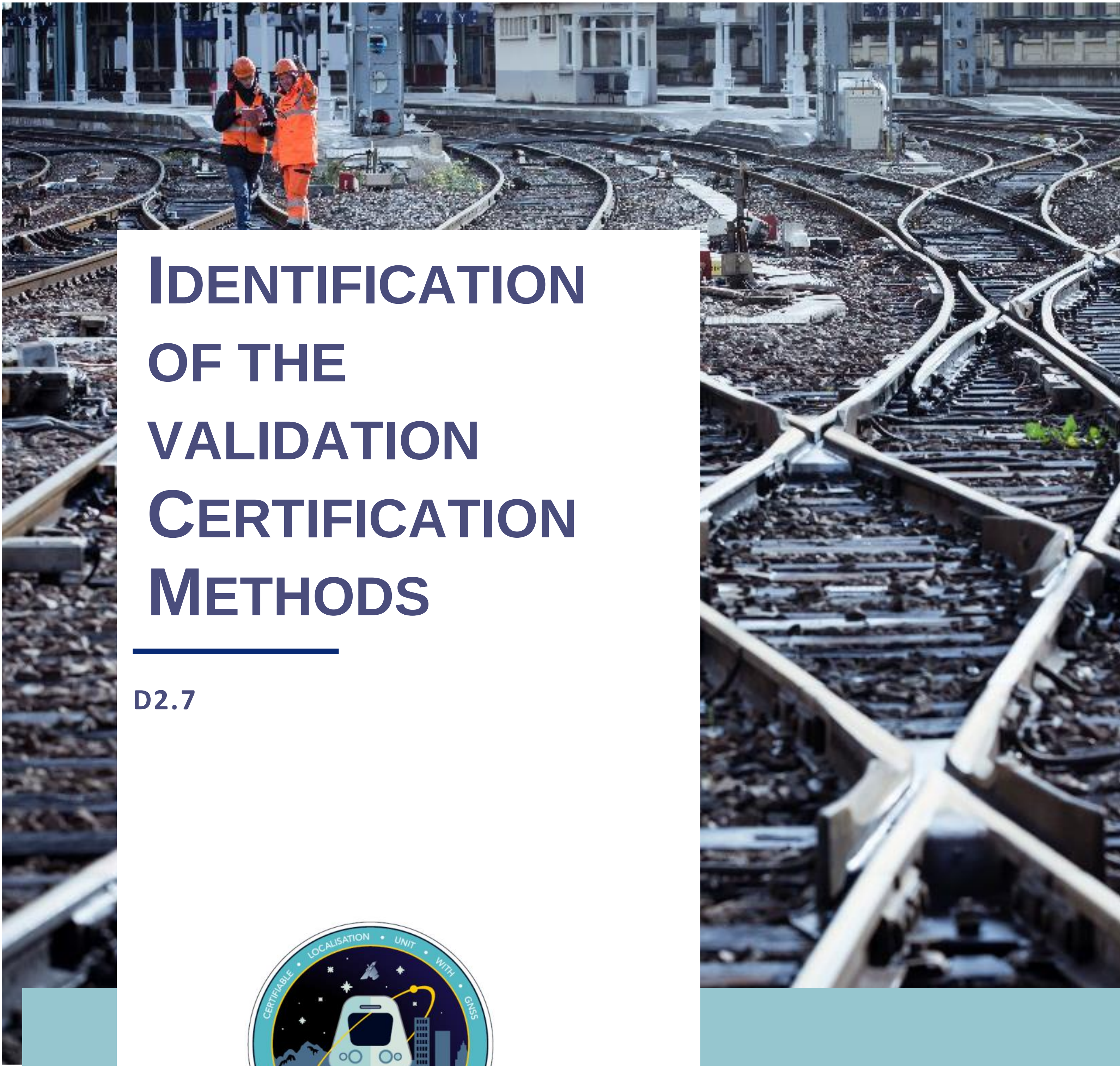


Identification of the validation Certification Methods

D2.7

25. SEPTEMBER 2021

VERSION 1.5

European
Global Navigation
Satellite Systems
Agency

This project has received funding from the European Union’s Horizon 2020

D2.7D2.7 - IDENTIFICATION OF THE VALIDATION CERTIFICATION METHODS IDENTIFICATION OF THE VALIDATION CERTIFICATION METHODS

DOCUMENT'S ADMINISTRATION	
Title	Identification of the validation Certification Methods
Deliverable number	D2.7
Leader/Responsible of this Deliverable	NavCert
Author(s)	Oliver Schneider (NavCert) Ernst Phillip Mrohs (NavCert) Sravan Machiraju (NavCert)
Reviewer(s)	Anna Grzebellus (NavCert) Ernst Phillip Mrohs (NavCert)
Validator(s)	Iban Lopetegi (CAF) Marco Moss (SBB) Marc Sarrat (SNCF) Alain Ruaudel (Airbus)
Due date of deliverable:	31. May 2021
Submission date	18. November 2021
Version	1.5
Status	submited

DISSEMINATION LEVEL		
PU	Public	
CO	Confidential, restricted under conditions set out in Model Grant Agreement	X

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 870276

VERSIONS OF THE DOCUMENTS

Revision	Date	Description
0.1	10.03.2020	Initial Skeleton
0.2	31.03.2020	Update
0.3	16.06.2020	Update based on input from Questionnaire
0.4	07.09.2020	Update for section 3. Methodology adjustment and enhancement
0.5	25.02.2021	Update and extension of all section based on review comments
0.6	15.03.2021	Update based on input from other deliverables
1.0	31.03.2021	Finalization based on NavCert internal review
1.1	30.04.2021	Update based on review feedback
1.2	26.05.2021	Released Version
1.3	15.07.2021	Version released to external reviewers after internal quality review

EXECUTIVE SUMMARY

This document is the deliverable "D2.7 – Identification of the validation Certification Methods" of the European project "CERTIFIABLE LOCALISATION UNIT WITH GNSS IN THE RAILWAY ENVIRONMENT" (hereinafter also referred to as "CLUG).

The certifiability of the developed safety-relevant train localisation system is one of the main focuses of the project. Hence it is of major importance to identify and evaluate possible validation and certification methods at an early point in the project. This must take the considerations from the WP2.3 preliminary hazard analysis and WP2.6 architectural properties of the system into account. This is especially important for the concepts of sensor fusion with the consequences on availability, reliability, integrity, and protection level (or confidence interval, respectively) of the provided localization data. This will serve as input to WP5.3 for the prototypical certification.

This document is based on the terms and conditions established in the Grant Agreement (GA) and its Annexes, as well as in the Consortium Agreement (CA).

The use of the present guidelines can ensure better collaboration among the consortium partners.

This deliverable is to be used by all the project partners to ensure quality assurance of project processes and outputs and prevent possible deviations from the project work plan.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

APPLICABLE DOCUMENTS

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

- Grant Agreement N°870276 (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: This defines the obligations towards all project partners.

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.

LIST OF APPLICABLE DOCUMENTS

The following are the applicable documents with Identifier, title, reference, and issue date, used to identify and define the validation and certification methods for the development and certification processes.

