CLUG Demonstration of Readiness for Rail – CLUG 2.0

D3.6 CLUG LOC-OB PRELIMINARY SYSTEM RELIABILITY AND AVAILABILITY ANALYSIS

Due date of deliverable: 31/05/2024

Actual submission date: 12/11/2024

Leader of this Deliverable: Karin Nebe, SMO

Reviewed: Y

Document status		
Revision	Date	Description
0.1	12/01/2024	Draft version (plan)
0.2	15/01/2024	Draft version (general concept)
0.3	19/04/2024	Methodology version
0.4	29/05/2024	Submitted version for technical review
0.5	27/06/2024	Submitted version for subsequent technical review
0.6	29/07/2024	Submitted version for subsequent technical review
1.0	26/08/2024	Final version after quality check
2.0	12/11/2024	Final version officially submitted to EUSPA

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

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

REPORT AUTHORS

NAME	COMPANY	DETAILS OF CONTRIBUTION
Karin Nebe / Alejandro Lopez Hernandez	SMO	V0.1: Draft version (plan)
Alejandro Lopez Hernandez	SMO	V0.2: Draft Version (general concept) - Structure of the document
Alejandro Lopez Hernandez / Marc Sarrat / Marielle Petit-Doche	SMO SNCF	V0.3: Methodology version - Addition of the RAM analyse methodology. - Version for review based on V0.2
Alejandro Lopez Hernandez	SMO	V0.4: Submitted version for technical review based on V0.3
Alejandro Lopez Hernandez	SMO	V0.5: Submitted version for technical review based on V0.4
Alejandro Lopez Hernandez	SMO	V0.6: Submitted version for technical review

REPORT REVIEWERS

NAME	COMPANY	DETAILS OF CONTRIBUTION
Karin Nebe	SMO	V0.1, V0.2, V0.3, V0.4
Marc Sarrat	SNCF	V0.1, V0.2, V0.3, V0.4
Marielle Petit-Doche	SNCF	V0.1, V0.2, V0.3, V0.4
Claus Thies-von-der-Bey	DB	V0.3, V0.4
Thidarat Panthong	DB	V0.3, V0.4
Valentin Barreau	SNCF	V0.5 and V0.6
Mariya Kayalova	RINA-C	Quality check
Jose Bertolin	UNIFE	Final check and submission to reviewers and EUPSA

EXECUTIVE SUMMARY

This document is the deliverable "D3.6 PRELIMINARY SYSTEM RELIABILITY AND AVAILABILITY ANALYSIS" (hereinafter also referred to as "RAM analysis" in this document).

Delivery D3.6 focuses on the RAM Analysis of the system architecture and the operational context of the LOC-OB system (see chapter 3 in [R2]).

The purpose of this preliminary RAM Analysis is to provide the overall documentary evidence of the reliability, maintainability, and availability performance level of the system architecture of the LOC-OB.

It was important to determine hypotheses and assumptions. These hypotheses and assumptions provided a stable framework and operational conditions for carrying out the RAM analysis of the LOC-OB.

The RAM Analysis carried out on the LOC-OB constitute the core part of the documentary evidence to be considered to establish or to perform onward the LOC-OB regarding RAM.

In addition, this RAM analysis approach shows that the first approach of the architecture of the LOC-OB does not meet all relevant reliability, availability, and maintainability requirements.

This deliverable is to be used by all the project partners of LOC-OB to provide recommendations in terms of RAM.

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.

LIST OF ACRONYMS

ACRONYM	CONCEPTS
Ai	Intrinsic Availability
Ao	Operational Availability
CCS	Control, Command and Signalling
CLUG	Certifiable Localisation Unit with GNSS in the railway environment
CM	Corrective Maintenance
CMT	Corrective Maintenance Time
DR	Digital Register
FDE	Fault Detection and Exclusion
FIT	Failure in Time (1 FIT corresponds to a 1E-09 failures/hour)
FMEA	Failure Modes and Effects analysis
GNSS	Global Navigation Satellite Systems
IMU	Inertial Measurement Unit
LOC	Localisation
LRU	Line-Replaceable-Unit
MDT	Mean Down Time (mean standstill or failure time)
MRT	Mean Repair Time
MTBF	Mean Operating Time Between Failure
MTBPM	Mean Time Between Preventive Maintenance
MTTPM	Main Time to Preventive Maintenance
MTTR	Mean Time to Recovery /Restoration
RAM	Reliability, Availability, Maintainability

TERMS AND ABBREVIATIONS

The definitions of terms about RAM in this document are oriented toward [R1]. However, as the terms in these standards are to be used unambiguously, the key terms and variables are summarized in the table below.

Term	Explanation
Failure mode	The failure mode is the symptom by which a failure manifest itself. Complex units under consideration normally have various functions that can fail in different ways. In the case of on-board equipment, for example, there is a difference as to whether the emergency brake is activated due to a failure or whether the diagnostics interface is no longer available due to a failure. Consequences and causes as well as frequencies of the failures can differ. For this reason, every reliability analysis of a system includes a definition of failure modes that have been considered. To what extent this definition should be complete depends on the individual case.
Failure rate	The failure rate for a given unit under consideration is equal to the probability of failure, relative to ∂t, in the interval $(t, t + \partial t]$, subject to the condition that it has not failed by the time t. The failure rate is simplified in many places as follows: The frequency per time unit at which the failure occurs is designated as the failure rate. The symbol for the failure rate is the Greek letter lambda (λ). The failure rate is often specified as the unit FIT (failure in time): $1\,FIT = 10^{-9}\,\frac{Failures}{Hour}$ For electronic components there is a justifiable and frequently applied assumption that the reliability function is an exponential function. In this case, the failure rate is constant.
Maintainability	It is probability that, given the specified materials and subject to personnel conditions, the time spent on maintenance or for a repair is less than a pre-defined period.
Corrective maintenance	Maintenance is performed after detection of a failure in order to restore a product to a condition in which it can fulfill a required function.
Mean Down Time	The mean down time (MDT) is the average time that a system is non-operational. This includes all downtime associated with repair, corrective and preventive maintenance, self-imposed downtime, and any logistics or administrative delays.

Term	Explanation
Mean Operating Time Between Failures	The mean operating time between failures (MTBF) defines the mean value of the failure-free operating time of a unit under consideration. The MTBF is also referred to as the mean lifetime. The term MTBF is applied to repairable units. For units with constant failure rates, the MTBF is the reciprocal value of the failure rate: MTBF = 1/lambda The general definition of the mean lifetime (even for non-constant failure rates) is: $\mathrm{MTBF} = \int_0^\infty R(t)\,dt$
Mean Time to Restoration/Repair	The mean time to restoration/repair (MTTR) designates the mean time required for restore (for corrective maintenance), see [R6].
Unavailability	It is probability that the unit under consideration does not perform the required function under specified operating conditions at a specified time. The unavailability is normally specified as a ratio of MDT to MTBF+MDT. The parameter for unavailability is U. In accordance with the definition, the following relationship applies: U + A = 1.
Preventive maintenance	The maintenance at specified intervals or according to specified criteria that is provided in order to reduce the probability of failure or the deterioration of the function of a unit.
System failure	System Failure: System mode which is assumed on detection of safety-related failures that do not result in a computer stop and for which no other reaction is provided.
Subsystem	Board(s) and associated driver software.
Availability	The ability of a product to be in a condition in which it can meet the required function under specified conditions or within a specified period, subject to the condition that the required external resources are available. The availability is normally specified as a ratio of MTBF to MTBF+MDT or MTBF to MTB +MTTR. The parameter for availability is A. $$Ao = \frac{MTBF}{MTBF + MDT}$$ In this case the operational availability Ao is referred to. $$Ai = \frac{MTBF}{MTBF + MTTR}$$ In this case the intrinsic availability Ai is referred to.

Term	Explanation
Reliability	Ability to perform as required, without failure, for a given time interval, under given conditions. Reliability is described by the reliability function R(t). The reliability function delivers the probability that the unit is still functioning at time t. R is the abbreviation for reliability.

To illustrate the corresponding terms, the relationships between MTBF and MDT are represented graphically in Figure 1.

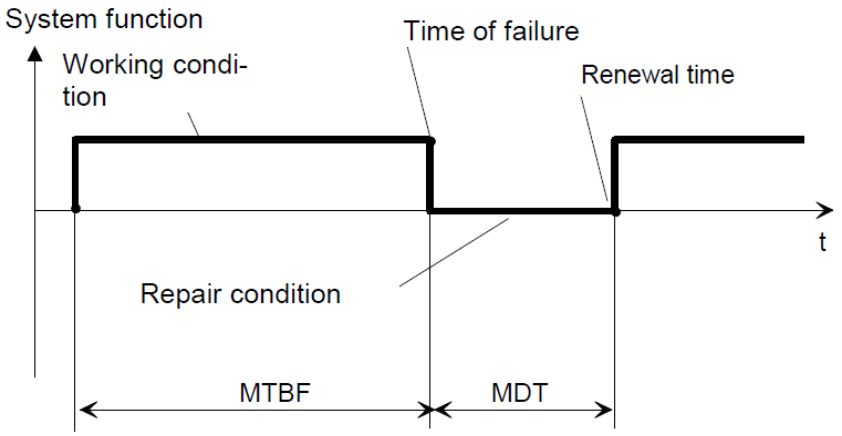

Figure 1: Representation of the system function over time with respect to MTBF and MDT

According to the chapter B.4 in [R1] the MDT will be considered the same to the MTTR under certain conditions, for instance constant failure rate, constant repair rate and no preventative maintenance.

