of the SRS. It should be noted that information from EGNOS received by the EVLF via the GADF and via the SBAS SIS interface cannot be mixed in a single GNSS processing channel.

6.3 FMEA EVLF

6.3.1 Timestamping of GA Message Received from GADF

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.3.1.1	Timestamping of GA Message Received from GADF	**Early, Late, Erroneous** Incorrect timestamp of reception of GA message by EVLF ($t_{EVLF,GAMrx}$)	• Erroneous CED, ranging data • Incorrect reference time (i.e., for SBAS, not SNT) • EVLF software fault • EVLF hardware fault	Failure in TTA supervision; potential violation of maximum end to end TTA (T_NVGAMAXTTA); GNSS channel not transitioned to a safe state (i.e., within T_NVGAMAXTTA for missed / delayed GA messages that could be alerts)	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	EVLF software and hardware design assurance (EN 50128, EN 50129)
6.3.1.2	Timestamping of GA Message Received from GADF	**No or Not** Timestamp of reception of GA message by EVLF not available	• Insufficient number of GNSS satellites, (unavailable CED, ranging data) • EVLF software fault • EVLF hardware fault	TTA supervision unavailable	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	

6.3.2 Supervision and Management of TTA

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.3.2.1	TTA supervision	**Early** TTA supervision transitions GNSS channel into safe state earlier than it should	• Erroneous timestamp of reception GA message by EVLF ($t_{EVLF,GAMrx}$) • Erroneous timestamp of reception of GA	GNSS channel is in a safe (unavailable) state	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	EVLF software and hardware design assurance (EN 50128, EN 50129)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			message by GATF ($T_{GATF,GAMrx}$) • EVLF software fault • EVLF hardware fault					
6.3.2.2	TTA supervision	**Late, Erroneous** Erroneous TTA supervision, transitions GNSS channel into safe state later than it should	• Erroneous timestamp of reception GA message by EVLF ($t_{EVLF,GAMrx}$) • Erroneous timestamp of reception of GA message by GATF ($T_{GATF,GAMrx}$) • EVLF software fault • EVLF hardware fault	Potential violation of maximum end to end TTA (T_NVGAMAXTTA); GNSS channel not transitioned to a safe state (i.e., within T_NVGAMAXTTA for missed / delayed GA messages that could be alerts); pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	EVLF software and hardware design assurance (EN 50128, EN 50129) SRS: • The GATF/GADF shall ensure continuity of signal by providing a GA message for each GAC at least every T_NVGAMBUR milliseconds
6.3.2.3	TTA supervision	**No or Not** No TTA supervision	• Timestamp of reception of GA message by EVLF unavailable (same GAT reference as indicated by Q_GAT) • Timestamp of reception of GA message by GATF unavailable • EVLF software fault • EVLF hardware fault	TTA supervision unavailable; GNSS channel is in a safe (unavailable) state	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	SRS: • If TTA supervision is unavailable, all GA integrity data for affected GA message streams become unavailable [2.2.7]

6.3.3 Supervision of GA Message Content Timeout

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.3.3.1	GA message content timeout supervision	**Early** GA message content timed out earlier than it should	• Erroneous EVLF time • Incorrect EVLF reference time (i.e., for SBAS, not SNT, different from $T_{GATF,GAMrx}$) • Erroneous timestamp of reception of GA message by GATF ($T_{GATF,GAMrx}$) • EVLF software fault • EVLF hardware fault	Message content times out before it should; GNSS channel is in a safe (unavailable) state	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	EVLF software and hardware design assurance (EN 50128, EN 50129)
6.3.3.2	GA message content timeout supervision	**Late, Erroneous** Erroneous GA message content timeout supervision, GA message content timed out later than it should	• Erroneous EVLF time • Incorrect EVLF reference time (i.e., for SBAS, not SNT, different from $T_{GATF,GAMrx}$) • Erroneous timestamp of reception of GA message by GATF ($T_{GATF,GAMrx}$) • EVLF software fault • EVLF hardware fault	Use of message content that is not valid (i.e., has timed out); pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	EVLF software and hardware design assurance (EN 50128, EN 50129)
6.3.3.3	GA message content timeout supervision	**No or Not** No GA message content timeout supervision	• EVLF time unavailable (same GAT reference as indicated by Q_GAT) • Timestamp of reception of GA message by GATF unavailable • EVLF software fault • EVLF hardware fault	GA message content timeout supervision unavailable; GNSS channel is in a safe (unavailable) state	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	SRS: • If TTA supervision is unavailable, GA message content shall be discarded by the EVLF [2.2.8]

6.3.4 GA Message Processing

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.3.4.1	GA message processing	**Erroneous, Late** Erroneous GA message processing, GA message processing executed later / takes longer than it should	• EVLF software fault • EVLF hardware fault	Pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-OB-MOPS provides requirements for GA message processing. EVLF software and hardware design assurance (EN 50128, EN 50129).
6.3.4.2	GA message processing	**No or Not** GA message processing not performed	• EVLF software fault • EVLF hardware fault	GA message (alert) not processed; alert missed; pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SRS: • Under nominal conditions, GAS guarantees integrity for any valid combination of active data where resilience against GA message loss is provided through timeouts for message content and timeout supervision, and application of degradation parameters [2.2.7, 2.2.8] • In the case of an alert condition or DNU GA message, message loss at EVLF is detected through acknowledgement mechanism and TTA supervision [2.2.7] EVLF software and hardware design assurance (EN 50128, EN 50129)

6.3.5 GNSS Pseudorange Determination and Use

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.3.5.1	GNSS pseudorange determination and use	**Erroneous** Erroneous pseudorange determination, used when should not be used	• EVLF software fault • EVLF hardware fault	Pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-OB-MOPS provides requirements on usage criteria. EVLF software and hardware design assurance (EN 50128, EN 50129).
6.3.5.2	GNSS pseudorange determination and use	**No or Not** Pseudorange not used when should be used	• EVLF software fault • EVLF hardware fault	Fewer satellites available	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	EVLF software and hardware design assurance (EN 50128, EN 50129)

6.3.6 Computation and Application of GA Corrections to Smoothed Pseudorange

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.3.6.1	Computation and application of GA corrections to smoothed pseudorange	**Erroneous** Erroneous computation and/or application of GA corrections to smoothed pseudorange	• EVLF software fault • EVLF hardware fault	Pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-OB-MOPS provides requirements on computation and application of GA corrections to smoothed pseudorange. EVLF software and hardware design assurance (EN 50128, EN 50129).

6.3.7 Computation and Application of GNSS Pseudorange Error Models

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.3.7.1	Computation and application of GNSS pseudorange error models	**Erroneous** Erroneous computation and/or application of pseudorange error models	• EVLF software fault • EVLF hardware fault	Pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-OB-MOPS provides requirements on computation of pseudorange error models. EVLF software and hardware design assurance (EN 50128, EN 50129).

6.4 FMEA EVLF-GADF Interface (F1 ↔ F2)

6.4.1 GA Messages (Q_GAMT = 0, Nominal GA message)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.1.1	GA message (Q_GAMT = 0, Nominal GA message)	**Corruption** Reception of corrupted GA message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of corrupt GA message; erroneous corrections and/or integrity data; pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption) SBAS-TS-MOPS: • GATF checks the CRC of SBAS messages received via the SBAS SIS. SBAS-OB-MOPS: • EVLF checks the CRC of the encapsulated SBAS message.
6.4.1.2	GA message (Q_GAMT = 0, Nominal GA message)	**Deletion** Deleted GA message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	GA message(s) not received; potential timeout of GA message content	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Timeout mechanism provides resilience against GA message deletion. SBAS-OB-MOPS: • Timeout intervals for SBAS L1 data [DMS:298] • Timeout intervals for SBAS L5 data • Message content timeout [DMS:047] SRS: • EVLF supervision of GA message content timeout [2.2.8]
6.4.1.3	GA message (Q_GAMT = 0, Nominal GA message)	**Delay** Reception of delayed GA message	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services)	Delayed reception of GA messages; potential timeout of GA message content	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Timeout mechanism provides resilience against GA message delay. SBAS-OB-MOPS: • Timeout intervals for SBAS L1 data [DMS:298]

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault					• Timeout intervals for SBAS L5 data • Message content timeout [DMS:047] SRS: • EVLF supervision of GA message content timeout [2.2.8]
6.4.1.4	GA message (Q_GAMT = 0, Nominal GA message)	**Repetition, Re-sequence** Reception of repeated or out-of-sequence GA message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of repeated or out-of-sequence GA messages; potential timeout of GA message content	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Timeout mechanism provides resilience against GA message deletion. GA messages (except alerts) are not acknowledged and therefore no retransmissions. SBAS-OB-MOPS: • Timeout intervals for SBAS L1 data [DMS:298] • Timeout intervals for SBAS L5 data • Message content timeout [DMS:047] SRS: • EVLF supervision of GA message content timeout [2.2.8] • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition / out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.1.5	GA message (Q_GAMT = 0, Nominal GA message)	**Insertion, Masquerade** Reception of inserted or masqueraded GA message	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of inserted / masqueraded GA messages; erroneous corrections and/or integrity data; pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

6.4.2 GA Messages (Q_GAMT = 1, GA alert message)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.2.1	GA message (Q_GAMT = 1, GA alert message)	**Corruption** Reception of corrupted GA message (alert)	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of corrupt GA message (alert); alert missed or processed with erroneous information; pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption) SBAS-TS-MOPS • GATF checks the CRC of SBAS messages received via the SBAS SIS. SBAS-OB-MOPS • EVLF check the CRC of the encapsulated SBAS message.

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.2.2	GA message (Q_GAMT = 1, GA alert message)	**Deletion** Deleted GA message (alert)	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	GA message (alert) not received; pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Supervision of TTA and acknowledgement of GA alert messages SRS: • Required acknowledgement of GA message (alert) [2.2.5] • Suspension of the GA message stream until GA message (alert) is acknowledged [2.2.7] • Supervision of TTA where GA integrity data becomes unavailable in case of timeout of T_GATIMEOUT timer [2.2.7]
6.4.2.3	GA message (Q_GAMT = 1, GA alert message)	**Delay** Reception of delayed GA message (alert)	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault	GA message (alert) delayed; potential violation of maximum end to end TTA (T_NVGAMAXTTA); GNSS channel not transitioned to a safe state (i.e., within T_NVGAMAXTTA for missed / delayed GA alert messages); pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Supervision of TTA and acknowledgement of GA alert messages SRS: • Required acknowledgement of GA message (alert) [2.2.5] • Suspension of the GA message stream until GA message (alert) is acknowledged [2.2.7] • Supervision of TTA where GA integrity data becomes unavailable in case of timeout of T_GATIMEOUT timer [2.2.7]
6.4.2.4	GA message (Q_GAMT = 1, GA alert message)	**Repetition** Reception of repeated GA message (alert)	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of repeated GA message (alert) (SRS: if message not acknowledged within T_GAMRTIMEOUT, GADF shall re-send GA message until acknowledged or safe radio connection is terminated [2.2.5])	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.2.5	GA message (Q_GAMT = 1, GA alert message)	**Re-sequence** Reception of out-of-sequence GA message (alert)	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence GA message (alert)	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.2.6	GA message (Q_GAMT = 1, GA alert message)	**Insertion / Masquerade** Reception of inserted or masqueraded GA message (alert)	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of inserted / masqueraded GA message (alert); alert missed or not processed with erroneous information; pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

6.4.3 GA Messages (Q_GAMT = 3, DNU GA message stream)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.3.1	GA message (Q_GAMT = 3, DNU GA message stream)	**Corruption** Reception of corrupted GA message (DNU)	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of corrupt GA message (DNU); EVLF ceases using wrong GA message stream; pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption) SBAS-TS-MOPS • GATF checks the CRC of SBAS messages received via the SBAS SIS. SBAS-OB-MOPS • EVLF checks the CRC of the encapsulated SBAS message.
6.4.3.2	GA message (Q_GAMT = 3, DNU GA message stream)	**Deletion** Deleted GA message (DNU)	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	GA message (DNU) not received; message stream indicated by DNU continues to be used; pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Supervision of TTA, immediate suspension of GA message stream and required acknowledgement of GA message (DNU) SRS: • Required acknowledgement of GA message (DNU) [2.2.5] • Suspension of the GA message stream [2.2.5] • Supervision of TTA where GA integrity data becomes unavailable in case of timeout of T_GATIMEOUT timer [2.2.7]
6.4.3.3	GA message (Q_GAMT = 3, DNU GA message stream)	**Delay** Reception of delayed GA message (DNU)	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection	GA message (DNU) delayed; potential violation of maximum end to end TTA (T_NVGAMAXTTA); GNSS channel not transitioned to a safe state (i.e., within	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Supervision of TTA, immediate suspension of GA message stream and acknowledgement of GA message (DNU) SRS: • Required acknowledgement of GA message (DNU) [2.2.5]

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	T_NVGAMAXTTA for missed / delayed GA message); pseudorange errors potentially not bounded				• Suspension of the GA message stream [2.2.5] • Supervision of TTA where GA integrity data becomes unavailable in case of timeout of T_GATIMEOUT timer [2.2.7]
6.4.3.4	GA message (Q_GAMT = 3, DNU GA message stream)	**Repetition** Reception of repeated GA message (DNU)	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of repeated GA message (DNU) (SRS: if message not acknowledged within T_GAMRTIMEOUT, GADF shall re-send GA message until acknowledged or safe radio connection is terminated [2.2.5])	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.3.5	GA message (Q_GAMT = 3, DNU GA message stream)	**Re-sequence** Reception of out-of-sequence GA message (DNU)	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence GA message (DNU)	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.3.6	GA message (Q_GAMT = 3, DNU GA message stream)	**Insertion / Masquerade** Reception of inserted or masqueraded GA message (DNU)	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault	Reception of inserted / masqueraded GA message (DNU); EVLF ceases using wrong GA message stream;	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
		(DNU event – e.g., reception of SBAS MT0)	• GADF software fault	pseudorange errors potentially not bounded				A1 from EN 50159), which provides origin authentication and message integrity)
6.4.3.7	GA message (Q_GAMT = 3, DNU GA message stream)	**Insertion / Masquerade** Reception of inserted or masqueraded GA message (DNU) (No DNU event)	• Cyber-attack against safe radio connection • GADF hardware fault • GADF software fault	Reception of inserted / masqueraded GA message (DNU); EVLF ceases using indicated GA message stream; GA provided integrity unavailable	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

6.4.4 GNSS Navigation Data Sets

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.4.1	GNSS navigation data set	**Corruption** Reception of corrupted GNSS navigation data set message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of corrupt GNSS navigation data; erroneous CED; erroneous GNSS ranging data; erroneous EVLF time	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption) GATF Barriers: • Refer to Section 6.7.3 (GATF, maintain GNSS navigation data sets) and Section 6.9 (GATF-GNSS interface).

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• Corrupted navigation data from GATF (e.g., due to reception of corrupted navigation data from SIS, GATF hardware / software fault)					
6.4.4.2	GNSS navigation data set	**Deletion** Deletion of GNSS navigation data set message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault • Deletion of GNSS navigation data from GATF (e.g., due to interference environment, cyber-attack for reception from SIS, GATF hardware / software fault)	One or more messages of GNSS navigation data set not received; CED not available for one or more GNSS satellites	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	GNSS navigation data sets are provided as assistance data to reduce start-up time (i.e., related to reception of navigation data), especially in difficult start-up environments (e.g., where there is significant obscuration of GNSS satellites). The EVLF continuously decodes the navigation data bit train from the SIS for each tracked GNSS satellite and is the primary source of GNSS navigation data. SRS: • Messages of GNSS navigation data set are acknowledged by EVLF to indicate GADF ready for next message of set. GADF re-sends unacknowledged messages [2.2.4] GATF Barriers: • Refer to Section 6.7.3 (GATF, maintain GNSS navigation data sets) and Section 6.9 (GATF-GNSS interface).
6.4.4.3	GNSS navigation data set	**Delay** Reception of delayed GNSS navigation data set	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault	Reception of old navigation data (earlier IOD); applicable set of corrections (from SBAS messages) do not correspond to IODC/IODE or IODnav, of GNSS navigation data; even if navigation data is still within curve fit interval, absence of GA corrections	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	SRS: • Messages of GNSS navigation data set are acknowledged by EVLF to indicate GADF ready for next message of set. GADF re-sends unacknowledged messages [2.2.4] GATF Barriers:

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• GADF hardware fault • GADF software fault • Delay of GNSS navigation data from GATF (e.g., due cyber-attack for reception from SIS, GATF hardware / software fault)	for IOD would result in unavailability				• Refer to Section 6.7.3 (GATF, maintain GNSS navigation data sets) and Section 6.9 (GATF-GNSS interface).
6.4.4.4	GNSS navigation data set	**Repetition** Reception of repeated GNSS navigation data set messages	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of repeated GNSS navigation data set message (SRS: if message not acknowledged within T_GNSSNDSRTIMEOUT, GADF shall re-send GNSS navigation data set message until acknowledged or unsuccessful transmissions reaches N_GNSSNDSMAXRETRIES [2.2.4])			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.4.5	GNSS navigation data set	**Re-Sequence** Reception of out-of-sequence GNSS navigation data set messages	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence GNSS navigation data set message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
								safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.4.6	GNSS navigation data set	**Insertion, Masquerade** Reception of inserted or masqueraded GNSS data set message(s)	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of masqueraded GNSS navigation data set message; erroneous CED; erroneous GNSS ranging data; erroneous EVLF time	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

6.4.5 Acknowledgement

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.5.1	Acknowledgement	**Corruption** Reception of corrupted acknowledgement message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault	Acknowledgement of wrong message (erroneous T_TRAIN timestamp of message that is acknowledged); missed alert or DNU message incorrectly acknowledged	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• GADF software fault					
6.4.5.2	Acknowledgement	**Deletion** Deletion of acknowledgement message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Acknowledgement message not received; GADF re-sends message requiring acknowledgment; for alert and DNU GA messages, GA message stream suspended; timeout of GA message content	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.5.3	Acknowledgement	**Delay** Reception of delayed acknowledgement	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Delayed reception of acknowledgement; for alert and DNU GA messages, GA message stream suspended; timeout of GA message content	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.5.4	Acknowledgement	**Repetition** Reception of repeated acknowledgment message	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault	Reception of repeated acknowledgement message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24]

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• GADF hardware fault • GADF software fault					Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.5.5	Acknowledgement	**Re-sequence** Reception of out-of-sequence acknowledgment message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence acknowledgement message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.5.6	Acknowledgement	**Insertion / Masquerade** Reception of inserted or masqueraded acknowledgement	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of masqueraded / inserted acknowledgement message; incorrect acknowledgement of an alert or DNU; alert not processed; pseudorange error potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

6.4.6 Initiate GA Session

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.6.1	Initiate GA session	**Corruption** Reception of corrupted initiate GA session message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Erroneous GA versions supported by on-board; GADF establishes a GA session with an incompatible GA-TS version.	Potential incompatibilities between GA-OB and GA-TS (currently not possible to determine, to be re-assessed in the future when multiple versions exist)		TBD	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)
6.4.6.2	Initiate GA session	**Deletion** Deletion of initiate GA session message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Initiate GA session message not received; EVLF re-sends message	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.6.3	Initiate GA session	**Delay** Reception of delayed initiate GA session message	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault	Delayed reception of initiate GA session message	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• GADF software fault					
6.4.6.4	Initiate GA session	**Repetition** Reception of repeated initiate GA session message	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of repeated acknowledgement message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.6.5	Initiate GA session	**Re-sequence** Reception of out-of-sequence initiate GA session message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence initiate GA session message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
								authentication and message integrity)
6.4.6.6	Initiate GA session	**Insertion / Masquerade** Reception of inserted or masqueraded initiate GA session message	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of masqueraded / inserted initiate GA session message; erroneous GA versions supported by on-board; GADF establishes a GA session with an incompatible GA-TS version.	Potential incompatibilities between GA-OB and GA-TS (currently not possible to determine, to be re-assessed in the future when multiple versions exist)		TBD	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

6.4.7 GA Active Data Request

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.7.1	GA active data request	**Corruption** Reception of corrupted GA active data request message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault	Erroneous GA message stream identifier; GA active data requested for wrong GA message stream; delay in provision of GA active data for correct GA message stream; potential for timeout of message content	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• GADF hardware fault • GADF software fault					
6.4.7.2	GA active data request	**Deletion** Deletion of GA active data request message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	GA active data request message not received; EVLF re-sends message	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.7.3	GA active data request	**Delay** Reception of delayed GA active data request	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Delayed reception of GA active data request	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.7.4	GA active data request	**Repetition** Reception of repeated GA active data request message	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault	Reception of repeated GA active data request message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24]

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• GADF hardware fault • GADF software fault					Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (i.e., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.7.5	GA active data request	**Re-sequence** Reception of out-of-sequence GA active data request message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence GA active data request message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.7.6	GA active data request	**Insertion / Masquerade** Reception of inserted or masqueraded GA active data request message	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of masqueraded / inserted GA active data request; request made for wrong GA message stream; potential to be exploited by attacker to increase utilisation of radio channel with possible delays of other messages	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

6.4.8 GNSS Navigation Data Request

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.8.1	GNSS navigation data request	**Corruption** Reception of corrupted GNSS navigation data request message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Erroneous SV mask and/or selection of GNSS navigation data sets required; delay in receiving complete datasets	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	GNSS navigation data sets are provided as assistance data to reduce start-up time (i.e., related to reception of navigation data), especially in difficult start-up environments (e.g., where there is significant obscuration of GNSS satellites). The EVLF continuously decodes the navigation data bit train from the SIS for each tracked GNSS satellite and is the primary source of GNSS navigation data. Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)
6.4.8.2	GNSS navigation data request	**Deletion** Deletion of GNSS navigation data request message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	GNSS navigation data request message not received; EVLF re-sends message	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.8.3	GNSS navigation data request	**Delay** Reception of delayed GNSS navigation data request	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Delayed reception of GNSS navigation data request	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.8.4	GNSS navigation data request	**Repetition** Reception of repeated GNSS navigation data request message	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of repeated GNSS navigation data request message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.8.5	GNSS navigation data request	**Re-sequence** Reception of out-of-sequence GNSS active data request message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault	Reception of out-of-sequence GNSS navigation data request message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection:

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• GADF software fault					• Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.8.6	GNSS navigation data request	**Insertion / Masquerade** Reception of inserted or masqueraded acknowledgement	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of masqueraded / inserted GA active data request; request made for wrong GA message stream; potential to be exploited by attacker to increase utilisation of radio channel with possible delays of other messages	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

6.4.9 Allocate GA Message Stream

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.9.1	Allocate GA message stream	**Corruption** Reception of corrupted allocate GA message stream message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment)	Reception of allocate GA message stream message with erroneous GA services supported by on-board and versions	Potential incompatibilities between GA-OB and GNSS augmentation service provided		Marginal	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault					
6.4.9.2	Allocate GA message stream	**Deletion** Deletion of allocate GA message stream message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Allocate GA message stream message not received; EVLF re-sends message	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.9.3	Allocate GA message stream	**Delay** Reception of delayed allocate GA message stream message	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Delayed reception of allocate GA message stream message	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.9.4	Allocate GA message stream	**Repetition** Reception of repeated allocate GA message stream message	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault	Reception of repeated allocate GA message stream message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24]

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• GADF hardware fault • GADF software fault					Safe Radio Connection • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.9.5	Allocate GA message stream	**Re-sequence** Reception of re-sequenced allocate GA message stream message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence allocate GA message stream message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.9.6	Allocate GA message stream	**Insertion / Masquerade** Reception of inserted or masqueraded allocate GA message stream message	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of masqueraded / inserted allocate GA message stream message with erroneous GA services supported by on-board and versions	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

6.4.10 Resume GA Message Stream

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.10.1	Resume GA message stream	**Corruption** Reception of corrupted resume GA message stream message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of corrupted resume GA message stream message; erroneous timestamp of last GA message reception, GA reference time; missed alert sequences not provided by GA-TS	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)
6.4.10.2	Resume GA message stream	**Deletion** Deletion of resume GA message stream message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Resume GA message stream message request message not received; EVLF re-sends message	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.10.3	Resume GA message stream	**Delay** Reception of delayed resume GA message stream message	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault	Delayed reception of resume GA message stream message	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• EVLF software fault • GADF hardware fault • GADF software fault					
6.4.10.4	Resume GA message stream	**Repetition** Reception of repeated resume GA message stream message	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of repeated resume GA message stream message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.10.5	Resume GA message stream	**Re-sequence** Reception of out-of-sequence resume GA message stream message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence resume GA message stream message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
								authentication and message integrity)
6.4.10.6	Resume GA message stream	**Insertion / Masquerade** Reception of inserted or masqueraded resume GA message stream message	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of inserted / masqueraded resume GA message stream message; erroneous timestamp of last GA message reception, GA reference time; missed alert sequences not provided by GA-TS	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

6.4.11 GA Session Established

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.11.1	GA session established	**Corruption** Reception of corrupted GA session established message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of corrupted GA session established message; erroneous GA version to be used; EVLF assumes session with a different GA version	Potential incompatibilities between GA-OB and GA-TS		Marginal	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.11.2	GA session established	**Deletion** Deletion of GA session established message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	GA session established message not received; EVLF re-sends message	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.11.3	GA session established	**Delay** Reception of delayed GA session established message	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Delayed reception of GA session established message	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.11.4	GA session established	**Repetition** Reception of repeated GA session established message	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of repeated GA session established message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
								secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.11.5	GA session established	**Re-sequence** Reception of out-of-sequence GA session established message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence GA session established message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.11.6	GA session established	**Insertion / Masquerade** Reception of inserted or masqueraded GA session established message	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of inserted / masqueraded GA session established message; erroneous GA version to be used; EVLF assumes session with different GA version	Potential incompatibilities between GA-OB and GA-TS		Marginal	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection origin authentication and message integrity)

