CLUG Demonstration of Readiness for Rail – CLUG 2.0

D3.5 LOC-OB SYSTEM FUNCTIONAL SAFETY ANALYSIS

Due date of deliverable: 31/05/2024

Actual submission date: 21/01/2025

Leader of this Deliverable: Thidarat Panthong, DB InfraGO AG

Reviewed: Y

Document status		
Revision	Date	Description
0.1	21/05/2024	First Draft
0.2	14/06/2024	Review comments on stable version implemented
0.3	19/06/2024	Updated refer to proposal from SNCF
0.4	21/06/2024	Stable version
0.5	04/07/2024	Stable Version plus quality (no content update)
0.6	26/08/2024	Final version: updated refer to SNCF's comment and according to the latest versions of inputs documents (D4.1, D4.9, D4.8, D4.6)
0.7	02/10/2024	Final version: updated refer to SNCF's comment
0.8	14/10/2024	Final version: DB internal quality check
0.9	04/11/2024	Implemented review comments of the TMT review
1.0	18/11/2024	Final version after quality check
1.1	17/01/2025	Updated refer to EUSPA's comment
2.0	21/01/2025	Final version submitted to EUSPA

Project funded from the European Union's Horizon 2020 research and innovation programme		
Dissemination Level		
PU	Public	
SEN	Sensitive, limited under the conditions of the Grant Agreement	X
Classified R-UE/EU-R	EU RESTRICTED under the Commission Decision No2015/444	
Classified C-UE/EU-C	EU CONFIDENTIAL under the Commission Decision No2015/444	
Classified S-UE/EU-S	EU SECRET under the Commission Decision No2015/444	

Start date of project: 01/02/2023 Duration: 24 months

REPORT CONTRIBUTORS

NAME	COMPANY	DETAILS OF CONTRIBUTION
Thidarat Panthong	DB InfraGO	Author
Claus Thies-Von Der Bey Lena Alexandra Tillemann Martin Brandt Andreas Staudte	DB InfraGO	Reviewer
Marc Sarrat Marielle Petit-Doche	SNCF	Reviewer
Karin Nebe Alejandro Lopez Hernandez	SMO	Reviewer
Alain Ruaudel	Airbus	Reviewer
Valentin Barreau	SNCF	TMT Validator
Mariya Kayalova	RINA-C	Quality check
Jose Bertolin	UNIFE	Final check and submission to reviewers and EUSPA

EXECUTIVE SUMMARY

This document is the deliverable of the "T3.5 - LOC-OB System Functional Safety Analysis" of the CLUG 2.0 project which stands for Certifiable Localisation Unit using Global Navigation Satellite System (GNSS) in the railway environment. The main goal of the project is to demonstrate the readiness of using EGNSS and multisensory fusion systems for safe rail localisation.

The objective of deliverable D3.5 is to analyse the System Functional failure to consolidate the Preliminary Hazards Analysis and CLUG RAMS Report of TLOBU solution A and validate the functional system specification and the architecture defined in WP2 and WP4. Fault Tree Analysis and Failure Mode Effect Analysis techniques are included in this task.

The first part of the analysis uses Failure mode effect analysis to analyse the internal function of the LOC-OB, as defined by the LOC-OB functional architecture (see §3.3). These include functions such as Sensor & System data FDE, Along track localisation function, Integrity function and LOC-OB INIT function, and Track selectivity function. The analysis aims to identify the potential failure modes of the inputs, their causes, and their effects on system safety.

The Second part of the Analysis (FTA) includes safety analysis approach to demonstrate that the LOC-OB System meets safety requirements and can achieve Safety Integrity Level 4 in terms of hardware. This is achieved by utilizing hardware information from D4.1 and the demonstrator as a guideline for proposing a potential LOC-OB hardware system architecture with a safety level equivalent to the existing train localisation system that relies solely on balises.

As concluded in this document, the design of the LOC-OB should incorporate Composite Fail-safety. With this technique, each safety related function is performed at least on two hardware items in order to avoid common cause failure. The proposed hardware configuration of LOC-OB can achieve SIL4 by using IMUs, each with the failure rate of less than or equal to 5E-05 per hour for both chains. For LOC-OB initialisation function, the Cold Movement Detection is needed to start up fusion algorithm. If there is no Cold Movement Detection, then the balise data is necessary as input to LOC-OB system. For the Track Selectivity function, the point position information is required as an input to ensure the safe train movement. Regarding the second chain Shape and Heading Map maching technique, the route information from infrastructure is needed. Additionally, it is recommended to use separate hardware for chain 1 and chain 2, with the failure rate of each component of less than or equal to 1E-05 per hour. For the Combiner hardware, which combine outputs from chain 1 and chain 2, a failure rate of less than or equal to 1E-09 per hour is proposed.

LIST OF ACRONYMS

ACRONYM	CONCEPTS
CCS	Control, Command and Signalling
CEM	Conducted and Electromagnetic Disturbance
CLUG	Certifiable Localisation Unit with GNSS
CMD	Cold Movement Detector
CSM	Common Safety Methods
CI	(computed) Confidence Interval
COTS	Commercial Off The Shelf
DAL	(Aviation) Design Assurance Level
DFMC	Dual Frequency Multi Constellation
DFMC+PR+PV	Proposed optimized EGNOS stream for rail and terrestrial users, implementing DFMC, Pseudo-Range and Pseudo-Velocity integrity
DM	Digital Map
ECEF	Earth-Centred, Earth-Fixed
EGNOS	European GNSS Navigation Overlay Service
EKF	Extended Kalman Filter
EMC	ElectroMagnetic Compatibility
ERJU	European Rail Joint Undertaking
ERTMS	European Rail Traffic Management System
estFE	Estimated Front End
ETCS	European Train Control System
ESA	European Space Agency

ACRONYM	CONCEPTS
EUSPA	European Union Agency for the Space Programme
EVC	European Vital Computer
FDE	Fault Detection and Exclusion
FE	Front End
FFFIS	Form Fit Functional Interface Specification
FMEA	Failure Modes and Effects Analysis
FOG (IMU)	Fiber Optical Gyroscope (IMU techno)
FRMCS	Future Railway Mobile Communication System
FTA	Fault Tree Analysis
GA-OB	GNSS Augmentation On-board
GA-TS	GNSS Augmentation Trackside
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM-R	GSM for rail, will be replaced by FRMCS
ICD	Interface Control Document
IMU	Inertial Measurement Unit
INIT	Initialisation phase
LOC-OB	Localisation System On Board
LWG	Localisation Working Group
MDT	Mean Down Time (mean standstill or failure time)
MTBF	Mean Time Between Failure

ACRONYM	CONCEPTS
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
OCORA	Open CCS On-board Reference Architecture
ODO	Odometry
OPG	Odometer Pulse Generator
PHA	Preliminary Hazard Analysis
PIS	Passenger Information System
PVT	Position Velocity Time
RAMS	Reliability, Availability, Maintainability and Safety
RBC	Radio block Centre
SBAS	Space-Based Augmentation System
SFSC	Single Frequency, Single Constellation - typically EGNOS V2, V3.1 (and V3.2) providing in EGNOS L1 safely augmentation of the GPS L1 only
SIL	Safety Integrity Level
SiS	Signal in Space
SoL	Safety of Life
SRAC	Safety Related Application Condition
TBC	To Be Confirmed
TFFR	Tolerable Functional Failure Rate
TSD	Track Selectivity Determination function
THR	Tolerable Hazard Rate
TSI	Technical Specification of Interoperability

ACRONYM	CONCEPTS
WLS	Weighted Least-Squares
WSF	Wrong Side Failure
WSoI	Wider System-of-Interest

CONTENTS

Table of figures

List of tables

1 INTRODUCTION

The objective of this System Functional Safety Analysis is to identify and analyse the effects of the input failure on the functional of LOC-OB system. The effects can be clustered into initial effects, subsystem effects and system operability effects. This document comprises two parts of analysis. The first part uses a qualitative analysis, focusing on the navigation core of the LOC-OB System and linked to PHA D3.2, which includes the following functions:

- Sensor and System Data FDE
- LOC-OB Initialisation
- Track Selectivity
- Along-track localisation
- Integrity

The second part uses a quantitative analysis, conducting a Fault Tree Analysis based on the hypothesis described in the following chapter. The objective of the Fault Tree Analysis is to evaluate the design justification from D4.1 to determine if it meets TFFR level which less than 1E-08per hour for vital output functions and to propose a hardware architecture that can attain SIL 4 requirement.

In scope of the CLUG 2.0 project only the functional architecture is defined, no detailed Hardware System Architecture is described. To conduct a quantitative analysis, the hardware of the LOC-OB system is required as input. Therefore, we assume that the information on COTS-IMU candidates and the GNSS-EGNOS receiver as outlined in D4.1 [11] – Functional Architecture and D4.2 [12] – GNSS Receiver can be utilized. This detail can be used as the input to perform the Fault Tree Analysis (FTA). Additionally, the demonstrator from WP5 is useful as it provides detailed hardware information on wheel speed sensors (Tachometer, Doppler Radar, Optical Sensor). These sensors are also inputs to the LOC-OB system and are considered in the FTA. The FTA is performed, and the result of FTA can be used as a guideline for the LOC-OB configuration of Hardware System Architecture.

The document focuses on an analysis based on the high – level architecture described in D2.3 [3], Start of Mission and Track Selectivity in D2.2 [2] and the design documents in work package 4 which are mainly D4.1 LOC-OB System Functional Architecture [11], D4.6 -Along Track Localisation [15], D4.7-Confidence Intervals Computation and Integrity Algorithm [16], D4.8- Track Selectivity [13], D4.9 – LOC-OB INIT [14].

Note: D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version).

2 METHODOLOGY FOR SYSTEM FUNCTIONAL SAFETY ANALYSIS

2.1 Overall Methodology

The System Functional Safety Analysis is part of risk analysis process. Failures from the logical functions are linked to hazards identified in PHA-D3.2. The method used to carry out the System Functional Safety Analysis utilizes the FMEA technique to analyse the LOC-OB system. The first part of this analysis aims to identify the potential failure modes of the inputs, their causes, and their effects on system safety. The focus of this analysis is on the functions as defined by the LOC-OB functional architecture (see §3.3), including Sensor & System data FDE, Along track localisation function, Integrity function and LOC-OB INIT function, Track selectivity function. Safety Integrity of a function can be affected both by random and systematic failures; therefore, safety integrity comprises two parts: systematic and random safety integrity.

Prevention of systematic and random failures requires different approaches:

- the Random safety integrity is achieved by product design (e.g., diversity, redundancy, protection against expected environmental conditions foreseen in specific Codes of Practice etc.);
- the Systematic safety integrity can benefit from technical mechanisms embedded in a product (for instance diversity), but it is mainly based on process solutions, as quality management, safety management, and organizational measures.

The quantitative assessment can be carried out for the random failure aspect of safety integrity. There is currently no commonly accepted basis for quantifying systematic failures. To address systematic failures, a qualitative approach should be followed in compliance with the EN50128 standard.

To demonstrate that the system can achieve SIL 4 level, both hardware and software need to meet SIL 4 requirements. For hardware, a quantitative analysis must be performed. In this analysis, a Fault Tree Analysis (FTA) is used to demonstrate the safety level for random failures. Due to the lack of Hardware System Architecture input, and the knowledge of the failure detection/negation time, this system functional safety analysis cannot confirm the explicit SIL Level of LOC-OB. However, the Fault Tree Analysis can be performed based on the safety design justification from D4.1 [11] and wheel speed sensors hardware from the demonstrator. These assumptions will help assess the potential for the LOC-OB hardware system architecture to achieve SIL4 and provide guidance on designing the LOC-OB Hardware system architecture to meet SIL4 requirement. FTA is a proven common method to determine failure rate propagation through a given system. This FTA is based on input failure rates for the used hardware (sensors, platform) and calculates the failure rate of the LOC-OB system, based on this. The Fusion Algorithm can compute wrong output calculation based on algorithm failures or wrong input information from the sensors and data sources.

The objective of CLUG 2.0 is to continue the work started in CLUG with the same main objectives of demonstrating that an onboard GNSS-EGNOS-based multisensory fusion architecture enables absolute safe train positioning and navigation, and to consolidate the safe localisation system architecture by improving the design of the safe functional architecture. Regarding the LOC-OB

system's inability to reach SIL 4 level with a single configuration (one GNSS-EGNOS receiver, one IMU) as referenced in the result from CLUG I-RAMS Analysis Report D3.2.1 [22], therefore the design justification from CLUG 2.0- D4.1 [11] is proposed and used in this analysis to demonstrate the safety integrity level of LOC-OB.

In the meantime, an analysis of IMU DAL A level for both chains are proposed to compare the results. Therefore, two hardware configurations of LOC-OB will be used in the analysis. More detail can be found in chapter 6.3.

Note : D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version).

2.2 Requirement of WP2

To ensure that the requirements of the specifications (WP2) are considered, the most important conclusions and recommendations from D2.2 [2] (chapter 4.6.1 and 4.6.2) (Start of Mission and track selectivity) are copied here.

SCENARIOS	CONCLUSION
Start of Mission	C02: When the sensor accuracy of GNSS and IMU performance don't allow determination of Track Selectivity, operational measures of waiting and repositioning can improve sensor accuracy LOC-OB positioning performance. The repositioning could be carried out following the ETCS "staff responsible" operational procedures. However, repositioning with the absence of balises will not provide a guaranteed result and possible challenges arising, should be further analyzed. The ability of the LOC-OB to provide a Track Selective position is fundamental to Start a Mission without additional technical or operational measures.
Start of Mission	C03: The determination of the reference location by the LOC-OB without data from the previous train operation might not be safely possible.
Perform Mission	C01: For GNSS-centric solutions, especially in challenging environments, where no GNSS signal can be tracked, the LOC-OB's Area of Uncertainty can grow very large.
Perform Mission	C04: In certain topologies i.e., when passing a point in a Parting Tracks topology Track Selectivity determination might not be possible instantly, and especially in challenging environments establishing of Track Selectivity can take longer.
Perform Mission	C05: Consideration of protected train running path. To determine a track selective train position during a mission, trackside can consider the protected train running path if the train position is located inside this path.
Perform Mission	C06: Consideration of point positions. Another possibility for trackside to determine a track selective train position is the evaluation of the point position.

Table 1: Conclusion from D2.2 [2]

SCENARIOS	RECOMMENDATION	NOTE
Start of Mission	R01: The LOC-OB functional architecture should take several different sensor principles into account. In particular, the solution should not be too GNSS-centric to avoid the related disadvantages. The LOC-OB solution should rather consider GNSS-independent threads/channels in addition to channels using GNSS.	Balises are considered in this analysis as the second source of the reference location.
Start of Mission	R02: If environmental conditions are challenging, valid and safe dynamic trackside data such as point position or safe route information could be helpful as input to determine Track Selectivity. Please, note that usage of trackside information such as route information by LOC-OB input needs to be analysed for applicability and confirmed particularly from safety perspective. - For waiting and repositioning are operational measures that could be applied to improve GNSS positioning. These operational measures should be taken into account for the LOC-OB and be further detailed as operational solutions particularly when starting a mission. m safety perspective.	Point position information is considered in this analysis for track selectivity function.
Start of Mission	R03: CMD input data should be used if available. It can be complemented by LOC-OB positions, or CMD functionality could even become obsolete in certain cases e.g., when the LOC-OB remains in “always-on” state and the reported position is track selective.	CMD input data is considered as the input for LOC-OB Initialisation function.
Start of Mission	R04: A time limit for determination of Track Selectivity during Starting a Mission (cf. Section 4.5.1) should be defined. If the Starting a Mission scenario requires repositioning this step should be limited in distance to avoid influence on traffic (cf. Section 3.8). The limit could be application-specific and/or configurable for specific parts of the track network. This limit should be oriented towards current ETCS performance, especially to target current safety requirements.	

SCENARIOS	RECOMMENDATION	NOTE
Perform Mission	R05: A wide range of sensors based on different physical principles (this could be vision-based sensors like stereo cameras, etc.) should be considered to determine the correct track leg e.g., after passing a point, and render a position track selective.	There are 5 Unitary Solution for Track Selectivity Determination. As of now it is implements only two unitary solutions which combine GNSS and IMU to determine track selectivity.
Perform Mission	R06: The time or the distance when the Track Selectivity is determined after passing a point should be limited. The limit could be application-specific and/or configurable for specific parts of the track network. This limit should be oriented towards current ETCS performance, especially to target current safety requirements.	No define time or distance from D4.8 [13]
Perform Mission	R07: The position of the estFE should be reported as frequent as possible, but particularly at triggers. Triggers when positions should be reported can either be locations or events of the LOC-OB. • A position should be reported when track nodes or any defined locations on the track are passed, following current ETCS procedures. • A position report should also be triggered at certain events such as when Track Selectivity is established or lost, etc.	
Perform Mission	R08: If challenging environments lead to delayed determination of Track Selectivity in Shunting, the definition of shunting borders or operational procedures should reflect this.	

Table 2: Recommendation from D2.2 [2]

From D2.4 [4], chapter 7 and chapter 9, the requirements linked to Track Selectivity and SoM are listed below:

Req ID	**SpecSysReq[001]**
Requirement	The 1D localisation dataset toward the train front end provided by LOC-OB shall include: - Reference location id - Train orientation - Position qualifier (w.r.t. to the reference location) - Estimated distance - Underestimation of the estimated distance - Overestimation of the estimated distance - Track edge id - Validity timestamp
Additional information	Reference location id: Unique identifier of the element from which an estimated distance is given. Comparable to NID_LRBG but not limited to balise technology. could be any point in the digital map set as a reference point/node. Train orientation: Orientation of the train in relation to the direction of the reference location. Comparable to Q_DIRLRBG (refer to SUBSET-026-7 (cf. Ref [28])) but not limited to balise technology. Position qualifier: It tells on which side of the reference location the estimated train front end position is. Comparable to Q_DLRBG (refer to SUBSET-026-7 (cf. Ref [28])), but not limited to balise technology. Estimated distance: Distance along the track between the last relevant reference location and the estimated train front end position. Comparable to D_LRBG (refer to SUBSET-026-7 (cf. Ref [28])) but not limited to balise technology. Underestimation of the estimated distance: The safe distance along the track the train may have travelled further than the estimated train front end position. Comparable to L_DOUBTUNDER (refer to SUBSET-026-7 (cf. Ref [28])) but not limited to balise technology. Overestimation of the estimated distance: The safe distance along the track the train may have travelled shorter than the estimated train front end position. Comparable to L_DOUBTOVER (refer to SUBSET-026-7 (cf. Ref [28])) but not limited to balise technology. Track edge id: ID of the track edge where the train front end real position is. Validity timestamp: Time stamping of the output, i.e., the time when the localisation information was valid.
Category / classification	Functional
Traceability	UR[001]; UR[019]; SF-001
Acceptance Method	Analysis; Test
Safety assumption	Refer the dataset definition table in D2.4 [4], chapter 7.1.1

Req ID	SpecSysReq[027]
Requirement	LOC-OB, from the train power on, shall initialise itself and provide the outputs with no human supervision.
Additional information	refer to D2.2 (cf. Ref [2], Section 4.3.1)
Category / classification	Functional
Traceability	UR[004]
Acceptance Method	Analysis; Test
Safety assumption	Not related to safety

Req ID	SpecSysReq[028]
Requirement	After being powered up and its initialisation stage ended, LOC-OB shall provide data continuously.
Additional information	LOC-OB is a data provider. User's application shall receive updated data continuously with regard to SpecSysReq[033].
Category / classification	Functional; Performance
Traceability	UR[007]
Acceptance Method	Analysis; Test
Safety assumption	Not related to safety

Req ID	SpecSysReq[029]
Requirement	After the LOC-OB is powered-on, it shall fulfil entire operational capability in less than 1 minute when initial position is valid under the following conditions: 1. Initial position is known (e.g., last known position is saved before LOC-OB is switched-off). 2. Track edge id is known (e.g., last track edge id is saved before LOC-OB is switched-off). 3. Cold Movement Detection (CMD) doesn't indicate a train movement while the train has been powered off.
Additional information	Refer to D2.2 (cf. Ref [2], Section 6.1.5, Section 6.6.1 & Section 6.6.2)
Category / classification	Performance
Traceability	UR[004]; D2.2 (cf. Ref [2], Section 6.1.5, Section 6.6.1 & Section 6.6.2)
Acceptance Method	Analysis; Test
Safety assumption	Not related to safety
Req ID	SpecSysReq[030]

Requirement	After the LOC-OB is powered-on, it shall fulfil entire operational capability in less than 10 minutes when initial position is not valid under any of the following conditions: 1. Initial position is unknown (e.g., last known position is not saved before LOC-OB is switched-off). 2. Track edge id is unknown (e.g., last track edge id is not saved before LOC-OB is switched-off). 3. CMD indicates a train movement during the train is powered off.
Additional information	Refer to D2.2 (cf. Ref [2], Section 6.1.5, Section 6.6.1 & Section 6.6.2)
Category / classification	Performance
Traceability	UR[004]; D2.2 (cf. Ref [2], Section 6.1.5, Section 6.6.1 & Section 6.6.2)
Acceptance Method	Analysis; Test
Safety assumption	Not related to safety

Req ID	**SpecSysReq[031]**
Requirement	In case the LOC-OB cannot reach full operational capability after the system is powered on (e.g., Unknown track segment / track edge), estimated speed and travelled distance since the LOC-OB is powered on shall always be provided.
Additional information	Refer to D2.2 (cf. Ref [2], Section 6.1.5, Section 6.6.1 & Section 6.6.2)
Category / classification	Performance
Traceability	UR[005]; D2.2 (cf. Ref [2], Section 6.1.5, Section 6.6.1 & Section 6.6.2)
Acceptance Method	Analysis; Test
Safety assumption	Not related to safety

From D2.4, chapter 7.1, the requirement linked to Track Selectivity are listed below:

Req ID	**SpecSysReq[002]**
Requirement	LOC-OB shall provide the track edge ID where the train front end position is.
Additional information	Refer to D2.2 (cf. Ref [2], Section 6.4.1)
Category / classification	Functional
Traceability	UR[022]
Acceptance Method	Analysis ; Test
Safety assumption	Not related to safety

Req ID	SpecSysReq[007]
Requirement	The train front end true position shall be included in the LOC-OB computed confidence interval towards the train front end position within the most constraining user exported THR. Train true position is within [(Reference location id + Estimated distance - Overestimation of the estimated distance); (Reference location id + Estimated distance + Underestimation of the estimated distance)].
Additional information	The Automatic Train Protection (ATP) will process safe protection of the train considering the worst cases possible (max safe front end / min safe front end). To be noticed that the 1D dataset specified is following Ref [28] principles with an estimated value (most probable value) expressed by a distance to a reference location and bounded by and over and an underestimation. Therefore: Min safe front end = Reference location + Estimated distance - Overestimation of the estimated distance. Max safe front end = Reference location + Estimated distance + Underestimation of the estimated distance. THR values will be defined in the scope of WP3.
Category / classification	RAMS
Traceability	UR[022]; UR[025]
Acceptance Method	Lab test; field test; verification
Safety assumption	Related to safety

Req ID	SpecSysReq[070]
Requirement	The track edge ID provided by LOC-OB shall refer to the track edge occupied by the train front end real position within the most constraining user exported THR.
Additional information	Refer to D2.2 (cf. Ref [2], Section 6.4.1). THR values will be defined in the scope of WP3.
Category / classification	RAMS
Traceability	UR[022]
Acceptance Method	Lab test; field test
Safety assumption	Related to safety

2.3 Result from the PHA

The Safety Results from Preliminary Hazard Analysis [10] are reused, and System Functional Safety Analysis in chapter 5.2 is traced against the Hazard Identification list from PHA.

