CLUG Demonstration of Readiness for Rail – CLUG 2.0

D3.1 CLUG LOC-OB SYSTEM CONTEXT ANALYSIS AND RAMS PLAN

Due date of deliverable: 31/07/2023

Actual submission date: 22/03/2024

Leader of this Deliverable: Marc SARRAT, SNCF

Reviewed: Y

Document status		
Revision	Date	Description
0.1	29/03/2023	Draft version (plan)
0.2	24/04/2023	Draft version (parts RAMS Management and RAMS Activities)
0.3	28/04/2023	Draft version for review (parts RAMS Management and RAMS Activities)
0.4	04/07/2023	Draft version for review (all parts)
0.5	28/07/2023	Stable version
0.6	29/08/2023	Draft final version
0.7	10/11/2023	Submitted version for technical review
1.0	27/11/2023	Final version
1.1	31/01/2024	Integration of external review comments
1.2	12/03/2024	Update considering approved WP2 deliverables
2.0	22/03/2024	Final version submitted to EUSPA

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

Project funded from the European Union's Horizon 2020 research and innovation programme		
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: 24 months

REPORT AUTHORS

NAME	COMPANY	DETAILS OF CONTRIBUTION
Marc Sarrat / Marielle Petit-Doche	SNCF	V0.1: Draft version : - Plan- §1 Introduction
Karin Nebe Claus Thies-Von-Der-Bey Marc Sarrat / Marielle Petit-Doche	SMO DB Netz SNCF	V0.2: Draft version: - Plan - §1 Introduction - §2 Risk Analysis Objectives and Methodology - §3 Risk Analysis Activities
Marc Sarrat / Marielle Petit-Doche	SNCF	V0.3: Draft version for review
Marc Sarrat / Marielle Petit-Doche	SNCF	V0.4: Draft version for review based on v0.1 version of D2.1 and D2.3
Marc Sarrat / Marielle Petit-Doche	SNCF	V0.5: Stable version based on v0.1 version of D2.1 and D2.3
Marc Sarrat / Marielle Petit-Doche	SNCF	0.6: Draft final version based on v1.0 version of D2.1 and D2.3
Marc Sarrat / Marielle Petit-Doche	SNCF	V0.7: Final version submitted for review based on v1.0 version of D2.1 and D2.3
Marc Sarrat / Marielle Petit-Doche	SNCF	V1.0: Final version after technical review
Marc Sarrat / Marielle Petit-Doche	SNCF	V1.1: Integration of external review comments

REPORT REVIEWERS

NAME	COMPANY	DETAILS OF CONTRIBUTION
Karin Nebe	SMO	V0.1, V0.3, V0.4
Claus Thies-Von-Der-Bey	DB Netz	V0.1, V0.3, V0.4
Alain Ruaudel	ADS	V0.1, V0.3, V0.4, V0.5
Jaun Kurt	SBB CFF	V0.3
Aitor Erdozain Ibarra	CAF	V0.2
Iban Lopetegi Zinkunegi	CAF	V0.3
Valentin Barreau	SNCF	V0.7
Mariya Kayalova	RINA-C	Quality check
Jose Bertolin	UNIFE	Final check and submission to reviewers and EUPSA
Denis Dusso	EUPSA	V1.1

EXECUTIVE SUMMARY

CLUG 2.0 deliverable D3.1 – CLUG LOC-OB SYSTEM CONTEXT ANALYSIS AND RAMS PLAN aims at defining and coordinating the RAMS objectives and activities of CLUG 2.0 for the LOC-OB system.

According to the criteria defined by the CSM RA [R8], the potential impact induced by the implementation of the LOC-OB system on the safety of the railway system should be considered as a significant change**.** Thus, it is essential to follow the risk management recommendations described, and therefore to carry out risk analyses as part of CLUG 2.0. The European Regulations CSMs recommends following the requirements of the CENELEC standard EN50126 for RAMS activities.

Thus, the purpose of this document is to describe the targeted RAMS activities in the scope of the CLUG 2.0 project. It notably contains:

- the context of use of the LOC-OB system in regards of Reliability, Availability, Maintainability and Safety (RAMS) requirements,
- the RAMS objectives for the LOC-OB system prototyped during the CLUG 2.0 project,
- the RAMS activities to be carried out as part of the WP3 activities of the CLUG 2.0 project.

This document is a RAMS plan, it therefore does not provide any results. However, it will be a guideline to perform the tasks T3.2 to T3.7 of the CLUG 2.0 project, in order to define, at the end of the project, if the LOC-OB system can be recommended as a certifiable product in the future.

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 Union Agency for the Space Programme which defines what has to be done, how and the relevant efforts.
- Consortium Agreement (signed version 13/04/2023): This defines the obligations of the consortium members 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 case of any such update, the latest formal issued version shall apply.

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

REFERENCES

[R1] [EN 50126-1-2017] Railway Applications - The Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1: generic RAMS process

[R2] [EN 50126-2-2017] Railway Applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 2: systems approach to safety

[R3] [EN 50129-2018] Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

[R4] [EN 50128-2011] Railway application – Communication, signalling and processing systems – Software for railway control and protection systems

[R5] [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

[R6] [DIR-2016-798] Directive (EU) 2016/798 of the European parliament and council of 11 May 2016 on railway safety

[R7] [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

[R8] [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

[R9] [CSM-DT-1136-2015] Commission Implementing Regulation (EU) 2015/1136 on the Common Safety Method for Risk Evaluation and Assessment

[R10] [Guide CSM-RA] Guide for the application of the Commission Regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)'a) of the Railway Safety Directive reference

[R11] [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

[R12] [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

[R13] [TSI-CCS-776-2019] Commission Implementing Regulation (EU) 776/2019 of 30 April 2013 on the technical specification for interoperability

[R14] [TSI-CCS-2022] Recommendation ERA 1175-1218 of the European Union Agency for Railways on The TSI revision package 2022 – Digital Rail and Green Freight - Annex 1 TSI-CCS

[R15] [SUBSET-023 v4.0.0] ERTMS/ETCS - Glossary of Terms and Abbreviations

[R16] [SUBSET-026 v4.0.0] ERTMS/ETCS - System Requirements Specification

[R17] [SUBSET-088 v3.7.0] ETCS Application Levels 1 & 2 - Safety Analysis

[R18] [SUBSET-091 v4.0.0] Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2
[R19] [SUBSET-035 v4.0.0] ERTMS/ETCS Specific Transmission Module FFFIS, 3.2.0, 16.12.2015
[R20] [SUBSET-041 v4.0.0] ERTMS/ETCS Performance Requirements for Interoperability, Issue 3.2.0, 17.12.2015
[R21] [OCORA-TWS01-030] OCORA - System Architecture, v3.00, 30.11.2022
[R22] [OCORA-TWS01-035] OCORA - CCS-On-Board-(CCS-OB)-Architecture, v3.00, 30.11.2022
[R23] [OCORA-TWS01-100] OCORA - Localisation-On-Board-(LOC-OB) Introduction, v3.0, 30.11.2022
[R24] [Loc-OB_22E126] Loc-OB System Definition & Operational Context, v1.1, 30/11/2022
[R25] [Loc-OB_22E135] Loc-OB Risk Analysis, V2.0, 16/12/2022.
[R26] [CLUG2.0 – D2.1] Loc-OB Operational Needs and System Capabilities of Localisation On-Board System, v2.0
[R27] [CLUG2.0 – D2.2] Loc-OB Start of Mission and Track Selectivity, v2.0
[R28] [CLUG2.0 – D2.3] Loc-OB System boundary, Architecture, and External interfaces (incl. DM), v2.0
[R29] [CLUG2.0 – D2.4] Loc-OB System requirements, v2.0
[R30] [CLUG2.0 – D4.1] Loc-OB Functional System Architecture
[R31] [CLUG2.0 – D4.8] Track Selectivity Determination algorithm design document
[R32] [CLUG2.0 – D4.9] Start of Mission preliminary design
[R33] [CLUG2.0 – D4.10] On board Digital Map definition and interfaces

LIST OF ACRONYMS

ACRONYM	CONCEPTS
ADS	Airbus Defense and Space
ATO	Automatic Train Operation
CAF	Construcciones y Auxiliar de Ferrocarriles
CCS	Control, Command and Signalling
CLUG	Certifiable Localisation Unit with GNSS in the railway environment
CSM	Common Safety Methods
DBN	Deutsche Bahn Netz
DM	Digital Map
ERA	European Railway Agency
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EUG	ERTMS Users Group
EUPSA	European Union Agency for the Space Programme
EVC	Embedded Vital Computer
FFFIS	Form Fit Functional Interface Specification
FMEA	Failure Modes and Effects analysis
GNSS	Global Navigation Satellite Systems
IEC	International Electronical Commission
IMU	Inertial Measurement Unit
LOC	Localisation
LWG	Localisation Working Group

ACRONYM	CONCEPTS
NTC	National Train Control
OB	On-Board
OCORA	Open CCS On-board Reference Architecture
PHA	Preliminary Hazard Analysis
RAM	Reliability, Availability, Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RCA	Reference CCS Architecture
RINA	Registro Italiano Navale e Aeronautico
ROE	Return Of Experience
SBB	Schweizerische Bundesbahnen AG
SIL	Safety Integrity Level
SMO	Siemens Mobility
SNCF	Société nationale des chemins de fer français
TFFR	Tolerable Functional Failure Rate
TSI	Technical Specification of Interoperability
UNIFE	Union des industries ferroviaires européennes
UNISIG	Union Industry of Signalling

Table of Contents

Table of figures

List of tables

1 INTRODUCTION

1.1 Objectives of the CLUG 2.0 Project

Based on the experience gained during CLUG, the rail operators with the support of the industry suppliers have been able to consolidate the set of high-level user needs and subsequently the system requirements – including RAMS - for the Localisation On-Board (LOC-OB) System. In CLUG 2.0 (CLUG Demonstration of Readiness for Rail), the LOC-OB system architecture aims to replace the existing European Train Control System (ETCS) odometry system by a GNSS-based multi-sensor fusion architecture to enable absolute safe train positioning whilst also transforming the way of train localisation is done. In CLUG 2.0 (CLUG Demonstration of Readiness for Rail), the system architecture aims at transforming the way of train localisation is done today by demonstrating a GNSS-based multi-sensor fusion architecture. To ensure that an enhanced on-board localization in ERTMS/ETCS using GNSS is interoperable, the technological readiness of the LOC-OB System shall be demonstrated in CLUG 2.0.

