CLUG Demonstration of Readiness for Rail – CLUG 2.0

D3.7 CLUG LOC-OB SYSTEM EVALUATION REPORT

Due date of deliverable: 31/03/2025

Actual submission date: 04/06/2025

Leader of this Deliverable: Marc SARRAT, SNCF

Reviewed: Y

Document status		
Revision	Date	Description
0.1	13/11/2024	Draft version
0.2	29/11/2024	Workshop conclusion
0.3	26/02/2025	Final version including task reviewers. review
0.4	20/03/2025	Version including technical review comments
0.5	11/04/2025	Version for quality review
1.0	25/04/2025	Quality check version
1.1	17/04/2025	Final approved version
1.2	27/05/2025	Final version officially submitted to EUSPA
2.0	04/06/2025	Final version officially submitted to EUSPA

Project funded from the European Union's Horizon 2020 research and innovation program		
Dissemination Level		
PU	Public	X
SEN	Sensitive, limited under the conditions of the Grant Agreement	
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: 30 months

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

REPORT AUTHORS

NAME	COMPANY	DETAILS OF CONTRIBUTION
Marc Sarrat / Marielle Petit-Doche	SNCF	V0.1: Draft version: - Plan - § Introduction
Marc Sarrat / Marielle Petit-Doche **Thidarat Panthong** **Alejandro Lopez Hernandez**	SNCF DB InfraGO SMO	V0.2: - Remarks on draft plan - Results of the workshop - Preparation of the version for internal review
Marc Sarrat / Marielle Petit-Doche **Alejandro Lopez Hernandez**	SNCF SMO	V0.3: - Results of internal review - Version for technical review
Marc Sarrat / Marielle Petit-Doche	SNCF	V0.4: - Results of technical review
Marc Sarrat / Marielle Petit-Doche	SNCF	V0.5: - Clean up for quality review
Mariya Kayalova	RINA	V1.0: quality check
Marc Sarrat / Marielle Petit-Doche	SNCF	V1.1: Final version after last modifications
Marc Sarrat / Marielle Petit-Doche	SNCF	V1.2: Comments from external review

REPORT REVIEWERS

NAME	COMPANY	DETAILS OF CONTRIBUTION
Karin Nebe	SMO	Author and internal reviewer
Alejandro Lopez Hernandez	SMO	Author and internal reviewer
Thidarat Panthong	DB InfraGO	Author and internal reviewer
Lena-Alexandra Tillemann	DB InfraGO	Author and internal reviewer
Valentin Barreau	SNCF	Technical Review
Adrien Gharios	SNCF	Technical Review
Mariya Kayalova	RINA-C	Quality check
Jose Bertolin	UNIFE	Final check and submission to reviewers and EUSPA

EXECUTIVE SUMMARY

This document is the deliverable “D3.7 – LOC-OB Evaluation Report” of the European project “CLUG Demonstration of Readiness for Rail” (hereinafter also referred to as “CLUG 2.0”). This document evaluates what has been produced during the project (WP2 + WP3 + WP4) to cover the RAMS objectives defined during T3.1 and to consider Safety and RAM results defined in T3.2 to T3.6.

The document provides a coverage of the WP2 requirements by the analyses made in WP3: all WP2 requirements assumed as safety related are confirmed safety related by WP3 analyses; a few requirements assumed as non-safety related by WP2 have been declared safety related by the WP3 analysis.

A synthesis of the results of WP3 analyses has been then performed, notably explaining how the RAMS requirements identified are covered by the solution designed in WP4 documents. These analyses recommend the choice of a dual chain architecture and the definition of several control functions to detect and eliminate errors on the inputs as soon as possible.

The aim of CLUG 2.0 is to provide a TRL6 demonstrator and not to deliver an industrial product. So WP3 activities have been limited to the RAMS activities of the early phase of the life cycle defined in EN50126-1 [R20]. The remaining steps before obtaining a certifiable product have then been listed. This concerns mainly the deployment of a design, verification and validation process for an industrial system.

And the main topics to be tackled during these remaining steps have been discussed, notably:

- Precise the operational context and the user needs and use cases.
- Set a definitive architecture and select the relevant hardware components.
- Clarify the safety functional mechanism to detect and mitigate failures.
- Identify the process to design, verify and validate in safety a software implementing fusion algorithms.

The RAMS analyses provided during CLUG 2.0 project give detailed results that lead to the conclusion that the system can reach a high-level safety target.

This architecture is based on some strong assumptions on the inputs: an EGNOS for Rail service is considered to improve the safety related to GNSS, a safe digital map is necessary, balises are needed for a safe initialization of the system. These first results give confidence that a certifiable product based on the solution with a two-chains architecture can be designed to reach a SIL4 target for an ERTMS operational context.

LIST OF ACRONYMS

ACRONYM	CONCEPTS
CCS	Control, Command and Signalling
CCN	CCS Communication Network
CLUG	Certifiable Localisation Unit with GNSS in the railway environment
CSM	Common Safety Methods
CTMS	Capacity and Traffic Management System
ERA	European Railway Agency
ERTMS	European Rail Traffic Management System
estFE	Estimate Train Front End Position
ETCS	European Train Control System
FFFIS	Form Fit Functional Interface Specification
FMEA	Failure Modes and Effects analysis
ICD	Interface Control Document
LOC	Localisation
LWG	Localisation Working Group
OCORA	Open CCS On-board Reference Architecture
ODO	ODOmetry
PHA	Preliminary Hazard Analysis
RAMS	Reliability, Availability, Maintainability and Safety
SCI-*	Standard Communication Interface
SFAS	System Functional Safety Analysis

ACRONYM	CONCEPTS
SIL	Safety Integrity Level
SRAC	Safety Related Application Condition
TCMS	Train Control Management System
TFFR	Tolerable Functional Failure Rate
THR	Tolerable Hazard Rate
TPS	Train Protection System
TSI	Technical Specification of Interoperability
TSN	Time-Sensitive Networking
WSoI	Wider System-of-Interest

APPLICABLE DOCUMENTS

The following documents define the contractual requirements that all project partners are required to comply with:

- Grant Agreement N°101082624 (which includes Description of Work, Grant Preparation Forms and annexes): This is the contract with the European Commission which defines what has to be done, how and the relevant efforts.
- Consortium Agreement (signed version 13/04/2023): This defines our obligations towards each other.

Each of the above documents was established at the start of the project, and copies were supplied to each partner. Each document could potentially be updated independently of the others during the course of the project following a prescribed process. In the event of any such update, the latest formal issued version shall apply.

In the event of a conflict between this document and any of the contractual documents referenced above, the contractual document(s) shall take precedence.

CONTENTS

List of figures

List of tables

1 INTRODUCTION

1.1 Objectives

The objective of this task is to evaluate what has been produced during the project (WP2 + WP3 + WP4) to cover the RAMS objectives defined during T3.1 and to consider Safety and RAM results defined in T3.2 to T3.6.

The requirements defined in D2.4 are first recalled and the RAMS labels confirmed.

Then, the conclusions of each WP3 deliverable are summarized as well as the coverage of the RAMS requirements defined in WP3 relatively to the system descriptions given in WP4.

The remaining steps are eventually presented, notably to obtain an authorization agreement for an industrial solution according to the CSM-RA 403/2013 [R27] and PAVA 545/2018 [R26] and the CENELEC standards [R20], [R21], [R22] and [R23].

And the main gaps identified during the WP3 analysis concerning user needs, hardware and functional architecture, critical functions…, are discussed.

1.2 Scope of the document

This document covers the RAMS activities performed during the CLUG 2.0 project.

The analysis is based on the current version of the CLUG 2.0 documents: WP3 deliverables, except this one and WP2 deliverables are all approved. WP4 and WP5 documents are approved or in a stable version.

The analyses made in this deliverable are based on a draft and stable version of D4.1 [R10], as the official final version of this document is not yet available. However, the elements form D4.1 used in this document (functions identification and the two functional architectures proposed) are stable and any change on D4.1 will not significantly impact this analysis.

2 LOC-OB SYSTEM REQUIREMENTS ISSSUED FROM WP2

2.1 High Level User Requirements (D2.1)

This list of requirements has been defined in D2.1 [R1]

Req ID	Requirement	Category according WP2	WP3 Task coverage	Coverage Id	Coverage comments
UR[001]	LOC-OB shall provide 1D localisation information: - Acceleration (estimated, underestimation, overestimation). - Speed (estimated, underestimation, overestimation). - Position (estimated, underestimation, overestimation). - Train movement direction - Train orientation - Side of the position from/to reference location - Track Edge Id.	Functional	D3.2 §3.2	Risk assessment of **LOC-OB_SF-001**	Considered as safety related by WP3: LOC-OB_SF-001 function shall be designed with a TFFR <= 10^{-9}/h LOC-OB_SF-002 function shall be designed with a TFFR <= 10^{-9}/h LOC-OB_SF-003 function shall be designed with a TFFR <= 10^{-9}/h
UR[002]	LOC-OB shall provide acceleration, velocity and position in a common 3D reference system.	Functional	-	-	Not RAMS related
UR[003]	LOC-OB shall provide vehicle attitude in a common 3D reference frame.	Functional	-	-	Not RAMS related
UR[004]	After being powered up and its initialisation stage ended, LOC-OB shall provide data continuously.	Functional	-	-	Not RAMS related

Req ID	Requirement	Category according WP2	WP3 Task coverage	Coverage Id	Coverage comments
UR[005]	Even if LOC-OB is not able to provide the train position, speed shall be provided by LOC-OB in order to move the train.	Functional	-	-	Not RAMS related
UR[006]	LOC-OB shall provide localisation information with an accuracy that fulfils the existing and future users' application needs (estimated position/speed, min/max safe front end) as specified in the operational needs.	Performance	-	-	Not RAMS related
UR[007]	LOC-OB shall provide localisation information in adequacy with the temporal constraints of the existing and future users' application needs as specified in the operational needs.	Performance	-	-	Not RAMS related
UR[008]	None	-	-	-	-
UR[009]	If safety is not in concern, LOC-OB, between two successive localisation information, shall not provide a variation of the confidence interval that leads to brake intervention or trip (TR) mode.	Performance	-	-	Not RAMS related
UR[010]	When compared to the current ERTMS baseline, the same performances shall be achieved by LOC-OB using a significantly reduced number of balises.	Performance / Economic constraints	-	-	Not RAMS related
UR[011]	If safety is not in concern, the absolute maximum allowed value of the LOC-OB confidence interval shall be lower compared to baseline ETCS BL3 R2 [SS041].	Performance / Economic constraints	-	-	Not RAMS related

Req ID	Requirement	Category according WP2	WP3 Task coverage	Coverage Id	Coverage comments
UR[012]	LOC-OB shall guarantee all its functionalities for trains running up to 500km/h.	Performance / Compatibility	-	-	Not RAMS related
UR[013]	LOC-OB shall add economic benefits (opex and capex) to IM and RU in comparison to Ref [30] odometry definition.	Economic constraints	-	-	Not RAMS related
UR[014]	LOC-OB shall be designed as an independent constituent of the Control Command and Signalling On-Board (CCS-OB) with standardised interfaces.	Modularity	-	-	Not RAMS related
UR[015]	LOC-OB shall be a constituent separated from the core ETCS through a standardised interface.	Interoperability	-	-	Not RAMS related
UR[016]	LOC-OB being an electronic embedded component, LOC-OB shall comply with applicable environmental standards.	Operational and environmental conditions	D3.2 §3.2	**RA-RAMS-07**	Partially covered: the need should be specified depending on the hardware architecture.
UR[017]	None.	-	-	-	-
UR[018]	LOC-OB shall achieve all performance targets under the following train behaviour or surrounding environment: All types of physical environments such as station areas surrounded by high buildings, forests, etc. all types of Rail infrastructure (e.g., tunnels, bridges, with or without catenary, concrete track, ballast track, etc).	Operational and environmental conditions	-	-	Not RAMS related

Req ID	Requirement	Category according WP2	WP3 Task coverage	Coverage Id	Coverage comments
	Under all types of train acceleration/deceleration conditions Under train jerk conditions Under coasting mode Under slip/slide conditions Under sparks with overhead line Under ballast throw Under steep ramp/slope Under small radius curve				
UR[019]	LOC-OB shall achieve backward compatibility with ETCS L2 defined in Ref [30].	Compatibility	-	-	Not RAMS related
UR[020]	The safety of the LOC-OB shall be ensured and demonstrated according to the Common Safety Methods [ERA CSM] and the [EN 50126] standard.	RAMSS	D3.2 §3.2	**RA-RAMS-01**	Covered by the PHA, considered as RAMS related.
UR[021]	LOC-OB shall not degrade safety toward odometry as defined in the ETCS BL3 R2.	RAMSS	D3.2 §3.2	**RA-RAMS-02**	Covered by the PHA, considered as safety related.
UR[022]	The true train position shall be always inside the confidence interval.	RAMSS	D3.2 §3.2	**RA-RAMS-03** **RA-RAMS-08**	Covered by the PHA, considered as safety related.
UR[023]	The true train speed shall be always inside the confidence interval.	RAMSS	D3.2 §3.2	**RA-RAMS-04**	Covered by the PHA, considered as safety related.