Identifier	Title	Reference	Issue and date
AD-01.	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Part 1: Generic RAMS Process	EN 50126-1	Issue: 2017
AD-02.	The specification and demonstration of reliability, availability, maintainability, and safety (RAMS)- Part 2: System approach to safety	EN 50126-2	Issue: 2017
AD-03.	Railway applications – Communication, signalling and processing systems-Software for railway control and protection systems	EN 50128	Issue:2011
AD-04.	Railway applications-communication, signalling and processing systems-safety related electronic system for signalling	EN 50129	Issue: 2018
AD-05.	Communication, signalling and processing systems-safety-related communication in transmission systems	EN 50159-1	Issue: 2010

Identifier	Title	Reference	Issue and date
AD-06.	Safety of machines-functional safety of electrical, electronics and programmable machine controls	EN 62061	Issue: 2013
AD-07.	Railways Applications - Rolling stock applications - Software on Board Rolling Stock	EN 50657	Issue: 2017
AD-08.	Railway applications - Quality management system - Business management system requirements for rail organizations: ISO 9001:2015 and particular requirements for application in the rail sector	ISO/TS 22163	Issue: 2018
AD-09.	Railway applications- Environmental conditions for equipment - Part 1: Equipment Train vehicles	EN 50125-1	Issue:2014
AD-10.	Environmental conditions for equipment: equipment for signalling and telecommunications	EN 50125-3	Issue:2003
AD-11.	Type Approval Test on Electronic Equipment for Railway Applications	EN50155	Issue:2018
AD-12.	Railway applications - Electromagnetic compatibility - Part 3-2: Rolling stock - Apparatus	EN 50121-3-2	Issue:2017-11
AD-13.	Railway applications - Rolling stock equipment - Shock and vibration tests	IEC 61373	Issue:2010
AD-14.	Railway applications - Rolling stock - Protective provisions relating to electrical hazards;	EN 50153	Issue:2018
AD-15.	Railway applications - Rolling stock - Rules for installation of cabling	EN 50343	Issue:2014
AD-16.	Classification of environmental conditions - Part 3-3: Classification of groups of environmental parameters and their severities - Stationary use at weather protected locations	IEC 60721-3-3	Issue:2019
AD-17.	Railway applications - Fire protection on railway vehicles - Part 2: Requirements for fire behavior of materials and components	EN 45545-2	Issue: 2020
AD-18.	Electric railway equipment Train communication network conformance testing	IEC-61375-2	Issue: 2019

Identifier	Title	Reference	Issue and date
AD-19.	Industrial communication networks - Network and system security	62443-1-1	Issue:2017
AD-20.	Road vehicles – Functional safety	ISO 26262 series	Complete series was issued 2011
AD-21.	Annex VI of the Delegated Regulation	DR 2017/79	Issue:2017
AD-22.	Use of GNSS-based positioning for road Intelligent Transport Systems (ITS)	CEN/EN16803-Series	Issue:2019
AD-23.	Satellite Earth Stations and Systems (SES); GNSS based location systems;	ETSI TS 103 246-Series	Issue:2017
AD-24.	Rail-Report-on-User-Needs-and-Requirements	GSA Report	Issue:2021
AD-25.	Radio equipment operating in the 1 164 MHz to 1 300 MHz: Global Navigation Satellite System (GNSS) User Equipment (GUE)	ETSI EN 303 413 V 1.2.0	Issue:2020
AD-26.	Functional safety standards for the lifecycle of electrical, electronic, or programmable electronic (E/E/PE) systems and products.	IEC 61508 Series	Issue:2013
AD-27.	Technology readiness level (TRL) guidelines	CEN/TR 17603 - 11	Issue:2019
AD-28.	Specification of the test facilities, definition of test scenarios, description, and validation of the procedures for field tests related to security performance of GNSS-based positioning terminals.	PD CEN/TR 17475	Issue:2020
AD-29.	Test procedures for assessment of robustness to security attacks.	CEN/TR 17475	Issue:2020
AD-30.	Galileo for railway operations: question about the positioning performances analogy with the RAMS requirements allocated to safety applications	ETRR	Issue:2010
AD-31.	Performance Evaluation of GNSS for Train Localization	IEEE	Issue:2015

Identifier	Title	Reference	Issue and date
AD-32.	Information technology - Security techniques - Information security management systems - Overview and vocabulary.	ISO/IEC 27000	Issue:2016
AD-33.	RAMS evaluation of GNSS for railway localisation	IEEE	Issue:2013
AD-34.	Space-Use of GNSS-based positioning for road Intelligent Transport Systems (ITS)-Field tests definition for basic performance	CEN/TR17465	Issue:2020
AD-35.	General requirements for the competence of testing and calibration laboratories	ISO 17025	Issue:2017
AD-36.	Conformity assessment : Requirements for bodies certifying products, processes, and services	ISO 17065	Issue:2012
AD-37.	Evaluation of measurement data - Guide to the expression of uncertainty in measurement	JCGM 100	Issue:2008

Table 1: List if applicable documents

LIST OF REFERENCE DOCUMENTS

Identifier	Title	Reference	Issue
RD-1	CLUG – Glossary of terms		Issue: 1
RD-2	Grant Agreement.	Number 870276	Issue: 2019
RD-3	Project Management Plan	D1.1	Issue: 2020
RD-4	Project Quality Plan	D1.2	Issue: 2020
RD-5	Data Management Plan	D1.4	Issue: 2020
RD-6	Communication Strategy and Action Plan (CSAP).	D5.1	Issue: 2020
RD-7	High level mission requirements definition	D2.1	Issue: 2.5
RD-8	Operational scenarios	D2.2	Issue: 2.2
RD-9	High level system requirements	D2.3	Issue: 2.3
RD-10	Preliminary Hazard Analysis and Safety Requirements	D2.4	Issue: 1.4
RD-11	Preliminary Architecture Definition	D2.5	Issue: 3.7
RD-12	Preliminary External Interface Definition	D2.6	Issue: 4.2
RD-13	ERTMS Longer Term Perspective.		Issue: 2015
RD-14	ERTMS -LWG-Railways Localization System Localization Performance Requirements from use cases		Issue: 2019
RD-15	Integrity Concepts & Algorithms	D3.1.4	Issue:1.2

Identifier	Title	Reference	Issue
RD-16	Galileo for railway operations: question about the positioning performances analogy with the RAMS requirements allocated to safety applications	Rail Advisory Forum requirements	Issue 14 May 2010
RD-17	Handbook, Chapter 8: Safety Analysis/Hazard Analysis Tasks	FAA System Safety	Issue December 30, 2000
RD-18	Bidirectional Requirements Traceability by Linda Westfall		Issue May 2006

Table 2: List of reference documents

1 INTRODUCTION

1.1 Purpose

This document is intended for the following readers:

- Localisation specialists
  - Wishing to understand the process how to identify validation methods for a later certification with the background of railway under consideration of applicable standards
- Railway specialists
  - Wishing to understand the process how to identify validation methods for a later certification with the background of a safe localisation under consideration of applicable standards
- Certification and standardisation specialist
  - Wishing to understand the background of a safe localisation for the railway applications and how to apply the known standards

This report intend is to identify and define the validation and certification methods for the development and prototypical certification processes. Additionally, it provides guidance for related topics.

For this topic, this report shows the process how to identify suitable validation and certification methods step by step. For the identification, the state-of-the-art process within the railway environment for the certification and type approval of electric components with similar/comparable use are analyzed and transferred to the project's topic. Here the field of electronic components for:

- Critical communication system
- Train management system
- Information systems to customer

Additional approaches from the automotive and others industry will be analyzed if they could be integrated.

For the purpose of certification of the localization unit the following standards for example are acknowledged:

- International Railway Industry Standard (ISO/TS 22163) certification
- DIN EN 50126-1:2017- The specification and demonstration of reliability, availability, maintainability, and safety (RAMS)- Part 1: Generic RAMS Process
- DIN EN 50126-2:2017- The specification and demonstration of reliability, availability, maintainability, and safety (RAMS)- Part 2: System approach to safety
- EN 50125-1: 1999, Railway applications - Environmental conditions for equipment - Part 1: Equipment Train vehicles
- EN 50125-3 Environmental conditions for equipment: equipment for signalling and telecommunications
- EN 50129 Railway applications-communication, signalling and processing systems-safety related electronic system for signalling
- EN 50159-1 Communication, signalling and processing systems-safety-related communication in transmission systems

- EN 62061 Safety of machines-functional safety of electrical, electronics and programmable machine controls
- EN 50155 Type Approval Test on Electronic Equipment for Railway Applications
- EN 50128:2011 – Railway applications – Communication, signalling and processing systems- Software for railway control and protection systems.
- ISO 26262-series
- CEN/EN16803 "Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) series
- ETSI TS 103 246-1 activities for the GNSS-based Location Systems (GBLS)
- ETSI TS 103 246-2 Satellite Earth Stations and Systems (SES); GNSS based location system, Reference architecture.