To achieve its objectives, the consortium continues the work started in the first CLUG project, by consolidating and completing the specification of the LOC-OB system as well as improving the design of the safe functional architecture and validating it against the requirements defined by the operators.

The main objectives of the CLUG 2.0 project, are:

- EO1: To review, consolidate and complete the high-level user needs and system requirements for the LOC-OB System including Start of Mission and Track Selectivity.
- EO2: To consolidate the safe localisation system architecture and to prototype further the functions of the CLUG LOC-OB.
- EO3: To consolidate by live demonstration the readiness of the CLUG LOC-OB multi-sensor fusion algorithms.
- EO4: To perform an analysis of Reliability, Availability, Maintainability, and Safety (RAMS) on the consolidated functional architecture of the system.

1.2 Objectives of the RAMS Plan

This Reliability, Availability, Maintainability and Safety (RAMS) plan describes the RAMS objectives and activities that will be performed for the development of a railway Localisation On-board Unit (LOC-OB) in the WP3 of CLUG 2.0 in order to cover the CLUG 2.0 objective "*EO4: To perform an analysis of Reliability, Availability, Maintainability, and Safety (RAMS) on the consolidated functional architecture of the system*."

The aim of the CLUG 2.0 is to develop a prototype for demonstrating the readiness of the CLUG solution, not to provide an industrial fully developed product. Thus, this document will not cover all the steps of RAMS activities expected for an industrial project, but only the early steps related to risk analysis. However, it is proposed to identify the RAMS objectives and activities to perform during the

CLUG 2.0 project in the case of a new LOC-OB is developed to be integrated in a train in the context of an ERTMS system. As described in Article 14 of [R7], this plan is defined to cover an embedded subsystem for the case of 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*".

It follows the requirements of:

- The European Directive on interoperability [R5] and the one on safety [R6].
- The European Regulation [R7] 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 [R8] and [R9] 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 [R11], [R12] and [R13].

As proposed by these regulations, this document follows the recommendations of the CENELEC standard [R1], [R2] for the safety and RAM (Reliability, Availability, Maintainability) plans.

1.3 Scope of the document

The LOC-OB is a sub-system of the safe control command embedded system in charge of performing the safe train localisation functionality as described in the OCORA project [R21], [R24]. The LOC-OB is a safe CCS On-Board building block that uses sensor data and supporting information to provide train localisation output information safely and reliably. The LOC-OB shall provide the absolute and relative position of the front-end of the train, train orientation information as well as kinematic parameters such as speed, acceleration, or rotational angles.

The operational context used as a basis for this plan is based on the existing ERTMS/ETCS level 2 where the concepts of independent onboard vehicle localisation component and digital map are added. It can be adapted for hybrid train detection or automatic driving (ATO). In CLUG 2.0, the RAMS activities are performed in the context of the ERTMS/ETCS system described in the TSI [R12] and [R13] and subset 26 [R16], in particular, the safety analysis is based on the hazards of the ERTMS/ETCS system identified in subset 88 [R17] and subset 91 [R18]. This corresponds to the current state of art at the beginning of the CLUG 2.0 project. However, this basis will be reviewed during CLUG 2.0, with identification of feared events and safety targets related to the localisation system.

General description of the LOC-OB system under analysis in this document is given in section 2 and more details can be found in the deliverables of [R26] and [R27].

Section 3 gives the RAMS objectives to follow during the CLUG 2.0 project.

Section 4 details the RAMS activities planned for WP3 of the CLUG 2.0 project.

1.4 Limits and Hypotheses

This section provides a list of limits and hypotheses related to the RAMS activities during the CLUG 2.0 project, to consolidate the scope of the analyses and to identify open points at this stage of the project.

1.4.1 Coverage of CENELEC 50126 [R1], [R2]

The WP3 activities will follow the recommendations of the CENELEC standards which are applied in the railway domain. In particular, this document will follow some recommendations related to the definition of a RAM plan and a Safety plan as described for the "Phase 2: System definition and operational context" in EN50126-1 [R1].

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" will be described in this document (see Figure 3 - Phases of V-cycles as defined in EN50126-1.

Besides, some items recommended by EN50126 as roles, documentation management, planning, hazard log management will not be covered in this document and during the WP3 activities.

1.4.2 Scope of the RAMS activities

The activities of the stakeholder related to the authorisation request are not described in this plan.

Only internal functional architecture is designed in CLUG 2.0, material architecture is out of scope.

1.4.3 Scope of the LOC-OB system and User needs

The RAMS activities presented are limited to the LOC-OB system presented in section 2 and documents [R26] and [R27].

NTC systems are not covered, only ETCS level 2 and 3 are considered.

1.4.4 Operational context

The CLUG 2.0, as research project, the operational context of the LOC-OB system is not clearly identified. The high-level RAMS target linked to the use of the system (such as the operating time of the system) are not defined.

2 LOC-OB SYSTEM CONTEXT

2.1 Project Description and Context

The safe on-board localisation unit (LOC-OB) specified in CLUG 2.0 has the following characteristics:

- on-board multi-sensor safe localisation system consisting of a navigation core combining GNSS, Inertial Measurement Unit (IMU) and digital map information among others,
- continuous on-board localisation providing safe and non-safe location data, notably position, speed, movement direction and other dynamics of the train,
- localisation system that is operational and interoperable across the entire European rail network,
- localisation system that is compatible with European Railway Traffic Management System (ERTMS) TSI current status and future evolutions.

A detailed description of the LOC-OB system is given in the WP2 deliverables D2.1 [R26] and D2.3 [R28].

This current version of the document is based on v2.0 version of D2.1 and D2.3 ([R26] and [R28] respectively).

2.2 Operational Needs and System Capabilities

The LOC-OB architecture has been defined following the OCORA on board architecture principles, based on building block (see D2.3 [R28]).

The operational needs have been identified in D2.1 [R26] as Wider System of Interest as recalled in the Figure 1:

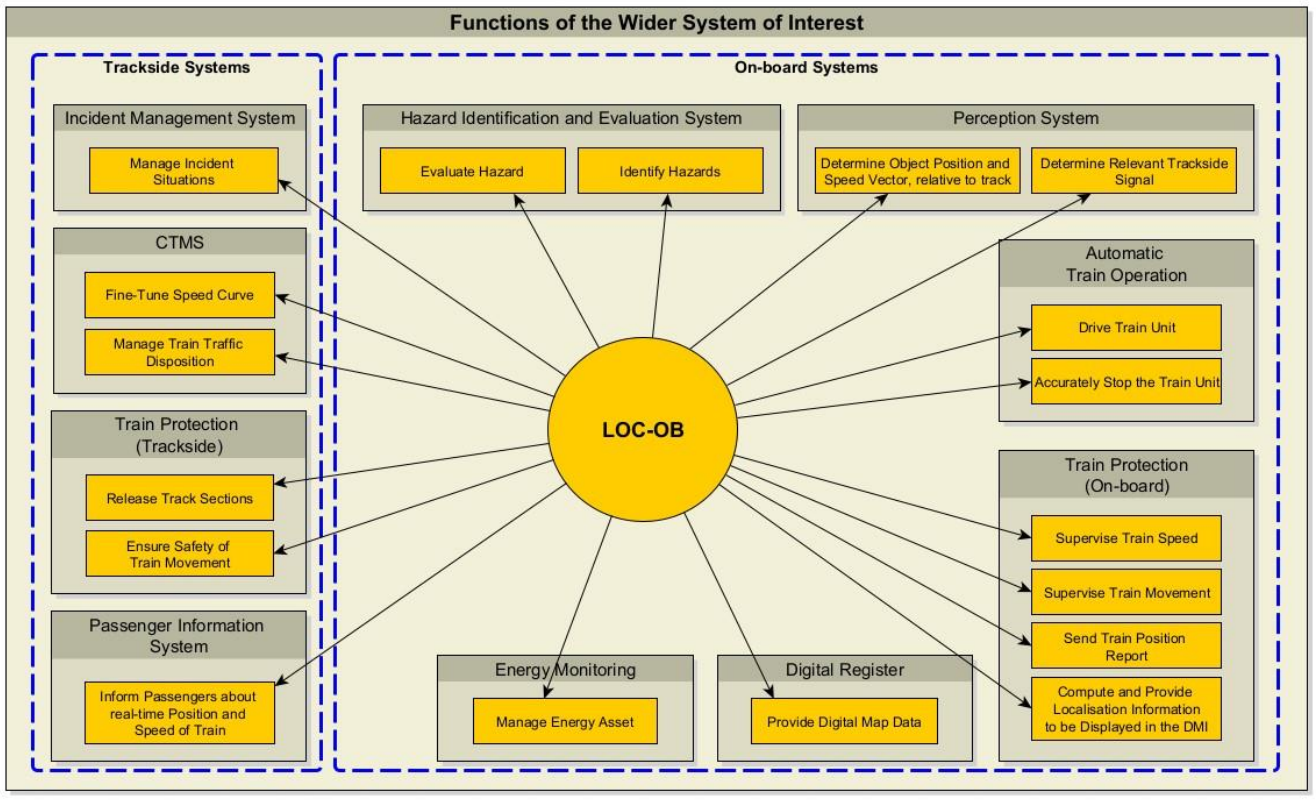


Figure 1 - LOC-OB Functions of Wider System of Interest (Extract from D2.1 [R26])