CLUG 2.0 EVENT ID	CLUG 2.0 EVENT DESCRIPTION	LOC-OB FEARED EVENT DESCRIPTION
LOC-OB-HZ-02	Speed provided by LOC-OB underestimates trains actual speed	Fail to provide upper bound speed higher than the actual train speed
LOC-OB-HZ-03	Incorrect movement speed direction related to the last reference point	Fail to provide the correct train movement direction Fail to provide the correct train orientation Fail to use the correct reference point information from digital map Fail to use the correct reference point id
LOC-OB-HZ-04	The confidence interval for distance measurement and calculation does not include the real position of the train	Fail to provide confidence interval which include the real train position (measured distance interval and position qualifier and reference point id) Fail to provide the correct train movement direction Fail to provide the correct train orientation Fail to use the correct reference point information from digital map Fail to use the correct reference point id Fail to provide upper bound speed higher than the actual train speed Fail to provide confidence interval which include the real train position (measured distance interval and position qualifier and reference point id)
LOC-OB-HZ-05	Acceleration provided by LOC-OB overestimates trains actual acceleration	Fail to provide lower bound acceleration lower than the actual train acceleration
LOC-OB-HZ-06	The track edge id is not the correct one	Fail to provide the correct track edge id
LOC-OB-HZ-07	The computation of the confidence interval for distance measurement does not allow a safe reaction to odometry errors	Fail to provide confidence interval which include the real train position (measured

CLUG 2.0 EVENT ID	CLUG 2.0 EVENT DESCRIPTION	LOC-OB FEARED EVENT DESCRIPTION
		distance interval and position qualifier and reference point id)
LOC-OB-HZ-08	The relocation of location does provide a wrong position of the train	Fail to provide confidence interval which include the real train position (measured distance interval and position qualifier and reference point id)
LOC-OB-HZ-09	Intentionally deleted	
LOC-OB-HZ-10	Incorrect vehicle attitude	Fail to provide 3D vehicle attitude which include the real train position
LOC-OB-HZ-11	Incorrect 3D estimated position	Fail to provide 3D position uncertainty which include the real train position
LOC-OB-HZ-12	Incorrect 3D estimated speed	Fail to provide 3D speed uncertainty which include the actual train speed
LOC-OB-HZ-13	Incorrect 3D estimated acceleration	Fail to provide 3D acceleration uncertainty which include the actual train acceleration
LOC-OB-HZ-14	Electrical shocks with passengers during normal operation (travel, or on-station) or by staff during maintenance phases due to LOC-OB.	Fail to protect against electrical choc
LOC-OB-HZ-15	Disturbance of signalling trackside of onboarded system to EMC emission/conduction from LOC-OB system leading to accident	Fail to protect against CEM disturbance
LOC-OB-HZ-16	Disturbance of LOC-OB due to EMC emission/conduction from other train systems or track side equipment.	Fail to protect against CEM disturbance

CLUG 2.0 EVENT ID	CLUG 2.0 EVENT DESCRIPTION	LOC-OB FEARED EVENT DESCRIPTION
LOC-OB-HZ-17	Mechanical interference of the LOC-OB with other physical equipment	Fail to ensure mechanical requirement
LOC-OB-HZ-18	Collision with Trackside/Infrastructure due to new train size (new equipment exceeding train size/envelop)	Fail to ensure mechanical requirement

Table 3: List of derived hazard from PHA result – D3.2 [10] chapter 6.1

3 LOC-OB SYSTEM DEFINITION

3.1 WP2 high-level block diagram

The goal of LOC-OB is to provide the train localisation information while allowing the train safely running on the European railway networks.

LOC-OB in the context of CLUG 2.0 with a preliminary defined sensor set mainly aims to aggregate GNSS and EGNOS data with other sensors such as inertial sensors, speed sensors and additional information like Map Data or - if applicable - route information [20]. The result shall be an improvement of localisation through multi-sensor fusion, to deliver more robust, accurate and safe localisation information.

To guide the development of the LOC-OB unit, the following functional blocks are structured and defined as follows:

- On-board Measurement: This functionality handles the acquisition and processing of localisation sensor data.
- Integrity: This functionality guarantees the integrity of all LOC-OB functions and outputs.
- Navigation: Multi-sensor fusion algorithms are processing the measured data together with supporting information such as Map Data or augmentation data to compute localisation information. The result of this calculation is delivered to consumer functions/systems as safe and non-safe information. While non-safe information is used for uncritical consumer systems like the PIS, safe information come from both integrity functional blocks and navigation functional block.
- Map Data Processing: Within the LOC-OB, the acquired Map Data needs to be processed according to the use-case of the navigation functionality.
- Interfaces: They are responsible for receiving and providing information from or to other systems of the CCS-OB.

These Functional blocks exchange data with each other and external systems. Some components consume and provide information from and to external systems.

In Figure 1 the complete structure of LOC-OB is presented, including all interfaces and external systems. The clustered functionalities, such as on-board Measurement, Integrity, Navigation, Map Data Processing, Safe and Non-Safe Information, and all system functions SF-xxx, are provided as a guide and visual aid to enhance comprehension.

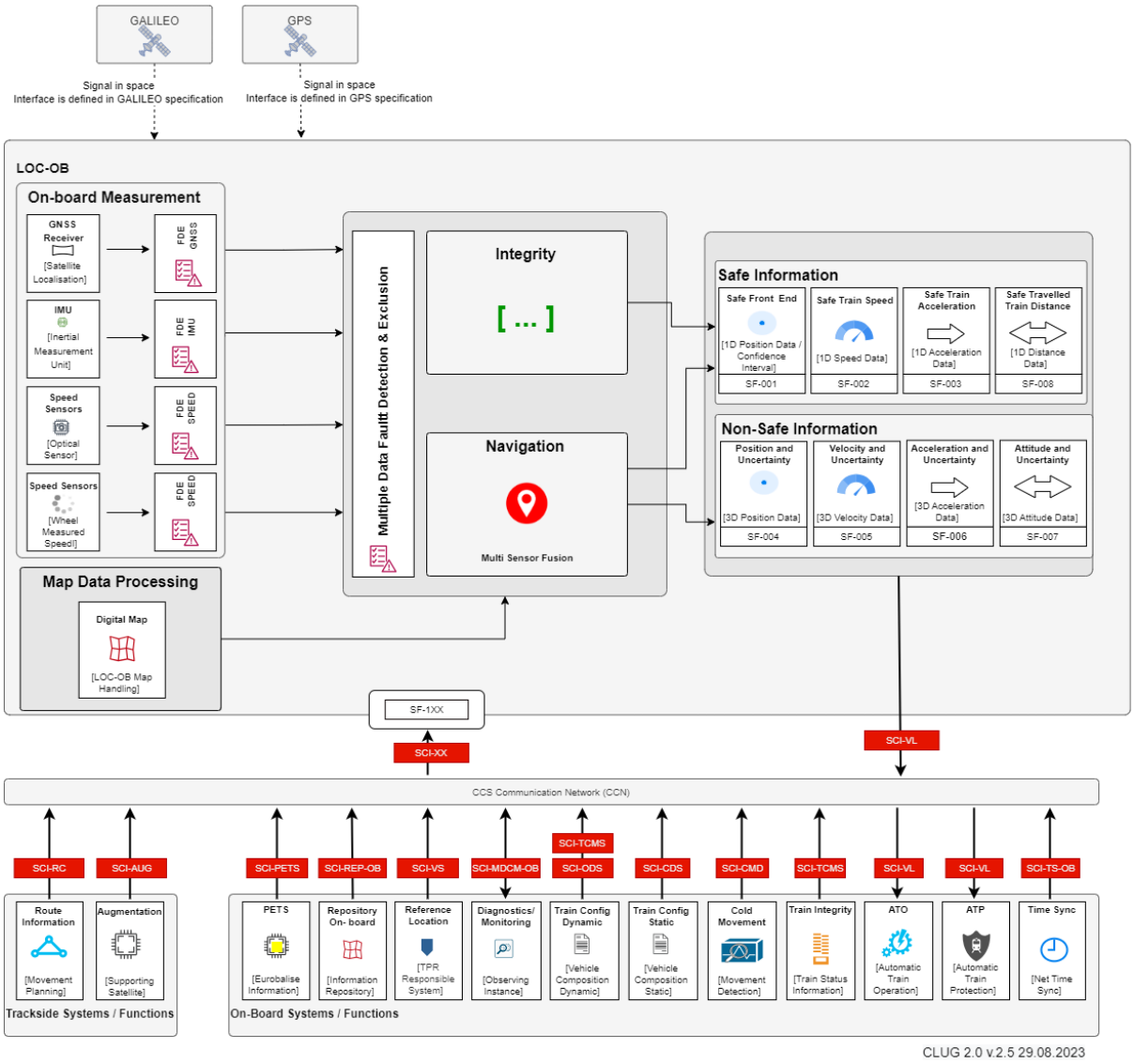


Figure 1: Main External System Constituents (extract from D2.3 [3])

More detail can be found in D2.3 LOC-OB System Definition and Operational Context [3].

3.2 Architectural description of the solution

The LOC-OB functional architecture relies on multi-sensor tight fusion, empowered with integrity algorithms. It consists in merging GNSS navigation data, made safe by EGNOS, with other sensors (inertial sensors, tachometer, digital map, trackside equipment, etc.) to improve the performances of standalone GNSS, especially in the rail operational environment with reduced GNSS satellite availability. The simplified functional architecture has become as followed:

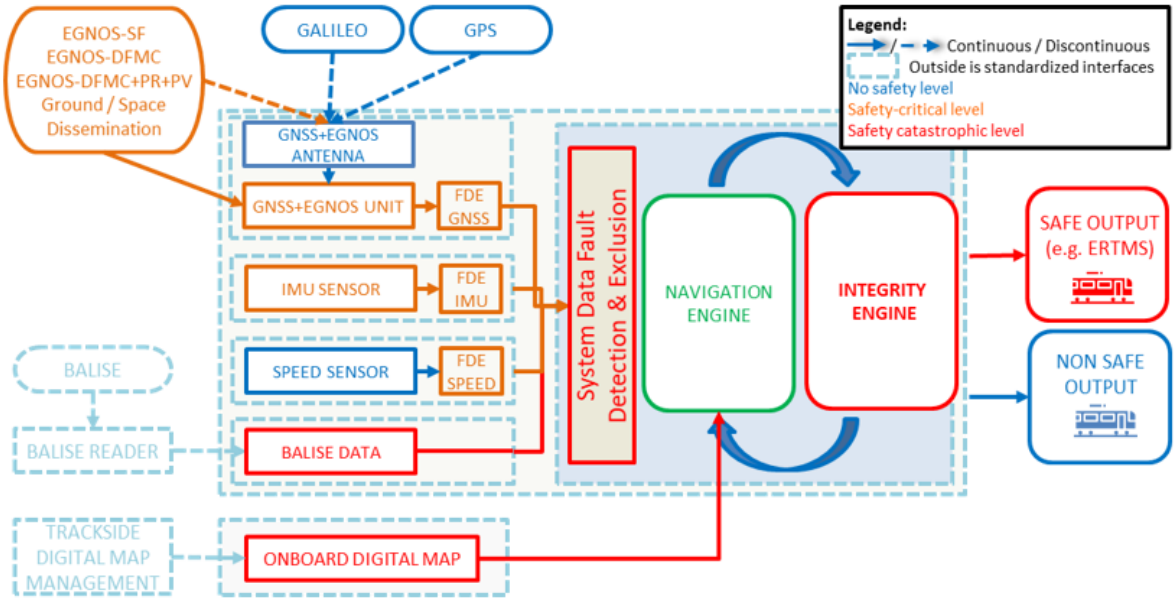


Figure 2: CLUG 2.0 LOC-OB high level functionoal architecture (extract from D4.1 [11])

The LOC-OB is principally composed of:

- Set of Sensors:
    - GNSS+EGNOS unit and its data FDE: that receives the Galileo (E1 & E5) and GPS (L1 & L5) signals via one or two roof antenna, safely augmented by the EGNOS data received via the rail ground network, and via SIS (Signal in Space) as the GNSS antenna are SBAS compatible. Unlike the GNSS discontinuity, the EGNOS stream, whatever the one that would be selected in rail domain, has to be continuously received in order to safely use any of GNSS satellite signal, even discontinuous. More detail can be found in chapter 3.2.1.
    - IMU (inertial unit) sensor and its data FDE: that measures and provides 3D acceleration and angular rate (attitudes: yaw, roll, pitch); More detail can be found in chapter 3.2.2.
    - Speed sensor (e.g. tachometer or equivalent) and its data FDE: that measures and provides along track speed and that is not to be confused with any legacy “SIL4 odometer system” embedding several independent speed sensors. More detail can be found in chapter 3.2.3.
- Balise data: Even CLUG 2.0 aims to reduce as much as possible trackside balises used for localisation and for providing reference points, this sensor is kept as mitigation sensor in too harsh and demanding areas where the {IMU + speed sensor} can’t cope with a lack of GNSS access for too long (i.e. position and speed CIs become too large). More detail can be found in chapter 3.2.4.
- Onboard Digital map: that contains all the 3D multitrack layers enabling the navigation engine to compute track selectivity and 1D kinematic data. The digital map is assumed to be up to date, regardless of the operational process from a centralized maps database centre (“offline" download before the train start of mission of “periodic” download), that is not in the scope of this document. A more detailed description is available in chapter 3.2.5, [CLUG (1) D3.1.2.5] [21] and in [CLUG 2.0 D4.10 [20]].

- "Navigation and Integrity engine" module containing algorithms:
    - System data Fault Detection and Exclusion (FDE),
    - LOC-OB Initialisation function,
    - Track selectivity function,
    - Sensors tight fusion along track function,
    - Integrity confidence intervals and confidence status computation.

  More detail can be found in chapter 3.3.

Note: Data Fault Detection and Exclusion (FDE) aim at detecting, and at filtering/excluding the faulty data before their uses into the algorithms. They are ventilated into sensor perimeters and into the localisation engine. More detail can be found in D4.1 LOC-OB Functional Architecture [11].

Note : D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version).

3.2.1 LOC-OB with GNSS and EGNOS high level block diagram

Following the [CLUG (1) D3.4] initiative, and based on the previous sections, here is illustrated the higher-level representation on how the LOC-OB should interface to the GNSS signals and EGNOS facilities to continuously receive the selected EGNOS data stream:

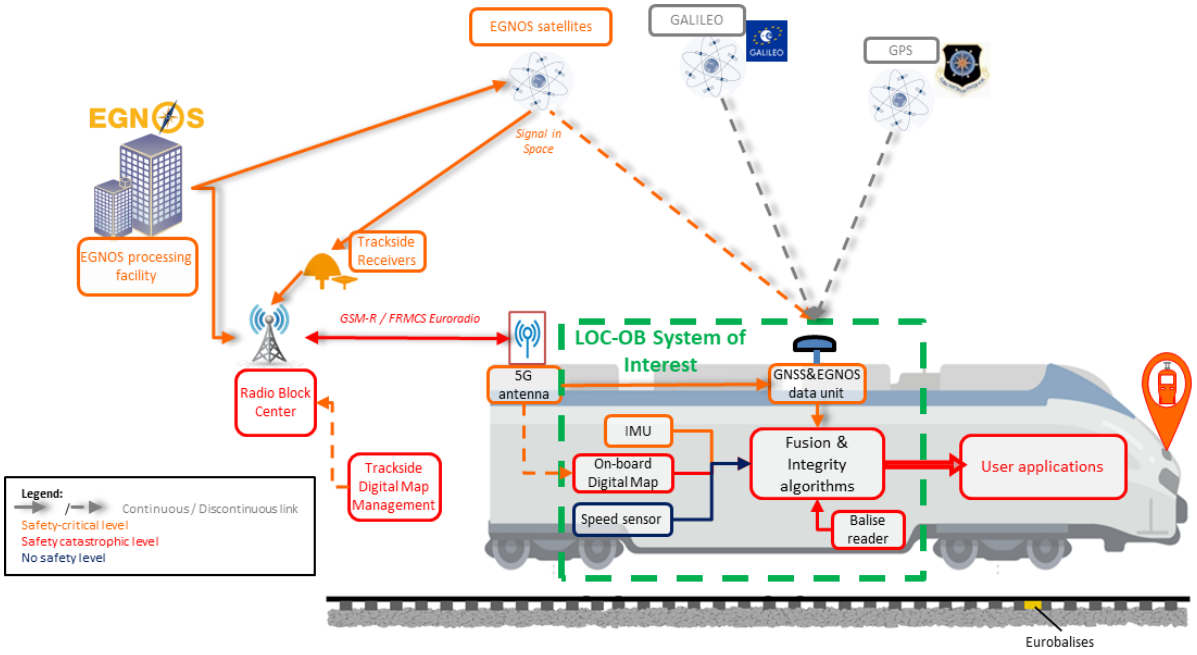


Figure 3: CLUG LOC-OB High level functional architecture (extract from D4.1 [11])

Three ways of EGNOS data stream dissemination are illustrated on **Figure 3**:

- Signal in Space broadcast by 2 geostationary satellites in hot redundancy: Current legacy safe dissemination via space dissemination that produces non continuous reception from rail (or terrestrial) users as mentioned in previous section.
- Via rail trackside fixed receivers tracking GEO SiS: On-going ERTMS change request (CR1368 – GNSS Augmentation for ERTMS/ETCS System Functional Hazard Analysis) targeted to be part of the TSI update in 2027/2028 TBC and limited to disseminate SFSC and DFMC streams from space, so preventing to disseminate future EGNOS stream optimized for rail or terrestrial users if not entirely available from space. The objective of this change request is to define a high-level EGNOS-based functional architecture for safety analyses. This includes presenting the reference functional architecture for the GNSS Augmentation On-board (GA-OB) and GNSS Augmentation Trackside (GA-TS) systems. Please note that GA-TS is not applicable in CLUG2.0.
- Via direct connection(s) between EGNOS facility and rail networks: it consists in creating direct connection from the EGNOS facility to a set of European rail Radio Block Centre gates, that after relay EGNOS stream withing the Euroradio up to each train. This dissemination type consisting in adding a dedicated EGNOS subsystem named “EGNOS Safe Gate” is, submitted by Airbus to EUSPA and ESA in ERJU/R2DATO/EGNOS initiative, offering larger bandwidth capacity to any EGNOS streams, existing and optimized future ones. From Airbus point of view, adding an EGNOS Safe Gate would be much more efficient than the ERTMS CR1368 and could be put in place in the same time order in magnitude, i.e. mid-term.
- Note regarding the 2 last bullets involving GSM-R/FRMCS: in the event of a communication failure (GSM-R/FRMCS) or interruptions lasting several tens of seconds, there is forced braking until the vehicle comes to a standstill.

The D4.1 approach consists in disseminating the EGNOS data stream via the 2 following streams:

1) Primarily via the terrestrial network Euroradio (GSM-R/FRMCS) implementing a safe communication protocol (cf. subset 37 for instance) ensuring SoL certified at catastrophic safety level (THR <1E-9/h). But noting EGNOS is developed at THR < 1E-7/h in data integrity (DAL B critical safety level), the link from the EGNOS Safe Gate to the RBC (access points to the Euroradio) won’t reach the catastrophic safety level a priori, even if the communication protocol is developed at such THR (data and time integrity protection).
2) And combined with a space SoL dissemination with an easy data integrity check mechanism and a very low latency capacity safely ensured up to each LOC-OB under the coverage (same data integrity mechanism as for Aviation).

Note: FRMCS is not yet operational and remains in the test phase.

For FDE of GNSS-EGNOS data, the data FDE algorithms detect and exclude inputs that are not in line with their nominal distributions. This can happen in particular due to the local environment effects (e.g. multipath). “Out of nominal GNSS measurement due to local effect” shall be rejected by the data FDEs prior to enter the system data FDE. SBAS cannot correct local errors as SBAS ground segment has no knowledge of user environment (not correlated enough in space, unlike ionospheric errors).
Finally, this FDE outputs safe and filtered pseudo ranges, Doppler ranges, satellites positions data and constellations time to the other functions for localisation computation requiring the usage of valid data. More detail can be found in D4.1 LOC-OB Functional Architecture [11].

Please note that D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version). As we are at the end of the project, "To Be Confirmed" (TBC) elements shall be properly justified and addressed. "TBC" can be addressed in the release version of D4.1 or in further study (e.g. CLUG 3.0 project).

3.2.2 Inertial Measurement Unit (IMU)

Inertial Measurement Unit (IMU) is an electronic device that measures body's specific force in terms of accelerations and angular rates. The IMUs basically consist of 3 accelerometers and 3 gyroscopes; the first ones provide 3 accelerations corresponding to the accelerations in three orthogonal axes and the gyroscopes provide 3 angular velocities of the body in the same 3 orthogonal axes. While gyroscopes provide orientation, accelerometers deliver information on speed and direction of acceleration, based on a measurement of linear acceleration of the vehicle relative to itself. Angular velocity together with linear acceleration can provide accurate information for all position changes of the moving vehicle.

There are 3 types of IMU as following:

- Mechanical
- Optical
- MEMS (Micro Electro – Mechanical Systems)

An inertial navigation system (INS) devices operate on a dead reckoning system, which means that the initial position, velocity, and orientation of the vehicle are provided by an external source, which can be a GNSS satellite receiver or an operator. Equipped with this data, the INS can begin calculating position, velocity, and other movement elements. As the vehicle continues to move, the INS device will keep calculating and updating, on its own, all motion elements via the information received from motion sensors.

Concerning the performances for the inertial sensors, a first technical consideration considers the composition of IMU being accelerometers and/or gyroscopes. Indeed, accelerometers and gyroscopes can be used as individual inertial sensors, but most applications combine these sensors together into an inertial measurement system (IMU). When a gyroscope is used in conjunction with an accelerometer, the performance of the gyroscope typically has the greater impact on the inertial navigation performance. Due to this, the gyroscope in-run bias stability is often used as a short-hand measure of inertial system quality providing what is usually associated to the performance grade. So, to narrow down the parameters, only gyroscope characteristics are considered for the classification, because they have the biggest impact in the navigation performances.

However, there are still IMU errors influence on fusion algorithm of the LOC-OB solution. Vibration effect in signals is noise, so, the fusion algorithm cannot do anything to estimate the effect of vibration. The only way to reduce its effect is to select better IMUs with less dependency on vibrations. Regarding temperature, the fusion algorithm assumes that the effect of temperature is compensated

by the IMU itself, so, a mandatory requirement for the IMU is the temperature compensation. More detail can be found in D4.3 Safe IMU sensor and data FDE for LOC-OB [17].

As information from D4.1 [11] , Airbus proposes to use IMU DAL B level and provide the list of first COTS IMU DAL B objective that could comply the LOC-OB are identified:

- Emcore EN300-1: Emcore supported Boeing to DAL B certify another IMU (SDI300) but not adapted for railway; Emcore "*do not have any IMU train certified but the way we usually work is that our customers do the certification of the complete system and we/Emcore is providing all technical support needed during this process*".
- Honeywell HG1700: targeting DAL B but not promoted in their website (https://aerospace.honeywell.com/us/en/learn/products/sensors/hg1700-inertial-measurement-unit)
- Analog Device ADIS16487: "DAL B certification intent" (https://www.analog.com/en/products/adis16487.html); it is not the model equipping the SMO/SBB Domino test train
- Northrop-Grumman LN200 (FOG): "certifiable DAL A" but not demonstrated yet, so sceptical to reach higher THR demonstration than DAL B (https://www.northropgrumman.com/what-we-do/air/ln-200-fog-family-advanced-airborne-imu-ahrs/)

In the Fault Tree Analysis (FTA), the IMU from Honeywell (HG 1700, MTBF 2000 hours) and the DAL A level IMU from Northrop-Grumman (LN200, MTBF 2000 hours) are used.

For Fault Detection Exclusion of IMU, there are not much possible solutions to apply FDE strategies to an isolated IMU or pair of IMUs. Indeed, in the bibliography it is difficult to find any solution. The comparisons between both IMUs will only serve to detect that at least one of them is in error, but not to detect which of the two is the one in error. To be able to identify the faulty IMU, another trustful information source will be necessary. For multiple IMUs, obviously, the operations described in Section 5.2 can be applied pairwise between the IMUs. In this case, if only one of the IMUs is in faulty state, then it is possible to identify the IMU in error. However, it is indicated that multiple IMUs is out of scope of the CLUG 2.0 refer to D4.3 – Safe IMU sensor and data FDE [17].

3.2.3 Wheel Speed Sensors

On railroads, tachometers, or Odometer Pulse Generators (OPG) on the wheel/rail system, Doppler radars and sometimes optical correlations sensors are usually used for speed measurement.

The aim should be to detect the train speed and its travelled distance along the track. The OPGs provided for this purpose are usually mounted on axle covers or gearboxes and scan gear wheels or pinholes that move with the rotation of the axle/wheel. Depending on the number of teeth/holes, the wheel is divided into angular steps with OPGs typically outputting one pulse per angular step. These pulses integrated by counters result in a cumulative angle over time. It is also possible to measure the main frequency of the pulses directly.

However, only the absolute timestamps of the individual pulses are recorded. With the knowledge about the wheel diameter as well as the pulses per revolution the current speed can be derived. Due

to e.g., changes in the wheel diameter, slip and slide, the *wheel speed* will deviate from the linear *vehicle speed* and the distance it has travelled.

Effects that make the wheel velocity differ from the train velocity are slip and slide of the wheels and wear of the wheel leading to incorrect wheel diameter.

Furthermore, it is important to know at the capturing platform, what type of axle the OPG is mounted on. Depending on the equipment, different behaviour of the axles can occur. E.g., a controlled axle shows less likely slipping or sliding of the wheel. The OPGs should preferably be mounted on different axles that are not driven or braked. However, these are often not available. For example, locomotives designed for maximum tractive power only have driven and braked axles. In train formations, driven and non-driven wagons often alternate, so that non-driven axles can at least be found on the neighbouring wagon. Non-braked axles are not usually present, in the best case there are some that are not braked operationally but only when the emergency brake is applied.

Combinations of the equipment for an individual axle are possible.

It is important from a signal processing perspective, that if using multiple OPGs, the axles are independent of each other. This means that they are mounted on different bogies, and if controlled, braked and/or driven, the engines should be independent (also have different frequency converter). This is best practice, how OPG sensors should be implemented on the train and is in favour of data FDE purposes. More detail can be found in D4.4 Speed sensor and data FDE for LOC-OB [18].

For FDE of Wheel Speed Sensors, the OPG and its data FDE dedicated to the most root cause of inaccuracy that are mainly slip and slide events, were presented with associated limitation to properly filter faulty data or to excessively filter valid data. Thus, a Sensor Level FDE would need to be complemented at System Level if the objective is to improve the separation between faulty and valid data.