Req ID	Requirement	Category according WP2	WP3 Task coverage	Coverage Id	Coverage comments
UR[024]	The true train acceleration shall be always inside the confidence interval.	RAMSS	D3.2 §3.2	**RA-RAMS-05**	Covered by the PHA, considered as safety related.
UR[025]	Each localisation information shall fulfil safety target requirements in accordance with the user's application requirements.	RAMSS	D3.2 §3.2	**RA-RAMS-06**	Covered by the PHA, considered as safety related.
UR[026]	The LOC-OB shall fulfil requirements and recommendations for cybersecurity as specified in [CLC/TS 50701:2021] with the purpose to demonstrate that the system is up to date from a cybersecurity perspective and that it meets and maintains the target level of security for the entire system life cycle.	RAMSS	-	-	Not RAMS related but Security. Out of the scope of WP3

Table 1: User requirements of LOC-OB extracted from D2.1 [R1] and coverage by WP3 analysis

2.2 Specification requirements (D2.4)

This list of requirements has been defined in D2.4 [R3]

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[001]	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	**Safety**	D3.2 §3.2	Risk assessment of **LOC-OB_SF-001**	LOC-OB_SF-001 function shall be designed with a TFFR <= 10^{-9}/h
SpecSysReq[002]	LOC-OB shall provide the track edge ID where the train front end position is.	None	D3.2 §3.2 D3.5	**RA-RAMS-08** **RA-RAMS-37**	This requirement is covered by SpecSysReq[070]. D3.5 considers this requirement as safety relevant covered by RA-RAMS-37.

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[003]	The absolute value of the Overestimation related to the estimated distance and the absolute value of the Underestimation related to the estimated distance shall be lower than ten meters. surrounding: - An operational stop or speed limitation. - A stop in train station. Surrounding shall be interpreted as +- 500m of a stopping point.	None	-	-	Not RAMS related
SpecSysReq[004]	The absolute value of the Overestimation related to the estimated distance and the absolute value of the Underestimation related to the estimated distance shall be lower than sixty meters anywhere the SpecSysReq[003] requirement is not requested.	None	-	-	Not RAMS related
SpecSysReq[005]	The absolute error of the estimated distance to the reference location shall not exceed 1.25m, for at least 95% of the cases, surrounding: - An operational stop or speed limitation - A stop in train station. Surrounding shall be interpreted as +- 500m of a stopping point.	None	-	-	Not RAMS related

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[006]	The absolute error of the estimated distance calculated by LOC-OB shall not exceed 4m (for at least 95% of the cases), anywhere the SpecSysReq[005] requirement is not requested.	None	-	-	Not RAMS related
SpecSysReq[007]	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)].	**Safety**	D3.2 §3.2	**RA-RAMS-03** and Risk assessment of **LOC-OB_SF-001**	LOC-OB_SF-001 function shall be designed with a TFFR <= 10^{-9}/h
SpecSysReq[008]	The 1D speed (along the track) dataset provided by LOC-OB shall include: - Movement direction - Estimated train speed - Underestimation train speed - Overestimation train speed - Validity timestamp	**Safety**	D3.2 §3.2	Risk assessment of **LOC-OB_SF-002**	LOC-OB_SF-002 function shall be designed with a TFFR <= 10^{-9}/h
SpecSysReq[009]	The confidence interval calculated by LOC-OB (Underestimation of the estimated train speed - Overestimation of the	None	-	-	Not RAMS related

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
	estimated train speed) toward estimated speed shall be better than 2 km/h for speeds lower than 30 km/h, and increasing linearly up to 12 km/h for speeds between 30 km/h and 500 km/h.				
SpecSysReq[010]	The absolute error of the estimated train speed provided by LOC-OB shall not exceed ± 1 km/h for speeds from 0 km/h to 100 km/h and ± 1% * v for speeds from 100 km/h to 500 km/h for at least 95% of the cases.	None	-	-	Not RAMS related
SpecSysReq[011]	The train true speed shall be lower than the LOC-OB computed max safe speed (Estimated train speed + Underestimation train speed) within the most constraining user exported THR.	**Safety**	D3.2 §3.2	**RA-RAMS-04** and Risk assessment of **LOC-OB_SF-002**	LOC-OB_SF-002 function shall be designed with a TFFR <= 10^{-9}/h
SpecSysReq[012]	The 1D acceleration (along the track) dataset provided by LOC-OB shall include: - Estimated train acceleration - Underestimation train acceleration - Overestimation train acceleration - Validity timestamp	**Safety**	D3.2 §3.2	Risk assessment of **LOC-OB_SF-003**	LOC-OB_SF-003 function shall be designed with a TFFR <= 10^{-9}/h

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[013]	The computed confidence interval (Underestimation train acceleration - Overestimation train acceleration) toward the estimated train acceleration shall not exceed 0.2 m/s2.	None	-	-	Not RAMS related
SpecSysReq[014]	The absolute error of the estimated train acceleration shall not exceed 0.05 m/s2 for at least 95% of the cases.	None	-	-	Not RAMS related
SpecSysReq[015]	The train true acceleration shall be included in the LOC-OB computed confidence interval toward the estimated train acceleration within the most constraining user exported THR.	**Safety**	D3.2 §3.2	**RA-RAMS-05** and Risk assessment of **LOC-OB_SF-002**	LOC-OB_SF-003 function shall be designed with a TFFR <= 10^{-9}/h
SpecSysReq[016]	The 3D train position dataset provided by LOC-OB shall include: - 3D Position - 3D Position uncertainty - Coordinate reference system - Validity timestamp	None	-	-	Not RAMS related ***See section 5.2***
SpecSysReq[017]	The absolute error of the estimated 3D position shall not exceed 1,25 m for at least 95% of the cases.	None	-	-	Not RAMS related

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[018]	The 3D train velocity dataset provided by LOC-OB shall include: - 3D Velocity - 3D Velocity uncertainty - Validity timestamp	None	-	-	Not RAMS related ***See section 5.2***
SpecSysReq[019]	The absolute error of the estimated 3D train velocity shall not exceed 2 km/h on each axis of the 3D reference frame (refer to definitions) for at least 95% of the cases.	None	-	-	Not RAMS related
SpecSysReq[020]	The 3D train acceleration dataset provided by LOC-OB shall include: - 3D Acceleration - 3D Acceleration uncertainty - Validity timestamp	None	-	-	Not RAMS related ***See section 5.2***
SpecSysReq[021]	The absolute error of the estimated 3D train acceleration shall not exceed 0.05 m/s2 on each axis in the 3D reference frame (refer to definitions) for at least 95% of the cases.	None	-	-	Not RAMS related
SpecSysReq[022]	The train attitude (rotational angles) dataset provided by LOC-OB shall include: - Attitude - Attitude uncertainty - Angular rate - Angular rate uncertainty - Validity timestamp	None	-	-	Not RAMS related ***See section 5.2***

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[023]	The absolute error of the estimated attitude (rotational angles) shall not exceed 0,1° for yaw, and 0,5° for pitch and roll for at least 95% of the cases.	None	-	-	Not RAMS related
SpecSysReq[024]	The dataset toward estimated distance travelled provided by LOC-OB shall include: - Estimated distance travelled - Estimated distance max - Estimated distance min - Validity timestamp	Safety	D3.2 §3.2	Risk assessment of **LOC-OB_SF-008**	Loc-OB-OP-19: The users of the estimated distance in safety (output of LOC-OB-SF-008) has not been identified.
SpecSysReq[025]	Only if safety is not to be compromised, LOC-OB shall not provide a sudden variation of the position and the speed confidence intervals that leads to brake intervention or trip (TR) mode. The increase of the confidence interval shall allow the train to adapt its behaviour to avoid emergency braking.	None	-	-	Not RAMS related
SpecSysReq[027]	LOC-OB, from the train power on, shall initialise itself and provide the outputs with no human supervision.	None	D3.5	**RA-RAMS-35**	D3.5 considers this as requirement as safety related : RA-RAMS-35.
SpecSysReq[028]	After being powered up and its initialisation stage ended, LOC-OB shall provide data continuously.	None	D3.5	**RA-RAMS-36**	D3.5 considers this as requirement as safety related : RA-RAMS-36 This is to be confirmed by further analysis.

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[029]	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.	None	-	-	Not RAMS related
SpecSysReq[030]	After the LOC-OB is powered-on, it shall fulfil entire operational 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.	None	-	-	Not RAMS related

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[031]	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.	None	D3.5	**RA-RAMS-38**	D3.5 considers this as requirement as safety related: RA-RAMS-38 This is to be confirmed by further analysis.
SpecSysReq[032]	LOC-OB dataset time validity shall not exceed 200 ms when transferred to users.	None	-	-	Not RAMS related
SpecSysReq[033]	LOC-OB shall provide the processed dataset with a frequency at least equal to 10Hz.	None	-	-	Not RAMS related
SpecSysReq[034]	LOC-OB shall embed a safe and secure mechanism to detect delays and time incoherencies within the most constraining user exported THR.	**Safety**	D3.4 §3.4	**RA-RAMS-FTA-04**	**RA-RAMS-FTA-04** gives a quantified TFFR
SpecSysReq[035]	LOC-OB, equipment user and equipment provider shall use data exchange mechanisms in accordance with the safety, security and interoperability requirements.	**Safety**	D3.4 §3.4	**RA-RAMS-FTA-01**	Full coverage
SpecSysReq[036]	LOC-OB shall provide its dataset in compliance with the future TSI through the SCI - Vehicle Locator (SCI-VL) interface.	None	D3.4 §3.4	**RA-RAMS-FTA-02**	Contrary to the assumption of WP2, the WP3 analysis assumes this requirement is safety related: A safe protocol, ideally standardized, shall be defined to provide in safety the outputs.

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[037]	If needed, LOC-OB shall acquire the Digital Map in accordance with the future TSI through the SCI - Map Repository On-Board (SCI-REP-OB) interface.	None	D3.4 §3.4	**RA-RAMS-FTA-03**	Contrary to the assumption of WP2, the WP3 analysis assumes this requirement is safety related.
SpecSysReq[038]	If available and needed by LOC-OB, LOC-OB shall acquire the train routing information (Movement authority, journey profile or switch information etc) in accordance with the future TSI through the SCI - Route Control (SCI-RC) interface.	**Safety**	D3.4 §3.4	**RA-RAMS-FTA-03**	**RA-RAMS-FTA-03** gives a quantified TFFR
SpecSysReq[039]	If available and needed, LOC-OB shall comply with the future TSI concerning the use of the Augmentation Data (definition of the dataset and exchange mechanism) through the SCI - Augmentation (SCI-AUG) interface.	None	D3.4 §3.4	**RA-RAMS-FTA-03**	Contrary to the assumption of WP2, the WP3 analysis assumes this requirement is safety related.
SpecSysReq[040]	If available and needed by LOC-OB, LOC-OB shall comply with the future TSI concerning the use of Train integrity status. (Definition of the dataset and exchange mechanism) through the SCI - Train Control Management System (SCI-TCMS) interface.	None	D3.4 §3.4	**RA-RAMS-FTA-03**	Contrary to the assumption of WP2, the WP3 analysis assumes this requirement is safety related.
SpecSysReq[041]	If existing, LOC-OB shall acquire the train static configuration from the common on-board Configuration Data Storage (CDS) component through the SCI - Configuration Data Storage (SCI-CDS) interface. Otherwise, specific static configuration	None	D3.4 §3.4	**RA-RAMS-FTA-03**	Contrary to the assumption of WP2, the WP3 analysis assumes this requirement is safety related.

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
	information shall be managed as an internal component of LOC-OB.				
SpecSysReq[042]	If needed, LOC-OB shall acquire the dynamic train configuration, as active cab, train length, rigid definition of the primary moving direction, or definition of trains front end from Train Control Management System (TCMS) through the SCI - Operational Data Storage (SCI-ODS) interface.	None	D3.4 §3.4	**RA-RAMS-FTA-03**	Contrary to the assumption of WP2, the WP3 analysis assumes this requirement is safety related.
SpecSysReq[043]	If needed and available, LOC-OB shall acquire the EUB Telegram in accordance with the future TSI through the SCI - Physical ETCS Transponder Service (SCI-PETS) interface.	None	D3.4 §3.4	**RA-RAMS-FTA-03**	Contrary to the assumption of WP2, the WP3 analysis assumes this requirement is safety related.
SpecSysReq[044]	If needed, LOC-OB shall use the LRBG reference provided by ETCS through the SCI - Vehicle Supervisor (SCI-VS) interface.	None	D3.4 §3.4	**RA-RAMS-FTA-03**	Contrary to the assumption of WP2, the WP3 analysis assumes this requirement is safety related.
SpecSysReq[045]	If needed, LOC-OB shall use the reference points defined in the Digital Map through the SCI-VS interface.	None	D3.4 §3.4	**RA-RAMS-FTA-03**	Contrary to the assumption of WP2, the WP3 analysis assumes this requirement is safety related.
SpecSysReq[046]	If available and needed, LOC-OB shall comply with the future TSI concerning the use of Cold Movement information.	None	D3.4 §3.4	**RA-RAMS-FTA-03**	Contrary to the assumption of WP2, the WP3 analysis assumes this requirement is safety related.