1.2 Position in the project

This work package and deliverable form the connecting point to the later validation and testing in WP4 and the prototypical certification in WP5.3.

1.3 Definitions

Identifier	*Definition*
3D	Three-Dimensional space
AL	Alert limit
(Ai)	Intrinsic availability
ASD	Accelerated spectral density
ASIL	Automotive Safety Integration Level
ATO	Automatic Train Operation
BTM	Balise transmission module
CA	Consortium Agreement
CLUG	Certifiable localisation unit with GNSS in the railway environment
CEN	Committee of European Norms
CS	Cold Start
CTP	Conformance test procedure
DOP	Dilution of Precision
DoS	Denial of service
DYN	Dynamics
DUT	Device under test
E2E	End to End
eCall	Emergency call

EGNOS	European Geostationary Navigation Overlay Service
ELM	European land mass
EMC	Electromagnetic compatibility
ERTMS	European railway traffic management system
ETCS	European train control system
EUSPA	European Union Agency for the Space Programme
EUT	Equipment under Test
FMECA	Failure Modes, Effects, and Criticality Analysis
FRs	Foundational requirements
FTA	Fault tree analysis
GA	Grant Agreement
GBLS	GNSS based location system
GBPTs	GNSS based positioning terminal system
GNSS	Global Navigation Satellite System
GRES	GPS + GLONAS + Galileo + EGNOS
GSA	European GNSS Space Agency
GSM-R	Global System for Mobile Communications Railway
HARA	Hazard analysis and risk assessment
HHSD	High Safety and High Impact on Operation and Speed Dependent
HHPLOC	High Safety and High Impact on Operation &Precise Location
HAZOP	Hazard Operationality Study
HL	Hazard Level
HR	Hazard Rate
HS	Hot start
IAC	Identification and authentication control
IMU	Inertial Measurement Unit
IR	Integrity Risk
ISMS	Information security management systems
IVS	In-vehicle system
KPI	Key performance Indicators
LEU	Lineside encoder unit
LH	Low Safety High Impact on Operation
LHPLOC	Low Safety High Impact on Operation and Precise Location
LTE	Long Term Evolution

MCA	Minor change approval
MCI	Mission Confidence Interval for Operations
NA	Not Available
MTTR	Mean Time to Restore
NMEA	National marine electronic association
OBU	On Board Unit
O&SHA	Operating & Support Hazard Analysis
PE	Position error
PDOP	Dilution of Precision
Pfa	Probability of false alarm
PFH$_D$	Probability of a dangerous failure per hour
PICS	Protocol implementation conformance statement
PL	Protection level
PrHA	Preliminary Hazard Analysis
PVT	Position, Velocity and Time
QoS	quality of Service
RAMS	Reliability, Availability, Maintainability, and Safety
RAP	Risk-acceptance principle
RBC	Radio Block Centre
RF	Radio Frequency
RTMes	Reference Trajectory measurement Systems
SBAS	Satellite-Based Augmentation System
SIL	Safety-integrity levels
SIS	Signals in Space
SL	Security level
SL-C	Security level control system
SoL	Safety of Life
SPT	simulation prototypes tools
SRECS	Safety-related electrical, electronics and programmable electronic control systems
SRs	System requirements
SSIL	Software safety integrity level
STC	Supplemental Type Certificate
SUT	System under testing
TBD	To be defined
TCN	Train communication network

TFFR	Tolerable Functional Failure Rate
THR	Tolerable Hazard Rate
TIR	Target Integrity Risk
TRA	Technology readiness assessment
TLOBU	Train Localisation on Board Unit
TLS	Train Localisation system
TLU	Train Localization Unit
TRL	Technology Readiness Level
TTA	Time to Alert
TTFF	Time to First Fix
TUFE	Train Unit Front End
TURE	Train Unit Rear End
WGS84	World geodetic system 1984
WS	Warm Start

Table 3: Abbreviation and definition table

2 STATE OF THE ART

The scope of the Project CLUG is to have crucial building block to achieve the goal of the project to develop a Certifiable Localisation System using GNSS for the railways. Since the technology has not been yet standardized, the approach of CLUG is to integrate the development of process and tools for certification of localisation units, allowing CLUG project to prepare the adoption of new standards and regulation for localisation of trains.

The development of certifiable localisation technology using GNSS is expected to make the railway transport system providing more cost effective and ecological alternative for public transport, with many positive impacts on public mobility and regional development.

In this chapter the state of the art, as an first step for the certification of train localisation unit with multi-sensor approach, as a matter of fact, a critical evaluation focusing on the existing standards, regulations, references what already carried out for the GNNS in the different domains for type approval and certification processes will be addressed and presented a list of significant applicable documents that are related to Railway safety, Non-Safety and set of references which had focus on hardware, software and service requirements for positioning applications has been investigated.

Based upon this state of the art, methods based on the existing methodology, i.e., the applicable test methods and standards are then will be adapted and enhanced in the Section 3. These are then translated into technical requirements for the Localisation System within the Train Signalling System.

2.1 CURRENT STATE OF TYPE APPROVAL OF ELECTRIC ASSISTANCE COMPONENTS IN RAILWAY VEHICLES

The localization unit is a device that fulfils specific functions for location, basically the provision at the device's output interface of information on position and if necessary other information, for example: speed, direction of movement and acceleration. Such localization unit comprises of several electrical assistance components that support the unit. So, there is the need for type approval of electric components and the device itself. As there are no regulations for the GNSS requirements in railway vehicles. Regulations are needed for the type of approval of safety relevant train localization system. If equipment shall be installed in a type-certified railway vehicle, mainly two types of legal requirements must be fulfilled:

- The equipment must be approved
    - ○ First requirement concerns the approval of the equipment itself. It does not take into consideration the specific railway vehicle into which the equipment shall be installed. Normally, equipment is installed in railway vehicles because there is a requirement for this. Examples are GNSS receivers, IMU, Odometer, etc. in the domain of localization. Mandatory equipment must be compliant with a European Technical Standard or delegated regulation.
    - ○ Independently from the Technical Standard or delegated regulation requirement, there is a requirement for evidence that the part has been manufactured according to approved design data. This is called an authorized release certificate.

- The installation itself must be approved
    - If additional equipment is installed in a railway vehicle, the railway vehicle and the basis for its type certificate is changed. It is within the installer's responsibility to ensure that the installation is safe, and that the railway vehicle conforms to the application certification specifications also after the change. Such a change has normally to be approved.
    - Changes are distinguished in two classes: minor changes and major changes. Minor Changes require a Minor Change Approval (MCA) whereas Major Changes require a Supplemental Type Certificate (STC).

These two requirements are distinct and shall not be mixed up. For the type of approval, some tests shall demonstrate compliance and effectiveness of RAMS aspects (e.g.: Safety barriers implementation). The test result shall be put in evidence that safety criteria expected is reached.

2.2 Scope of Localization Unit with GNSS in the Railway Environment Certification

Certification is a process commonly used by many industry sectors to assess and assess that product, services are meeting certain requirements and to deliver certificates when the corresponding test results confirm the right state of compliance.

In the context of the railway vehicle, where the localization unit will be embedded, currently no regulations regarding GNSS topics are under development. Type approval requirements are also mandatory so that only minimum requirements are usually considered. In this section might however be retained for the regulation if these requirements are safety critical for instance.

Type approval targets

The targets are the type of components of the localization unit, being candidate for the localization unit with GNSS (Global Navigation Satellite System) in the railway environment certification. Localization units in railway vehicles, which are likely to combine several components, each one implementing a part of the localization functionalities and likely to implement several functionalities, need to be type approved as for instance:

- GNSS Receiver
    - to provide Galileo /EGNOS-based information used for calculation of PVT solution
- Inertial Measurement Unit (IMU)
    - to provide information upon physical forces applying to the train which are used as an additional input to the localisation algorithms
- Speed sensors/ wheel sensors
    - to provide information upon the travelled distance of the train on a general level and balise id level. This sensor is responsible for calculating the distance run by the train, typically consisting of redundant tachometry and radar, able to calculate distance, speed, and acceleration.
- Balise
    - Electronic beacon placed between the two rails responds to radio frequency energy broadcast by Transmission Module mounted under the train. It is a passive device that lays on the track, storing data (fixed or switchable, i.e., with the possibility of changing information content) related to the infrastructure, such as speed limits, position

references, gradients, etc.). It is a passive device because it does not need an electric supply, since it is the train antenna (BTM) that energizes it when passing over it.