3.2.4 Balises

The aim of CLUG 2.0 is to reduce the use of trackside balises, it is anticipated that some balises will still be needed in critical areas, such as where the loss of GNSS cannot be sustained by the remaining sensors over the required time, respectively distance. When used, the balises have a direct impact on the system performance of the LOC-OB at least where the lack of the GNSS augmented by SBAS would be required to be compensated. Balises could also play a role in start of mission function, e.g., after a cold start or when the cold movement detector reports “cold movement”. The main benefits of Eurobalises are that they work even under extreme environmental conditions, at speeds of up to 500 km/h and provide an absolute position (along track and track selective) in SIL4. The main disadvantage is that they have to be removed and reinstalled for certain types of track work. By reducing the number of balises, it can reduce the installation cost and maintenance cost.

Data Fault detection and exclusion (FDE) algorithms are implemented in the LOC-OB for all sensors, to prevent faulty data being used in the Sensor fusion. The need for such algorithms on the balise produced data has been discussed, and subsequently rejected, as the Balise Transmission System

delivers SIL 4 data to the onboard system. More detail can be found in CLUG 2.0 D4.5 Eurobalise Reader Sensor and data FDE for LOC-OB Description [19].

3.2.5 Digital Maps

The digital map contains multiple information layers (Track network topology through track edges and Track nodes and Track Centreline, Balise, Curvature, Cant, Gradient) are used to compute the track edge and then the 3D position to 1D along track position.

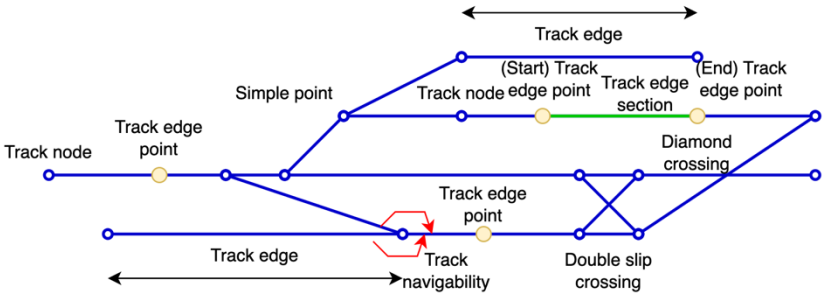


Figure 4: Sketch of an example railway network topology including the most relevant terms. (extract from D4.10 [20])

The railway network can be described by a node-edge model. An example is shown in Figure 4. The most basic elements which are needed for a common understanding are explained below.

- A **track node** represents a simple point, a system border, a buffer stop, or an end of a track. In the figure above, track nodes are represented by blue circles.
- A **track edge** connects two track nodes as indicated by a blue line between two blue circles. The track edge is associated with a direction, meaning that it starts at a defined track node and ends at another one.
- The **track navigability** describes which track edges on a track node are subsequently driveable.
- A **track edge point** is a location on a track edge.
- A **track edge section** is a part of a track edge and is defined by a start and end track edge point.

The digital track map is stored in the trackside and in the on-board computers of the system on a memory card, which is being exchanged when changes are made to the trackside or to onboard parameters. The trackside system includes a data index in each data telegram to allow the onboard unit to select the correct database, as different versions of the database can be stored in the memory cards.

More detail can be found in CLUG 2.0 D4.10 Onboard Digital Map Definition and Interfaces [20].

3.3 System Functional Description

The objective of the LOC-OB (Localisation On-Board Unit) is to provide a safe localisation to railway users by applying GNSS measurements, SBAS information, data from multiple sensors (IMU, speed sensors, balise reader and digital map), and integrity concepts. The functional architecture of the LOC-OB is presented in the Figure 5 below.

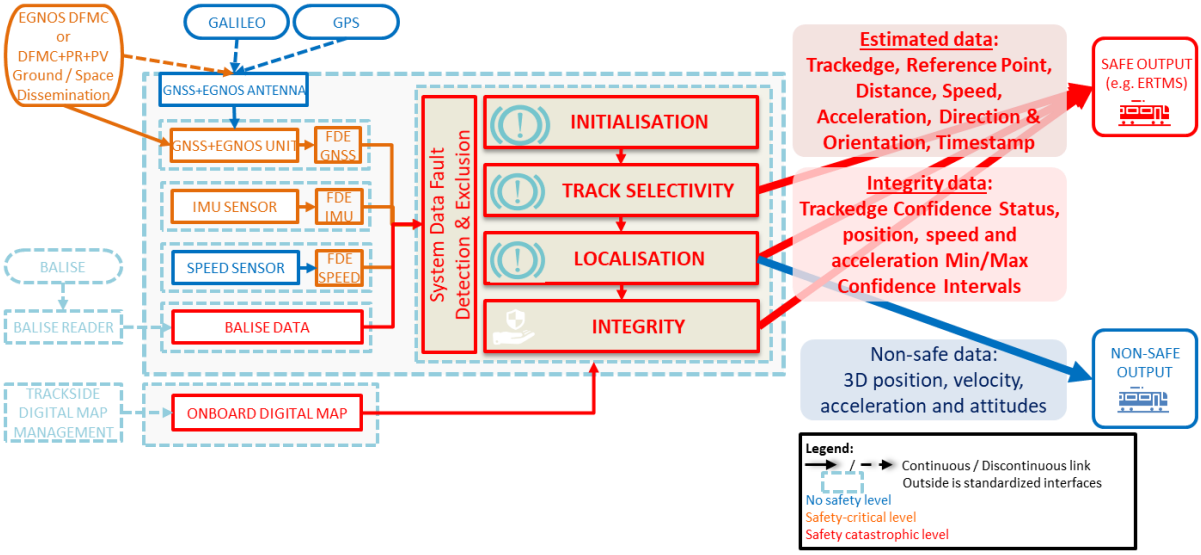


Figure 5: Overall functional architecture of the LOC-OB optimized solution (extract from D4.1[11][3])

For simplicity, the global architecture can be split into two main groups: the measurements processing core and the navigation core. The measurements processing core of the LOC-OB includes the digital processing of GNSS and SBAS signals, IMU unit, speed sensor, balise and digital map database process unit. The navigation and Integrity engine includes the following functions:

- System and Multiple data Fault Detection and Exclusion
- Initialisation and start of the mission
- Track selectivity
- Along track Localisation
- Integrity

There is a relationship between the integrity and localisation functions as both use information from each other. As an example, the confidence interval (CI) at the output of the integrity module is computed from estimates by the localisation function. In reverse, the integrity function provides safety information about the state of the filter implemented at the localisation function.

The LOC-OB INIT is an Initialisation function addressed in WP4.9 [14] and aims at identifying possible ways to provide safe Initialisation means to the LOC-OB. The along track localisation function is addressed in the scope of WP4.6 [15] and it provides estimation of the train states like position and velocity. It is anticipated that this function builds on top of the already mature EKF developed and tested in the frame of CLUG 1.0 by Airbus. The track selectivity function (addressed in WP4.8 [13]) has

the task to estimate safe track segment of the network that the train is actually occupying and providing it to the along-track localisation. The Integrity monitoring function has the objective to guarantee safety on the sensor tightly fusion output. This is achieved by (1) monitoring the raw sensor data with FDE algorithms (or barriers) and (2) providing safe over bounding of the sensor fusion algorithm errors. For what concerns the former point, two types of FDEs are identified in CLUG 2.0:

- Data FDEs: detection and exclusion are attempted by making use only of the sensor data itself.
- System FDEs: detection and exclusion are attempted with higher-level state information coming from the along-track localisation function.

The integrity monitoring function is addressed in multiple CLUG 2.0 WPs: WP 4.7 for the computation of the Confidence Intervals [16], WP4.6 for the system FDEs [15] and other work packages for each sensor data FDE (for example, WP4.2 for GNSS data FDEs [12], WP4.3 for IMU FDEs [17], WP 4.4 for Tacho FDE [18]).

CLUG 2.0 pragmatic architecture / 2 independent chains

In the CLUG 2.0 pragmatic architecture, there are 2 independent chains. The first chain is functionally unchanged from the optimized architecture. In that first chain, the Navigation and Integrity engine is decreased in SIL level to make it more feasible and at the THR level that Kalman filter has been already certified in aviation domain, so at THR 2.4E-6/h aviation PA or 1E-7/h aviation NPA that the {GNSS+ENGOS} inputs offer. The delta value for THR to reach the THR < 1E-9/h at the LOC-OB output is thus allocated to a second independent chain, named “Shape and heading map matching”. Then the 2 chains deliver their outputs, i.e. the 1D along track pos./speed/acc. estimation, computed CIs and optionally THR, to a new function, named “Combiner” that compute average estimates, perform the union of the computed CIs that is the LOC-OB outputted CI at the (mathematical) product of both THR. The Combiner function is a simple function making the union of the computed CIs, as described in [CLUG 2.0 D4.7], that should be easily feasible at SIL 4.

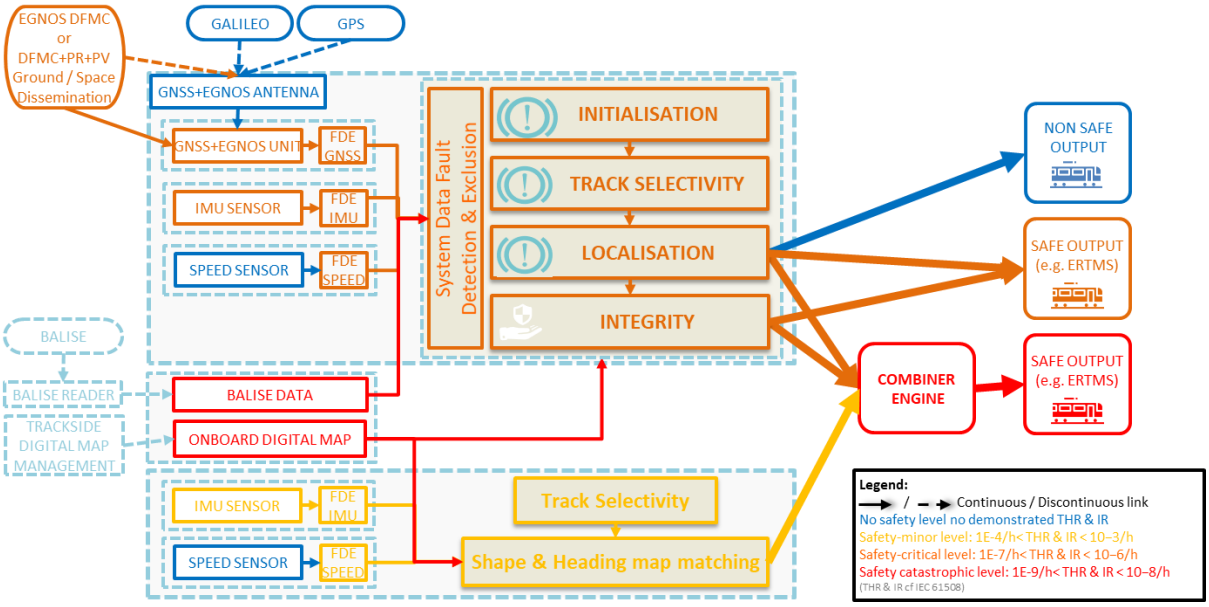


Figure 6: CLUG LOC-OB functional architecture pragmatic solution / 2 independent chains (extract from D4.1[11])

Note: D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version).

3.3.1 Sensors and System Data FDE

Raw measurements from the sensors require to be analysed to detect and to exclude faulty ones, i.e. exceeding configurable thresholds defined by the targeted THR values. These faulty data can come from LOC-OB external and internal feared events. Data FDE are revealed to be needed for the LOC-OB sensors that are not assumed pragmatically compatible to SIL4 THR, i.e. {GNSS+SBAS}, speed and IMU sensors. Indeed:

- The balise data sensor has been assessed in [CLUG 2.0 D4.5] section §1.1 to not need (additional) data FDE as "… *Eurobalises … provide an absolute position (along track and track selective) in SIL4… The need for* [Data Fault detection and exclusion (FDE) algorithms] *on the balise produced data has been discussed, and subsequently rejected, as the Balise Transmission System delivers SIL 4 data to the onboard system*."
- The on-board Digital Map is assumed already providing data in SIL4 quality, so no need of data FDE algorithm.

Data FDE algorithms are introduced into the LOC-OB at sensor level (cf. previous section) and at system level (i.e. mix of the sensor outputs). These multiple algorithms aim to detect and filter any faulty data before their uses into the navigation and integrity engines, contributing in the targeted THR.

Data FDE at sensor level

Some sensors already implement internal data FDEs that exclude data, so to not output data detected not compliant to the sensor specifications, or to output them with a flag alerting these data may be outside the sensor specifications (for instance when the temperature is outside its operational range).

The most the sensor is certified at a safety level, the most the sensor implements internal FDE to output safe data with defined accuracy performance associated to the certified safety level.

For the LOC-OB design, additional data FDE have been defined and are prototyped within CLUG 2.0 taking into account the usage of the sensors into a carriage.

Data FDE at system level using the multi-sensors measurements

By comparing the sensors data fully independently of each other, when simultaneously available, system data FDE can detect and filter more deeply faulty sensors or faulty sensor measurements/data. For example:

- Speed sensor data can be compared with IMU speed estimated from acceleration and with GNSS Doppler (or local PVT) to exclude data with large differences like slip and slide event.
- Because of multipath for instance, several GNSS satellite data (range and range rate) contributing to excessive estimated position or speed when mixing with IMU and/or speed sensor can be excluded.

Data FDE at system level are described in [CLUG 2.0 D4.6] *LOC-OB Along track localisation fusion algorithm design document*.

The following **Table 4** describes the inputs/outputs of the "System Data FDE" function:

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
LOC-OB internal Time	absolute time in GPS and/or Galileo and/or UTC, enslaved to GPS and/or Galileo reference system time	Input	System FDE	GNSS-EGNOS Receiver
Galileo Code & Phase Pseudo ranges	Raw & filtered Code & Phase Pseudo range per Galileo satellite	Input	System FDE	GNSS-EGNOS Receiver

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
GPS Code & Phase Pseudo ranges	Raw & filtered Code & Phase Pseudo range per GPS satellite	Input	System FDE	GNSS-EGNOS Receiver
Galileo Doppler (range-rate)	Raw & filtered Doppler (range-rate) per Galileo satellite	Input	System FDE	GNSS-EGNOS Receiver
GPS Doppler (range-rate)	Raw & filtered Doppler (range-rate) per GPS satellite	Input	System FDE	GNSS-EGNOS Receiver
Galileo Navigation Data	Augmented & safe Navigation Data (Ephemeris, Clock …) per Galileo satellite	Input	System FDE	GNSS-EGNOS Receiver
GPS Navigation Data	Augmented & safe Navigation Data (Ephemeris, Clock …) per GPS satellite	Input	System FDE	GNSS-EGNOS Receiver
SBAS bounding data	Bounding information from SBAS navigation message	Input	System FDE	GNSS-EGNOS Receiver

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
Acceleration	Safe & filtered IMU 3D Acceleration Measurements after sensor FDE	Input	System FDE	GNSS-EGNOS Receiver
Angular Rate	Safe & filtered IMU 3D Angular Rate Measurements after sensor FDE	Input	System FDE	GNSS-EGNOS Receiver
Speed Data	(Safe TBC) filtered Speed Data after sensor FDE	Input	System FDE	GNSS-EGNOS Receiver
Galileo Code & Phase Pseudo ranges	Raw & filtered Code & Phase Pseudo range per Galileo satellite	Output	Navigation Engine and Integrity Engine	System FDE
GPS Code & Phase Pseudo ranges	Raw & filtered Code & Phase Pseudo range per GPS satellite	Output	Navigation Engine and Integrity Engine	System FDE
Galileo Doppler (range-rate)	Raw Doppler (range-rate)per Galileo satellite	Output	Navigation Engine and Integrity Engine	System FDE

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
GPS Doppler (range-rate)	Raw Doppler (range-rate) per GPS satellite	Output	Navigation Engine and Integrity Engine	System FDE
Galileo Navigation Data	Augmented & safe Navigation Data (Ephemeris, Clock …) per Galileo satellite	Output	Navigation Engine and Integrity Engine	System FDE
GPS Navigation Data	Augmented & safe Navigation Data (Ephemeris, Clock …) per GPS satellite	Output	Navigation Engine and Integrity Engine	System FDE
Acceleration	Safe & filtered IMU 3D Acceleration Measurements after system FDE	Output	Navigation Engine and Integrity Engine	System FDE
Angular Rate	Safe & filtered IMU 3D Angular Rate Measurements after system FDE	Output	Navigation Engine and Integrity Engine	System FDE
Speed Data	(Safe TBC) filtered Speed Data after system FDE	Output	Navigation Engine and Integrity Engine	System FDE

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
Detection Capacities	Minimum Detectable Bias provided by the FDE to Confidence interval	Output	Navigation Engine and Integrity Engine	System FDE

Table 4: List of System data FDE function input and output

Note: D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version). As we are at the end of the project, "To Be Confirmed" (TBC) elements shall be properly justified and addressed. "TBC" can be addressed in the release version of D4.1 or in further study (e.g. CLUG 3.0 project).

3.3.2 LOC-OB Initialisation (LOC_OB INIT)

LOC-OB INIT is used to describe the Initialisation phase of the LOC-OB subsystem. Start of Mission is an ETCS procedure which is not related to the LOC-OB Initialisation phase. LOC-OB INIT defines the LOC-OB initialisation which occurs when the LOC-OB is powered on. After its initialisation phase, LOC-OB shall provide the processed data (1D position, 1D speed etc) whatever is the ETCS mode. If the LOC-OB cannot process one type of data (for example position), it still must provide the other processed data. In this case, the LOC-OB cannot be considered fully available, but the train can still be operated is some ETCS modes (Staff Responsible if speed is available but not the position for instance). To be noticed that the LOC-OB has no access to the ETCS mode.

There are two types of Initialisation LOC-OB:

- Initialisation with saved data.
- Initialisation without saved data.

The details are described in subchapters.

3.3.2.1 Initialisation with saved data

"Initialisation with saved data" is defined as a LOC-OB INIT which relies **on recorded data.** This initialisation is possible only if the train is equipped with a Cold Movement Detector.

Indeed, when the train is powered off, the context of INIT is saved. On the next power on, if the CMD indicates that no movement was detected awhile the train was powered off, the LOC-OB INIT can take benefit of the saved context.

3.3.2.2 Initialisation without saved data

"Initialisation without saved data" is defined as a LOC-OB INIT with **no recorded data**. If the train is not equipped with a Cold Movement Detector or if a cold movement is detected, then the localisation algorithms can only rely on the data provided by each available sensor. In this case, processing the localisation data is dependent on the sensors and some of them may not be ready directly after being powered on (GNSS or IMU for example).

3.3.2.3 Limitation of available data

There is limitation of possibly available sensors in the LOC-OB System. To initialise LOC-OB, the initial train position and initial track edge ID are needed as inputs. There is no issue to initialise LOC-OB with saved data approach which mean the CMD data is available. However, there is the issue to initialise LOC-OB without saved data. The issue is GNSS and IMU cannot provide the initial track edge ID and train position when the train is powered on.

To initialise LOC-OB from scratch (without saved data), it seems not possible without the intervention of the driver to drive the train to pass the balises to get initial position.

The overview of Initialisation methods available to the sensor fusion algorithm includes several approaches. Some options are marked in yellow because, although feasible, they present some critical issues.

	POSITION	VELOCITY	HEADING	ROLL & PITCH	TRACKEDGE_ID
GNSS single antenna	YES	YES	YES	NO	NO (multi track) /Yes (mono track or distanced track)
GNSS double antenna	YES	YES	YES	NO	NO multi track) /Yes (mono track or distanced track)
IMU	NO	NO	YES	YES	NO
Speed sensor	NO	YES	NO	NO	NO
Magnetometer	NO	NO	YES	NO	NO
Balises	YES	NO	YES	NO	YES
CMD	YES	YES	YES	YES	YES
Digital Map	YES	NO	NO	NO	YES

Table 5: Sensor Overview of Initializtation method available (extract from D4.9 [14][3])

RED	The sensor cannot provide outputs to estimate the parameter.
YELLOW	The sensor can't provide outputs / valuable outputs under given circumstances.
GREEN	The sensor can provide outputs to estimate the parameter.

The detail of sensor overview of Initialisation function can be explained as following:

GNSS single antenna and double antenna

GNSS is widely adopted as an Initialisation tool for the user position and velocity. Such estimated position, however, would not have the accuracy level required to determine the *TrackEdge_ID* currently occupied. In fact, especially in environments like train stations, the tracks are densely packed and the accuracy of the GNSS solution would be affected by local effects like multipath and or RF interferences. It is also well known that GNSS alone cannot provide the computation of roll and pitch. With single antenna GNSS the heading can be computed based on the estimated velocity, under the assumption that the vehicle is travelling in the vehicle forward direction. However, this method would not allow estimating the heading at standstill or low velocity. On the other side, this problem could be fixed with dual antenna- For the scope of CLUG, however, GNSS visibility is not always guaranteed

during the Initialisation, which then represents a big limitation for the GNSS-based Initialisation. For this reason, the GNSS entries in the **Table 5** above are marked in yellow.

IMU

IMU can be used at standstill to initialize the roll and pitch of the sensor fusion and, depending on the IMU grade, also to initialize the heading. The performance of the Initialisation, especially for the heading, are strongly dependent on the IMU grade and, therefore, on the IMU cost.

Speed sensors

Speed sensors can provide the speed in the vehicle reference frame. However, in order to compute the velocity in the navigation reference frame, the orientation state components must be all known.

Magnetometers

Magnetometers could potentially provide the heading Initialisation, but this solution is marked as critical because it would be impossible to prevent local disturbances of the magnetic field within the train environment.

Balises

Besides GNSS, balises are the only input that can guarantee absolute position information. Moreover, they could also ensure a safe Initialisation of the *TrackEdge_ID*. From the *TrackEdge_ID* and the position, also the heading could be computed thanks to the digital map.

Their main limitation is only represented by the maintenance cost. However, it should be also taken into account that, for such an Initialisation, the first balise must be reached and therefore a certain degraded operation mode must be foreseen. In such operation, the train would move towards the first balise without the sensor fusion algorithm being initialized.

CMD - A priori info

A priori information about the latest train status prior to switch-off could be provided to the sensor fusion algorithm, if the CMD module does not report the occurrence of motion since the last switch-off. This would allow initializing all the necessary quantities but the velocity. However, since this kind of Initialisation is done at standstill the velocity can be obviously initialized to zero.

More detail can be found in CLUG 2.0 D4.9 Start of Mission Preliminary Definition (LOC-OB INIT) [14].

3.3.2.4 Interface Specification

The interface input and output of LOC-OB INIT are given in **Table 6** :

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
LOC-OB internal Time	Absolute time in GPS and/or Galileo and/or UTC, enslaved to GPS and/or Galileo reference system time	Input	LOC-OB Initialisation function	GNSS-EGNOS Receiver
Cold Movement Detector – Standstill status	Safe CMD confirmation that there was no movement since the last train power off. The detection threshold is set to +/- 2m TBC[1] that has to be added in the initial +/- 1/2 CI in along track position. Note in along track Speed and Acceleration, initial CI should not be enlarged by the CMD confirming the train is in standstill.	Input	LOC-OB Initialisation function	CMD
Galileo Code & Phase Pseudoranges	Raw & filtered Pseudorange Code & Phase Pseudorange per Galileo satellite	Input	LOC-OB Initialisation function	GNSS FDE EGNOS
GPS Code & Phase Pseudoranges	Raw & filtered Pseudorange Code & Phase per GPS satellite	Input	LOC-OB Initialisation function	GNSS FDE EGNOS
Galileo Doppler (range- rate)	Raw & filtered Doppler (range-rate) per Galileo satellite	Input	LOC-OB Initialisation function	GNSS FDE
GPS Doppler (range-rate)	Raw & filtered Doppler (range-rate) per GPS satellite	Input	LOC-OB Initialisation function	GNSS FDE

[1] 2m is the current value proposed in ERJU/R2DATO/WP21 specifications.

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
Galileo Navigation Data	Augmented & safe Navigation Data (Ephemeris, Clock …) per Galileo satellite	Input	LOC-OB Initialisation function	GNSS FDE
GPS Navigation Data	Augmented & safe Navigation Data (Ephemeris, Clock …) per GPS satellite	Input	LOC-OB Initialisation function	GNSS FDE
Angular Rate	Safe and Filtered IMU 3D Angular Rate Measurements after system FDE	Input	LOC-OB Initialisation function	IMU FDE
Digital Map	Safe Digital map layer information	Input	LOC-OB Initialisation function	Digital Map
Initial Track Edge ID	Safe Initial Track Edge ID where the train is	Output	Track Selectivity function Along Track Localisation function	LOC-OB Initialisation function
Initial Along track Position	Safe Initial Along track Position	Output	Along Track Localisation function	LOC-OB Initialisation function
Initial Heading	Initial estimated Heading of the Train Unit with respect to the North direction	Output	Along Track Localisation function	LOC-OB Initialisation function
Initial Attitude	Estimated Initial Yaw, Pitch and Roll angles	Output	Along Track Localisation function	LOC-OB Initialisation function

Table 6: List of Initialisation function input and output

Note: D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version). As we are at the end of the project, “To Be Confirmed" (TBC) elements shall be properly justified and addressed. “TBC” can be addressed in the release version of D4.1 or in further study (e.g. CLUG 3.0 project).

