



CLUG Demonstration of Readiness for Rail – CLUG 2.0

D3.2 LOC-OB PRELIMINARY HAZARD ANALYSIS

Due date of deliverable: 29/09/2023

Actual submission date: 06/06/2024

Leader of this Deliverable: Marc SARRAT, SNCF

Reviewed: Y

Document status		
Revision	Date	Description
0.1	03/04/2023	Draft version
0.2	05/05/2023	Draft version for review (parts 1, 2 and 3)
0.3	21/06/2023	Draft version for review (parts 5,6,7, 8, 9) see excel file
0.4	27/10/2023	Draft final version – full document
0.5	10/11/2023	Submitted version
1.0	20/12/2023	Submitted version - after technical review and quality check
1.1	02/05/2024	Answers on external review
1.2	30/05/2024	Submitted version (after external review)
2.0	06/06/2024	Final version officially submitted to EUSPA

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 - § Introduction - § Risk Analysis Objectives - § Risk Analysis Methodology - § LOC-OB System Definition
Marc Sarrat / Marielle Petit-Doche	SNCF	V0.2: Draft version for review - parts 2,3,4
Alain Ruaudel	ADS	V0.3: Draft version for review - parts 5,6,7, 8,9
Marc Sarrat / Marielle Petit-Doche	SNCF	
Alain Ruaudel	ADS	V0.4: Draft version for review – full document
Marc Sarrat / Marielle Petit-Doche	SNCF	
Marc Sarrat / Marielle Petit-Doche	SNCF	V05.: Submitted version for review – full document
Marc Sarrat / Marielle Petit-Doche	SNCF	V1.0: Final version
Marc Sarrat / Marielle Petit-Doche	SNCF	V1.1: Comments from external review
Marielle Petit-Doche	SNCF	V1.2: Final comments from external review taken into account after meeting with Denis DUSSO the 17/05/24

REPORT REVIEWERS

NAME	COMPANY	DETAILS OF CONTRIBUTION
Karin Nebe	SMO	V02, V0.3, V0.4
Claus Thies-Von-Der-Bey	DB Netz	V02, V0.3, V0.4
Alain Ruaudel	ADS	V0.2, V0.3, V0.4
Valérie Girard	ADS	V0.5
Kurt Jaun	SBB CFF	V0.2, V0.3, V0.4
Tarek Vennemann	SBB CFF	V0.2, V0.3, V0.4
Valentin Barreau	SNCF	V0.5, TMT validator
Mariya Kayalova	RINA-C	V1.0 and V2.0 Quality check
Jose Bertolin	UNIFE	V1.0 and V2.0 Final check and submission to reviewers and EUSPA

EXECUTIVE SUMMARY

This document is the deliverable “D3.2 – LOC-OB Preliminary Hazard Analysis” of the European project “CLUG Demonstration of Readiness for Rail” (hereinafter also referred to as “CLUG 2.0”). This document provides a preliminary safety analysis of the LOC-OB system, identifying hazards, assessing the severity of the potential accidents and identifying safeguards for reducing the risks associated with the hazards.

The PHA is based on the description of the LOC-OB system given in WP2, as a black-box: thus, the PHA focuses on the RAMS requirements of the output functions of the LOC-OB system.

The hazards were identified using several approaches in parallel to ensure optimum coverage (ERTMS subset analysis, user needs analysis, new services analysis and railway accident-based analysis).

Then the document follows the PHA method listing Hazards, providing feared events and assessment of the output functions (TFFR expected).

As conclusion of this document are provided a first list of safety requirements to be refined and complete during the further RAMS analyses, list of assumptions and a list of open points.

No part of this work may be reproduced or used in any form or by any means (graphic, electronic, or mechanical including photocopying, recording, taping, or information storage and retrieval systems) without the written permission of the copyright owner(s) in accordance with the terms of the CLUG Consortium Agreement (EC Grant Agreement 101082624).

APPLICABLE DOCUMENTS

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

- Grant Agreement N°101082624 (which includes DOW, 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.

REFERENCE DOCUMENTS

- [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 v4.0.00] 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] [CLUG1.0 – D2.4]– Preliminary Hazard Analysis and Safety Requirements
- [R27] [CLUG2.0 – D2.1] LOC-OB Operational Needs and System Capabilities of Localisation On-Board System
- [R28] [CLUG2.0 – D2.3] LOC-OB System boundary, Architecture, and External interfaces (incl. DM)
- [R29] [CLUG2.0 – D3.1] LOC-OB System Context Analysis and RAMS Plan

LIST OF ACRONYMS

ACRONYM	CONCEPTS
CCS	Control, Command and Signalling
CLUG	Certifiable Localisation Unit with GNSS in the railway environment
CSM	Common Safety Methods
DOW	Description of Work
ERA	European Railway Agency
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
FFIS	Form Fit Functional Interface Specification
HR	Hazard Rate
IEC	International Electronical Commission
LOC	Localisation
LWG	Localisation Working Group
NTC	National Train Control
OCORA	Open CCS On-board Reference Architecture
ODO	ODOMetry
PAVA	Practical Arrangements for the railway Vehicle Authorisation
PHA	Preliminary Hazard Analysis
RAMS	Reliability, Availability, Maintainability and Safety
SIL	Safety Integrity Level
SRAC	Safety Related Application Condition
TFFR	Tolerable Functional Failure Rate

ACRONYM	CONCEPTS
THR	Tolerable Hazard Rate
TSI	Technical Specification of Interoperability