- Balise Transmission Module (BTM)
    - The BTM is a module inside the ERTMS/ETCS on-board equipment for intermittent transmission between track and train, which processes signals received from the onboard antenna and retrieves application data messages from a balise.

- Radio Block Centre (RBC)
    - The RBC is a device used at ETCS Level 2 acting as a centralised safety unit which, using radio connection via GSM-R, receives among others information train position information and sends movement authorisation and further information required by the train for its movement. The RBC interacts with the interlocking to obtain signalling-related information, route status, etc. It is also able to manage the transmission of selected trackside data and communicate with adjacent RBCs.

- Lineside Encoder Unit (LEU)
    - The LEU plays a key role in the signalling system and works together with the balises. It acquires information (e.g., traffic) and forwards them to the balises. Each LEU can be connected to several balises and forward the information to them.

2.3 PROCESS OF CONFORMITY ASSESSMENT

The international standard ISO/IEC 17000 defines conformity assessment as a “demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.” Conformity assessment procedures, such as testing, inspection, and certification, offer assurance that products fulfil the requirements specified on the design particularly linked to RAMS topics and in accordance with regulations and standards (e.g., CEN EN 5012x series, functional safety IEC 61508 and common safety method CSM 402/2013).

Conformity to standards process is be based on the definition of test plans. For measurement equipment, conformity assessments shall be conducted by notified bodies in accordance with the conformity assessment procedures provided.

The test cases to be performed are defined with uniquely pass and fail criteria. This process requires the identification of key performance indicators (KPI’s), associated metrics and the minimum performance levels taken from the standard recommendations, regulations or the specification performed during the design.

The test cases used for testing or certification will encompass different situations (system architecture or module dependent) which are not all reflected in a unique standard. This means that several different standards might have to be used to define more tests. Thus, the definition of a test plan will be done according to available standards and regulations and the test plan will be extended to include other aspects based on the expertise and experience of the consortium.

The regulatory actions on positioning performance conformity testing will be based to a large extend on the standards. Respective technical requirements are provided by the regulations on indicating design, construction and performance requirements and testing standards for positioning equipment.

2.3.1 Reliability, Availability, Maintainability, and Safety (RAMS) analysis

RAMS is a measure of the technical performance of a system or subsystem or component. Poor RAMS results can cause high life-cycle cost and lead non-certifiability.

RAMS is made up of different elements which are reliability, availability, maintenance, and safety of the system under study. The data needed for RAMS analysis are extracted from operational, maintenance and design data and the results show the performance of the system in terms of failure and maintenance activities. Some relevant RAMS indicators are reliability/maintainability functions, failure/maintenance rates or the mean times to failure/repair/restoration.

The statistical model and the set of RAMS parameters that can be calculated depend strongly on the level of detail of the available data. Commonly used methodology for RAMS analysis includes Failure Modes, Effects, and Criticality Analysis (FMECA), Failure Mode and Effect Analysis (FMEA), Fault Tree Analysis (FTA), or Preliminary Hazard Analysis (PHA). These methodologies can be very specialized and sophisticated depending on how many factors one is willing to consider. Reliability and maintainability are modelled, and availability is calculated as the quotient of the mean-up-time (mean time available) to the total operational time.

2.3.1.1 <u>Failure Mode and Effect Analysis (FMEA)</u>

FMEA is an exhaustive analysis which identify all possible single failure of a system / subsystem or component. For each failure mode (corresponding to type of failure), the effect and associated consequences are analyzed. Failure mode stands for the modes in which a system might fail, and Effect analysis means the studying of the consequences of those failure.

FMEA can be said to be a frequently applied, systematic method for analyzing an item in order to identify its potential failure modes, their likelihood of occurrence, and their effects on the performance of the respective item and of the system that embeds it. The purpose of FMEA is preventing process and product problem before they occur.

Failure is prioritized according to the seriousness of their consequences and how frequent these failures occur and are detected. One of the purposes of FMEA is the elimination or reduction of those failures.

FMEA can be conducted in the design and planning phase of an item, as well as in the later stages of development, for example manufacturing and operational phases. It is especially important to distinguish between system FMEA, Design FMEA and process FMEA.

1. System FMEA – It analyze the failure mode and effect in relation to the risks in the system design. Its main objective is the development of a promising product concept, which is feasible within given boundary conditions.
2. Design FMEA – It is use on an added item design or previous existing design and helps determine potential failure modes of the item. Only the component level analysis is need and the goal of the design FMEA is to develop a flawless and robust design of the item.
3. Process FMEA – It consider an existing or previous process and help to determine the potential failure mode of the process.

<u>Ten steps for FMEA</u>

There are ten steps that all product/design and process FMEAs must follow. They are:

1. Review the process or product
2. Analysis of potential failure mode or use of existing library of hardware failure mode.
3. List potential effect of each failure mode
4. Each effect should be assigned severity ranking
5. Each failure mode should be assigned occurrence ranking
6. Evaluate and assign a detection ranking for each failure mode or effect
7. Determination of priority risk number for each effect
8. Failure mode for action should be prioritize
9. Actions should be taken to eliminate or reduce the high-risk failure mode
10. Determine the resulting risk priority number (RPN) as the failure modes are reduced or eliminated.

<u>Procedure of an FMEA</u>

FMEA procedure has to do with the steps of planning, performing and documentation. It is usually a team effort.

1. Planning phase – This is the first phase, and it involves the definition of the objectives of the analysis and the identification of the analysis boundaries and operating conditions. If it involves large and complex systems, then the systems need to be divided into subsystems before FMEA is performed on each of them.

2. Performing phase – This is the second phase and at this stage, the functions, the potential failure modes, and the consequence of the failure modes are identified and recorded.
3. Documentation phase – Documentation is done throughout the FMEA process. It is the documentation of all relevant information.

2.3.1.2 **Failure Modes, Effects and Criticality Analysis (FMECA)**

If failure modes are to be prioritized according to some criticality measure, then the process is called failure mode, effects, and criticality analysis (FMECA).

It is a method that is used to identify and analyze all potential failure modes of the various parts of the system and the effects these failures will have on the system and the process or method to avoid the failures or process to mitigate the effects of these failures.

FMECA is performed at the conceptual and initial design phases of the system to assure that all potential failure modes have been considered and the proper provisions have been made to eliminate these failures. FMECA is perform on the initial design phases because it is at this stage that we have the greatest impact on the equipment reliability.

There are diverse types of FMECA. They are Design FMECA, Process FMECA and System FMECA.

1. Design FMECA – It is done to eliminate failure during design of the equipment, considering all types of failures during the whole lifespan of the equipment.
2. Process FMECA – It focus on problems from how the system/ subsystem or component is manufactured, maintained, and operated.
3. System FMECA – It has to do with finding potential problems. It looks for potential problems and bottlenecks in larger processes, such as entire production lines. It can be done by analyses of each functional failure mode and associated effect for each equipment.

2.3.1.3 Fault Tree Analysis (FTA)

Fault tree analysis (FTA) can be described as an analytical technique, whereby an undesired state of the system is specified (mostly a state that is critical from a safety standpoint), and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur. The fault tree is a graphical model of the various parallel and sequential combinations of fault that will result in the occurrence of the predefined undesired event.

Fault tree analysis is a type of failure analysis in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events. This analysis method is used mainly to quantitatively determine the probability of a complex safety hazard in order to develop actions to mitigate or eliminate the hazard.

Fault tree analysis depicts the risk-based path to a root cause or based-level event. The identified risks drive actions which are intended to mitigate the risk prior to program launch. Fault tree analysis is applied when:

1. A hazard analysis previously indicated a safety concern.
2. There is a modern design with added content.
3. There is a current design with modifications, which may include changes due to past failure.
4. Investigation of a safety or regulatory concern.