3.3.3 Track Selectivity Function

Track Selectivity is the function dedicated to determine in real time on which track id the train is after crossing a switch point. It remains valid to detect track edge changes too. The track id and its confidence status versus time/distance is outputted to the along track algorithm and the integrity algorithm It needs safe and filtered inputs from sensors and digital map.

3.3.3.1 Overall architecture for Track Selectivity Function

The overall architecture of the TSD function is illustrated on the **Figure 7**:

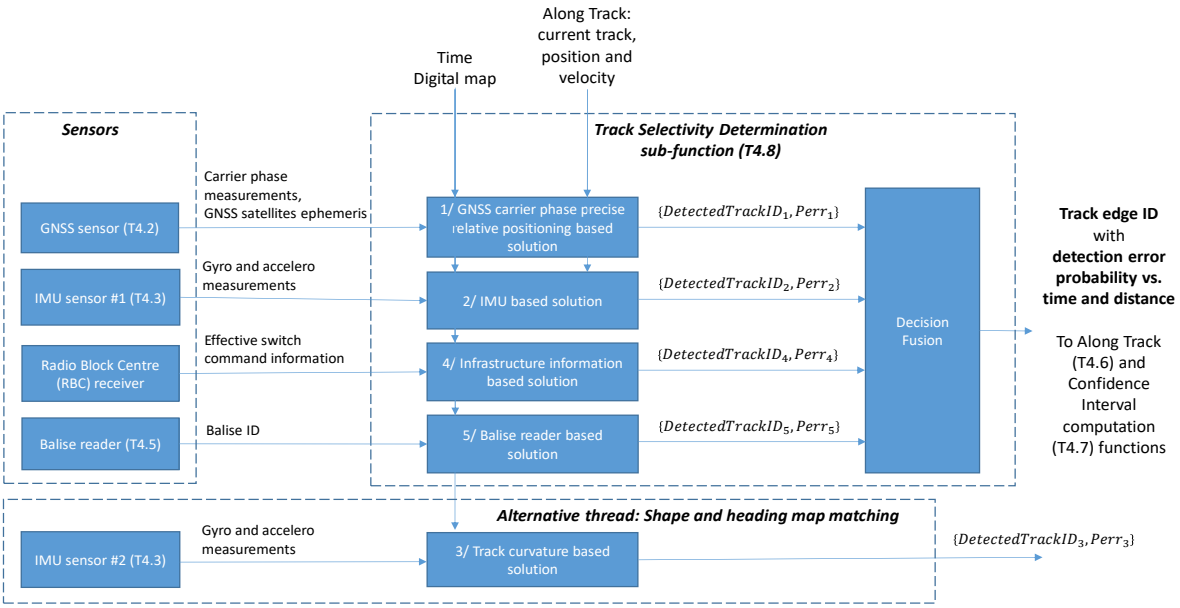


Figure 7: Overall architecture of the Track Selectivity Determination sub-function (extract from D4.8 [13])

It consists in a modular architecture of a set of Unitary Solutions. Each Unitary solution implements independent algorithms which are running in parallel. Each algorithm uses independent measurements provided by non-coupled sensors. Each sensor provides independent information with associated integrity metrics to a Decision Fusion algorithm, which is in charge to provide a decision regarding the most probable track edge ID the train is located after crossing any switch. Such detected track edge ID is given with an error probability which results from each detector algorithm and uncertainties on measurements and on the Digital Map. With this approach, independent decisions and associated probabilities of error are computed by each unitary solutions resulting in globally reducing the probability of error at the output of the Decision Fusion.

The following five independent Unitary Solutions are listed:

- Unitary Solution 1: GNSS carrier phase measurements-based positioning solution
- Unitary Solution 2: IMU-based relative positioning solution
- Unitary Solution 3: Track curvature-based solution

- Unitary Solution 4: Infra information-based solution (switch command info shared from Infra to On-Board)
- Unitary Solution 5: Balise reader

The baseline of Unitary Solution 1 consists in estimating precisely the GNSS antenna trajectory and to compare it with the possible tracks to decide which one is the most likely.

When arriving close to a switch, precise trajectory of the train is computed from safe and filtered GNSS carrier phase measurements, relatively to an initial position being provided by the Along Track function. Such trajectory is then compared with all possible tracks being present at the output of the switch using likelihood metrics accumulated all estimated train trajectory information since the switch position, as they are updated each time a new train position is computed. All possible tracks after the switch are characterized by a set of mono-track maps built from relevant information from the Digital Map description files and specified by a set of waypoints. Then, the most probable currently travelled track is selected and is provided at each new epoch (1 to 5Hz measurement rate is suggested) under the form of the Track Edge ID as referred into the Digital Map database, with its corresponding probability of error. The algorithm is complete when the probability of error is below a given acceptable value.

For Unitary 2 - the solution consists in performing track selection by comparing train trajectory estimates based on a IMU navigation algorithm with possible track options coming from the provided Digital Map of the area of operation. The selection of the track is performed by looking for the best likelihood between the computed trajectory and all possible mono-track options available after the switch. This is performed the same manner it was previously described for the Unitary Solution 1 implementing positioning based on GNSS carrier phase measurements.

Please note that mainly the Unitary Solutions 1 and 2 are deeply worked for prototyping in CLUG 2.0 WP5, meaning that algorithm detailed design activities are mainly focused on these two unitary solutions.

Note: The unitary solutions 1, 2, 4 and 5 are analysed in this analysis. However, due to insufficient information, Unitary Solution 3 could not be included in the analysis.

More detail can be found in CLUG 2.0 D4.8 Track Selectivity [13].

3.3.3.2 Interface Specification

The interface input and output of Track Selectivity function [13] are given in:

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
LOC-OB internal Time	Current LOC-OB system time	Input	Track Selectivity	GNSS-EGNOS Receiver
Galileo Carrier Phase Measurements	Raw Carrier Phase Measurement per Galileo satellite	Input	Track Selectivity	GNSS FDE
GPS Carrier Phase Measurements	Raw Carrier Phase Measurement per GPS satellite	Input	GNSS carrier phase measurements based unitary solution.	GNSS FDE
Galileo Satellite Positions	Galileo satellites current positions in the ECEF referential	Input	GNSS carrier phase measurements based unitary solution.	GNSS FDE
GPS Satellites Positions	Galileo satellites current positions in the ECEF referential	Input	GNSS carrier phase measurements based unitary solution.	GNSS FDE
Angular Rate	Filtered IMU 3D Angular Rate Measurements from gyroscope	Input	Track selectivity function Used by the IMU measurements based unitary solution.	IMU FDE
Acceleration	Filtered IMU 3D Acceleration Measurements from accelerometer	Input	Track selectivity function Used by the IMU measurements based unitary solution.	IMU FDE

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
Trigger	Informs the function to start the track determination as the train is close to a switch. This input is triggered by the Data Fusion algorithm	Input	Track selectivity function Used as a command input.	Along Track localisation function
Kalman Matrices State vector and Error Estimates Covariance	Internal quantities like IMU sensor biases, receiver clock error and clock error drift, speed sensor scale factors. The covariance matrices produced by the EKF for the position, velocity, acceleration, attitude, and such internal quantities are also provided.	Input	Track selectivity function Used by the IMU measurements based unitary solution (gyro and accelerometer bias estimates).	Kalman Matrixes
Digital Map	Digital map layer information	Input	Track selectivity function Used for map matching processes.	Digital Map
Balise Telegram (ID)	Balise Identifier	Input	Track selectivity function Used by the Balises based unitary solution.	Balise Reader
Effective switch command information	Effective switch command information received from the Radio Block Center (RBC)	Input	Track selectivity function Used by the infrastructure information based unitary solution.	Trackside

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
Initial TrackEdge_ID	Initial TrackEdge ID where the train is	Input	Track selectivity function Used to initialize the TSD function.	LOC-OB Initialisation function
Current TrackEdge ID with current position on track	Current TrackEdge ID with current position on track.	Input	Track selectivity function Used to re-initialize the TSD function when approaching a new switch. Such info is provided by the Along Track sub-function.	Along track localisation function
TrackEdge_ID	TrackEdge ID as defined in the Digital map	Output	Along Track Localisation function	Track Selectivity function
Confidence Status	Confidence Status provided as the THR associated with the TrackEdge ID versus time.	Output	Integrity function	Track Selectivity function

Table 7: List of Track selectivity function input and output

3.3.4 Along Track Localisation

The along track localisation provides estimation of the train states like Safe along track position, Safe along track velocity and Safe along track acceleration. This function based fusion algorithm to provide LOC-OB outputs in real time main functions.

Sensor fusion processes independently all the measurements streams coming from the different sensors (after the Failure Detection and Exclusion stage). Therefore, each time a new measurement is available, the specific computation corresponding to sensor's measurement is launched and executed. Sensor fusion function can deal with asynchronous input measurements streams.

This function will compute other safe parameters:

- The TrackEdge ID based on Track Edge Determination function augmented, when available, through balise data.
- The safe direction of the Train Unit movement, Nominal, Reverse, Unknown versus digital map definition.
- Estimated Time stamp of each outputs every 200 ms in UTC time frame in milliseconds (using GNSS or SBAS system time in relation with UTC time).

In addition to these safe parameters, this function will compute non-safe parameters:

- Attitude angles and rates (Yaw, Pitch and roll rate) with associated standard deviations
- 3D position with associated standard deviations
- 3D velocity with associated standard deviations
- 3D acceleration with associated standard deviations

Internal Functions: Trigger Data who informs the Tack Edge Selectivity module to start the track determination as the train is close to a switch and also provides the Kalman matrixes to the selectivity module.

3.3.4.1 Along track localisation Algorithm

GNSS, IMU and wheel tachometers are the main on-board sensors in the along track train localisation function. Track map data is also necessary, although this represents a static information rather than sensor data. Finally, balise data are optional: these data can be provided to the EKF in order to improve the localisation accuracy, particularly in GNSS denied areas. However, the EKF can completely fulfil its function also not being exposed at all to any balise data.

The general idea of this sensor fusion concept is to process independently all the data streams coming from the different sensors. Therefore, each time a new measurement is available from a certain sensor, the specific operation corresponding to that sensor is launched and executed. Such operation consists in the implementation of the EKF update based on that specific sensor, which in turn is based on the mathematical relationship between the state vector of the EKF and the output of the sensor, i.e. in the measurement equation for that sensor.

With this logic, the sensor fusion system can deal with an input data stream that is completely asynchronous, with different sensor data independently deliver data for EKF processing. A qualitative scheme of the multi-rate data flow data can be handled by the EKF is depicted in the following picture.

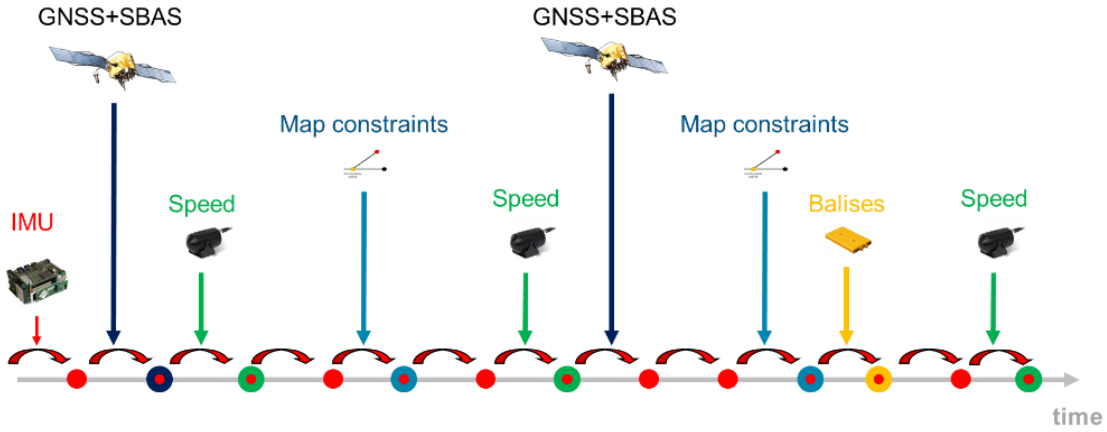


Figure 8: Interleaving of sampling times from different sensors (extract from D4.6 [15][11][3])

The EKF proposed in this section is represented by a tightly-coupled framework. This means that the raw measurements of the sensors are fused together in order to deliver a single PVT solution with an increased accuracy. More detail can be seen in CLUG 2.0- D4.1 LOC-OB functional architecture [11] and D4.6 Sensor fusion and system FDE [15].

3.3.4.2 List of Along track localisation input and output

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
LOC-OB internal time	Absolute time in GPS and/or Galileo and/or UTC, enslaved to GPS and/or Galileo reference system time	Input	Along Track Localisation	GNSS-EGNOS Receiver
Galileo Code & Phase Pseudoranges	Raw & filtered Pseudorange Code & Phase per Galileo satellite	Input	Along Track Localisation	GNSS FDE
GPS Code & Phase Pseudoranges	Raw & filtered Pseudorange Code & Phase per GPS satellite	Input	Along Track Localisation	GNSS FDE
Galileo Doppler (range rate)	Raw & filtered Doppler (range rate) per Galileo satellite	Input	Along Track Localisation	GNSS FDE
GPS Doppler (range-rate)	Raw & filtered Doppler (range-rate) per GPS satellite	Input	Along Track Localisation	GNSS FDE
Galileo Navigation Data	Augmented & Safe Navigation Data (Ephemeris, Clock …) per Galileo satellite	Input	Along Track Localisation	GNSS FDE
GPS Navigation Data	Augmented & safe Navigation Data (Ephemeris, Clock …) per GPS satellite	Input	Along Track Localisation	GNSS FDE
Acceleration	Safe & Filtered IMU 3D Acceleration Measurements after system FDE	Input	Along Track Localisation	System FDE
Angular Rate	Safe & Filtered IMU 3D Angular Rate Measurements after system FDE	Input	Along Track Localisation	System FDE
Speed Data	(Safe TBC) filtered Speed Data (Tachometer, Optical sensor, etc.) after system FDE	Input	Along Track Localisation	Speed FDE

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
Digital Map	Safe Digital map layer information	Input	Along Track Localisation	Digital Map
Balise ID	Safe Balise Identifier when available	Input	Along Track Localisation	Absolute Reference Point
TrackEdge_ID	After triggered, TrackEdge ID where the train front end is.	Input	Along Track Localisation	Track edge selectivity
Initial TrackEdge_ID	Initial TrackEdge ID where the train front end is	Input	Along Track Localisation	Initialisation function
Initial Along Track Position	Safe Initial along track position	Input	Along Track Localisation	Initialisation function
Initial Heading	Initial estimated Heading of the Train Unit with respect to the North direction	Input	Along Track Localisation	Initialisation function
Initial Attitude	Estimated Initial Yaw, Pitch and Roll angles	Input	Along Track Localisation	Initialisation function
Outputs used for LOC-OB internal usage				
Trigger	Informs the Track Selectivity function to start the track selectivity as the train is close to a switch.	Output	Track Selectivity	Along Track Localisation
All Kalman Matrixes	Fusion Algorithm EKF State Vector, error estimates covariance, geometry matrix, transition matrix, Kalman Gain	Output	Along Track Localisation	Kalman matrixes
Fusion Localisation Computed Time	Absolute time computed by the localisation function	Output	Protection level	Along Track Localisation
Safe Outputs for LOC-OB external usage and for LOC-OB internal usage				
Balise_ID	Reference ID of the balise (when available)	Output	SF-001 Provide Safe Train Front End 1D Position Dataset	Along Track Localisation
MapNode_ID	Reference ID of the start Track Node	Output	SF-001	Along Track Localisation

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
	(corresponding to last shunting) of TrackEdge ID		Provide Safe Train Front End 1D Position Dataset	
TrackEdge ID	TrackEdge ID where the train front end is	Output	SF-001 Provide Safe Train Front End 1D Position Dataset	Along Track Localisation
Estimated Safe Along-track position	Along-track estimated safe Distance on Track Edge from last digital map reference point (could be a balise, a start track node, a shunting…) of TrackEdge ID	Output	SF-001 Provide Safe Train Front End 1D Position Dataset	Along Track Localisation
Estimated Safe Along-track Speed	Along-track estimated safe Speed on Track Edge axis	Output	SF-002 Provide Safe Train Speed	Along Track Localisation
Estimated Safe Along-track Acceleration	Along-track estimated safe Acceleration on Track Edge axis	Output	SF-003 Provide Safe Train Acceleration	Along Track Localisation
Safe Direction	Nominal, Reverse, Unknown versus digital map definition	Output	SF-001 Provide Safe Train Front End 1D Position Dataset	Along Track Localisation
Estimated Timestamp	Estimated Time put as timestamp of each outputs every 200ms, in UTC time frame in milliseconds (YYYY-MM-DD hh:mm:ss.sss).	Output	All SF	Along Track Localisation
Non Safe Outputs for LOC-OB external usage and for LOC-OB internal usage				
3D FE Position	3D estimated position in WGS84 and its associated 3σ standard deviation	Output	SF-004 Provide 3D Position and Uncertainty	Along Track Localisation

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
3D Velocity	3D estimated Velocity and its associated 3σ standard deviation	Output	SF-005 Provide 3D Velocity and Uncertainty	Along Track Localisation
3D Acceleration	3D estimated acceleration and its associated 3σ standard deviation	Output	SF-006 Provide 3D Acceleration and Uncertainty	Along Track Localisation
Attitude	Estimated Yaw, Pitch and Roll angles and its 3σ associated standard deviations	Output	SF-007 Provide 3D Attitude (Rotational Angles) and Uncertainty	Along Track Localisation
Attitude Rates	Estimated Yaw, Pitch and Roll rates and 3σ associated standard deviations	Output	SF-007 Provide 3D Attitude (Rotational Angles) and Uncertainty	Along Track Localisation
Direction	Nominal, Reverse, Unknown	Output	SF-001 SF-001 Provide Safe Train Front End 1D Position Dataset	Along Track Localisation
Estimated Timestamp	Timestamp of the Non Safe outputs in UTC time frame	Output	All non-safe SF	Along Track Localisation

Table 8: Inputs and Outputs of the Along track localisation function

Note: D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version). As we are at the end of the project, "To Be Confirmed" (TBC) elements shall be properly justified and addressed. "TBC" can be addressed in the release version of D4.1 or in further study (e.g. CLUG 3.0 project).

3.3.5 Integrity Function

The goal of integrity monitoring is to ensure that the probability of undetected errors exceeding the safe bounds is sufficiently low to achieve the Tolerable Functional Failure Rate (TFFR) assigned. This is achieved through a combination of monitors (Fault Detection and Exclusion metrics) and the computation of protection levels (PL) used to determine the confidence intervals bounding errors at the output of the EKF-based localisation algorithm up to the required probability.

This function computes the position / speed / acceleration safe confidence intervals ensuring at a certain THR the real train kinematic (pos./speed/acc.) are inside those computed CIs.

Note: contrary to aviation domain, there are no alerts neither time to alert required by the rail users.

The two main PVT techniques that can be considered for localisation are:

(1) Snapshot, where GNSS measurements corrected by SBAS are used in stand-alone to estimate the navigation solution. The WLS is the estimation technique typically used by the navigation users.

(2) Sensor fusion, where GNSS is integrated with other sensor measurements, such as tachometer or IMU. In this case, the EKF is used as estimation technique, enabling to improve PVT performances with respect to the use of individual sensors.

Although recursive estimation implies additional challenges with respect to snapshot methods, the multisensory approach is necessary to achieve improved localisation performances. Therefore, the tightly-coupled EKF is selected as the core navigation algorithm of the LOC-OB.

The input of the Navigation Engine consists in GNSS measurements augmented by EGNOS, IMU data, wheel tachometer data and track map information. All measurements data is first filtered through integrity barriers, consisting in Fault Detection and Exclusion (FDE) algorithms.

All measurements data is first filtered through integrity barriers, consisting in 2 Fault Detection and Exclusion (FDE) algorithms as mentioned in section 4.3. Two types of FDE can be distinguished:

(1) Data FDE acting at sensor level to detect and flag data, which is not compliant with sensor specifications, and

(2) System-FDE based on information from the sensor fusion localisation algorithm, which aims to detect and filter faulty sensor data induced by external feared events.

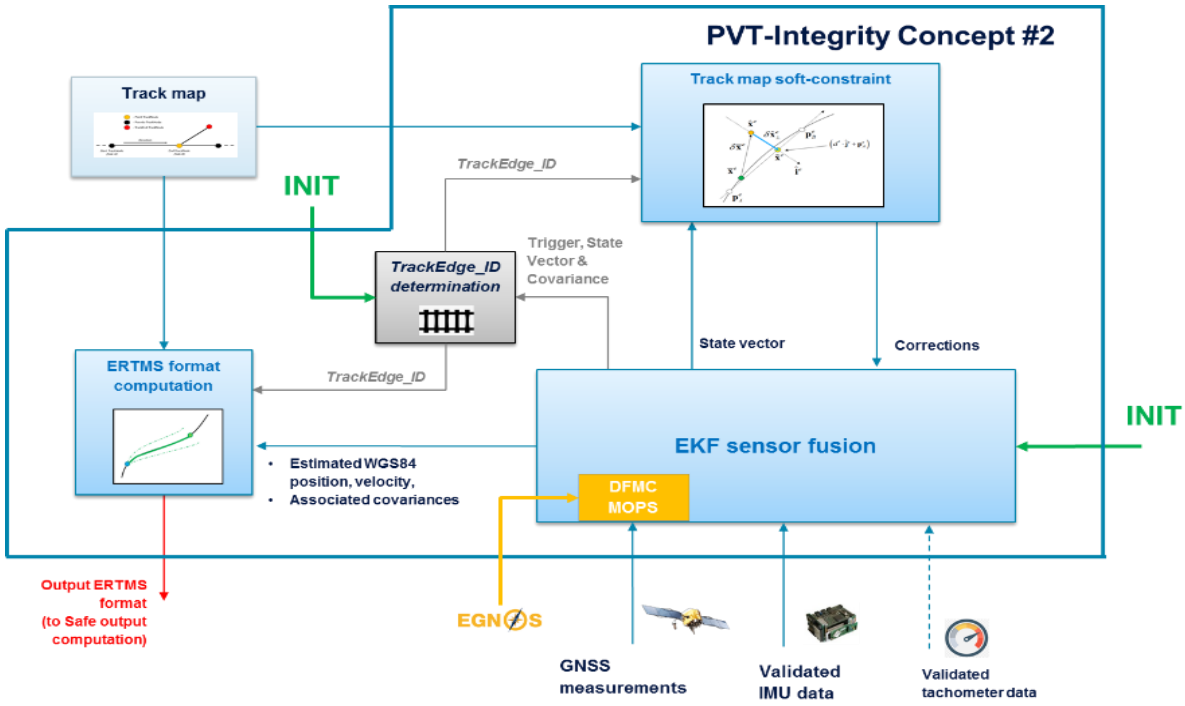


Figure 9: Architecture of the PVT block of the LOC-OB (extract from D4.7 [16][15][3])

More detail can be found in CLUG 2.0 – D4.6 Confidence Intervals Computation and Integrity Algorithm [16].

3.3.5.1 Allocation Integrity requirements

The Integrity function of the LOC-OB is intended to compute safely the Confidence Interval for both the along track position, speed and acceleration of the front-end (head) of the train. All functions providing 1D data must be implemented with a SIL4 safety level which corresponds to an integrity risk of 10^{-9}/h.

3.3.5.2 Inputs/Outputs of Integrity function

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
LOC-OB internal Time	Absolute time in GPS and/or Galileo and/or UTC, enslaved to GPS and/or Galileo reference system time	Input	Integrity function	GNSS_EGNOS Data Module
Fusion Localisation Computed Time	Absolute time computed by the localisation function	Input	Integrity function	Along Track Localisation
Detection Capacities	Minimum Detectable Bias provided by the FDE to Confidence interval	Input	Integrity function	Fault Detection and Exclusion
All Kalman Matrixes	Fusion Algorithm EKF State Vector, error estimates covariance, geometry matrix, transition matrix, Kalman Gain	Input	Integrity function	Along Track Localisation
TrackEdge ID (TBC)	TrackEdge ID where the train front end is	Input	Integrity function	Along Track Localisation
Safe Underestimation of the estimated distance	Safe Underestimation of the estimated distance of the train Front End (relative value to be added to the estimated one)	Output	Integrity function	GNSS_EGNOS Data Module
Safe Overestimation of the estimated distance	Safe Overestimation of the estimated distance of the train Front End (relative value to be added to the estimated one)	Output	SF-001 Provide Safe Train Front End 1D Position Dataset	Data Bounding
Maximum Safe Along-track FE position	Maximum Safe Front End on Position domain	Output	SF-001 Provide Safe Train Front End 1D Position Dataset	Data Bounding
Safe Underestimation of the estimated Speed	Safe Underestimation of the estimated speed of	Output	SF-002	Data Bounding

NAME	DATA DESCRIPTION	IN/OUT	CONSUMERS	PROVIDER
	the train Front End (relative value to be added to the estimated one)		Provide Safe Train Speed	
Safe Overestimation of the estimated Speed	Safe Overestimation of the estimated speed of the train Front End (relative value to be added to the estimated one)	Output	SF-002 Provide Safe Train Speed	Data Bounding
Safe Underestimation of the estimated Acceleration	Safe Underestimation of the estimated acceleration of the train Front End (relative value to be added to the estimated one)	Output	SF-003 Provide Safe Train Acceleration	Data Bounding
Safe Overestimation of the estimated Acceleration	Safe Overestimation of the estimated acceleration of the train Front End (relative value to be added to the estimated one)	Output	SF-003 Provide Safe Train Acceleration	Data Bounding
TrackEdge ID (TBC)	TrackEdge ID where the train front end is	Output	SF-001 Provide Safe Train Front End 1D Position Dataset	Data Bounding
Estimated Time Error	Estimated time error impacting {position, speed, and acceleration}	Output	All SF	Data Bounding

Table 9: Inputs and Outputs of the Integrity function

More information can be found in D4.1 LOC-OB Functiional Architecture [11].