6.4.12 GA Message Stream Allocated / Resumed

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.12.1	GA message stream allocated / resumed	**Corruption** Reception of corrupted GA message stream allocated / resumed message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of corrupted GA message stream allocated / resumed message; erroneous GAMS, GAP, GAS, GAC, GASVER, national values (T_NVGAMAXTTA, T_NVGAMAXSYSTTA, T_NVGAMBUR); erroneous GA service assumptions made by EVLF; potential for missed alerts; pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)
6.4.12.2	GA message stream allocated / resumed	**Deletion** Deletion of GA message stream allocated / resumed message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	GA message stream allocated / resumed message not received; EVLF re-sends message	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	
6.4.12.3	GA message stream allocated / resumed	**Delay** Reception of delayed GA message stream allocated / resumed message	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault	Delayed reception of GA message stream allocated / resumed message	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• GADF software fault					
6.4.12.4	GA message stream allocated / resumed	**Repetition** Reception of repeated GA message stream allocated / resumed message	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of repeated GA message stream allocated / resumed message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.12.5	GA message stream allocated / resumed	**Re-sequence** Reception of out-of-sequence GA message stream allocated / resumed message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence GA message stream allocated / resumed message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
								authentication and message integrity)
6.4.12.6	GA message stream allocated / resumed	**Insertion / Masquerade** Reception of inserted or masqueraded GA message stream allocated / resumed message	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of inserted / masqueraded GA message stream allocated / resumed message; erroneous GAMS, GAP, GAS, GAC, GASVER, national values (T_NVGAMAXTTA, T_NVGAMAXSYSTTA, T_NVGAMBUR); erroneous GA service assumptions made by EVLF; potential for missed alerts; pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

6.4.13 Terminate GA Session

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.13.1	Terminate GA session	**Corruption** Reception of corrupted Terminate GA session message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment)	Reception of corrupted Terminate GA session message; GA session not terminated; EVLF potentially continues to receive GA messages for active GA message stream(s)			No Effect	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault					
6.4.13.2	Terminate GA session	**Deletion** Deletion of Terminate GA session message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Terminate GA session message not received by GADF; EVLF does not receive acknowledgement from GADF with GA session terminated message.			No Effect	SRS • Termination of GA message stream is acknowledged by the GADF with a GA session terminated message [2.2.1]
6.4.13.3	Terminate GA session	**Delay** Reception of delayed Terminate GA session message	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Delayed reception of Terminate GA session message			No Effect	
6.4.13.4	Terminate GA session	**Repetition** Reception of repeated Terminate GA session message	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault	Reception of repeated Terminate GA session message; GA session already terminated			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24]

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• GADF hardware fault • GADF software fault					Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.13.5	Terminate GA session	**Re-sequence** Reception of out-of-sequence Terminate GA session message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence Terminate GA session message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.13.6	Terminate GA session	**Insertion / Masquerade** Reception of inserted or masqueraded Terminate GA session message	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of inserted / masqueraded Terminate GA session message; GA session incorrectly terminated	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection origin authentication and message integrity)

6.4.14 Suspend GA Message Stream

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.14.1	Suspend GA message stream	**Corruption** Reception of corrupted Suspend GA message stream message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of corrupted suspend GA message stream message; wrong message stream suspended; EVLF continues receiving GA messages associated with intended message stream (EVLF can request suspension of a message stream; however, this request is not related to suspension of message stream(s) for safety-related supervision functions).	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)
6.4.14.2	Suspend GA message stream	**Deletion** Deletion of Suspend GA message stream message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Suspend GA session message not received by GADF; EVLF does not receive acknowledgement from GADF with GA message stream suspended message.			No Effect	SRS • Suspension of GA message stream is acknowledged by the GADF with a GA message stream suspended message [2.2.1]

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.14.3	Suspend GA message stream	**Delay** Reception of delayed Suspend GA message stream message	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Delayed reception of Suspend GA message stream message			No Effect	
6.4.14.4	Suspend GA message stream	**Repetition** Reception of repeated Suspend GA message stream message	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of repeated Suspend GA message stream message; GA message stream already suspended			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.14.5	Suspend GA message stream	**Re-sequence** Reception of out-of-sequence Suspend GA message stream message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault	Reception of out-of-sequence Suspend GA message stream message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection:

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• GADF software fault					• Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.14.6	Suspend GA message stream	**Insertion / Masquerade** Reception of inserted or masqueraded Suspend GA message stream message	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of inserted / masqueraded Suspend GA message stream message; GA session incorrectly suspended	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection origin authentication and message integrity)

6.4.15 GA Session Error

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.15.1	GA Session Error	**Corruption** Reception of corrupted GA session error message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference /	Reception of GA session error message; EVLF incorrectly receives error condition (e.g., no compatible GA service version, unable to resume GA message stream); incorrect error condition potentially results in a	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	service or message stream unavailability				
6.4.15.2	GA Session Error	**Deletion** Deletion of GA session error message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	GA session error message not received; EVLF not aware of error condition (e.g., no compatible GA service version, unable to resume GA message stream); EVLF unaware of error condition; however, there is no safety impact.			No Effect	SRS • GADF responds to request for allocation of a GA message stream with a GA message stream allocated / resumed message or a GA session error message. The GADF does not start sending messages related to allocated message stream until GA message stream allocated / resumed message is acknowledged by EVLF [2.2.1].
6.4.15.3	GA Session Error	**Delay** Reception of GA session error message	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Delayed reception of GA session error message			No Effect	
6.4.15.4	GA Session Error	**Repetition** Reception of repeated GA session error message	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault	Reception of repeated GA session error message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
			• EVLF software fault • GADF hardware fault • GADF software fault					protection against repetition [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.15.5	GA Session Error	**Re-sequence** Reception of out-of-sequence GA session error message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence GA session error message; potentially associated with response to additional request for allocation of GA message stream; incorrect error condition potentially results in message stream unavailability	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	SRS: • GADF responds to request for allocation of a GA message stream with a GA message stream allocated / resumed message or a GA session error message. The GADF does not start sending messages related to allocated message stream until GA message stream allocated / resumed message is acknowledged by EVLF [2.2.1]. • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.15.6	GA Session Error	**Insertion / Masquerade** Reception of inserted or masqueraded GA session error message	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of inserted / masqueraded GA session error message; GA session incorrectly suspended; incorrect error condition potentially results in service or message stream unavailability	Train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection origin authentication and message integrity)

6.4.16 GA Session Terminated

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.16.1	GA session terminated	**Corruption** Reception of corrupted GA session terminated message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of corrupted GA session terminated message; no effect as reception of this message only makes sense after EVLF sends Terminate GA Session message to GADF.			No Effect	SRS • The EVLF can terminate the GA session by sending a Terminate GA session message; the GADF acknowledges with a GA session terminated message [2.2.1] Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.16.2	GA session terminated	**Deletion** Deletion of GA session terminated message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	GA session terminated message not received by GADF; EVLF does not receive acknowledgement from GADF for GA session termination request; EVLF resends request.			No Effect	SRS • The EVLF can terminate the GA session by sending a Terminate GA session message; the GADF acknowledges with a GA session terminated message [2.2.1]
6.4.16.3	GA session terminated	**Delay** Reception of delayed GA session terminated message	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Delayed reception of GA session terminated message			No Effect	
6.4.16.4	GA session terminated	**Repetition** Reception of repeated GA session terminated message	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of repeated GA session terminated message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
								secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.16.5	GA session terminated	**Re-sequence** Reception of out-of-sequence GA session terminated message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence GA session terminated message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.16.6	GA session terminated	**Insertion / Masquerade** Reception of inserted or masqueraded GA session terminated message	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of inserted / masqueraded GA session terminated message			No Effect	SRS: • The EVLF can terminate the GA session by sending a Terminate GA session message; the GADF acknowledges with a GA session terminated message [2.2.1] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
								protection origin authentication and message integrity)

6.4.17 GA Message Stream Suspended

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.17.1	GA message stream suspended	**Corruption** Reception of corrupted GA message stream suspended message	• Corruption of messages received over safe radio connection (e.g., due to bit errors caused by radio frequency interference / propagation environment) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of corrupted GA message stream suspended message; no effect as reception of this message only makes sense after EVLF sends a Suspend GA message stream message to GADF (NID_GAMS in acknowledgement would need to agree with that of request)			No Effect	SRS • The EVLF can suspend a GA message stream by sending a Suspend GA message stream message; the GADF acknowledges with a GA message stream suspended message [2.2.1] Safe Radio Connection: • Safe radio connection protocol shall provide protection against corruption (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides protection against corruption)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.4.17.2	GA message stream suspended	**Deletion** Deletion of GA message stream suspended message	• Safe radio connection message loss (e.g., due to excessive radio frequency interference in airgap) • Cyber-attack against safe radio connection (e.g., radio frequency jamming) • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	GA message stream suspended message not received by GADF; EVLF does not receive acknowledgement from GADF for Suspend GA message stream request; EVLF resends request.			No Effect	SRS • The EVLF can suspend a GA message stream by sending a Suspend GA message stream message; the GADF acknowledges with a GA message stream suspended message [2.2.1]
6.4.17.3	GA message stream suspended	**Delay** Reception of delayed GA message stream suspended message	• Delay due to safe radio connection (e.g., high utilisation of safe radio channel by other services) • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Delayed reception of GA message stream suspended message			No Effect	
6.4.17.4	GA message stream suspended	**Repetition** Reception of repeated GA message stream suspended	• Retransmissions due to safe radio connection message delay / loss • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of repeated GA message stream suspended message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against repetition [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
								secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.17.5	GA message stream suspended	**Re-sequence** Reception of out-of-sequence GA message stream suspended message	• Asynchronous, multiplexed, and bi-directional nature of safe radio connection • Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of out-of-sequence GA message stsream suspended message			No Effect	SRS: • Messages exchanged between GA-TS and GA-OB contain T_TRAIN (time, according to trainborne clock, at which message is sent) providing protection against out-of-sequence [2.2.24] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides origin authentication and message integrity)
6.4.17.6	GA message stream suspended	**Insertion / Masquerade** Reception of inserted or masqueraded GA message stream suspended message	• Cyber-attack against safe radio connection • EVLF hardware fault • EVLF software fault • GADF hardware fault • GADF software fault	Reception of inserted / masqueraded GA message stream suspended message			No Effect	SRS: • The EVLF can suspend a GA message stream by sending a Suspend GA message stream message; the GADF acknowledges with a GA message stream suspended message [2.2.1] Safe Radio Connection: • Safe radio connection protocol shall provide origin authentication and message integrity (e.g., Euroradio uses cryptographic safety code using secret key (type A1 from EN 50159), which provides

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
								protection origin authentication and message integrity)

6.5 FMEA GADF

6.5.1 Selection of GA Service and Channel

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.5.1.1	Selection of GA service and channel	**Erroneous** Erroneous selection of GA service and channel	• GADF software fault • GADF hardware fault	Selection of a service / service version not supported by EVLF	EVLF does not use service		No effect	GADF software and hardware design assurance (EN 50128, EN 50129)
6.5.1.2	Selection of GA service and channel	**Erroneous** Service reported in GA message stream allocated / resumed message does not correspond to the service from which messages are provided in the GA stream	• GADF software fault • GADF hardware fault	Service reported in GA message stream allocated / resumed message does not correspond to the service from which messages are provided in the GA stream; potentially hazardous	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Encapsulated messages that are incompatible with the reported service (different message structure) would fail CRC check. For compatible messages (e.g., SBAS with different service provider or channel (PRN) than expected), can be detected by EVLF from service provider ID and PRN in SBAS MTs.

6.5.2 Resumption of Suspended GA Message Streams

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.5.2.1	Resumption of suspended GA message stream	**Erroneous** Erroneous resumption of GA message stream (resumption before to acknowledgement of any alerts by EVLF)	• GADF software fault • GADF hardware fault	Alert sequences potentially missed (not acknowledged by EVLF); pseudorange errors potentially not bounded	Train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	GADF software and hardware design assurance (EN 50128, EN 50129)

6.6 FMEA GADF-GATF Interface (F2 ↔ F3)

6.6.1.1 The interface between the GADF and GATF has not been defined as this interface is not considered relevant for interoperability. It is currently assumed that the GADF and GATF are co-located (i.e., internal interface). Safety requirements for the internal interface are therefore the responsibility of the supplier.

6.6.1.2 It is currently an open point whether multiple GATFs shall be supported, via a standardised interface. If this is agreed, it will be addressed in a future issue of the SRS and SFHA.

6.7 FMEA GATF

6.7.1 Selection of GACs

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.7.1.1	Selection of GACs	**Erroneous** Erroneous selection of GA service and channel	• GATF software fault • GATF hardware fault	Selection of non-authorized service (i.e., without railway SoL service integrity commitments);	Use of non-authorized service by EVLF; train position error potentially not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	GATF software and hardware design assurance (EN 50128, EN 50129)

6.7.2 Timestamping Reception of Messages from GAS and Encapsulation in GAM Packets

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.7.2.1	Timestamping reception of messages from GAS	**Early, Late, Erroneous** Incorrect timestamp of reception of SBAS message by GATF ($T_{GATF,GAMrx}$)	• Erroneous CED, ranging data • Incorrect reference time (i.e., for SBAS, not SNT) • GATF software fault • GATF hardware fault	Incorrect timestamp; encapsulation of SBAS messages in GAM packets with incorrect timestamp	GA message with incorrect timestamp received by EVLF; erroneous message content supervision in EVLF; use of message content that is not valid; erroneous TTA supervision in EVLF; potential violation of maximum end to end TTA (T_NVGAMAXTTA); GNSS channel not transitioned to a safe state (i.e., within T_NVGAMAXTTA for missed / delayed GA messages that could be alerts);	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	GATF software and hardware design assurance (EN 50128, EN 50129)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
					pseudorange errors potentially not bounded; train position error not bounded by protection level			
6.7.2.2	Timestamping reception of messages from GAS	**No or Not** Timestamp of reception of SBAS message by GATF not available	• Insufficient number of GNSS satellites, (unavailable CED, ranging data) • GATF software fault • GATF hardware fault	Timestamp unavailable; encapsulation of SBAS messages in GAM packets with unknown timestamp	Reception of GA messages without timestamp by EVLF; TTA supervision unavailable; train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	

6.7.3 Maintain GNSS Navigation Data Sets

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.7.3.1	Maintain GNSS navigation data sets	**Erroneous** Erroneous navigation data sets	• Erroneous CED (due to failures of GATF-GNSS interface) • GATF software fault • GATF hardware fault	Erroneous CED sent to EVLF via GADF	Reception of GNSS navigation data set message with erroneous CED; erroneous GNSS ranging data; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	GATF software and hardware design assurance (EN 50128, EN 50129) GATF-GNSS Interface Barriers: • Refer to Section 6.9 (GATF-GNSS interface).
6.7.3.2	Maintain GNSS navigation data sets	**No or Not, Late** Last 4 different sets of GNSS navigation data for each visible satellite of the core	• Unavailable navigation data (due to failures of GATF-GNSS interface, radiofrequency interference) • GATF software fault	Last 4 different sets of GNSS navigation data for each visible satellite of the core constellations not available; only available	Reception of GNSS navigation data set message with IODs that do not match the current broadcast SBAS corrections;	Impact on operational availability (train delay)	RAM Issue	GATF software and hardware design assurance (EN 50128, EN 50129) GATF-GNSS Interface Barriers: • Refer to Section 6.9 (GATF-GNSS interface).

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
		constellations not maintained	• GATF hardware fault	sets of GNSS navigation data set to EVLF via GADF	train position with degraded performance or unavailable			

6.7.4 Maintain GA Active Data for Each GAC

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.7.4.1	Maintain GA active data for each GAC	**Erroneous** Erroneous GA active data	• Erroneous GA active data (due to failures of GATF-SBAS interface) • GATF software fault • GATF hardware fault	Erroneous GA active data sent to EVLF via GADF	Reception of GA active data with erroneous SBAS correction and/or integrity data; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	GATF software and hardware design assurance (EN 50128, EN 50129) GATF-SBAS Interface Barriers: • Refer to Section 6.8 (GATF-SBAS interface).
6.7.4.2	Maintain GA active data for each GAC	**No or Not, Late** GA active data (data most recently received that has not timed out) not maintained	• Unavailable GA active data (due to failures of GATF-SBAS interface, radiofrequency interference) • GATF software fault • GATF hardware fault	GA active data (data most recently received that has not timed out) not available	Reception of incomplete set of GA active data; delay for GNSS channel to become available with integrity due to time EVLF waits until complete active data set can be obtained via GA message reception (at SBAS broadcast update rate of 1 Hz)	Impact on operational availability (train delay)	RAM Issue	GATF software and hardware design assurance (EN 50128, EN 50129) GATF-GNSS Interface Barriers: • Refer to Section 6.8 (GATF-SBAS interface).

6.7.5 Maintain GA Active Alerts for Each GAC

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for functional failure modes)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.7.5.1	Maintain GA active alerts for each GAC	**Erroneous** Erroneous GA active alerts	• Erroneous GA active alerts (due to failures of GATF-SBAS interface) • GATF software fault • GATF hardware fault	Erroneous GA active alerts sent to EVLF via GADF when resuming a GA message stream	Reception of erroneous GA active alerts; erroneous SBAS integrity data; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	GATF software and hardware design assurance (EN 50128, EN 50129) GATF-SBAS Interface Barriers: • Refer to Section 6.8 (GATF-SBAS interface).
6.7.5.2	Maintain GA active alerts for each GAC	**No or Not, Late** GA active alerts not maintained	• Missed GA active alerts (due to failures of GATF-SBAS interface, radiofrequency interference) • GATF software fault • GATF hardware fault	Not all GA active alerts are sent to EVLF via GADF when resuming a GA message stream	GA active alerts missed and not processed by EVLF; pseudorange error potentially not bound; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	GATF software and hardware design assurance (EN 50128, EN 50129) GATF-GNSS Interface Barriers: • Refer to Section 6.8 (GATF-SBAS interface).

6.8 FMEA GATF-SBAS Interface (F3:IN<SBAS>)

6.8.1 Acquisition and Tracking of SBAS Signals (L1 and L5)

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.8.1.1	Acquisition and Tracking of SBAS signals	**Incorrect** Mistaking one SBAS L1 signal for 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. (Service provider ID verified by MT27 ensuring a supported provider is used – i.e., providing railway SoL service)	In the case of primary and secondary message streams provided to EVLF for redundancy, potentially two GACs (two different PRNs) are the same SBAS source (same PRN); no redundancy – i.e., event affecting primary message stream also affects secondary		RAM Issue	SBAS-TS-MOPS: • An acceptable means of preventing cross-correlation effects during acquisition is to reject the SBAS L1 signal if there is a 200 km separation between the satellite positions derived from the most recent almanac (received within 15 minutes) and the broadcast ephemerides [DMS:254].
6.8.1.2	Acquisition and Tracking of SBAS signals	**Incorrect** Mistaking one SBAS L5 signal for 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. (Service provider ID verified by MT47 ensuring a supported provider is used – i.e., providing railway SoL service)	In the case of primary and secondary message streams provided to EVLF for redundancy, potentially two GACs (two different PRNs) are the same SBAS source (same PRN); no redundancy – i.e., event affecting primary message stream also affects secondary		RAM Issue	SBAS-TS-MOPS: • After acquisition or reacquisition of any SBAS L5 signal, the use of any correction or integrity data collected from this signal shall be forbidden until reception of an MT 47 whose Broadcast Indicator is set to 1 and whose Satellite Slot Delta corresponds to the SBAS L5 PRN code number used for signal tracking, or until reception of an MT 39 whose Satellite Slot Delta corresponds to the SBAS L5 PRN code number used for signal tracking [DMS:030].

6.8.2 SBAS Data Demodulation, FEC Decoding and Processing

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.8.2.1	SBAS data	**Corruption** Reception of corrupted SBAS L1 data	• Interference environment (C/N0 degraded, increased BER) • Erroneous frame sync • Receiver hardware fault • Receiver firmware / software fault	Reception of erroneous SBAS message; erroneous SBAS data sent to EVLF via GADF	Erroneous SBAS correction and/or integrity data; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Receiver firmware / software and hardware design assurance SBAS-TS-MOPS: • Corruption detected by 24-bit CRC in SBAS message [SBAS L1 signal specification] • Frame synchronisation provided by correlation with 24-bit preamble (distributed over three successive 8-bit blocks for SBAS L1) [SBAS L1 signal specification]
6.8.2.2	SBAS data	**Corruption** Reception of corrupted SBAS L5 data	• Interference environment (C/N0 degraded, increased BER) • Erroneous frame sync • Receiver hardware fault • Receiver firmware / software fault	Reception of erroneous SBAS message; erroneous SBAS data sent to EVLF via GADF	Erroneous SBAS correction and/or integrity data; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Receiver firmware / software and hardware design assurance SBAS-TS-MOPS: • Corruption detected by 24-bit CRC in SBAS message [SBAS L5 signal specification] • Frame synchronisation provided by correlation with 24-bit preamble (distributed over six successive 4-bit blocks for SBAS L5) [SBAS L5 signal specification]

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.8.2.3	SBAS data	**Deletion** Deletion of SBAS L1 data	• Radiofrequency interference (C/N0 degraded below demodulation threshold) • Cyber-attack (intentional jamming) • Receiver hardware fault • Receiver firmware / software fault	Deletion of one or more SBAS messages; missed alert sequence or MT0	Pseudorange error potentially not bounded; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Receiver firmware / software and hardware design assurance SRS: • In the case of a communications link failure between the GATF and GAS (SBAS SIS), the GADF shall send a Message 62: GA Message to the EVLF requiring acknowledgement (M_ACK=1), with Packet 212 and Q_GAMT = 2 (DNU GA message stream) indicating that the EVLF shall no longer use the GA message stream [2.2.5]. • A communications link failure is indicated when no valid SBAS message has been received (by the GATF) for 4 seconds. [2.2.5]. • The EVLF shall cease using and discard any ranging data and GA data obtained from the GA message stream identified by the GA message [2.2.6]. • (Communication link failure is considered a low occurrence event assuming reliable reception of SBAS messages at the trackside) SBAS-TS-MOPS (GATF): • The data link broadcasts a valid message every second to provide a continuity of signal [SBAS L1 signal specification]

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.8.2.4	SBAS data	**Deletion** Deletion of SBAS L5 data	• Radiofrequency interference (C/N0 degraded below demodulation threshold) • Cyber-attack (intentional jamming) • Receiver hardware fault • Receiver firmware / software fault	Deletion of one or more SBAS messages; missed alert sequence or MT0	Pseudorange error potentially not bounded; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Receiver firmware / software and hardware design assurance SRS: • In the case of a communications link failure between the GATF and GAS (SBAS SIS), the GADF shall send a Message 62: GA Message to the EVLF requiring acknowledgement (M_ACK=1), with Packet 212 and Q_GAMT = 2 (DNU GA message stream) indicating that the EVLF shall no longer use the GA message stream [2.2.5]. • A communications link failure is indicated when no valid SBAS message has been received (by the GATF) for 4 seconds. [2.2.5]. • The EVLF shall cease using and discard any ranging data and GA data obtained from the GA message stream identified by the GA message [2.2.6]. • (Communication link failure is considered a low frequency event assuming reliable reception of SBAS messages at the trackside) SBAS-TS-MOPS (GATF): • The data link broadcasts a valid message every second to provide a continuity of signal [SBAS L5 signal specification]

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.8.2.5	SBAS data	**Delay** Delayed reception of SBAS L1 data	• Cyber-attack targeting SBAS signals (e.g., SBAS spoofing, record & replay) • Receiver hardware fault • Receiver firmware / software fault	Delayed reception of SBAS messages; delayed reception of alert sequences / MT0; potential timeout of message content; potential violation of TTA	Undetected delayed reception of GA messages by EVLF; pseudorange error potentially not bounded; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Receiver firmware / software and hardware design assurance SRS: • Barrier for detection of delay of L1 SBAS data (i.e., from cyber-attack related to SBAS signals received by the GATF) to be addressed in future issue of the SFHA. • If a cyber-attack is detected, the GADF shall send a Message 62: GA Message to the EVLF requiring acknowledgement (M_ACK=1), with Packet 212 and Q_GAMT = 2 (DNU GA message stream) indicating that the EVLF shall no longer use the GA message stream [2.2.5]

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.8.2.6	SBAS data	**Delay** Delayed reception of SBAS L5 data	• Cyber-attack targeting SBAS signals (e.g., SBAS spoofing, record & replay) • Receiver hardware fault • Receiver firmware / software fault	Delayed reception of SBAS messages; delayed reception of alert sequences / MT0; increased TTA (violation of TTA requirements)	Undetected delayed reception of GA messages by EVLF; incorrect supervision of message content timeouts; potential violation of T_NVGAMAXTTA; pseudorange error potentially not bounded; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Receiver firmware / software and hardware design assurance SBAS-TS-MOPS: • The equipment shall drop (i.e., stop tracking) an SBAS L5 signal (PRN code) and discard all previously received data from that signal (PRN code) if the following conditions are both met: a) The GNSS second of week is determined; and b) The equipment receives a message that passes the CRC, but whose 4-bit preamble block does not match the expected block corresponding to the GNSS second of the week. [DMS:235] SRS: • Barrier for detection of delay of L5 SBAS data (i.e., from cyber-attack related to SBAS signals received by the GATF) to be addressed in future issue of the SFHA. • If a cyber-attack is detected, the GADF shall send a Message 62: GA Message to the EVLF requiring acknowledgement (M_ACK=1), with Packet 212 and Q_GAMT = 2 (DNU GA message stream) indicating that the EVLF shall no longer use the GA message stream [2.2.5]

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.8.2.7	SBAS data	**Repetition, Re-sequence** Reception of repeated or out-of-sequence SBAS data	• Cyber-attack targeting SBAS signals (e.g., SBAS spoofing, record & replay) • Receiver hardware fault • Receiver firmware / software fault	Reception of a repeated or out-of-sequence SBAS messages; repeated or out-of-sequence SBAS messages sent to EVLF via GADF	Undetected reception of repeated or out-of-sequence SBAS messages by EVLF; incorrect supervision of message content timeouts; pseudorange error potentially not bounded; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Receiver firmware / software and hardware design assurance Cyber-attacks related to SBAS signals received by the GATF are to be addressed in a future issue of the SFHA.
6.8.2.8	SBAS data	**Insertion, Masquerade** Reception of non-authentic SBAS data designed to appear authentic	• Cyber-attack targeting SBAS signals (e.g., SBAS spoofing, record & replay)	Reception of erroneous SBAS data; erroneous SBAS data sent to EVLF via GADF	Undetected reception of erroneous SBAS data (corrections and integrity information) by EVLF; pseudorange error not bounded; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Receiver firmware / software and hardware design assurance Cyber-attacks related to SBAS signals received by the GATF are to be addressed in a future issue of the SFHA.