Besides some System Capabilities have been defined in D2.1:

SysCap [1] Provide 1D Train Front End Position

SysCap [2] Provide 1D Train Speed

SysCap [3] Provide 1D Train Acceleration

SysCap [4] Provide Train Movement Direction

SysCap [5] Intentionally deleted

SysCap [6] Provide vehicle attitude (yaw, pitch and roll)

SysCap [7] Provide 3D Position

SysCap [8] Provide 3D Speed

SysCap [9] Provide 3D Acceleration

SysCap [10] Provide Track Edge ID

2.3 LOC-OB System Definition and Boundaries

The LOC-OB system definition is given in D2.1 [R26] by a set of high-level requirements, and synthetized in the following table:

Req ID	Requirement
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
UR[002]	LOC-OB shall provide acceleration, velocity and position in a common 3D reference system.
UR[003]	LOC-OB shall provide vehicle attitude in a common 3D reference frame.
UR[004]	After being powered up and its initialisation stage ended, LOC-OB shall provide data continuously.
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.
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.
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.
UR[008]	Intentionally deleted.
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.
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.
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].
UR[012]	LOC-OB shall guarantee all its functionalities for trains running up to 500km/h.
UR[013]	LOC-OB shall add economic benefits (opex and capex) to IM and RU in comparison to odometry definition [SS041].

Req ID	Requirement
UR[014]	LOC-OB shall be designed as an independent constituent of the Control Command and Signalling On-Board (CCS-OB) with standardised interfaces.
UR[015]	LOC-OB shall be a constituent separated from the core ETCS through a standardised interface.
UR[016]	LOC-OB being an electronic embedded component, LOC-OB shall comply with applicable environmental standards.
UR[017]	Intentionally deleted.
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). - 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 [SS041].
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.
UR[021]	LOC-OB shall not degrade safety toward odometry as defined in the ETCS BL3 R2.
UR[022]	The true train position shall be always inside the confidence interval.
UR[023]	The true train speed shall be always inside the confidence interval.
UR[024]	The true train acceleration shall be always inside the confidence interval.
UR[025]	Each localisation information shall fulfil safety target requirements in accordance with the user's application requirements.
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.

Table 1 - LOC-OB High level requirements (extract from D2.1)

The boundaries of the LOC-OB system are defined in D2.3: the LOC-OB is a CCS on-board component of the OCORA architecture.

2.4 External Functions Identification (Application users)

The external functions of the LOC-OB system are defined in D2.3 [R28], from the list of interface functions defined in LWG-EUG project (see [R24]):

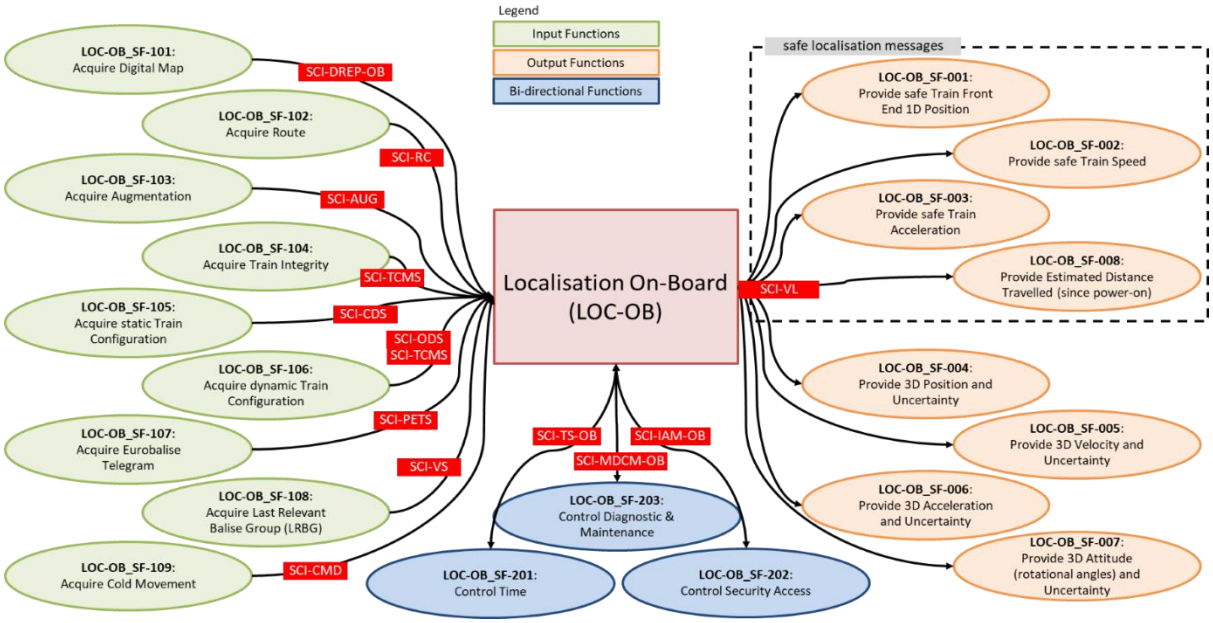


Figure 2 - LOC-OB interface Functions (extract from LWG-EUG [R24])

For a more detailed description of the functions, see [R28].

3 RAMS OBJECTIVES AND MANAGEMENT

3.1 Railway legislative context

The preliminary phase of the system definition and system requirements defines the limits of the system and its main components. This first phase is a prerequisite before carrying out a risk assessment for identifying system behaviour leading to unsafe events, to danger and is defined during the WP2 CLUG 2.0 project, see §2.

For railway operations, safety is of the most importance and must be carefully monitored and assessed all along the life cycle of system and products from the engineering phases to the operation and maintenance activities until the system, the products are removed from operation.

At European Union level, the legislation sets the framework for harmonized approach to rail safety across the European Union. It lays down the conditions for granting the safety certifications that every railway company must obtain before it can run trains on the European network.

Among harmonized safety regulations, the Common Safety Methods (CSMs) [R8] and [R9] describe how the safety levels, the achievement of safety targets and compliance with other safety requirements should be fulfilled[1]. The CSMs are established in accordance with the Directive (EU) 2016/798 [R6]. Six CSMs adapted for various purposes have been elaborated by the European Commission:

- CSM for risk evaluation and assessment
- CSM for monitoring
- CSM on safety management system requirements
- CSM on supervision
- CSM on common safety targets
- CSM for conformity assessment

The CSMs are directly applicable and enforceable in the Member States. Depending on their scope, they are applied either by authorities or bodies, or by specific actors of the railway system (e.g. railway undertakings, infrastructure managers, entities in charge of maintenance), or even by both.

The CSM for Risk evaluation and Assessment (CSM-RA) is commonly used in the railways to assess risks and elicit safety measures and requirements and is proposed to be used for the activities of WP3. The CSM-RA is established by two EC Regulations:

- Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009 [R8]

[1] https://www.era.europa.eu/activities/common-safety-methods_en

- Commission Implementing Regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment [R9]

These Regulations set out the risk assessment process to be applied in case of technical, operational, or organisational changes, the criteria to be fulfilled by the assessment body and the harmonised design targets for technical systems.

The CSMs support CENELEC 5012x series of standards or IEC 61508 standard to demonstrate the achievement of quantified design targets and to cope with systematic failures which cannot be quantified.

For the RAMS analysis, the following railway related standards have been identified:

- EN 50126-1:2017- The specification and demonstration of reliability, availability, maintainability, and safety (RAMS)- Part 1: Generic RAMS Process [R1]
- EN 50126-2:2017- The specification and demonstration of reliability, availability, maintainability, and safety (RAMS)- Part 2: System approach to safety [R2]

The EN 50126 standard aims at introducing reliability, availability, maintainability, and safety (RAMS) management process in the railway sector and enabling the implementation of a consistent approach to the management of the RAMS parameters. In all WP3 activities, and to ease the reuse of CLUG 2.0 results in the future, the EN 50126 terminology is used wherever applicable.