CONTENTS

1	Introduction	13
1.1	Objectives of the PHA	13
1.2	Scope of the document	13
1.3	Limits and Hypotheses	14
2	Risk Analysis CONTEXT	15
2.1	Railway legislative context.....	15
2.2	LOC-OB System use	16
2.3	Risk Assessment Criteria.....	16
2.4	Accidents	18
3	Risk Analysis Methodology	19
3.1	Overall Description.....	19
3.2	Hazard Identification	19
3.3	Risk acceptance principle	20
3.4	Hazard Classification	21
3.5	Derived Hazards and Feared Events.....	21
3.6	Risk Evaluation	21
3.7	Derived RAMS Requirements	22
3.8	Apportionment and TFFR	22
3.9	Discussion on other assessment approaches	23
4	LOC-OB System Definition	24
5	Hazard identification.....	25
5.1	Fault Tree analysis.....	25
5.2	New functionalities analysis	25
5.3	New technologies/new services	25
5.4	Accident analysis.....	25
6	Derived Hazard and Fear Events.....	26



6.1	Summary of Derived Hazard for LOC-OB.....	26
6.2	Summary of Fear Events for LOC-OB.....	29
7	Risk Assessment.....	31
8	RAMS Requirements and Safety related Application Conditions	33
9	Apportionment	35
10	Assumptions and Open Points.....	36
11	Conclusion	38
12	APPENDIX A – DETAILED PHA	39



Table of figures

Figure 1: Risk analysis methodology	19
Figure 2: CLUG 2.0 Hazard Identification Process	20
Figure 3: ERTMS/ETCS apportionment between the 3 subsystems	22

List of tables

Table 1: Frequency categories as per EN50126	16
Table 2: Severity level as per EN50126	17
Table 3: SIL Level as per EN50126	17
Table 4: Risk acceptance categories as per EN50126	18
Table 5: Railway Accident	18
Table 6: PHA Table Elements.....	22
Table 7: Derived hazard and fear events	28
Table 8: Summary of feared events.....	30
Table 9: Risk Assessment of LOC-OB.....	32
Table 10: RAMS	33
Table 11: SRAC.....	34
Table 12: Safety apportionment.....	35
Table 13: Assumptions.....	36
Table 14: Open points.....	37

1 INTRODUCTION

1.1 Objectives of the PHA

The aim of this Preliminary Hazard Analysis (PHA) of the LOC-OB system is to identify hazards, to assess the severity of the potential accidents that could occur and to identify safeguards for reducing the risks associated with the hazards. This allows to define barrier/mitigation measures to reduce identified risks and to derive THR/TFFR apportionments.

For the LOC-OB system, this PHA:

- a) give the risk analysis objectives,
- b) define the risk analysis methodology,
- c) describe the system under analysis, its external functions and its mission profile,
- d) provide hazard and risk assessment,
- e) identify the safety requirements,
- f) allocate safety target to the functions,
- g) list the assumptions made during the analysis.

1.2 Scope of the document

This analysis is based on the output elements of the ERTMS Users Group LWG [R25], the CLUG project [R26] and the OCORA project. 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 (see [R29]).

The system context used to carry out this PHA is based on the existing ERTMS/ETCS for level 2 where the concepts of independent onboard vehicle localisation component, virtual balise and digital map are added. It can be adapted for Hybrid train detection of ERTMS/ETCS or automatic driving, when inputs for this level are available. Thus, in this first stage of LOC-OB deployment, the RAMS activities are performed within the context of the ERTMS/ETCS system [R13] and [R16], in particular, the safety analysis is based on the hazards of the ERTMS/ETCS system identified in [R17] and [R18]. This corresponds to the current state of art at the beginning of the CLUG 2.0 project. However, this basis is 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 4. More details can be found in WP2 deliverables [R27] and [R28]. For the PHA, the analysis is limited to the outputs, inputs and when possible extended to some operational contexts of the LOC-OB system.

1.3 Limits and Hypotheses

This section gives a list of limits and hypotheses related to the PHA during the CLUG2.0 project.

The PHA activity is limited to the LOC-OB system presented in section 4 and documents [R27] and [R28].

NTC systems are not covered, only ETCS level 2 with or without hybrid train detection and ATO are considered.

The new sensors technologies and input information considered in this PHA analysis for the LOC-OB system are:

- GNSS
- IMU
- Digital Map

These new technologies are going to be covered in a dedicated analysis.

The LOC-OB system also uses other input information, for example tachometer or balise reader (BTM), which are already analysed in Subset 088 [R17] and Subset 091 [R18].

The analysis in this document is based on the information available in WP2 deliverables [R27] and [R28] and in the current state of the art on the user needs of the LOC-OB system outputs. In some cases information are not sufficient, thus an open point is defined. These open points will be reevaluated in the case of new information provided.

2 RISK ANALYSIS CONTEXT

2.1 Railway legislative context

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 present PHA. 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]
- Commission Implementing **Regulation (EU) 1136/2015** 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 harmonized 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 this safety analysis, the following safety 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. Considering that the present document is limited to a Preliminary Hazard Analysis (PHA) and to ease the reuse of CLUG2.0 results in the future, the EN 50126 terminology is used wherever applicable.

Within the framework of the CLUG2.0 project, the CLUG2.0 demonstrator is required to be compatible with the ETCS architecture. Accordingly, the following references are considered as applicable within the context of the CLUG2.0 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]

2.2 LOC-OB System use

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 architecture OCORA, in which is included the LOC-OB, is new and different of what is 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 the use of new kind of sensors to replace odometer systems.

LOC-OB is a subsystem of the OCORA architecture, and it contributes also to the overall performance of the system ERTMS/ETCS. Thus, in this first stage of LOC-OB deployment, the risk analysis is performed within the context of the ERTMS/ETCS system. Thus, the analysis is mainly based on the hazards of the ERTMS/ETCS system identified in Subset 091 [R18].

2.3 Risk Assessment Criteria

The risk assessment criteria are the same than for the CLUG project (see [R27]) and are recalled here:

Based on EN50126-1 standards [R1], the following levels of Hazard Rate are considered for the assessment of the accidents and feared events in CLUG 2.0. Hazard Rate means the tolerate rate of occurrence of a hazard per hour.