6.9 FMEA GATF-GNSS Interface (F3:IN<GNSS>)

6.9.1 Acquisition and Tracking of GNSS Signals

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.9.1.1	Acquisition and Tracking of GNSS Signals	**Incorrect** Mistaking one GPS L1 C/A code signal with another	• Cross-correlation effects during acquisition or reacquisition	GPS L1 C/A LNAV data does not correspond to PRN code number used for signal tracking; incorrect GNSS navigation data sent to EVLF via GADF	Reception of erroneous GNSS navigation data by EVLF; erroneous CED; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-TS-MOPS: • An acceptable means of compliance for acquisition is to reject L1 ranging data if there is a 3000 km separation between satellite positions computed from the L1 LNAV almanac and from the L1 LNAV ephemerides currently broadcast by the satellite [DMS:247]. • Requirement also applied to use of L1 LNAV data for GA-TS; ranging data is needed for SNT to support timestamp.
6.9.1.2	Acquisition and Tracking of GNSS Signals	**Incorrect** Mistaking one GPS L5 signal with another	• Cross-correlation effects during acquisition or reacquisition	GPS L5 C/NAV data does not correspond to PRN code number used for signal tracking	Reception of erroneous GNSS navigation data by EVLF; erroneous CED; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-TS-MOPS: • After acquisition, the equipment shall only use GPS L5 ranging data when the PRN code number used for signal tracking is confirmed at least once by the PRN parameter broadcast in L5 CNAV messages [DMS:015]. • Requirement also applied to use of L5 C/NAV data for GA-TS); ranging data is needed for SNT to support timestamp.

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.9.1.3	Acquisition and Tracking of GNSS Signals	**Incorrect** Mistaking one GAL E1 signal with another	• Cross-correlation effects during acquisition or reacquisition	Galileo E1 I/NAV data does not correspond to primary code number used for signal tracking	Reception of erroneous GNSS navigation data by EVLF; erroneous CED; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	SBAS-TS-MOPS: • After acquisition, the equipment shall only use Galileo E1 ranging data when the primary code number used for signal tracking is confirmed at least once by the satellite ID provided in E1 I/NAV Word Type 4 [DMS:023]. • Requirement also applied to use of E1 I/NAV data for GA-TS; ranging data is needed for SNT to support timestamp.
6.9.1.4	Acquisition and Tracking of GNSS Signals	**Incorrect** Mistaking one GAL E5a signal with another	• Cross-correlation effects during acquisition or reacquisition	Galileo E5a F/NAV data does not correspond to primary code number used for signal tracking	Reception of erroneous GNSS navigation data by EVLF; erroneous CED; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard		SBAS-TS-MOPS: • The equipment shall decode continuously E5a F/NAV and E1 I/NAV navigation data streams for each tracked Galileo satellite [DMS:021]. • Use of I/NAV to verify satellite ID (TBC)
6.9.1.5	Acquisition and Tracking of GNSS Signals	**Absent** Unable to acquire / track GNSS signals	• Radiofrequency interference • Cyber-attack (intentional jamming)	Degraded C/N0, below acquisition and tracking threshold	GNSS navigation data unavailable to EVLF; train position with degraded performance or unavailable until navigation can be received by EVLF from GNSS SIS	Impact on operational availability (train delay)	RAM Issue	Cyber-attacks related to GNSS signals received by the GATF are to be addressed in a future issue of the SFHA. External barriers: • Trackside GNSS receiver antennas shall be installed in an environment that is compliant with the requirements of the standard interference environment for trackside installations [to be addressed in a future specification – refer to open points].

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for discrete signals)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.9.1.6	Acquisition and Tracking of GNSS Signals	**Timing** Acquisition and tracking of delayed GNSS signals	• Cyber-attack targeting GNSS signals (e.g., GNSS meaconing, reradiation, record & replay) • Environment of trackside receiver (e.g., presence of multipath, etc.)	Erroneous GNSS ranging data; erroneous GATF time; erroneous timestamp (T_GAM in Packet 212) in GA messages	Reception of GA message with erroneous timestamp by EVLF; erroneous supervision of message content timeout; erroneous TTA supervision; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Cyber-attacks related to GNSS signals received by the GATF are to be addressed in a future issue of the SFHA (e.g., detection using PDM). External barriers: • Trackside GNSS receiver antennas shall be installed in an environment that is compliant with the requirements of the standard interference environment for trackside installations [to be addressed in a future specification – refer to open points]. • Trackside GNSS receiver antennas shall be installed in an environment that is compliant with the standard multipath environment for trackside installations [to be addressed in a future specification – refer to open points]. • The interference and multipath environment shall be monitored to ensure assumptions are met during operations [to be addressed in a future specification – refer to open points].
6.9.1.7	Acquisition and Tracking of GNSS Signals	**Insertion** Acquisition and tracking of non-authentic GNSS signals	• Cyber-attack targeting GNSS signals (e.g., GNSS spoofing, meaconing, reradiation, record & replay)	Erroneous GNSS ranging data; erroneous GATF time; erroneous timestamp (T_GAM in Packet 212) in GA messages	Reception of GA message with erroneous timestamp by EVLF; erroneous supervision of message content timeout; erroneous TTA supervision; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Cyber-attacks related to GNSS signals received by the GATF are to be addressed in a future issue of the SFHA (e.g., detection using PDM).

6.9.2 Navigation Data Demodulation, FEC Decoding and Processing

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.9.2.1	GNSS Navigation Data	**Corruption** Reception of corrupted GPS LNAV navigation data	• Interference environment (C/N0 degraded, increased BER) • Erroneous frame sync • Receiver hardware fault • Receiver firmware / software fault	Reception of subframe with corrupted word(s) resulting in use of erroneous CED; erroneous GNSS ranging data; erroneous GATF time	Reception of GA message with erroneous timestamp by EVLF; erroneous supervision of message content timeout; erroneous TTA supervision; reception of erroneous GNSS navigation data set; erroneous GNSS ranging data; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	IS-GPS-200: • Corruption detected by parity 6-bit parity for each 24-bit LNAV word (300-bit LNAV subframe of 10 words), words failing parity check discarded • 8-bit preamble in each subframe for frame sync SBAS-OB-MOPS: • Except for L1 LNAV information leading to the exclusion of a GPS satellite, the equipment shall only use clock and ephemeris data when it is verified by reception of a second message (subframes 1, 2, and 3 of the GPS L1 LNAV navigation message) containing the same data, with a broadcast IODE that matches the 8 least-significant bits of the broadcast IODC [DMS:249]. • Note: this requirement ensures residual risk of undetected corruption is acceptable.
6.9.2.2	GNSS Navigation Data	**Corruption** Reception of corrupted navigation data (GPS C/NAV, Galileo I/NAV, Galileo F/NAV)	• Interference environment (C/N0 degraded, increased BER) • Erroneous message/page sync • Receiver hardware fault • Receiver firmware / software fault	Reception of subframe with corrupted word(s) resulting in use of erroneous CED; erroneous GNSS ranging data; erroneous GATF time	Reception of GA message with erroneous timestamp by EVLF; erroneous supervision of message content timeout; erroneous TTA supervision; reception of erroneous GNSS navigation data set; erroneous GNSS ranging data; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	IS-GPS-705: • Corruption detected by 24-bit CRC in CNAV message • 8-bit preamble in each CNAV message for sync to message boundary GAL-OS-SIS-ICD: • Corruption detected by 24-bit CRC in I/NAV page • Corruption detected by 24-bit CRC in F/NAV word • 10-bit sync pattern in I/NAV page for sync to page boundary

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
								• 12-bit sync pattern in each F/NAV page for sync to page boundary
6.9.2.3	GNSS Navigation Data	**Deletion** Deleted GNSS navigation data	• Radiofrequency interference (C/N0 degraded below demodulation threshold) • Cyber-attack (intentional jamming) • Receiver hardware fault • Receiver firmware / software fault	GNSS navigation message not available for one or more satellites	GNSS navigation data set not available to EVLF; train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Cyber-attacks related to GNSS signals received by the GATF are to be addressed in a future issue of the SFHA (e.g., detection using PDM).
6.9.2.4	GNSS Navigation Data	**Delay, Repetition** Delay of GNSS navigation data / repetition of old navigation data (earlier IOD)	• Cyber-attack targeting GNSS signals (e.g., GNSS spoofing, record & replay) • Receiver hardware fault • Receiver firmware / software fault	Reception of old navigation data (earlier IOD)	Reception of old GNSS navigation data set by EVLF; applicable set of corrections (from SBAS messages) do not correspond to IODC/IODE or IODnav of GNSS navigation data; even if navigation data is still within curve fit interval, absence of GA corrections for IOD would result in unavailability; train position with degraded performance or unavailable	Impact on operational availability (train delay)	RAM Issue	Cyber-attacks related to GNSS signals received by the GATF are to be addressed in a future issue of the SFHA (e.g., detection using PDM).

Ref ID	Macro Function Data Item	Failure Mode (Guidewords for data transmission)	Failure Causes	Failure Effects			Severity	Internal Mitigation Barriers / Internal Barriers from SRS, MOPS, ICD
				Local Effect	Intermediate Effect	Initial End Effect		
6.9.2.5	GNSS Navigation Data	**Insertion, Masquerade** Reception of non-authentic navigation data designed to appear authentic	• Cyber-attack targeting GNSS signals (e.g., GNSS spoofing / record & replay)	Erroneous CED; erroneous GNSS ranging data; erroneous GATF time	Reception of GA message with erroneous timestamp by EVLF; erroneous supervision of message content timeout; erroneous TTA supervision; reception of erroneous GNSS navigation data set; erroneous GNSS ranging data; train position error not bounded by protection level	GATE58 (Incorrect determination of train position ref to LRBG), ETCS Core Hazard	Critical	Cyber-attacks related to GNSS signals received by the GATF are to be addressed in a future issue of the SFHA (e.g., detection using PDM).
6.9.2.6	GNSS Navigation Data	**Re-sequence** Out of sequence (messages / subframes / pages)	• Cyber-attack targeting GNSS signals (e.g., GNSS spoofing) • Receiver hardware fault • Receiver firmware / software fault	Reception of GNSS navigation messages / subframes / pages out of sequence (i.e., with respect to frame / subframe layout in ICD)			No Effect	Cyber-attacks related to GNSS signals received by the GATF are to be addressed in a future issue of the SFHA (e.g., detection using PDM).

7 Safety Requirements

7.1.1.1 This section defines generic high-level quantitative safety requirements needed for technical interoperability of the GA for ERTMS/ETCS. Note: user-level safety requirements specific to the GA service are contained within the GA-OB-MOPS (i.e., for legacy and DFMC railway SoL services, refer to [ESSP-TN-25931] and [ESSP-TN-26136]). Safety requirements specific to the trackside interface with the GAS are contained within the GA-TS-MOPS (i.e., for legacy and DFMC railway So services, refer to [ESSP-TN-26038] and [ESSP-TN-26137]).

7.1.1.2 Safety requirements are given as tolerable hazard rates (THRs) and tolerable functional failure rates (TFFRs). Apportionment to GA on-board (GA-OB), GA trackside (GA-TS) and the GA transmission channels is performed in Annex B. Safety integrity levels (SILs) shall be derived from the THRs / TFFRs.

7.1.1.3 The dangerous failures of the GA on-board and trackside elements are connected to the GA top-level hazard:

PRIR: Pseudorange integrity risk (correction residual or ionospheric vertical error not bound and TTA > T_NVGAMAXTTA).

7.2 GA On-board (GA-OB)

7.2.1 Enhanced Vehicle Localisation Function (EVLF)

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: 1.0E-8 dangerous failures / hour

7.2.1.1 Attainment of $THR_{GA\text{-}OB}$ shall consider at least the following events (refer to Annex B, B.2.4)[7]:

- F1.5: Failure of function for timestamping reception of GA message from GADF
- F1.6: Failure of TTA supervision
- F1.7: SBAS message content timeout supervision function failure
- F1.8: Failure of GA message processing function
- F1.9: Failure if GNSS signal processing including:
  - F1.9.1: Failure of GNSS pre-correlation signal processing function
  - F1.9.2: Failure of GNSS signal acquisition and tracking function
  - F1.9.3: Failure of GNSS navigation data demodulation and FEC decoding function
  - F1.9.4: Failure of GNSS navigation data processing function
- F1.10: Failure of GNSS pseudorange determination and use function
- F1.11: Failure of function for computation and application of GA corrections to smoothed pseudorange

[7] Note that direct reception of SBAS messages by the EVLF via the SBAS SIS is not currently considered but shall be addressed in a future release of this document.

- F1.12: Failure of function for computation and application of GNSS pseudorange error models
- TRANS-EVLF: safety radio transmission function including (trusted parts):
  - EVLF-RADIO-H1: Radio message corrupted in EVLF such that message appears as consistent
  - EVLF-RADIO-H2: Radio message deleted in EVLF in an undetectable way
  - EVLF-RADIO-H3: Radio message inserted in EVLF such that message appears as consistent

7.3 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: 1.1E-8 dangerous failures / hour

7.3.1.1 Attainment of $THR_{GA\text{-}TS}$ shall consider at least the following events (refer to Annex B, B.2.3):

GATF events:

- F3.8: Failure of function for timestamping reception of messages from SBAS SIS
- F3.11: GNSS signal processing failure including:
  - F3.11.1: Failure of GNSS signal acquisition and tracking function
  - F3.11.2: Failure of GNSS navigation data demodulation and FEC decoding function
  - F3.11.3: Failure of GNSS navigation data processing
- F3.12: SBAS signal processing failure including:
  - F3.12.1: Failure of SBAS L1 / L5 signal acquisition and tracking function
  - F3.12.2/3: Failure of SBAS L1 / L5 demodulation and FEC decoding function
  - F3.12.4/5. Failure of SBAS L1 / L5 message processing function

GADF events:

- F2.11: Failure of resume suspended GA message stream function
- TRANS-GADF: Safety-related radio transmission function (trusted parts)
  - GADF-RADIO-H1: Radio message corrupted in GADF such that message appears as consistent
  - GADF-RADIO-H2: Radio message deleted in GADF in an undetectable way
  - GADF-RADIO-H3: Radio message inserted in EVLF such that message appears as consistent

7.4 GA Transmission Channels

7.4.1 SBAS SIS to GATF transmission channel

SBAS-GATF/GA-UCR	**Undetected SBAS message corruption** The THR for the GATF non-trusted part of the SBAS SIS to GATF transmission channel related to message corruption is: 5.4E-8 dangerous failures / hour For EGNOS L1 and L5 SBAS messages, the hazard rate has been estimated as 5.36E-8 / hour.
SBAS-GATF/GA-UIM	**Undetected inserted / masqueraded SBAS message** The THR for the GATF non-trusted part of the SBAS SIS to GATF transmission channel related to message insertion / masquerade (SBAS spoofing) is: 1.0E-8 dangerous failures / hour [UNSTABLE] Note: cyber-security barriers to be defined in the next release of this document
SBAS-GATF/GA-UDL	**Undetected SBAS message delay** The THR for the GATF non-trusted part of the SBAS SIS to GATF transmission channel related to GNSS signal spoofing (signal delay) is: 1.0E-8 dangerous failures / hour [UNSTABLE] Note: cyber-security barriers to be defined in the next release of this document

7.4.2 GNSS to GATF transmission channel

GNSS-GATF/GN-UCR	**Undetected GNSS navigation message corruption** The THR for the GATF non-trusted part of the GNSS SIS to GATF transmission channel related to message corruption is: 5.0E-9 dangerous failures / hour For EGNOS DFMC (GPS + Galileo) railway safety of life service, the hazard rate has been estimated as 3.47E-9 / hour.
GNSS-GATF/GN-UIM/USI	**Undetected inserted GNSS signal / masqueraded GNSS navigation message** The THR for the GATF non-trusted part of the GNSS SIS to GATF transmission channel related to GNSS spoofing hazards is: 1.0E-8 dangerous failures / hour [UNSTABLE] Note: cyber-security barriers to be defined in the next release of this document
GNSS-GATF/GN-USD	**Undetected delay of GNSS signals** The THR for the GATF non-trusted part of the GNSS SIS to GATF transmission channel related to GNSS signal spoofing (signal delay) is: 1.0E-8 dangerous failures / hour [UNSTABLE]

	Note: cyber-security barriers to be defined in the next release of this document

7.4.3 GADF to EVLF transmission channel

7.4.3.1 The TRANS-EVLF/RADIO-1 and TRANS-GADF/RADIO-1 allocations of CH/GADF-EVLF reflect the bi-directional nature of the safe radio connection and that the potential for corruption is present in either direction (GADF to EVLF or EVLF to GADF).

TRANS-EVLF/RADIO-1	**Corruption of radio messages** The THR for the EVLF non-trusted part of the GADF to EVLF transmission channel related to message corruption is: 1.0E-11 dangerous failures / hour
TRANS-GADF/RADIO-1	**Corruption of radio messages** The THR for the GADF non-trusted part of the EVLF to GADF transmission channel related to message corruption: 1.0E-11 dangerous failures / hour

7.4.4 GNSS to EVLF transmission channel

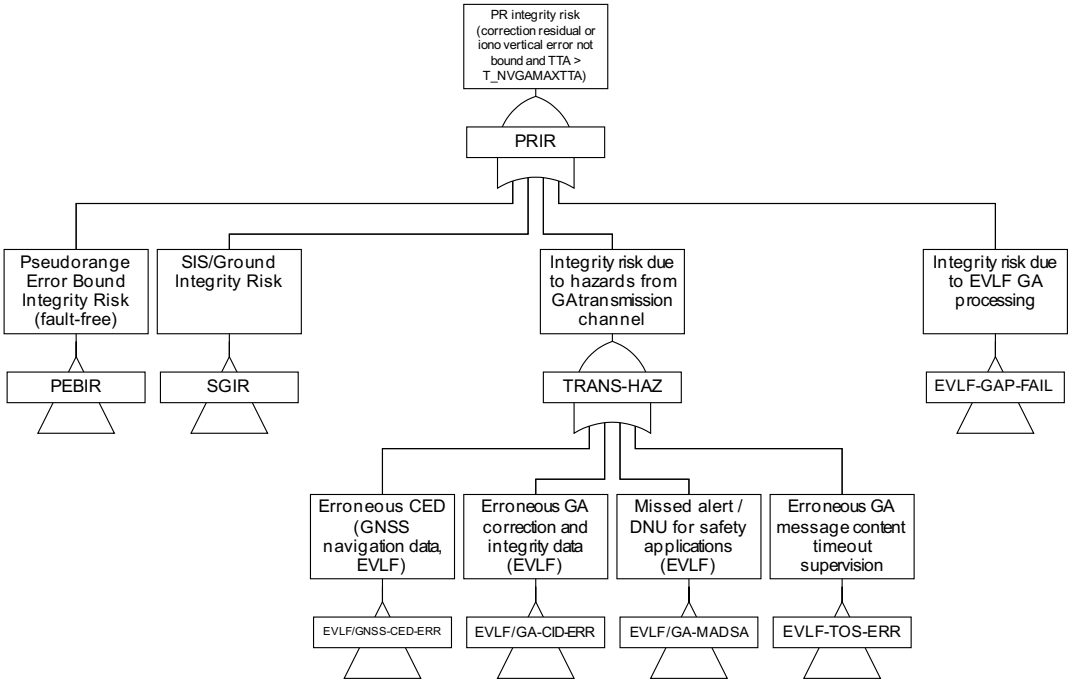
GNSS-EVLF/GN-UCR	**Undetected GNSS navigation message corruption** The THR for the EVLF non-trusted part of the GNSS SIS to EVLF transmission channel related to message corruption is: 7.1E-8 dangerous failures / hour For EGNOS DFMC (GPS + Galileo) railway safety of life service, the hazard rate has been estimated as 7.07E-8 / hour.
GNSS-EVLF/GN-UIM/USI	**Undetected inserted GNSS signal / masqueraded GNSS navigation message** The THR for the EVLF non-trusted part of the GNSS SIS to EVLF transmission channel related to GNSS spoofing hazards is: 1.0E-8 dangerous failures / hour [UNSTABLE] Note: cyber-security barriers to be defined in the next release of this document
GNSS-GATF/GN-USD	**Undetected delay of GNSS signals** The THR for the GATF non-trusted part of the GNSS SIS to GATF transmission channel related to GNSS signal spoofing (signal delay) is: 1.0E-8 dangerous failures / hour [UNSTABLE] Note: cyber-security barriers to be defined in the next release of this document

GNSS-GATF/GN-USI	**Undetected insertion of GNSS signals** The THR for the GATF non-trusted part of the GNSS SIS to GATF transmission channel related to GNSS signal spoofing (signal synthesis) is: 1.0E-8 dangerous failures / hour [UNSTABLE] Note: cyber-security barriers to be defined in the next release of this document

Annex A Functional Fault Tree

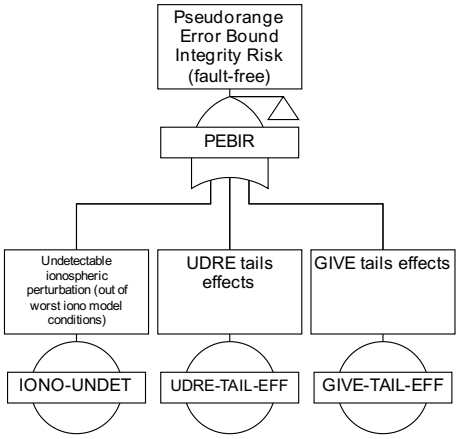
A.1.1.1 A preliminary functional fault tree analysis is provided in this annex using the failure modes identified in the FMEA for GNSS Augmentation for ERTMS/ETCS based on SBAS Legacy and DFMC services.

A.2 Pseudorange Integrity Risk



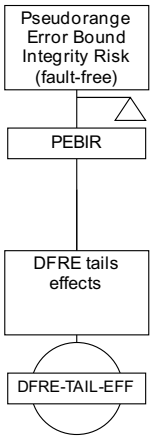
ID	Gate / Event	Description
PRIR	Pseudorange integrity risk (correction residual or ionospheric vertical error not bound and TTA > T_NVGAMAXTTA)	
PEBIR	Pseudorange Error Bound Integrity Risk (fault-free)	
SGIR	SIS / Ground integrity risk	
TRANS-HAZ	Integrity risk due to hazards from the GA transmission channel	
EVLF/GNSS-CED-ERR	Erroneous CED (GNSS navigation data)	
EVLF/GA-CID-ERR	Erroneous GA correction and integrity data	
EVLF/GA-MADSA	Missed alert / GNU for safety applications (EVLF)	
EVLF-TOS-ERR	Erroneous GA message content timeout supervision	
EVLF-GAP-FAIL	Integrity risk due to EVLF GA processing	

A.3 PEBIR: Pseudorange Error Bound Integrity Risk (Legacy Railway SoL Service)



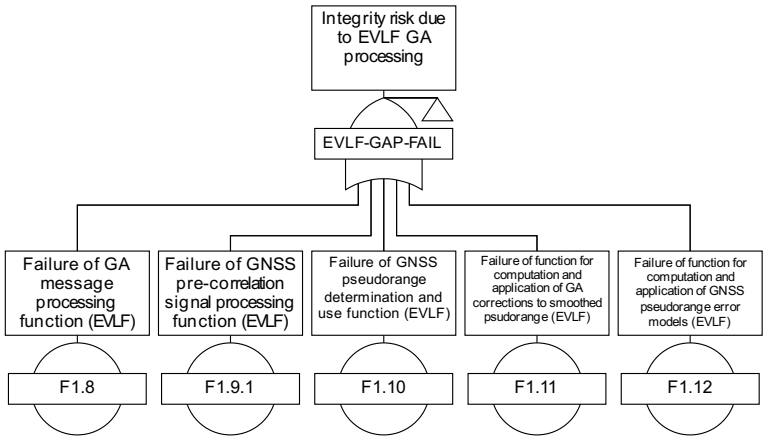
ID	Gate / Event	Description
PEBIR	Pseudorange Error Bound Integrity Risk (fault-free)	(Transfer gate)
IONO-UNDET	Undetectable ionospheric perturbation (out of worst ionospheric model conditions)	Residual risk related to undetectable ionospheric perturbation outside the worst-case ionospheric model conditions.
UDRE-TAIL-EFF	UDRE tail effects	Residual risk related to tail effects of the error distributions that were not bounded by the UDRE to the target level of integrity.
GIVE-TAIL-EFF	GIVE tail effects	Residual risk related to tail effects of the error distributions that were not bounded by the GIVE to the target level of integrity.

A.4 PEBIR: Pseudorange Error Bound Integrity Risk (DFMC Railway SoL Service)



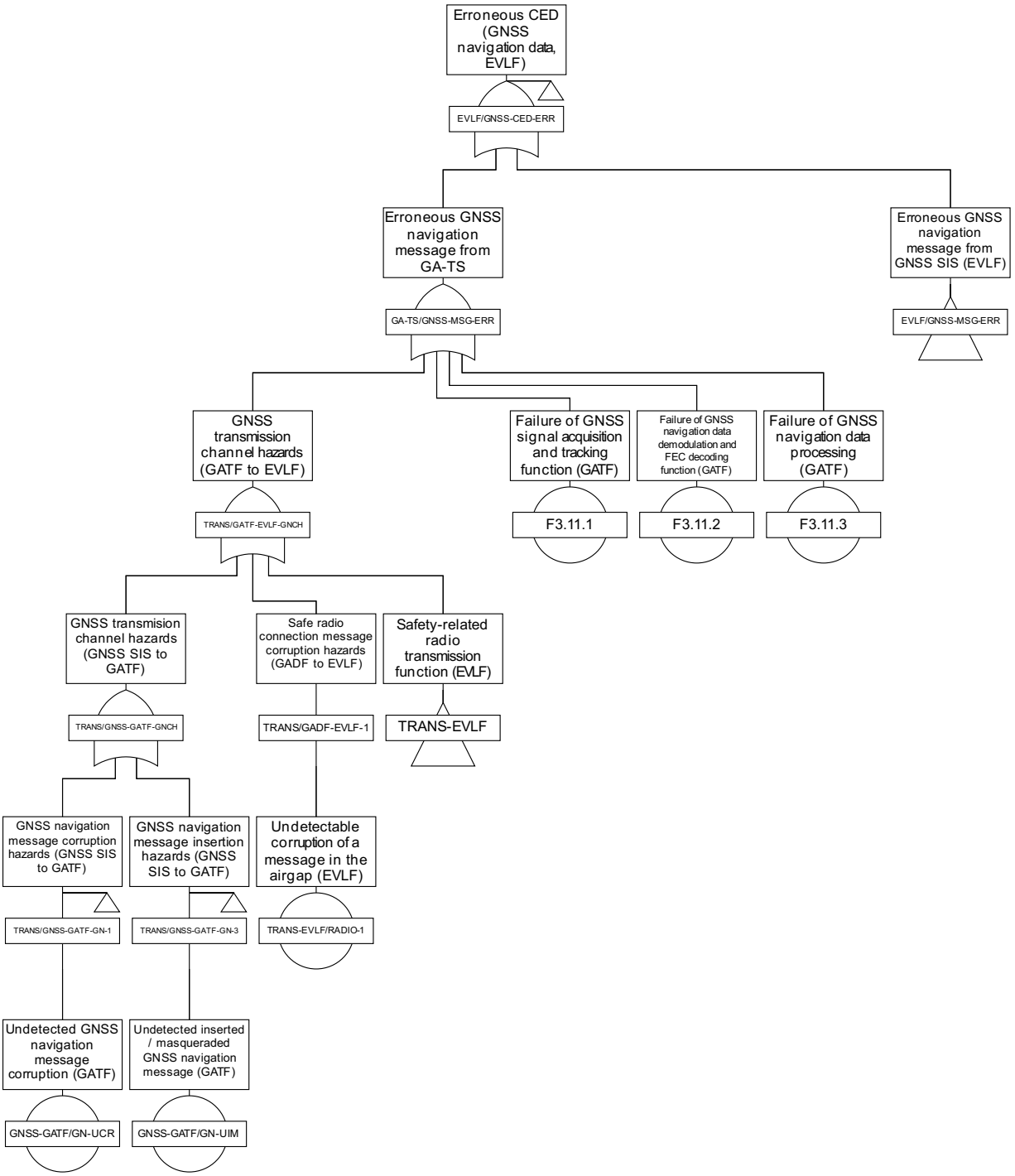
ID	Gate / Event	Description
PEBIR	Pseudorange Error Bound Integrity Risk (fault-free)	(Transfer gate)
DFRE-TAIL-EFF	DFRE tail effects	Residual risk related to tail effects of the error distributions that were not bounded by the DFRE to the target level of integrity.