Within the framework of the CLUG 2.0 project, the CLUG 2.0 demonstrator is required to be compatible with the ETCS architecture. Accordingly, the following references will be considered as applicable within the context of the CLUG 2.0 safety analysis:

- Glossary of Terms and Abbreviations (UNISIG Subset 023) [R15]
- System Requirements Specifications (UNISIG Subset 026) [R16]
- Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2 (UNISIG Subset 091) [R18]
- ETCS Application Level 2 - Safety Analysis (Parts 1 & 2) (UNISIG Subset 088) [R17]

3.2 Risk Analysis Objectives

According to CSM-RA, the Risk Analysis takes place only in case of “significant change”. In the case of the LOC-OB the following significant changes are identified:

- The OCORA architecture, in which is included the LOC-OB, is new and different of what was previously done by the industrials, with identification of independent components.
- Due to this new architecture the localisation function is now redefined independently of the whole ERTMS functions.
- LOC-OB input interfaces have been deeply redefined with use of new kind of sensors to replace odometer systems.

LOC-OB is a subsystem of the OCORA system, and it contributes also to the overall performance of the system ERTMS/ETCS. Thus, the requirements of the European Common Safety Methods [R8] and [R9] of risk management process description for the railway systems implementing a **significant change** shall be covered. Such risk management process shall be described for the application to place in service of a train embedding the new LOC-OB.

Based on this safety management policy, a Safety Definition Document shall be defined for the new vehicle to be set into service, from which are deduced the high-level safety target for the LOC-OB system. In the context of CLUG 2.0, as research project without operational context clearly identified, the high-level safety target are defined in WP2 deliverables [R26] and [R29], and are validated in WP3.

The RAM strategy is also defined, usually, by the railway operator for the new vehicle to place in service, to be declined for the LOC-OB system. In the context of CLUG 2.0, the RAM targets will be defined in WP2 deliverables [R26] and [R29].

3.3 Safety Management

The safety strategy implements the principles defined in the CENELEC standards ([R1] and [R2]). Safety takes precedence over all other aspects of rail operation. The safety program will create awareness throughout the entire project that accident prevention and protection of humans and property are of overriding importance and will receive top priority, support and participation from all participants. Safety issues will be considered from the very beginning of the project (during design phase) and will continue through manufacturing, integration, commissioning, and revenue service. The main safety objective is the identification and elimination/control of hazards that could lead to injury, loss of life, or damage to equipment.

This objective will be achieved as outlined in this document, in the context of the CLUG 2.0 demonstrator.

The risk analysis is the first step in the system safety process to identify and categorize hazards associated with the operation of the system and will be covered during the CLUG 2.0 project by the T3.2 task (see § 4.3). The method used to carry out the risk analysis follows the principles applicable to the risk management process defined in the CSMs.

Further safety analysis will be conducted during the CLUG 2.0 project, in the scope of the definition of the system as provided by WP2 and WP4 (see Task descriptions T3.3 §4.4, T3.4 §4.5 and T3.5 §4.6).

As required by the [R8], [R9] and [R1], in the context of an industrial project, an Hazard Log shall be initialized at the early stage of the project, to log all the risk identified during the life cycle and related to the LOC-OB system and its environment, and the assessment of these risks. Control and completion of the hazard log are reported in the final Safety Case. The Safety Case contains also all the required conclusions to assess the compliance of the LOC-OB system with the safety requirements.

However, as the aim of CLUG 2.0 is a demonstrator and not an industrial and market-ready system, only the early phases described in the EN50126-1 (see Figure 3 - Phases of V-cycles as defined in 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", will be performed in WP3. Hazard Log and Safety Case will not be produced during the CLUG 2.0 project.

3.4 RAM Management

In the context of an industrial project the task of the RAM management is to plan, coordinate and execute the necessary activities to achieve the required RAM performance of the system. As CLUG 2.0 is a demonstrator and not an industrial system a RAM demonstration will not be performed.

In the CLUG 2.0 project a RAM analysis based on the system definition will be performed.

RAM requirements and failure categories are defined in Loc-OB System requirements, v1.0 [R29] as follows:

- Minor failure
  A minor failure of the LOC-OB hardware could lead to a warning information requiring service intervention within a failure specific period to prevent reduced performance.
- Reduced service failure
  A reduced service failure of the LOC-OB hardware could lead as a consequence to reduced performance.
- Immobility failure
  A failure of the LOC-OB hardware that could lead to immobility, for instance in case of a transition into the System Failure (SF) mode.

4 RAMS ACTIVITIES

4.1 High Level Description

4.1.1 Objectives

The main objective of WP3 is to specify RAMS requirements and to precise, in the limit of the known operational context as defined in WP2, the RAMS targets for the CLUG LOC-OB. The work is based on the previous analysis performed by the EUG-LWG, as well as the work of the CLUG project and the OCORA project and will be conducted with respect to Common Safety Methods and CENELEC standards.

More specifically, the objectives are:

- To specify the Reliability, Availability, Maintainability and Safety (RAMS) requirements in line with the overall SIL criteria of a railway embedded system to obtain a certifiable CLUG Localisation On-Board (LOC-OB) System.
- To analyse the CLUG LOC-OB functional system architecture and interfaces and allocate the specified RAMS targets.
- To consolidate the remaining work to be performed to obtain a certifiable localisation unit in the future.

The activities defined in WP3 must aim to provide a risk assessment of the LOC-OB system as defined in EN50126. As the material architecture will be not defined during the project, the risk evaluation as defined in EN50126 is not covered during the CLUG 2.0 project.

4.1.2 Planned activities

The RAMS activities are defined according to the phases of the V-cycle defined in [R1] in Figure 3 - Phases of V-cycles as defined in EN50126-1.

In this plan, only the activities related to RAMS and perform during the early phases ("*Risk Assessment*") are covered.

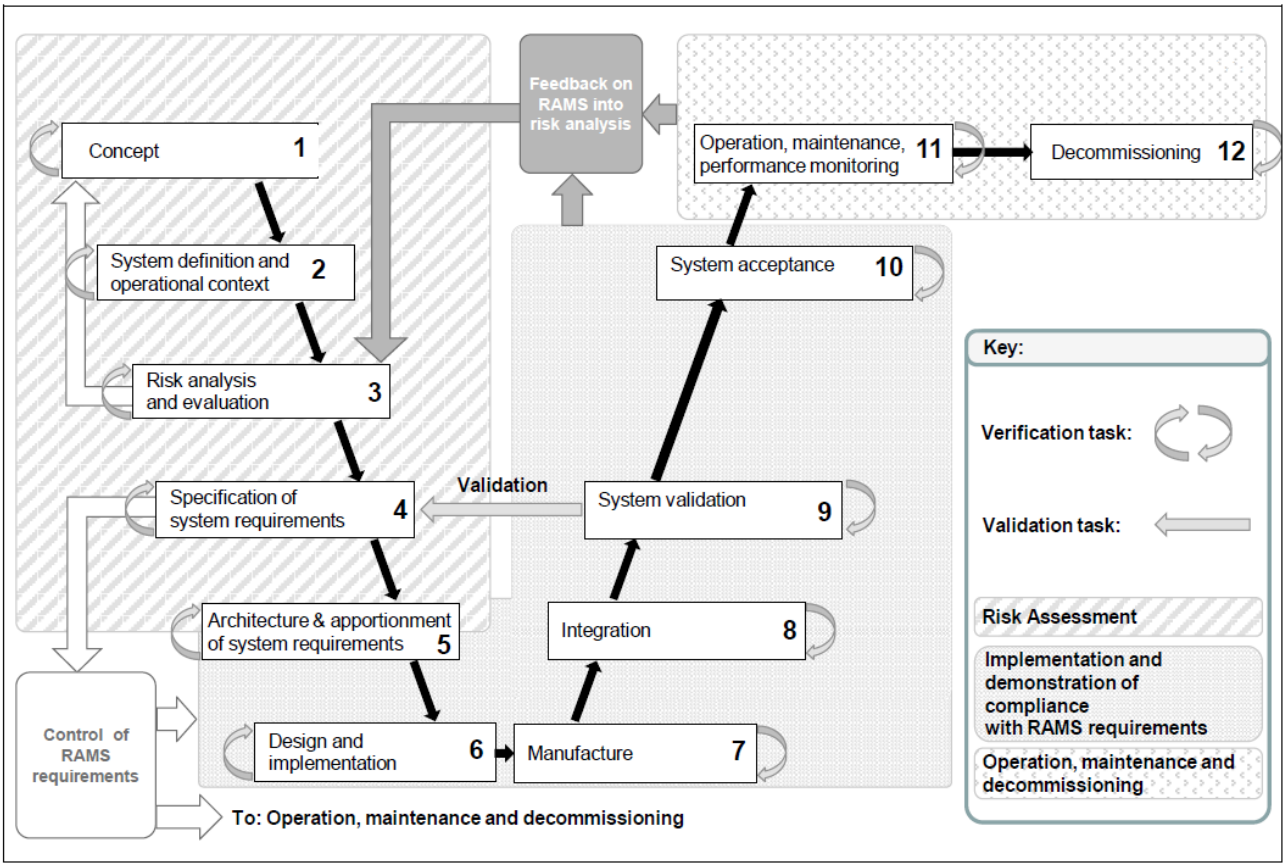


Figure 3 - Phases of V-cycles as defined in EN50126-1

RAMS objectives will be identified during the T3.1 of the WP3, based on the results of previous projects as CLUG or EUG-LWG. T3.1 will also detail the Preliminary Hazard Analysis (performed during T3.2), the Safety System Analysis (performed during T3.3, T3.4 and T3.5) and the Reliability Availability Maintainability System Analysis (performed during T3.6). The T3.7 will evaluate the results of the project (data from W3, WP4 and WP5) in regards of the objectives defined during WP2 and WP3. It will also identify the remaining steps to obtain a certifiable system (as during phase 9 & 10).