The five basic steps to perform a fault tree analysis are as follows:

1. Identify the hazard.
2. Obtain understanding of the system being analysed.
3. Create fault tree.
4. Identify the cut sets.
5. Mitigate the risk.

2.3.1.4 Preliminary Hazard Analysis (PHA)

The Preliminary hazard analysis (PHA) is an analysis of the generic hazard groups present in a system. It is mostly the first attempt in the system safety process to identify and categorize hazards or potential hazards associated with the operation of a proposed system, process, or procedure.

The PHA is usually developed using the system safety techniques known as Failure Modes and Effects Analysis (FMEA) and/or the Energy Trace and Barrier Analysis (ETBA). PHA development can be somewhat simplified through the use of a Preliminary Hazard Matrix identifying a Generic Hazard Group. The PHA Report can be generated based upon the evaluation and analysis of system hazard risk.

Preliminary hazard analysis (PHA) is a semi-quantitative analysis that is performed to:

1. Identify all potential hazards and accidental events that may lead to an accident.
2. Rank the identified accidental events according to their severity.
3. Identify required hazard controls and follow-up actions.

The PHA shall consider:

- Hazard components.
- Safety related interfaces between various system elements, including software.
- Environmental constraints including operating environments.
- Facilities, real property installed equipment, support equipment, and training.

The PHA main steps are:

1. PHA prerequisites
2. Hazard identifications
3. Consequence and frequency estimation
4. Risk ranking and follow-up actions.

2.4 Applicable Documents Related to Railway Safety

The following chapter contains a briefly summary of available, applicable norms. For the further analysis, the complete norm was considered.

2.4.1 Applicable Document [AD-01]: EN 50126-1 -THE SPECIFICATION AND DEMONSTRATION OF RELIABILITY, AVAILABILITY, MAINTAINABILITY, AND SAFETY (RAMS)- PART 1: GENERIC RAMS PROCESS

This standard aim at introducing the application of a systematic RAMS management process in the railway sector and enable the implementation of a consistent approach to the management of reliability, availability, maintainability, and safety (RAMS). This standard provides a mutual understanding and approach to the managements of RAMS and the processes for the specification and demonstration of RAMS requirements.

EN 50126-1 provides a safety management process. This standard can be applied systematically, throughout all Phases of the lifecycle of a railway application fields, namely command, control, and signalling, rolling stock and fixed installations, to develop railways specific RAMS requirements and to achieve compliance with these requirements. EN 50126-1 considers RAMS and the generic aspects of the RAMS life cycle.

EN 50126-1 Life-cycle Phases

EN 50126-1 takes a system level view and establishes a sequence of life cycle Phases each product passes through. However, systems are composed mainly of both hardware and software.

The life cycle approach provides a structure for planning, managing, controlling, and monitoring all aspects of a system, including RAMS, as the system under consideration progress throughout the life cycle Phases. The life cycle model is fundamental to the successful implementation of this standard. This standard represents the life cycle sequentially. It shows the individual Phases and the links between Phases.

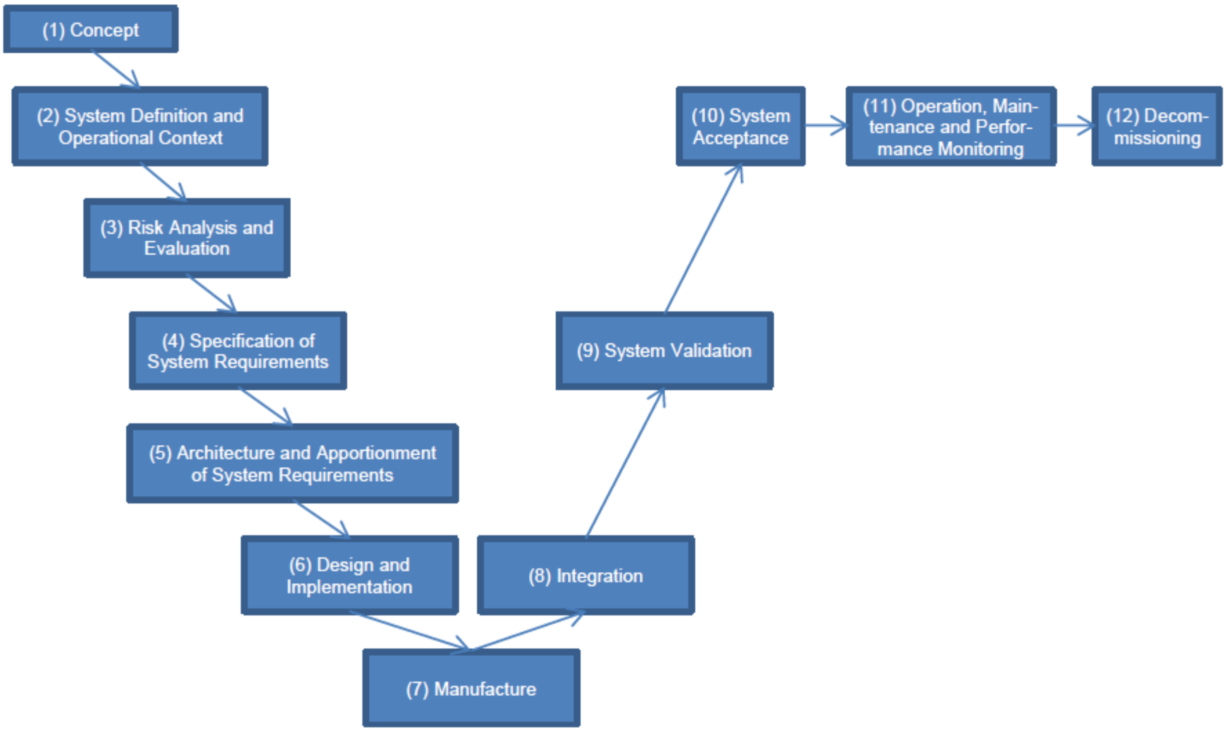

(1) Concept
(2) System Definition and Operational Context
(3) Risk Analysis and Evaluation
(4) Specification of System Requirements
(5) Architecture and Apportionment of System Requirements
(6) Design and Implementation
(7) Manufacture
(8) Integration
(9) System Validation
(10) System Acceptance
(11) Operation, Maintenance and Performance Monitoring
(12) Decommissioning

Figure 1:System life cycle (V-Model)

The general RAMS-Process consists of three blocks:

1. Risk analysis including determination of RAMS requirements
2. Implementation and proof for meeting of requirements
3. Operation, maintenance, and decommissioning of the system

The life cycle Phases are classified below:

- Concept:
  - To develop a sufficient understanding of the system to ensure a proper performance of all RAMS life cycle activities.
- System definition and operational context:
  - This Phase describes the essential characteristics and functions of the system, and clarification of the interfaces to other systems including the input to provided and the output that can be expected.
- Risk analysis and evaluation:
  - Risk analysis is the systematic use of all available information to identify hazards and its RAM equivalent, related potential losses and to evaluate the associated risk. It distinguishes between the hazard or its RAM equivalents that do not need to be analysed further from the hazards or RAM equivalents that need to be further analysed.
- Specification of system requirements:
  - This Phase details the initial system requirements and the ones derived from risk assessment as well as defining criteria for acceptance.
- Architecture and apportionment of system requirements:

  - This Phase apportions the system requirements (including all RAMS requirements) to the designated subsystems and/or components. It designs subsystems and components that work together as a system which fulfils the require functions at the system level. It identifies and evaluate the significance of the interactions between the subsystems.
- Design and implementation:
  - This Phase creates subsystems and components conforming to RAMS and other requirements and demonstrate how subsystems and components conforms to these requirements.
- Manufacture:
  - The manufacturing Phase establish and apply RAMS-centred assurance arrangements and manufacture the subsystems and components.
- Integration:
  - This Phase demonstrate that integrated system and components meet their RAMS requirements and initiate system support arrangements.
- System validation:
  - To confirm that the system under consideration in combination with its safety related application conditions complies with RAMS requirements.
- System acceptance:
  - This Phase checks the compliance of the total combination of the subsystems, components, and safety related application conditions with the RAMS requirements.
- Operation, maintenance, and performance monitoring:
  - This Phase makes sure that the compliance with RAMS requirements is maintained. It supports the system under consideration.