In Figure 2 (see too chapter B.4 in [R6]), the time components of the MTTR are represented in graphical form:

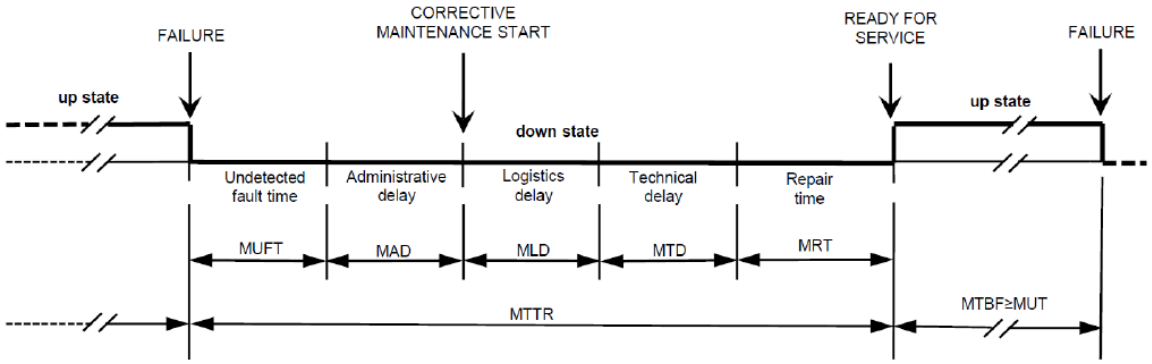

Figure 2: More detailed representation of the system function over time with respect to MTBF and MTTR

Note: The following time components of the MTTR are within the sphere of responsibility of the railway operators and they will be considered only informative in this document:

- Undetected fault time MUFT (time interval between failure and detection of the resulting fault);
- Administrative delay MAD (delay to maintenance action incurred for administrative reasons);
- Logistic delay MLD (delay, excluding administrative delay, incurred for the provision of resources needed for a maintenance action to proceed or continue;
- Technical delay MTD (delay incurred in performing auxiliary technical actions associated with, but not part of, the maintenance action).

The following time component will be considered in this document:

- Repair time MRT (part of active corrective maintenance time taken to complete repair action).

At the same time the MRT owns the following sub-time components

- Fault localization time (see 192-07-18 in [R6])
- Fault correction time (see 192-07-14 in [R6])
- Function checkout time (see 192-07-16 in [R6])

In Figure 3, time components of the MRT are represented in graphical form:

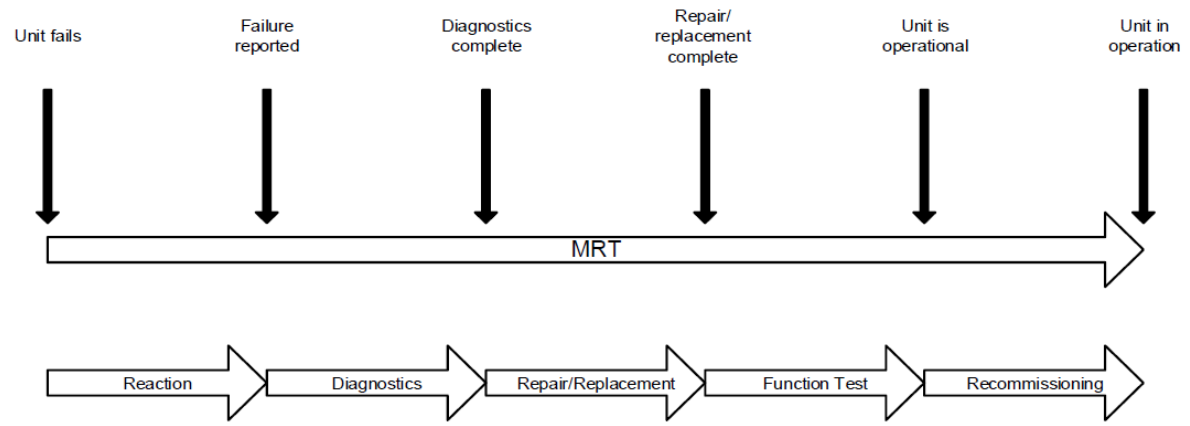

Figure 3: Time components of the MRT

Observation: In the past the definition of MTTR covered the fault localization time, the fault correction time and the function checkout time. The actualized definition of the MTTR is extended and it covers more sub times that are not relevant for this document. The new expression MRT covers the same sub-times as the old MTTR definition. Because of this the MTTR definition in this document will be used further in the document without the consideration of the undetected fault time, administrative delay, logistic delay and technical delay.

CONTENTS

Table of figures

List of tables

1 INTRODUCTION

1.1 Purpose

CLUG 2.0 deliverable D3.6 – CLUG LOC-OB Preliminary System Reliability, Availability and Maintainability analysis aims at describing the RAM objectives and activities of CLUG 2.0 for the LOC-OB system.

The RAM activities are in scope of WP3 (see Figure 4).

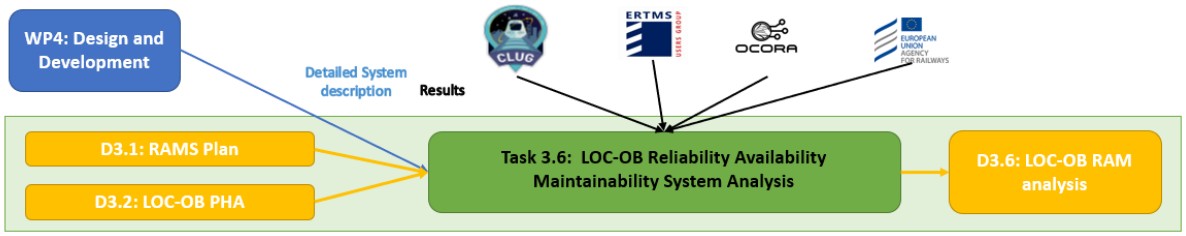

Figure 4: RAM activities regarding WP3

This document is based on the European standard EN50126 and EN50129 (see [R1] and [R9]).

This RAM analysis was planned in [R4] and covers only the components of the consolidated functional architecture of LOC belonging to the LOC-OB system (see [R2]).

1.2 Objectives of the Preliminary System Reliability, Availability and Maintainability Analysis

The main objective of this document is to provide a realistic estimation of the components of the consolidated functional architecture of LOC-OB system in regards of system reliability, availability, and maintainability performance in the CLUG 2.0 project.

In order to provide this realistic estimation, the following analyses, determinations and estimations will be carried out:

- FMEA regarding the specified failure categories.
  - The focus is the effect of single failures of the components of the LOC-OB on the function of the LOC-OB system according to the defined failure categories.
- Reliability Block Diagrams regarding the specified failure categories.
  - The focus is the graphic description of effect of multiple failures of the components of the LOC-OB on the function of the LOC-OB system according to the defined failure categories.
- FTA to quantify the failure rate and MTBF of the system reliability regarding the specified failure categories on basis of the results of the FMEA.

- The reliability block diagrams will help to confirm the correctness of elaboration of the fault trees.

- Determination of the MTTR and MTTPM of the components of the LOC-OB for corrective and preventive maintenance of the LOC-OB as well as the estimation of the MTTR and MTTPM of the LOC-OB system.
- Estimation of the intrinsic availability of the LOC-OB.

This document contains a traceable estimation of the reliability of the LOC-OB system.

Software reliability is not part of the analysis because the origin of software failures has a systematic nature.

The RAM analysis covers only random failures of the components.

1.3 Methodology for the RAM Analysis

In order to perform this RAM analysis, the following methodology is followed:

- Some hypotheses regarding the possible hardware components of the LOC-OB will be created.
  - HW components that correspond to the LOC-OB will be identified.
- The necessary RAM parameters for realizing the RAM analysis regarding the RAM requirements will be determined.
  - MTBF and failure rate of the assumed HW components;
  - MTBF and failure rate of the LOC-OB regarding failure categories;
  - MTTR of the assumed HW components;
  - MTTR of the LOC-OB.
- The scope of the analysis and its boundaries will be explained.
  - Architecture of the LOC-OB will be presented.
- Failure mode effect analysis of the assumed HW components will be executed to determine the effect of single failure according to the defined failure categories.
- Reliability block diagrams of the LOC-OB regarding the defined failure categories will be elaborated with the goal to show in a graphic form the way to the failure of the LOC-OB because of single or multiple failures of the assumed HW components.
- With help of an FTA tool failure trees will be elaborated for the LOC-OB to determine the effect of multiple failures of the assumed HW components regarding the defined failure categories.
- The RAM parameters values of the assumed hardware components of the LOC-OB will be determined or collected and listed.
  - To determine the RAM parameters of the assumed hardware components of the LOC-OB, it will be checked that they were estimated using the methods "Part Count and Part Stress Analysis Prediction".