A.5 EVLF-GAP-FAIL: Integrity Risk due to EVLF GA Processing



ID	Gate / Event	Description
EVLF-GAP-FAIL	Integrity risk due to EVLF GA processing	(Transfer gate)
F1.8	Failure of GA message processing function (EVLF)	
F1.9.1	Failure of GNSS pre-correlation signal processing function (EVLF)	
F1.10	Failure of GNSS pseudorange determination and use function (EVLF)	
F1.11	Failure of function or computation and application of GA corrections to smoothed pseudorange (EVLF)	
F1.12	Failure of function for computation and application of GNSS pseudorange error models (EVLF)	

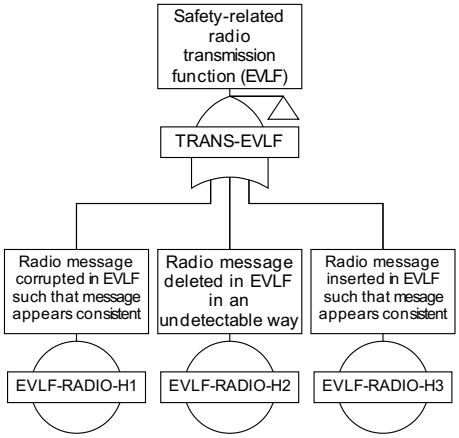
A.6 GNSS-CED-ERR: Erroneous CED (GNSS navigation data, EVLF)



ID	Gate / Event	Description
EVLF/GNSS-CED-ERR	Erroneous CED (GNSS navigation data, EVLF)	(Transfer gate)
GA-TS/GNSS-MSG-ERR	Erroneous GNSS navigation message from GA-TS	
TRANS/GATF-EVLF-GNCH	GNSS transmission channel hazards (GNSS SIS to GATF)	

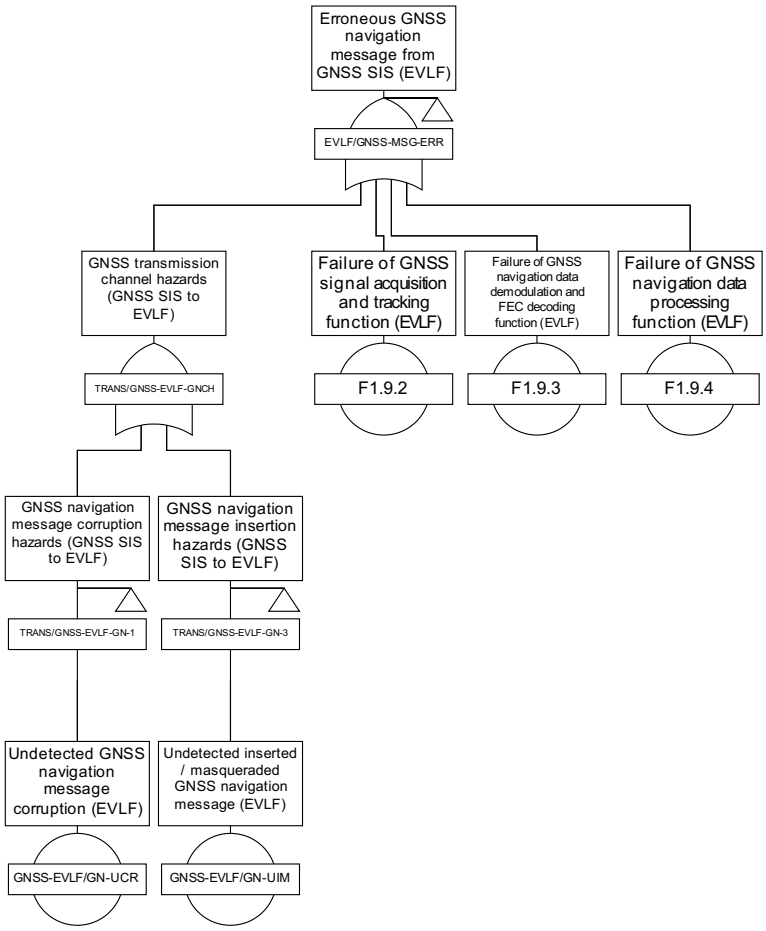
TRANS/GNSS-GATF-GNCH	GNSS transmission channel hazards (GNSS SIS to GATF)	
TRANS/GNSS-GATF-GN-1	GNSS navigation message corruption hazards (GNSS SIS to GATF)	
GNSS-GATF/GN-UCR	Undetected GNSS navigation message corruption (GATF)	
TRANS/GNSS-GATF-GN-3	GNSS navigation message insertion hazards (GNSS SIS to GATF)	
GNSS-GATF/GN-UIM	Undetected inserted / masqueraded GNSS navigation message (GATF)	(e.g., from cyber-attack: spoofing)
TRANS/GADF-EVLF-1	Safe radio connection message corruption hazards (GADF to EVLF)	
TRANS-EVLF/RADIO-1	Undetectable corruption of a message in the airgap (EVLF)	
TRANS-EVLF	Safety-related radio transmission function (EVLF)	
F3.11.1	Failure of GNSS signal acquisition and tracking function (GATF)	
F3.11.2	Failure of GNSS navigation data demodulation and FEC decoding function (GATF)	
F3.11.3	Failure of GNSS navigation data processing (GATF)	
EVLF/GNSS-MSG-ERR	Erroneous GNSS navigation message from GNSS SIS (EVLF)	

A.7 TRANS-EVLF: Safety-related radio transmission function (EVLF)



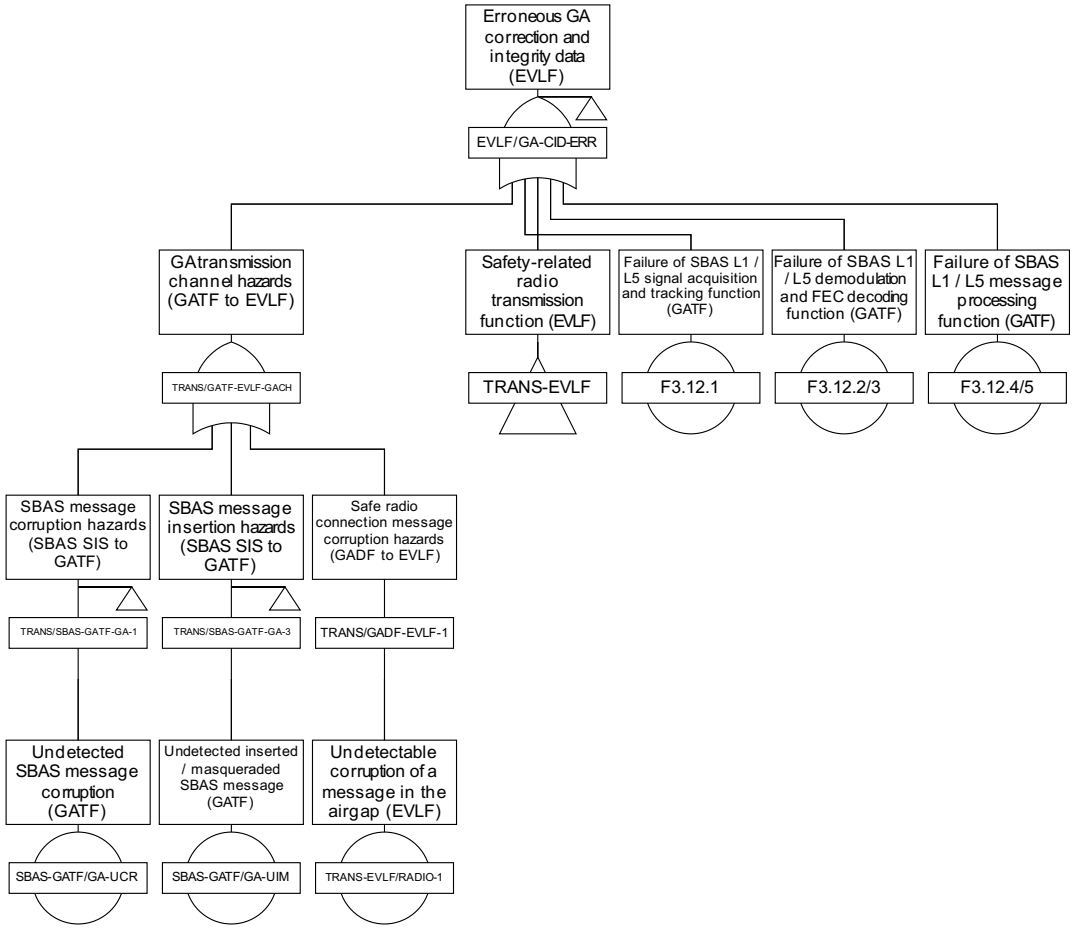
ID	Gate / Event	Description
TRANS-EVLF	Safety-related radio transmission function (EVLF)	(Transfer gate)
EVLF-RADIO-H1	Radio message corrupted in EVLF such that message appears consistent	
EVLF-RADIO-H2	Radio message deleted in EVLF in an undetectable way	
EVLF-RADIO-H3	Radio message inserted in EVLF such that message appears consistent	

A.8 EVLF/GNSS-MSG-ERR: Erroneous GNSS navigation message from GNSS SIS (EVLF)



ID	Gate / Event	Description
EVLF/GNSS-MSG-ERR	Erroneous GNSS navigation message from GNSS SIS (EVLF)	(Transfer gate)
TRANS/GNSS-EVLF-GNCH	GNSS transmission channel hazards (GNSS SIS to EVLF)	
TRANS/GNSS-EVLF-GN-1	GNSS navigation message corruption hazards (GNSS SIS to EVLF)	
GNSS-EVLF/GN-UCR	Undetected GNSS navigation message corruption (EVLF)	
TRANS/GNSS-EVLF-GN-3	GNSS navigation message insertion hazards (GNSS SIS to EVLF)	
GNSS-EVLF/GN-UIM	Undetected inserted / masqueraded GNSS navigation message (EVLF)	(e.g., from cyber-attack: spoofing)
F1.9.2	Failure of GNSS signal acquisition and tracking function (EVLF)	
F1.9.3	Failure of GNSS navigation data demodulation and FEC decoding function (EVLF)	
F1.9.4	Failure of GNSS navigation data processing function (EVLF)	

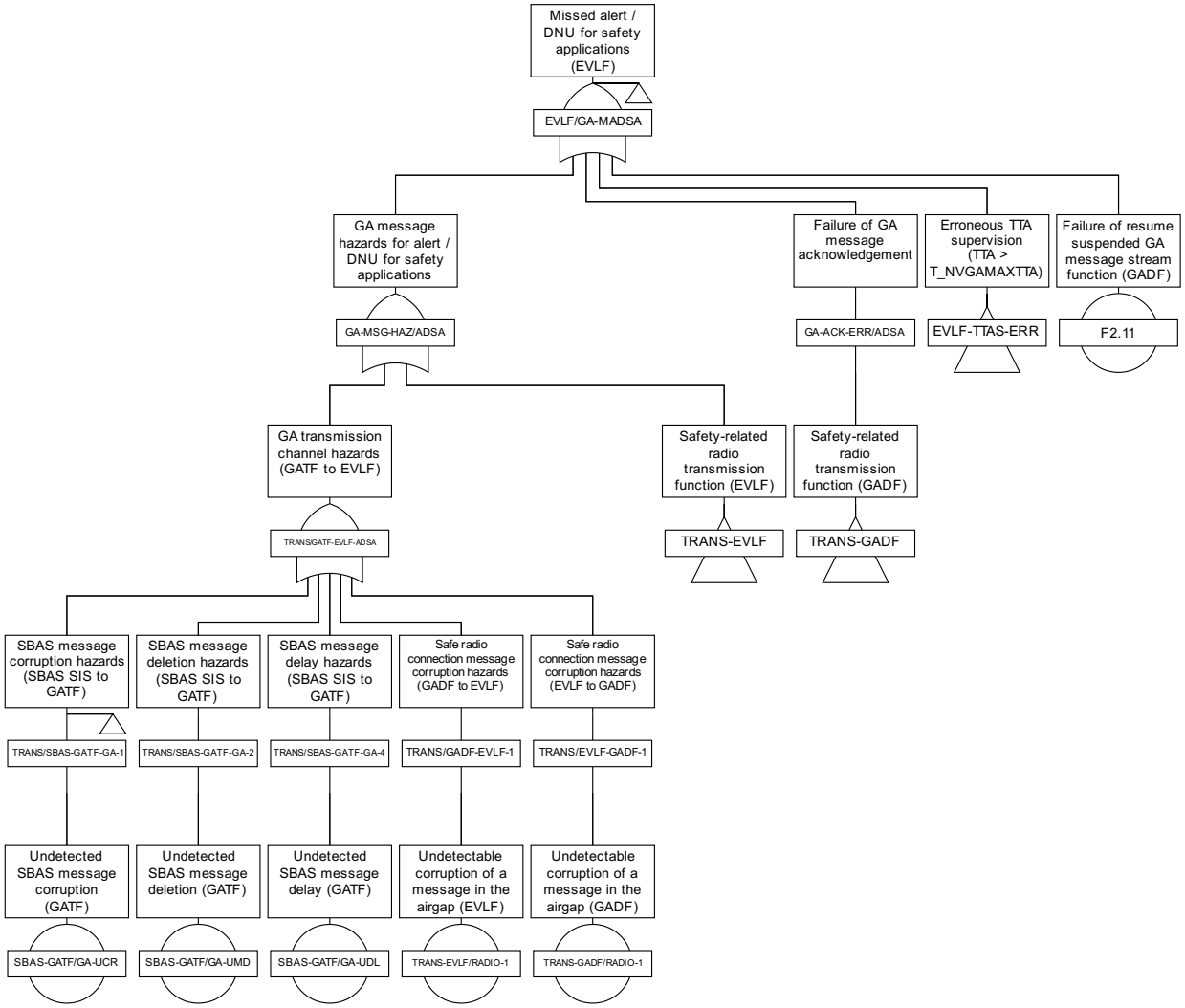
A.9 EVLF/GA-CID-ERR: Erroneous GA correction and integrity data



ID	Gate / Event	Description
EVLF/GA-CID-ERR	Erroneous GA correction and integrity data (EVLF)	(Transfer gate)
TRANS/GATF-EVLF-GACH	GA transmission channel hazards (GATF to EVLF)	
TRANS/SBAS-GATF-GA-1	SBAS message corruption hazards (SBAS SIS to GATF)	
SBAS-GATF/GA-UCR	Undetected SBAS message corruption (GATF)	
TRANS/SBAS-GATF-GA-3	SBAS message insertion hazards (SBAS SIS to GATF)	
SBAS-GATF/GA-UIM	Undetected inserted / masqueraded SBAS message (GATF)	(e.g., from cyber-attack: spoofing)
TRANS/GADF-EVLF-1	Safe radio connection message corruption hazards (GADF to EVLF)	
TRANS-EVLF/RADIO-1	Undetectable corruption of a message in the airgap (EVLF)	
TRANS-EVLF	Safety-related radio transmission function (EVLF)	
F3.12.1	Failure of SBAS L1 / L5 signal acquisition and tracking function (GATF)	
F3.12.2/3	Failure of SBAS L1 / L5 demodulation and FEC decoding function (GATF)	

F3.12.4/5	Failure of SBAS L1 / L5 message processing function (GATF)	

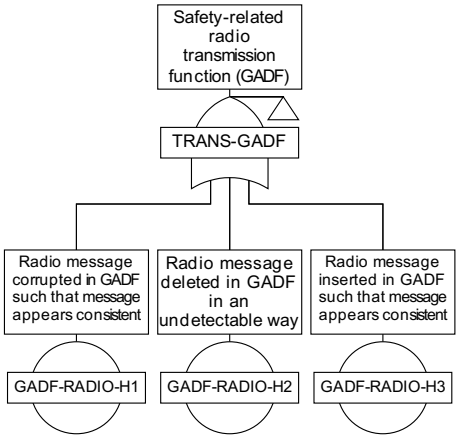
A.10 EVLF/GA-MADSA: Missed alert / DNU for safety applications



ID	Gate / Event	Description
EVLF/GA-MADSA	Missed alert / DNU for safety applications (EVLF)	(Transfer gate)
GA-MSG-HAZ/ADSA	GA message hazards for alert / DNU for safety applications	
TRANS/GATF-EVLF-ADSA	GA transmission channel hazards (GATF to EVLF)	
TRANS/SBAS-GATF-GA-1	SBAS message corruption hazards (SBAS SIS to GATF)	
SBAS-GATF/GA-UCR	Undetected SBAS message corruption (GATF)	
TRANS/SBAS-GATF-GA-2	SBAS message deletion hazards (SBAS SIS to GATF)	
SBAS-GATF/GA-UMD	Undetected SBAS message deletion (GATF)	
TRANS/SBAS-GATF-GA-4	SBAS message delay hazards (SBAS SIS to GATF)	
SBAS-GATF/GA-UDL	Undetected SBAS message delay (GATF)	(e.g., from cyber-attack: record & replay / meaconing)
TRANS/GADF-EVLF-1	Safe radio connection message corruption hazards (GADF to EVLF)	

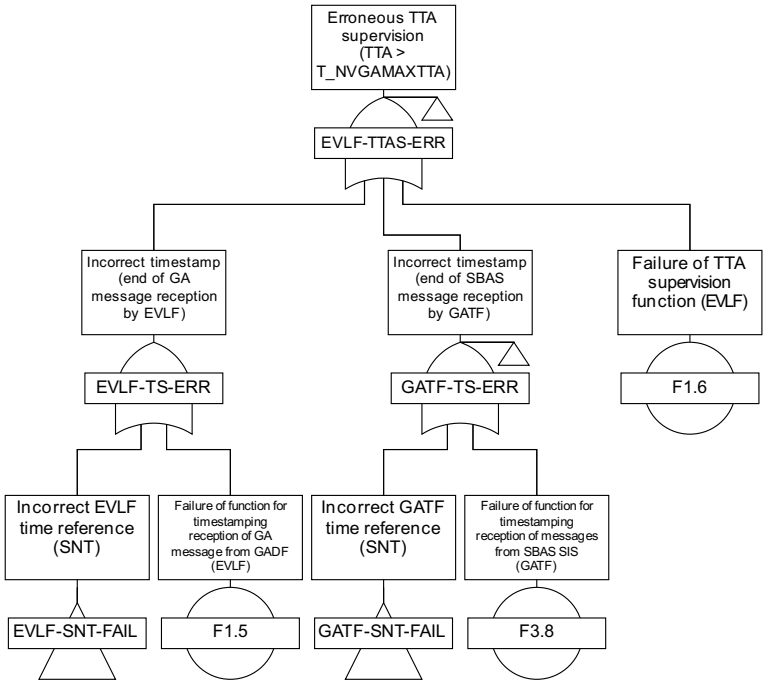
TRANS-EVLF/RADIO-1	Undetectable corruption of a message in the airgap (EVLF)	
TRANS/EVLF-GADF-1	Safe radio connection message corruption hazards (EVLF to GADF)	
TRANS-GADF/RADIO-1	Undetectable corruption of a message in the airgap (GADF)	
TRANS-EVLF	Safety-related radio transmission function (EVLF)	
GA-ACK-ERR/ADSA	Failure of GA message acknowledgement	
TRANS-GADF	Safety-related radio transmission function (GADF)	
EVLF-TTAS-ERR	Erroneous TTA supervision (TTA > T_NVGAXTTA)	
F2.11	Failure of resume suspended GA message stream function (GADF)	

A.11 TRANS-GADF: Safety-related radio transmission function (GADF)



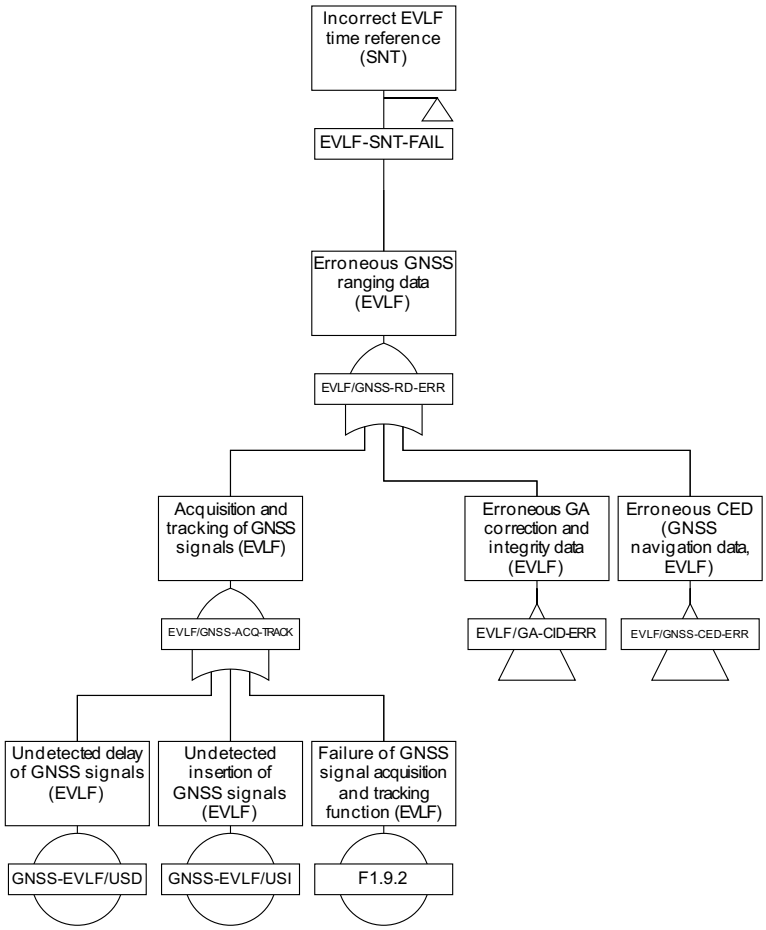
ID	Gate / Event	Description
TRANS-GADF	Safety-related radio transmission function (GADF)	(Transfer gate)
GADF-RADIO-H1	Radio message corrupted in GADF such that message appears consistent	
GADF-RADIO-H2	Radio message deleted in GADF in an undetectable way	
GADF-RADIO-H3	Radio message inserted in GADF such that message appears consistent	

A.12 EVLF-TTAS-ERR: Erroneous TTA supervision (TTA > T_NVGAMAXTTA)



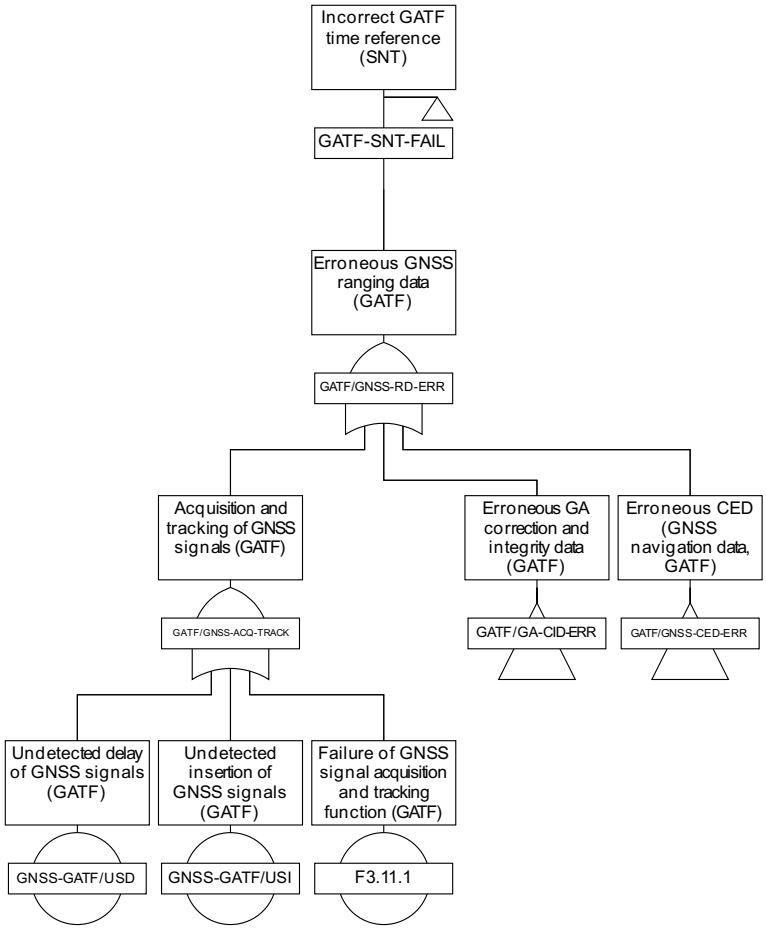
ID	Gate / Event	Description
EVLF-TTAS-ERR	Erroneous TTA supervision (TTA > T_NVGAMAXTTA)	(Transfer gate)
EVLF-TS-ERR	Incorrect timestamp (end of GA message reception by EVLF)	
EVLF-SNT-FAIL	Incorrect EVLF time reference (SNT)	
F1.5	Failure of function for timestamping reception of GA message from GADF (EVLF)	
GATF-TS-ERR	Incorrect timestamp (end of SBAS message reception by GATF)	
GATF-SNT-FAIL	Incorrect GATF time reference (SNT)	
F3.8	Failure of function for timestamping reception of messages from SBAS SIS (GATF)	
F1.6	Failure of TTA supervision function (EVLF)	