Note: D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version). As we are at the end of the project, "To Be Confirmed" (TBC) elements shall be properly justified and addressed. "TBC" can be addressed in the release version of D4.1 or in further study (e.g. CLUG 3.0 project).

3.4 System of Interest of the current analysis and assumptions

The system of interest used in this analysis is from chapter 3.3 , the following assumptions have been set to perform the internal LOC-OB System Functional Safety Analysis.

NO	ASSUMPTION	REFERENCE
ASS-01	Point position information from track side is used as the input for the Track selectivity function. This information is assumed as SIL 4 input.	D4.8 Track Selectivity [13] D2.2 Attachment Appendix A [2] Justification from D2.2 - R
ASS-02	Cold Movement Detection data is available as the input of LOC-OB INIT. Cold Movement Detection is assumed as SIL 4 input.	D4.9 LOC-OB INIT [14] Justification from D2.2 - R
ASS-03	Balise Data is assumed as SIL4 input.	D4.5 Balise Reader Sensor [19] D4.1 LOC-OB Functional Architecture [11]
ASS-04	Balise data is used where GNSS-EGNOS signal is not available, for example, in harsh environment (tunnels, in mountain, under the bridge etc.).	D4.1 LOC-OB Functional Architecture [11] Justification from D2.2[2] - C, R
ASS-05	Balise data is used as the input for LOC-OB Initialisation function.	D4.9 LOC-OB INIT [14]
ASS-06	Balise data is used for track selectivity function.	D4.8 Track Selectivity [13] Justification from D2.2 - C, C
ASS-07	Digital Map is assumed as SIL4.	D4.1 LOC-OB Functional Architecture [11]
ASS-08	The MTBF and failure rates of the hardware (for tachometer, doppler radar and optical sensors) are taken from the demonstrator [33] and used in Fault Tree Analysis.	CLUG2_DATA-FORMAT-DEFINITION [33]
ASS-09	There are two types of IMU used in the analysis. The first is IMU DAL B level which has a low MTBF value (Honeywell 1700 - 2000 hours) and the second is IMU DAL A level (Northrop-Grumman LN200 (FOG)-20000 hours) which has a higher MTBF than IMU DAL B.	D4.1 LOC-OB Functional Architecture [11]

NO	ASSUMPTION	REFERENCE
ASS-10	GNSS-EGNOS Receiver from Syntony is used.	D4.2 GNSS Receiver [12]
ASS-11	Safety Design justification from D4.1 [11] is used in FTA. There is 1 solution analysed in this analysis. A solution providing two independent chains (shape and heading map matching- 2 IMUs DAL B level).	D4.1 LOC-OB Functional Architecture [11]
ASS-12	The separate hardware for chain 1 and chain 2 is proposed. The failure rate of each hardware is assumed as 1 E-05 per hour. • Chain 1 hardware executes system FDE, fusion algorithm, navigation engine, integrity engine. • Chain 2 hardware executes shape and heading map matching. Note: If a single hardware component were used for all functions, it would need to meet a highly stringent failure rate of 1E-09 per hour. This is a reason that we propose to implement separate hardware, enhancing system reliability and optimization.	Due to lack of detailed information regarding the hardware processing of the fusion algorithm, system FDE, navigation engine, integrity engine and shape and heading map matching. So, we assume this hardware will execute all these functions.
ASS-13	Combiner hardware is assumed the failure rate as 1E-09 per hour.	Due to lack of detailed information regarding the Combiner, so we assume this hardware to execute Combiner function.
ASS-14	Route information is assumed as SIL 4 data.	Based on D4.1 [11], Route information from infrastructure is needed for Shape and Heading Map matching.

Table 10: List of Assumption

Note: D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version).

4 HARDWARE REFERENCE

Since the hardware system architecture out of scope for CLUG 2.0, it was decided for the second part of this document to base the analysis on the configuration of the project's test train. Each test train is equipped with identical sensors. Therefore, ASS-08, ASS-09, ASS-10 are used.

It is currently planned to use the following sensors for data collection. The potential hardware of LOC-OB system is listed in the Table 11. Mean Time Between Failure and Failure rate that used for the demonstrator in Work package 5 [33] and IMU COTS candidate proposed in D4.1 [11] are used in the analysis.

The failure rate of each hardware component is used to calculate the THR and TFFR in the fault tree analysis.

Therefore, the number in Table 11 below shall be understood as assumptions.

COMPONENT	PRODUCT / MODEL	MTBF DATA (HOURS)	FAILURE RATE (FR) (LAMBDA (λ) = 1/MTBF)	ASSUMPTION
GNSS-EGNOS Receiver	Syntony	66,365	1.507E-05	This product is taken from D4.2
IMU safety critical (DAL B level)	HG 1700	2,000	5E-04	This product is taken from D4.1
IMU safety catastrophic (DAL A level)	Northrop-Grumman LN200 (FOG)	20,000	5E-05	This product is taken from D4.1
Tachometer	Odometer board (ODO5)	784,020	1.28E-06	This product is taken from test train (WP5)
Doppler Radar	DOP Rail 1000	400,000	2.50E-06	This product is taken from test train (WP5)
Doppler Radar	DRS05/03 Deuta	205,000	4.88E-06	This product is taken from test train (WP5)
Optical Sensor	CorRail2000	500,000	2.00E-06	This product is taken from test train (WP5)

Table 11: Failure rate of LOC-OB component

Note: D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version).

Important to note: In aviation, Design Assurance Level (DAL) refers to the classification used in safety-critical systems to determine the rigor and level of assurance required in the design, testing and certification of software and hardware. DAL is not exactly equivalent to Safety Integrity Level (SIL) used in railway system because they use different standards and criteria for achieving safety.

For the following analyses, our focus is primarily on the Mean Time Between Failure (MTBF) and Failure rates for each IMU Model. Therefore, for IMU of safety critical level, the MTBF values of an IMU safety critical (DAL B) has been used (HG 1700), and for IMU of safety catastrophic level, the MTBF values of an IMU safety catastrophic (DAL A) has been used (LN200).

5 SYSTEM FUNCTIONAL SAFETY ANALYSIS

The System Functional Safety Analysis follows the principle of risk assessment process. The objective is to identify the causes of Navigation Core functional failures. Therefore, the focus is on the logical functions and consider the impact of the input functions, given by the system functional architecture (LOC-OB INIT function, Track selectivity function, Along track localization function, Integrity function, System Data FDE). Finally, the effects of these failures on subsystem and system operability are considered.

5.1 Method

The System Functional Safety Analysis is based on Failure Mode and Effect Analysis technique. Failure Modes and Effect Analysis is a systematic procedure for the analysis of a system to identify the potential failure modes, their causes and effects on system performance. It is presented in the form of a column table, the formalism of which, is outlined below.

COLUMN	DECRIPTION	EXPLANATION
Column A	ID	The numbering of the line
Column B	Logical function	The logical function name considered in the analysis
Column C	Operational Scenarios	The operational scenarios on the train operation, only Start of mission and perform mission are considered in this analysis
Column D	Input	All inputs need for the logical function
Column E	Output	Outputs of the logical function
Column F	Failure Mode	The failure mode of the input for each Logical function we aim to analyse. The failure modes are as follows: • Omission: the input is missing • Incorrect: the input is incorrect
Column G	Failure Description	The description of the failure
Column H	Potential Cause	The possible cause that can lead to the logical function failure mode
Column I	Initial Effect	Initial effects of the occurrence of the failure mode on the logical function
Column J	Effect on subsystem	Effect of the logical function failure on LOC-OB Subsystem
Column K	Effect on system operability	Effect of logical function failure on overall system operation

COLUMN	DECRIPTION	EXPLANATION
Column L	Impact Safety	Impact to safety, yes or no
Column M	Failure detection	The way to detect the failure
Column N	RAMS Requirement	Link to RAMS requirements
Column O	Link to Hazard ID	Link to Hazard ID identified in D3.2 PHA

Table 12: Format of System Functional Safety Analysis

5.2 The analysis

See the table of the analysis in Appendix A.

5.3 Result of the analysis

According to the System Functional Analysis results, potential failure modes, their causes, and effects on local subsystem, and system operations have been identified, and traceability with PHA has been established. Mitigations were only partially defined at this step due to incomplete information from the design. The Failure Detection and Exclusion (FDE) for each sensor is still unclear regarding the concept that will be used, for example, the detection and negation time (the maximum total time to detect and react in a safe way to all single faults affecting the safe operation) . Additionally, there is column M for failure detection based on the available information, such as FDE and System Data FDE, but it is remain incompleted due to the lack of sufficient information.

Generally, mitigation strategies should be brainstormed by design engineers and safety engineers, and this should be done in a further step. From the current perspective, the design of the LOC-OB should incorporate Composite Fail-safety for instance 2 out of 2 configuration (refer to EN 50129 – B.3) to meet SIL 4 requirements.

Sensor Fault Detection Exclusion and System Fault Detection Exclusion :

The analysis in 6.2 shows that the incorrect failure mode of GNSS-EGNOS, IMU and the Failure effects on LOC-OB (Column J) can be mitigated by Sensor FDE and System FDE. A simple example is the situation described in SFSA-14, where incorrect GNSS-EGNOS data lead to a wrong train position and in worst case cause the provision of Movement Authorities based on the incorrect position. Another example is described in SFSA-16, where incorrect IMU Data have the potential to lead to the same operational impact as in SFSA-14. A sensor FDE and System FDE excluding erroneous GNSS-EGNOS and IMU failures safely would be needed to reduce the risk of the appearance of the system operational impact (column K) mentioned in SFSA-14 and SFSA-16 and to get rid of balises for parting track in open sky conditions.

Additionally, these FDE measures could mitigate risks in SFSA-02, SFSA-08, SFSA-10, SFSA-08, SFSA-24, SFSA-26, SFSA-28, SFSA-36, SFSA-38, and SFSA-40.

Track Selectivity Function:

Besides the FMEA analysis from D4.8, the Track Selectivity design indicates that when two switches are positioned close together, GNSS-IMU cannot provide the track edge ID after the train pass the first switch, they will provide the track edge ID after the train crosses the second switch. This highlights the necessity of obtaining point position from infrastructure as an input. The reception of SIL 4-point position information from the trackside is highly recommended, in all the environmental conditions. This is also align with the proposal from D2.2 to consider the point positon for track selectivity function refer to chapter 2.2 - C, R SpecSysReq[001] and SpecSysReq[070]. Based on the analysis, this recommendation R07 considered as a safety requirement **RA-RAMS-34**

The need for the specified SIL 4 input was derived by SFSA-19 and SFSA-20. As a consequence, the requirement RA-RAMS-29 is a result of this analysis. The interface needs to be defined for how to get point position information to LOC-OB system. The point position information can either be sent directly to LOC-OB or LOC-OB can receive the point position from ETCS-OB.

For parting track topology in harsh environments, the challenge is to ensure the Safe Train Front end is correctly determined by IMU and speed sensor without GNSS-EGNOS, further investigation is needed. Depending on the performance to be analysed in WP 5, if the track selectivity function using the point position as the input does not show the right performance, the balises may be required to be installed on parting track in harsh environments. The distance between the balises and the switches must be carefully considered to maintain system reliability and safety refer to D2.2 [2].

LOC-OB Initialisation function :

For the LOC-OB Initialisation function without saved data (NO CMD), when the train powers on (transitioning from NP to SB mode), the driver must enter Staff Responsible mode to drive the train to pass two consecutive balises so the LOC-OB can be initialized. However, driving by line of sight may be hazardous, indicating that balises are essential for LOC-OB Initialisation. For the LOC-OB Initialisation function with saved data (CMD), if the CMD detect train movement during power off or sleep mode is more than 2 m then the LOC-OB cannot initialise at standstill.

Consequently, the requirements **RA-RAMS-27**, **RA-RAMS-28** and **RA-RAMS-30** were defined as an outcome of theis analysis.

Effect to System Operation :

If the LOC-OB cannot determine the position, the ETCS-OB will not be able to provide a train position report, this could be hazardous, as the train would be running with an unknown position. This hazard should be escalated to the system integration level. Mitigation for this hazard should be addressed at the system level (e.g., Automatic Train Protection or Interlocking). From an operational viewpoint, if the LOC-OB cannot provide the train position within the defined time, the train should be delocalized, and either a service brake or an emergency brake should be applied to stop the train. The last train position report should be frozen. However, these actions are outside the scope of the LOC-OB system.

For the second chain using Shape and Heading Map Matching technique, with this technique the Route Information is required from Infrastructure. This input should be SIL4 data - **RA-RAMS-33**.

List of Safety Requirement issues from System Functional Safety Analysis

ID	SAFETY REQUIREMENTS	RATIONALE
RA-RAMS-27	Cold Movement Detection shall be installed for starting LOC-OB Initialisation process.	Refer to SFSA-05 related to Safety and D4.9 [14]. If no cold movement detection, the train cannot initialisation automatically. Human intervention needs to be involved in the initialisation process.
RA-RAMS-28	Cold Movement detection shall meet a TFFR of less than 1E-08 /h (SIL 4 input data to the LOC-OB).	Refer to SFSA-05 related to Safety. If this input is not SIL4, it can affect to LOC-OB System to achieve SIL4.
RA-RAMS-29	Point position information shall meet a TFFR of less than 1E-08 / h (SIL 4 input data to the LOC-OB).	Refer to C, RSFSA-19 and SFSA-20 related to Safety. It is one crucial input that can provide to track selectivity function to define track edge ID after crossing the switch because GNSS-EGNOS and IMU can provide track edge ID after passing two successive switch to ensure safe train movement.
RA-RAMS-30	If there is no CMD installed on the train, LOC-OB Initialisation function shall get initial train position from Balises.	Refer to SFSA-05 related to Safety and D4.9 [14]. If no initial train position from GNSS, fusion algorithm cannot start up. This is the reason why the train should get initial position from balises in order to start up fusion algorithm.

Table 13: List of new Safety Requirements after analysis

List of Safety Requirement issues from Design safety analysis in D2.2 [2], D4.1 [11], and D4.8 [13]

ID	SAFETY REQUIREMENTS	RATIONALE
RA-RAMS-31	Point position information shall be provided to track selectivity function.	Based on the test results from chapter 5 of D4.8 [13], the test results demonstrate that when two switches are positioned close to each other, the GNSS-EGNOS and IMU systems are unable to provide the track edge ID after passing the first switch. However, GNSS-IMU is able to provide the track edge ID after both switches have been crossed successfully. Therefore, the point position information from infrastructure is crucial input for the track selectivity function in determining the track edge ID after the train pass the first switch to ensure safe train movement.
RA-RAMS-32	The time or the distance when the Track Selectivity is determined after passing a point shall be limited.	Based on the recommendation from D2.2 [2] refer to chapter 2.2. Time to passing the switch is crucial because LOC-OB shall report track edge ID immediately to ensure the safe train movement. However, the design team should evaluate the time constraint.
RA-RAMS-33	For the second chain using Shape and Heading Map Matching technique, with this technique the Route Information is required from Infrastructure. This input should be SIL4 data (TFFR less than 1E-08 per hour).	Based on the new information from D4.1 v0.4 [11] and ASS-14, it is required Route information from infrastructure for the second chain using Shape and Heading Map Matching technique.
RA-RAMS-34	The position of the estFE should be reported as frequent as possible, but particularly at triggers. Triggers when positions should be reported can either be locations or events of the LOC-OB. A position should be reported when track nodes or any defined locations on the track are passed, following current ETCS procedures. A position report should also be triggered at certain events such as when Track Selectivity is established or lost, etc.	After analysing the recommendations in D2.2 [2], specifically concerning the point position for the track selectivity function (chapter 2.2 - C, R), we propose adding this recommendation as a safety requirement.

Table 14: List of new Safety Requirements from design safety analysis

Note: D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version).

The following list of safety requirements derived from D2.4 (see §3.2) [4] is confirmed as safety related after the analysis.

ID	SAFETY REQUIREMENTS	RATIONALE
SpecSysReq[027]	**RA-RAMS-35** LOC-OB, from the train power on, shall initialise itself and provide the outputs with no human supervision.	If we want to run train in GOA3 and GOA4 system, LOC-OB initialisation process should be done automatically.
SpecSysReq[028]	**RA-RAMS-36** After being powered up and its initialisation stage ended, LOC-OB shall provide data continuously.	Refer to SFSA, LOC-OB Initialisation function is related to safety. If LOC-OB does not provide data continuously to ETCS-OB then the system cannot detect train position and lead to hazard at the end.
SpecSysReq[002]	**RA-RAMS-37** LOC-OB shall provide the track edge ID where the train front end position is.	Refer to Track selectivity function (SFSA-13, SFSA-14, SFFSA-15, SFSA-16) are related to safety.
SpecSysReq[031]	**RA-RAMS-38** In case the LOC-OB cannot reach full operational capability after the system is powered on (e.g., Unknown track segment / track edge), estimated speed and travelled distance since the LOC-OB is powered on shall always be provided.	If the train does not receive estimated speed and travelled distance, the ETCS-OB is unable to calculate the braking curve, monitor speed, control speed effectively. As a result, the train cannot operate safely.

Table 15: List of Safety Requirements derived from D2.4 [4]

6 FAULT TREE ANALYSIS

6.1 General Fault Tree Methodology

FTA is a top-down method and generally employed to analyse the causes for a given fault state (top event) of a system. For the safety analyses (Wrong Side Failure Analysis (WSF)) described in this document, the Fault Trees are constructed with the top event being “wrong side failure” of the LOC-OB system or subsystem. A WSF is a failure which could result in or lead to a potentially unsafe operating state.

The causes at different lower levels for such a top event WSF are logically combined with the ‘OR’, ‘AND’ and ‘N/M’ gates. This analysis results in a hierarchical tree structure finally. The basic structure of a Fault Tree is illustrated:

“AND” gate

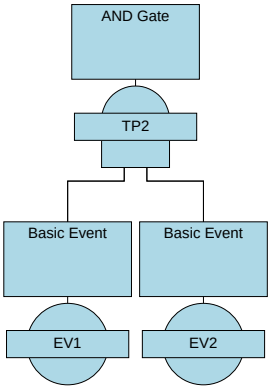
Failures are to be combined by an “AND” gate if they coincidentally, and only in this manner, establish a WSF.

Based on the safety principles applied in the Signalling System, the “coincidence” of two failures means in this context that

- the failures have to exist simultaneously, and
- in case of checked redundant comparison (in contrast to a supervision function), the failures cannot be distinguished by comparing their effects.

$$\lambda_{AND} = \lambda_1 \lambda_2 (MTTR_1 + MTTR_2) \quad or \quad MTBF_{AND} = \frac{MTBF_1 \cdot MTBF_2}{MTTR_1 + MTTR_2}$$

$$\frac{1}{MTTR_{AND}} = \frac{1}{MTTR_1} + \frac{1}{MTTR_2}$$



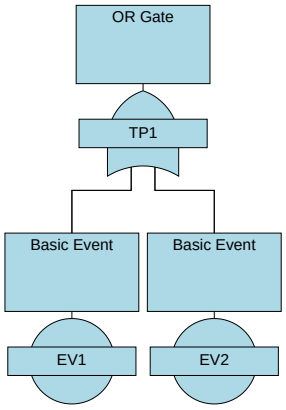
"OR" gate

The "OR" gate is used for two purposes:

- To determine the total failure rate λ of several components, the failures of which are used as an integral entry to an "AND" gate.
- To sum all failures, which have been identified as WSF. This applies to the WSF output of "AND" gates only, as single basic failures do not constitute WSFs.

$$\lambda_{OR} = \lambda_1 + \lambda_2 \quad or \quad \frac{1}{MTBF_{OR}} = \frac{1}{MTBF_1} + \frac{1}{MTBF_2}$$

$$MTTR_{OR} = \frac{\lambda_1}{\lambda_1 + \lambda_2} MTTR_1 + \frac{\lambda_2}{\lambda_1 + \lambda_2} MTTR_2 = \frac{\lambda_1 MTTR_1 + \lambda_2 MTTR_2}{\lambda_1 + \lambda_2}$$



Construction of the fault trees

Based on this understanding of the "OR" and "AND" conditions the rules for setting up the fault tree are:

- Wrong side failures arising from LOC-OB Hardware Component (e.g. GNSS receiver, IMU, Speed sensors) and contributing in-dependently are combined by an "OR" gate.
- Component failures which might cause a WSF but are prevented from becoming effective by a supervision function, are combined by an "AND" gate with the failure probability of the component executing that supervision function.
- Failures of components working in checked redundancy are combined by an "AND" gate with the failure probability of their "partner" component.

Top Gate Event

For the top gate event, the LOC-OB system function failure is selected, it means LOC-OB fail to provide the output data.

The hardware failure rate (FR) outlined in chapter 4 is used as an input for the Fault Tree Analysis (FTA). The resulting top gate outcome is the Total Functional Failure Rate (TFFR).

6.2 Operational Context

For GNSS-centric solutions, particularly in challenging environments, where no GNSS signal can be tracked, the LOC-OB's Area of Uncertainty can grow very large. This presents a challenge in developing the LOC-OB system to fulfil safety requirements in all operational environment compared to current ETCS which rely solely on balises for localisation. The Operational context outlined below are analysed to demonstrate the safety level of train localisation by LOC-OB system and the necessity of balises in harsh environment, parting track topology and LOC-OB initialisation function.

The following functionals and operational scenarios are considered in FTA:

1. Along Track Localisation and Integrity functions with Open Sky (Good GNSS-EGNOS signal) without using Balises refer to FTA chapter 6.4.1.
2. Along Track Localisation and Integrity functions with Harsh Environment area without using balises, for example, in tunnels, under the bridges, in mountain or urban area refer to FTA chapter 6.4.2.
3. Along Track Localisation and Integrity functions with Harsh Environment area with using balises refer to FTA chapter 6.4.3.
4. Track Selectivity function (Parting Track Topology) without using Balises refer to FTA chapter 6.4.4 (6.4.4.1, and 6.4.4.2).
5. Track Selectivity function (Parting Track Topology) with using Balises refer to FTA chapter 6.4.4.3, and 6.4.4.4 .
6. LOC-OB INIT which required Cold movement detector and without Balises refer to FTA chapter 6.4.5 (6.4.5.1, 6.4.5.2).
7. LOC-OB INIT which required Cold movement detector but with using Balises refer to FTA chapter 6.4.5.3, and 6.4.5.4.

Note: In term of hardware for FTA chapter 6.4.1 and 6.4.2 are not different, however, the train operates under different operational scenarios.

6.3 Architectures used in the FTA

As concluded in the result from CLUG RAMS Analysis Report D3.2.1, the LOC-OB system's is not able to reach SIL 4 level with one single chain (see Figure 10 with one GNSS-EGNOS receiver, and one IMU). The "Optimized architecture / 1 single chain" is very similar to the CLUG (1) architecture. The LOC-OB Navigation and Integrity engines embed the following functions that are fed on one hand by the non-synchronized filtered and safe data from the set of sensors (1 GNSS receiver, 1 IMU and 1 Tachometer),

and on the second hand the digital map data base. These engines consist of five core functions, detailed in chapter 3.3. More detail can be found in chapter 6 – D4.1 [11].

Therefore, CLUG 2.0 - D4.1 proposed an updated architecture (see Figure 11) which is used in this analysis to evaluate the safety integrity level of LOC-OB. The architecture proposed by D4.1 contains two independent chains:

- Chain 1: The architecture of CLUG1 using a GNSS/EGNOS Receiver with one IMU of safety critical level.
- Chain 2: The second chain "Shape and heading map matching" computes along track 1D position using a tachymeter (OPG) speed information, the train dynamics reported by a second IMU, and a digital vector map that features a continuous representation of the azimuth and curvature for the track edges.