		<i>Hazard Rate</i>
1	Highly Improbable	$HR \leq 10^{-9}$
2	Improbable	$10^{-9} < HR \leq 10^{-7}$
3	Rare	$10^{-7} < HR \leq 10^{-5}$
4	Occasional	$10^{-5} < HR \leq 10^{-4}$
5	Probable	$10^{-4} < HR \leq 10^{-3}$
6	Frequent	$10^{-3} < HR$

Table 1: Frequency categories as per EN50126

According to EN50126-1 standards [R1], the following levels are considered for the impact assessment in CLUG2.0.

A	Insignificant	<ul style="list-style-type: none"> • Possible minor injury
B	Marginal	<ul style="list-style-type: none"> • No possibility of fatality, severe or minor injuries only, and/or • minor damage to the environment
C	Critical	<ul style="list-style-type: none"> • Affecting a very small number of people and resulting in at least one fatality, and/or • large damage to the environment
D	Catastrophic	<ul style="list-style-type: none"> • Affecting a large number of people and resulting in multiple fatalities, and/or • extreme damage to the environment

Table 2: Severity level as per EN50126

According to Table 2 in §10.2.7 of EN50126-2 [R1], the SIL Level is determined based on the tolerable functional failure rate (TFFR) as follows:

TFFR [h ⁻¹]	SIL allocation
$10^{-9} \leq \text{TFFR} < 10^{-8}$	4
$10^{-8} \leq \text{TFFR} < 10^{-7}$	3
$10^{-7} \leq \text{TFFR} < 10^{-6}$	2
$10^{-6} \leq \text{TFFR} < 10^{-5}$	1

Table 3: SIL Level as per EN50126

A certain level of acceptability is then defined depending on the system safety criticality. Based on the above-mentioned likelihood and impact assessment levels, the following risk acceptance matrix is used.

In this step, we apply the risk acceptance principle laid out in CSM-RA for explicit risk estimation.

			Frequency					
			1	2	3	4	5	6
			<i>Highly Improbable</i>	<i>Improbable</i>	<i>Rare</i>	<i>Occasional</i>	<i>Probable</i>	<i>Frequent</i>
Severity	A	<i>Insignificant</i>	Negligible	Negligible	Negligible	Tolerable	Tolerable	Undesirable
	B	<i>Marginal</i>	Negligible	Negligible	Tolerable	Undesirable	Undesirable	Intolerable
	C	<i>Critical</i>	Negligible	Tolerable	Undesirable	Undesirable	Intolerable	Intolerable
	D	<i>Catastrophic</i>	Tolerable	Undesirable	Undesirable	Intolerable	Intolerable	Intolerable

Table 4: Risk acceptance categories as per EN50126

2.4 Accidents

The following table gives the common railway accident occurring on a train, that shall be considered in the PHA analysis:

Accident	Explanation
Collision	Collision of a train with a) another train or b) infrastructure or c) obstacle on track or d) one or more persons on track
Derailment	A train derailing due to a) overspeed on area with speed restriction or b) spurious change of switch position or c) bad tracks (wide incorrect) or d) broken tracks
Fall	Fall of one or more passengers (from a train or inside a train or in train/platform gap)
Fire	Fire caused by undue or kept electrical connection of a train to the catenary (pantograph not lowered; circuit breaker not opened)
Asphyxia	Passenger affected by fire related smoke, when stopping in unsafe area
Electric hazards	Electrical chocs with passengers during operational phases or by staff during maintenance staff
Hurting of person	Passenger or staff are hurt for another cause than collision, fall, fire, asphyxia or electric hazards

Table 5: Railway Accident

Derailment due to a collision are counted as collision, as it is the first accident. In the same way, a collision due to a derailment are counted as derailment.

3 RISK ANALYSIS METHODOLOGY

3.1 Overall Description

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 1 (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 [R10]).

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

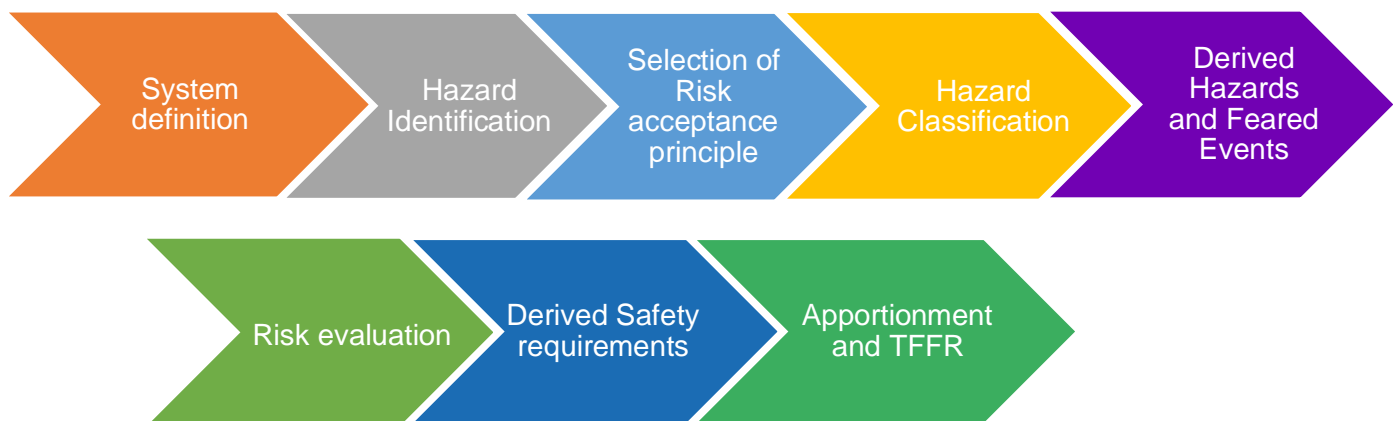


Figure 1: Risk analysis methodology

System definition is described in §4. The methodologies used during the other steps are defined in the sequel.