Figure 4 describes the interactions between the tasks and the input required from previous projects or the other work-packages of CLUG 2.0.

Appendix: EN50126-1 traceability gives a high-level traceability with the phases description given in chapter 7 of EN50126-1 [R1].

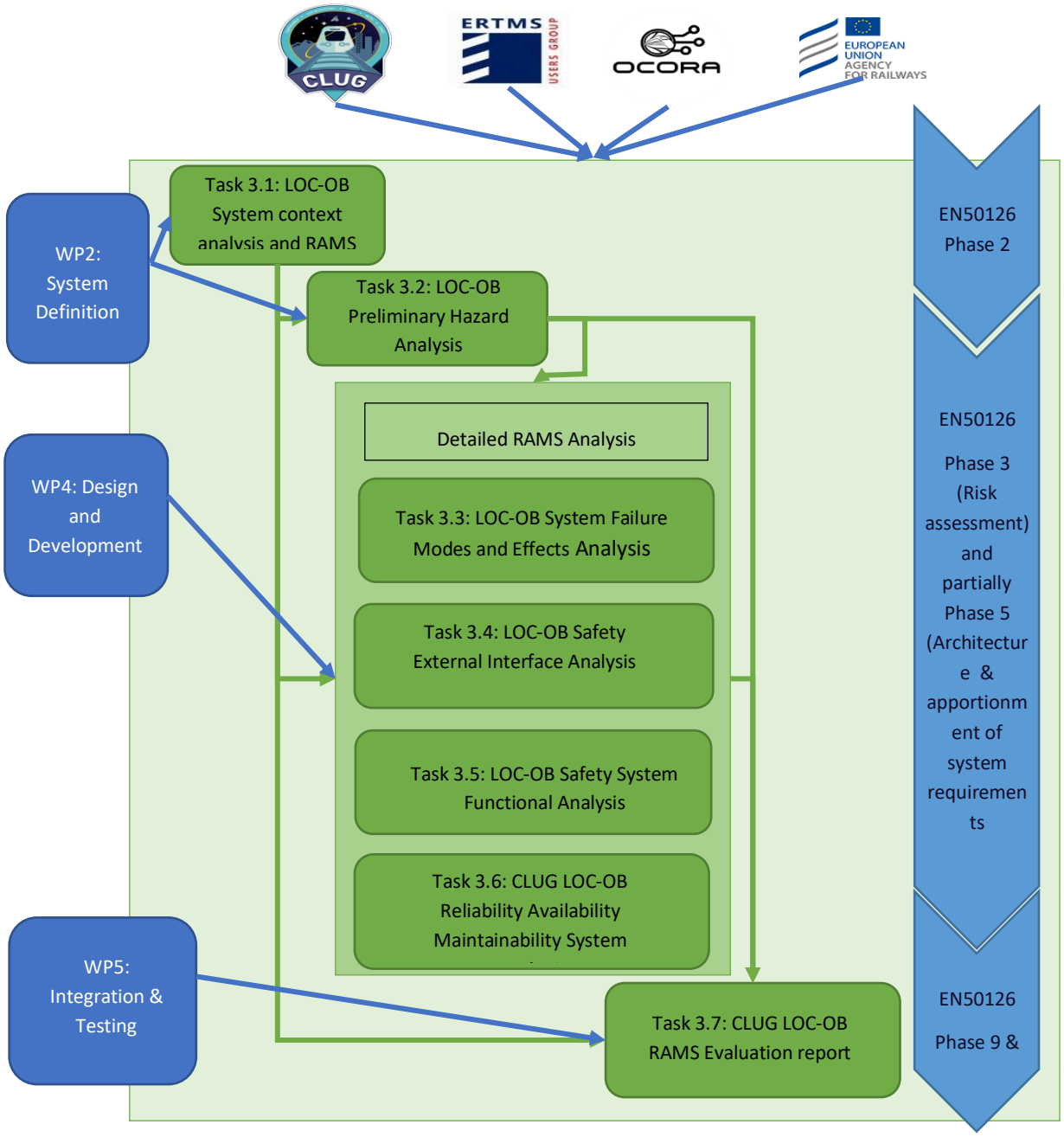


Figure 4 - WP3 tasks organisation

4.2 System context analysis and RAMS Plan (T3.1)

4.2.1 Objectives

The main activity of this task is to define and coordinate the RAMS targets and activities for the LOC-OB system. The scope of the LOC-OB system and its RAMS operational and environmental context is defined based on the descriptions provided by the WP2. In particular the trains on which the LOC-OB

system will be embedded and the surrounding systems (for example an EVC as in the OCORA architecture) will be identified.

Then the RAMS objectives to obtain a certifiable system according railway standards is described.

Finally, the RAMS activities to be carried on in Task 3.2 to Task 3.7 are detailed.

4.2.2 Methodology – Activities

D3.1 provides a common understanding of the LOC-OB system and the RAMS objectives to address during WP3.The deliverable contains:

- A description of the LOC-OB system including:
    - the operational context,
    - the definition of the system and its boundaries,
    - the operational needs and system capabilities,
    - the external functions and users' requirements.
- A description of the RAMS management during CLUG 2.0 project including a description of the RAMS policy and Strategy.
- A description of the RAMS activities conducted during the CLUG 2.0 project.

4.2.3 Inputs

The results of the CLUG project (RAMS and performance analysis) and EUG-LWG project, are considered during this task to define the scope of the system (by describing the new functions and operational contexts detailed during CLUG 2.0) or to determine the RAMS objectives, based on the Returns of Experience (ROE) of these projects. Results from other European projects as OCORA or RCA, are considered if available at the beginning of the task.

The WP2 outputs are the reference documents for the description of the LOC-OB system and its user needs:

- [CLUG2.0 – D2.1] Loc-OB Operational Needs and System Capabilities of Localisation On-Board System [R26]
- [CLUG2.0 – D2.2] Loc-OB Start of Mission and Track Selectivity [R27]
- [CLUG2.0 – D2.3] Loc-OB System boundary, Architecture, and External interfaces (incl. DM)[R28]
- [CLUG2.0 – D2.4] Loc-OB System requirements [R29]

4.2.4 Deliverables

These results will be described in a RAMS Plan (D3.1) (this document).

4.2.5 Responsible

D3.1 will be prepared by SNCF, with SMO, ADS, DBN and CAF as reviewer.

4.2.6 Coverage of EN50126

This activity aims to address a part of §7.3 of EN50126-1 [R1], that describes the requirements to define a RAM plan and a Safety Plan during the Phase 2 “System definition and Operational Context”.

4.3 Preliminary Hazard Analysis (T3.2)

4.3.1 Objectives

The main activity of this task is a Preliminary Hazard Analysis of the LOC-OB system.

The aim of this PHA is to identify the hazards, to assess the severity of the potential accidents that could occur and to mitigate the risks associated with the hazards. This analysis is based on the output elements of the ERTMS Users Group LWG, the CLUG project and the OCORA project. For example, the results of the CLUG project will be reused, consolidated and extended to the Start of Mission and Track Selectivity functions in the frame of CLUG 2.0. This PHA is conducted under the operational context defined in Task 3.1 to identify the hazards related to the use of the LOC-OB system and to address the users’ requirements.

This task will identify a list of RAMS requirements on the system as a black box (from an external viewpoint, i.e. from the users viewpoint) as it was proceeded in WP2 deliverables. For the PHA, the analysis will be limited to the outputs, inputs and when possible extended to some operational contexts (start of mission, automatic or manual driving,…) of the LOC-OB system. It will be based on the deliverables provided by WP2 [R26] and [R28].

4.3.2 Methodology

The method used to carry out the risk analysis follows the principles applicable to the risk management process defined in the CSMs and depicted in the Figure 5 see Guide for the application of the Commission Regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of the Railway Safety Directive [R5].

The main phases of the risk analysis can be defined as follows:

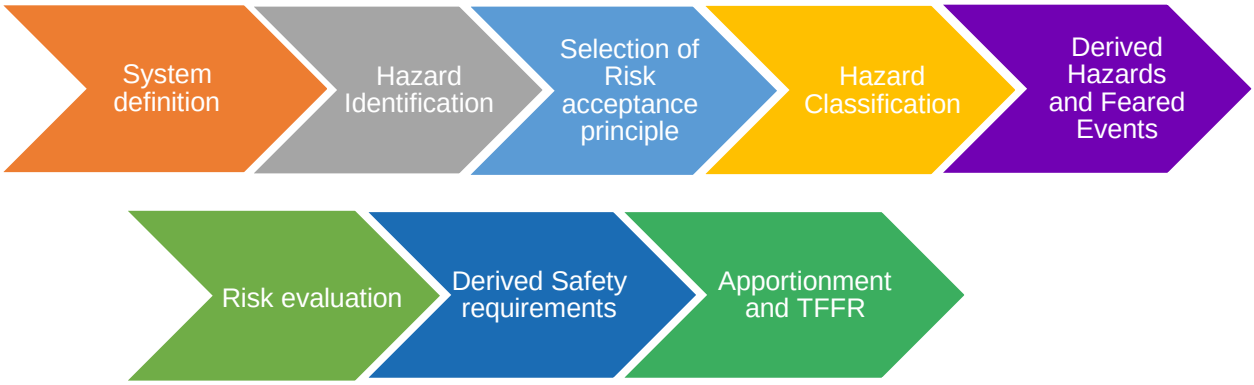


Figure 5 - Risk analysis methodology

The detailed methodology of each step will be given in the deliverable LOC-OB Preliminary Hazard Analysis (D3.2).