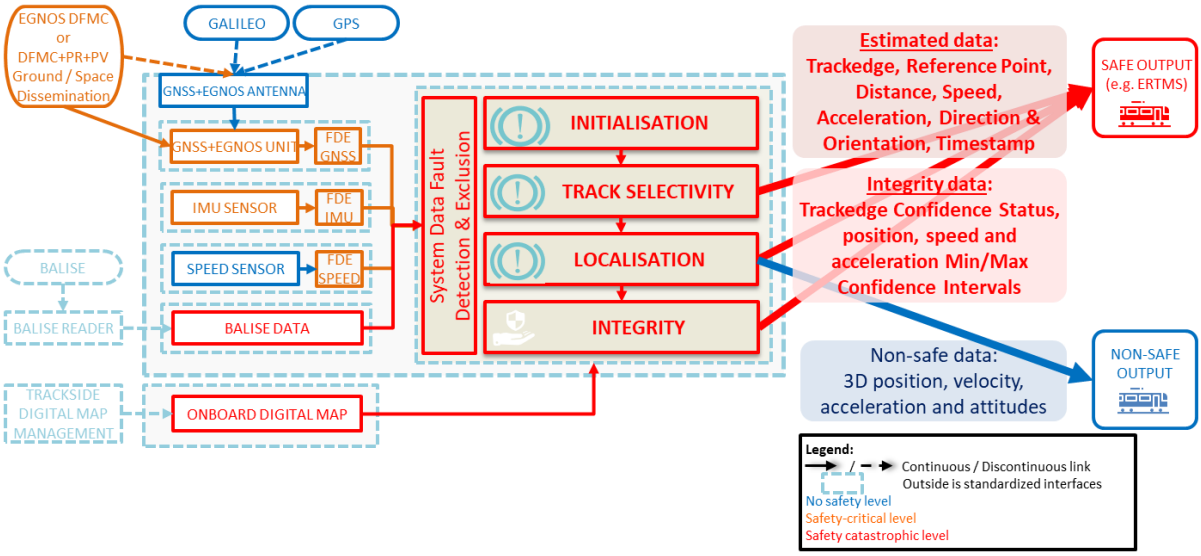


Figure 10: CLUG LOC-OB functional architecture – Optimized solution (See §2.4 from [11])

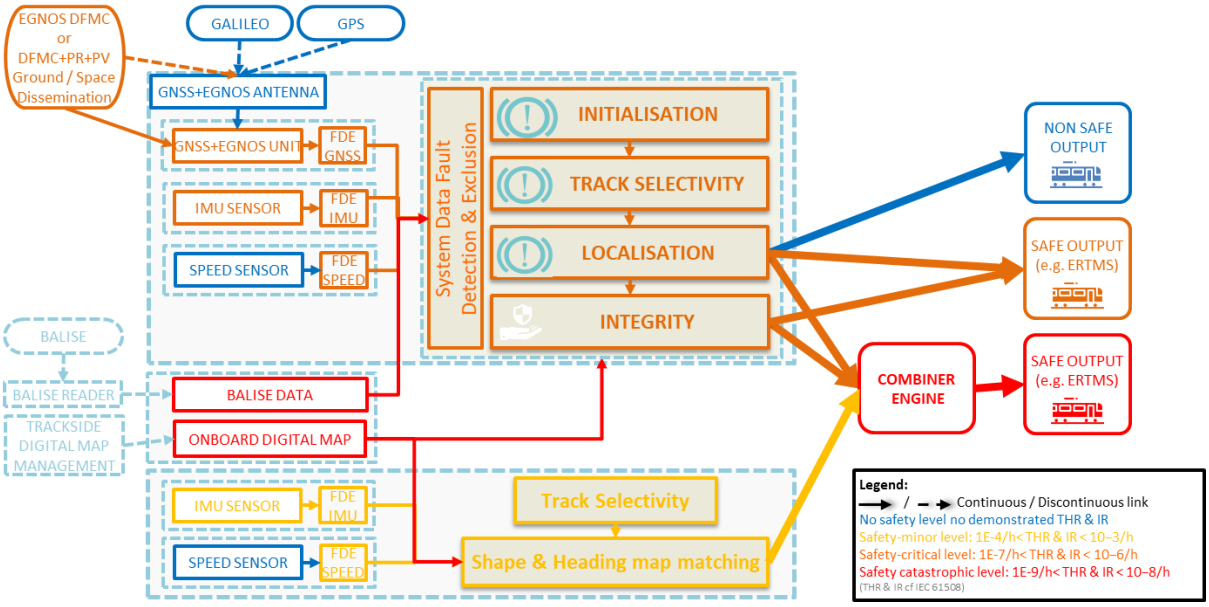


Figure 11: LOC-OB dual chain overall architecture (See §6.5 from [11])

Note: D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version).

In the following analysis, two configurations of LOC-OB are used: Config 1 and Config 2 use a separate hardware (refer to ASS-12) for LOC-OB processing with of IMU safety critical and IMU catastrophic levels respectively.

LOC-OB CONFIGURATION		GNSS - EGNOS RECEIVER	IMU OF SAFETY CRITICAL LEVEL	IMU OF SAFETY CATASTROPHIC LEVEL	TACHO METER	REFERENCE
Config-01	Chain_1	1	1		1	D4.1 Safety Design justification – two chains with using IMU of safety critical level
	Chain_2		1		1	
Config-02	Chain_1	1		1	1	Propose IMU of safety catastrophic level (lower failure rate)
	Chain_2			1	1	

Table 16: List of LOC-OB configurations

The main Feared Events from the LOC-OB System point of view is listed below:

- **GNSS-EGNOS Receiver Fault**, when the GNSS data provided by the receiver is faulty even after the application of the corresponding GNSS data FDE.
- **IMU Fault**, when the inertial data used in the localisation algorithm is faulty.
- **Tachometer Fault**, when the tachometer data used in the localisation algorithm is faulty.
- **Digital Map Fault,** when LOC-OB get incorrect Digital Map data (from external subsystem and it assumes as SIL4 input (refer to ASS-07)).
- **Balise Reader Fault,** when LOC-OB get incorrect balise data (from external subsystem and it assumes as SIL4 input (refer to ASS-03)).
- **Point Position Fault,** when LOC-OB get incorrect Point Position data (from external subsystem and it assumes as SIL4 input (refer to ASS-01)).
- **Cold Movement Detector Fault,** when LOC-OB get incorrect Cold Movement data (from external subsystem and it assumes as SIL4 input (refer to ASS-02)).
- **LOC-OB Processing Hardware Fault,** due to lack of detailed information regarding the hardware processing of the fusion algorithm, system FDE, navigation engine, integrity engine, and shape and heading map matching so we assume the separate hardware between chain 1 and chain 2 to execute all these functions refer to ASS-12. the failure rate of each hardware is assumed as 1E-05 per hour.
- **Combiner Hardware** to execute combiner function is assumed the failure rate as 1E-09 per hour (refer to ASS-13).
- **Route information from infrastructure** is needed and it is assumed as SIL4 input data (refer to ASS-14).

Note: The Doppler Radar and Optical Sensors are not included in Fault Tree Analysis because the IMU and System FDE functions are designed to mitigate minor drift, and slip/slide issue. A minimum set of multi sensors is proposed to evaluate whether the hardware configuration to meet SIL4 compliance. Future test results will determine whether the System FDE function alone sufficiently mitigates minor drift errors and slip/slide issues. If it does not, the Doppler radar and optical sensor are required for the LOC-OB system.

6.4 Fault Tree Analysis

The hardware failure rate in FTA is taken from chapter 2.

6.4.1 Along Track Localisation and Integrity functions with Open Sky (Good GNSS-EGNOS signal) without using balises

6.4.1.1 Config 1: 1 GNSS-EGNOS Receiver, 2 Safety-Critical IMUs, 1 Tachometer

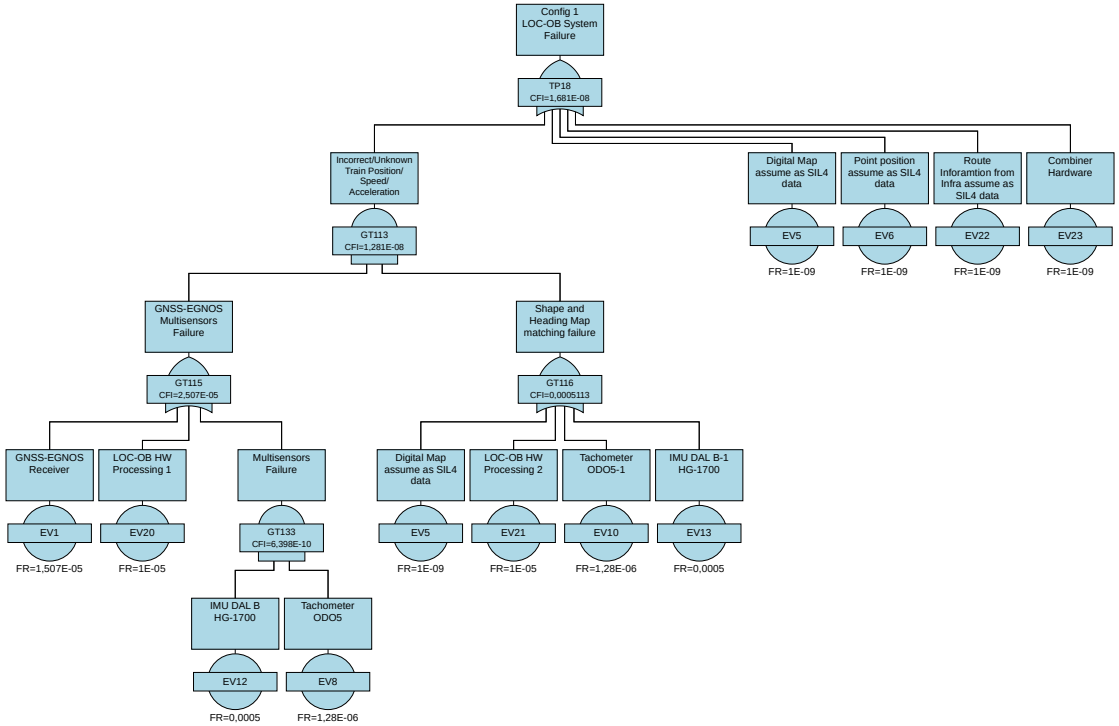


Figure 12: FTA Config 1 – LOC -OB System Failure in Open Sky (no balise)

6.4.1.2 Config 2: 1 GNSS – EGNOS Receiver, 2 Safety-Catastrophic IMUs, 1 Tachometer

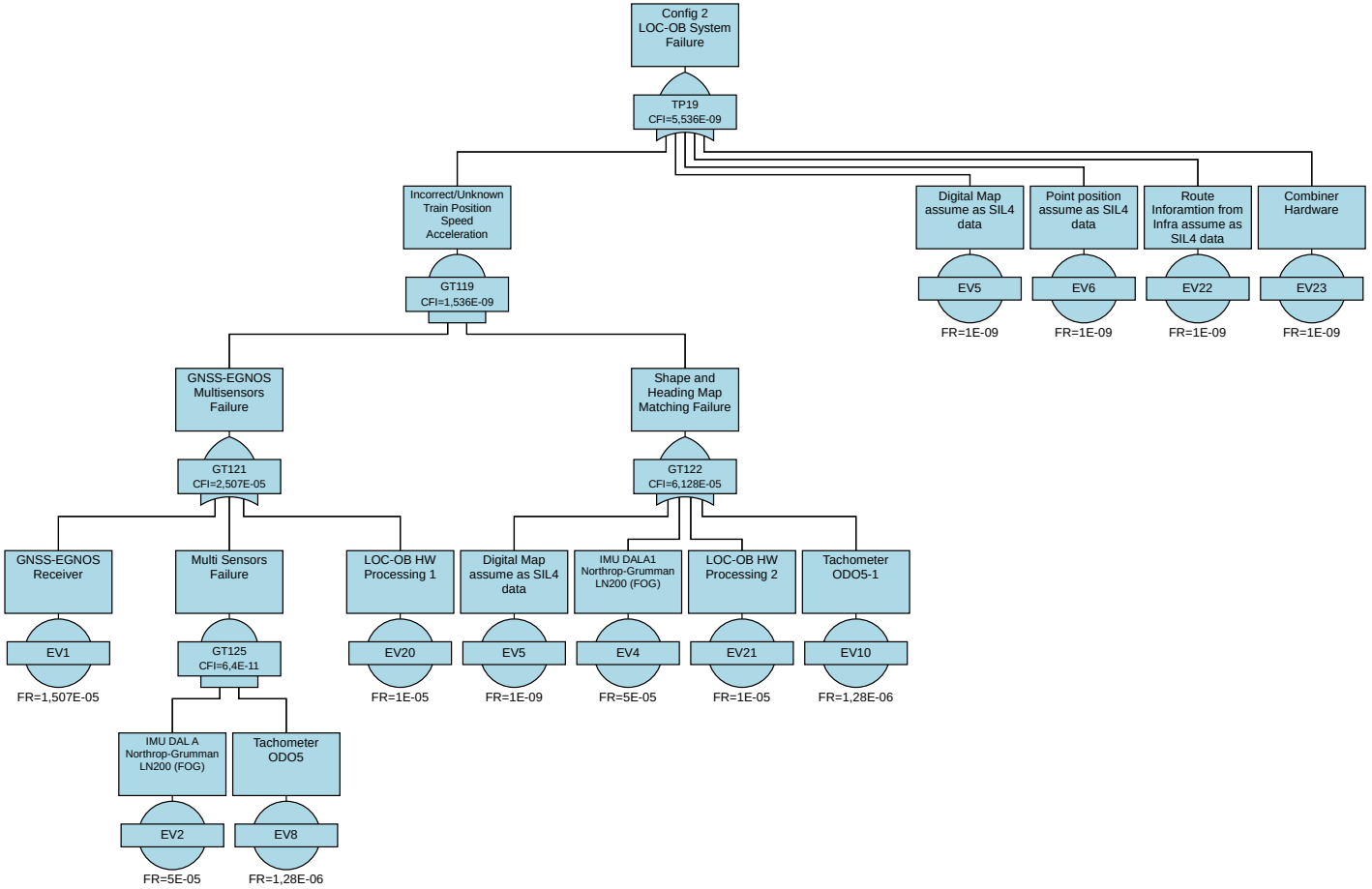


Figure 13: FTA Config 2 – LOC -OB System Failure in Open Sky (no balise)

6.4.2 Along Track Localisation and Integrity functions with harsh environment area (for example, in tunnel, in urban area, under the bridges, in the mountain)

6.4.2.1 Config 1: 1 GNSS – EGNOS receiver, 2 Safety-Critical IMUs, 1 Tachometer without balises

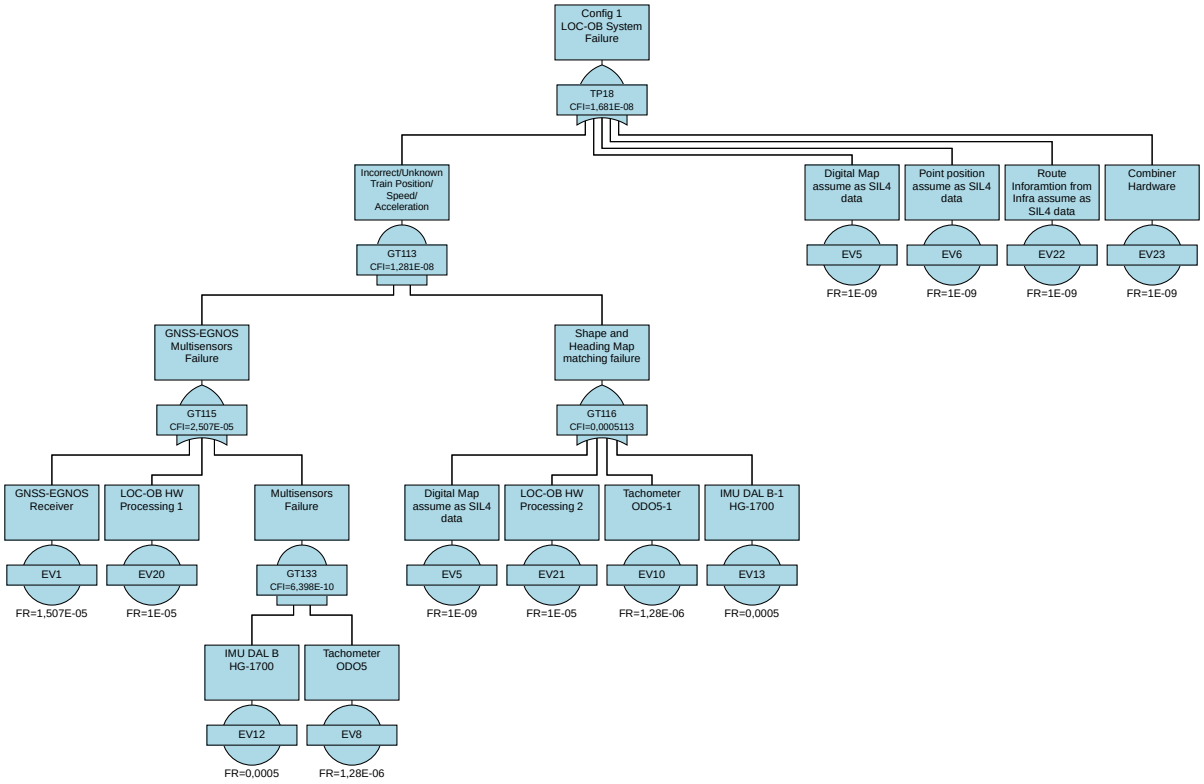


Figure 14: FTA Config 1 – LOC -OB System Failure in Harsh environment (no balise)

6.4.2.2 Config 2: 1 GNSS – EGNOS receiver, 2 Safety-Catastrophic IMUs, 1 Tachometer without balises

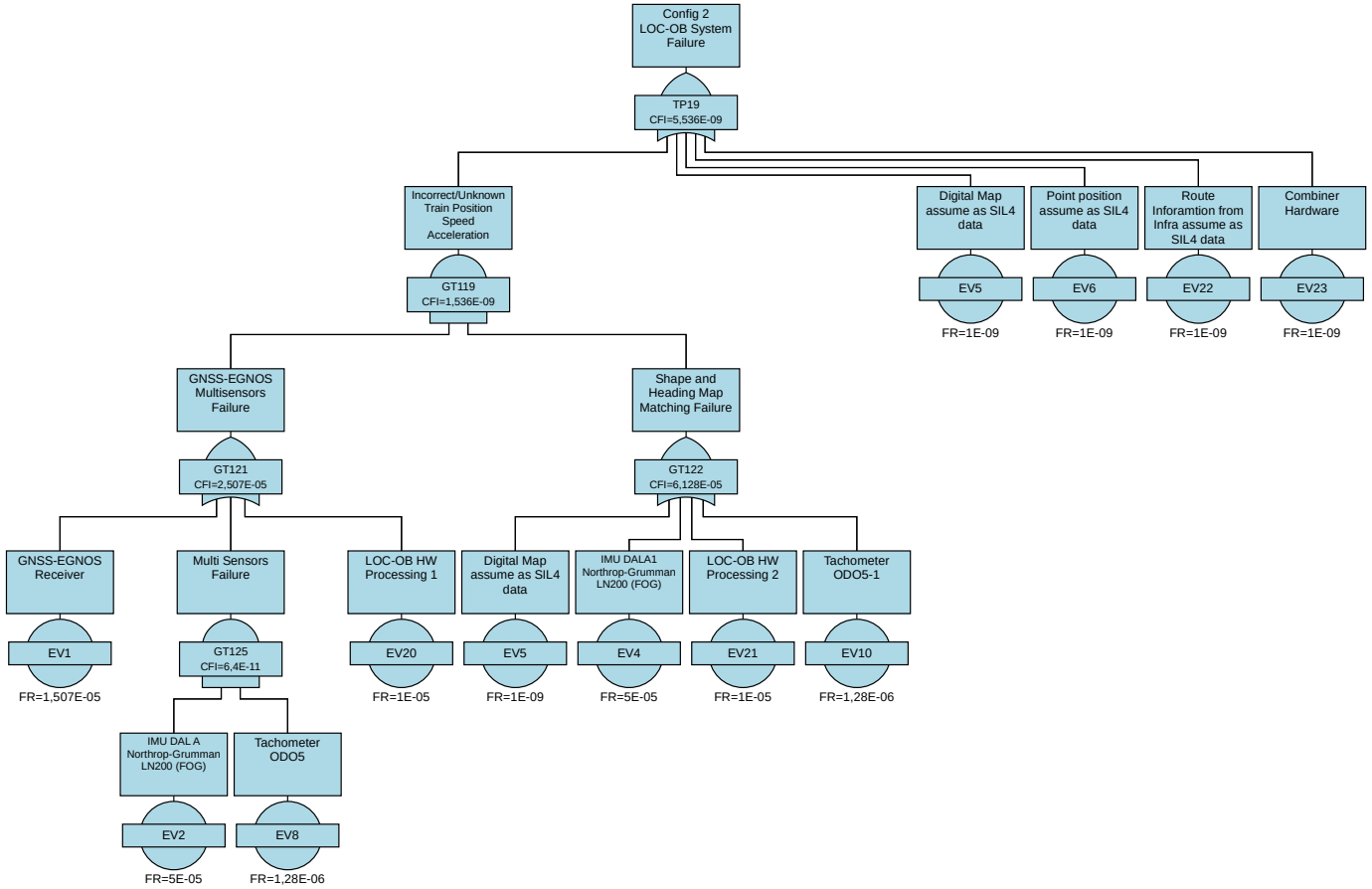


Figure 15: FTA Config 2 – LOC -OB System Failure in Harsh environment (no balise)

6.4.3 Along Track Localisation and Integrity functions with harsh environment and using balise

6.4.3.1 Config 1: 1 GNSS – EGNOS receiver, 2 Safety-Critical IMUs, 1 Tachometer with Balises

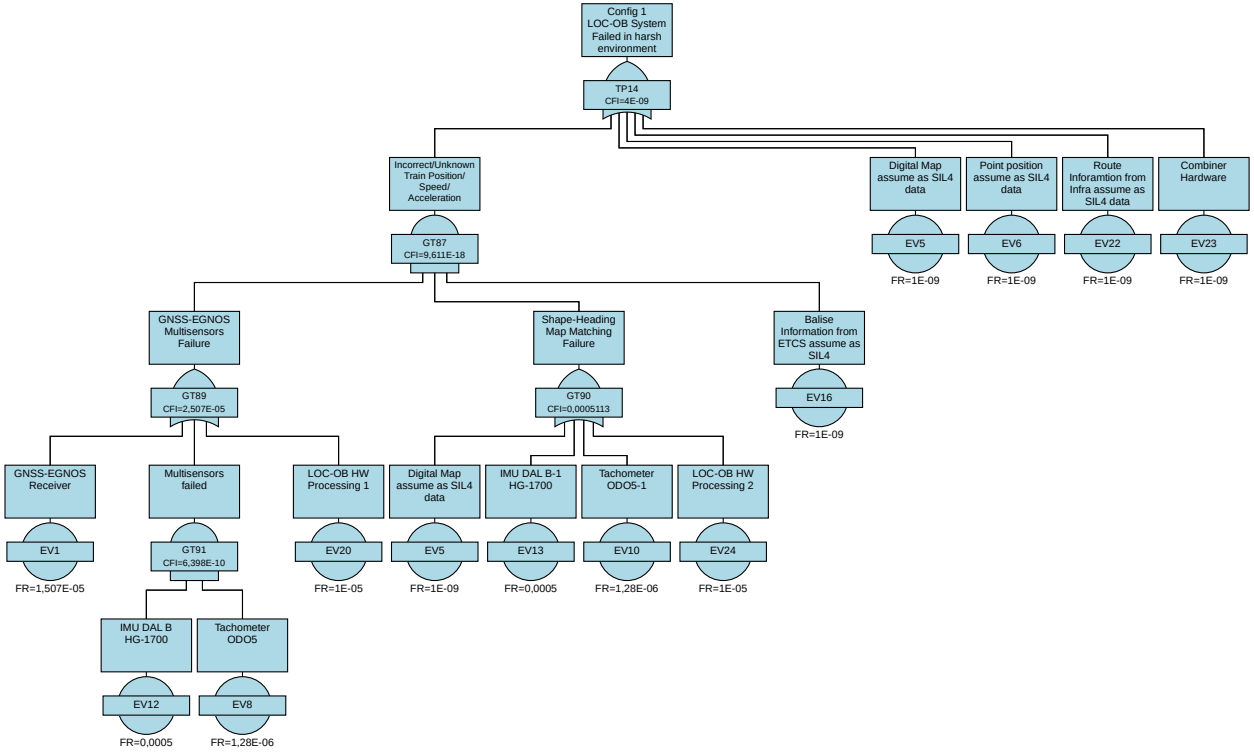


Figure 16: FTA Config 1 – LOC -OB System Failure in Harsh environment (with balises)