3.2 Hazard Identification

Hazard identification starts by analyzing the results for **Similar reference system**: thus LOC-OB hazards are carried by the ERTMS/ETCS and based on the hazards defined in Subset 091 [R18], that provides a list of hazards related to the localization function. A detailed analysis of the fault tree provided by the Subset 088 [R17] confirms this list.

However, the hazard provided by these subsets are only related to the main role of the ETCS **“To provide the driver with information to allow him to drive the train safely and to enforce respect of this information, to the extent advised to ETCS.”** Thus, the two hazards considered for this first list are:

- **“ETCS Core Hazard”:** *Exceedance of the safe speed or distance as advised to ETCS.*
- **“ETCS Auxiliary Hazard”:** *ETCS interacts erroneously with the driver so that safe train operation, not supervised by ETCS, is jeopardized.*

Further analysis will then be conducted to complete this first list of hazards, by considering hazards related to other user needs (e.g. ATO, Perception, Doors management, ...) or to functions not covered by the current version of [R16] and [R18], as for example functionalities related to level 3 and identified in the scope of the LOC-OB system (as defined in [R28]).

Then an analysis of the new technologies and new services related to the LOC-OB system is done to identify potential hazards, added to the first list.

Finally, to complete the previous analysis, a classical railway accident analysis is performed.

The list will then be reviewed by the partners during a formal workshop to finalize a list of hazards as input of the risk evaluation.

This process is described in the following figure:

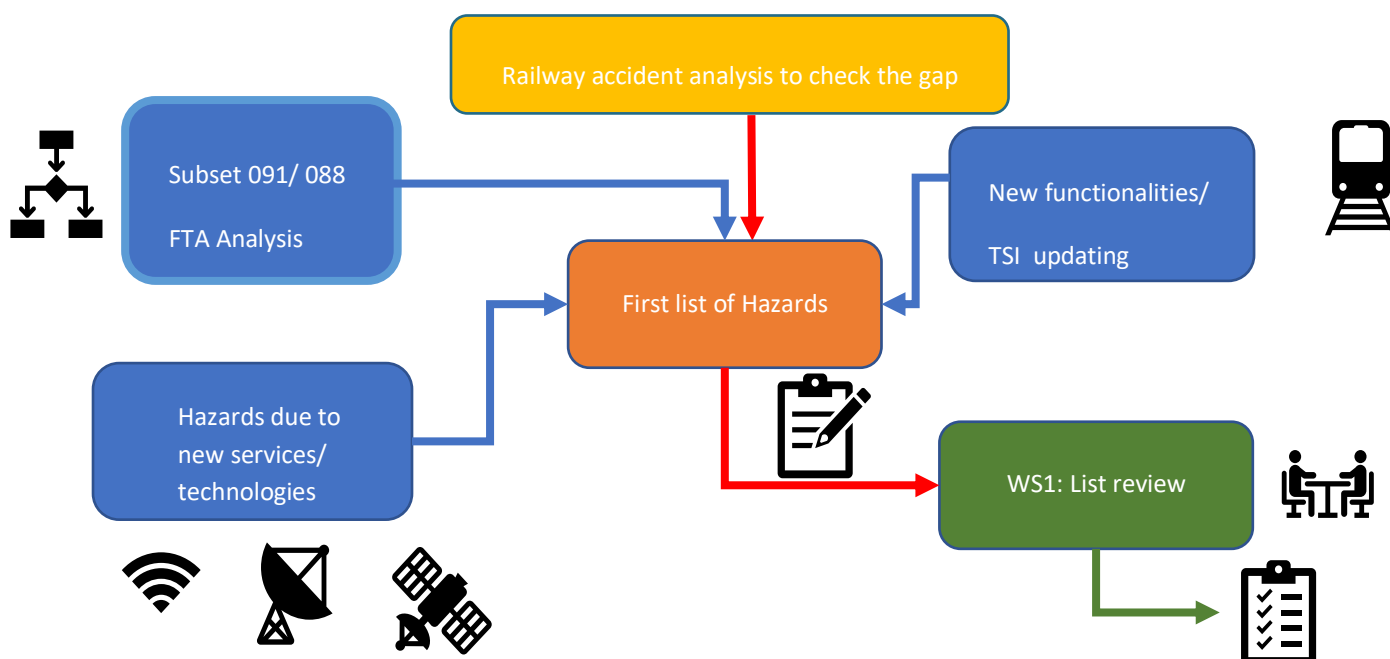


Figure 2: CLUG 2.0 Hazard Identification Process

3.3 Risk acceptance principle

The risk acceptability of the system under assessment shall be evaluated by using one or more of the following acceptance principles according to [R8]:

- 1) Code of practice: application of codes of practice.
- 2) Similar reference system: similarly, analysis with reference system.
- 3) Explicit risk estimation: identification of scenarios & associated safety measures, if safety criteria is quantitative risk estimation based on frequency and severity has to be carried out.

CSM guide [R10] for the application of the Common Safety Method recommends:

“When the hazards are not covered by one of the two risk acceptance principles code of practice or similar reference system, the demonstration of the risk acceptability shall be performed by explicit risk estimation and evaluation. Risks resulting from these hazards shall be estimated either quantitatively or qualitatively, taking existing safety measures into account.”

By applying the CSM guideline to the LOC-OB, a first selection of risk acceptance method for each part of the LOC-OB has been done. “*Similar reference system*” has been selected: this risk assessment criteria might be applied for initial focus if equivalent system could be identified. This risk assessment criteria is relevant to the LOC-OB as it contributes to the overall performances of the ERTMS/ETCS. In our context at system level, the reference system is ERTMS/ETCS. LOC-OB hazards are carried by the ERTMS/ETCS and based on the hazards defined in Subset 091 [R18]. This approach is completed by following “*Explicit risk estimation*” criteria for new functions not covered by the current version of TSI or to analyze hazards related to the use of new technologies.