- Decommissioning:
  - This Phase objective is the control of RAMS implication of the system decommissioning and disposal tasks.

EN 50126-1 General issues to be outlined before type approval analysis or analysis of the RAMS

Before any type of approval analysis and RAMS analysis is undertaken, boundaries and functions of the system under consideration shall be established. Therefore, at least the following issues shall be outlined:

a. the system objective (intended purpose) and its mission profile, including:
   - description of the system under consideration, including system functions and elements which are to be included and system functions which are to be excluded in the analysis:
     - long term operating strategy and conditions.
     - long term maintenance strategy and conditions.
     - system lifetime considerations.
     - logistic considerations.

b. the system boundary, including:
   - interfaces and interactions with physical environment (e.g., climatic conditions, mechanical conditions, altitude) and with other systems.
   - interfaces and interactions with other technological systems.
   - interfaces and interactions with humans.
   - interfaces and interactions with other railway duty holders.

In addition to the functional interfaces, the location(s) of the system parts and their interfaces can influence neighboring systems and environment.

c. the scope of operational requirements influencing the system, including:
    - constraints imposed by existing infrastructure.
    - system operating conditions and constraints.
    - system maintenance conditions.
    - logistic support considerations.
    - review of past-experience data for similar systems.
    - Influence on operational and maintenance personnel, passengers and public, or how they are prevented.
    - the description of operating procedures, identification of personnel permitted to conduct these actions and indication of the skills, qualifications and time-resources required, if part of the system operating conditions and constraints.
    - if no human activities have been included in the analysis, the reasons for this should be stated.
    - the different modes of operation (i.e., normal, abnormal/degraded, maintenance mode), states and transitions and their interactions, if they could have an impact on the systems functionality and safety.

d. existing safety measures and assumptions that determine the limits for the risk assessment.

e. identification of the system and related documents, including assumptions made about functions or subsystems that are different from an existing reference version, explicitly stating and justifying the deviations

Technical concepts concerning availability are based on knowledge of:

- Reliability concerning:
    - All possible system failure modes in the specified application and environment.
    - The frequency of occurrence or the likelihood of each failure mode.
    - The consequences of each failure mode.
- Maintainability concerning:
    - Frequency of planned and unplanned maintenance work and time resources needed for it
    - Time resources needed for error search and detection
    - Time resources needed for the recovery of an error-prone system
- Operation and maintainability concerning:
    - All possible operational modes and required maintenance (considering cost issues), over the system life cycle.
    - The human factor issues.
    - Tools, facilities, and procedures for efficient maintenance of the system.

The operation and maintainability can be identified and analyzed using O&SHA. O&SHA refers to operating and support hazard analysis.

According to [7] O&SHA is performed primarily to identify and evaluate the hazards associated with the environment, personnel, procedures, operation, support, and equipment involved throughout the total life cycle of a system/element.

O&SHA is a systematic analysis of the controlling documents (e.g., procedures and tasks) to ensure hazard elimination or control with emphasis on the performance of people and their relationship to hazards within the tasks.

The OSHA focus is on the:

- Operation & Maintenance
- Identification of hazards for operating and maintenance personnel.
- Risk evaluation.
- Events leading to dangerous situations.
- Measures to cover each risk.
- Testing
- Special Tools & Test Equipment

of the system rather than system components.

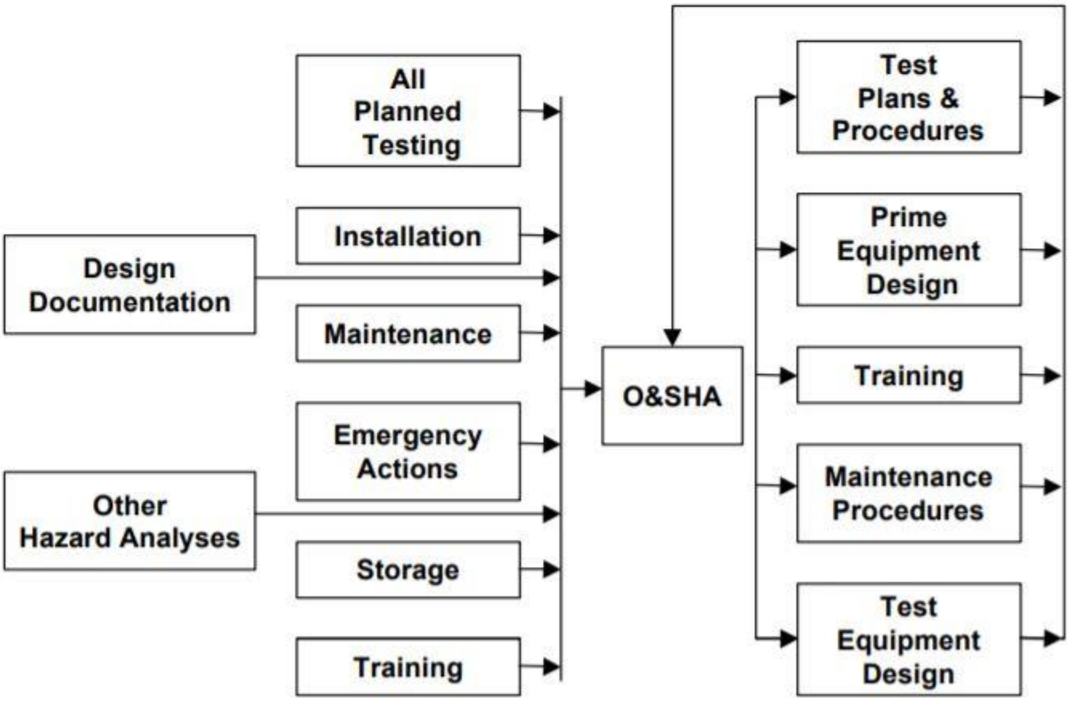


Figure 2:Operating & Support Hazard Analysis (O&SHA) Elements [7]

Technical concepts concerning safety are based on knowledge of:

- All accidents and hazards connected with them, originating from errors in the system or it´s maintenance.
- The characteristics of each safety threat
- Safety-related system failures concerning:
  - Types of system errors which could lead to a hazard.
  - Frequency of occurrence or probability of those errors
  - Sequence and/or simultaneity of events, errors, etc. which could lead to accidents.

  - Frequency of occurrence or probability of decisive events, errors, … in the application
- Maintainability of safety-related parts of the system concerning:
  - Ease of conducting maintenance work on parts of the system which are related with a safety-related error source or a possible hazard.
  - Possible maintenance errors that could occur in the work process mentioned above.
- Operation of the system and for maintenance of safety-related parts concerning:
  - The influence of the human factor on maintenance of the system
  - Tools, facilities, and procedures for safety maintenance of the system and secure operation
  - Efficient control and activities for dealing with hazards and the reduction of their consequences.

Failures in the System

Failures in the system effect reliability, availability, and safety of the system. Magnitude of these effects is determined by the systems functionality and design.

Beside the system properties also the environment of its operation and its operating rules can have an influence.