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
	(Definition of the dataset and exchange mechanism).				
SpecSysReq[047]	The LOC-OB hardware shall comply with the overall CCS-OB reliability as defined in Ref [57] Chapter 2. Minor failure: λ <1,25 10-4/h. Reduced service failure: λ < 3,3 10-6/h. Immobility failure: λ < 3,7 10-7/h.	**Reliability**	D3.6	D3.6 §3.1 and §7	Covered by the analysis of D3.6 (see failure trees of the chapter 4.5.1, 4.5.2 and 4.5.3 and the summary of chapter 7).
SpecSysReq[048]	If the confidence intervals are larger than the acceptable position confidence interval (position), maximum acceptable speed confidence interval (speed) or maximum acceptable acceleration confidence interval (acceleration) for a cumulative 60 seconds (or more) for two hours, the time is accounted in the overall LOC-OB unavailability.	**Availability**	D3.6	None	The WP3 analysis did not cover this requirement. Functionalities or properties have to be developed in future projects before it can be evaluated.
SpecSysReq[049]	The LOC-OB shall have an overall availability of 99,998% during operation.	**Availability**	D3.6	D3.6 §3.2 and §7	Covered by the analysis of D3.6 (see the determination of availability of chapter 6 and the summary of chapter 7).
SpecSysReq[050]	LOC-OB shall manage useful data toward maintenance in an internal log memory and through the SCI - Monitoring, Diagnostic, Configuration, Maintenance On-Board (SCI-MDCM-OB) interface.	**Maintainability**	D3.6	None	The WP3 analysis did not cover this requirement. Functionalities or properties must be developed in future projects before it can be evaluated.

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[051]	LOC-OB shall be designed as a generic application (cf.EN50126 [5] [6]).	**Maintainability**	D3.6	None	The WP3 analysis did not cover this requirement. Functionalities or properties have to be developed in future projects before it can be evaluated.
SpecSysReq[052]	LOC-OB shall be designed to ease software updates (including security patches) by avoiding complex workshop procedures requiring bench testing.	**Maintainability**	D3.	None	The WP3 analysis did not cover this requirement. Functionalities or properties have to be developed in future projects before it can be evaluated.
SpecSysReq[054]	The LOC-OB's design and maintenance concept shall meet a Mean Time To Restore (MTTR) ≤ 1h.	**Maintainability**	D3.6	D3.6 §3.3 and §7	Covered by the analysis of D3.6 (see the determination of maintainability of chapter 5.1 and the summary of chapter 7).
SpecSysReq[055]	Preventive maintenance or periodic sensor calibration period of the overall LOC-OB shall exceed 2 years.	**Maintainability**	D3.6	D3.6 §3.3 and §7	Covered by the analysis of D3.6 (see the preventive maintenance and determination of the MTTPM and MTBPM of the LOC-system of chapter 5.2 and the summary of chapter 7).
SpecSysReq[056]	The safety of the LOC-OB shall be ensured and demonstrated according to the Common Safety Methods (cf. Ref [34]) and the EN 50126 standard (cf. Ref [5] and Ref [6]).	**Safety**	D3.2 §3.2	**RA-RAMS-01**	Full coverage

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[057]	If needed, calibration procedure(s) shall fulfil with the safety requirement.	**Safety**	None	None	Coverage of this requirement is not done in WP3, however safety aspect of calibration is discussed in §5.5 related to the FDE mechanisms.
SpecSysReq[058]	LOC-OB shall fulfil requirements and recommendations for cybersecurity as specified in CLC/TS 50701 (cf. Ref [36]) with the purpose of demonstrating that the system is up to date from a cybersecurity perspective and that it meets and maintains the target level of security for the entire system life cycle.	**Security**	-	-	Not RAMS but Security related Out of the scope of WP3
SpecSysReq[059]	LOC-OB components shall comply with applicable environmental standards.	None	D3.2 §3.2	**RA-RAMS-07**	Contrary to the assumption of WP2, the WP3 analysis +assumes this requirement is safety related.
SpecSysReq[060]	LOC-OB components shall comply with the Ref [42] standard: Railway applications - Fire protection on railway vehicles. The latest edition shall apply.	**Safety**	D3.2 §3.2	**RA-RAMS-07**	Full coverage
SpecSysReq[061]	LOC-OB components shall comply with the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) and RoHS2 directives. The latest edition shall apply.	**Safety**	D3.2 §3.2	**RA-RAMS-07**	Full coverage

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[066]	If LOC-OB cannot guarantee safe operation due to internal safety process faults (for ex: safe computer failure): LOC-OB shall not provide any information to the users.	**Safety**	D3.3 §3.3	**RA-RAMS-FMEA-02**	Full coverage
SpecSysReq[067]	LOC-OB shall log overall availability issues and specific relevant events as timestamped events.	**Maintainability**	D3.6	None	The WP3 analysis did not cover this requirement. Functionalities or properties have to be developed in future projects before it can be evaluated.
SpecSysReq[068]	If LOC-OB is unable to produce data within the awaited THR due to insufficient information to guarantee safe results (one or several sensor failure or unavailability), LOC-OB shall provide a default invalid value for the data concerned and shall provide all other data as specified.	**Safety**	D3.3 §3.3	**RA-RAMS-FMEA-03 RA-RAMS-FMEA-04 RA-RAMS-FMEA-05**	Full coverage
SpecSysReq[069]	LOC-OB computed localisation data shall be considered unsafe if: • The LOC-OB (including all sensors) is not located in the front of the train (cab) AND • The train consists of coupled wagons, locomotives, etc. AND • Train integrity is not confirmed	**Safety**	-	-	This requirement has not been analyzed during the project as the integration of the LOC-OB system in a train, and the configuration of the train were out of the scope of the demonstrator in this project. ***See section 5.2***

Req ID	Requirement	RAMSS related from WP2 assumption	WP3 Task coverage	Coverage Id	Coverage comments from WP3 on RAMSS allocation
SpecSysReq[070]	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.	**Safety**	D3.2 §3.2	**RA-RAMS-08** and Risk assessment of **LOC-OB_SF-001**	LOC-OB_SF-001 function shall be designed with a TFFR <= 10^{-9}/h
SpecSysReq[071]	LOC-OB shall take into consideration each sensor specific challenging environmental condition and each sensor failure mode to perform in all situations not considered as incredible or Improbable.	**Safety**	D3.3 §3.3	**RA-RAMS-FMEA-16**	
SpecSysReq[072]	If the LOC-OB does not provide data at the defined rate, the LOC-OB is considered as unavailable during this time.	**Availability**	D3.6	-	The WP3 analysis did not cover this requirement. Functionalities or properties must be developed in future projects before it can be evaluated.

Table 2: System Specification requirements of LOC-OB extracted from D2.4 [R3] and coverage by WP3 analysis

3 RAMS REQUIREMENTS ISSUED FROM WP3

3.1 RAMS Plan (D3.1)

The deliverable D3.1 [R4] has described the safety activities which will be carried out as part of the CLUG 2.0 project. It explains, among other things, the objectives, the methodology used, the required inputs and actors involved in each task of WP3.

The safety studies carried out as part of tasks T3.2 to T3.6 will allow measuring the remaining work to be performed in terms of safety activities to obtain a certifiable product. These results are synthetized in the sequel of this chapter.

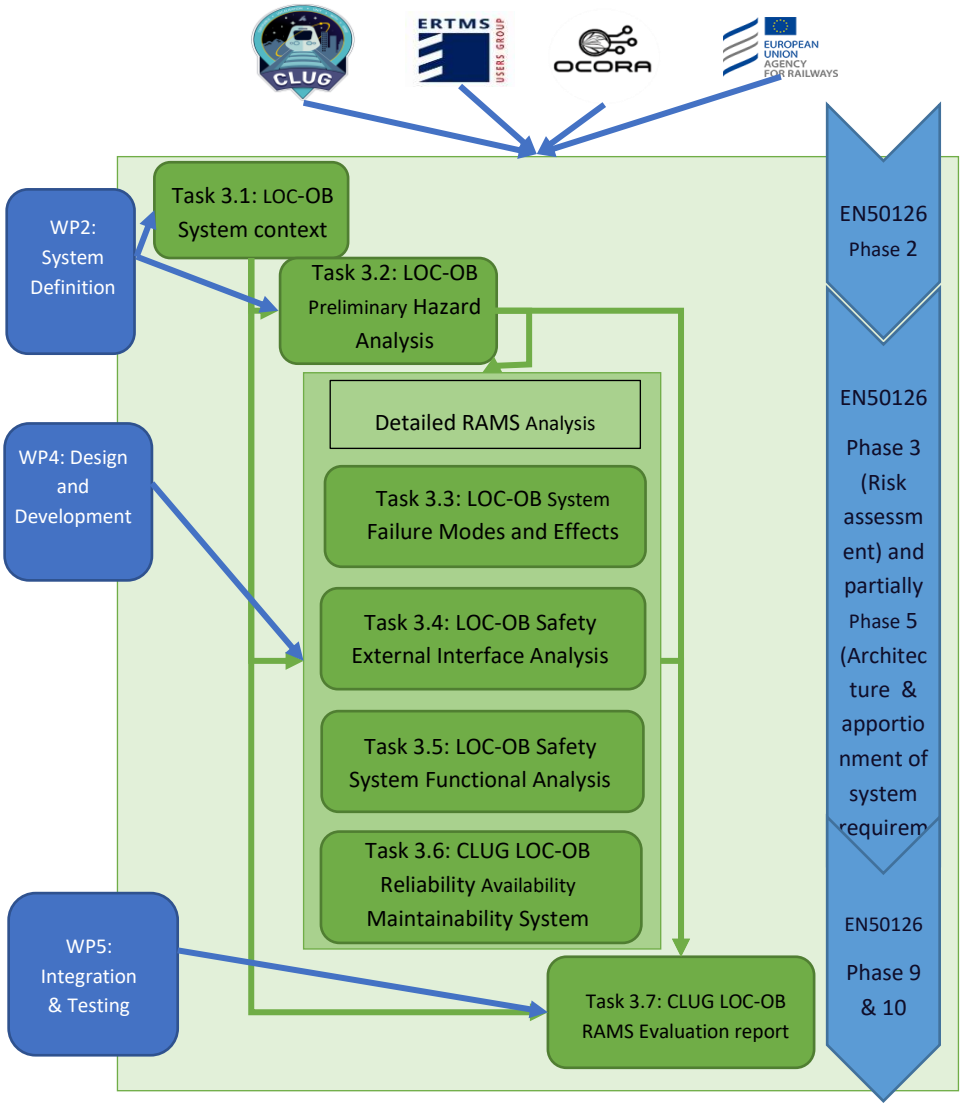

Figure 1 – WP3 tasks organisation

However, as the aim of CLUG 2.0 is to develop a demonstrator and not an industrial and market-ready system, only the early phases described in the EN50126-1 and related to Phase 2 “System definition and Operational Context”, “Phase 3: Risk analysis and evaluation” and “Phase 5: Architecture and apportionment of system requirements” are covered by the activities of WP3. The remaining steps to obtain a certifiable product are discussed in §4.

3.2 PHA results (D3.2)

The deliverable D3.2 [R5] has provided a preliminary safety analysis of the LOC-OB system, identifying hazards, accessing the severity of the potential accidents and identifying safeguards for reducing the risks associated with the hazards.

It is based on the description of the LOC-OB system given in D2.1 [R1] and D2.3 [R2].

The hazards were identified using several approaches in parallel to ensure optimum coverage:

- Analysis of the results for ERTMS/ETCS system based on Subset 091 [R34] and Subset 088 [R33].
- Analysis based on user needs or to functions not covered by the current Subsets.
- Analysis of the new technologies and new services related to the LOC-OB system.
- Analysis based on classical railway accident, which has confirmed the results of the previous analyses.

This work enables to conclude about the TFFR level expected for the LOC-OB output functions. Based on current assumptions of the on-board CCS system, all functions providing 1D data must be implemented with a SIL4 safety level, as they are needed by the users for critical functions. For the functions providing 3D data, the user needs are not sufficient to conclude to a defined safety level. This point will be discussed in section 5.2.

In the sequel, we discuss through several tables the coverage of D3.2 results and assumptions by the design (WP4) and the tests (WP5) deliverables.

The following Risk assessment of the output functions is identified in the PHA:

Functions		Feared Events		Design Target TFFR	D3.2 Comments	Coverage in WP4	Coverage in WP5
LOC-OB_SF-001	Provide Safe Train Front End 1D Position Dataset	LOC-OB_FE_03	Fail to provide the correct train orientation	< 10^{-9}/h		In this demonstrator, train orientation need is not covered inWP4 (see D4.1 [R10] §5).	Not covered
		LOC-OB_FE_04	Fail to use the correct reference point information from digital map			The use of a safe reference point provided by the digital map is identified in WP4 (see D4.1 [R10] §5). However, it is to precise how the information is used by the internal functions (See § 5.3 for more details).	Not covered
		LOC-OB_FE_05	Fail to use the correct reference point id			The use of a safe reference point provided by the digital map is identified in WP4 (see D4.1 [R10] §5) but not the reference point received from an external provider (for example the LRBG).	Not covered
		LOC-OB_FE_06	Fail to provide confidence interval which include the real train position (measured distance interval and position qualifier and reference point id and track edge id)		Related to **RA-RAMS-03**	The definition of a safe confidence interval containing the real position of the train is considered as a major goal in D4.1 [R10] and detailed by the detailed function description D4.6 [R14] and D4.7 [R15].	Test of SpecSysReq[007] (related to RA-RAMS-03) is considered in D5.2.2 §3.2 and §5.1 [R17]. However, safety aspects are not considered by the test plan.
		LOC-OB_FE_17	*Fail to provide the correct track edge id*		Related to **RA-RAMS-08**	The definition of the track edge id of the train is considered as a major goal in D4.1 [R10] and detailed by the detailed	Test of SpecSysReq[002] (related to RA-RAMS-08) is considered in D5.2.2 §3.2 [R17].