4.3.3 Inputs

Results from CLUG project, EUG-LWG project and other European projects as OCORA or RCA, are considered available at the beginning of the task. The current versions of subset 88 [R17] and 91 [R18] are also considered as input references.

The WP2 outputs are the reference documents for the description of the LOC-OB system and its user needs:

- [CLUG2.0 – D2.1] Loc-OB Operational Needs and System Capabilities of Localisation On-Board System [R26]
- [CLUG2.0 – D2.2] Loc-OB Start of Mission and Track Selectivity [R27]
- [CLUG2.0 – D2.3] Loc-OB System boundary, Architecture, and External interfaces (incl. DM)[R28]
- [CLUG2.0 – D2.4] Loc-OB System requirements [R29]

4.3.4 Deliverables

These results will be described in the LOC-OB Preliminary Hazard Analysis (D3.2) with the list of feared events where the LOC-OB is involved and associated targets (Safety & RAM).

4.3.5 Responsible

SNCF will prepare the D3.2 with the support of ADS as co-writer of the PHA.

DBN and SMO will support SNCF through workshops and meetings and will act as reviewer.

4.3.6 Coverage of EN50126

This activity aims to address a part of §7.3 of EN50126-1 [R1], that describes the requirements for the Phase 3 “Risk analysis and evaluation”.

4.4 System Failure Modes and Effects Analysis (T3.3)

4.4.1 Objectives

The aim of this WP is to provide a FMEA on the LOC-OB system in order to analyse the single failure impact and identify potential safeguards on each function of the system or external safeguards. This FMEA will complete the PHA (which is limited to an external point of view) with a view of the inside of the LOC-OB system.

This WP will identify a list of RAMS requirements on the system (from an internal viewpoint).

4.4.2 Methodology

This more detailed safety analysis will focus on a detailed FMEA of the failure mode of the functions and components of the LOC-OB system. This table bottom-up analysis will complete a top-down fault tree analysis to allocate the feared events identified in the PHA to the internal function and component according to the functional architecture available.

The detailed methodology of this activity will be given in the deliverable LOC-OB FMEA (D3.3), according to architecture and system description defined in WP4.

As a material architecture will not be provided, the analysis will be limited.

4.4.3 Inputs

The PHA (T3.2) is the main input of this task.

The internal system description will be provided by the deliverables of WP4:

- [CLUG2.0 – D4.1] Loc-OB Functional System Architecture [R30]
- [CLUG2.0 – D4.9] Start of Mission preliminary design [R32]
- [CLUG2.0 – D4.10] On board Digital Map definition and interfaces [R33]

4.4.4 Deliverables

These results will be described in a LOC-OB System FMEA (D3.3).

4.4.5 Responsible

D3.3 will be prepared by SNCF.

SMO, ADS, DBN and CAF will support SNCF through workshops and meetings and will act as reviewer.

4.4.6 Coverage of EN50126

This activity aims to address a part of §7.3 of EN50126-1 [R1], that describes the requirements for the "Phase 5: Architecture and apportionment of system requirements".

4.5 External Interfaces Safety Analysis (T3.4)

4.5.1 Objectives

The main activities will be to complete the PHA defined in T3.2 by a detailed safety analysis on the external interfaces of the system. It will focus on how the data are exchanged with the external actors.

This task will identify a list of safety requirements on the system (in particular on the interfaces) and focusses in particular to the interfaces requirements linked to a modular onboard architecture as OCORA (Data exchanged, Standard Communication Interface, …).

4.5.2 Methodology

This more detailed safety analysis will focus on the external interfaces and failure related to the inputs and outputs of the failure mode of the LOC-OB system.

The detailed methodology of this activity will be given in the deliverable LOC-OB External Interface Analysis (D3.4), according to architecture and system description defined in WP4.

However, as a material architecture will not be provided, the analysis will be limited.

4.5.3 Inputs

The PHA (T3.2) is the main input of this task. The OCORA documents [R21] and [R22] will be used to provide a description on the system in which the LOC-OB will be integrated.

The internal system description will be provided by the deliverables of WP4:

- [CLUG2.0 – D4.1] Loc-OB Functional System Architecture [R30]
- [CLUG2.0 – D4.9] Start of Mission preliminary design [R32]
- [CLUG2.0 – D4.10] On board Digital Map definition and interfaces [R33]

4.5.4 Deliverables

These results will be described in a LOC-OB External interfaces Analysis (D3.4).

4.5.5 Responsible

D3.4 will be prepared by SNCF.

SMO, DBN and CAF will support SNCF through workshops and meetings and will act as reviewer.

4.5.6 Coverage of EN50126

This activity aims to address a part of §7.3 of EN50126-1 [R1], that describes the requirements for the "Phase 5: Architecture and apportionment of system requirements".

4.6 System Functional Safety Analysis (T3.5)

4.6.1 Objectives

The system functional analysis on the localization function will be conducted to consolidate the PHA and Safety System Analysis and validate the functional system specification and the architecture defined in WP2. Fault tree Analysis and FMEA techniques will be included in this task. Especially, the Start of Mission and Track Selectivity functionalities of the whole embedded system as described in [R27] will be analysed in detail.

This task will identify a list of safety requirements on the system related to the functions analysed.

4.6.2 Methodology

Detailed FMEAs of specific functions (SoM and Track Selectivity) are performed in D3.5. The resulting Risk Control Measures (and SRAC's if directed to systems outside of CLUG 2 scope) are formulated as testable system safety requirements. (Testability of requirement is proven by providing feasible "test verification criteria" on system level). Additional safety functions might be identified and described. It is foreseeable that the result depends on many assumptions. Part of the approach will be to estimate how much a single assumption might influence the outcome in terms of safety needs.

Depending on completeness and stability of available architecture the Risk Control Measures will be linked to logical function elements to support usage of system level FTA analysis.

4.6.3 Inputs

The results of the PHA (T3.2), completed by the results of FMEA (T3.3), are the main inputs of this task. The OCORA documents [R21] and [R22] will be used to provide a description on the system in which the LOC-OB will be integrated.

The description of the functionalities are given by the WP2 deliverable:

- [CLUG2.0 – D2.2] Loc-OB Start of Mission and Track Selectivity [R27]

The internal system description will be provided by the deliverables of WP3 and WP4:

- [CLUG2.0 – D4.1] Loc-OB Functional System Architecture [R30]
- [CLUG2.0 – D4.8] Track Selectivity Determination algorithm design document [R31]
- [CLUG2.0 – D4.9] Start of Mission preliminary design [R32]
- [CLUG2.0 – D4.10] On board Digital Map definition and interfaces [R33]

4.6.4 Deliverables

These results will be described in a LOC-OB System Functional Analysis (D3.5). It contains the function related portion of safety requirements specification that outlines the safety goals, safety functions and safety requirements for the system.

4.6.5 Responsible

D3.5 will be prepared by DBN.

SMO, SNCF, ADS and CAF will support DBN through workshops and meetings and will act as reviewer.

4.6.6 Coverage of EN50126

This activity aims to address a part of §7.3 of EN50126-1 [R1], that describes the requirements for the “Phase 5: Architecture and apportionment of system requirements”.

4.7 Reliability Availability Maintainability System Analysis (T3.6)

4.7.1 Objectives

The main activity of this task is to perform a Reliability and Availability analysis of the LOC-OB system.

This analysis is based on the system definition and architecture provided by WP2 and WP4 of the CLUG 2.0 project.

4.7.2 Methodology

The Reliability and Availability analysis will focus on a FMEA of the failures of the components of the LOC-OB system.

The detailed methodology of this activity will be given in the deliverable Preliminary System Reliability and Availability analysis (D3.6), once draft versions of WP4 documents will be provided.

4.7.3 Inputs

The main input of this task are the system descriptions provided by the deliverables of WP2 and WP4:

- [CLUG2.0 – D2.3] Loc-OB System boundary, Architecture, and External interfaces [R28]
- [Loc-OB_22E126] Loc-OB System Definition & Operational Context, v1.1, 30/11/2022 [R24]
- [CLUG2.0 – D4.1] Loc-OB Functional System Architecture [R30]
- [CLUG2.0 – D4.9] Start of Mission preliminary design [R32]
- [CLUG2.0 – D4.10] On board Digital Map definition and interfaces [R33]

4.7.4 Deliverables

The results will be described in Preliminary System Reliability and Availability analysis (D3.6).

4.7.5 Responsible

D3. 6 will be prepared by SMO.

SNCF, DBN and CAF will support SMO through workshops and meetings and will act as reviewer.

4.7.6 Coverage of EN50126

This activity aims to address a part of §7.3 of EN50126-1 [R1], that describes the requirements for the "Phase 4: Specification of system requirements"" and "Phase 5: Architecture and apportionment of system requirements".

4.8 RAMS Evaluation report (T3.7)

4.8.1 Objectives

The main activities will be 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. A synthesis of how the RAMS requirements are covered by these WPs will also be made.

Then the remaining effort to obtain an authorization agreement will be identified according to the CSM-RA 403/2013 [R8] and PAVA 545/2018 [R7] and the CENELEC standards [R1], [R2], [R3] and [R4].