Parameters for railway

1. Reliability parameters

Parameter	Symbol	Unit/Dimension
Failure rate	$\lambda(t)$	1/time, 1/distance, 1/cycle
Mean up time	MUT	Time (distance, cycle, hours))
Mean operation time to failure (for non-repairable items)	MTTF	Time (distance, cycle, hours))
Mean operating time between failure (for repairable items)	MTBF	Time (distance, cycle, hours))
Failure probability	F(t)	Dimensionless
Reliability (Success probability)	R(t)	Dimensionless

Table 4: Example of reliability parameter

2. Maintainability parameters

Parameter	Symbol	Unit/Dimension
Mean down time	MDT	Time (distance, cycle)
Mean operating time between maintenance	MTBM	Time (distance, cycle)
MTBM (corrective or preventive)	MTBM (c), MTBM (p)	Time (distance, cycle)
Mean time to maintain	MTTM	Time

MTTM (corrective or preventive)	MTTM (c), MTTM (p)	Time
Mean time to restore	MTTR	time
Mean repair time	MRT	Time
Fault coverage	FC	dimensionless
Repair coverage	RC	dimensionless

Table 5:Example of maintainability parameter

3. Availability parameter

Parameter	Symbol	Unit/Dimension
Availability Inherent operational	A Ai Ao	Dimensionless
Fleet	FA	Dimensionless
Schedule Adherence	SA	Dimensionless or time

Table 6: Example of availability parameters

If there is constant failure rate, constant repair rate and no preventive maintenance (MTTR = MDT), the steady-state availability can be expressed by

$$A = \frac{MUT}{MUT + MDT} \leq 1$$

where A is usually in the range of 0 till 1. A has generally a value close to 1. Its complement is called unavailability U.

$$U = 1 - A == \frac{MDT}{MUT + MDT} \geq 0$$

4. Safety parameters

Parameter	Symbol	Dimension
Hazard rate[1]	h(t)	1/time, 1/distance, 1/cycle
Probability of wrong-side failure	paws	Dimensionless
Active time to return to safe state	-	time

Table 4: Example of safety performance parameters

[1] The hazard rate is the probability of occurrence to have a feared event.

2.4.2 Applicable Document [AD-02]: EN 50126-2 -THE SPECIFICATION AND DEMONSTRATION OF RELIABILITY, AVAILABILITY, MAINTAINABILITY, AND SAFETY (RAMS)- PART 2: SYSTEMS APPROACH TO SAFETY

This standard deals with the System Approach to Safety concerns the safety-related generic aspects of the RAMS life cycle and defines tools and procedures which are independent of the actual techniques used in systems and subsystems.

It provides:

- the user understanding on the approach of the safety concept
- procedures for derivation of safety and integrity requirements on the system and its subsystems
- procedures for derivation of safety-integrity levels (SIL) for safety-related electronic functions

Hourglass model gives an overview on the relevant safety-related activities which are necessary to guarantee an acceptable level of safety. The aim of this model is separation of risk analysis (as part of risk assessment) and hazard analysis. These are also the two main parts of the model:

- Risk assessment
    - Includes risk analysis and risk evaluation.
    - Result: Catalogue of safety requirements, which are then part of the system requirements specification
    - It is performed at the railway system level.
    - It explains the high-level system safety requirements

Risk analysis: derived from system definition, includes hazard assessment, impact analysis and choice of risk-acceptance principle (RAP)

- Hazard control
    - Hazard control: Phase of hazard control in the hourglass model to make sure the system satisfies the safety requirements.
    - Developer of the technical system is responsible for hazard control.
    - The important task for this activity is the hazard analysis and it comprises causal analysis, dedicated hazard identification and a common cause analysis.

Safety process: risk assessment and hazard management

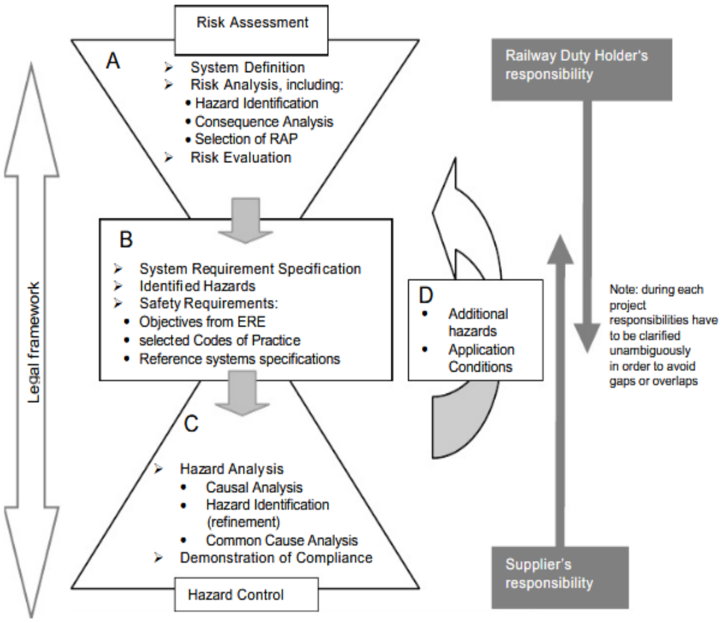

Risk Assessment
A
System Definition
Risk Analysis, including:
• Hazard Identification
• Consequence Analysis
• Selection of RAP
Risk Evaluation
B
System Requirement Specification
Identified Hazards
Safety Requirements:
• Objectives from ERE
• selected Codes of Practice
• Reference systems specifications
C
Hazard Analysis
• Causal Analysis
• Hazard Identification (refinement)
• Common Cause Analysis
Demonstration of Compliance
Hazard Control
D
• Additional hazards
• Application Conditions
Legal framework
Railway Duty Holder's responsibility
Supplier's responsibility
Note: during each project responsibilities have to be clarified unambiguously in order to avoid gaps or overlaps

Figure 3: The hourglass model

Proof/Verification of safety and safety inspection

Needed for:

- System design
- Implementation

Includes:

1. Definition of system
2. QM report
3. Safety management report
4. Technical safety report
5. Relationship to other safety proofs
6. Conclusion

    - Is done prior to system acceptance.
    - independent verification must be conducted according to EN 50126-1:2017.

Safety inspection should include:

- System definition and the operational context
- System requirements and characteristics, including safety requirements.
- Safety verification/proof – to specify safety criteria for simulation and tests linked to bring safety requirement proofs. And results shall be tracked on test reports and where safety criteria success shall be clearly highlight.
- Report of independent safety inspection

Safety-Integrity levels (SIL) Table

The following table of SILs identifies, from the TFFR, the SIL required for a safety-related electronic function. Thus, if the TFFR of a function has been determined by a quantitative method, the required SIL must be determined using the table.

NOTE 1: Similarly, if a qualitative allocation is made by applying explicit risk estimation, it is still required to select the required is still required to select a quantitative TFFR target associated with the SIL level.

NOTE 2: The set of relevant qualitative measures to be applied for each SIL is within the scope of the sector-specific standards.

TFFR (h^{-1})	Allocation of SIL	Qualitative measurement of SIL
$10^{-9} \leq TFFR < 10^{-8}$	4	Defined in the sector-specific standards
$10^{-8} \leq TFFR < 10^{-7}$	3	
$10^{-7} \leq TFFR < 10^{-6}$	2	
$10^{-6} \leq TFFR < 10^{-5}$	1	

Figure 4: Quantitative and Qualitative SIL measures

If the derived TFFR is less demanding (higher) than 10-5 (h^{-1}), the attribute "basic integrity" shall be assigned to the function, with the associated requirements defined below.

If the derived TFFR is more demanding (lower) than 10-9 (h^{-1}), the function should be treated in one of the following ways:

- If it is possible to divide the function into functionally independent functions, the TFFR can be divided between these functions and a SIL allocated to each.
- if the function cannot be divided, at least the measures and methods applicable to SIL 4 must be conducted, and the function must be used in combination with other technical or operational measures to achieve the required TFFR.

Basic integrity requirements

For functions classified with the attribute "basic integrity", the life cycle requirements still apply, namely:

1. In the 'initial stages', the function should be assessed as part of the risk analysis process and the results recorded in the hazardous occurrence register. The appropriate independence requirements apply.
2. At the design phase of the system, failure management measures should be provided (e.g., diagnostics, maintenance, operator training and adequate procedures).
3. In the integration phases:
    - All (non-routine) assumptions made in the process of allocating safety requirements should be recorded as safety-related application conditions (SRAC)
    - the function should be included in the system validation evaluates (including analysis of impacts on other SIL functions)
    - Non-intrusion (the function has no impact on other safety-related functions) must be demonstrated.

- the function must be present during the safety qualification tests.