- Part Count and Part Stress Analysis Prediction are procedures for the calculation of failure rate of parts of modules or assemblies by adding the failure rate of each part of the module in consideration of their environmental and operation conditions.

- The elaborated failure trees will be quantified with the use of the determined failure rates of the assumed hardware components of the LOC-OB.
  - The results of the quantification are the RAM parameters failure rate and MTBF of the LOC-OB regarding the defined failure categories.
- The total MTBF and mean MTTR of the LOC-OB are determined based on the failure rates and MTTR of the individual hardware components of the LOC-OB.
  - The results of the quantification are the RAM parameters failure rate and MTBF and MTTR of the LOC-OB regarding the corrective maintenance.
- The total MTTPM of the LOC-OB are determined based on the MTTPM of the individual hardware components of the LOC-OB.
  - The results of the quantification are the RAM parameter MTTPM of the LOC-OB regarding the preventive maintenance.
- The "intrinsic availability Ai" for the LOC-OB will be estimated by using of the MTBF values of the LOC-OB regarding the defined failure categories and the mean MTTR of the LOC-OB.
- The results of the RAM Analysis will be compared to the expected RAM targets defined in the RAM requirements and conclusions about the results will be summarized.

The following Figure 5 shows the methodology for the RAM analysis in a short form:

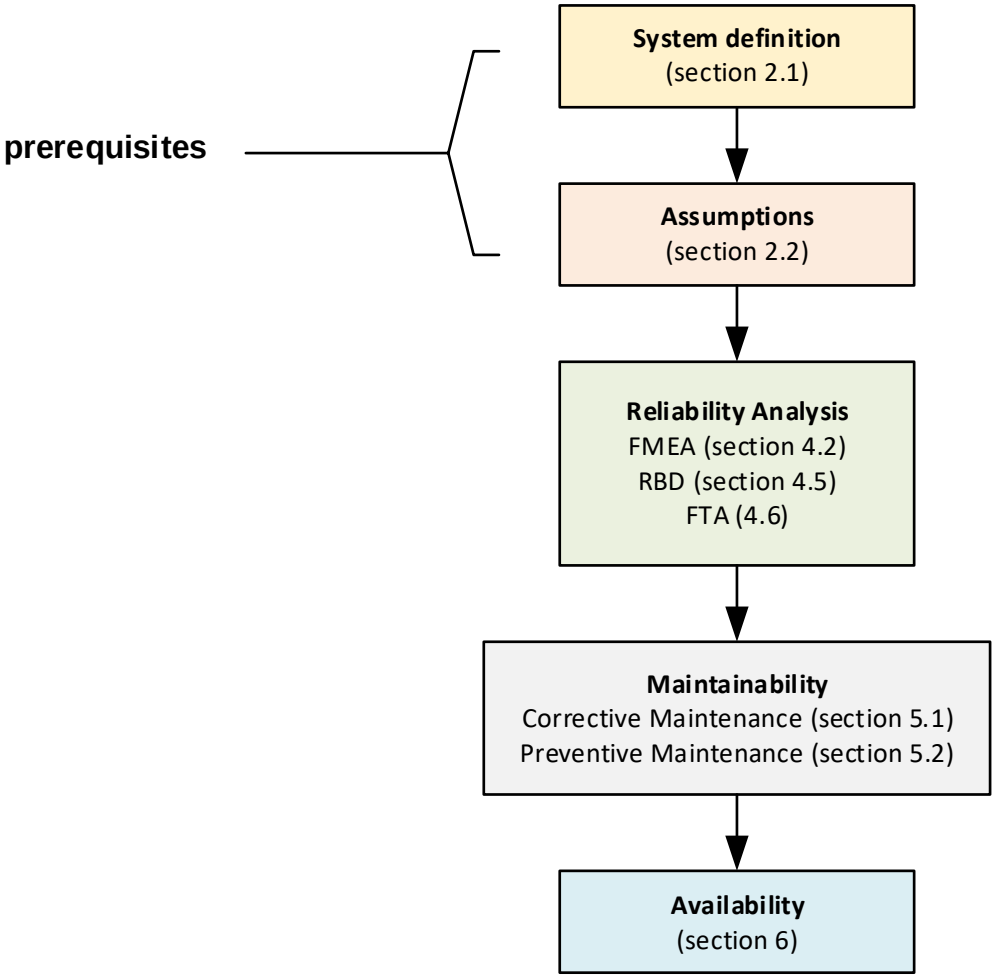

Figure 5: Methodology for the RAM analysis

2 LOC-OB SYSTEM DEFINITION

The complete structure of LOC-OB system is presented in the Figure 6, including all interfaces and external systems.

The clustered functionalities, such as on-board Measurement, Integrity, Navigation, Map Data Processing, Safe and Non-Safe Information, and all system functions SF-xxx, are provided as a guide and visual aid to enhance comprehension.

It is important to note that these functionalities are not compulsory for the design or implementation of LOC-OB as a system (see section 5.2.5.1 in [R2]).

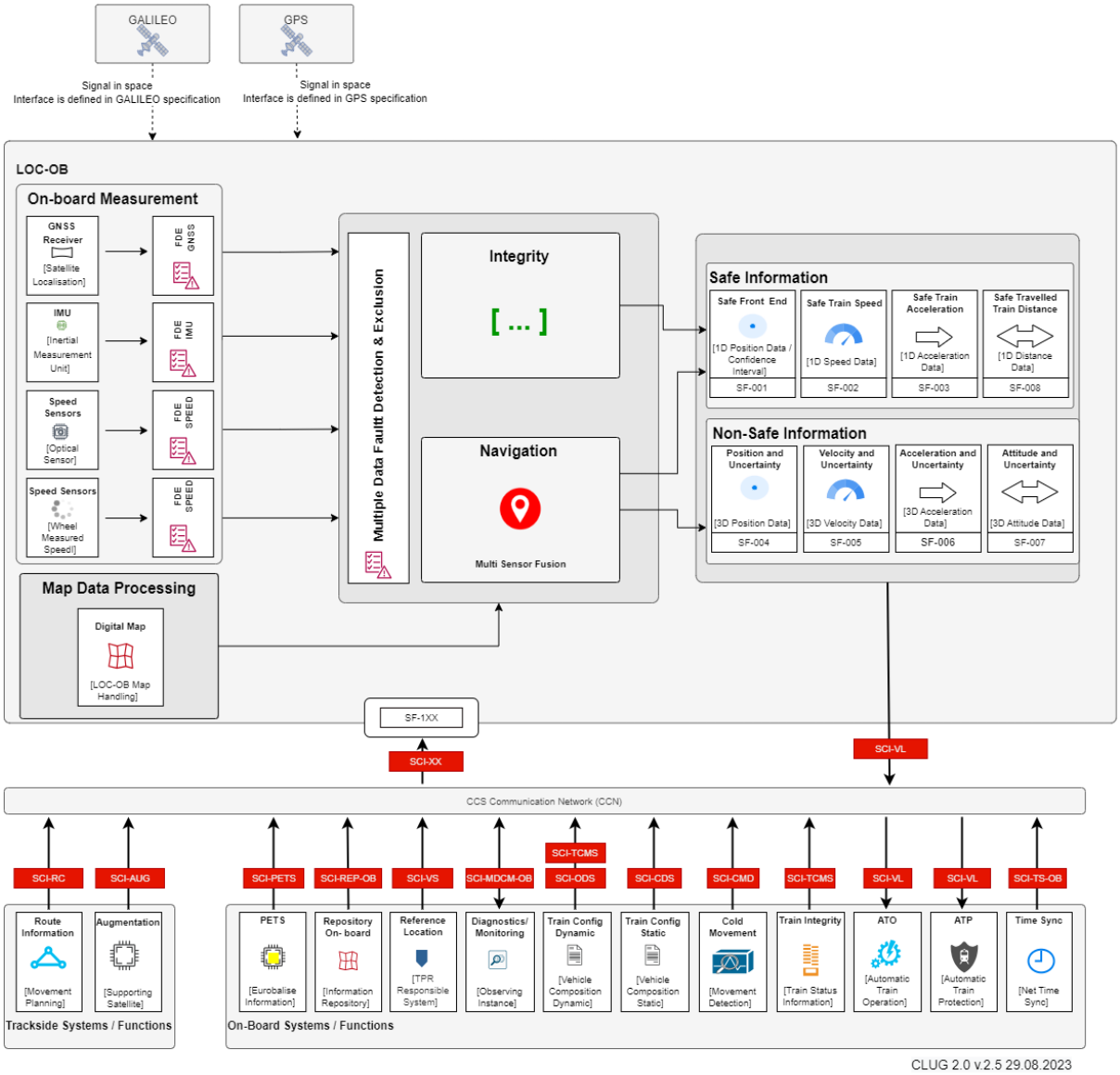

Figure 6: Main External System Constituents (see section 5.2.5 in [R2])

This RAM Analysis considers RAM characteristics of components within the system boundaries of LOC-OB system as well as the Map Data (located in block “Repository On-board”).