6.4.3.2 Config 2: 1 GNSS – EGNOS receiver, 2 Safety-Catastrophic IMUs , 1 Tachometer with balises

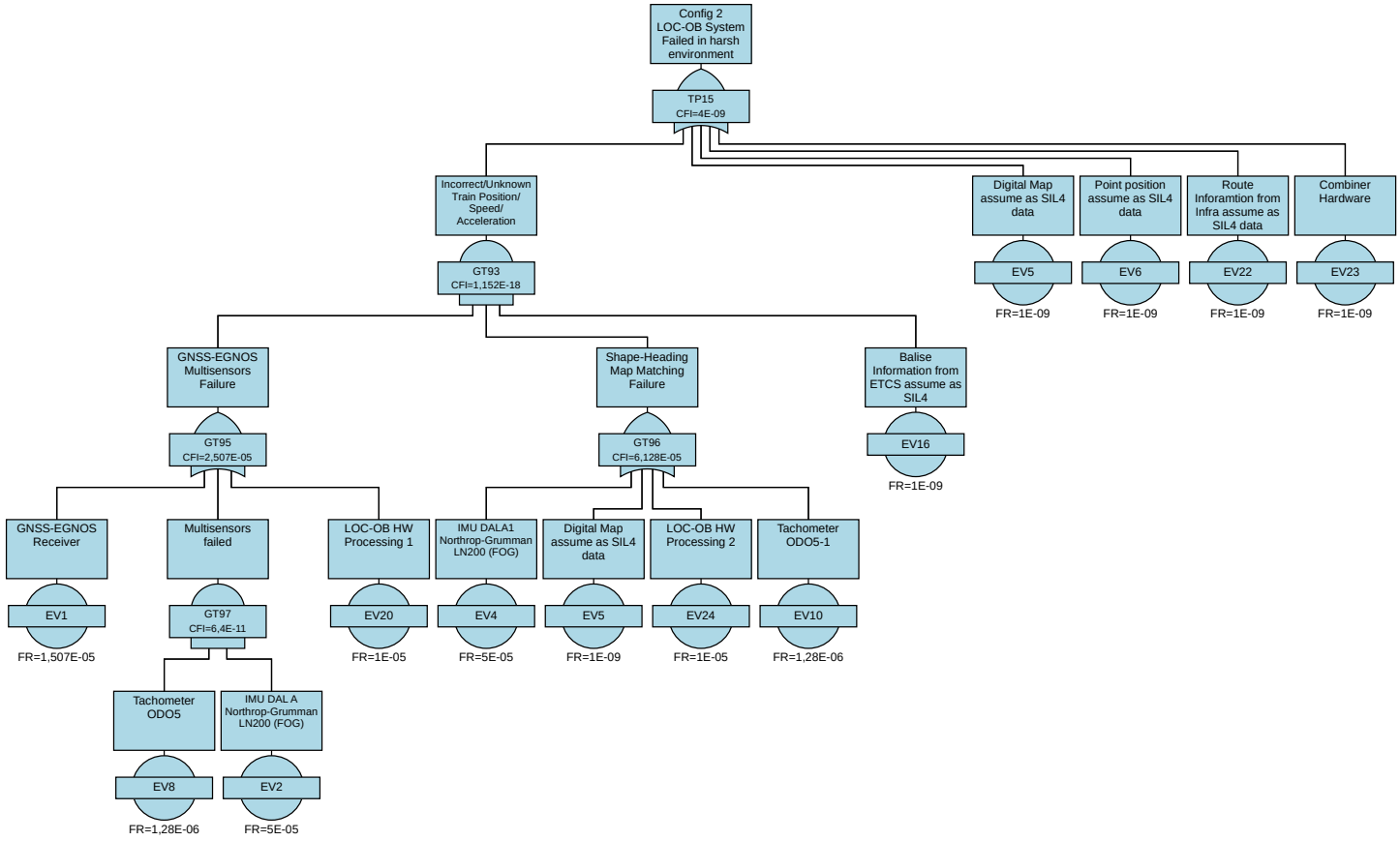


Figure 17: FTA Config 2 – LOC -OB System Failure in Harsh environment (with balises)

6.4.4 Track Selectivity (Parting Track Topology)

6.4.4.1 Config 1: 1 GNSS – EGNOS receiver, 2 Safety-Critical IMUs, 1 Tachometer without balises

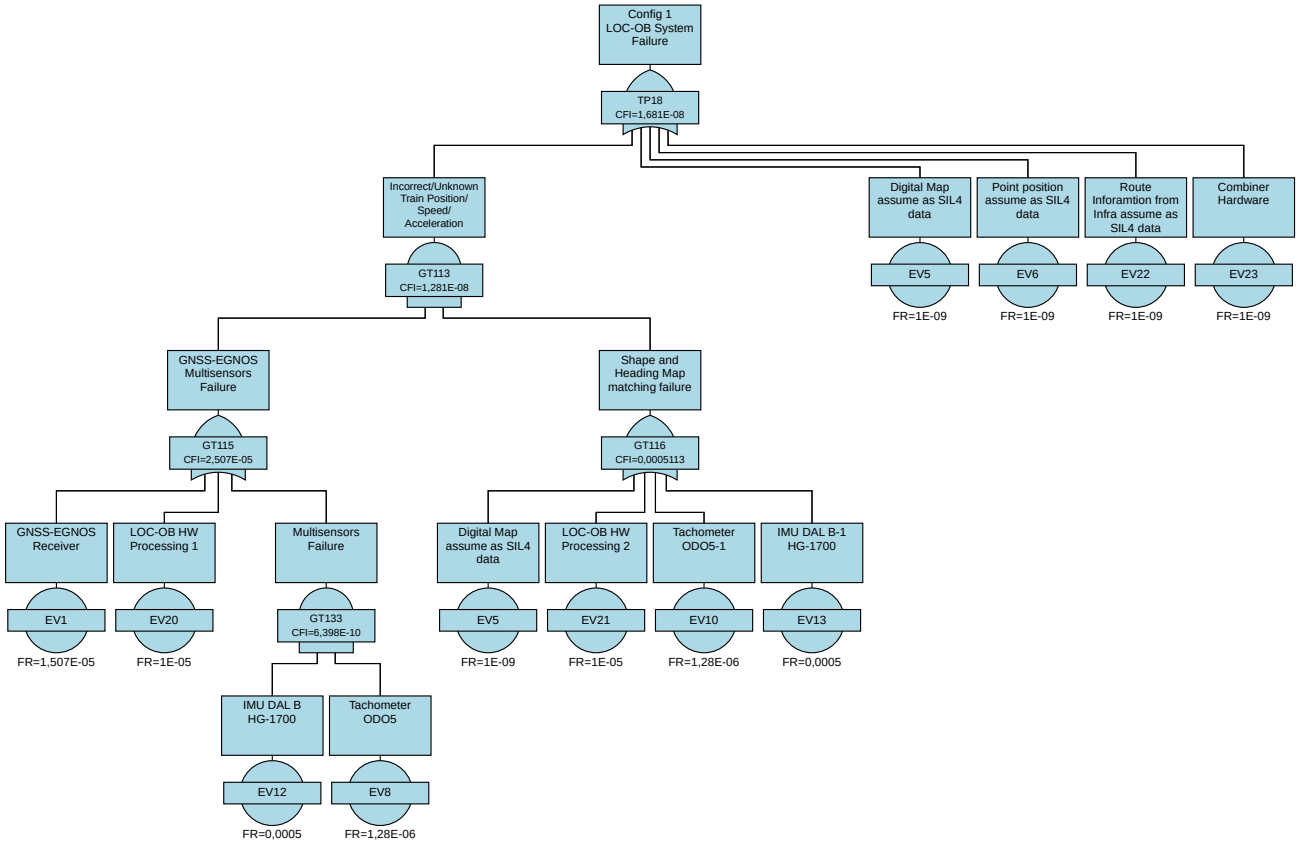


Figure 18: FTA Config 1 – Track Selectivity Function Failure (without balises)

6.4.4.2 Config 2: 1 GNSS – EGNOS receiver, 2 Safety-Catastrophic IMUs, 1 Tachometer without balises

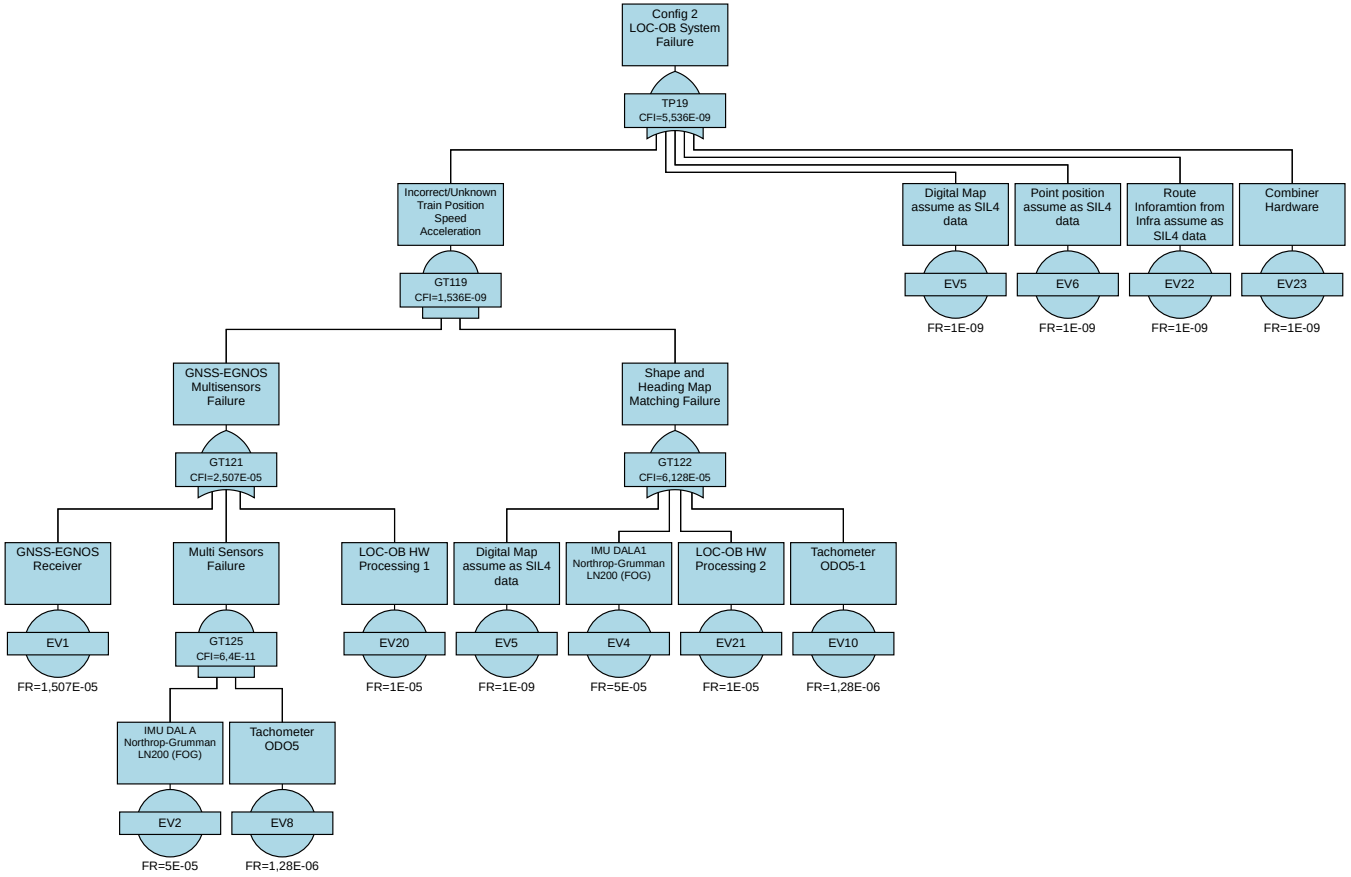


Figure 19: FTA Config 2 - Track Selectivity Function Failure (without balises)

6.4.4.3 Config 1: 1 GNSS – EGNOS receiver, 2 Safety-Critical IMUs, 1 Tachometer with balises

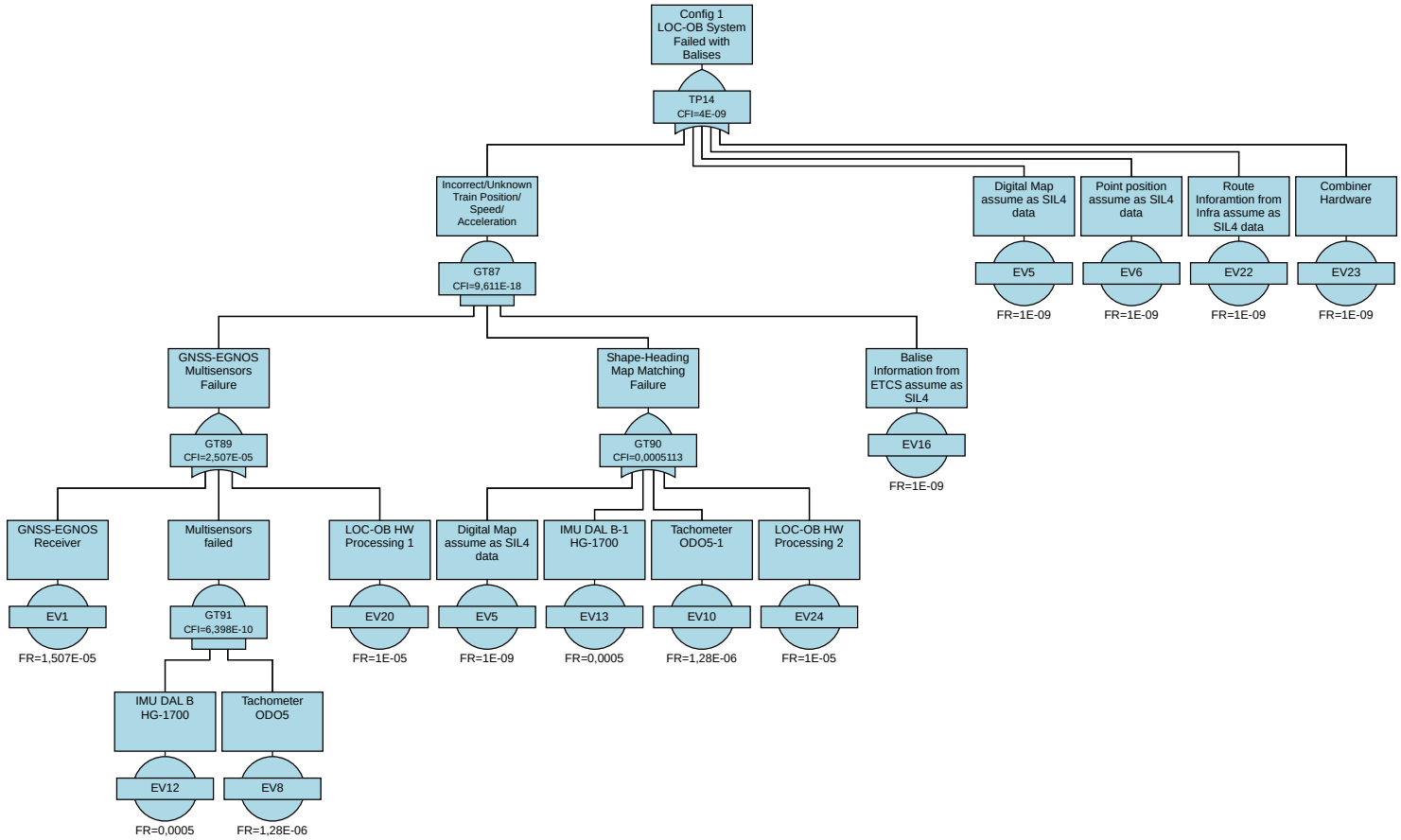


Figure 20: FTA Config 1 - Track Selectivity Function Failure (with balises)

6.4.4.4 Config 2: 2 GNSS – EGNOS receivers, 2 Safety-Catastrophic IMUs, 1 Tachometer with balises

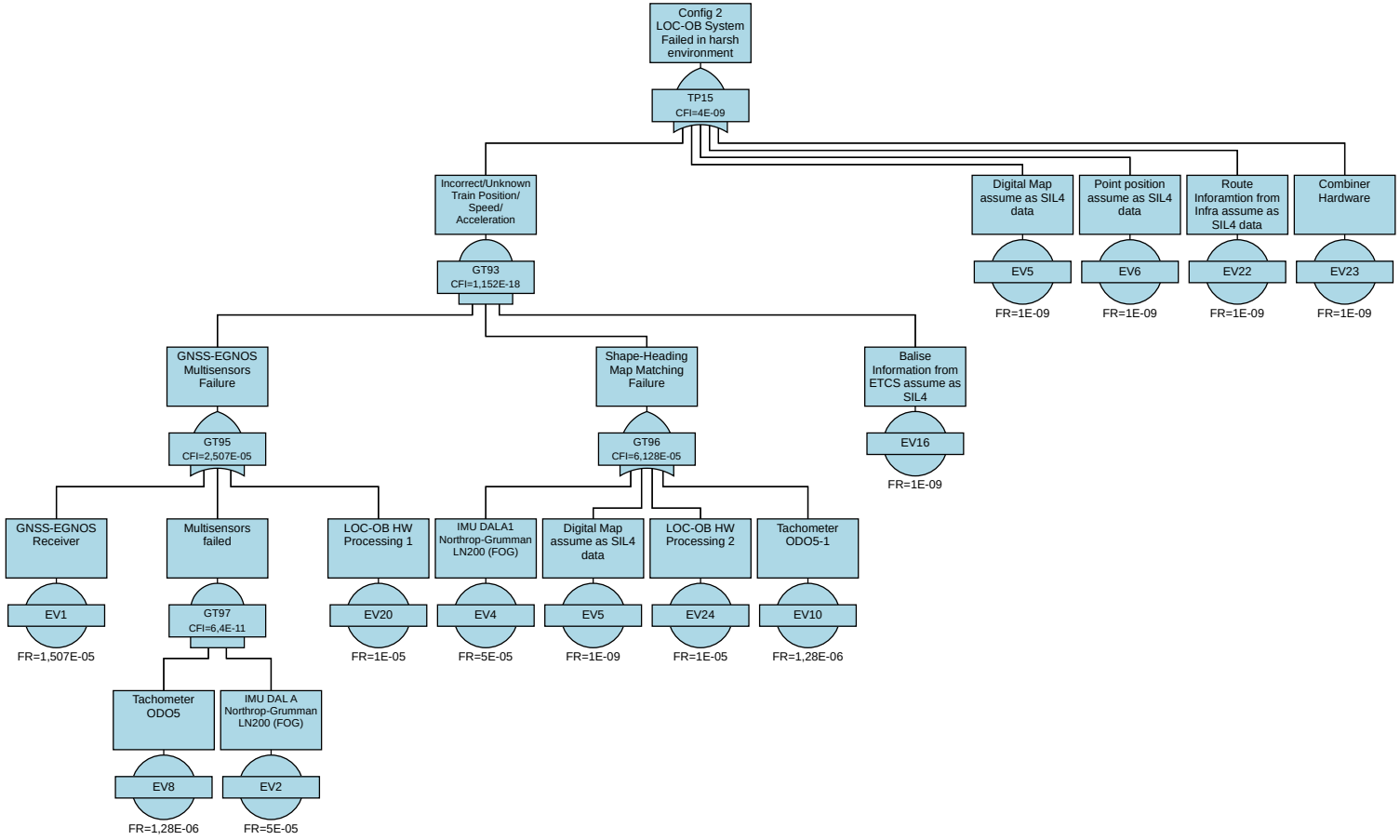


Figure 21: FTA Config 2 - Track Selectivity Function Failure (with balises)

6.4.5 LOC-OB Initialisation

6.4.5.1 Config 1: 1 GNSS – EGNOS receiver, 2 Safety-Critical IMUs, 1 Tachometer without balises

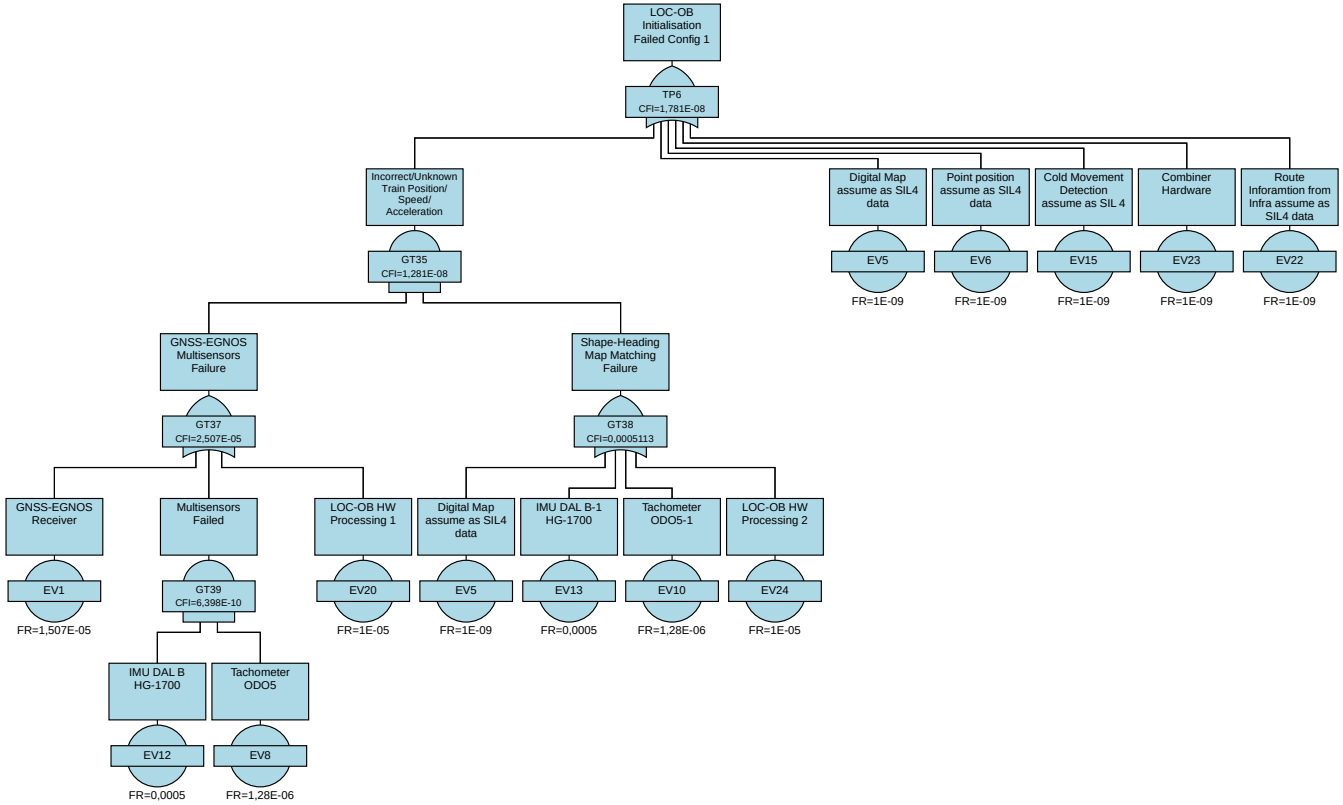


Figure 22: FTA Config 1 – LOC-OB Initialisation Failure (without balises)

6.4.5.2 Config 2: 1 GNSS – EGNOS receiver, 2 Safety-Catastrophic IMUs, 1 Tachometer without Balises

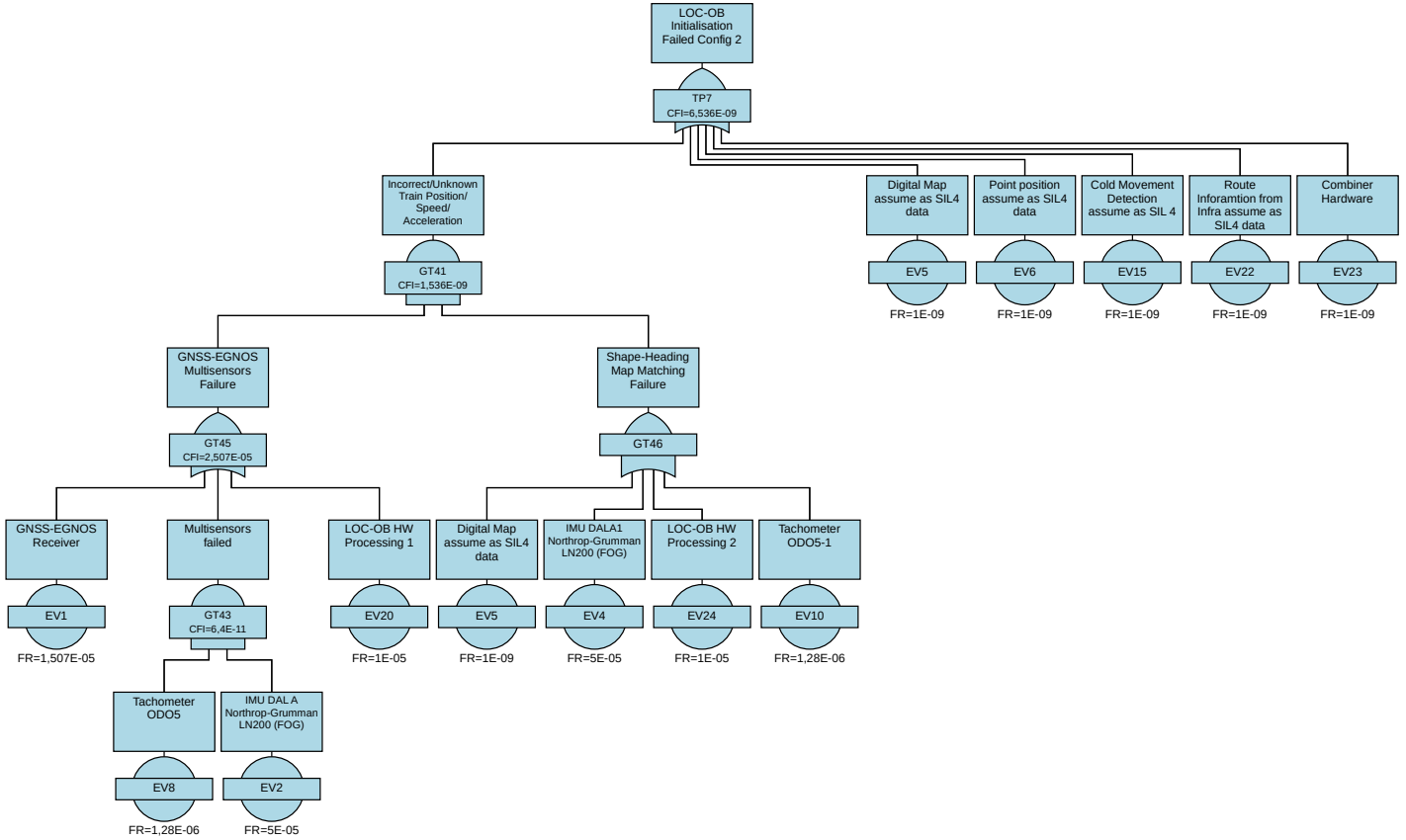


Figure 23: FTA Config 2 – LOC-OB Initialisation Failure (without balises)