4.8.2 Methodology

The document will be a synthesis of the results of WP3 regarding the RAMS activities.

It will also provide some conclusions and recommendations on the future steps to the development of an industrial product.

4.8.3 Inputs

All the deliverables of WP2, WP3, WP4 and WP5 are inputs for this task.

4.8.4 Deliverables

The results will be described in the LOC-OB System Evaluation report (D3.7).

4.8.5 Responsible

D3.7 will be prepared by SNCF.

SMO, ADS, DBN and CAF will support SNCF through workshops and meetings and will act as reviewer.

4.8.6 Coverage of EN50126

This activity aims to address a part of §7.3 of EN50126-1 [R1], that describes the requirements for the “Phase 9: System Validation” and “Phase 10: System acceptance”.

5 CONCLUSION

According to the criteria defined by the CSM RA, the potential impact induced by the implementation of the LOC-OB system on the safety of the railway system should be considered as a **significant change.** Thus, it is essential to follow the risk management recommendations described, and therefore to carry out risk analyses as part of CLUG 2.0.

This document describes 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 in the future. These results will be synthetized in T3.7.

6 APPENDIX: EN50126-1 TRACEABILITY

This appendix with provide a high level traceability of the activities proposed in this RAMS plan in regards to EN50126-1 [R1].

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" will be described in this document (see Figure 3 - Phases of V-cycles as defined in EN50126-1.

EN50126-1 section	Coverage in this document	Comments
7.3 Phase 2: System definition and operational context	-	-
7.3.1 Objectives The objectives of this life cycle phase are: **a)** define the system and its mission profile; **b)** define the boundary of the system; **c)** establish the operational requirements influencing the characteristics of the system; **d)** define the scope of system risk analysis; **e)** establish the initial RAM plan for the system; **f)** establish the initial Safety plan for the System; **g)** define the functions to be provided by the system; **h)** define the organisation for RAM and safety management of the system; as far as they affect the potential RAMS performance of the system.	§2 §1 and §3 §4.2 §1.4.1	System definition, mission and boundaries and operational requirements and functions are described in WP2 documents, as remind in §2 here. Scope of the RAMS activities are given in §1, Scope of the risk analysis in §3. Establishing the initial RAM and Safety plan is the aim of this document. Organisation is out of scope of the project.

EN50126-1 section	Coverage in this document	Comments
7.3.2 Activities	-	-
7.3.1 Objectives	-	-
7.3.2.1 General Before any analysis relating to RAMS is undertaken (e.g. hazard identification), boundaries and functions of the system under consideration shall be established. […]	§2	Describe in WP2 documents, as remind in §2 here.
A RAMS policy shall be established which shall include a policy for resolving conflicts between safety and other aspects like availability, reliability, etc.	§3	The policy is described only on the context of the production of a demonstrator.
An organisation shall be established which shall allocate the roles, responsibilities, competencies, independencies and relationships of organisations undertaking RAMS tasks within the life cycle process. This shall also serve to resolve conflicts as indicated above.	§1.4.1	Organisation is out of scope of the project.
A process for on-going consideration of safety issues and the communication of relevant system safety requirements between the stakeholders should be established. This	§1.4.1	Organisation and RAMS Management is out of scope of the project.

EN50126-1 section	Coverage in this document	Comments
includes the review of the adequacy of the safety requirements if new findings call for reconsiderations.		
7.3.2.2 RAM Plan The RAM plan for the remaining life cycle tasks shall be established, reviewed and maintained throughout the life cycle of the system. The RAM plan shall include the tasks which are judged to be the most effective to the attainment of the RAM requirements for the system under consideration. The RAM plan should be agreed by the railway duty holder and the railway suppliers for the system under consideration. […]	§3.4 and §4.2	This document. RAM activities are limited to those can be afforded for the production of a demonstrator, without operational context formally identified.
7.3.2.3 Safety Plan The Safety Plan for the system shall be established. The Safety Plan shall be implemented, reviewed and maintained throughout the life cycle of the system. Thus it is necessary to define the relationship between the involved stakeholders. […]	§ 3.3 and §4.2	This document. Safety activities are limited to those can be afforded for the production of a demonstrator, without operational context formally identified.
7.3.3 Deliverables	§1.4, §2 and § 4.2.4	System definition is provided by WP2.

EN50126-1 section	Coverage in this document	Comments
The results of this life cycle phase shall be documented, including: a) a system definition; b) a RAM plan; c) a safety plan. This documentation shall include any assumptions and justifications made during this life cycle phase.		
7.4 Phase 3: Risk analysis and evaluation	-	-
7.4.1 Objectives The objectives of this life cycle phase are to: a) identify and classify hazards / RAM equivalents associated with the system; b) select risk acceptance principles (RAP); c) define and apply risk acceptance criteria (RAC); d) assess risks; e) establish a process for on-going risk management. […]	§4.3	Risk identification, acceptance principles, acceptance criteria and risk assessment are defined in the WP3 PHA of the project (deliverable D3.2). However the risk management (including hazard log definition) is out of scope of the project.

EN50126-1 section	Coverage in this document	Comments
7.4.2 Activities	-	-
7.4.2.1 Risk assessment Risk assessment for the system under consideration, includes also the system definition phase (life cycle phase 2) and shall be undertaken in accordance with the requirements given in 6.3. Risk assessment comprises risk analysis and risk evaluation. […]	§4.3	Detailed activities of the risk assessment, including limits and assumptions, will be given in D3.2.
7.4.2.2 Hazard Log A hazard log shall be established as the basis for on-going risk management for safety. It represents a tool to track hazards and their closure. The hazard log shall be updated throughout the life cycle whenever a change to identified hazards occurs or a new hazard is identified. […]	§1.4.1	Hazard log definition and management is out of scope of the project.
7.4.3 Deliverables The results of this life cycle phase shall be documented, including: a) the risk assessment; b) the hazard log;	§4.2.4 and §4.3.4	This document and D3.2.

EN50126-1 section	Coverage in this document	Comments
c) updated safety plan (if appropriate); d) updated RAM plan (if appropriate); e) establish indipendent safety assessment plan (if appropriate). This documentation shall include any assumptions and justifications made during this life cycle phase.		
7.5 Phase 4: Specification of system requirements	-	-
7.5.1 Objectives The objectives of this life cycle phase are to: a) specify the overall RAMS requirements for the system under consideration; b) specify the overall demonstration process and criteria for acceptance of RAMS of the system; c) provide a comprehensive and identified set of requirements for the subsequent life cycle phases; d) specify necessary monitoring requirements according to the process for analysing operation and maintenance performance arranged in the	§4.3, §4.4, §4.5, §4.6, §4.7 and §4.8	Identification of the RAMS requirements will be made in each deliverable of WP3 according to the deliverable of WP2. No demonstration or monitoring will be performed during this project, but a synthesis list of the RAMS requirements will be given in D3.7.

EN50126-1 section	Coverage in this document	Comments
Safety Plan (that enable the system to perform the required tasks in life cycle phase 11).		
7.5.2 Activities The overall RAMS requirements for the system shall be specified on the basis of the system definition of sub-clause 7.3 and the risk analysis and evaluation of sub-clause 7.4. The RAMS requirements for the system under consideration shall include: […]	§4.3, §4.4, §4.5, §4.6, §4.7 and §4.8	The identification of the requirements is made mainly in WP2 and WP4. This first list of RAMS requirements is challenged and completed in WP3 (especially PHA and System Analysis).
7.5.3 Deliverables The results of this life cycle phase shall be documented, including a) the RAMS system requirements specification; b) Safety-Related Application Conditions (if appropriate); c) updated hazard log (if appropriate); d) updated safety plan (if appropriate); e) updated RAM plan (if appropriate); f) the Validation Report covering phases 1 to 4;	§4.3.4 and §4.8.4	A first set of RAMS requirement will be identified with the PHA (D3.2) and a final list will be given in the synthesis (D3.7). No demonstration will be performed during the project.

EN50126-1 section	Coverage in this document	Comments
g) RAM validation plan for the subsequent phases; h) Safety validation plan for the subsequent phases. This documentation shall include any relevant assumptions and justifications made during this life cycle phase.		
7.5.4 Specific validation tasks General requirements for validation tasks are described in 6.7.3. […]	-	Validation is out of scope of this project.
7.6 Phase 5: Architecture and apportionment of system requirements		
7.6.1 Objectives The objectives of this life cycle phase are to: a) apportion the system RAMS requirements to the designated subsystems and/or components; b) design subsystems and components that work together as a system which fulfils the required functions at the system level;	§4.4, §4.5, 4.6 and § 4.7	System and subsystem RAMS analysis will be performed during task T.3.3, T3.4, T3.5 and T3.6 according to the inputs provided by WP4.

EN50126-1 section	Coverage in this document	Comments
c) describe the RAMS requirements and specify the interfaces for all subsystems and components derived from the RAMS requirements (which prepares later integration activities); d) define the acceptance criteria to demonstrate fulfilment of the RAMS requirements for the system, subsystem, equipment in subsequent lifecycle phases; e) identify and evaluate the significance of the interactions between the subsystems. NOTE Interactions can be defined at different abstraction levels. Such interactions can be described in interface specifications.		
7.6.2 Activities A system architecture shall be developed and defined that fulfils the RAMS requirements. The architecture shall be based on a structured decomposition into subsystems and/or components with completely defined interfaces between the subsystems and/or components. For each subsystem or component a set of RAMS requirements shall be allocated which is derived from the system requirements	§4.4, §4.5, 4.6 and § 4.7	System and subsystem RAMS analysis will be performed during task T.3.3, T3.4, T3.5 and T3.6 according to the inputs provided by WP4. Details of the activities will be provided in each document. No demonstration will be performed during the project.