2.1 Components of the LOC-OB

The components of the LOC-OB system that are considered in the RAM Analysis belong to the functionality “On-Board Measurement”, “Navigation engine” and “Integrity engine” and “Map Data Processing” (see block LOC-OB and block Repository On-board in Figure 6).

The on-board measurement functionality is responsible for the sensor operation, data acquisition and processing of information on the train movement as input to the sensor fusion algorithm.

No detailed description of the LOC-OB system is given here, as this has been done in [R2].

Figure 6 shows the LOC-OB system and its physical environment.

Five external interfaces were determined:

1) GPS (satellite navigation)
2) GAL (satellite navigation)
3) EGNOS (Europe ‘s regional satellite-based augmentation system)
4) Trackside Digital Map Management
5) User Applications (user interface to the LOC-OB system)

Five internal interfaces were determined:

1) FDE GNSS (satellite localization)
2) FDE IMU (inertial measurement unit)
3) FDE Speed (wheel measured speed)
4) FDE Speed (optical sensor, radar sensor)
5) Digital Map (LOC-OB map handling)

The LOC-OB system consists of various components. The following components will be considered for the RAM analysis:

1) GNNS Receiver with GNSS Antenna
2) IMU
3) Odometer (pulse generator)
4) Repository On-Board (digital map)
5) Navigation Engine
6) Integrity Engine

The components 1) until 3) of the LOC-OB system are briefly described in Table 1.

Component	Description
GNSS Receiver	A satellite navigation receiver is a user equipment that uses one or more of several global navigation satellite systems (GNSS) to calculate the device's geographical position and provide navigational advice.
GNSS Antenna	GNSS Antenna to receive GNSS signals.
IMU	An inertial measurement unit (IMU) is an electronic device that measures and reports a body's specific force, angular rate, and sometimes the orientation of the body, using a combination of accelerometers, gyroscopes, and sometimes magnetometers.
Odometer	An odometer or odograph is an instrument used for measuring the distance travelled by a vehicle. The device may be electronic, mechanical, or a combination of the two (electromechanical). Odometer units could be pulse generators.

Table 1: Brief description of the components of the LOC-OB system

2.2 Hypotheses about a possible architecture for the LOC-OB

There are not defined HW components for the LOC-OB at this moment. Because of this it is necessary to determine some hypotheses for a possible architecture (see Figure 7). With help of these hypotheses the RAM Analysis will be executed.

- Hypothesis 1: For the components GNSS Receiver with GNSS Antenna, the following HW components will be assumed.
  - "HW-GNSS-Receiver" and "HW-GNSS-Antenna".
- Hypothesis 2: For the component IMU, a HW component IMU will be assumed.
  - HW-IMU
- Hypothesis 3: For the component Odometer (pulse generator), a HW component pulse generator will be assumed.
  - HW-Pulse-Generator
- Hypothesis 4: For the component Map Data Processing (digital map), a HW component Digital-Map will be assumed:
  - HW-Digital-Map
- Hypothesis 5: For the component Navigation Engine, a HW component Navigation Engine will be assumed:
  - HW-Navigation-Engine

- Hypothesis 6: For the component Integrity Engine, a HW component Integrity Engine will be assumed:
    - HW-Integrity-Engine
- Hypothesis 7: For the component Multiple Data Fault Detection & Exclusion (FDE), a HW component FDE will be assumed:
    - HW-FDE

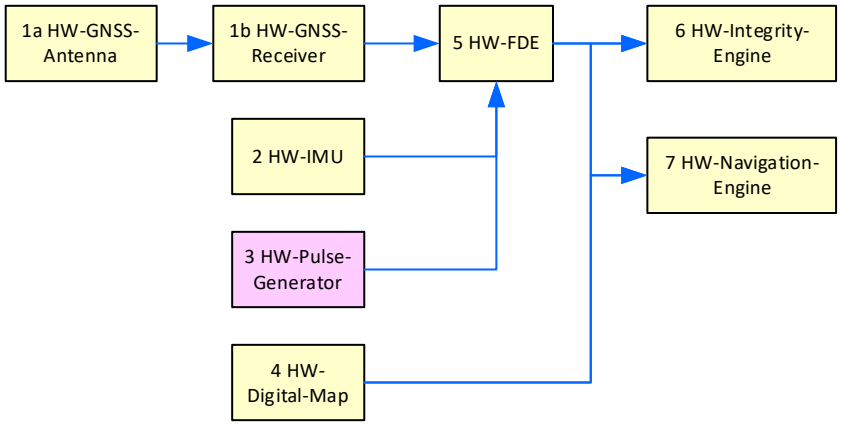

Figure 7: Assumed HW-Components of the LOC-OB

The following assumptions have been set to perform the RAM Analysis:

- Assumption 1: The failure rates that are used in the RAM Analysis are adopted of similar existent HW components.
- Assumption 2: It will be assumed that the LOC-OB will be broken up into the level LRU (smallest Line Replaceable Unit).
- Assumption 3: Each considered HW component corresponds to an LRU.
- Assumption 4: The FMEA, reliability block diagram and FTA will be executed considering the breakdown structure until the level LRU of the LOC-OB architecture.
- Assumption 5: The estimation of the MTTR and MTTPM will be executed considering the breakdown structure until the level LRU of the LOC-OB architecture.
- Assumption 6: A 100% operation time during the operation of the LOC-OB will be assumed (24 hours per day, 365 days per year).
    - The operation time of railway systems depends on the kind of service. It is possible that the LOC-OB system operates all the time or during a partial time. Because of this for the LOC-OB was assumed conservative a 100% operation time
- Assumption 7: Only random failures will be considered in the RAM Analysis.
- Assumption 8: The FMEA will consider failure causes as HW failures.
    - These can be short circuits, parasitic currents, insulation faults, high ohmic circuits, degradation of the integrated circuits etc.

- Assumption 9: It is assumed that the single failure of the components GNSS receiver, IMU, pulse generator, radar sensor and Digital Map conduce to a reduction of performance of the LOC-OB system.

3 LOC-OB SYSTEM RAM REQUIREMENTS

For the RAM analysis in this document, the requirements *SpecSysReq* with respect to reliability, availability and maintainability which are specified in chapter 12 of [R3] are considered. Functional requirements are not considered.

The processing of the RAM requirements was described in section 9, Phase 4 of [R4].

The results of this analysis show whether these RAM requirements can be fulfilled. The results of this analysis also could serve as a basis for architecture decisions. In section 7 will be showed if the RAM requirements could be covered for future architecture decisions on basis of the results of the RAM Analysis for LOC-OB prototype.

The RAM requirements for LOC-OB are listed in the corresponding tables of sections 3.1, 3.2, and 3.3.

3.1 Reliability

Requirement	Description	Acceptance Method
SpecSysReq[047]	The LOC-OB hardware shall comply with the overall CCS-OB reliability as defined in Ref [57] Chapter 2. Minor failure: λ <1,25 10-4/h. Reduced service failure: λ < 3,3 10-6/h. Immobility failure: λ < 3,7 10-7/h.	Analysis
Additional Information	The mission profile for these values is defined in document Ref [57] Chapter 2. These values are defined at the overall CCS-OB system level and should be derived in accordance with a future. To be overall noticed: - 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. - A failure of the LOC-OB hardware could lead to a reduced service with the consequence of a reduced performance. - A failure of the LOC-OB hardware could lead to immobility, for instance in case of a transition into the System Failure (SF) mode.	

Table 2: Requirement SpecSysReq[047]

The reference "[57]: EEIG 92S126 - ERTMS/ETCS RAMS Requirements Specification Chapter" is listed in [R3].

The failure categories of requirement SpecSysReq[047] for the LOC-OB are explained as follows:

- Minor failure: This kind of 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: This kind of failure of the LOC-OB hardware could lead to a reduced service with the consequence of a reduced performance.
- Immobility failure: This kind of failure of the LOC-OB hardware could lead to immobility, for instance in case of a transition into the System Failure (SF) mode.

3.2 Availability

Requirement	Description	Acceptance Method
SpecSysReq[048]	If the confidence intervals are larger than the acceptable position confidence interval (position), maximum acceptable speed confidence interval (speed) or maximum acceptable acceleration confidence interval (acceleration) for a cumulative 60 seconds (or more) for two hours, the time is accounted in the overall LOC-OB unavailability. If the LOC-OB is not providing data at the defined rate, the LOC-OB is considered as unavailable during this time.	Analysis
Additional Information	Since exceeding the confidence interval accuracy targets may not lead to any incidence on the railway operations, this requirement is to be considered as a tolerance toward the performance requirements.	

Table 3: Requirement SpecSysReq[048]

Requirement	Description	Acceptance Method
SpecSysReq[072]	If the LOC-OB is not providing data at the defined rate, the LOC-OB is considered as unavailable during this time.	Analysis
Additional Information	If the users are not receiving the data within the defied time out, user my enter in safe procedures.	

Table 4: Requirement SpecSysReq[072]

Requirement	Description	Acceptance Method
SpecSysReq[049]	The LOC-OB shall have an overall availability of 99,998% during operation.	Analysis
Additional Information	Refer to the availability target analysis from document 22E126 (cf. Ref [17]). Note that req 048 affects the overall availability defined in this requirement.	