Functions		Feared Events		Design Target TFFR	D3.2 Comments	Coverage in WP4	Coverage in WP5
						function description D4.6 [R14] and D4.7 [R15]. The notion of correct track edge id is to be defined in the future: the track edge id is not always unique as the confidence interval can cover two track edge.	However, safety aspects are not considered by the test plan: see in D5.2.2 §3.2 [R17] coverage of SpecSysReq[070]
LOC-OB_SF-002	1D speed with safe confidence interval	LOC-OB_FE_01	Fail to provide upper bound speed higher than the actual train speed	$< 10^{-9}$/h	Related to **RA-RAMS-04**	The definition of a safe confidence interval containing the actual speed of the train is considered as a major goal in D4.1 [R10] and detailed by the detailed function description D4.6 [R14] and D4.7 [R15].	Test of SpecSysReq[011] (related to RA-RAMS-04) is considered in D5.2.2 §3.2 and §5.1 [R17]. However, safety aspects are not considered by the test plan.
		LOC-OB_FE_02	Fail to provide the correct train movement direction			The definition train movement is considered in D4.1 [R10] as defined in the ICD [R18].	Test of SpecSysReq[011] (related to RA-RAMS-04) is considered in D5.2.2 §3.2 and §5.1 [R17]. However, safety aspects are not considered by the test plan.
LOC-OB_SF-003	1D acceleration with safe confidence interval.	LOC-OB_FE_07	Fail to provide lower bound acceleration lower than the actual train acceleration	$< 10^{-9}$/h	Related to **RA-RAMS-05**	The definition of a safe confidence interval containing the actual acceleration of the train is considered as a major goal in D4.1 [R10] and detailed by the detailed function description D4.6 [R14] and D4.7 [R15].	Test of SpecSysReq[015] (related to RA-RAMS-05) is considered in D5.2.2 §3.2 and §5.1 [R17]. However, safety aspects are not considered by the test plan.

Functions		Feared Events		Design Target TFFR	D3.2 Comments	Coverage in WP4	Coverage in WP5
LOC-OB_SF-004	Provide 3D Position and Uncertainty	LOC-OB_FE_09	Fail to provide 3D position uncertainty which include the real train position	Not evaluated	There are no sufficient inputs of the use of the 3D Position and Uncertainty to confirm the TFFR	Not evaluated	Not evaluated
LOC-OB_SF-005	Provide 3D Velocity and Uncertainty	LOC-OB_FE_10	Fail to provide 3D speed uncertainty which include the actual train speed	Not evaluated	There are no sufficient inputs of the use of the 3D Velocity and Uncertainty to confirm the TFFR	Not evaluated	Not evaluated
LOC-OB_SF-006	Provide 3D Acceleration and Uncertainty	LOC-OB_FE_11	Fail to provide 3D acceleration uncertainty which include the actual train acceleration	Not evaluated	There are no sufficient inputs of the use of the 3D Acceleration and Uncertainty to confirm the TFFR	Not evaluated	Not evaluated
LOC-OB_SF-007	Provide 3D Attitude (Rotational Angles) and Uncertainty	LOC-OB_FE_08	Fail to provide 3D vehicle attitude which include the real train position	Not evaluated	There are no sufficient inputs of the use of the 3D Vehicle attitude to confirm the TFFR	Not evaluated	Not evaluated
LOC-OB_SF-008	Provide Estimated Distance	None	The PHA does not identified feared events related to this function	Not evaluated	Loc-OB-OP-19: The users of the estimated distance (output of LOC-OB-	Not evaluated	Not evaluated

Functions		Feared Events		Design Target TFFR	D3.2 Comments	Coverage in WP4	Coverage in WP5
	Travelled (since power on)				SF-008) has not been identified. However, this can be considered for STM.		

Table 3: Feared events related to LOC-OB output functions extracted from D3.2 [R5]

However, the assessment of the hazards and the functions are limited by the lack, due to the research context of CLUG 2.0, of a precise description of the user needs and the environment of the LOC-OB system. See § 5.2 for discussion on this subject.

A set of Safety requirements has been deduced from the PHA and are listed in the Table 4.

Id	RAMS requirements	WP4 Task coverage	Coverage comments
RA-RAMS-01	The safety of the LOC-OB shall be ensured and demonstrated according to the Common Safety Methods [ERA CSM] and the [EN 50126] standard.	None	In the scope of CLUG 2.0 only a demonstrator is provided. The full process to achieve a certifiable solution has not been defined. See §4 For more details
RA-RAMS-02	LOC-OB shall not degrade safety toward odometry as defined in the ETCS BL3 R2.	None	In the scope of CLUG2.0 only a demonstrator is provided. The full process to achieve a certifiable solution has not been defined. This process shall cover interoperability requirements and ensur the system safety in regards of TSI (BL4 for the future systems). See §4 For more details
RA-RAMS-03	The true train position shall be always inside the confidence interval.	D4.1 D4.7 in §3	One of the entry elements of D4.7 is the fact that the true train position shall be in the confidence interval. However, a demonstration that the function shall provide in safety this information should be done.
RA-RAMS-04	The true train speed shall be always inside the confidence interval.	D4.1 D4.7 in §3	One of the entry elements of D4.7 is the fact that the actual train speed shall be in the confidence interval. However, a demonstration that the function shall provide in safety this information should be done.
RA-RAMS-05	The true train acceleration shall be always inside the confidence interval.	D4.1 D4.7 in §3	One of the entry elements of D4.7 is the fact that the actual train acceleration shall be in the confidence interval. However, a demonstration that the function shall provide in safety this information should be done.

Id	RAMS requirements	WP4 Task coverage	Coverage comments
RA-RAMS-06	Each localisation information shall fulfil safety target requirements in accordance with the consumer's application requirements.	D3.3, D3.4	More detailed safety analysis has been performed in D3.3 and D3.4 but as the HW architecture and validation step are out of the scope of the project, no safety demonstration can be given. This is discussed in § 4
RA-RAMS-07	Loc-OB shall respect some standards EN 50121 EN 50125.	None	In the scope of CLUG2.0 only a demonstrator is provided. The full process to achieve a certifiable solution has not been defined. See §4 For more details
RA-RAMS-08	The track edge ID provided by LOC-OB shall always be the track edge occupied by the train front end real position.	D4.1 D4.7 in §3	One of the entry elements of D4.7 is the fact that the actual train acceleration shall be in the confidence interval. However, a demonstration that the function shall provide in safety this information should be done. The track edge id is not always unique as the confidence interval can cover two track edge.

Table 4: Safety requirements of LOC-OB (extract from D3.2 [R5])

The following Safety Related Application Conditions (SRAC) are identified in the PHA:

Id	SRAC	Receiver	Coverage ID	Coverage comments
Loc-OB-SRAC-01	The input from Cold Movement Detector (CMD) shall be safe (THR < 10-9/h)	CMD function provider	See ODO-5	No cold movement detection is a feared event defined in subset 91 [R34], thus this information is expected at a high safety level.
Loc-OB-SRAC-02	The Reference point shall be a safe input of Loc-OB System (THR < 10-9/h)	System who provides the reference point	See KERNEL-7	Incorrect LRBG is a feared events defined in subset 91 [R34], thus by analogy Reference point is expected at a high level of safety.

Id	SRAC	Receiver	Coverage ID	Coverage comments
Loc-OB-SRAC-03	If the BTM information is used by Loc-OB, the BTM information shall be safe (THR < 10-9/h)	BTM system	See KERNEL-1, KERNEL-2, KERNEL-7	Information provided by BTM are expected in Safety by ETCS in the current version of subset 26 [R32], See [R33] and [R34].
Loc-OB-SRAC-04	The LOC-OB uses a safe digital map as input (THR < 10-9/h, worst case assumed)	Digital map	See OCORA documents	The preliminary studies on digital map request that it will be provided in safety see, OCORA architecture documents for example [R35], [R36] and [R37].

Table 5: SRAC of LOC-OB (extract from D3.2 [R5])

The following assumptions are identified during the PHA of the LOC-OB.

Id	Assumptions	Coverage ID	Coverage comments
LOC-OB-Ass-01	The Standstill function is not provided by the LOC-OB system	None	To check on the target architecture of the train.
LOC-OB-Ass-02	1D position function gives the distance related to a reference point	See SpecSysReq[001]	It is in the definition to the position dataset.
LOC-OB-Ass-03	It is assumed that there is no loop between Cold Movement Detector (CMD) system and LOC-OB system to avoid common mode	None	To check on the target architecture of the train.
LOC-OB-Ass-04	The new feared events of Subset 091 (TCS 2023) are taken into account in this PHA (ODO-5, KERNEL-35, KERNEL-36)	See D3.2	See the PHA appendix, this feared event is taken into account in the PHA.
LOC-OB-Ass-05	It is assumed that the LOC-OB system does not share the same sensors than the system supporting the standstill function to avoid common mode failure	None	To check on the target architecture of the train. If Standstill information is not used by LOC-OB this assumption is not relevant (no common mode).

Id	Assumptions	Coverage ID	Coverage comments
LOC-OB-Ass-06	CTMS is designed with basic integrity	See section 5.2	The use cases and user need of this component have not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-Ass-07	MA computation by TPS (trackside) is based essentially on the localisation report provided to trackside by on-board	See section 5.2	The use cases and user need of this component have not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-Ass-08	TPS (trackside) provides safety MA information or request on-sight mode as soon as its input are not unavailable or checked.	See section 5.2	The use cases and user need of this component have not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-Ass-09	As soon an object is detected, without sufficient information, a safe reaction is launched by the Perception system	See section 5.2	The use cases and user need of this component have not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-Ass-10	ATO is a Basic Integrity system, with TPS is supervising in safety the ATO functions	See section 5.2	The use cases and user need of this component have not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-Ass-11	If ATO has not sufficient information, a safety speed profile and stopping point is computed	See section 5.2	The use cases and user need of this component have not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-Ass-12	TPS control function are SIL4 and based only on LOC-OB output for localisation	See section 5.2	The use cases and user need of this component have not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-Ass-13	If TPS does not receive localisation information during a given time, emergency brake is commanded	See section 5.2	The uses cases and user need of this component have not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-Ass-18	Perception is a SIL2 system, with TPS controlling the Perception	See section 5.2	The uses cases and user need of this component have not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-Ass-19	It is assumed that TPS detects reverse movement and computes backward distance from the 1D position provided by LOC-OB	See section 5.2	The uses cases and user need of this component have not yet been clearly identified and shall be confirmed for further analysis.

Id	Assumptions	Coverage ID	Coverage comments
LOC-OB-Ass-20	LOC-OB sends information in safety to TPS to release route and compute the MA	See section 5.2	The uses cases and user need of this component have not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-Ass-21	DR only needs the 1D position (including movement direction) to provide the relevant reliable map (being DR system in charge of checking and ensuring that the provided map part is relevant).	See section 5.2	The uses cases and user need of this component have not yet been clearly identified and shall be confirmed for further analysis.

Table 6: Assumptions on LOC-OB (extract from D3.2 [R5])

Note: In the table above, TPS (trackside) means only the trackside system, TPS only means the onboard system.

3.3 FMEA results (D3.3)

The deliverable D3.3 [R6] provides a functional safety analysis of the LOC-OB system, identifying how the failure of the internal functions of the LOC-OB system shall be designed to cover the safety requirements already identified in the previous works, D2.1 [R1], D2.4 [R3] and D3.2 [R5]. This qualitative analysis discusses, by a classical FMEA approach, how the failure of an internal function leads to the failure of the LOC_OB system to provide its outputs.

Besides, it reuses the results of the apportionment and FTA analysis done in D3.4 [R7] and remind in section 3.4.

In the sequel we discuss through several tables the coverage of D3.3 requirements and assumptions by the design (WP4) and the tests (WP5) deliverables.