A.13 EVLF-SNT-FAIL: Incorrect EVLF time reference (SNT)



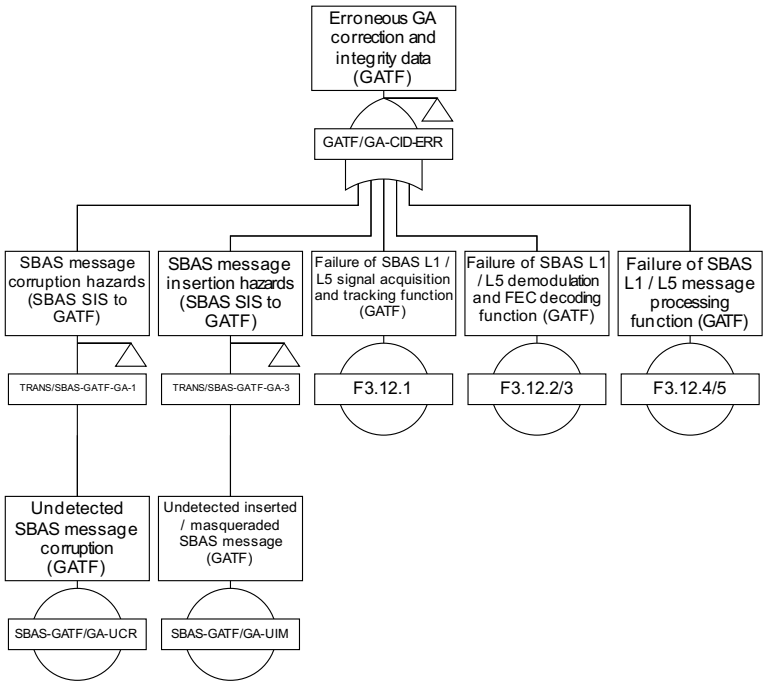
ID	Gate / Event	Description
EVLF-SNT-FAIL	Incorrect EVLF time reference (SNT)	(Transfer gate)
EVLF/GNSS-RD-ERR	Erroneous GNSS ranging data (EVLF)	
EVLF/GNSS-ACQ-TRACK	Acquisition and tracking of GNSS signals (EVLF)	
GNSS-EVLF/USD	Undetected delay of GNSS signals (EVLF)	(e.g., from cyber-attack: record & replay / meaconing)
GNSS-EVLF/USI	Undetected insertion of GNSS signals (EVLF)	(e.g., from cyber-attack: spoofing)
F1.9.2	Failure of GNSS signal acquisition and tracking function (EVLF)	
EVLF/GA-CID-ERR	Erroneous GA correction and integrity data (EVLF)	
EVLF/GNSS-CED-ERR	Erroneous CED (GNSS navigation data, EVLF)	

A.14 GATF-SNT-FAIL: Incorrect GATF time reference (SNT)



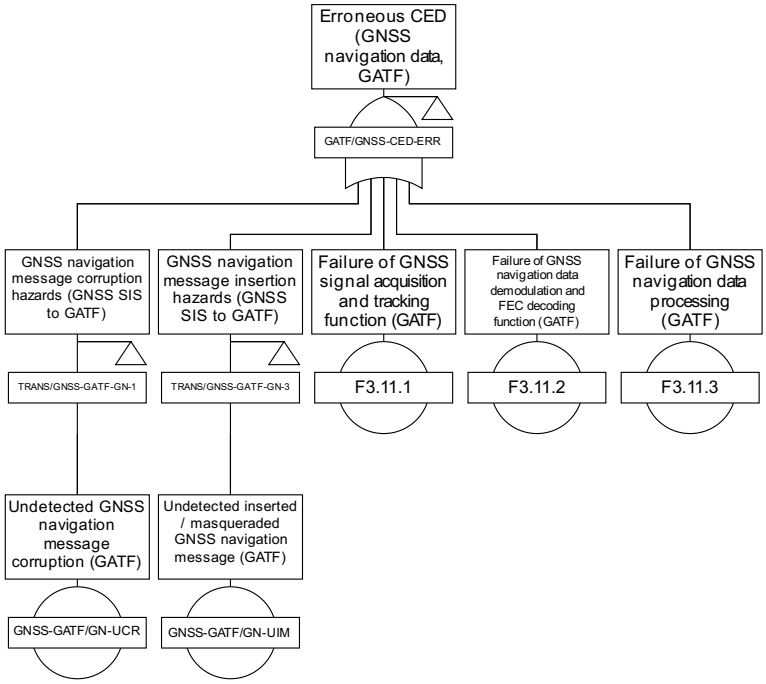
ID	Gate / Event	Description
GATF-SNT-FAIL	Incorrect GATF time reference (SNT)	(Transfer gate)
GATF/GNSS-RD-ERR	Erroneous GNSS ranging data (GATF)	
GATF/GNSS-ACQ-TRACK	Acquisition and tracking of GNSS signals (GATF)	
GNSS-GATF/USD	Undetected delay of GNSS signals (GATF)	(e.g., from cyber-attack: record & replay / meaconing)
GNSS-GATF/USI	Undetected insertion of GNSS signals (GATF)	(e.g., from cyber-attack: spoofing)
F3.11.1	Failure of GNSS signal acquisition and tracking function (GATF)	
GATF/GA-CID-ERR	Erroneous GA correction and integrity data (GATF)	
GATF/GNSS-CED-ERR	Erroneous CED (GNSS navigation data, GATF)	

A.15 GATF/GA-CID-ERR: Erroneous GA correction and integrity data (GATF)



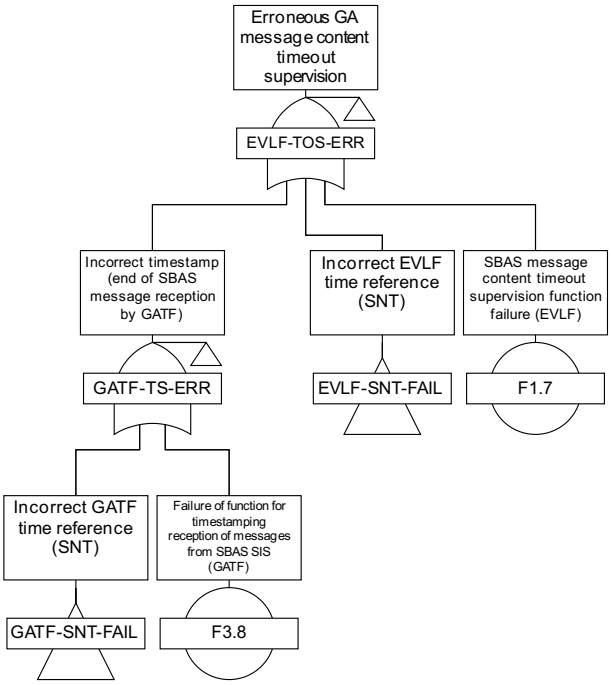
ID	Gate / Event	Description
GATF/GA-CID-ERR	Erroneous GA correction and integrity data (GATF)	(Transfer gate)
TRANS/SBAS-GATF-GA-1	SBAS message corruption hazards (SBAS SIS to GATF)	
SBAS-GATF/GA-UCR	Undetected SBAS message corruption (GATF)	
TRANS/SBAS-GATF-GA-3	SBAS message insertion hazards (SBAS SIS to GATF)	
SBAS-GATF/GA-UIM	Undetected inserted / masqueraded SBAS message (GATF)	
F3.12.1	Failure of SBAS L1 / L5 signal acquisition and tracking function (GATF)	
F3.12.2/3	Failure of SBAS L1 / L5 demodulation and FEC decoding function (GATF)	
F3.12.4/5	Failure of SBAS L1 / L5 message processing function (GATF)	

A.16 GATF/GNSS-CED-ERR: Erroneous CED (GNSS navigation data, GATF)



ID	Gate / Event	Description
GATF/GNSS-CED-ERR	Erroneous CED (GNSS navigation data, GATF)	(Transfer gate)
TRANS/GNSS-GATF-GN-1	GNSS navigation message corruption hazards (GNSS SIS to GATF)	
GNSS-GATF/GN-UCR	Undetected GNSS navigation message corruption (GATF)	
TRANS/GNSS-GATF-GN-3	GNSS navigation message insertion hazards (GNSS SIS to GATF)	
GNSS-GATF/GN-UIM	Undetected inserted / masqueraded GNSS navigation message (GATF)	(e.g., from cyber-attack: spoofing)
F3.11.1	Failure of GNSS signal acquisition and tracking function (GATF)	
F3.11.2	Failure of GNSS navigation data demodulation and FEC decoding function (GATF)	
F3.11.3	Failure of GNSS navigation data processing (GATF)	

A.17 EVLF-TOS-ERR: Erroneous GA message content timeout supervision



ID	Gate / Event	Description
EVLF-TOS-ERR	Erroneous GA message content timeout supervision	(Transfer gate)
GATF-TS-ERR	Incorrect timestamp (end of SBAS message reception by GATF)	
GATF-SNT-FAIL	Incorrect GATF time reference (SNT)	
F3.8	Failure of function for timestamping reception of messages from SBAS SIS (GATF)	
EVLF-SNT-FAIL	Incorrect EVLF time reference (SNT)	
F1.7	SBAS message content timeout supervision function failure (EVLF)	

Annex B THR Apportionment

B.1.1.1 This annex details the methodology and results of an initial apportionment of the GA for ERTMS/ETCS top-level hazard: PRIR, pseudorange integrity risk (correction residual or ionospheric vertical error not bound and TTA > T_NVGAMAXTTA).

B.1.1.2 Note that allocations are preliminary and will be finalised in the next issue of the document.

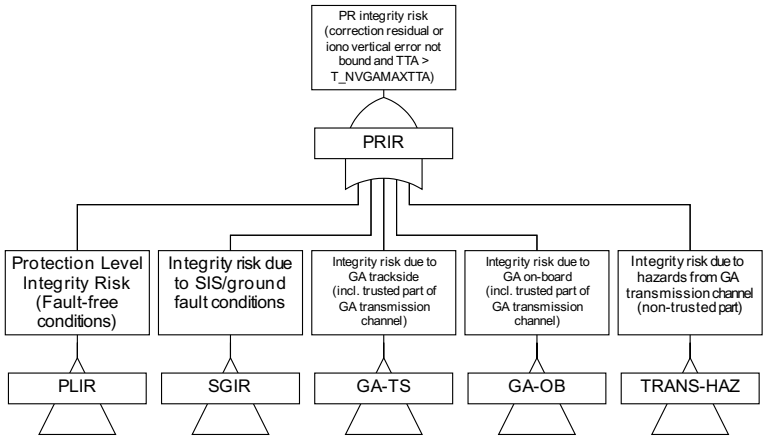
B.2 Apportionment of PRIR: Pseudorange integrity risk

B.2.1.1 The safety target for the GA transmission channel (end-to-end, non-trusted parts) is allocated 4% of the safety target for the GA top-level level hazard, such that:

$$THR_{PRIR} = 5.0E\text{-}6 \text{ / hour}$$

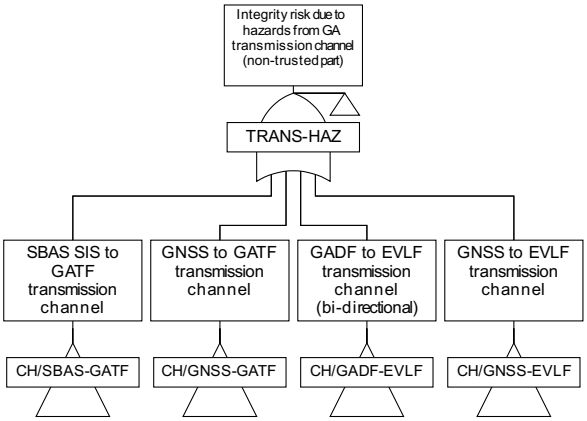
$$THR_{TRANS\text{-}HAZ} = 2.0E\text{-}7 \text{ / hour}$$

B.2.1.2 The transmission channel is apportioned between trusted and untrusted parts as described in [EN50159]. An initial apportionment is detailed below:



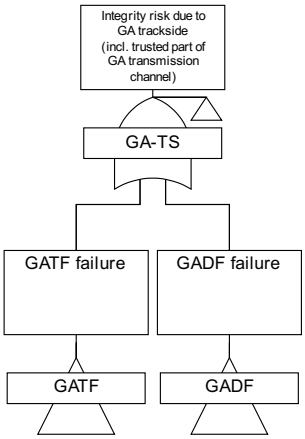
ID	Gate / Event	Description	Allocation (THR)
PRIR	Pseudorange integrity risk (correction residual or ionospheric residual error bout bound and TTA > T_NVGAMAXTTA	Top level GA hazard and THR allocation	5.0E-6 / hour
PLIR	Protection level integrity risk (fault-free conditions)	Performance supported by SBAS	2.4E-6 / hour
SGIR	Integrity risk due to 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	1.1E-8 / hour
GA-OB	Integrity risk due to GA on-board (including trusted part of the GA transmission channel)	Preliminary allocation	1.0E-8 / hour
TRANS-HAZ	Integrity risk due to hazards from GA transmission channel (non-trusted part)	Preliminary allocation	2.0E-7 / hour

B.2.2 TRANS-HAZ: Integrity risk due to hazards from GA transmission channel (non-trusted part)



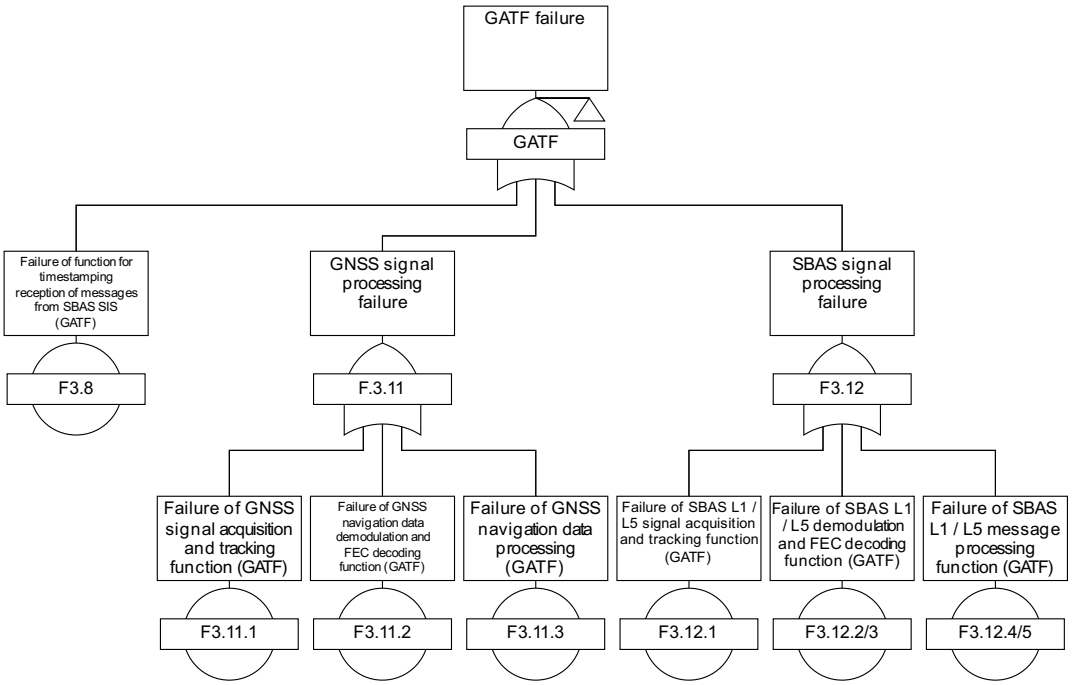
ID	Gate / Event	Description	Allocation (THR)	Estimated HR
CH/SBAS-GATF	SBAS SIS to GATF transmission channel	Preliminary allocation	7.4E-8 / hour	7.36E-8 / hour
CH/GNSS-GATF	GNSS to GATF transmission channel	Preliminary allocation	2.5E-8 / hour	3.35E-8 / hour
CH/GADF-EVLF	GADF to EVLF transmission channel (bi-directional)	Preliminary allocation	2.0E-11 / hour	2.0E-11 / hour
CH/GNSS-EVLF	GNSS to EVLF transmission channel	Preliminary allocation	9.1E-8 / hour	9.07E-8 / hour
		Margin	1.0E-8 / hour	
TRANS-HAZ	Total estimated HR for GA transmission channel (non-trusted part)		2.00E-7 / hour	1.98E-7 / hour

B.2.3 GA-TS: Integrity risk due to GA trackside (including trusted part of GA transmission channel)

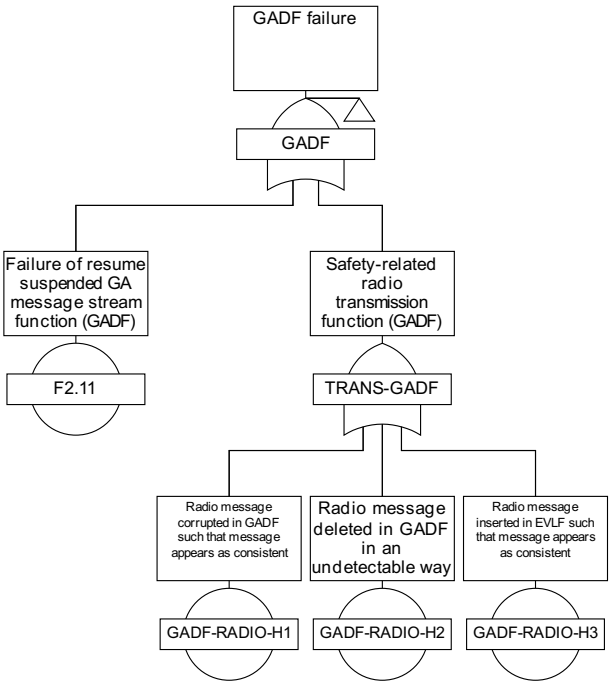


ID	Gate / Event	Description	Allocation (THR)	Estimated HR
GATF failure	GATF including GNSS receiver	Allocation of SIL3 (SIL3: 1E-8 / hour ≤ TFFR < 1E-7 / hour)	1.0E-8 / hour	1.0E-8 / hour
GADF failure	GADF (dissemination function only)	Allocation of SIL4 (SIL4: 1E-9 / hour ≤ TFFR < 1E-8 / hour)	1.0E-9 / hour	1.0E-9 / hour
GA-TS	Total estimated HR for GA trackside (including trusted part of GA transmission channel)		1.1E-8 / hour	1.1E-8 / hour

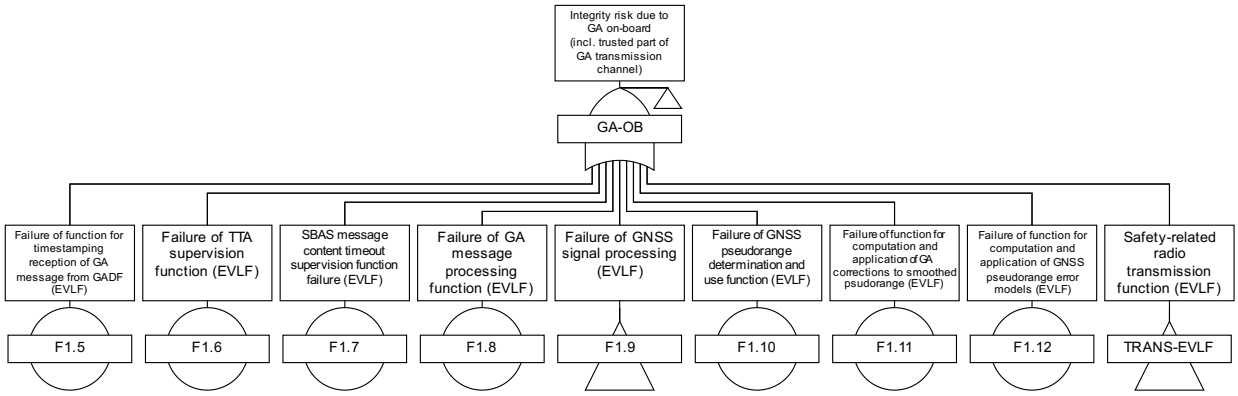
B.2.3.1 GATF: GATF failure



B.2.3.2 GADF: GADF failure

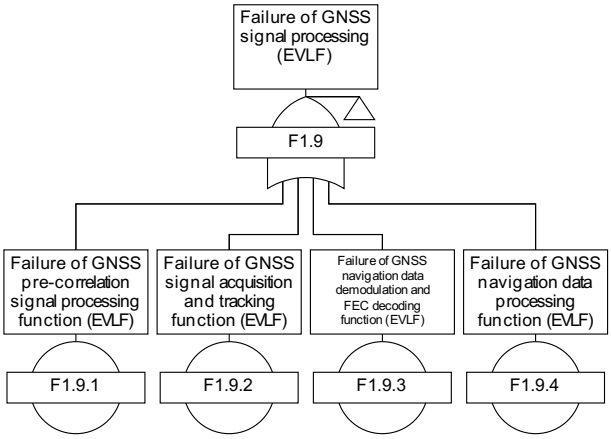


B.2.4 GA-OB: Integrity risk due to GA on-board (including trusted part of GA transmission channel)

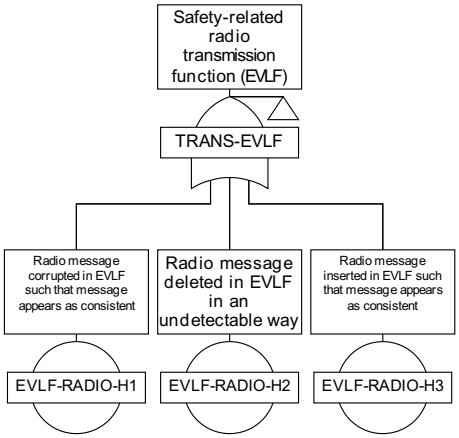


ID	Gate / Event	Description	Allocation (THR)	Estimated HR
GA-OB	Total estimated HR for GA on-board (including trusted part of GA transmission channel)	GA-OB including GNSS receiver allocated SIL3 (SIL3: 1E-8 / hour ≤ TFFR < 1E-7 / hour)	1.0E-8 / hour	1.0E-8 / hour

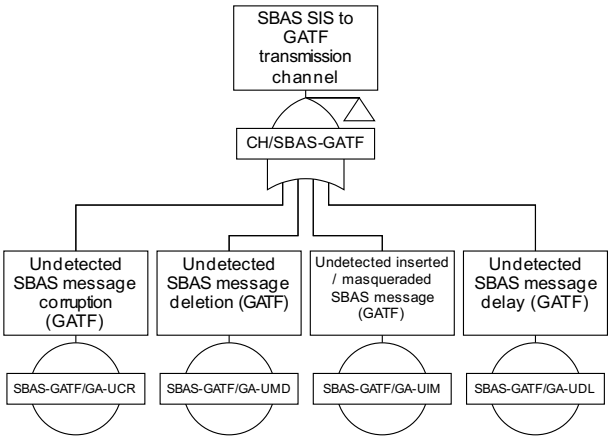
B.2.4.1 F1.9: Failure of GNSS signal processing (EVLF)



B.2.4.2 TRANS-EVLF: Safety-related radio transmission function (EVLF)



B.2.5 CH/SBAS-GATF: SBAS SIS to GATF transmission channel

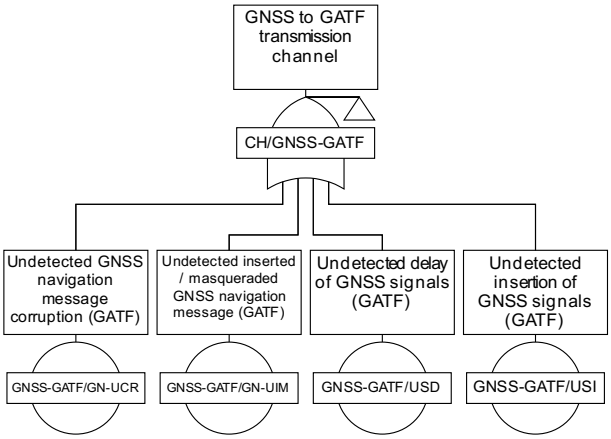


ID	Gate / Event	Description	Allocation (THR)	Estimated HR
SBAS-GATF/GA-UCR	Undetected SBAS message corruption (GATF)	(Refer to Section B.3)	5.4E-8 / hour	5.36E-8 / hour
SBAS-GATF/GA-UMD	Undetected SBAS message deletion refers to deletion of critical alert sequence or MT0 messages	See notes below.	N/A	N/A
SBAS-GATF/GA-UIM	Undetected inserted / masqueraded SBAS message (GATF)	Cyber-security barrier to be defined in next release of document. *Preliminary allocation TBC by analysis	1.0E-8 / hour*	TBC
SBAS-GATF/GA-UDL	Undetected SBAS message delay (GATF)	Cyber-security barrier to be defined in next release of document. *Preliminary allocation TBC by analysis	1.0E-8 / hour*	TBC
CH/SBAS-GATF	Total estimated HR for SBAS SIS to GATF transmission channel (non-trusted part)		7.4E-8 / hour	7.36E-8 / hour

B.2.5.1 Notes on SBAS-GATF/GA-UMD:

- SBAS message deletion is detectable because of continuity of signal (an SBAS message broadcast by every second).
- Alert sequences consist of 4 messages broadcast by the SBAS in 4 consecutive seconds.
- Loss of 4 consecutive messages results in a safety reaction by the GATF/GADF as this corresponds with the possibility to have missed an alert sequence.
- In this case, GADF sends “DNU GA message stream” to the EVLF indicating that the EVLF shall no longer use the GA message stream, requiring the EVLF to cease using and discard any ranging data and GA data obtained from the message stream (SRS section 2.2.5).
- MT0 messages are broadcast with a maximum update rate of 6 seconds and indicate the service cannot be used for safety applications.