3.4 Hazard Classification

The guideline for the application of the CSM design targets [R9], [R10] provides classification of hazards when they arise as a result of failures of functions of the technical system. The following harmonized design targets shall apply to those failures:

- 1) Class a: where a failure has a credible potential to lead directly to an accident typically affecting a large number of people and resulting in multiple fatalities, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable. Those the design target for the function involves in this failure is $10^{-9}/h$.
- 2) Class b: where a failure has a credible potential to lead directly to an accident typically affecting a very small number of people and resulting in at least one fatality, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be less improbable. Therefore, the design target for the function involves in this failure is $10^{-7}/h$.
- 3) Acceptable risk: when the risk is acceptable it is classified as broadly acceptable risks.

This classification is followed to allocate a TFFR to the output functions of the LOC-OB system (see table proposed in §3.6).

3.5 Derived Hazards and Feared Events

The derived hazards and fear events are a synthesis of the Hazard Identification step.

3.6 Risk Evaluation

The PHA provides for each LOC-OB function; the possible feared events leading to the LOC-OB hazard and the barriers (safety relevant function) to be put in place.

The hazard analysis table contains the following information:

Functions		Feared Events		Explanations	Hazards	Barriers (external/Mitigation)	Design Target TFFR
The CLUG2.0 system function ID	The CLUG2.0 system function description	Feared events ID	Feared Events description	Detailed description of the hazard	Hazard ID	Identified Barriers and Safety requirements	Resulting design target

Table 6: PHA Table Elements

3.7 Derived RAMS Requirements

The RAMS requirements of functions are derived from the results of the risks analysis.

3.8 Apportionment and TFFR

In railway, the apportionment of the THR to the subsystem is derived from an overall target of the railway system. Then an apportionment of the THR is done as TFFR on the functions as proposed in EN50129 [R3]. For example, for the ERTMS/ETCS system, the apportionment between the onboard functions, the transmission functions and the trackside functions are defined in subset 091 [R18] as described in the following figure:

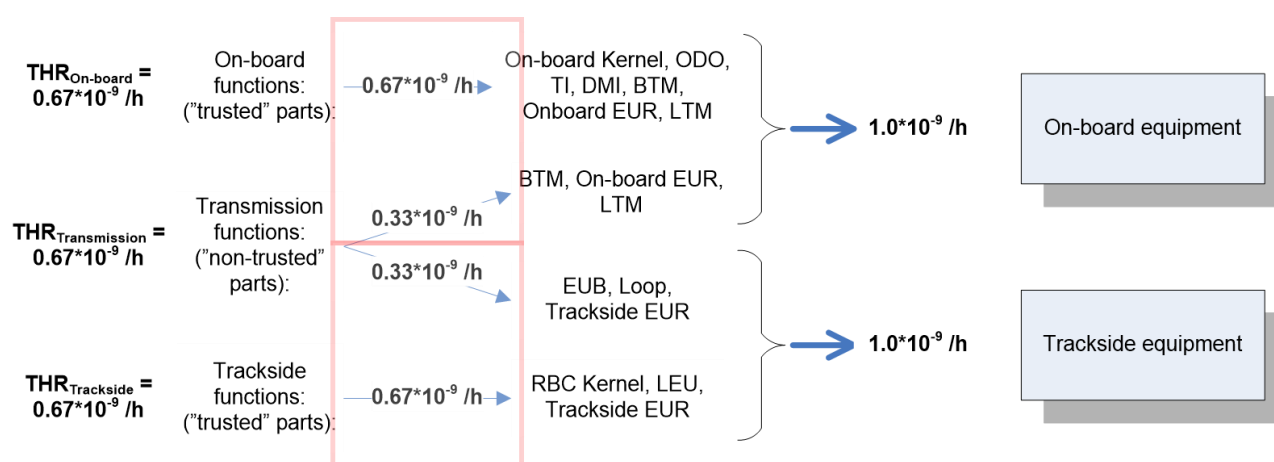


Figure 3: ERTMS/ETCS apportionment between the 3 subsystems

With the development of the vehicle locator and the main goal to reduce the number of trackside assets, the number of physical balises will be strongly reduced as much as feasible, new architecture or changes will be

introduced, therefore, this apportionment might be amended in the future, especially with risk analysis on the OCORA architecture.

However, at the current state of the OCORA architecture [R22], the apportionment of each feared events of the core ERTMS/ETCS on the OCORA subsystems is depending on the supplier design of the OCORA architecture. The apportionment of each hazard identified in [R18] is unknown with a THR defined only at the overall onboard level.

Such an apportionment approach cannot be applied during the CLUG 2.0 project as the on-board physical architecture is not defined (only functional architecture). Thus, the assessment is limited to apply the classification given in section 3.4 to the output functions of the LOC-OB system.

3.9 Discussion on other assessment approaches

In the railway domain, the risk analysis approach classically used is based on a long-term experience of the identification of safety requirements and the use of safety critical systems to prevent the accidents. Thus, common target criteria have been defined (see §3.3 and §3.4). It is expected for a new system to provide the same safety target, and no more, for its functions as those of the previous equivalent systems.

However, in other domains as automotive or aeronautic, a statistical approach, or a consensus between all stakeholders (e.g. in aviation: the Accident/Incident ratio is set to 10% in fault tree allocation for APV I, II and Cat-I operations), can be applied to adjust the THR allocated to the hazards depending on the operational context of the system. Such an approach can be relevant in the case of the introduction of a new subsystem which is going to use the output of the LOC-OB system (for example an ATO or a perception system which will use 3D information). Then a fine-tune THR on the user needs of these systems can be defined.

Such an approach requires a clear definition of the user needs and the environment of the LOC-OB, supported by either a theoretical analysis of set of external conditions necessary to lead to accidents or a large set of data to perform statistical analysis to reach the stakeholders consensus. These elements are not available in the context of CLUG 2.0.