Id	RAMS requirements	Coverage ID	Coverage comments
RA-RAMS-FMEA-02	If LOC-OB cannot guarantee safe operation due to internal process failure, LOC-OB shall not provide any information to the users and shall be isolated.	None	See SpecSysReq[066] In the scope of CLUG 2.0 only a demonstrator is provided. The full process to achieve a certifiable solution has not been defined. See §4 For more details

Id	RAMS requirements	Coverage ID	Coverage comments
RA-RAMS-FMEA-03	If LOC-OB is unable to produce a position confidence interval, such that the real position of the train is guaranteed to be inside this confidence interval (e.g. due to one or several sensor failure or unavailability or incorrect parameters), LOC-OB shall provide a default invalid value for the position confidence interval.	None	See SpecSysReq[068] and **RA-RAMS-03** In the scope of CLUG 2.0 only a demonstrator is provided. The full process to achieve a certifiable solution has not been defined. See §4 For more details
RA-RAMS-FMEA-04	If LOC-OB is unable to produce a speed confidence interval, such that the real speed of the train is guaranteed to be lower than the upper bound of this confidence interval (e.g. due to one or several sensor failure or unavailability or incorrect parameters), LOC-OB shall provide a default invalid value for the speed confidence interval.	None	See SpecSysReq[068] and **RA-RAMS-04** In the scope of CLUG 2.0 only a demonstrator is provided. The full process to achieve a certifiable solution has not been defined. See §4 For more details
RA-RAMS-FMEA-05	If LOC-OB is unable to produce an acceleration confidence interval, such that the real acceleration of the train is greater than the lower bound of this confidence interval (e.g. due to one or several sensor failure or unavailability or incorrect parameters), LOC-OB shall provide a default invalid value for the acceleration confidence interval.	None	See SpecSysReq[068] and **RA-RAMS-05** In the scope of CLUG 2.0 only a demonstrator is provided. The full process to achieve a certifiable solution has not been defined. See §4 For more details
RA-RAMS-FMEA-12	The ***LOC_OB_SF-306*** GNSS and SBAS Measurement and FDE function shall be designed in safety with mechanism to detect the errors of the measurements (e.g. duplication of sensors, fault-detection algorithms, …)	D4.1 in §2.3.1 D4.2	One of the aims of D4.2 is the description of the FDE related to the GNSS measurement. However, a demonstration that the function shall provide in safety this information should be done.

Id	RAMS requirements	Coverage ID	Coverage comments
RA-RAMS-FMEA-13	The ***LOC_OB_SF-307*** IMU Measurement and FDE function shall be designed in safety with mechanism to detect the errors of the measurements (e.g. duplication of sensors, fault-detection algorithms,…)	D4.1 in §2.3.2 D4.3	One of the aims of D4.3 is the description of the FDE related to the IMU measurement. However, a demonstration that the function shall provide in safety this information should be done.
RA-RAMS-FMEA-14	The ***LOC_OB_SF-308*** Wheel sensors Measurement and FDE function shall be designed in safety with mechanism to detect the errors of the measurements (e.g. duplication of sensors, fault-detection algorithms,…)	D4.1 in §2.3.3 D4.4	One of the aims of D4.4 is the description of the FDE related to the wheel sensors measurement. However, a demonstration that the function shall provide in safety this information should be done.
RA-RAMS-FMEA-16	The ***LOC_OB_SF-303*** System Data FDE function shall be designed to detect and eliminate the fault in the measurement's inputs. In particular it shall take into consideration each sensor specific challenging environmental condition and each sensor failure mode to perform in all situations not considered as incredible or Improbable.	D4.1 in §2.3.3 D4.6	See SpecSysReq[071] One of the aims of D4.6 is the description of the system FDE related to comparison of the different kind of measurements. However, a demonstration that the function shall provide in safety this information should be done.

Table 7: List of safety requirements identified in the FMEA

The following Safety Related Application Conditions (SRAC) are identified in the FMEA:

Id	SRAC	Receiver	Coverage ID	Coverage comments
Loc-OB-SRAC-FMEA-01	In case of omission of outputs provided by the LOC-OB, a safe reaction is expected from the users	Users of the safety outputs	None	To check on the target architecture of the train and the potential users

Table 8: SRAC identified in the FMEA

The table presents the synthesis of assumptions identified during this analysis of the LOC-OB.

Id	Assumptions	Coverage ID	Coverage comments
LOC-OB-Ass-FMEA-02	The function LOC_OB_SF-305 covered the specific processing on the map data made in the core of the LOC-OB system. Map Data is provided by the function LOC_OB_SF-101.		Already defined in D3.4 [R7] See §3.4, LOC-OB-FTA-Ass-23
LOC-OB-Ass-FMEA-03	In the document D3.3 the measurement functions cover the sensors, measurement algorithms and Fault detection and exclusion for a given technology.		Already defined in D3.4 [R7] See §3.4, LOC-OB-FTA-Ass-24
LOC-OB-Ass-FMEA-04	For analysis on the chain 2, it is assumed that the second chain need balise information provided in safety by the balise reader.		Already defined in in D3.4 [R7] See §3.4, LOC-OB-FTA-Ass-30

Table 9: Assumption used for the FMEA

3.4 External interfaces analysis results (D3.4)

The deliverable D3.4 [R7] provides a high level external interfaces safety analysis but largely completed by a safety functional system analysis of the LOC-OB system, identifying how the exchanges between the LOC-OB system and its environment and the internal functional blocks shall be designed to cover the safety requirements already identified in the previous works, D2.1 [R1], D2.4 [R3] and D3.2 [R5]. This analysis provides too, via an apportionment approach, indications on the selection of safety targets expected on the input measurement to achieve the TFFR expected on the output functions.

The analyses defined in this document are based on the description of the LOC-OB system given in D2.3 [R2] and in D4.1 [R10], in one case with only one chain of computation and in the second case with two chains and a combiner function.

In the sequel we discuss through several tables the coverage of D3.3 requirements and assumptions by the design (WP4) and the tests (WP5) deliverables.

First the safety requirements related to the apportionment according to Archi_1, i.e. the architecture with only one computation chain:

Id	RAMS requirements	Coverage ID	Coverage comments
RA-App-Archi_1-01	For Archi_1, the LOC_OB_SF-301 Compute Navigation function shall be designed in SIL4 with a TFFR ≤ 0.25e-9 per hour on the output	D4.1 §6.4	D4.1 provides a discussion on the feasibility to develop the core function of the system in SIL4 in the case of a one chain architecture.
RA-App-Archi_1-02	For Archi_1, the LOC_OB_SF-302 Compute Integrity function shall be designed in SIL4 with a TFFR ≤ 0.25e-9 per hour on the output	D4.1 §6.4	D4.1 provides a discussion on the feasibility to develop the core function of the system in SIL4 in the case of a one chain architecture.
RA-App-Archi_1-03	For Archi_1, the LOC_OB_SF-303 System Data FDE function shall be designed in SIL4 with a TFFR ≤ 0.5e-10 per hour on the output	D4.1 §6.4	D4.1 provides a discussion on the feasibility to develop the core function of the system in SIL4 in the case of a one chain architecture.
RA-App-Archi_1-04	For Archi_1, the LOC_OB_SF-304 On-Board Measurement function shall be designed in SIL4 with a TFFR ≤ 0.2e-9 per hour on the output	D4.1 §6.4	D4.1 provides a discussion on the feasibility to develop the core function of the system in SIL4 in the case of a one chain architecture.
RA-App-Archi_1-05	For Archi_1, the LOC_OB_SF-305 Map Data Processing function shall be designed in	D4.1 §2.4	D4.1 assumes the map data information is acquired in safety.

Id	RAMS requirements	Coverage ID	Coverage comments
	SIL4 with a TFFR ≤ 0.125e-9 per hour on the output		
RA-App-Archi_1-06	For Archi_1, the LOC_OB_SF-107 Acquire Eurobalise Telegram function shall be designed in SIL4 with a TFFR ≤ 0.125e-9 per hour on the output	D4.1 §2.4	D4.1 assumes the map data information is acquired in safety.

Table 10: List of safety requirements identified for apportionment on Archi_1

Second the safety requirements related to the apportionment according to Archi_2:

Id	RAMS requirements	Coverage ID	Coverage comments
RA-App-Archi_2-01	For Archi_2, the LOC_OB_SF-301 Compute Navigation function shall be designed in SIL2 with a TFFR ≤ 5.8e-6 per hour on the output	D4.1 §6.5	D4.1 provides a discussion on the feasibility to develop the core function of the system in SIL2 in the case of a two chains architecture.
RA-App-Archi_2-02	For Archi_2, the LOC_OB_SF-302 Compute Integrity function shall be designed in SIL2 with a TFFR ≤ 5.8e-6 per hour on the output	D4.1 §6.5	D4.1 provides a discussion on the feasibility to develop the core function of the system in SIL2 in the case of a two chains architecture.
RA-App-Archi_2-03	For Archi_2, the LOC_OB_SF-303 System Data FDE function shall be designed in SIL2 with a TFFR ≤ 0.8e-6 per hour on the output	D4.1 §6.5	D4.1 provides a discussion on the feasibility to develop the core function of the system in SIL2 in the case of a two chains architecture.
RA-App-Archi_2-04	For Archi_2, the LOC_OB_SF-304 On-Board Measurement function shall be designed in SIL2 with a TFFR ≤ 0.5e-5 per hour on the output	D4.1 §6.5	D4.1 provides a discussion on the feasibility to develop the core function of the system in SIL2 in the case of a two chains architecture.
RA-App-Archi_2-05	For Archi_2, the LOC_OB_SF-305 Map Data Processing function shall be designed in SIL4 with a TFFR ≤ 0.15e-9 per hour on the output	D4.1 §2.4	D4.1 assumes the map data information is acquired in safety.

Id	RAMS requirements	Coverage ID	Coverage comments
RA-App-Archi_2-06	For Archi_2, the LOC_OB_SF-107 Acquire Eurobalise Telegram function shall be designed in SIL4 with a TFFR ≤ 0.15e-9 per hour on the output	D4.1 §2.4	D4.1 assumes the map data information is acquired in safety.
RA-App-Archi_2-07	For Archi_2, each chain shall provide safe output functions with TFFR ≤ 1.7e-5 per hour.	D4.1 §6.5	D4.1 provides a discussion on the feasibility to develop the core function of the system in SIL2 in the case of a two chains architecture.
RA-App-Archi_2-08	For Archi_2, the LOC_OB_SF-312 Combiner function shall be designed in SIL4 with a TFFR ≤ 0.3e-9 per hour on the output	D4.1 §6.5	D4.1 identifies the need for a combiner in SIL4 in the case of a two chains architecture.
RA-App-Archi_2-09	In case of two chains with two independent computation functions and two independent sets of sensors, a combiner function shall implement a mechanism to detect and manage the failure of each chain in a given limited time in view to provide safe outputs.	D4.1 §6.5	D4.1 identifies the need for a combiner in SIL4 in the case of a two chains architecture. However, the necessity of a mechanism to detect and manage failure is not discussed. See §5.4 for more details.
RA-App-Archi_2-10	The two chains shall be designed with independent computation functions and independent sets of sensors.	D4.1 §6.5	D4.1 identifies the need for an independent chain of computation in the case of a two chains architecture. However, there is a necessity to clarify the independence of the input. See §5.3 for more details.

Table 11: List of safety requirements identified for apportionment on Archi_2

Finally, the safety requirements related to the interface analysis and the FTA:

Id	RAMS requirements	Coverage ID	Coverage comments
RA-RAMS-FTA-01	LOC-OB, user equipment and provider equipment shall use data exchange mechanisms in accordance with the safety, security and interoperability requirements.	None	In the scope of CLUG 2.0 only a demonstrator is provided. The full process to achieve a certifiable solution has not been defined. See §4 For more details
RA-RAMS-FTA-02	LOC-OB shall provide its dataset in compliance with the future TSI through the SCI - Vehicle Locator (SCI-VL) interface with a 1.0e-9 ≤ TFFR < 1.0e-8 per hour.	None	In the scope of CLUG 2.0 only a demonstrator is provided. The full process to achieve a certifiable solution has not been defined. See §4 For more details
RA-RAMS-FTA-03	LOC-OB shall receive in safety data set from the neighbours' on-board system in compliance with the future TSI through the dedicated SCI interfaces with a 1.0e-9 ≤ TFFR < 1.0e-8 per hour.	None	In the scope of CLUG 2.0 only a demonstrator is provided. The full process to achieve a certifiable solution has not been defined. See §4 For more details
RA-RAMS-FTA-04	LOC-OB shall embed a safe and secure mechanism to detect delays and time incoherencies a 1.0e-9 ≤ TFFR < 1.0e-8 per hour.	None	In the scope of CLUG 2.0 only a demonstrator is provided. The full process to achieve a certifiable solution has not been defined. See §4 For more details

Table 12: List of safety requirements identified in D3.4 FTA.

The table presents the synthesis of assumptions identified during this analysis of the LOC-OB.

Id	Assumptions	Coverage ID	Coverage comments
LOC-OB-FTA-Ass-23	This function LOC_OB_SF-305 covered the specific processing on the map data made in the core of the LOC-OB system. Map Data is provided by the function LOC_OB_SF-101.	See section 5.3	The details process of the input functions has not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-FTA-Ass-24	In this document the measurement functions cover the sensors, measurement algorithms and Fault detection and exclusion for a given technology.	See section 5.3	The details process of the input functions has not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-FTA-Ass-27	For analysis on the chain 1, it is assumed that the measurement information provided by the GNSS + EGNOS sensor has a failure of 2.00e-6 per hour and the FDE associated as a failure rate of 2.00e-6 per hour.	See section 5.6	This is an assumption to perform the preliminary analysis. Quantification shall be checked in regard to the final hardware architecture.
LOC-OB-FTA-Ass-28	For analysis on the chain 1, it is assumed that the measurement information provided by the IMU sensor as a failure of 2.00e-6 per hour and the FDE associated as a failure rate of 2.00e-6 per hour.	See section 5.6	This is an assumption to perform the preliminary analysis. Quantification shall be checked in regard to the final hardware architecture.
LOC-OB-FTA-Ass-29	For analysis on the chain 1, it is assumed that the measurement information provided by the wheel sensor as a failure of 1.00e-3 per hour and the FDE associated as a failure rate of 1.00e-3 per hour.	See section 5.6	This is an assumption to perform the preliminary analysis. Quantification shall be checked in regard to the final hardware architecture.
LOC-OB-FTA-Ass-30	For analysis on the chain 2, it is assumed that the second chain need balise information provided in safety by the balise reader.	See section 5.3	The details process of the input functions has not yet been clearly identified and shall be confirmed for further analysis.
LOC-OB-	For apportionment and analysis on the dual chain	See section 5.4	This is an assumption to perform the preliminary analysis.