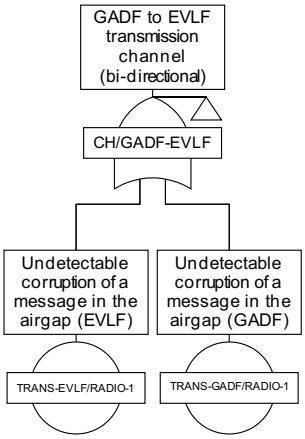
B.2.6 CH/GNSS-GATF: GNSS to GATF transmission channel



ID	Gate / Event	Description	Allocation (THR)	Estimated HR
GNSS-GATF/GN-UCR	Undetected GNSS navigation message corruption	Undetected LNAV corruption for a maximum of 12 GPS satellites for SoM (Refer to Section B.4)	5.0E-9 / hour	2.11E-9 / hour
		Undetected F/NAV corruption for a maximum of 12 Galileo satellites for SoM (Refer to Section B.5)		1.36E-9 / hour
GNSS-GATF/GN-UIM	Undetected inserted / masqueraded GNSS navigation message (GATF)	Cyber-security barrier to be defined in next release of document. *Preliminary allocation TBC by analysis	1.0E-8 / hour*	TBC
SBAS-GATF/USI	Undetected insertion of GNSS signals (GATF)			
GNSS-GATF/USD	Undetected delay of GNSS signals (GATF)	Cyber-security barrier to be defined in next release of document. *Preliminary allocation TBC by analysis	1.0E-8 / hour*	TBC
CH/GNSS-GATF	Total estimated HR for GNSS to GATF transmission channel (non-trusted part)		2.5E-8 / hour	3.35E-8 / hour

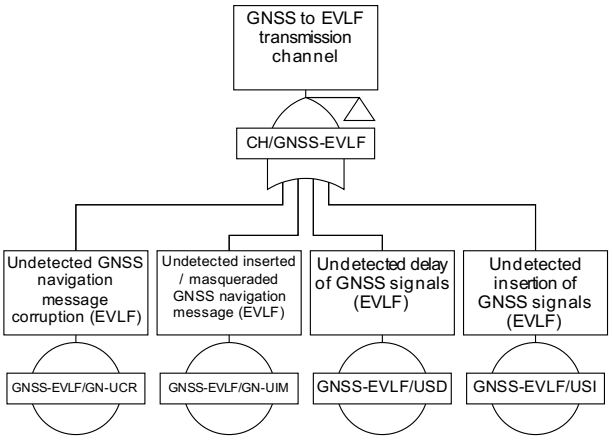
B.2.7 CH/GADF-EVLF: GADF to EVLF transmission channel

B.2.7.1 The TRANS-EVLF/RADIO-1 and TRANS-GADF/RADIO-1 allocations reflect the bi-directional nature of the radio link and that the potential for corruption is present in either direction (GADF to EVLF or EVLF to GADF).



ID	Gate / Event	Description	Allocation (THR)	Estimated HR
TRANS-EVLF/RADIO-1	Undetectable corruption of a message in the airgap (EVLF)	(Refer to Section B.7)	1.0E-11 / hour	1.0E-11 / hour
TRANS-GADF/RADIO-1	Undetectable corruption of a message in the airgap (GADF)		1.0E-11 / hour	1.0E-11 / hour
CH/GADF-EVLF	Total estimated HR for GADF to EVLF transmission channel (non-trusted part)		2.0E-11 / hour	2.0E-11 / hour

B.2.8 CH/GNSS-EVLF: GNSS to EVLF transmission channel



ID	Gate / Event	Description	Allocation (THR)	Estimated HR
GNSS-EVLF/GN-UCR	Undetected GNSS navigation message corruption	Undetected LNAV corruption for a maximum of 12 GPS satellites (Refer to Section B.4)	7.1E-8 / hour	3.80E-8 / hour
		Undetected F/NAV corruption for a maximum of 12 Galileo satellites (Refer to Section B.5)		3.27E-8 / hour
GNSS-EVLF/GN-UIM	Undetected inserted / masqueraded GNSS navigation message (GATF)	Cyber-security barrier to be defined in next release of document. *Preliminary allocation TBC though analysis	1.0E-8 / hour*	TBC
GNSS-EVLF/USI	Undetected insertion of GNSS signals (GATF)			
GNSS-EVLF/USD	Undetected delay of GNSS signals (GATF)	Cyber-security barrier to be defined in next release of document. *Preliminary allocation TBC though analysis	1.0E-8 / hour*	TBC
CH/GNSS-EVLF	Total estimated HR for GNSS to GATF transmission channel (non-trusted part)		9.1E-8 / hour	9.07E-8 / hour

B.3 Quantification of undetected SBAS message corruption

B.3.1.1 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 EVLF via the SBAS SIS (not currently defined but under consideration – to be addressed in the next revision of the SRS and SFHA).

B.3.1.2 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 B.6 for assumptions on the BER.

B.3.1.3 The probability of an error in an SBAS message (250 bits) given a BER of 1E-6 is:

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

B.3.1.4 Probability of erroneous SBAS message in an hour:

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

B.3.1.5 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 100% probability. The probability of large burst errors greater than parity length (b > 24) 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]

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

B.4 Quantification of GPS L1 LNAV navigation message corruption hazard

B.4.1.1 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 B.6 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 EVLF GNSS receivers is also foreseen, confirmation of BER with empirical data from representative railway environments is considered essential.

B.4.1.2 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.

B.4.1.3 The probability of an error in a word (30 bits) given a BER of 1E-6 is:

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

B.4.1.4 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.

B.4.1.5 The probability of erroneous navigation data (20 words) is:

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

B.4.1.6 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 100% probability. The probability of errors not detected in a codeword = $2^{26}/2^{32}$ = 1.56E-2.

B.4.1.7 Therefore, the probability of an undetected error in a frame is:

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

B.4.1.8 Considering that verified reception of a second frame is required prior to use of new data (requirement in SBAS-OB-MOPS / SBAS-TS-MOPS), the residual risk of undetected error in frame data assuming uncorrelated errors between consecutive frames is:

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

B.4.1.9 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 EVLF / hour.

B.4.2 LNAV provided by GA-TS at Start of Mission

B.4.2.1 It is assumed that at Start of Mission (SoM) the EVLF may request GNSS navigation data from the trackside to speed up the time to first fix (TTFF) if the EVLF 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).

B.4.2.2 A conservative assumption has been made that the EVLF 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

B.4.2.3 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:

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

B.4.3 LNAV CED sets received from the GNSS SIS by the EVLF

B.4.3.1 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

B.4.3.2 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:

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

B.5 Quantification of Galileo E5a F/NAV navigation message corruption hazard

B.5.1.1 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 EVLF GNSS receivers is also foreseen, confirmation of BER with empirical data from representative railway environments is considered essential.

B.5.1.2 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 × 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.

B.5.1.3 The probability of an error in an F/NAV page (238 bits) given a BER of 1E-6 is:

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

B.5.1.4 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.

B.5.1.5 The probability of erroneous navigation data (4 pages) is:

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

B.5.1.6 F/NAV pages are protected with a CRC-24Q, providing protection against burst as well as random errors with a probability of undetected error ≤ 2^{-24} = 5.96E-8 for all channel bit error probabilities ≤ 0.5.

B.5.1.7 Therefore, the probability of an undetected error in a subframe is:

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

B.5.1.8 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 EVLF / hour.

B.5.2 F/NAV provided by GA-TS at Start of Mission

B.5.2.1 It is assumed that at Start of Mission (SoM) the EVLF may request GNSS navigation data from the trackside to speed up the time to first fix (TTFF) if the EVLF 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).

B.5.2.2 A conservative assumption has been made that the EVLF 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-10 / hour

B.5.2.3 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:

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

B.5.3 F/NAV CED sets received from GNSS SIS by the EVLF

B.5.3.1 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:

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

B.5.3.2 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:

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

B.6 Assumptions on GNSS bit error rates (BER)

B.6.1.1 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.

B.6.1.2 Table B-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 B-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

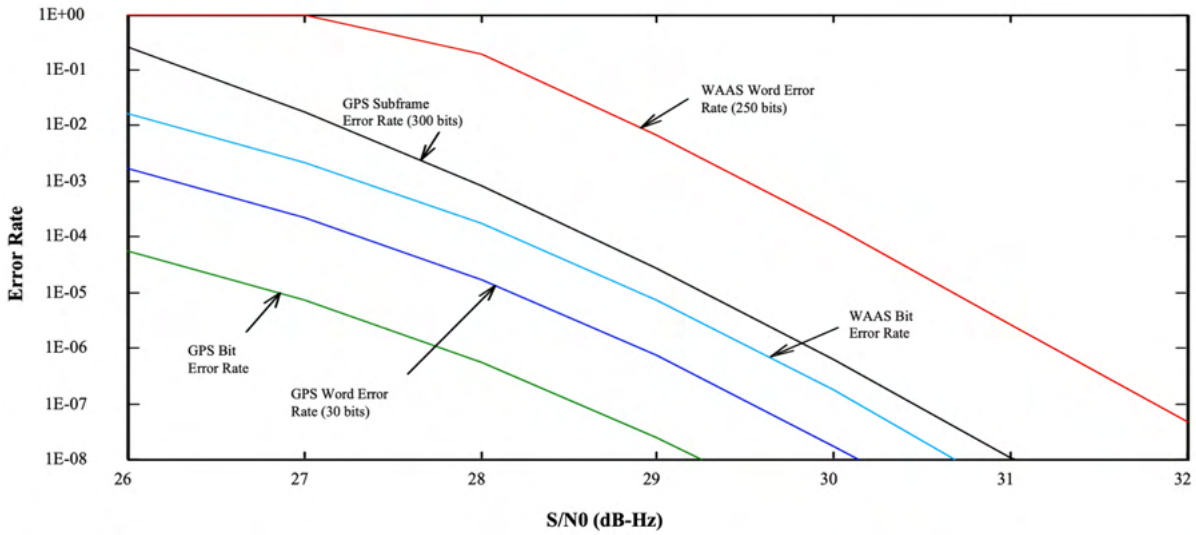


Figure B-1. GNSS bit and word error rates [DO235, Figure D-14]

B.6.1.3 Figure B-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

B.6.1.4 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.

B.6.1.5 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.

B.6.1.6 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.

B.7 Justification of safe radio connection message corruption hazard

B.7.1.1 The safe radio connection to be used for exchange of information between the GA-OB and GA-TS shall provide barriers against message level hazards that are at least as good as those specified for the EURORADIO protocol.

B.7.1.2 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.

B.7.1.3 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.

B.7.1.4 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.

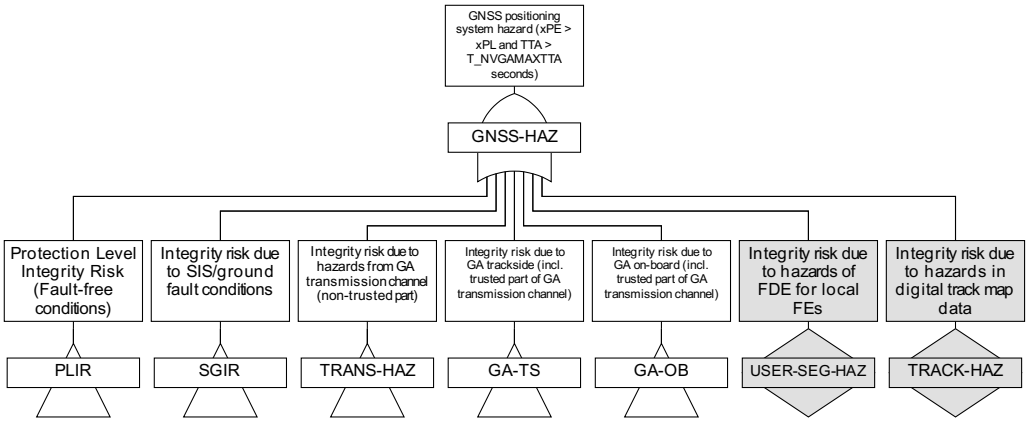
B.8 Example Fault Tree and Allocations for a GNSS Channel using GA for ERTMS/ETCS

B.8.1.1 This section provides an illustrative example of fault-tree allocations for a single GNSS channel using GA for ERTMS/ETCS. The example considers a complete set of events including those related to GA for ERTMS/ETCS (from B.2), and events that are outside the scope of GA (such as hazards related to fault-detection and exclusion (FDE) for local feared events, hazards related to digital track map, etc.) but contribute to the GNSS positioning system hazard (GNSS-HAZ). Events outside the scope of GA are shaded grey in the fault-tree below).

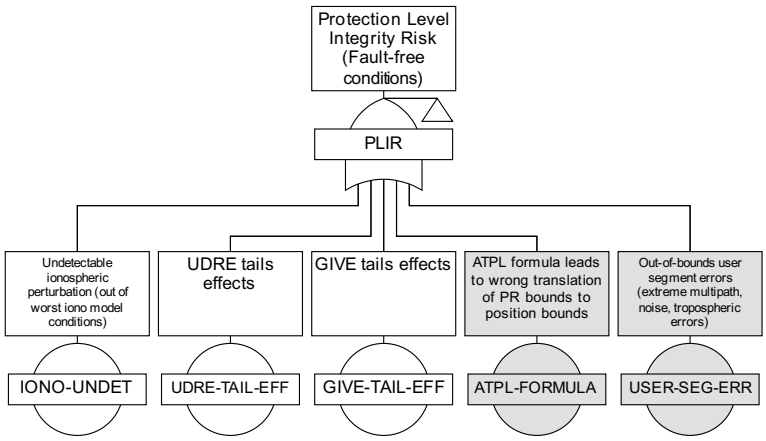
B.8.1.2 The top-level hazard, *GNSS-HAZ: GNSS positioning system hazard (xPE > xPL and TTA > T_NVGAMAXTTA seconds)*, has been allocated a THR of 7.5E-6 / hour based on the allocations from Section B.2 and additional allocations to USER-SEG-HAZ and TRACK-HAZ.

B.8.1.3 It is assumed that GNSS would be used with other sensors in an enhanced vehicle localisation function that is capable of meeting application-specific safety and performance targets (e.g., safety targets in the order of 0.33E-9 / hour for hazard related to real vehicle front-end position being outside the train confidence interval).

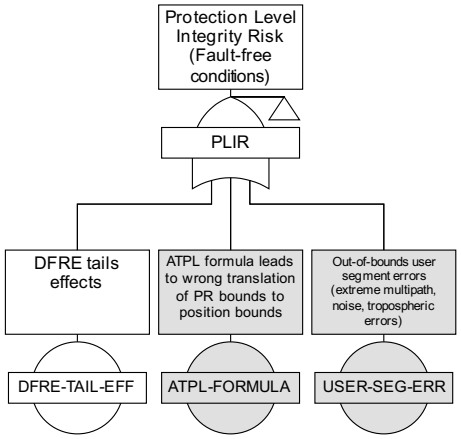
B.8.1.4 The stringent application targets can be met using GNSS in combination with other sensors, exploiting techniques such as diversity / dissimilarity. It should be noted that approaches to developing a multi-sensor enhanced on-board localisation function are outside the scope of this example.



B.8.1.5 PLIR: Protection level integrity risk (fault-free) for GA based on SBAS L1 Legacy service



B.8.1.6 PLIR: Protection level integrity risk (fault-free) for GA based on SBAS L5 DFMC service



B.8.1.7 The table below details the allocations that have been made:

ID	Gate / Event	Description	Allocation (THR)
PLIR	Protection level integrity risk (fault-free conditions)		2.4E-6 / hour
SGIR	Integrity risk due to SIS / ground fault conditions		2.4E-6 / hour
TRANS-HAZ	Integrity risk due to hazards from the GA transmission channel (non-trusted part)		2.0E-7 / hour
GA-TS	Integrity risk due to GA trackside (including trusted part of the GA transmission channel)		1.1E-8 / hour
GA-OB	Integrity risk due to GA on-board (including trusted part of the GA transmission channel)		1.0E-8 / hour
USER-SEG-HAZ	Integrity risk due to hazards of FDE for local feared events		2.4E-6 / hour

TRACK-HAZ	Integrity risk due to hazards in digital track map data	Allocation of SIL4 (SIL4: 1E-9 / hour ≤ TFFR < 1E-8 / hour)	1.0E-9 / hour
		Margin	7.8E-8 / hour
GNSS-HAZ	Total allocation for GNSS positioning system hazard (xPE > xPL and TTA > T_NVGAMAXTTA seconds)		7.5E-6 / hour

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

The following table provides a list of open points related to the SFHA to be addressed in future iterations of the analysis.

Table C-1. Open points list

Ref	Description	Solution / Workstream	Status / Notes
1	Cyber-attacks related to SBAS signals received by the GATF are to be addressed in a future issue of the SFHA	TBA by EUG (with support from ESA/EUSPA)	**Open.** Contribution from cyber vulnerability is currently unidentified; however, it can be considered a design requirement. Assessment of cybersecurity threats related to open SBAS transmission channel (EGNOS SIS-GATF) to performed.
2	Multi-disciplinary risk workshop to review FMEA and FTA	To be addressed by EUG (with support from ESA/EUSPA/ESSP)	**Open.**
3	Technical review of Annex B by EGNOS project	To be addressed by EUSPA (with support from ESA)	**Open.**
4	Assumptions on BER for computation of residual message corruption risk in Annex B	Activity to be defined (led by ESA / EUSPA)	**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	FMEA for GADF-GATF interface	To be addressed by EUG (with support from ESA/EUSPA)	**Open.** The GADF-GATF interface is currently left undefined as it is not considered relevant for interoperability. If it is decided that multiple GATFs shall be supported with a standardised interface, this will be addressed in the next issue of the SRS and an ICD for the GADF-GATF interface defined will need to be defined. In addition, the hazard analysis (FMEA) in the SFHA will need to be extended to include the GADF-GATF interface.
6	THR allocations to GA-TS / GADF, GATF	To be addressed by EUG (with support from ESA/EUSPA)	**Open.** Issue raised in review: In B.2.3 it was noted that from functional point of view the GA-TS should be a single block with a single THR apportionment (leaving the supplier freedom to implement the related functions as is done for GA-OB). THR allocations have been made to GATF and GADF functions separately to accommodate multiple GATFs.
7	Definition of requirements for Safe Radio Connection	To be addressed by EUG (with support from ESA/EUSPA)	**Open.** Issue raised in review: In B.7 (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

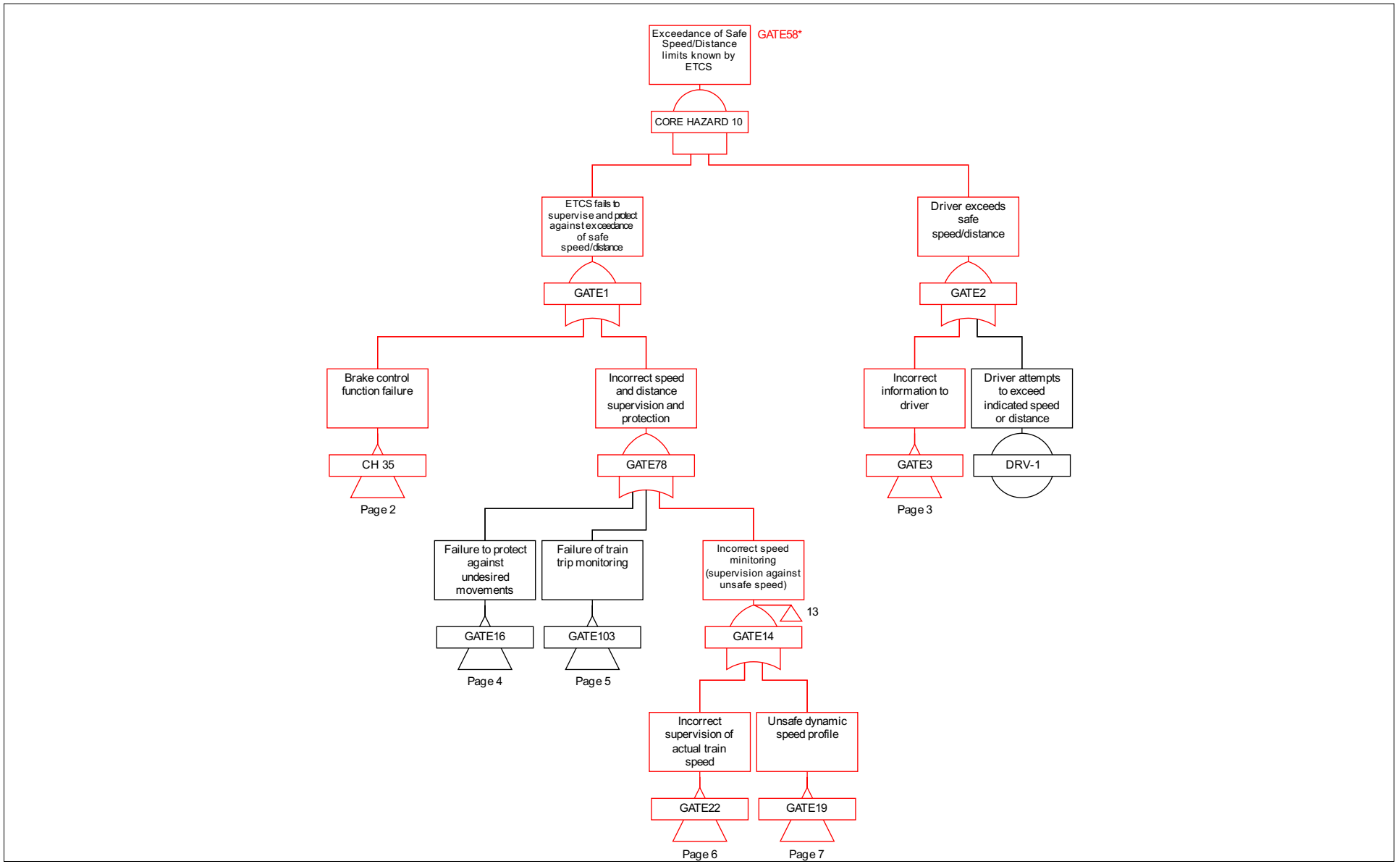
			as Euroradio. It was suggested that this was overly conservative, and requirements could be relaxed in the context of a relatively low top-level GA THR (i.e., ~ 5E-6 / hour).
8	Specification of requirements for trackside GNSS interference environment, guidelines for survey, etc.	Activity to be defined (led by ESA / EUSPA)	**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).

Annex D Trace of GATE58 Minimal Cut Set – SUBSET-88-2 Part 1

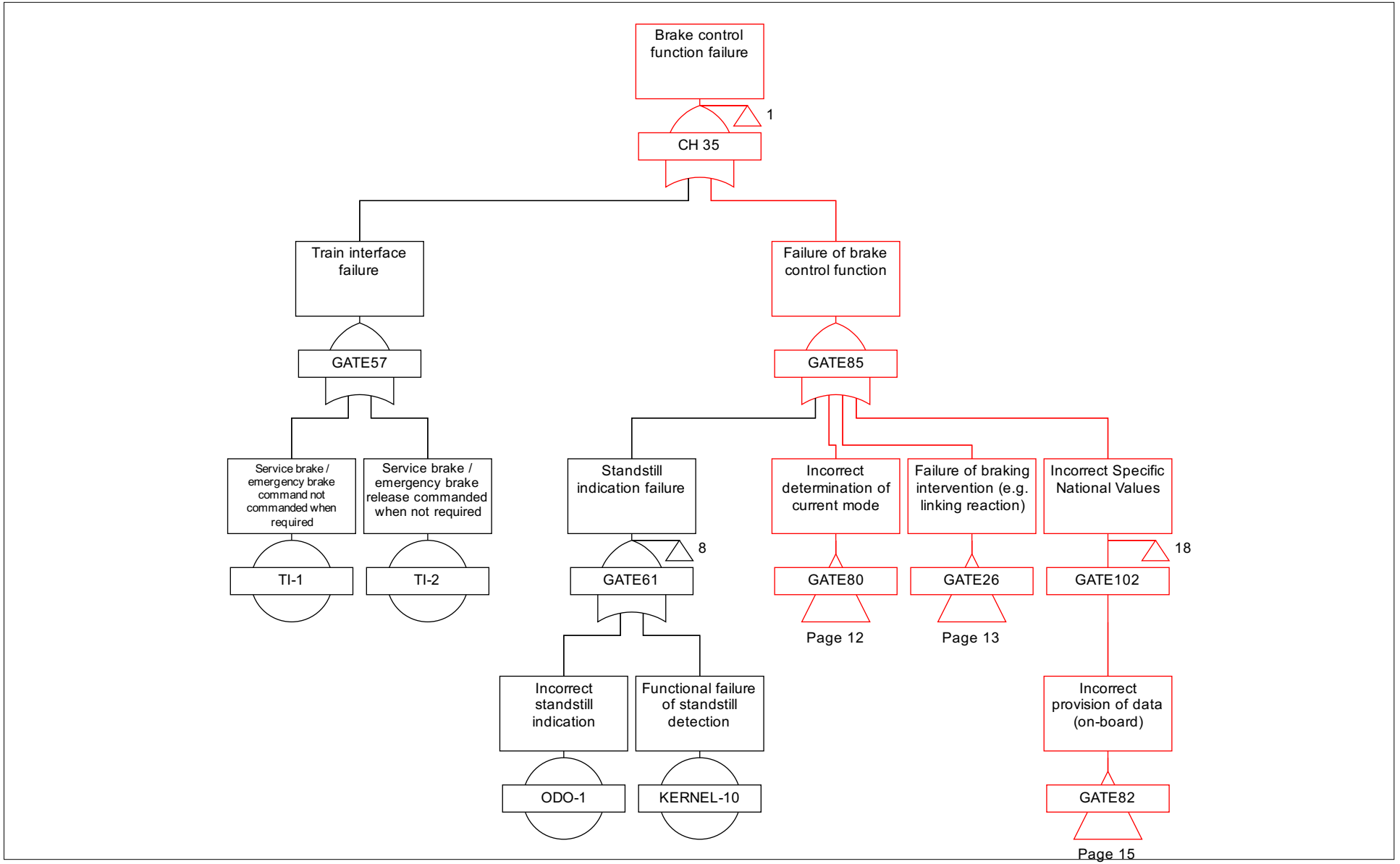
D.1.1.1 This annex provides a trace of the GATE58 minimal cut set in the SUBSET-088-2 Part 1 functional fault tree (ETCS application level 2).