However, this approach can be interesting as it may allow reducing the required safety level on the localization solution, but it would need to be consolidated and validated at European level by the rail certification bodies.

This is unrealistic to be realized in the time frame of CLUG 2.0 and without this rail sector approval, the CLUG 2.0 solution would face the risk not to be in line with the safety requirements requested in ERJU frame. In conclusion:

- This PHA (D3.2) proposes a qualitative approach, not a statistical approach as in aviation.
- As a matter of remaining in line with the current rail approach (qualitative) and rail safety targets followed by the other rail stakeholders, the CLUG LOC-OB should follow the safety requirements provided by D3.2.
- As the statistical approach present some important benefits to potentially reduce the price and complexity of the Safe localization solutions, notably CLUG 2.0 LOC-OB, a specific study is conducted in D3.7 proposing a way forward for such an approach (safety targets, validation approach, etc.). If conclusive, this approach could then be ported and debated by rail sector at EU level.

4 LOC-OB SYSTEM DEFINITION

The LOC-OB system definition considered in this PHA is succinctly described in the RAMS Plan [R29], and in more detailed in the specification documents [R27] and [R28].

The main characteristics of the LOC-OB system under analysis are:

- 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 location, 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.

Assumptions made on the LOC-OB system or its interfaces are synthetized in section 10.

5 HAZARD IDENTIFICATION

5.1 Fault Tree analysis

The analysis of Subsets 091 [R18] and 088 [R17] (Fault trees) to provide a first list of hazards by similarly analysis with reference system is given in APPENDIX A – DETAILED PHA, sheet “5a- Haz Id Subset 091”.

The most recent version of Subset 091 (v4.0.0 of TCS 2023) is covered. However, as the new version of Subset 088 is not yet available, some analyses are limited on some feared events (as KERNEL-35 and KERNEL-36).

Some LOC-OB hazards have been identified during this analysis, related to 1D data provided by the LOC-OB system (see § 6.1: **LOC-OB-HZ-02, LOC-OB-HZ-03, LOC-OB-HZ-04, LOC-OB-HZ-05, LOC-OB-HZ-06**). All these hazards on the LOC-OB are identified, as with the previous version of the ERTMS system, as a cause of a potential catastrophic accident (I.e.; collision or derailment).

5.2 New functionalities analysis

The analysis of new functionalities not defined in the current version of Subset 026 [R16] and Subset 091 [R18] but identified in the CLUG2.0 deliverable D2.1 [R27] is given in APPENDIX A – DETAILED PHA, sheet “5b- Haz Id New Functionalities”.

The LOC-OB hazards defined in the previous analysis have been reused here for the 1D data. More LOC-OB hazards have been identified for the 3D data analysis (see § 6.1: **LOC-OB-HZ-10, LOC-OB-HZ-11, LOC-OB-HZ-12, LOC-OB-HZ-13**). Besides, Assumptions and Open-Points (see §10) have been raised: the current state of information on the user needs for the consumers of the 3D data are not sufficient to comfort the safety analysis.

5.3 New technologies/new services

The analysis of new technologies and new services proposed for the LOC-OB system (as GNSS, IMU, digital Map) is given in the excel files in APPENDIX A – DETAILED PHA, sheet “5c- Haz Id New Technologies”.

LOC-OB hazards related to the new services or equipment's have been defined (see § 6.1: **LOC-OB-HZ-14, LOC-OB-HZ-15, LOC-OB-HZ-16, LOC-OB-HZ-17, LOC-OB-HZ-18**).

5.4 Accident analysis

The accident analysis, according to the accident list in § 2.4, is given in APPENDIX A – DETAILED PHA, sheet “5d- Haz Id from Accident”.

This analysis confirms the results of the 3 previous analyses: It gives operational scenarios involving the hazards of the LOC-OB system, identified during the three previous analyses, which can drive to an accident, without external barriers identified to prevent the accident.

6 DERIVED HAZARD AND FEAR EVENTS

6.1 Summary of Derived Hazard for LOC-OB

Following hazard identification at the ERTMS/ETCS system level, the following table presents the derived hazards, fear events at the level of the LOC-OB (extract from APPENDIX A – DETAILED PHA,).

CLUG 2.0 Event Id.	CLUG 2.0 Event Description	LOC-OB Feared Event Description	Accident Categories (see §2.4)
LOC-OB-HZ-01	Intentionally deleted		
LOC-OB-HZ-02	Speed provided by LOC-OB underestimates trains actual speed	Fail to provide upper bound speed higher than the actual train speed	Collision Derailment Fall Hurting of Person
LOC-OB-HZ-03	Incorrect movement speed direction related to the last reference point	Fail to provide the correct train movement direction Fail to provide the correct train orientation Fail to use the correct reference point information from digital map Fail to use the correct reference point id	Collision Derailment Fall Hurting of Person
LOC-OB-HZ-04	The confidence interval for distance measurement and calculation does not include the real position of the train	Fail to provide confidence interval which include the real train position (measured distance interval and position qualifier and reference point id) Fail to provide the correct train movement direction Fail to provide the correct train orientation Fail to use the correct reference point information from digital map Fail to use the correct reference point id Fail to provide upper bound speed higher than the actual train speed Fail to provide confidence interval which include the real train position (measured distance interval and position qualifier and reference point id)	Collision Derailment Fall Hurting of Person