Table 5: Requirement SpecSysReq[049]

The reference "[17]: EUG-22E126 – LOC-OB System Definition and Operation Context" is listed in [R3].

3.3 Maintainability

Requirement	Description	Acceptance Method
SpecSysReq[050]	LOC-OB shall manage useful data toward maintenance in an internal log memory and through the SCI - Monitoring, Diagnostic, Configuration, Maintenance On-Board (SCI-MDCM-OB) interface.	Analysis
Additional Information	LOC-OB is expected to be notified of system-wide update activity. This function provides means for system health measurement and fault recovery. The information provided by this function can be used by other functional blocks in CCS-OB to determine the state of the LOC-OB. With this insight, it is possible to establish proactive monitoring for system functionality.	

Table 6: Requirement SpecSysReq[050]

Requirement	Description	Acceptance Method
SpecSysReq[067]	LOC-OB shall log overall availability issues and specific relevant events as timestamped events.	Analysis
Additional Information	Availability issues are linked to the non-respect of: -SpecSysReq[003] -SpecSysReq[004] -SpecSysReq[009] -SpecSysReq[013] To achieve requirement: -SpecSysReq[050] Specific relevant events are to be determined and includes unusual activities of every sensor class.	

Table 7: Requirement SpecSysReq[067]

Requirement	Description	Acceptance Method
SpecSysReq[051]	LOC-OB shall be designed as a generic application (cf. EN50126, Ref [5] and Ref [6]).	Analysis
Additional Information	As a generic application, LOC-OB will ease its integration in the future CCS-OB and will ease technologic updates.	

Table 8: Requirement SpecSysReq[051]

The references "[5]: DIN EN 50126-1:2017 (E) – Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Generic RAMS Process" and "[6]: DIN EN 50126-2:2017 (E) – Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Generic RAMS Process" are listed in [R3].

Requirement	Description	Acceptance Method
SpecSysReq[052]	LOC-OB shall be designed to ease software updates (including security patches) by avoiding complex workshop procedures requiring bench testing.	Analysis
Additional Information	The ability of updating the LOC-OB software is essential. To minimize maintenance cost, the default update deployment mechanism shall be remotely (e.g., over-the-air) with no physical presence of any maintenance personnel on site (e.g., on the train).	

Table 9: Requirement SpecSysReq[052]

Requirement	Description	Acceptance Method
SpecSysReq[054]	The LOC-OB's design and maintenance concept shall meet a Mean Time to Restore (MTTR) ≤ 1h.	Analysis
Additional Information	The MTTR is defined in EN50126 (cf. Ref [R1]). The time elapsed to restore starts when the failure occurs and ends when the LOC-OB is ready for service. The administrative delay, Logistic Delay shall not be counted into the MTTR.	

Table 10: Requirement SpecSysReq[054]

Requirement	Description	Acceptance Method
SpecSysReq[055]	Preventive maintenance or periodic sensor calibration period of the overall LOC-OB shall exceed 2 years.	Analysis
Additional Information	If possible, preventive maintenance or periodic sensor calibration period shall be avoided if immobilisation of the train and staff intervention is needed. Also, if several sensors are used, the preventive maintenance plan shall factorise their preventive maintenance or calibration.	

Table 11: Requirement SpecSysReq[055]

4 RELIABILITY ANALYSIS OF THE LOC-OB SYSTEM EQUIPMENT

The reliability analysis refers to the architecture components of the LOC-OB system presented in Section 2.

In the following analysis, a Failure Mode Effect Analysis (FMEA) is performed in Section 4.2 to investigate the impact of single failures of the architecture components of the LOC-OB system (see FMEA methodology in [R5]).

This FMEA considers failures of the components and printed circuit boards (PCB) of the hardware of the LOC-OB system, respectively.

In Section 4.3, the failure rates of the components are determined, that are then included in the calculation of the system reliability carried out in Section 4.5.

4.1 Analysis of the impact of single failures (FMEA)

The primary goal of this FMEA is to assign the component failures that occur in the LOC-OB system equipment with respect to the failure categories described in Section 3.1 regarding the requirement SpecSysReq[047]:

To investigate the failures, the FMEA is carried out at the level of replaceable units/components and boards (LRUs).

Failures during preventive and corrective maintenance are not the object of the investigation. To exclude this type of failures, it is required to observe the procedures, work instructions, warnings, notes and rules during the maintenance of the LOC-OB system.

It should be noted that only failures in the architecture elements described in Section 2 are investigated; failures in components outside the system boundary defined in Section 2 are not object of the investigation.

Only permanent failures are considered, i.e. failures that are caused by hardware failures. External negative influences are controlled by the respective barriers (insulation clearances, EMC protection, ventilation, enclosures with specific IP protection, fuses etc.).

Temporary failures can also occur, e.g. due to interferences or software errors. However, these can be corrected at short notice. Temporary failures are defined as failures that can be corrected within 5 minutes without hardware repair.

4.2 FMEA for the components of the LOC-OB system

The FMEA investigates component failures with respect to the three failure categories: Immobility failure, Reduced service failure and Minor failure (see Section 3.1).

The failure impacts of the components of the LOC-OB system are listed in the Table 12.

The kind of failures of the components of the LOC-OB, that are considered in this analysis, are mostly complete HW failures, with exception of failure of memory parts. Partial failures of HW advances into complete failures after of a determined time. Because of these partial failures will not be considered in this analysis. In this analysis failures regarding of not defined environmental or operational conditions are not considered. Systematic failures because of deviations of the quality process or external events are not considered.

This table contains:

- the component to be analysed (second column "Component");
- the function or description of the component to be analysed (third column);
- the component-specific failure mode (fourth column);
- the failure cause (fifth column);
- the local impact (sixth column);
- the impact on the LOC-OB system (seventh column);
- the operational impact with respect to the vehicle functionality (eighth column);
- the detection method (ninth column);
- the compensating precautions against the failure (tenth column), and
- the failure category (eleventh column).

No.	Component	Function/description	Failure mode	Failure cause	Local impact	Impact on on-board equipment	Impact on train/operational	Possible detection methods	Compensating precautions against failure	Failure category
1a	HW-GNSS-Receiver	A satellite navigation receiver is a user equipment that uses one or more of several global navigation satellite systems (GNSS) to calculate the device's geographical position and provide navigational advice.	Failure of the GNSS receiver No calculation of position and speed Satellite telegrams are not processed	Hardware defect	Damaged GNSS receiver doesn´t generate more GNSS Telegrams	No immediate impact	Assumptions: Continued operation for up to defined period of time. The location information from the HW-Pulse generator and HW-IMU is used.	LED on board Diagnostics message	Train can continue to run within the period of time that is provided for this type of failure. Without the HW-GNSS functionality	Reduced service failure
1b	HW-GNSS-Antenna	Reception of GNSS signals	No GNSS data transmission between Satellite and HW-GNSS-receiver	Hardware defect	GNSS receiver doesn´t generate more GNSS Telegrams	No immediate impact	Assumptions: Continued operation for up to defined period of time. The location information from the HW-Pulse generator and HW-IMU is used.	LED on board Diagnostics message	Train can continue to run within the period of time that is provided for this type of failure. Without the HW-GNSS functionality	Reduced service failure
2	HW-IMU	An Inertial Measurement Unit (IMU) measures and reports a body's specific force, angular rate, and sometimes the orientation of the body, using a combination of accelerometers, gyroscopes, and sometimes magnetometers.	1 HW-IMU failure 2 HW-IMU failure of its register memory	Hardware defect	To 1: A faulty IMU does not generate IMU telegrams. To 2: IMU telegram is created incorrectly.	No immediate impact	Assumptions: Continued operation for up to defined period of time. The location information from the HW-Pulse generator and HW-GNSS is used	LED on board Diagnostics message	Train can continue to run within the period of time that is provided for this type of failure. Without the HW-IMU functionality	Reduced service failure
3	HW-Pulse Generator	The pulse generator is used to determine the distance and speed of railway vehicles.	The HW-Pulse Generator no longer provides path impulses	Hardware defect	Location information from the pulse generator is not available	No immediate impact	Assumptions: Continued operation for up to defined period of time. The location information from the HW-IMU and HW-GNSS is used	LED on board Diagnostics message	Train can continue to run within the period of time that is provided for this type of failure. Without the HW-Pulse generator functionality	Reduced service failure