D.1.1.2 GATE58 represents *Incorrect determination of train position reference to Last Relevant Balise Group (LRBG)*. This gate was selected to illustrate the causal pathways for hazardous events causing GATE58 to the ETCS Core Hazard (i.e., hazardous events relevant to an *enhanced vehicle localisation function*). Basic events under GATE58 were not linked to the analyses in this document as they are specific to ETCS train positioning based on the balise transmission system and ETCS odometry.

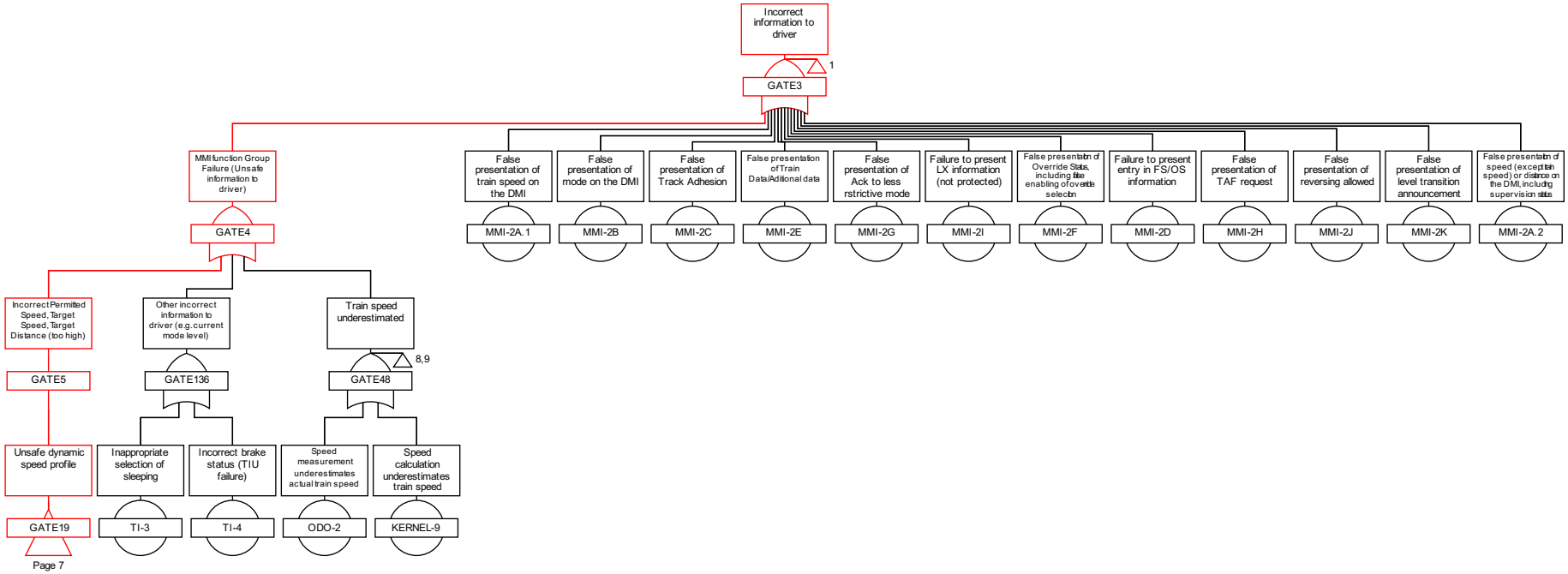
D.1.1.3 It should also be noted that an *enhanced vehicle localisation function* may also provide vehicle speed and therefore causal pathways for hazardous events causing GATE48, *train speed underestimated*, to the ETCS Core Hazard may also need to be considered.