Id	Assumptions	Coverage ID	Coverage comments
FTA-Ass-31	architecture, and to cover **RA-RAMS-FTA-06,** it is assumed that the combiner function can detect and manage the failure of each chain in less the 30 minutes.		Quantification shall be checked in regard to the detailed description of the combiner.

Table 13: List of assumptions identified in D3.4 FTA.

3.5 Functional system analysis results (D3.5)

Deliverable D3.5 [R8] provides a comprehensive Functional Analysis of the LOC-OB System as part of the CLUG 2.0 project. This analysis is divided into two main parts:

- Qualitative Analysis: an analysis of the internal functions of the LOC-OB system as defined by its functional architecture, utilizing the Failure Mode and Effects Analysis (FMEA) method.
- Quantitative Analysis: an analysis proving that the LOC-OB System meets safety requirements and achieves Safety Integrity Level 4 (SIL4) in terms of hardware. Assumptions were made to assess the feasibility of the LOC-OB hardware system architecture achieving SIL4. Furthermore, this analysis provides guidance on designing the hardware architecture to meet SIL4 standards.

The results of the analysis outline the necessary safety requirements for the LOC-OB system, supporting its development and ensuring adherence to high safety standards.

3.5.1 Safety requirement derived from part 1 of D3.5

SFSA-XX is the System Functional Safety Analysis no. XX which is the tracking number in Part 1 of D3.5.

ID	SAFETY REQUIREMENTS	RATIONALE	WP4 – Task Coverage
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 [R16]. If no cold movement detection, the train cannot initialisation automatically. Human intervention needs to be involved in the initialisation process.	Covered in D4.9
RA-RAMS-28	Cold Movement detection shall meet a TFFR of less	Refer to SFSA-05 related to Safety. If this input is not SIL4, it can affect the LOC-OB System to achieve SIL4.	Not covered in work package 4.

ID	SAFETY REQUIREMENTS	RATIONALE	WP4 – Task Coverage
	than 1E-08 /h (SIL 4 input data to the LOC-OB).		
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 D3.5 - SFSA-19 and SFSA-20 related to Safety. GNSS-EGNOS and IMU TS algorithm will need time to safely define the track edge after passing a switch. Therefore, point position is a crucial input to be provided to the track selectivity (TS) function as it will help defining safely the track edge ID right after passing a switch.	Not covered in work package 4.
RA-RAMS-30	If there is no CMD installed on the train, LOC-OB initialisation function shall get an initial train position from Balises.	Refer to D3.5 - SFSA-05 related to Safety and D4.9 If there is no initial train position from GNSS, fusion algorithm cannot start up. This is the reason why the train should get initial position from balises to initialise fusion algorithm. In case the CMD is not available, the train should start in Staff Responsible mode. In this case, crossing balises is the easiest way to obtain a first safe position.	Covered in D4.9

Table 14: List of Safety Requirement issues from Design safety analysis [R8] in D2.2, D4.1 [R10] and D4.9 [R16].

ID	SAFETY REQUIREMENTS	RATIONALE	WP4 – Task Coverage
RA-RAMS-31	Point position information shall be provided to track selectivity function.	Based on the test results from chapter 5 of D4.8, the test results demonstrate that when two switches are positioned close to each other, the Track Selectivity based on GNSS-EGNOS and IMU are unable to provide the track edge ID after passing the first switch. However, GNSS-IMU can 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 passes the first switch to ensure safe train movement.	Partly covered in D4.4 – Track Selectivity function. The point position information is one of the unitary solutions to determine track selectivity. However, there is no detailed design in D4,8 and it could be addressed in the future study.
RA-RAMS-32	The time or the distance for the Track Selectivity to determine the track after passing a point shall be limited.	Based on the recommendation from D2.2 refer to chapter 2.2. Time to pass 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.	Not covered in D4.8, there are the test results of algorithm behaviour/performance of GNSS and IMU to determine track edge ID after the train crossing the switch point but no requirement specific for limited time or distance when the track selectivity needs to determine after passing a switch.
RA-RAMS-33	For the second chain using Shape and Heading Map Matching technique, the Route Information is required. This input should be SIL4 data (TFFR less than 1E-08 per hour).	See D4.1 v0.4 and D3.5 [R8]),	Partly covered in D4.1. There is indicated that Route information is required.

Table 15: List of new Safety Requirements from design safety analysis Part 1 [R8]1

[1] The requirement **RA-RAMS-34** of D3.5 [R8] has been intentionally removed from this table because it was evaluated to be irrelevant at the end of the CLUG2.0 project.

The following list of safety requirements derived from D2.4 (see §3.2) [R3] is confirmed as safety related after the analysis of D3.5. Futher analyses on industrial product are needed to confirm these points.

ID	SAFETY REQUIREMENTS	RATIONALE	WP4 – Task Coverage
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. Note: Addition to RA-RAMS-35 Rationale: The interaction of the driver in case of non-compliance to SpecSysRec[027] is seen as a safety issue after analysis in D3.5	Partly covered in D4.9.
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 leads to hazard at the end. Note: The safety aspect of this requirement is covered by SpecSysReq[068], which requires that data are provided at any time (including default data if there are not enough inputs available).	Covered in D4.1 §3.7 Table 8

ID	SAFETY REQUIREMENTS	RATIONALE	WP4 – Task Coverage
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, SFSA-15, SFSA-16) are related to safety. Note: the safety aspect of this requirement is covered by SpecSysReq[070]. The track edge id is not always unique as the confidence interval can cover two track edges.	Partly covered in D4.8, the track edge id will be provided after the train crossing a switch. In case of two closing switches, the track edge id will be provided after the train crosses two successive switches.
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 monitor and control speed effectively. As a result, the train cannot be operated safely. Note: The safety aspect of this requirement is covered by SpecSysReq[068], which requires that data are provided at any time (including default data if there are not enough inputs available).	Not covered in work package 4 and especially D4.9.

Table 16: List of D2.4 [R3] requirements found safety relevant after D3.5 safety analysis [R8]

3.5.2 Safety Requirements derived from part 2 of D3.5 – FTA

ID	SAFETY REQUIREMENTS	RATIONALE	WP4 – Task Coverage
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.	Not covered
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.	Not covered
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.	Not covered

Table 17: List of Safety Requirements derived from FTA [R8]

3.6 RAM analysis results (D3.6)

Deliverable D3.6 [R9] provides a comprehensive preliminary system analysis regarding reliability, availability and maintainability of the LOC-OB System as part of the CLUG 2.0 project. This analysis is divided into three main parts:

- Part 1 – Reliability analysis: For this analysis were used the FMEA and FTA methods
  - FMEA Analysis: This part investigated single component failures and their operation impacts on the LOC-OB system with respect to the three failure categories: Immobility failure, Reduced service failure and Minor failure
  - FTA Analysis: This analysis method was used to understand how systems can fail, to identify the best ways to reduce risk and to determine failure rates of a particular system failure. With this analysis the system reliability was calculated. The results of

the FMEA were used to complement the analysis regarding the three failure categories.

- Part 2 – Determination of Maintainability: the ability of the LOC-OB system to be timely and easily maintained was checked, including topics like service, inspection and check, repair and /or modification.
- Part 3 – Determination of Availability: the ability of the LOC-OB system to be in operation in a specified time was checked.

The result of this preliminary analysis shows the possible RAM performance of the LOC-OB system and supports its further development to fulfil the specified RAM requirements.

ID	RAM REQUIREMENTS	WP4 Coverage of WP2 requirements
SpecSysReq[047]	The LOC-OB hardware shall comply with the overall CCS-OB reliability as defined in Ref [57] Chapter 2. Minor failure: λ <1,25 10-4/h. Reduced service failure: λ < 3,3 10-6/h. Immobility failure: λ < 3,7 10-7/h.	Not ok. Minor failure: the failures of the components of the LOC-OB System do not lead to this failure category. Reduced service failure: λ =3,95 10-6/h. Estimated failure rate exceeds the specified failure rate (see failure rate estimations in section 4.5.2 and section 7 in [R9]). Immobility failure: λ < 2,963 10-6/h. Estimated failure rate exceeds the specified failure rate (see failure rate estimations in section 4.5.3 and section 7 in [R9]). A proposal of improvement is detailed in ee section 5.3.
SpecSysReq[049]	The LOC-OB shall have an overall availability of 99,998% during operation.	Ok. According to section 6 in [R9] the LOC-OB system has an availability of 99,9996725 % during operation.
SpecSysReq[054]	The LOC-OB's design and maintenance concept shall meet a Mean Time To Restore (MTTR) ≤ 1h.	Ok. According to Table 14 in [R9] the LOC-OB System has a MTTR of 0,5 hours.
SpecSysReq[055]	Preventive maintenance or periodic sensor calibration period of the overall LOC-OB shall exceed 2 years.	Ok. The LOC-OB System does not need preventive maintenance.

Table 18: List of the RAM Requirements identified in D3.6

4 CERTIFICATION MISSING STEPS

The aim of CLUG 2.0 is to develop a prototype for demonstrating the readiness of the LOC-OB solution, but is not to provide an industrial fully developed product. Thus, WP3 activities do not cover all the steps of RAMS activities expected for an industrial project, but only the early steps related to risk analysis, as described in D3.1 [R4].

In the case of a new certifiable LOC-OB is developed to be integrated in a train in the context of an ERTMS system, it shall be provided a "*first authorisation: the vehicle type authorisation and/or the vehicle authorisation for placing on the market issued by the authorising entity for a new vehicle type, including its variants and/or versions if any, and, where applicable, the first vehicle of a type, pursuant to Article 21(1) of Directive (EU) 2016/797*" as described in Article 14 of [R26].

For this purpose, the design and validation of the Loc-OB system shall follow the requirements of:

- The European Directive on interoperability [R24] and the one on safety [R25].
- The European Regulation [R26] for the process to apply for a vehicle type authorisation and/or a vehicle authorisation for placing on the market.
- The European Common Safety Methods Regulations [R27] and [R28] of risk management process description for the railway systems implementing a significant change. Such risk management process shall be described for the application to place in service of a train embedding the new LOC-OB, as the integration of such new unit is considered as a significant change with impact on the safety.
- The European Regulations on Technical Specification for Interoperability [R29], [R30] and [R31].

As proposed by these regulations, the recommendations of the CENELEC standard [R20], [R21] for the safety and RAM (Reliability, Availability, Maintainability) activities shall be covered.

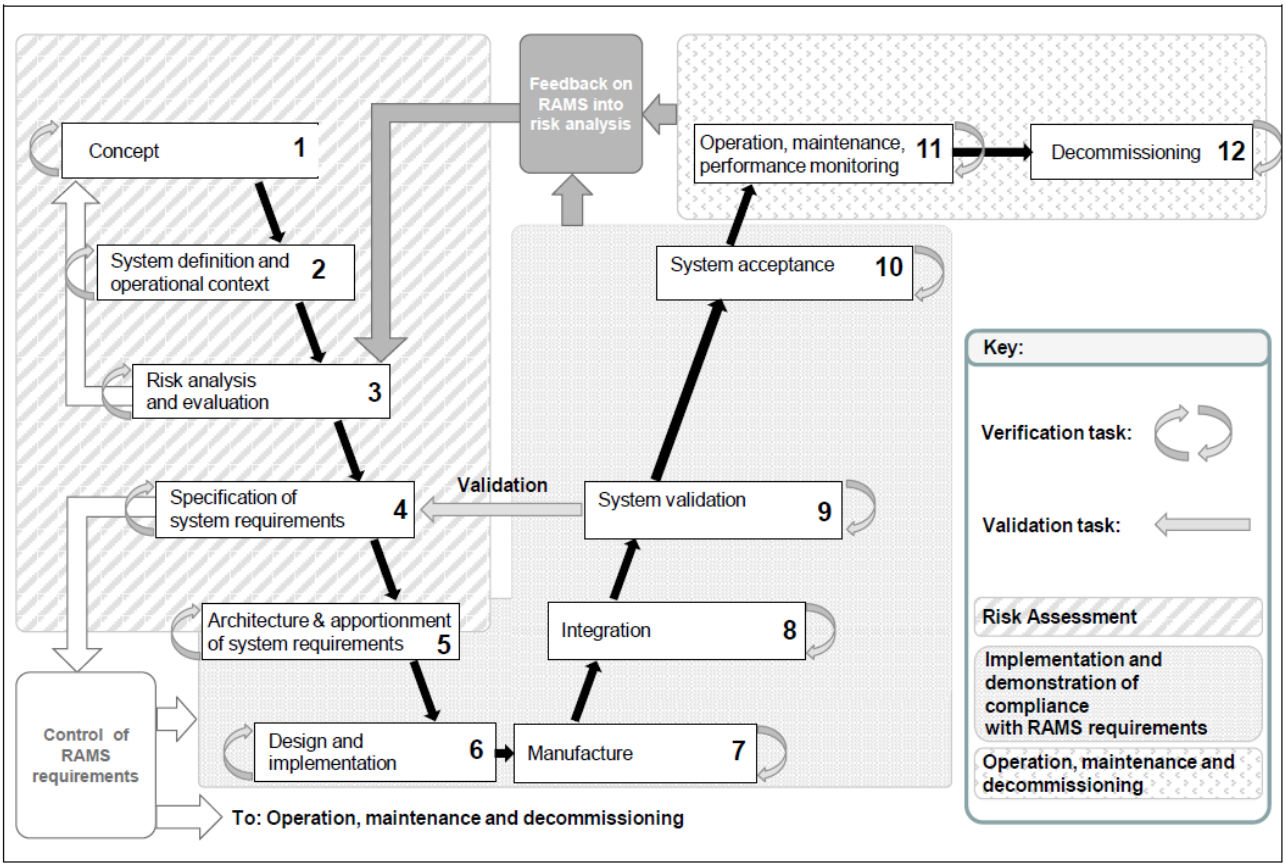

Figure 2 - Phases of V-cycles as defined in EN50126-1

The activities performed during CLUG 2.0 covered partially the first phases from 2 to 5 of the V cycle shown in Figure 2.