CLUG 2.0 Event Id.	CLUG 2.0 Event Description	LOC-OB Feared Event Description	Accident Categories (see §2.4)
LOC-OB-HZ-05	Acceleration provided by LOC-OB overestimates trains actual acceleration	Fail to provide lower bound acceleration lower than the actual train acceleration	Collision Derailment Fall Hurting of Person
LOC-OB-HZ-06	The track edge id is not the correct one	Fail to provide the correct track edge id	Collision Derailment Fall Hurting of Person
LOC-OB-HZ-07	The computation of the confidence interval for distance measurement does not allow a safe reaction to odometry errors	Fail to provide confidence interval which include the real train position (measured distance interval and position qualifier and reference point id)	Collision Derailment Fall Hurting of Person
LOC-OB-HZ-08	The relocation of location does provide a wrong position of the train	Fail to provide confidence interval which include the real train position (measured distance interval and position qualifier and reference point id)	Collision Derailment Fall Hurting of Person
LOC-OB-HZ-09	Intentionally deleted		
LOC-OB-HZ-10	Incorrect vehicle attitude	Fail to provide 3D vehicle attitude which include the real train position	Collision Derailment
LOC-OB-HZ-11	Incorrect 3D estimated position	Fail to provide 3D position uncertainty which include the real train position	Collision Derailment
LOC-OB-HZ-12	Incorrect 3D estimated speed	Fail to provide 3D speed uncertainty which include the actual train speed	Collision Derailment
LOC-OB-HZ-13	Incorrect 3D estimated acceleration	Fail to provide 3D acceleration uncertainty which include the actual train acceleration	Collision Derailment

CLUG 2.0 Event Id.	CLUG 2.0 Event Description	LOC-OB Feared Event Description	Accident Categories (see §2.4)
LOC-OB-HZ-14	Electrical shocks with passengers during normal operation (travel, or on-station) or by staff during maintenance phases due to LOC-OB	Fail to protect against electrical choc	Electric Hazards
LOC-OB-HZ-15	Disturbance of signaling trackside of onboarded system to EMC emission/conduction from LOC-OB system leading to accident	Fail to protect against CEM disturbance	Collision Derailment Fall Fire
LOC-OB-HZ-16	Disturbance of LOC-OB due to EMC emission/conduction from other train systems or track side equipment	Fail to protect against CEM disturbance	Collision Derailment
LOC-OB-HZ-17	Mechanical interference of the LOC-OB with other physical equipments	Fail to ensure mechanical requirement	Hurting of Person
LOC-OB-HZ-18	Collision with Trackside/Infrastructure due to new train size (new equipment exceeding train size/envelop)	Fail to ensure mechanical requirement	Collision

Table 7: Derived hazard and fear events

6.2 Summary of Fear Events for LOC-OB

From the previous section 6, hazards are identified at the level of the LOC-OB. Some feared events are related to new user needs identified in D2.1 [R27]

LOC-OB Feared Event Id.	LOC-OB Feared Event Description	Origin
LOC-OB_FE_01	Fail to provide upper bound speed higher than the actual train speed	Related to current ERTMS functions as in TSI 2023 [R12]
LOC-OB_FE_02	Fail to provide the correct train movement direction	Related to current ERTMS functions as in TSI 2023 [R12]
LOC-OB_FE_03	Fail to provide the correct train orientation	Related to current ERTMS functions as in TSI 2023 [R12]
LOC-OB_FE_04	Fail to use the correct reference point information from digital map	Related to current ERTMS functions as in TSI 2023 [R12]
LOC-OB_FE_05	Fail to use the correct reference point id	Related to current ERTMS functions as in TSI 2023 [R12]
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)	Related to current ERTMS functions as in TSI 2023 [R12]
LOC-OB_FE_07	Fail to provide lower bound acceleration lower than the actual train acceleration	Related to new user needs introduced in D2.1 [R27]
LOC-OB_FE_08	Fail to provide 3D vehicle attitude which include the real train position	Related to new user needs introduced in D2.1 [R27] Note: The feared event shall be mitigated by the open point Loc-OB-OP-18 (see §10)
LOC-OB_FE_09	Fail to provide 3D position uncertainty which include the real train position	Related to new user needs introduced in D2.1 [R27] Note: The feared event shall be mitigated by the open point Loc-OB-OP-15 (see §10)
LOC-OB_FE_10	Fail to provide 3D speed uncertainty which include the actual train speed	Related to new user needs introduced in D2.1 [R27] Note: The feared event shall be mitigated by the open point Loc-OB-OP-16 (see §10)
LOC-OB_FE_11	Fail to provide 3D acceleration uncertainty which include the actual train acceleration	Related to new user needs introduced in D2.1 [R27] Note: The feared event shall be mitigated by the open point Loc-OB-OP-16 (see §10)

LOC-OB Feared Event Id.	LOC-OB Feared Event Description	Origin
LOC-OB_FE_12	Intentionally deleted	
LOC-OB_FE_13	Intentionally deleted	
LOC-OB_FE_14	Fail to protect against electrical choc	Related to the technologies
LOC-OB_FE_15	Fail to protect against CEM disturbance	Related to the technologies
LOC-OB_FE_16	Fail to ensure mechanical requirement	
LOC-OB_FE_17	Fail to provide the correct track edge id	Related to new user needs introduced in D2.1 [R27]

Table 8: Summary of feared events

7 RISK ASSESSMENT

The following table provides the results risk assessment for each LOC-OB function (see §4), identifying the possible feared events leading to the LOC-OB hazard (see §5) and the barriers (safety relevant function) to be put in place.

Only the safety relevant functions and safe data identified previously are detailed in this table.

Some barriers are defined on the inputs of the LOC-OB unit, when these inputs have been identified as used by the function. However, this identification cannot be exhaustive as the LOC-OB unit is view as a black-box.