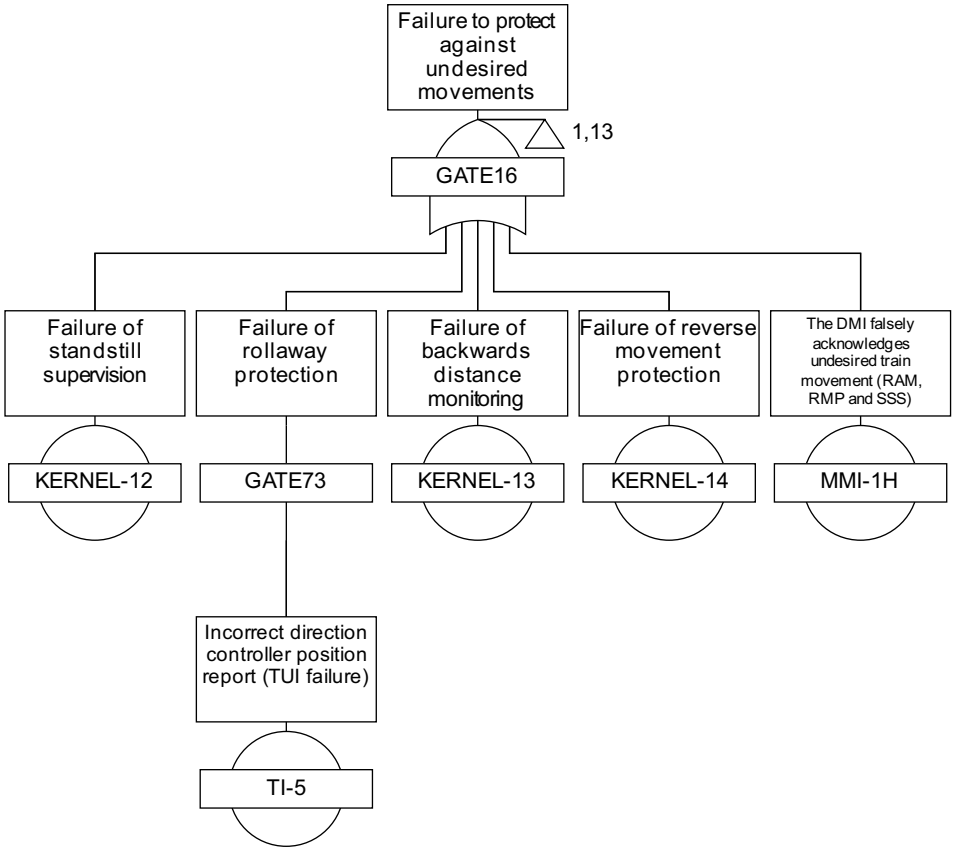
Fault Tree Page 1



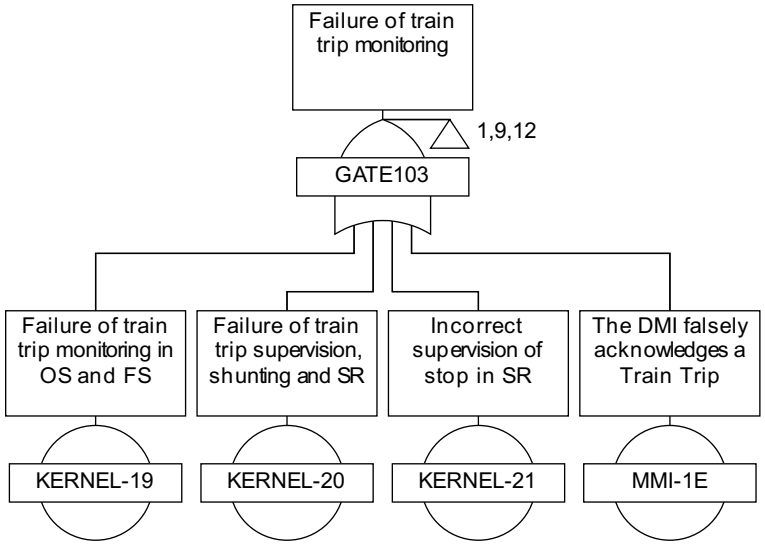
Fault Tree Page 2



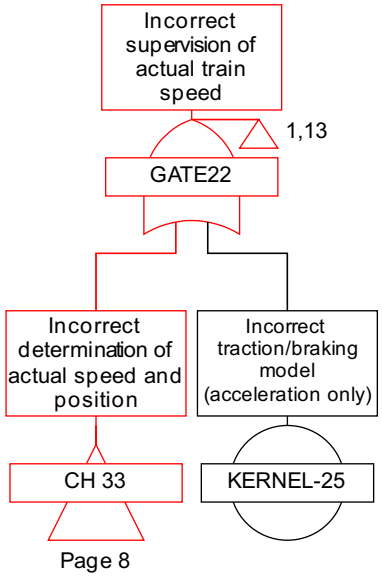
Fault Tree Page 3



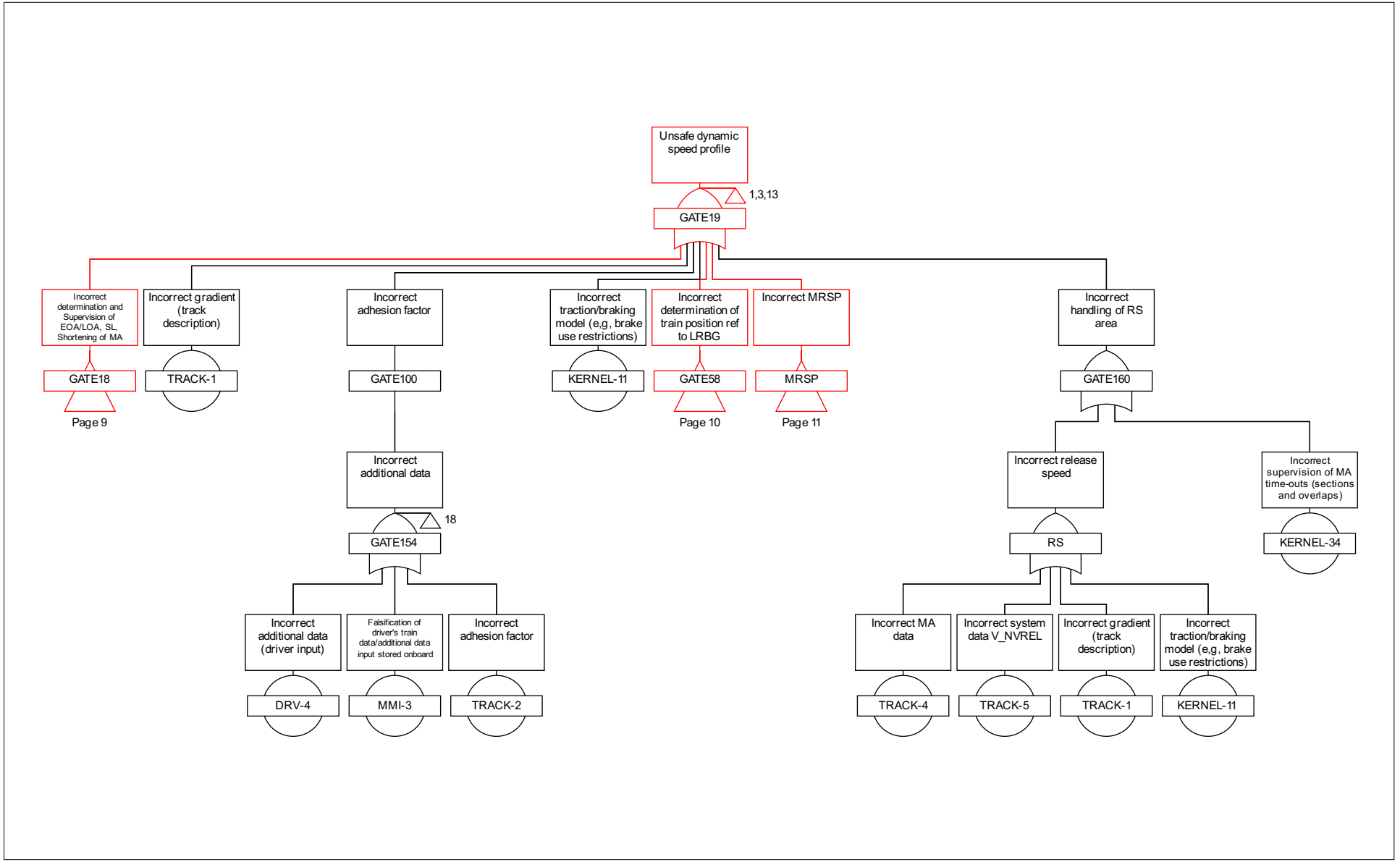
Fault Tree Page 4



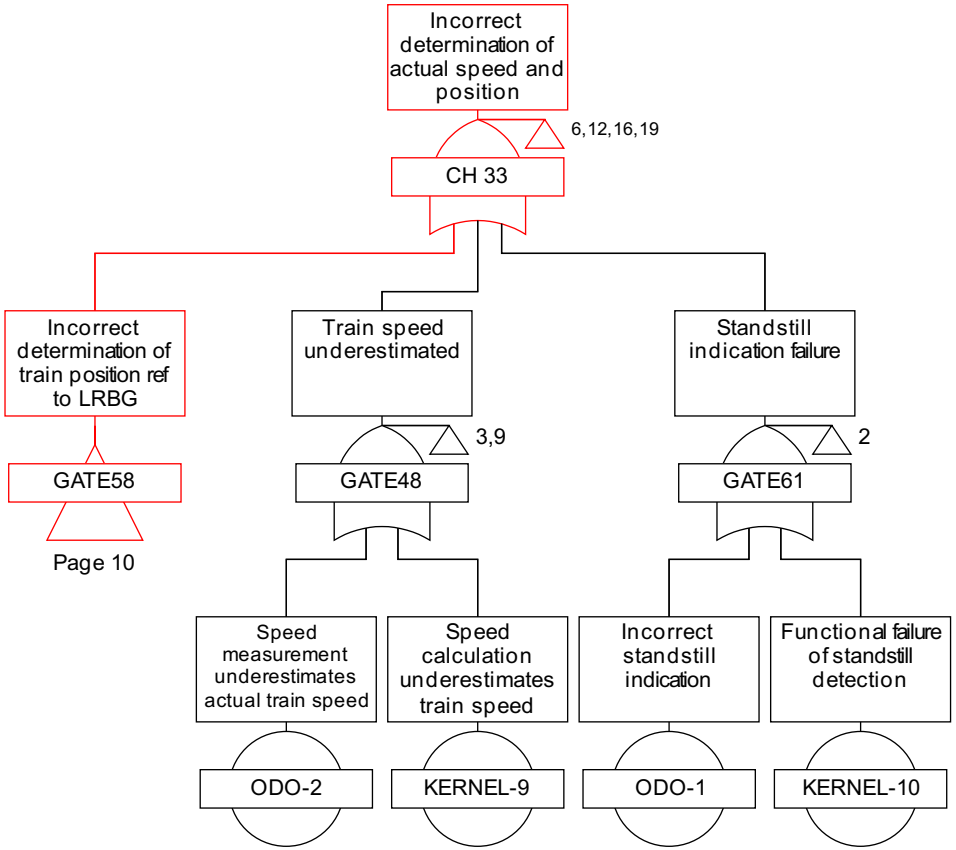
Fault Tree Page 5



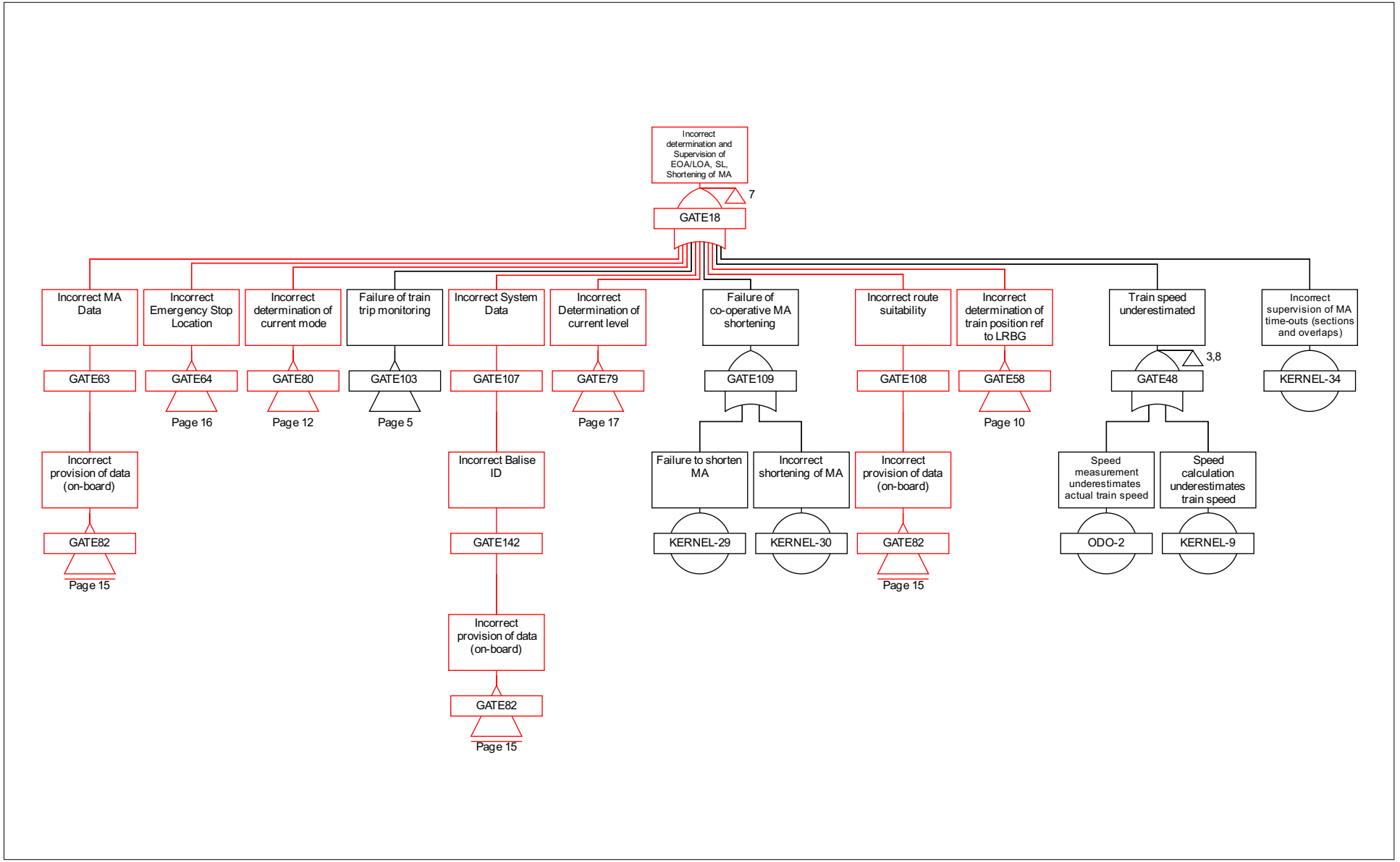
Fault Tree Page 6



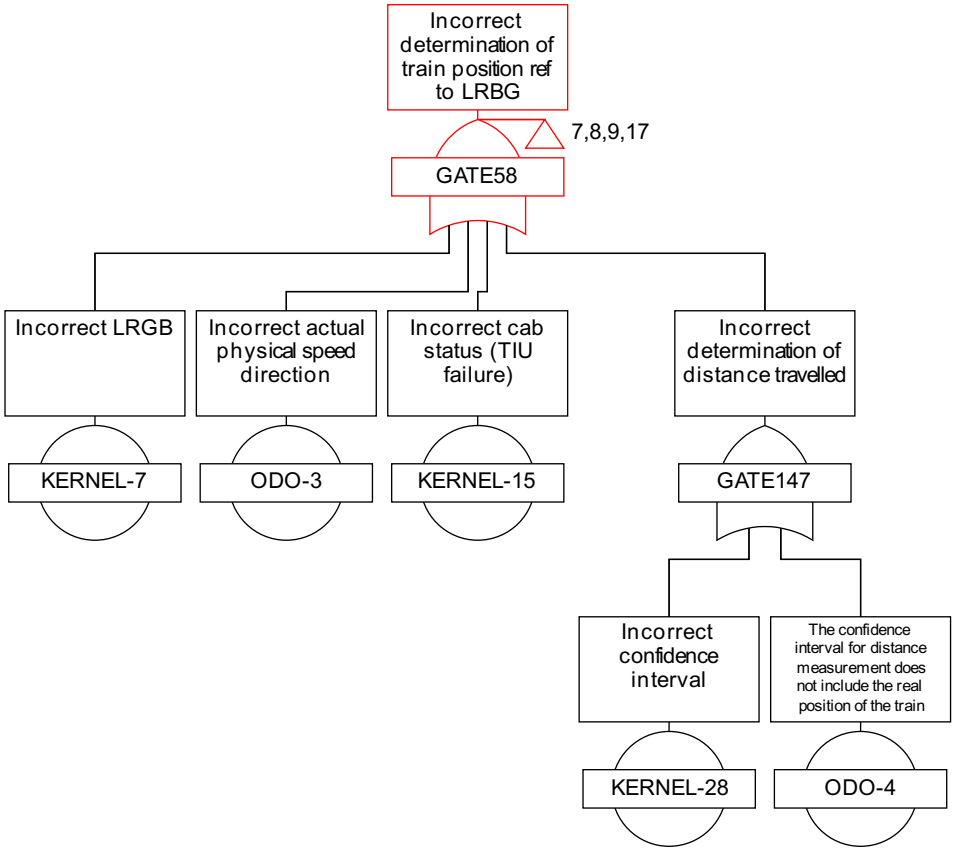
Fault Tree Page 7



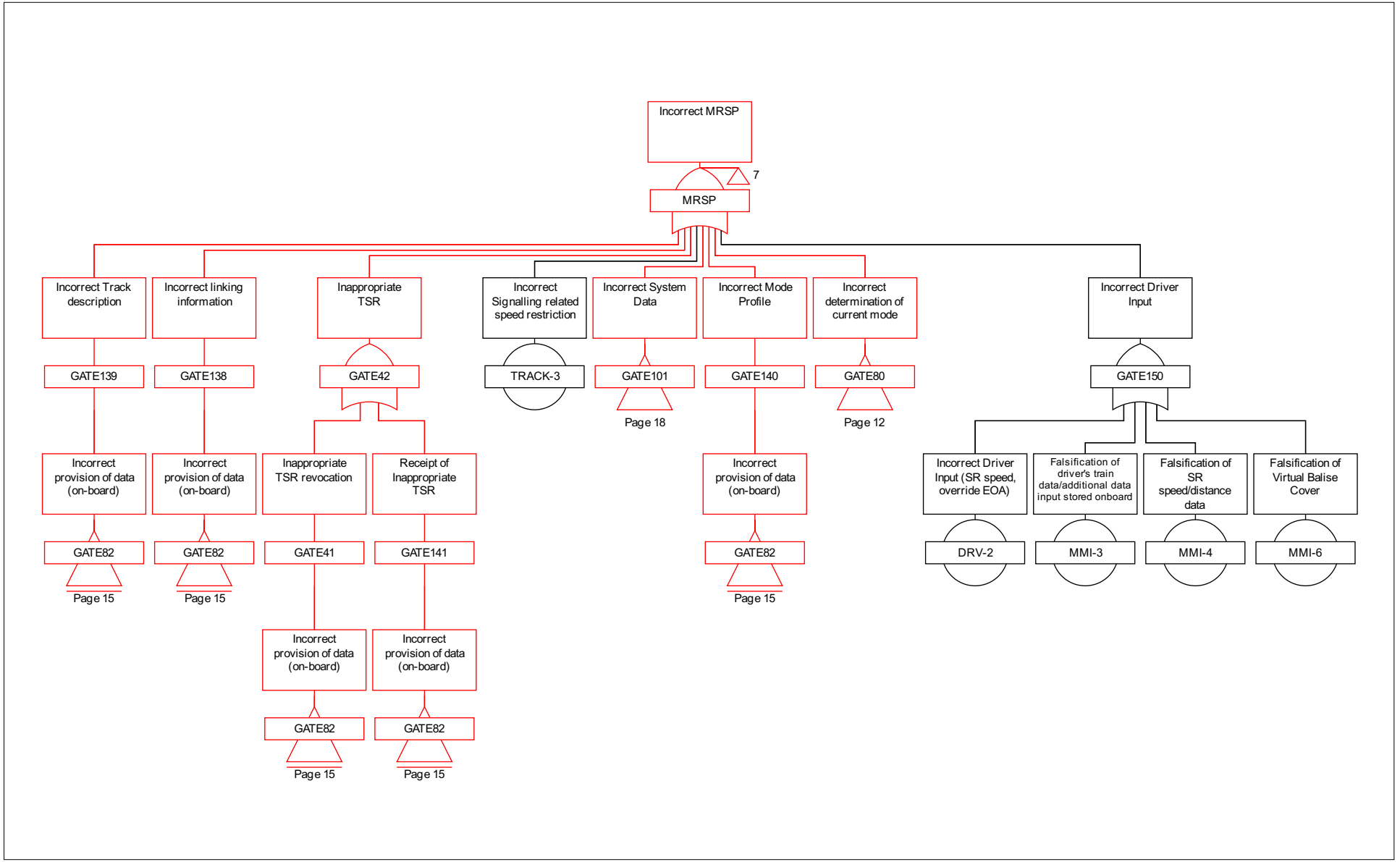
Fault Tree Page 8



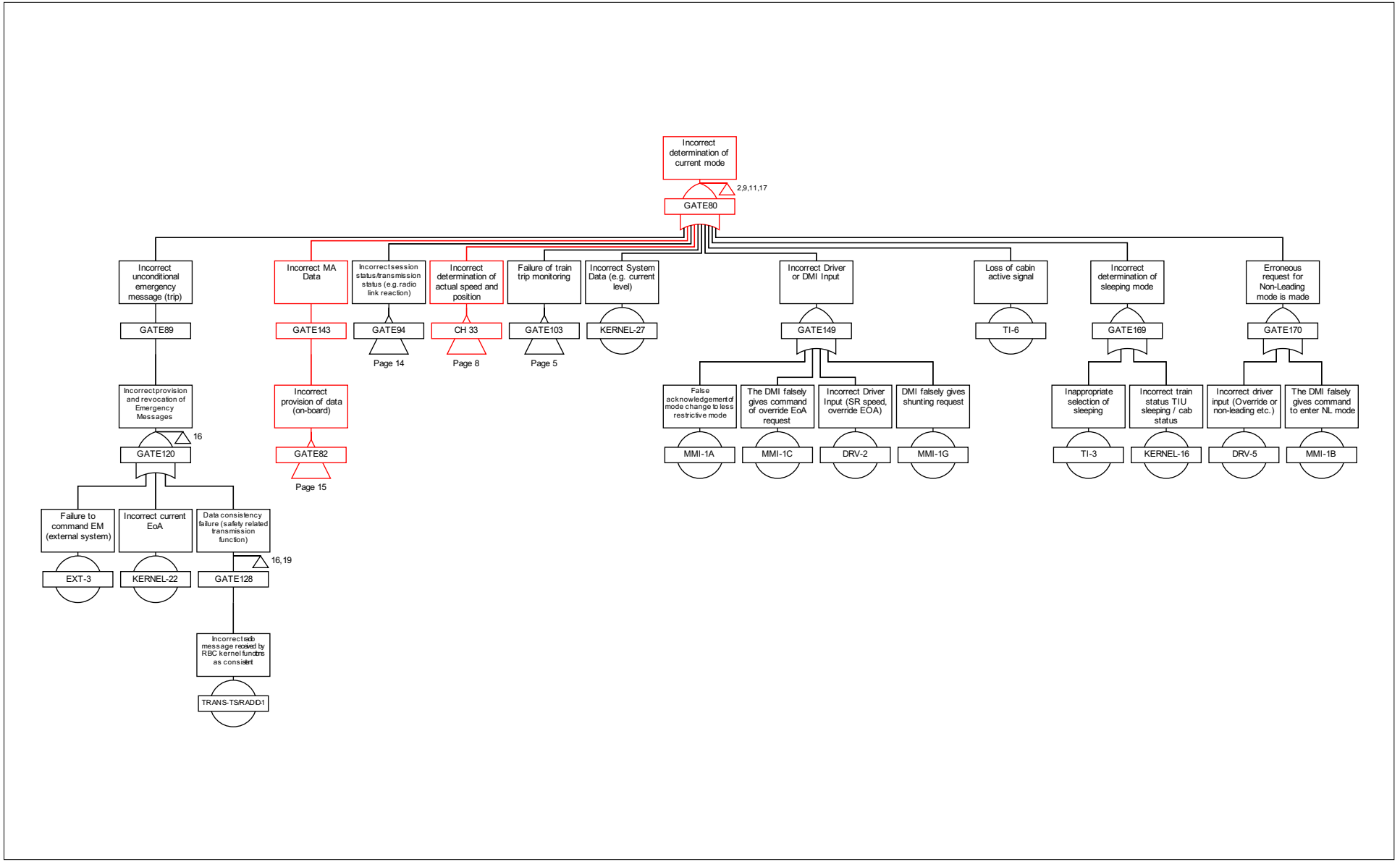
Fault Tree Page 9



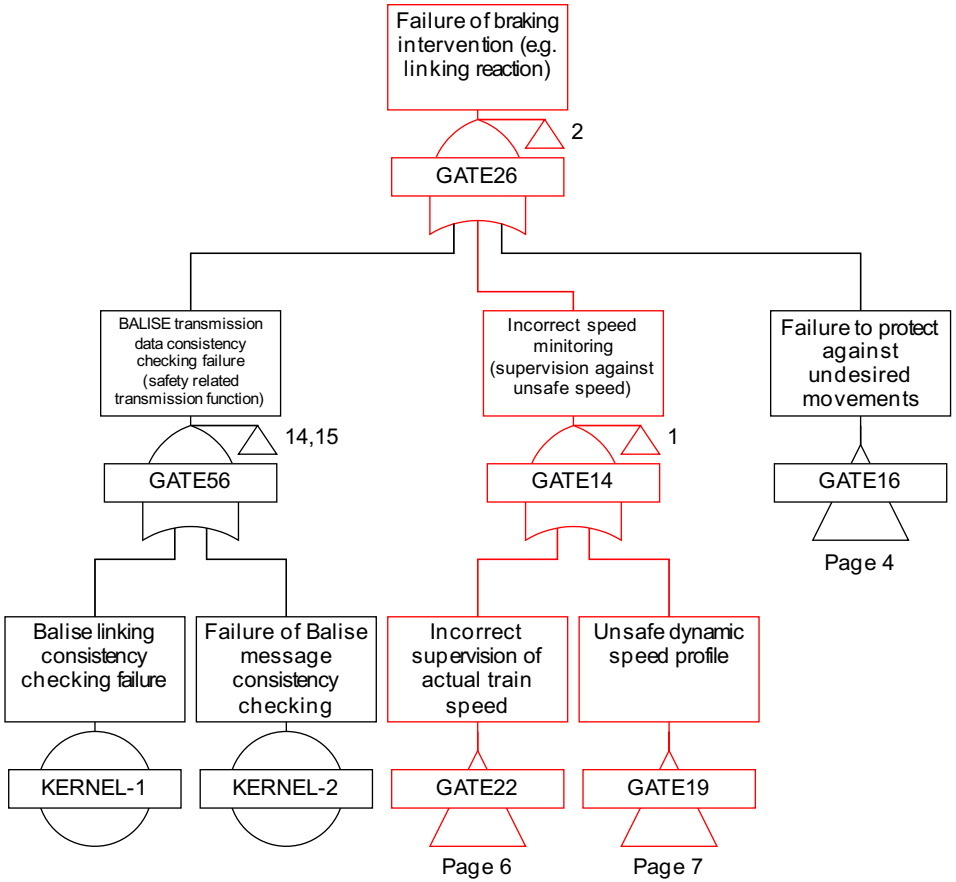
Fault Tree Page 10



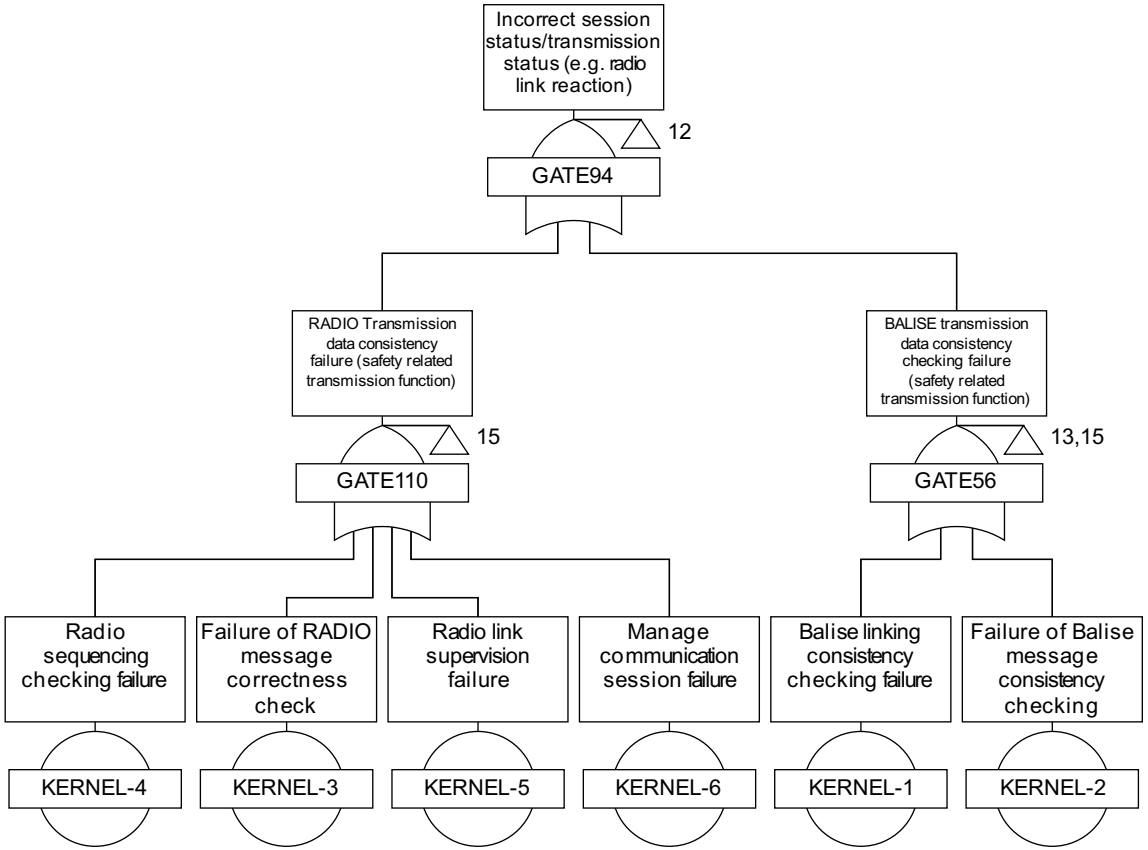
Fault Tree Page 11



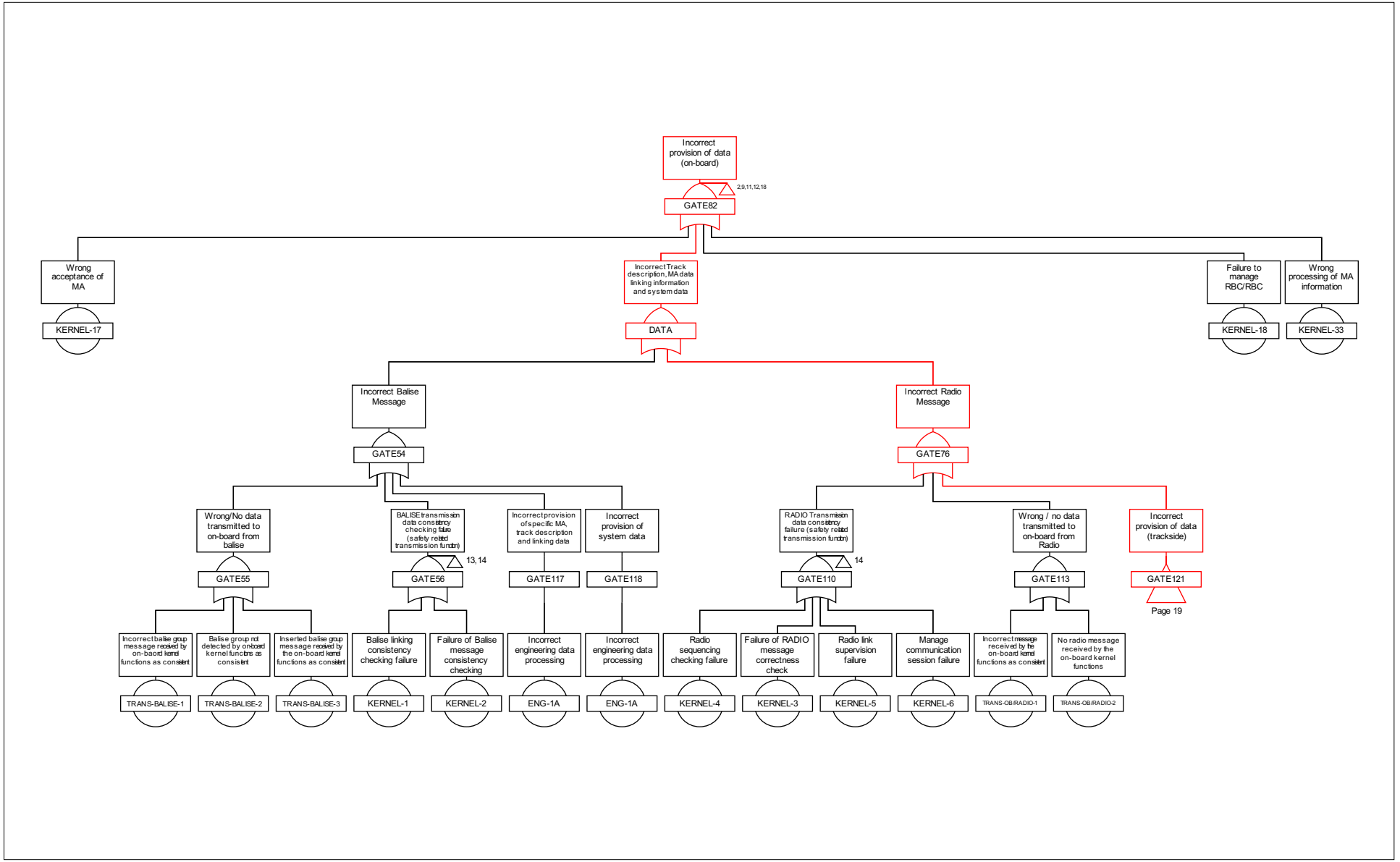
Fault Tree Page 12



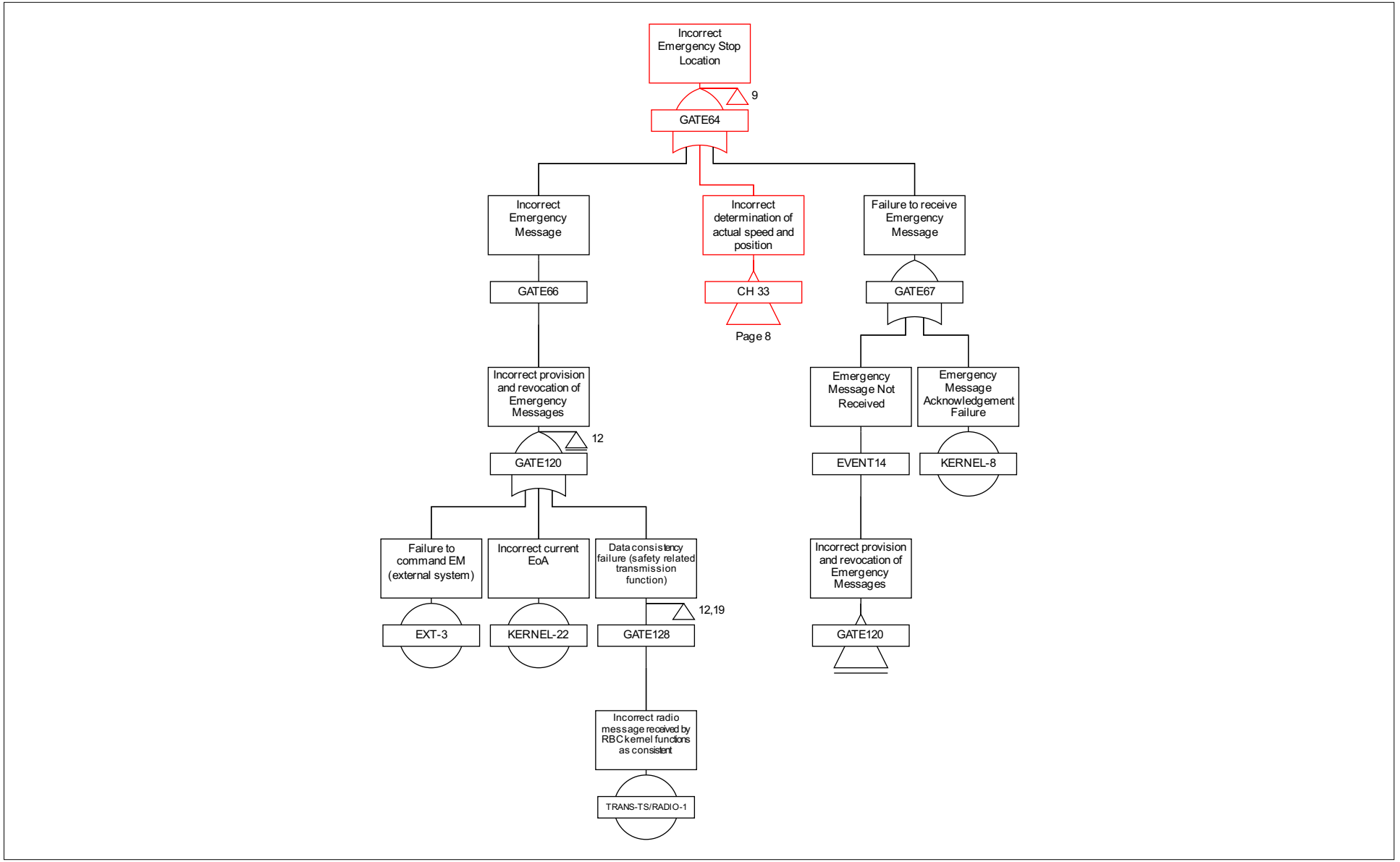
Fault Tree Page 13



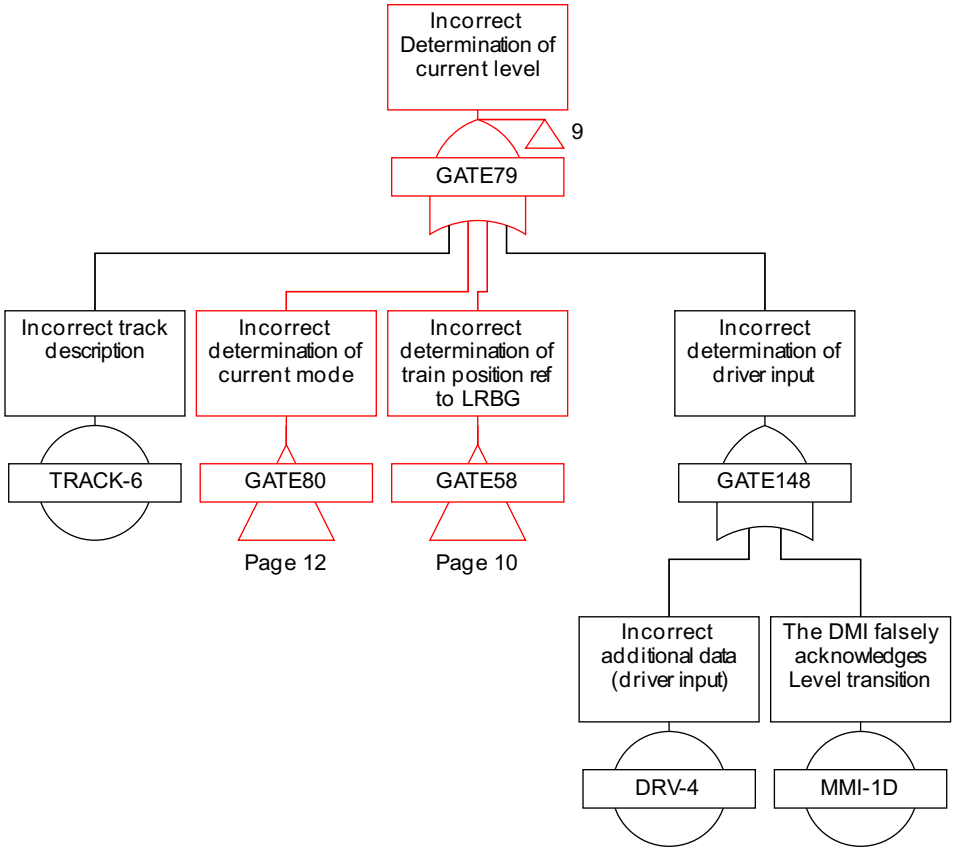
Fault Tree Page 14



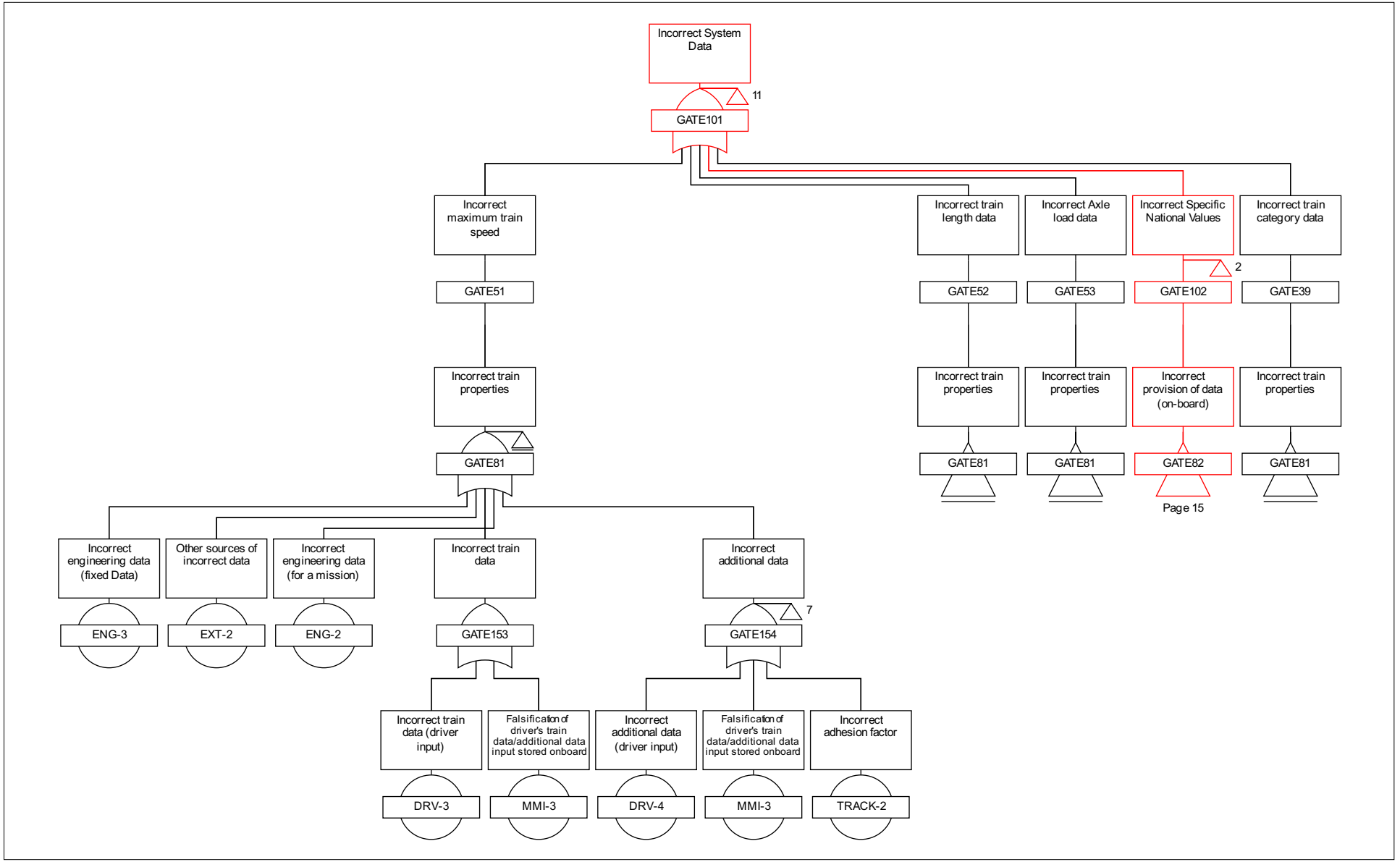
Fault Tree Page 15



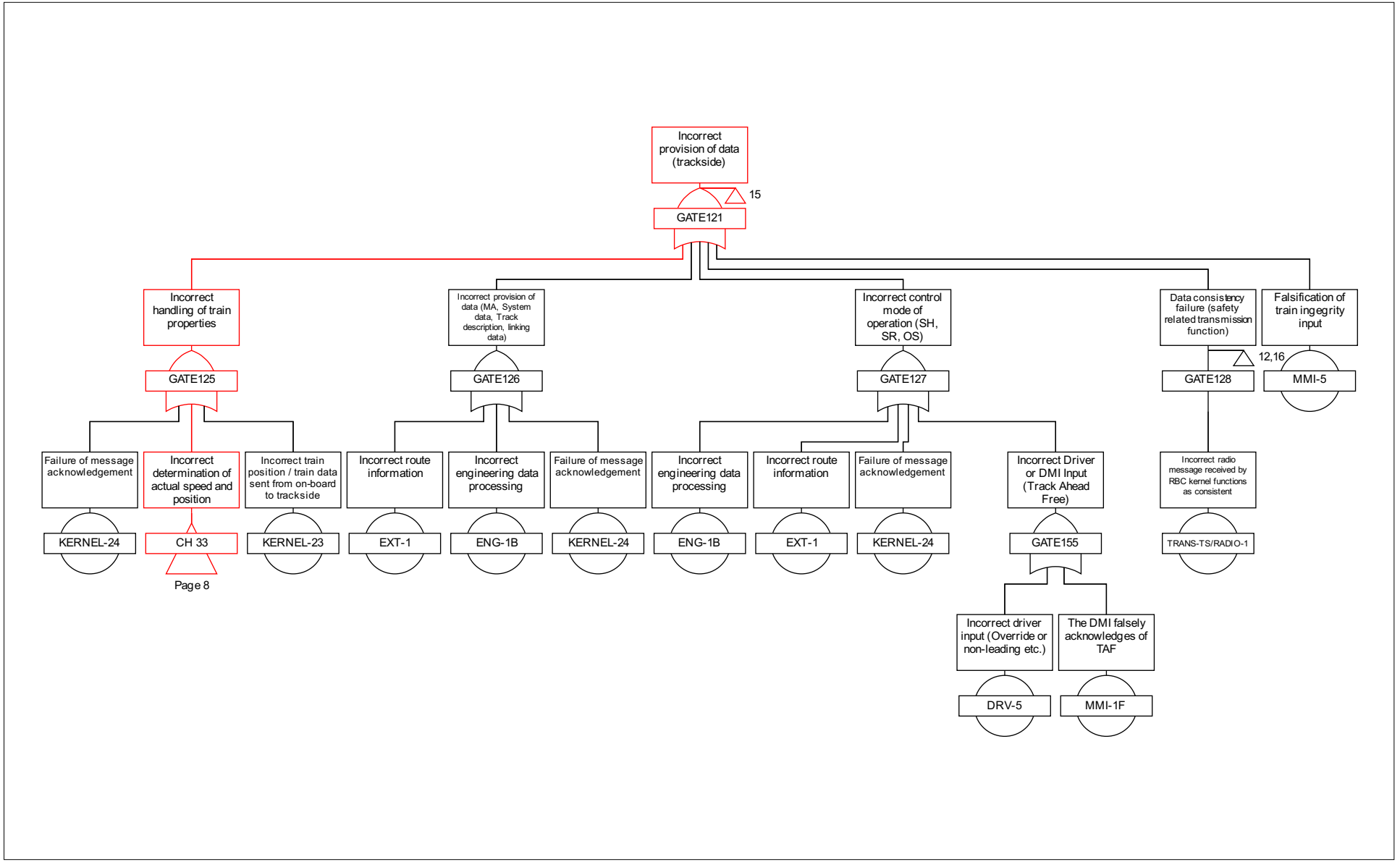
Fault Tree Page 16



Fault Tree Page 17



Fault Tree Page 18



Fault Tree Page 19

END OF DOCUMENT