No.	Component	Function/description	Failure mode	Failure cause	Local impact	Impact on on-board equipment	Impact on train/operational	Possible detection methods	Compensating precautions against failure	Failure category
4	HW-Digital-Map	Digital map data (provided by DR) provides geographical and topological description of the railway	Digital map data does not provide geographical and topological description of the railway	Hardware defect	HW-Navigation Engine and HW-Integrity-Engine do not receive geographical and topological description of the railway	System failure	Assumptions: Activation of emergency braking	LED on board Diagnostics message	Bypassing of emergency brake application is possible	Immobility
5	HW-FDE	Data Fault Detection and Exclusion (FDE) aim at detecting, and at filtering/excluding the faulty data before their uses into the algorithms	Data Fault Detection and Exclusion (FDE) does not aim at detecting, and at filtering/excluding the faulty data before their uses into the algorithms	Hardware defect	HW-Integrity-Engine and HW-Navigation engine does not deliver safe and not safe information because the outputs from HW-GNSS, HW-IMU and HW-Pulse-Generator cannot be processed	System failure	Assumptions: Activation of emergency braking	LED on board Diagnostics message	Bypassing of emergency brake application is possible	Immobility
6	HW-Navigation-Engine	The navigation engine computes track selectivity and 1D or 3D kinematic data.	The navigation engine does not compute track selectivity and 1D or 3D kinematic data.	Hardware defect	HW-Navigation-Engine does not deliver safe and not safe information because the outputs from the outputs from HW-FDE and HW-Digital-Map cannot be processed	System failure	Assumptions: Activation of emergency braking	LED on board Diagnostics message	Bypassing of emergency brake application is possible	Immobility
7	HW-Integrity-Engine	The integrity engine computes confidence intervals and tracks id confidence status	The integrity engine does not compute confidence intervals and tracks id confidence status	Hardware defect	HW-Integrity-Engine does not deliver safe information because the outputs from HW-FDE and HW-Digital-Map cannot be processed	System failure	Assumptions: Activation of emergency braking	LED on board Diagnostics message	Bypassing of emergency brake application is possible.	Immobility

Table 12: FMEA of the components of the LOC-OB system

4.3 Failure rates of the components of the LOC-OB system

The failure rates for the components of the LOC-OB system have been assumed according to the similar components of other current GNSS systems, current odometry components and similar digital modules (see examples of failure rates from the technical data sheets for the GNSS-Receiver, IMU and pulse generator in [R10], [R11] and [R12]). The assumed failure rates serve as a reference for an approximation of real values for the components of the LOC-OB system and they will be described in the following table:

No.	Components of the LOC-OB	Failure rate [Failures per hour]	Comments
1a	HW-GNSS- Receiver	5,0E-07	Value assumed from technical datasheet information for this device type
1b	HW-GNSS-Antenna	9,5E-07	Value assumed from field data information for this device type
2	HW-IMU	5,0E-07	Value assumed from technical datasheet information for this device type
3	HW-Pulse-Generator	2,0E-06	Value assumed from technical datasheet information for this device type
4	HW-FDE	5,0E-07	Value assumed from development experiences with small complex digital modules
5	HW-Digital-Map	5,0E-07	Value assumed from development experiences with small complex digital modules
6	HW-Navigation-Engine	8,0E-07	Value assumed from development experiences with medium complex digital modules
7	HW-Integrity-Engine	8,0E-07	Value assumed from development experiences with medium complex digital modules

Table 13: Failure rate of the components of the LOC-OB system

Remark: The assumption of constant failure rates is common practice in the reliability modelling of electronic components. All assumed failure rates must be adjusted by means of field data from customer projects when these are available.

4.4 Reliability block diagrams

Reliability block diagrams (RBDs) are a good graphical representation of the different components that are involved in a failure. The blocks are connected with direction lines that represent the reliability relationship between the blocks.

The failure of the overall system occurs whenever the path from the start to the end can no longer be executed. An involved component blocks the throughput when it fails. An RBD is shown for each failure category. However, the calculation of the system reliability is done by applying the FTA (see Section 4.5 for details).

4.4.1 Reliability block diagram “Minor Failure”

According to the FMEA results, there are not components involved in the "Minor failure" category.

4.4.2 Reliability block diagram “Reduced service failure”

According to the FMEA results, the components involved in the " Reduced service failure" category are represented in graphical format.

Figure 8: Reliability block diagram “Reduced service failure”

4.4.3 Reliability block diagram “Immobility failure”

According to the FMEA results, the components involved in the "Immobility failure" category are represented in graphical format.

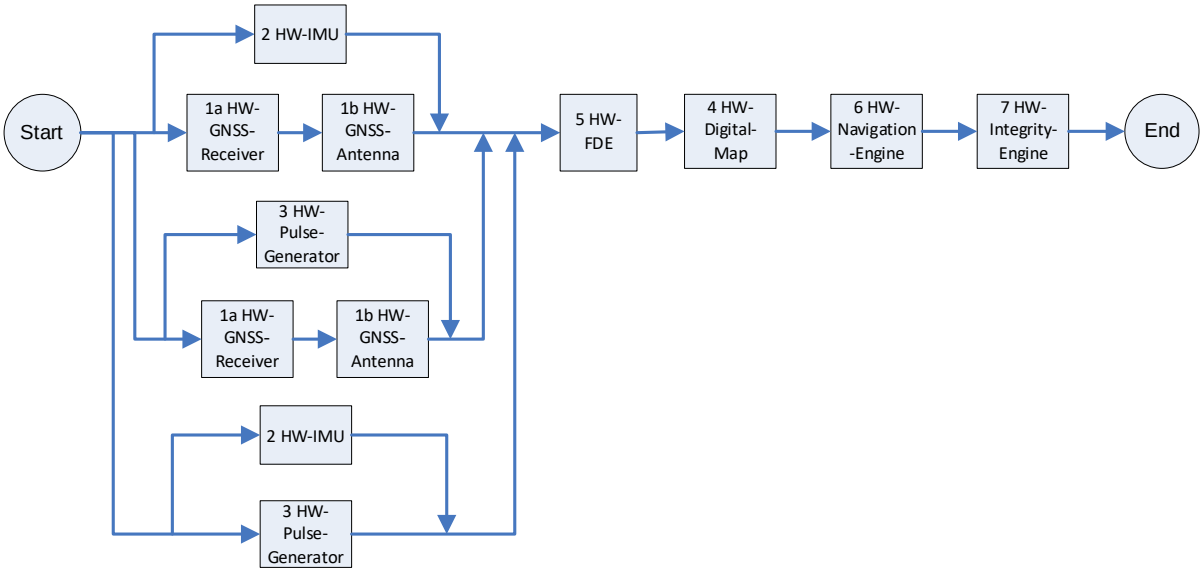

Figure 9: Reliability block diagram "Immobility failure"

4.5 FTA and calculation of system reliability of the LOC-OB system

The Fault Tree Analysis (FTA) is a type of failure analysis in which an undesired state of a system is examined. This analysis method is used to understand how systems can fail, to identify the best ways to reduce risk and to determine failure rates of a particular system failure. The fault tree analysis maps the relationship between faults, subsystems or components, and redundant design elements by creating a logic diagram of the overall system (see FTA methodology in [R8]).

For the modelling of the fault trees, a system lifetime of 25 years was assumed. When constant failure rates are assumed for the components, the system reliability is also time independent.

Moreover, the manufacturers' specifications concerning the intervals for preventive maintenance of the components shall be observed and documented accordingly in the customer documentation.

Note:

Since components come from different manufacturers and have different failure rates, components that are most frequently used based on the experience from customer projects were selected first for the FTA, and then components that have the lower failure rates.

4.5.1 Fault Tree for Failure category "Minor Failure"

According to the FMEA results, there are not components involved in the "Minor failure" category.

4.5.2 Fault Tree for Failure category “Reduced Service Failure”

From the FMEA, the following determination was considered for the failure category "Reduced service failure" for the FTA:

- Failure of the HW-GNSS-receiver, of the HW-GNSS-Antenna, of the HW-IMU, of the pulse generator, of the radar sensor and of the HW-Digital-Map results in a reduction of the LOC-OB performance. This kind of failures correspond to the category “Reduced Service Failure”.

The failure rate according to FTA for the failure category “Reduced service failure " is 3,95 E-06 failures/hour or an MTBF value of 28,90 years (see Figure 10).

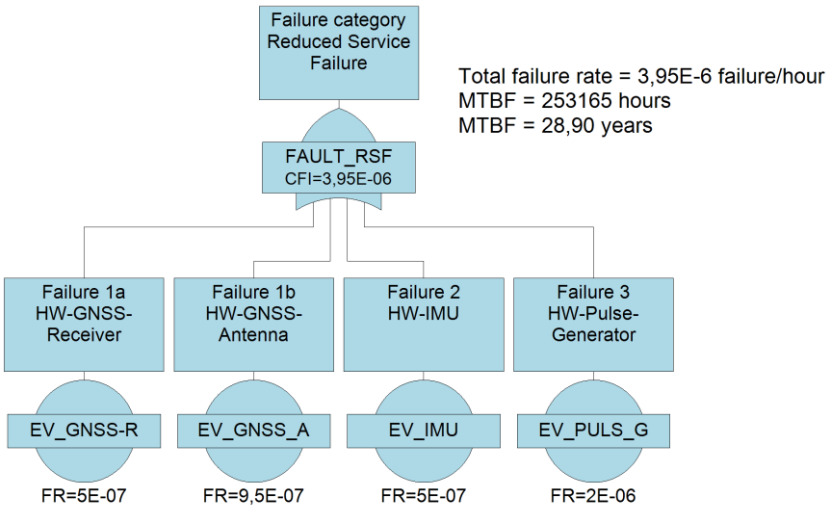

Figure 10: Fault Tree for Failure category “Reduced service failure”

4.5.3 Fault Tree for Failure category “Immobility failure”

From the FMEA, the following determination was considered for the failure category " Immobility failure " for the FTA:

Failure of the HW-Navigation-Engine, of the HW-Integrity-Engine, of the FDE results in an emergency brake. This kind of failures correspond to the category “Immobility failure”.