EN50126-1 section	Coverage in this document	Comments
and from the design in sufficient depth. To achieve this, a structured design methodology shall be applied. The system architecture should be expressed and structured in a way that it is clear, precise, unambiguous, verifiable, testable, maintainable and feasible. It should aid the comprehension by those who are likely to utilise the information at any phase of the life cycle and be traceable to the system requirement. Particular attention is required for the specification of RAMS requirements for the control of interfaces where safe and reliable interaction can be compromised. Constraints on the choice of technology (i.e. independence of functions or processes of development) shall be identified. All safety-related assumptions made during the development of the system architecture shall be specified and documented. The designated subsystems and/or components shall be specified to achieve the system RAMS requirements, including the impact of common cause and multiple failures. […]		
7.6.3 Deliverables The results of this life cycle phase shall be documented, including:	§4.4.4, §4.5.4, §4.6.4 and §4.7.4	No demonstration will be performed during the project. No hazard log will be provided.

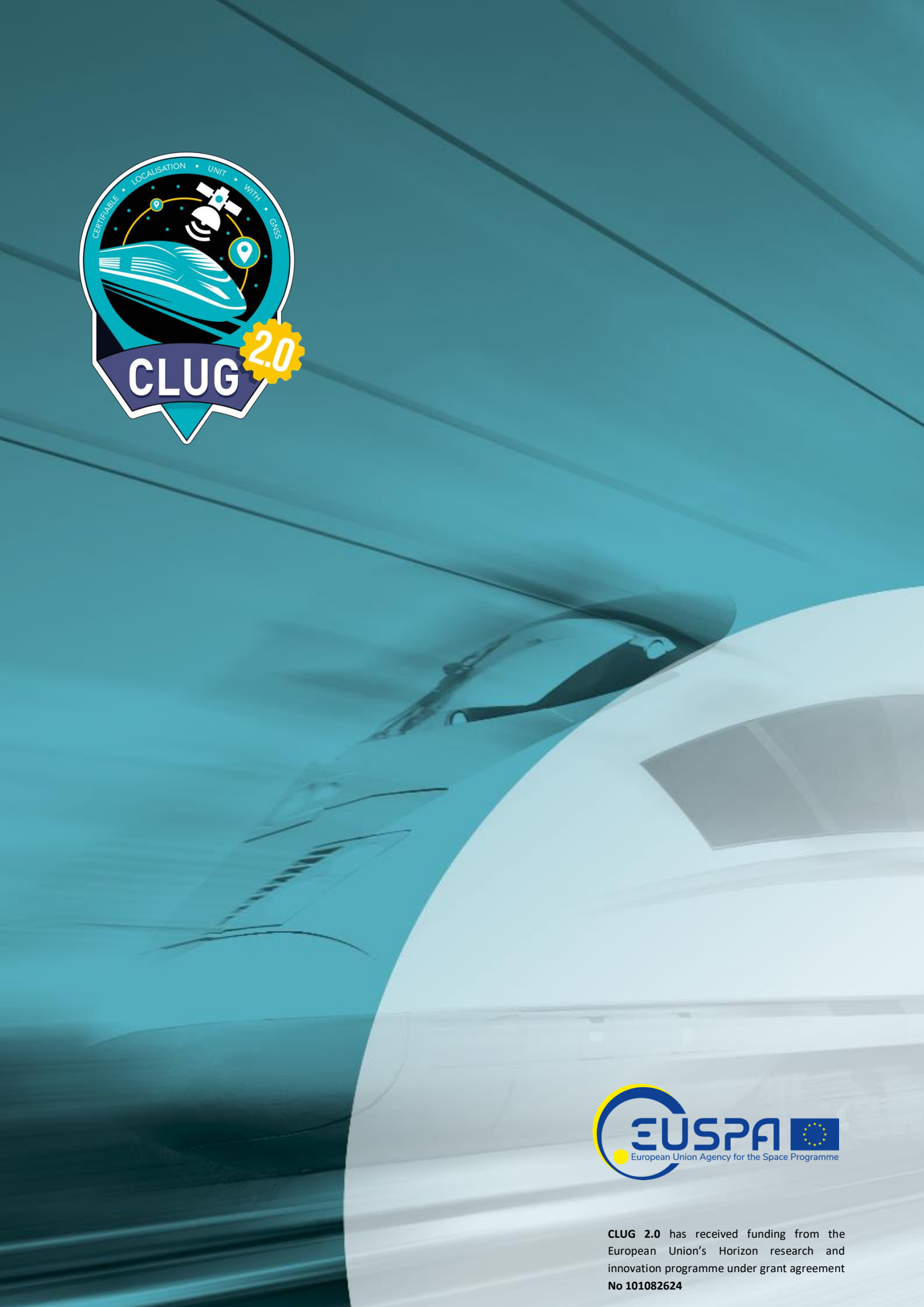
EN50126-1 section	Coverage in this document	Comments
a) system architecture (structure of decomposition into subsystems etc.) including interface specifications and system hazard analysis (architecture and hazard analysis of subsystem and components); b) allocation of RAMS requirement specification to subsystems and/or components; c) Acceptance Criteria and demonstration and acceptance processes and procedures; d) updated safety plan (if appropriate); e) updated RAM plan (if appropriate); f) updated RAM Validation Plan (if appropriate); g) updated Safety Validation Plan (if appropriate); h) updated Safety-Related Application Conditions (if appropriate); i) updated hazard log (if appropriate).		
7.7 Phase 6: Design and Implementation	-	Out of scope of the project
7.8 Phase 7: Manufacture	-	Out of scope of the project

EN50126-1 section	Coverage in this document	Comments
7.9 Phase 8: Integration	-	Out of scope of the project
7.10 Phase 9: System Validation	-	-
7.10.1 Objectives The objectives of this life cycle phase are to: a) confirm by examination and provision of objective evidence that the system under consideration in combination with its Safety-Related Application Conditions complies with the RAMS requirements; b) confirm or update the safety case for the system under consideration, according to the results of the validation.	§4.8	The synthesis D3.7 of the WP3 will give some RAMS results on the demonstrator, however no safety case or hazard log will be provided during the project.
7.10.2 Activities The general requirements on activities to be performed are described in 6.7.3. [..]	§4.8	The synthesis D3.7 of the WP3 will give some RAMS results on the demonstrator, however no safety case or hazard log will be provided during the project.
7.10.3 Deliverables The results of this life cycle phase shall be documented, including: – RAM validation report;	§4.8.4	D3.7 is limited to a synthesis of the results obtain during WP3 and the remaining steps to perform in view of an industrial product.

EN50126-1 section	Coverage in this document	Comments
– safety validation report; – updated hazard log (if appropriate); – updated safety plan (if appropriate); – updated safety case (if appropriate); – updated Safety-Related Application Conditions (if appropriate); – process for the acquisition and evaluation of operational data.		
7.11 Phase 10: System acceptance	-	-
7.11.1 Objectives The objectives of this life cycle phase are to: a) assess compliance of the total combination of subsystems, components, their interfaces and Safety-Related Application Conditions with the overall RAMS requirements; b) accept the system for entry into service. NOTE In this European Standard, the term system acceptance is used only for technical aspects of the acceptance procedure. Legal aspects of the system acceptance are not considered in this standard. It is advised	§4.8	The synthesis D3.7 of the WP3 will give the remaining steps to perform in view of a certifiable industrial product. However, no formal assessment will be done during the project.

EN50126-1 section	Coverage in this document	Comments
to clarify the legal aspects of system acceptance between the customer and the supplier in advance.		
7.11.2 Activities All system verification and validation tasks, specifically the RAMS verification & validation and the safety case, shall be assessed in accordance with the defined risk acceptance criteria. NOTE Risk acceptance criteria are given by contractual agreements or legal framework and were specified in life cycle phase 4. The results of this assessment shall be recorded in an acceptance report. The acceptance report should include a confirmation that the delivered product, system or process is fit for entry into service. The following tasks shall be undertaken by the entity which is accepting the system (railway duty holder or other): a) evaluation of the acceptance report with respect to the defined acceptance criteria; b) evaluation of the safety plan with regard to its continued applicability including the possible need of Independent Safety Assessment (if applicable); c) evaluation of the updated hazard log.	§4.8	The synthesis D3.7 of the WP3 will give the remaining steps to perform in view of a certifiable industrial product. However, no formal assessment will be done during the project.

EN50126-1 section	Coverage in this document	Comments
7.11.3 Deliverables The results of this life cycle phase shall be documented, including: - Independent Safety Assessment Report (if appropriate); - endorsement of Safety-Related Application Conditions (if appropriate); - Acceptance report. This documentation shall include assumptions and justifications made during this life cycle phase.	§4.8.4	D3.7 is limited to a synthesis of the results obtain during WP3 and the remaining steps to perform in view of an industrial product.
7.12 Phase 11: Operation, maintenance and performance monitoring	-	Out of scope of the project.
7.13 Phase 12: Decommissioning	-	Out of scope of the project.



EUSPA
European Union Agency for the Space Programme

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