Functions		Feared Events		Design Target TFFR	Comments
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	
		LOC-OB_FE_04	Fail to use the correct reference point information from digital map		
		LOC-OB_FE_05	Fail to use the correct reference point id		
		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)		
		LOC-OB_FE_17	Fail to provide the correct track edge id		
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	
		LOC-OB_FE_02	Fail to provide the correct train movement direction		
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	
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

Functions		Feared Events		Design Target TFFR	Comments
LOC-OB_SF-005	Provide Velocity Uncertainty 3D and	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
LOC-OB_SF-006	Provide Acceleration Uncertainty 3D and	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
LOC-OB_SF-007	Provide Attitude (Rotational Angles) Uncertainty 3D and	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
LOC-OB_SF-008	Provide Estimated Distance Travelled (since power on)	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-SF-008) has not been identified

Table 9: Risk Assessment of LOC-OB

8 RAMS REQUIREMENTS AND SAFETY RELATED APPLICATION CONDITIONS

The following RAMS Requirements are identified on the LOC-OB system:

Id	RAMS requirements	R/A/M/S	Receiver
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.	D2.1	See UR[020] in [R27]
RA-RAMS-02	LOC-OB shall not degrade safety toward odometry as defined in the ETCS BL3 R2.	D2.1	See UR[021] in [R27]
RA-RAMS-03	The true train position shall be always inside the confidence interval	D2.1	See UR[022] in [R27]
RA-RAMS-04	The true train speed shall be always inside the confidence interval.	D2.1	See UR[023] in [R27]
RA-RAMS-05	The true train acceleration shall be always inside the confidence interval.	D2.1	See UR[024] in [R27]
RA-RAMS-06	Each localisation information shall fulfil safety target requirements in accordance with the consumer's application requirements.	D2.1	See UR[025] in [R27]
RA-RAMS-07	Loc-OB shall respect some standards EN 50121 EN 50155	New	
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.	New	See UR[022] in [R27]

Table 10: RAMS

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

Id	SRAC	Receiver
Loc-OB-SRAC-01	The input from Cold Movement Detector (CMD) shall be safe (THR < 10-9/h)	CMD function provider
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
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
Loc-OB-SRAC-04	the LOC-OB uses a safe digital map as input (THR < 10-9/h, worst case assumed)	Digital map

Table 11: SRAC

9 APPORTIONMENT

The following table presents the synthesis of the safety requirements in terms of function classification and the design target with regard the TFFR.

RA Function ID	RA: Safety-related?	Design target TFFR
LOC-OB_SF-001	Yes	$< 10^{-9}/h$
LOC-OB_SF-002	Yes	$< 10^{-9}/h$
LOC-OB_SF-003	Yes	$< 10^{-9}/h$
LOC-OB_SF-004	see Loc-OB-OP-15	not evaluated
LOC-OB_SF-005	see Loc-OB-OP-16	not evaluated
LOC-OB_SF-006	see Loc-OB-OP-17	not evaluated
LOC-OB_SF-007	see Loc-OB-OP-18	not evaluated
LOC-OB_SF-008	see Loc-OB-OP-19	not evaluated

Table 12: Safety apportionment

10 ASSUMPTIONS AND OPEN POINTS

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

Id	Assumptions
LOC-OB-Ass-01	The Standstill function is not provided by the LOC-OB system
LOC-OB-Ass-02	1D position function gives the distance related to a reference point
LOC-OB-Ass-03	It is assumed that there is no be loop between Cold Movement Detector (CMD) system and LOC-OB system to avoid common mode
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)
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
LOC-OB-Ass-06	CTMS is designed with basic integrity
LOC-OB-Ass-07	MA computation by TPS (trackside) is based essentially on the localisation report provided to trackside by on-board
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.
LOC-OB-Ass-09	As soon an object is detected, without sufficient information, a safe reaction is launched by the Perception system
LOC-OB-Ass-10	ATO is a Basic Integrity system, with TPS is supervising in safety the ATO functions
LOC-OB-Ass-11	If ATO as not sufficient information, a safety speed profile and stopping point is computed
LOC-OB-Ass-12	TPS control function are SIL4 and based only on LOC-OB output for localisation
LOC-OB-Ass-13	If TPS does not receive localisation information during a given time, emergency break is commanded.
LOC-OB-Ass-14	Intentionally deleted
Loc-OB-Ass-15	Intentionally deleted
LOC-OB-Ass-16	Intentionally deleted
LOC-OB-Ass-17	Intentionally deleted
LOC-OB-Ass-18	Perception is a SIL2 system, with TPS controlling the Perception
LOC-OB-Ass-19	It is assumed that TPS detects reverse movement and computes backward distance from the 1D position provided by LOC-OB
LOC-OB-Ass-20	LOC-OB sends information in safety to TPS to release route and compute the MA
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).

Table 13: Assumptions

The following open points are remaining opened:

Open point #	Issue	Action
LOC-OB-OP-14	What happens at the beginning of a mission if localisation is not yet available?	Start of Mission will be analyzed within T3.5 with the inputs of D2.2 and D4.9
Loc-OB-OP-15	There are no sufficient inputs on the use of the 3D Position and Uncertainty to analyse the safety level of this output	To clarify in a future version if more information on ATO, incident management and perception systems
Loc-OB-OP-16	There are no sufficient inputs on the use of the 3D Velocity and Uncertainty to analyse the safety level of this output	To clarify in a future version if more information on ATO, incident management and perception systems
Loc-OB-OP-17	There are no sufficient inputs on the use of the 3D Acceleration and Uncertainty to analyse the safety level of this output	To clarify in a future version if more information on ATO, incident management and perception systems
Loc-OB-OP-18	There are no sufficient inputs on the use of the 3D Vehicle attitude to analyse the safety level of this output	To clarify in a future version if more information on incident management and perception systems
Loc-OB-OP-19	The users of the estimated distance (output of LOC-OB-SF-008) has not been identified	To clarify in a future version or in T3.7

Table 14: Open points

11 CONCLUSION

This document provides a preliminary safety analysis of the LOC-OB system, identifying hazards, assessing the severity of the potential accidents and identifying safeguards for reducing the risks associated with the hazards. 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.

It is based on the description of the LOC-OB system given in D2.1 [R27] and D2.3 [R28]. NTC systems are not covered, only ETCS level 2 with or without hybrid train detection and ATO are considered.

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 [R18] and Subset 088 [R17].
- 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.



12 APPENDIX A – DETAILED PHA

See Document “D3.2_detailed_PHA_v1-2.xlsx”



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