- The failure of components of the following combinations results in an emergency brake:
  - if the Radar Sensor and the Pulse Generator fail;
  - if the Radar Sensor and the HW-GNSS-Receiver and -Antenna fail;
  - if the Pulse Generator and the HW-GNSS-Receiver and -Antenna fail;

- If one of the components of the described combinations fails, the LOC-OB can work for 30 days before the defective component must be replaced. A CMT of 30 days is assumed for the replacement of the failed component of (see assumption 1 in Section 6.1).

The failure rate according to FTA for the failure category “Immobility failure" is 2,963 E-06 failures/hour or an MTBF value of 38,53 years (see Figure 11).

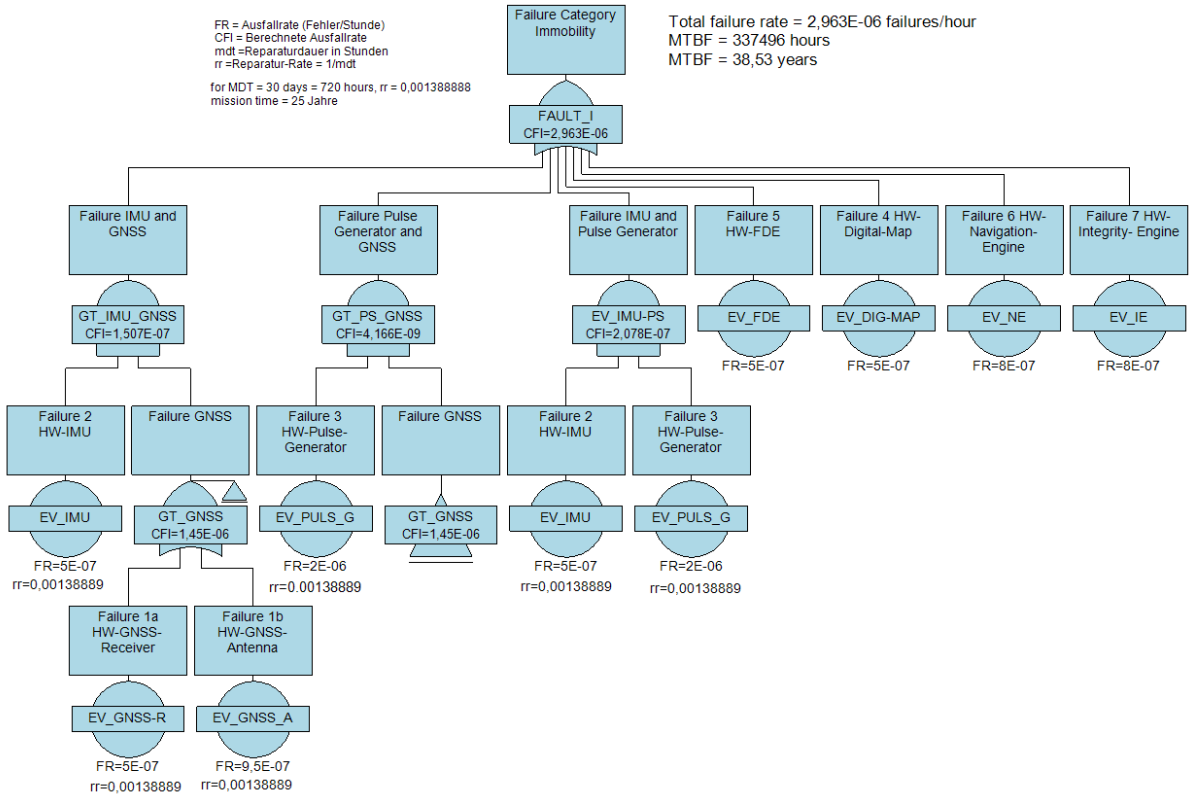

Figure 11: Fault Tree for Failure category “Immobility failure”

5 DETERMINATION OF MAINTAINABILITY

In order to determine the performance of LOC-OB system regarding maintainability it is necessary to check the ability of the LOC-OB system to be timely and easily maintained, including topics like service, inspection and check, repair and /or modification.

The following sections 5.1 and 5.2 look to the maintenance that involves functional checks, servicing, repairing or replacing of necessary components and equipment. The two basic types of maintenance "corrective maintenance" and "preventive maintenance" will be considered.

5.1 Corrective Maintenance and estimation of MTTR of LOC-OB System

The corrective maintenance is a maintenance task performed to identify, isolate, and rectify a fault so that the failed equipment, machine, or system can be restored to an operational condition within the tolerances or limits established for in-service operations.

The Mean Time to Repair (MTTR) is a basic measure of the maintainability of repairable items, and its time is usually expressed in hours. It represents the average time required to repair a failed component or device. It generally does not include lead time for parts not readily available or other administrative or logistic Downtime.

According to the MTTR definition, the MTTR comprises the diagnostic time, the effective time to replace a failed LRU with a failure-free LRU as well as the recommissioning time including software download and subsequent functional test (see Figure 3).

Thanks to the failure detection and error messages of the actual systems as well as the self-indicating components and boards, the diagnostic time for the LRUs in case of failure is reduced.

To calculate the MTTR of the on-board equipment (MTTRS), it is required to know MTBFi, MTTRi and the amount mi of each LRUi (i = 1, 2, …, n) of the LOC-OB system. The formula to calculate the MTTRS is showed as follow:

$$MTTR_S = \sum_{i=1}^{n} (m_i MTTR_i / MTBF_i) / \sum_{i=1}^{n} m_i / MTBF_i$$

In the case of components to be newly considered, it is necessary to contact the suppliers to verify or complement the maintenance information.

The Table 14 shows the break down structure of the LOC-OB until to the LRU level and it considers the assumed failure rates of the components of the LOC-OB according to table 13 as well as an assumed MTTR of 0,5 hours (30 minutes) for each of the components of the LOC-OB.

- The assumed MTTR of 0.5 hours corresponds to an approximate value derived from MTTR values of specific customer projects. These values are the result of time measurements of specific maintenance activities on board equipment. The values range from 20 minutes to 1 hour for corrective maintenance of components or modules in cabinets or enclosures. These

MTTR values include the time for failure detection, the time for replacement of the damaged component or module, and the time for functional testing of the component or module after replacement. The MTTR values of components depend on many factors such the accessibility of the components, the training level of the maintenance personal, the availability of maintenance documentation or tools.

The Table 14 also shows the result of the calculation regarding the total MTTR and MTBF of the LOC-OB.

Nr.	Name, Abbreviation	Hierarchy Level	Failure rate [FIT]	Quantity	Total failure rate [FIT]	MTBF [hours]	MTBF [years]	MTTR [hours]	Total failure rate* MTTR
	LOC-OB	Subsystem							
1a	HW-GNSS- Receiver	LRU	500	1	500,00	2000000	228,31	0,5	250,00
1b	HW-GNSS-Antenna	LRU	950	1	950,00	1052632	120,16	0,5	475,00
2	HW-IMU	LRU	500	1	500,00	2000000	228,31	0,5	250,00
3	HW-Pulse-Generator	LRU	2000	1	2000,00	500000	57,08	0,5	1000,00
4	HW-Digital-Map	LRU	500	1	500,00	2000000	228,31	0,5	250,00
5	HW-FDE	LRU	500	1	500,00	2000000	228,31	0,5	250,00
6	HW-Navigation-Engine	LRU	800	1	800,00	1250000	142,69	0,5	400,00
7	HW-Integrity-Engine	LRU	800	1	800,00	1250000	142,69	0,5	400,00
		Total Failure rate (LOC-OB) [FIT]			**6550,00**				3275,00
		Total MTBF (LOC-OB) [hours]			**152672**				
		Total MTBF (LOC-OB) [years]			**17,43**				
		Total (LOC-OB) [hours]							**0,50**

Table 14: Breakdown structure of the LOC-OB until to the LRU level, MTBF and MTTR

5.2 Preventive Maintenance and determination of the MTTPM and MTBPM of the LOC-system

The preventive maintenance is "a routine for periodically inspecting" with the goal of "noticing small problems and fixing them before major ones develop.

The preventive maintenance carried out at predetermined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the functioning of an entity.

The Mean Time to Preventive Maintenance (MTTPM) is a usual parameter of the preventive maintenance, and its time is usually expressed in hours. Preventive maintenance is carried out in defined periods of time (Mean Time between Preventive Maintenance MTBPM). The MTTPM and the MTBPM are empirical values.

The MTTPM for a component is determined similarly as the MTTR (see Section 5.1) except for the fact that the preventive maintenance activities are performed cyclically, and the maintenance work is less intensive since most of the units considered are electronic and are therefore "maintenance-free".

The determination of the system specific MTTPM is done by means of averaging, i.e. the individual MTTPM values of the considered components are added and then divided by the number of considered components.

Most of MTTPM values were derived from MTTR values of the components of LOC_OB System. For this purpose, it has been conservatively estimated which activities with respect to preventive maintenance were like the corrective maintenance and which time proportion these activities have in the MTTR of the considered components.