6.4.5.3 Config 1: 1 GNSS – EGNOS receiver, 2 Safety-Critical IMUs, 1 Tachometer with Balises

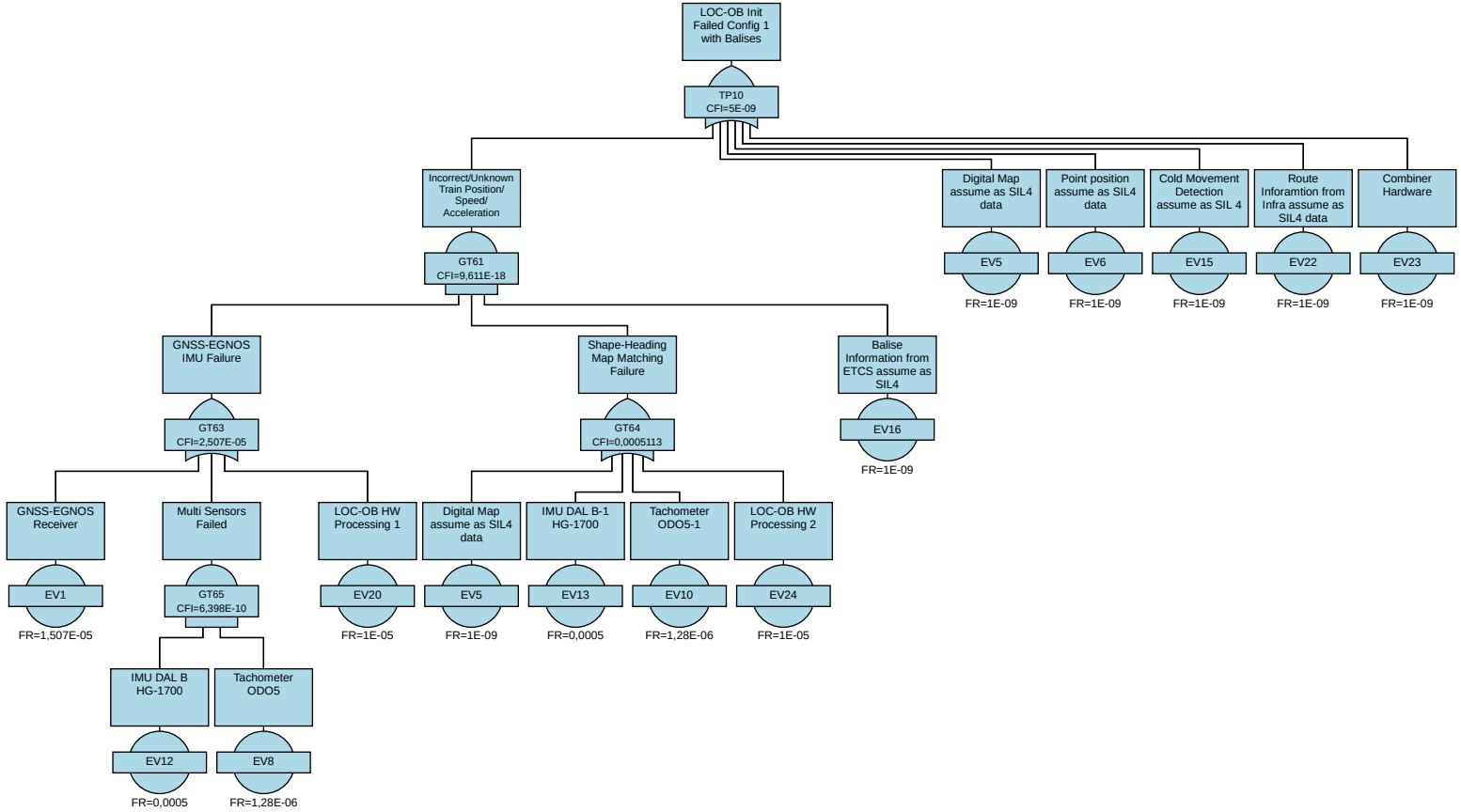


Figure 24: FTA Config 1 – LOC-OB Initialisation Failure (with balises)

6.4.5.4 Config 2: 1 GNSS – EGNOS receiver, 2 Safety-Catastrophic IMUs, 1 Tachometer with Balises

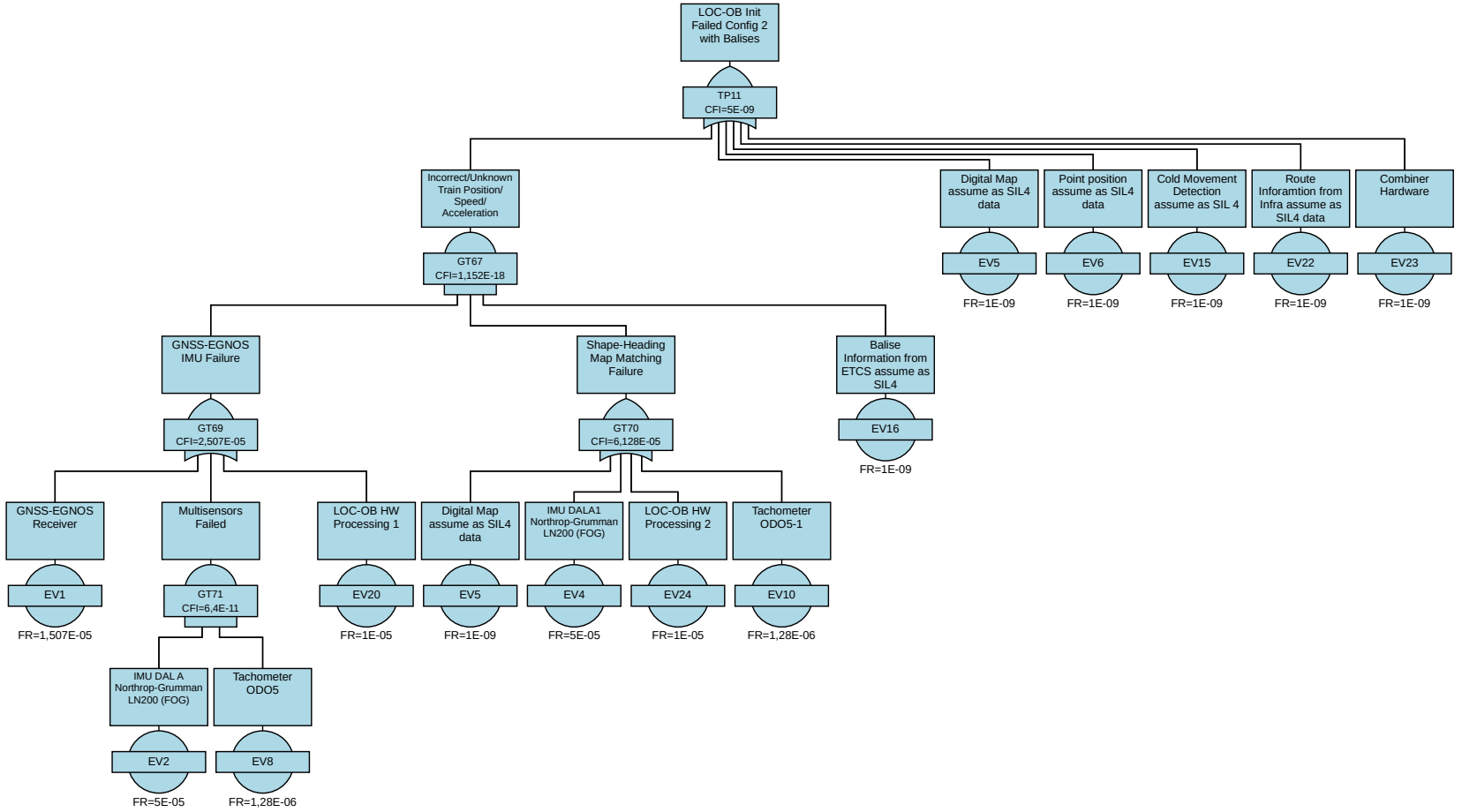


Figure 25: FTA Config 2 – LOC-OB Initialisation Failure (with balises)

6.5 Results of Fault Tree Analysis

The specific objective of the fault tree analysis, which is part of the safety analysis for the Localisation Onboard Unit (LOC-OB), is to demonstrate that:

- The safety integrity level of LOC-OB can achieve SIL 4 with a range of 1E-09 <= TFFR < 1E-08 through the safety design justification as outline in D4.1.

AREA/ SCENARIO/FUNCTION	CONFIG 1 1 GNSS-EGNOS Receiver + 2 Safety-Critical IMUs + 1 Tachometer		CONFIG 2 1 GNSS-EGNOS Receiver + 2 Safety-Catastrophic IMUs + 1 Tachometer	
	FTA RESULTS THR /TFFR		FTA RESULTS THR /TFFR	
	WITHOUT BALISES	WITH BALISES	WITHOUT BALISES	WITH BALISES
Along track localisation and Integrity function in Open Sky (Good GNSS-EGNOS signal)	TP18 1.681E-08	-	TP19 5.536E-09	-
Along track localisation and Integrity function in Harsh Environment area, for example, in tunnels, Urban area	TP18 1.681E-08	TP14 4E-09	TP19 5.536E-09	TP15 4E-09
Track Selectivity Function	TP18 1.681E-08	TP14 4E-09	TP19 5.536E-09	TP15 4E-09
LOC-OB initialisation function	TP6 1.781E-08	TP10 5E-09	TP7 6.536E-09	TP11 5E-09

Table 17: Fault Tree Analysis Result

Note : "-" means no FTA calculation because with Opn sky, the balises are not needed. Even if the balises are taken into FTA, the result will be reach SIL4 that's why it is green.

"TPx" represents the gate number in FTA analysis chapter 6.4.

Red highlight means the TFFR is not lower than 1E-8 which cannot achieved SIL 4 level. Green highlight mean the TFFR is lower than 1E-08 which can achieved SIL 4 level.

D4.1 is not yet officially released. The version referenced in this context is version 0.4 (internal version).

The results present those two independent chains utilizing Safety-Critical IMU(Honeywell-1700), with failure rate as 5E-4 per hour as the design proposed by Airbus (refer to chapter 6.5 - D4.1) are insufficient for the LOC-OB System to achieve SIL 4 level. To meet SIL4 requirements, the LOC-OB system requires two chains designed with Safety-Catastrophic IMU (Northrop Grumman LN200 (FOG))

with the failure rate of 5E-05 per hour. However, both chains are not entirely independent, as they rely on the same Digital Map which introduce the risk of common cause failure.

The Table 17 provided above summarises the result of the FTA conduct in chapter 6.4, the configuration 2 to have one GNSS-EGNOS Receiver, and two Safety-Catastrophic IMUs from Northrop Grumman LN200 (FOG) demonstrates the capability to achieve SIL 4 level in all operational scenarios. Additionally, a Cold Movement Detector is prerequisite for LOC-OB Initialisation without the need of balises. If there is no CMD as the input of LOC-OB INIT then the balises are necessary to LOC-OB Initialisation phase.

For track selectivity function, the point position is considered as an input. This input should meet SIL4 level. The point position information is necessary because the track selectivity function with GNSS-IMU navigation cannot determine the track edge ID after passing the first switch if there are two junctions close to each other. It can only determine the track edge ID after the train passes two successive switches. More detail can be found in chapter 5.3 and D4.8 [13].

Point position information, the Digital Map and Route Information from infrastructure need to be SIL4 inputs data; otherwise, they will affect the THR of the LOC-OB system.

For the unknown hardware components in the Navigation Engine, Integrity Engine, System FDE function, and Shape and Heading Map matching, the Hardware required to process all these functions must be integrated and enable the LOC-OB to meet SIL4 level. In the FTA demonstrates that using separate hardware for chain 1 and chain 2 with a failure rate for each hardware as 1E-5 per hour, enables the LOC-OB system to meet TFFR 1E-09 per hour (SIL 4 level).

For the Combiner hardware to execute combiner function shall have a failure rate less than or equal to 1E-09 per hour.

According to configuration 2 from the Fault Tree Analysis turn out to have a TFFR lower than 1E-08 per hour without balises. An isolated view at the Fault Tree Analysis (FTA) can lead to the conclusion that balises are not necessary in harsh environment. However, in harsh environments, the Area of Uncertainty of the LOC-OB can increase significantly due to the accumulation of minor drift errors, which can adversely affect system availability. From a safety perspective, further investigation into GNSS-IMU performance is crucial. Specifically, it is important to determine how the GNSS-IMU navigation system can accurately recalculate the train front-end position and confidence interval after transitioning from harsh environments to open sky conditions. Balises may be essential in harsh environments where GNSS-EGNOS signals are unavailable.

Safety requirement derived from Fault Tree Analysis:

ID	SAFETY REQUIREMENTS	RATIONALE
RA-RAMS-39	The IMU use for both chains shall have failure rate less than or equal to 5E-05 per hour.	This IMU characteristic can enable LOC-OB system to meet SIL4 requirements.
RA-RAMS-40	The separate hardware for chain 1 and chain 2, the failure rate of each hardware shall be less than or equal to 1 E-05 per hour. • Chain 1 hardware executes system FDE, fusion algorithm, navigation engine, integrity engine. • Chain 2 hardware executes shape and heading map matching.	These hardware characteristics can enable LOC-OB system to meet SIL4 requirements.
RA-RAMS-41	Combiner hardware to execute Combiner function shall have the failure rate less than or equal to 1 E-09 per hour.	This Combiner Hardware can enable LOC-OB system to meet SIL4 requirements.

Table 18: List of Safety Requirements derived from FTA

7 CONCLUSION

The analysis carried out as part of that document contained 2 parts. The first part (chapter 5) led to the following conclusions and proposals:

- The results of System Functional Safety analysis (chapter 5.3) provide a summary of the qualitative analysis and should be taken into consideration for the recommendations. A list of safety requirements (Table 13, Table 14, Table 15) was provided.
- The safety-related requirements, derived from D2.2 [2] and D2.4 [4], are listed in the respective chapter 5.3 and have been confirmed. Further detail can be found in chapter 5.3.

The second part (chapter 6 and 6.5), the Fault Tree Analysis is performed to demonstrate the random safety integrity achieved by the hardware design and the results led to the following conclusion and proposals:

- Concerning LOC-OB hardware system architecture and to respect safety requirements for the LOC-OB, it is proposed to use IMU with the failure rate of 5E-05 per hour on both chains (**RA-RAMS-39**). With this configuration, LOC-OB can achieve SIL 4 level in all areas. However, if any IMU with higher MTBF data more than 20,000 hours and lower failure rate than 5E-05 per hour is used, it would also be possible for the LOC-OB system to achieve SIL 4 level.
- Regarding the proposed design of two chains by incorporating shape and heading map matching techniques, it can enable the LOC-OB system to meet SIL4 requirements, but it is not a fully independent system, as both chains rely on the same Digital Map, which can result in common-cause failure, even if the software algorithms for both chains differ.
- It is recommended that the LOC-OB design should incorporate Composite Fail-safety. With this technique, each safety related function is performed at least by two items. Each of these items shall be independent from the other to avoid common cause failure. A hazardous fault in one item shall be detected and negated in sufficient time to avoid co-incident fault in a second item.
- Regarding Track Selectivity function point position status is required as input for this function to ensure safe train movement. This integration allows the system to correctly interpret track selection and make informed decisions regarding train routing and movement. The time or the distance when the Track Selectivity is determined after passing a point should be limited and defined. Moreover, the point position information from trackside is required as the SIL4 input data (**RA-RAMS-29**).
- For LOC-OB Initialisation, Cold Movement Detection is needed as input to start-up fusion algorithm. Without CMD, the balises are required if GNSS-EGNOS cannot determine initial position when the train start up (power on). The reasons for this are described in chapter 5.3. The cold movement detection is required as SIL4 input data (**RA-RAMS-28**).
- Regarding the unknown hardware for Navigation Engine, Integrity Engine, and System FDE, the following requirement apply regarding the hardware:

  RA-RAMS-40 : If separate Hardware are used for chain 1 and chain 2 to process these functions, then the failure rate of each hardware should be less than 1E-05 per hour. This configuration would allow the LOC-OB system to achieve SIL4 level.

- The following requirement apply to Combiner Hardware which execute combiner function, this hardware shall have the failure rate less than or equal to 1E-09 per hour refer to **RA-RAMS-41.**
- Regarding the second chains with Shape and Heading Map Matching technique, the Route Information is required as the input for second chains and it should be SIL4 input data (**RA-RAMS-33**).

Overall conclusion:

There are still several open points that require further study in the future. The table below includes unresolved aspect, the reason for pending issues, proposed actions and the responsible parties.

Unresolved Aspect	Reason for pending status	Responsible Party	Expected Resolution Phase	Proposed Action
Mitigation Strategies	It should generally be developed through collaboration between design engineers and safety engineers, which should occur in a subsequent phase. Some mitigations, such as System FDE and FDE, have been outlined in this document; however, they remain incomplete due to a lack of information. Additional safety barriers need to be defined in greater detail. Verification and validation of all mitigation measures should also be conducted in the next phase.	Airbus System Engineer and RAMS Engineer	Further study e.g. CLUG 3.0 Project	Hazard Workshop between System Engineer and Safety Engineer
The accuracy of GNSS-IMU Navigation system after transition from harsh environment to open sky	Further investigation is necessary to determine how accurately the GNSS-IMU navigation system can recalculate the train front-end position and confidence interval after transitioning from harsh	Airbus System Engineer (Designer) and Safety Engineer	Further study e.g . CLUG 3.0 Project	Further analysis and investigation are required to assess the performance of the LOC-OB system when transitioning from a harsh environment to open sky, particularly in scenarios involving

Unresolved Aspect	Reason for pending status	Responsible Party	Expected Resolution Phase	Proposed Action
	environments to open sky conditions. However, having balises in harsh environments can enhance the safety of the train localisation function. The tolerable hazard rate of the LOC-OB system is reduced by half compared to areas where balises are not used.			long tunnels. This investigation could be conducted within WP5 (if the test case for running the test train through the longest tunnel is included) or as part of a further study, such as the CLUG 3.0 project. The test case should involve running a test train through the Gotthard Base Tunnel in Switzerland, the longest tunnel in Europe, with a length of 57.1 km. Additionally, the longest tunnel in Germany, which passes through the Landrücken ridge in the Hesse region, measures 10.78 km.
Safety Integrity Level of Software development process	Systematic failures, particularly those related to software, require a different approach. To this end, the software development process will adhere strictly to the EN50128:2011and EN50716:2023 standard, which are recognized for its stringent requirements for software safety in railway applications. These standard mandates the implementation of rigorous quality management and safety	Airbus Software Designer	Further study, e.g. CLUG 3.0 Project or Industrialize phase	Demonstrate Safety Integrity level for LOC-OB Software.

Unresolved Aspect	Reason for pending status	Responsible Party	Expected Resolution Phase	Proposed Action
	management processes throughout the software lifecycle.			
No Train Position Report from LOC-OB send to ETCS-OB	A hazard remains if the LOC-OB does not send a train position report to the ETCS-OB, as the train would be operating with an unknown position if there is no track vacancy detection. To mitigate this hazard, it should be escalated to the system integration level (e.g., Automatic Train Protection or Interlocking). From an operational viewpoint, if the LOC-OB cannot provide the train position within the defined time, the train should be delocalized, and either a service brake or an emergency brake should be applied to stop the train. The last train position report should be frozen. However, these actions are outside the scope of the LOC-OB.	System Integration Level	Further study e.g. CLUG 3.0	Hazard Workshop for System Integration level.

Table 19: Open Points for CLUG 2.0 project

8 APPENDIX A

Appendix A – System Functional Analysis CLUG II

System Functional Analysis CLUG 2.0.xls

9 REFERENCES

REF	Document/Source	Title/WEBSITE	Version	Date
[1]	CLUG 2.0 D2.1	Operational Needs and System Capabilities of the LOC-OB System	1.0	30/11/2023
[2]	CLUG 2.0 D2.2	Start of Mission and Track Selectivity	1.0	30/11/2023
[3]	CLUG 2.0 D2.3	LOC-OB System Definition and Operational Context	1.0	30/11/2023
[4]	CLUG 2.0 D2.4	LOC-OB System Requirements	1.0	30/11/2023
[5]	EN 50126-1:2017 (E)	Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Generic RAMS Process	-	06/12/2017
[6]	EN 50126-2:2017 (E)	Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Systems Approach to Safety	-	07/12/2017
[7]	EN 50129:2018	Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling	-	06/2019
[8]	EN 50128	Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems	-	03/2012
[9]	CLUG 2.0 D3.1	CLUG LOC-OB System context analysis and RAMS Plan	2.0	22/03/2024
[10]	CLUG 2.0 D3.2	LOC-OB Preliminary Hazard Analysis	1.0	20/12/2023
[11]	CLUG 2.0 D4.1	LOC-OB Functional Architecture	0.4	30/09/2024
[12]	CLUG 2.0 D4.2	GNSS Receiver Interface Control Document	1.1	07/11/2023
[13]	CLUG 2.0 D4.8	Track Selectivity Determination Algorithm Design	0.2	07/03/2024
[14]	CLUG 2.0 D4.9	Start of Mission Preliminary Definition (LOC-OB INIT)	-	-
[15]	CLUG 2.0 D4.6	Along Track Localisation Fusion Algorithm Design Document	1.0	14/05/2024
[16]	CLUG 2.0 D4.7	Confidence Intervals Computation and Integrity Algorithm	-	-
[17]	CLUG 2.0 D4.3	Safe IMU Sensor and Data FDE for LOC-OB Description	0.2	26/02/2024
[18]	CLUG 2.0 D4.4	Speed Sensor and data FDE for LOC-OB Description	2.0	20/02/2024
[19]	CLUG 2.0 D4.5	Euro Balise Reader Sensor and data FDE for LOC-OB Description	2.0	21/02/2024
[20]	CLUG 2.0 D4.10	Onboard Digital Map Definition and Interfaces	2.0	28/02/2024
[21]	CLUG D3.1.5	TLOBU Solution A Architecture and Design	2.4	17/02/2022
[22]	CLUG D3.2.1	RAMS Report of TLOBU Solution A	2.3	31/01/2022
[23]	CLUG D3.1.2.2.4	Other Sensors Performances	1.4	17/01/2022
[24]	CLUG (1) D2.4	Preliminary Hazard Analysis and Safety Requirements	1.5	12/04/2021
[25]	CLUG (1) D2.3	High Level System Requirement	2.4	25/01/2021
[26]	CLUG (1) D5.7	Preliminary Definition of the System Performances and Interfaces	1.1	29/06/2022
[27]	ETCS BL3R2 – TSI CCS SUBSET-023	Glossary of Terms and Abbreviations	3.3.0	13/05/2016
[28]	ETCS BL3R2 – TSI CCS SUBSET-041	Performance Requirements for Interoperability	3.2.0	17/12/2015
[29]	ETCS BL3R2 – TSI CCS SUBSET-091	Safety Requirements for the Technical Interoperability of ETCS in Levels 1 and 2	3.6.0	12/05/2016
[30]	DIN EN 50159-2:2001	Railway applications – Communication, signalling and processing systems – safety related communication in transmission systems	-	04/2011
[31]	ETCS BL3R2 – TSI CCS SUBSET-035	Specific Transmission Module FFFIS	3.2.0	16/12/2015

REF	Document/Source	Title/WEBSITE	Version	Date
[32]	ETCS BL3R2 – TSI CCS SUBSET-088	ETCS Application Levels 1&2 – Safety Analysis	3.7.0	18/12/2019
[33]	CLUG 2.0 D5	Interface Control Document	0.14	09/04/2024

CLUG 2.0 has received funding from the European Union's Horizon research and innovation programme under grant agreement **No 101082624**