To obtain a certifiable product, the activities of this phases shall consolidate the system definition and RAMS analysis, in particular after a clarification of the use cases and the users 'needs (see § 5.2), the architecture (see §5.3), the control functions selected (see §5.4 and §5.5) and the hardware selected (see §5.6) for the final product.

Besides planification of the activities of all the following phases (from phase 6 of design to phase 10 of system acceptance) shall be done according to the CENELEC standards [R20], [R21], [R22]and [R23].

Concerning the RAMS activities, Control of the management and coverage of the RAMS requirements shall be performed along these phases. A particular attention shall be paid to the validation of this RAMS requirements (phase 9): the use of fusion algorithms complexifies the validation of safe functionalities. At the end of the process a Safety case shall be written to synthesis the proof that the system has been design according to the RAMS requirements and those of the European regulations.

5 GAP ANALYSIS

5.1 Introduction

This chapter focuses on the items identified during the CLUG 2.0 project as major elements in regards of RAMS.

The aim of CLUG2.0 is to provide a TRL6 demonstrator but not to deliver an industrial product. So WP3 activities have been limited to the RAMS activities of the early phases of the life cycle defined in EN50126-1 [R20]. This leads to necessary clarifications to be made during the design of a future certifiable product detailed in this chapter.

5.2 Use case and users' needs clarification

During the first analysis (PHA), two major limits have been reached on which users are going to use the data produced by the LOC-OB and in which context.

Users' needs identification:

In D2.1 [R1], a tentative has been made to identify the potential users of the data provided by the LOC-OB system. It has been easy to identify the Train Protection On-board system as a mandatory user of the 1D localization information (1D position, 1D speed and 1D acceleration) in safety. This can be done by comparing to the current need of an ETCS.

However, for the other potential users, as their specifications and needs have not yet been defined it is difficult to fix the outputs used and with which level of safety.

Some assumptions have been made during CLUG 2.0 and shall be confirmed for an industrial usage:

- 1D information (position, speed and acceleration) shall be provided in safety at least for the train protection needs. Other users as ATO can use this information but do not require a safe level.
- 3D information (position, velocity, acceleration, altitude, angular data) can be provided non-safe by the LOC-OB for the needs of Perception system for example.

Operational context and conditions of use:

In the context of the CLUG 2.0 project, it is assumed that the information provided by the LOC-OB is used to provide localization information to the vital on-board system in trains which are running on ERTMS lines. This operational context needs to be confirmed for the industrial product in view to fixing the RAMS target and consolidating the RAMS analyses.

Besides, any restriction of usage, with an impact on safety, shall be explicitly specified. This includes the configuration of the train (a locomotive with wagons or a multi units train) and the position of the system in the train in regards to the front of the train: if the integrity of the train cannot be ensured, or the position of the LOC-OB system in the train cannot be ensured, its outputs cannot be used in safety to define the position or speed of the head of the train.

5.3 LOC-OB Architecture definition

There is a need to define the definitive architecture, particularly the two chains, and clarify the purpose of redundancy. Additionally, it is crucial to establish and align the inputs to the LOC-OB system. The following points require attention:

- Clarification of Inputs for the Second Chain

The inputs necessary for executing the second chain need to be clearly defined and confirmed.

Information from D3.3 suggests that balises are used for the second chain, which contradicts the details provided in D4.1. Therefore, the LOC-OB architecture and all associated inputs must be reviewed, aligned, and clearly documented.

- Track Selectivity Function and Safety Analysis Findings

As outlined in D3.5, the results of the safety analysis indicate that point position feedback from the infrastructure is required as an input for the track selectivity function. This is because GNSS-IMU localisation alone cannot determine the track edge ID when the train passes two successive switches, and it can lead to hazardous events.

Further study is needed to enable the track selectivity function to receive point position feedback as an input. This input, combined with GNSS-IMU localisation, will be used to define and report the track edge ID after the train passes the first switch.

The interface between the infrastructure and the LOC-OB, required for providing point position feedback, needs to be defined in future studies.

- Route Information

It is necessary to determine whether route information is required for track selectivity. If route information is needed for the second chain (e.g., for shape and heading map matching), its potential use for the track selectivity function in the first chain should also be considered.

Future studies should define the interface between the infrastructure and the LOC-OB for providing route information.

- Redundant structures for reliability

The results of the RAM Analysis in D3.6 [R9] shows that the configuration with one chain is not enough to fulfil the RAM requirement SpecSysReq[047] regarding “Immobility failure”. Because of this, it is necessary to improve the architecture of the LOC-OB system with help of redundant structures. This situation must be considered for the further development of the second chain.

5.4 Combiner mechanism definition

More detailed information is required regarding the new combiner functions and logic. In D4.1, it is noted that the combiner function is a simple function that computes the union of the calculated Confidence Intervals (CIs).

Detailed description of the combiner function and the principles guiding its design shall be provided.

To reach the safety target SIL4 allocated to the output functions of the LOC-OB (see apportionment proposed in D3.4 [R7] and results in Table 11: List of safety requirements identified for apportionment on Archi_2), the following requirements shall be fulfilled :

- the combiner component shall be designed in SIL4,
- the combiner shall provide mechanisms to compare the results of the two chains, detecting and eliminating errors,
- both chains shall be designed at SIL2 for the functions providing safe outputs, detecting errors as soon as possible. Common failure modes between the two chains shall be analysed.

5.5 FDE mechanism identification

D3.3 and D3.4 demonstrate the necessity of Fault detection and elimination (FDE) algorithms to reach a high level of safety (see sections 3.3 and 3.4) by detecting and isolating some failures on the inputs measurements as soon as possible.

In WP4, two kinds of FDE have been identified:

- FDE at sensor level as:
    - GNSS+ EGNOS, see [R11]
    - IMU, see [R12]
    - Speed sensor, [R13]
- FDE at system level, see [R14] and [R15]

These documents identify the kind of failure related to the sensors (Hardware failure, measurement errors,…) and the fault detection linked to the main sensors is clearly identified.

It can be synthesized according to the following table:

Sensors	Failure	Local FDE detection	System FDE detection	Comments / way forward
GNSS	Hardware failure	None	Can be detected by comparison with other sensors	Clarification on how system FDE can detect hardware failures are needed.
	GNSS signal errors corrected by EGNOS service (i.e. clock errors, ionosphere errors, satellite failures)	None	None	Assumption: the current RAMS analyses assume that the EGNOS service is used as input and allow to correct GNSS errors at system level. Thus, it is not necessary to define a FDE mechanism to cover these errors in the LOC-OB.
	Time incoherency and cycle slip	Detected by local FDE with code minus carrier barrier and cycle monitoring. See D4.2 [R11]		Details should be provided on the conditions for implementing this FDE (number of fault measurements, number of cycles, type of sensors concerned).
	Doppler and multipath errors	Detected by local FDE with doppler monitoring and PVT level consistency check. See D4.2 [R11]		Precisions on the time measurement windows and the threshold are needed to further the analyses of the FDE.
	Uncertainty measure	Detected by local FDE with elevation measurement masks and C/NO measurement masks. See D4.2 [R11]		Precision on the thresholds is needed to further the analyses.

Sensors	Failure	Local FDE detection	System FDE detection	Comments / way forward
	Cumulative errors	None	Can be detected by comparison with other sensors	Clarification on how system FDE can detect cumulative errors are needed.
	Light deviations	None	Can be detected by comparison with other sensors	Clarification on how system FDE can detect light deviations are needed.
IMU	Hardware failure	None	Can be detected by comparison with other sensors	
	Measurement fault (noise, uncertainty)	Besides calibration operation and signal filtering, detected by local FDE when a measure is out of the window of acceptable measures. See D4.3 [R12]		Precisions on the measurement windows and thresholds are needed.
	Cumulative measurement fault (bias)	None	Can be detected by comparison with other sensors	
Speed Sensor	Hardware failure/ operating failure	None	Can be detected by comparison with other sensors	
	Measurement fault (slip and slide, jerk)	Detected and monitored by local FDE		Current tachymeter systems have a solution to detect errors such as the use of several sensors. Fixing the

Sensors	Failure	Local FDE detection	System FDE detection	Comments / way forward
		See D4.4 [R13]		number of sensors is a path to explore to mitigate this kind of errors. Precisions on the thresholds are needed.
	Measurement persistent fault (velocity oscillation, likely due to installation errors)	Detected by local FDE and lead to persistent fault See D4.4 [R13]		Installation and maintenance procedures shall be defined to prevent the occurrence of such errors.
	Omission from all the sensors	None	Detected by comparison with other sensors kind as GNSS	
	Wear of the wheel, wrong calibration	None	Detected by comparison with other sensors kind as GNSS	
	Light slip or slide	None	Detected by comparison with acceleration provided by IMU	

Way forwards and assumptions should be discussed in the future, once hardware will have been selected with a fixed architecture and once the sensors and the necessary inputs (EGNOSS service, digital map, balises,…) will be consolidated.

Besides, the functional description of the local FDE in case an error is detected should be detailed precising what information is used to provide the outputs of the LOC-OB function and how long it is acceptable to have an error.

Concerning the System FDE, D2.6 [R14] proposed two methods to detect and exclude measurement faults based on fusion-based algorithms:

- Sequential innovations based FDE (section 5.1)
- Generalized Pseudo-Bayesian Filter Bank (section 5.2)

However, these proposals are based on a probabilistic distribution of the errors. It should be justified in the future, the kind of errors detected by these FDE on the sensor measurements and on the solution. For each potential failure of an input sensors, it shall be shown how the failure is detected and mitigated.

5.6 Hardware definition

The Hardware System Architecture for LOC-OB must be clearly defined. This architecture is essential to facilitate the RAMS analysis effectively. The following aspects require precise specification:

- Quantity and Type of Sensors: How many GNSS Receivers, IMUs, tachometers, and optical sensors are incorporated into the LOC-OB System Architecture?
- Sensor Models and Hardware Processing: Which models of sensors will be utilized? Will separate hardware processing be implemented for Chain 1 and Chain 2?
- Navigation and Integrity Engines: Are the navigation engine and integrity engine executed on the same hardware platform?
- Combiner Hardware Engine: Where is the combiner engine located? Does it operate on the same hardware as Chain 1, or is it executed on separate hardware?
- Operational conditions for Hardware Engine: Which operational and environmental conditions have to be considered? For example: which environment temperature (40°C?), which operational profile (10 hours /day?), which mechanical operation conditions? Etc.

All this information must be explicitly detailed to ensure a comprehensive understanding of the system's architecture.

5.7 Algorithm analysis (Kalman algorithms / fusion algorithms)

The core algorithms of the CLUG2.0 demonstrator are based on fusion algorithms as Kalman filters. Those algorithms are described in D4.1 [R10], D4.6 [R14] and D4.7 [R15].

Fusion algorithms are not unknown in the railway domains but are usually not directly used in SIL2 or SIL4 function design.

For an industrial certifiable product, it shall be shown that the design of this function reach a SIL2 level, in particular that the requirements expected from the railway standard EN50126 [R20], [R21], EN50129 [R22] and EN50716 [R23] are covered.

A particular focus shall be made on the process of verification and validation of this algorithm and how they allow to conclude on the safety of the system. In aeronautic domains, probabilistic approaches can be used to demonstrate that the integrity rate associated to the outputs of a function allow to cover a safety target in case of non-systematic faults. It shall be studied how such an approach can be used in the railway domain.

5.8 Measurement integrity risk

Once safety analysis has produced some safety requirements, one of the most important questions is how this safety requirements can be covered by the design and the system validation. In some cases, quantified parameters on the measurement shall be determined, and a demonstration shall be done to validate this selection regarding the safety target.

For example, considering the safety requirement RA-RAMS-03 “The true train position shall be always inside the confidence interval”, the safety analysis concludes it shall be covered by a function with a $10^{-9} \leq TFFR < 10^{-8}$.