The results from this MTTPM and MTBPM estimation shall be considered as ideal values since these values can differ from the units considered in operation. The reason for these deviations is the different factors that influence the MTTPM values, such as the experience of the maintenance staff or the railway operator's maintenance organization.

In the case of components to be newly considered, it is necessary to contact the suppliers to verify or complement the maintenance information.

Because all considered components of the LOC-OB are electronic, these components do not need some kind of preventive maintenance. It is said that these components are maintenance-free.

6 DETERMINATION OF AVAILABILITY

In order to determine the performance of LOC-OB system regarding availability it is necessary to check the ability of the LOC-OB system to be in operation in a specified time.

For the LOC-OB system the "intrinsic availability Ai" will be considered according to chapter 15.2.3 of [R3]. The probability that an item will operate satisfactorily at a given point in time when used under stated conditions in an ideal support environment. It excludes logistics time, waiting or administrative downtime, and preventive maintenance downtime. It includes corrective maintenance downtime. Intrinsic availability is generally derived from analysis of an engineering design:

- The impact of a repairable element on the availability of the system, in which it operates, equals mean time between failures MTBF/ (MTBF+ mean time to repair MTTR):

  Ai = MTBFs / (MTBFs +MTTRs)

For the determination of the LOC-OB System availability will be considered the system MTTR (MTTRs) and the system MTBF (MTBFs) corresponding to the failure category "Immobility failure".

The Table 14 indicates that the MTBF for the LOC-OB System corresponds to 104712 hours and the MTTR for the LOC-OB System corresponds to 0,5 hours.

According to the formula for intrinsic availability:

Ai = 152672 hours / (152672 hours +0,5 hours) = 152672 hours / 152672,5 hours
Ai = 0,999996725 = 99,9996725 %

7 RESULT OF THE ANALYSIS VS RAM REQUIREMENTS

In this section will be considered only relevant RAM requirements for this document. The following requirements, specified in chapter 12 of [R3], have not considered : SpecSysReq[048], SpecSysReq[072], SpecSysReq[050], SpecSysReq[051], SpecSysReq[052] SpecSysReq[067]. These are functionalities or properties to be developed and they will be realized in other work packages.

For this document relevant RAM requirements regarding “Reliability”:

Requirement	Description	Results
SpecSysReq[047]	The LOC-OB hardware shall comply with the overall CCS-OB reliability as defined in Ref [57] Chapter 2. Minor failure: λ <1,25 10-4/h. Reduced service failure: λ < 3,3 10-6/h. Immobility failure: λ < 3,7 10-7/h.	Not ok. Minor failure: the failures of the components of the LOC-OB System do not conduce to this failure category (see section 4.5.1). Reduced service failure: λ =3,95 10-6/h (see section 4.5.2). Immobility failure: λ < 2,963 10-6/h (see section 4.5.3).

Observations:

The requirement about “Reduced service failure” could not be fully met. This is because the assumed failure rates are conservative. It is possible to improve the calculated failure rate if an accurate reliability prediction of the corresponding HW components could be performed using the “Part Stress Analysis Prediction” (see section 1.31.3). This way, the requirement could be met.

- For this failure category it is not recommended to introduce additional changes to the LOC-OB system, such as the use of additional redundant HW components to improve the reliability, due to unnecessary increase in development costs.
- The values used in the analysis are theorical, based on similar components. For a future product, the components will have to be carefully chosen to ensure meeting targets.

The requirement about “Immobility failure” could not be met. The estimated failure rate is too big in comparison to the requirement. It is possible to improve failure rate if the corresponding HW architecture is improved by using of redundancies. In this case it is necessary to test which redundancies of determined HW components could make sense. This way, the requirement could be met.

Remark: It is possible to use redundancies for almost each related HW component of the architecture. But at the end the best solution depends on a good balance between costs and complexity of the decided configuration. Because of this it was decided to do not propose some specific solution in this document. Important here are the quantitative results of the analysis because these are a good reference for taking decisions about necessary redundant HW components.

For this document relevant RAM requirements regarding “Availability”:

Requirement	Description	Results
SpecSysReq[049]	The LOC-OB shall have an overall availability of 99,998% during operation.	Ok. According to the section 6 the LOC-OB system has an availability of 99,9996725 % during operation.

Observation: The estimation for the required availability takes into account the calculated total MTBF of Table 14 as well as an MTTR that includes the diagnosis time, the effective time to replace a faulty LRU with a failure free LRU, and the time to resume operation including software download and subsequent functional testing. The result of this calculation corresponds to the intrinsic availability Ai.

- In order to estimate the real operational availability Ao of the LOC-OB system, it is necessary to take into account operational aspects such as logistical times, administrative times, time for the provision of spare parts, time for booking workshops, time to put in operation the vehicle, etc. This has the consequence that the estimated availability value could be reduced.
- Since these aspects vary from railway operator to railway operator, it is only possible for the manufacturer of railway technology to publish an intrinsic availability without taking into account the operational aspects of the railway operators.

For this document relevant RAM requirements regarding “Maintainability”:

Requirement	Description	Results
SpecSysReq[054]	The LOC-OB’s design and maintenance concept shall meet a Mean Time To Restore (MTTR) ≤ 1h.	Ok. According to the Table 14 the LOC-OB System has a MTTR of 0,5 hours

Requirement	Description	Results
SpecSysReq[055]	Preventive maintenance or periodic sensor calibration period of the overall LOC-OB shall exceed 2 years.	Ok. The LOC-OB System does not need preventive maintenance (see section 5.2)

Observation: Similar to the previous chapter the estimation for MTTR includes the diagnosis time, the effective time to replace a faulty LRU with a failure free LRU, and the time to resume operation including software download and subsequent functional testing.

- In order to estimate an operational MTTR of the LOC-OB system, it is necessary to take into account operational aspects such as logistical times, administrative times, time for the provision of spare parts, time for booking workshops, time to put in operation the vehicle, level of training of the maintenance teams, availability of spare parts etc. This has the consequence that the estimated MTTR could increase.

- Since these aspects vary from railway operator to railway operator, it is only possible for the manufacturer of railway technology to publish a MTTR without taking into account the operational aspects of the railway operators.

8 REFERENCES

Reference ID	Title	Content
[R1]	EN 50126-1-2017	Railway Applications - The Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1: generic RAMS process
[R2]	CLUG2.0 – D2.3	Loc-OB System Definition & Operational Context, v2.0
[R3]	CLUG2.0 – D2.4	Loc-OB System requirements, v2.0
[R4]	CLUG2.0 – D3.1	Loc-OB RAMS Plan, v1.0
[R5]	IEC_60812-2018	Failure modes and effects analysis (FMEA and FMECA)
[R6]	IEC_60050_192-2015	International electrotechnical vocabulary–Part 192: Dependability
[R7]	CLUG2.0 – D3.7	Loc-OB RAMS Evaluation report
[R8]	IEC_61025	Fault tree analysis (FTA)
[R9]	EN 50129-2018	Railway applications – Communication, signalling and processing systems – Safety-related electronic systems for signalling, EN 50129:2018 + AC:2019
[R10]	GNSS-750 MTBF	Hexagon, Novatel, Webseite GNSS-750 MTBF. NovAtel Inc. Hexagon Calgary Campus, 10921 14th Street NE, Calgary, Alberta, Canada, T3K 2L5. https://novatel.com/support/known-solutions/gnss-750-mtbf
[R11]	IMU-ADIS16003	Analog Devices, Data Sheet, FIT Report ADIS16003 MCM. https://ez.analog.com/cfs-file/__key/communityserver-wikis-components-files/00-00-00-01-13/ADIS16003_5F00_FIT.PDF
[R12]	HaslerRail OPG	HaslerRail, Datasheet Optical Pulse Generator (OPG)., 5.0301.035-04TEN – A02

9 CONCLUSION

The relevant RAM requirements for this document regarding availability and maintainability could be fulfilled according to the hypotheses and assumptions of section 2.2.

The relevant RAM requirements for this document regarding **Reliability** could not be fulfilled according to the hypotheses and assumptions of section 2.2.

In order to accomplish completely the reliability target of SpecSysReq[047] regarding “Reduced service failure” it is possible to improve the calculated failure rate if an accurate reliability prediction of the corresponding HW components could be performed using the “Part Stress Analysis Prediction” (see observation in section 7).

In order to accomplish completely the reliability target of SpecSysReq[047] regarding “Immobility failure” it is necessary to improve the architecture of the LOC-OB system with new redundancies.

In order to estimate a real MTTR and an operational **Availability** (Ao) of the LOC-OB system for the railway operators it is necessary to take into account operational aspects such as logistical times, administrative times, time for the provision of spare parts, time for booking workshops, time to put in operation the vehicle, level of training of the maintenance teams, availability of spare parts etc. This has the consequence that the estimated availability value could be reduced.

The temporal analysis concerning **Maintainability** shows that requirements from D2.4 (SpecSysReq[054] and SpecSysReq[055]) could be reached using the proposed architecture.

The RAM analysis can be further developed when new findings on functional architecture and HW are obtained. New findings obtained here will also lead to the further development of the existing RAM analysis.

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