Besides the safety analysis, a detailed quantitative analysis shall be performed to study if the integrity rate related to the outputs (especially the confidence interval) shall be reached by the combination of the results of both chains in view to validate the system. Due to the nature of the algorithms used on each chain (see §5.7), the integrity rate (on the outputs) is used to prove, by a probabilistic approach, the coverage of some safety requirements such as RA-RAMS-03 “The true train position shall be always inside the confidence interval”. The term “always” is covered by a high-level probability that the train is inside the confidence interval deduced from the integrity rate associated to this confidence interval: Probability = 1 – Integrity Rate. This integrity rate can be related to the size of the confidence interval, and thus the performance and accuracy of each chain.

During the design of the fusion function and control integrity function, some parameters are defined based on probabilistic models to determine how the confidence interval can be trusted. The term “always” is covered by a high-level probability that the train is inside the confidence interval deduced from the integrity rate associated to the measure: Probability = 1 – Integrity Rate. This integrity rate can be related to the size of the confidence interval, and thus the performance and accuracy of each chain. In the previous example the expected probability is at least $P\_safe = 1 - 10^{-9}$.

As the fusion algorithm follows a normal law, a standard deviation is used to define the confidence interval around an estimated value. In the example, a standard deviation of 7σ is necessary to reach P_safe for a single chain.

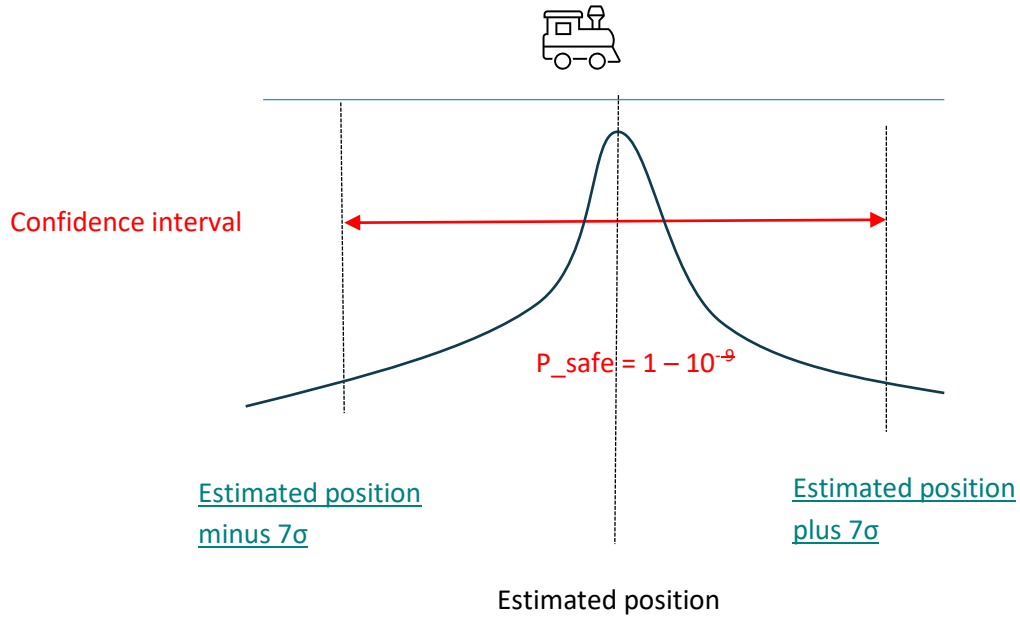

Figure 3 – Probability associated to Confidence Interval

As discussed in D4.1 [R10], and in WP3 analysis (see § 3.4), it can be very difficult to build an efficient safe solution with only one chain, and it is highly recommended to develop a two chains architecture, with independent functions.

In this case, the safe confidence interval provided by the combiner, is the union of the confidence intervals of both chains. Thus, the probability P_safe that the train is in the output confidence interval can be deduced from those of each chain as:

$$P\_Safe = P\_Safe\_A + P\_Safe\_B – (P\_Safe\_A * P\_Safe\_B)$$

Where P_Safe_A * P_Safe_B is the probability that the train is in the intersection of the confidence intervals, for independent functions.

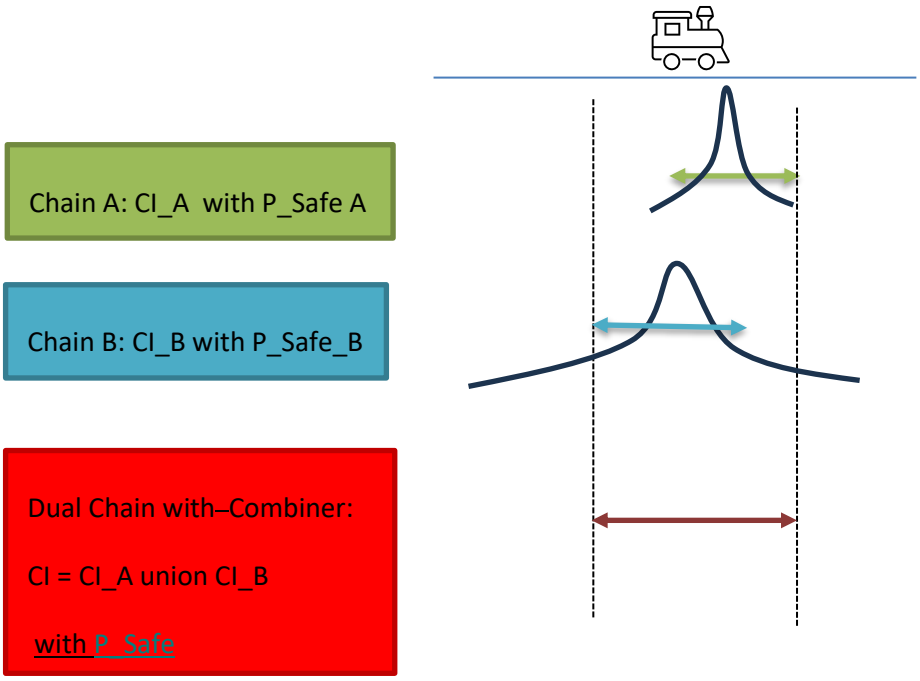

Figure 4 – Computation of the Confidence Interval for a dual chain architecture

It is worth noting that it is not necessary to have the same probability expected for each chain: if P_Safe_A = $1\text{-}10^{-6}$ and P_Safe_B = $1\text{-}10^{-3}$, P_Safe = $1\text{-}10^{-9}$.

Thus, integrity rate can be adapted for each chain to its performance to define the confidence interval.

This is what is proposed in D4.7 [R15] by allocating an integrity rate of 10^{-6} to one chain and 10^{-3} to the second. It remains to validate for each chain that the integrity rate allocated can be reached.

However, the definition of the measurement integrity rate must not be confused with the notion of safety associated with the development of each chain, and for which the same safety target shall be associated to both chain (see § 5.4).

5.9 Availability issues

Some availability issues can be raised in some particular environment, e.g. GNSS can be unavailable for a long time in a long tunnel, in which case balises shall be deployed to maintain good performance. This is discussed in the GAP analysis D6.6 [R19] § 5.2.5. In particular, impact on safety and common referential in particular subset 91 analysis [R34].

It left the question of availability to discuss performance results of the solution in different environment and degraded constraints should be analysed in detail to evaluate how many balises shall be necessary.

6 CONCLUSION

This deliverable presented a synthesis of the WP3 work related to the RAMS analyses and contains four sections.

A coverage of the WP2 requirements related to safety was first performed to be able to confirm the RAMS category assumed by WP2. Furthermore, WP3 analyses added a few of WP2 requirements to the safety category.

Then, a synthesis of the results of WP3 analyses was provided. Besides, an analysis of the coverage of the RAMS requirements by the designed solution described in WP4 documents has been performed. While the initial CLUG project focused on high-level requirements and architecture definition, CLUG2.0 introduces formal RAMS analyses to support future certification.

The aim of CLUG2.0 is to provide a TRL6 demonstrator but not to deliver an industrial product. So WP3 activities have been limited to the RAMS activities of the early phase of the life cycle defined in EN50126-1 [R20]. The third section lists the remaining steps to obtain a certifiable product. This concerns mainly the deployment of a design, verification, and validation process for an industrial system.

The necessary clarifications to be made during these remaining steps have been listed:

- Precise the operational context and the user needs and use cases (see § 5.2 and §5.9).
- Set a definitive architecture and select the relevant hardware components (see § 5.3 and § 5.6).
- Clarify the safety functional mechanism to detect and mitigate failures (see § 5.4 and § 5.5).
- Identify the process to design, verify and validate in safety a software implementing fusion algorithms (see §5.7 and §5.8).

The RAMS analyses provided during CLUG2.0 give detailed results that lead to the conclusion that the system can reach a high-level safety target.

This architecture is based on some strong assumptions on the inputs:

- an EGNOS for Rail service is considered to improve the safety related to GNSS (considering a failure rate of 2.00e-6 per hour),
- a safe digital map is necessary,
- balises are needed for a safe initialization of the system.

These first results give confidence that a certifiable product based on the solution with a two chains architecture can be designed to reach a SIL4 target for an ERTMS operational context.

7 REFERENCE DOCUMENTS

[R1] [CLUG2.0 – D2.1] LOC-OB Operational Needs and System Capabilities of Localisation On-Board System

[R2] [CLUG2.0 – D2.3] LOC-OB System boundary, Architecture, and External interfaces (incl. DM)

[R3] [CLUG2.0 – D2.4] LOC-OB System Requirements

[R4] [CLUG2.0 – D3.1] LOC-OB System Context Analysis and RAMS Plan

[R5] [CLUG2.0 – D3.2] LOC-OB Preliminary Hazard Analysis

[R6] [CLUG2.0 – D3.3] LOC-OB System Failure Modes and Effects Analysis

[R7] [CLUG2.0 – D3.4] LOC-OB External Interfaces Analysis

[R8] [CLUG2.0 – D3.5] LOC-OB System Functional Safety Analysis

[R9] [CLUG2.0 – D3.6] LOC-OB Preliminary System Reliability and Availability analysis

[R10] [CLUG2.0 – D4.1] LOC-OB Functional System Architecture

[R11] [CLUG2.0 – D4.2] LOC-OB GNSS+EGNOS unit prototype including data FDE for LOC-OB design and description document

[R12] [CLUG2.0 – D4.3] LOC-OB Safe IMU sensor and data FDE for LOC-OB description document

[R13] [CLUG2.0 – D4.4] LOC-OB Speed sensor and data FDE for LOC-OB description document

[R14] [CLUG2.0 – D4.6] LOC-OB Along track localization fusion algorithm design document

[R15] [CLUG2.0 – D4.7] LOC-OB Confidence Intervals computation & Integrity algorithm

[R16] [CLUG2.0 – D4.9] LOC-OB Start of Mission preliminary design

[R17] [CLUG2.0 – D5.2.2] LOC-OB Test plan

[R18] [CLUG2.0 – D5.xx] LOC-OB Interface Control Document

[R19] [CLUG2.0 – D6.6] Proposed Localisation on-board system requirements and Gap analysis

[R20] [EN 50126-1-2017] Railway Applications - The Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1: generic RAMS process

[R21] [EN 50126-2-2017] Railway Applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 2: systems approach to safety

[R22] [EN 50129-2018] Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

[R23] [EN 50716-2023] Railway Applications - Requirements for software development

[R24] [DIR-2016-797] Directive (EU) 2016/797 of the European parliament and council of 11 May 2016 on the interoperability of the rail system within the European Union

[R25] [DIR-2016-798] Directive (EU) 2016/798 of the European parliament and council of 11 May 2016 on railway safety

[R26] [PAVA-2018-545] Commission Implementing Regulation (EU) 2018/545 of 4 April 2018 establishing practical arrangements for the railway vehicle authorisation and railway vehicle type authorisation process pursuant to Directive (EU) 2016/797 of the European Parliament and of the Council

[R27] [CSM-RA-402-2013] Commission Implementing Regulation (EU) 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation

[R28] [CSM-DT-1136-2015] Commission Implementing Regulation (EU) 2015/1136 on the Common Safety Method for Risk Evaluation and Assessment.

[R29] [TSI-CCS-919-2016] Commission Regulation (EU) 919/2016 of 27 May 2016 on the technical specification for interoperability relating to the 'control-command and signalling subsystems of the rail system in the European Union

[R30] [TSI-CCS-1695-2023] Commission Implementing Regulation (EU) 2023/1695 of 10 August 2023 on the technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union and repealing Regulation (EU) 2016/919

[R31] [TSI-CCS-776-2019] Commission Implementing Regulation (EU) 776/2019 of 30 April 2013 on the technical specification for interoperability

[R32] [SUBSET-026 v4.0.0] ERTMS/ETCS - System Requirements Specification

[R33] [SUBSET-088 v3.7.0] ETCS Application Levels 1 & 2 - Safety Analysis

[R34] [SUBSET-091 v4.0.0] Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2

[R35] [OCORA-TWS01-030] OCORA - System Architecture, v3.00, 30.11.2022

[R36] [OCORA-TWS01-035] OCORA - CCS-On-Board-(CCS-OB)-Architecture, v3.00, 30.11.2022

[R37] [LOC-OB_22E126] LOC-OB System Definition & Operational Context, v1.1, 30/11/2022

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