4. In the operational phase, monitoring to ensure that the basic integrity function remains operational until dismantling (inspection and maintenance verification that the random failure target has been met).

NOTE: Specific requirements for "basic integrity" may also be defined by sector specific standards.

Allocation of SIL

The allocation of SIL must follow the rules defined for the distribution of TFFR. Therefore, for functions that control different hazards, the determination of the TFFR and the allocation of the SILs (according to 10.2.7) can be done independently.

2.4.3 Applicable Document [AD-03]: EN 50128 - RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS-SOFTWARE FOR RAILWAY CONTROL AND PROTECTION SYSTEMS.

EN 50128 specifies the procedures and prerequisites (organization, independency, and competencies, etc.) applicable to the development of programmable electronic systems used in railway control and protection applications.

EN 50128 is used in both safety-related and non-safety related domains. This standard is applied on all safety life cycles of electrical/electronic/programmable electronics systems which are used in safety of the system. For this reason, EN 50128 introduces software safety integrity level SSIL 0, which pertains to no-safety related software application. There are five (5) levels of safety with SIL 4 the most dependable and SIL 0 the least.

- SIL 0: No safety requirements
- SIL 1: Low safety requirements
- SIL 2: Medium safety requirements
- SIL 3: High safety requirements
- SIL 4: Extremely high safety requirements

Software Safety Integrity Level	Description of Software Safety Integrity
4	Very High
3	High
2	Medium
1	Low
0	Non-Safety Related

Table 5: Software safety integrity level: SSIL

Apportionment from accident to SIL/SSIL

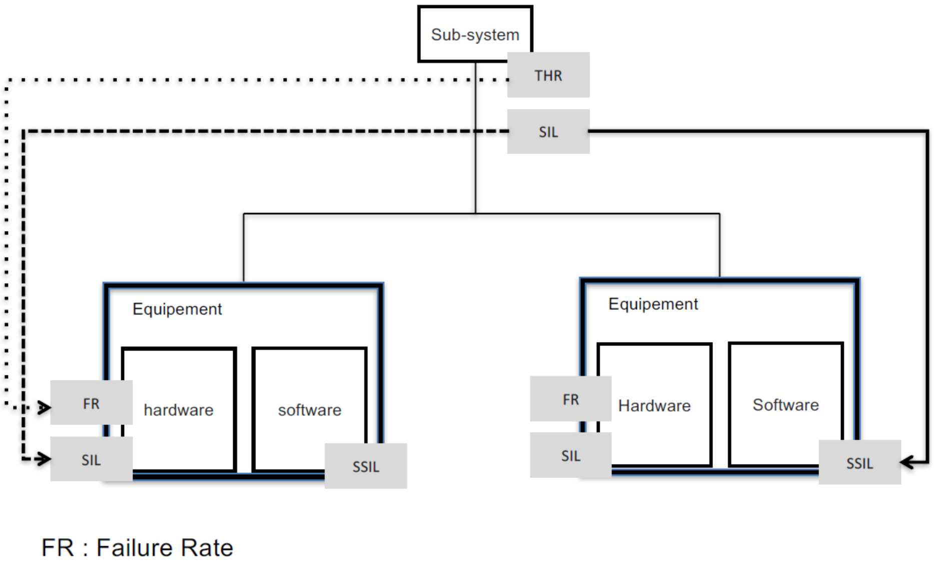


Figure 3: SIL and SSIL

In this standard, the requirements for SIL 3 are the same as for SIL 4, and the requirements for SIL 1 are the same as for SIL 2. There are in practice only three levels:

- SIL 0
- SIL 1 / SIL 2
- SIL 3 / SIL 4

This standard recommends the implementation of the V-lifecycle from the software specification to the overall software testing. It introduces new requirements such as separation between generic software and the setting data, certification of the tools, the need to document and the need to stay abreast of maintenance and the rollout of latest version of the software.

2.4.4 Applicable Document [AD-04]: EN 50129 - RAILWAY APPLICATIONS-COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS-SAFETY RELATED ELECTRONIC SYSTEM FOR SIGNALLING

This standard is intended to apply to all safety-related railway signalling systems/sub-system/equipment. But hazard analysis and risk assessment processes defined in EN 50126, and this standard are necessary for all railway signalling systems/sub-systems/equipment, to identify any safety requirements. This standard applies to generic sub-systems and equipment (both application-independent and those intended for a particular class of application), and to systems/sub-systems/equipment for specific applications.

The standard is primarily applicable to systems, sub-systems and equipment which have been specifically designed and manufactured for railways signalling applications. The standard should be applied to general purpose or industrial equipment, e.g., power supplies, modems, etc.

EN 50129 Safety Integrity

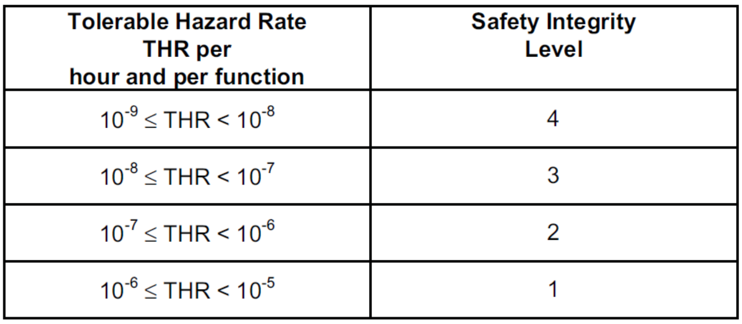
Safety integrity is the ability of a safety-related system to achieve its required safety functions. The higher the safety integrity, the lower the likelihood that it will fail to conduct the required safety functions. Safety integrity comprises two parts

- Systematic failure integrity
    - Systematic failure integrity is the non-quantifiable part of the safety integrity, and it includes the hazardous systematic faults (hardware or software). Systematic faults are caused by human errors in the various stages of the system, sub-system, and equipment.
- Random failure integrity is relating to hazardous random faults mostly random hardware faults.

EN 50129 Safety integrity level

Safety integrity is defined as one of four discrete levels. Level 4 has the highest level of safety integrity; level 1 has the lowest and level 0 is used to show that there are no safety requirements.

Table 7:SIL level



Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level
$10^{-9} \leq \text{THR} < 10^{-8}$	4
$10^{-8} \leq \text{THR} < 10^{-7}$	3
$10^{-7} \leq \text{THR} < 10^{-6}$	2
$10^{-6} \leq \text{THR} < 10^{-5}$	1

2.4.5 Applicable Document [AD-05]: EN 50159-1 COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS-SAFETY-RELATED COMMUNICATION IN TRANSMISSION SYSTEMS

This European standard is applicable to safety-related electronics systems using for digital communication purposes a transmission system. EN 50159-1 gives the basic requirements needed to achieve safety-related communication between safety-related equipment connected to the transmission system and the different category of the transmission system.

This European standard does not specify the transmission system, solution, equipment connected to the transmission system and data that are safety-related or not. The standard does not cover general IT security issues.

Categories for the classification of transmission systems

There are three category of the transmission system and below are the criteria or preconditions that must be meant for a transmission system to be classified into these categories.

Category 1:

A transmission system can be of category 1 if it fulfilled the following criteria below:

Pr1: The number of pieces of connected equipment to the transmission system should be known and fixed. In the system, the configuration should be embedded and fixed in a secured case and if there should be any change to the configuration, it should be preceded by review.

Pr2: The transmission system (e.g., transmission media, etc.) characteristics must be known, fixed, and maintained during the life cycle of the system.

Pr3: The risk of unauthorized access to the transmission system shall be insignificant.

Category 2:

When a transmission system does not meet the preconditions Pr1 or Pr2 as stated above but satisfy Pr3 precondition, it shall be considered as category 2 and an open system.

Category 3:

When a transmission system does not meet the precondition Pr3 as stated above, it shall be considered as category 3 and an open system.

2.4.6 Applicable Document [AD-06]: EN 62061 SAFETY OF MACHINES-FUNCTIONAL SAFETY OF ELECTRICAL, ELECTRONICS AND PROGRAMMABLE MACHINE CONTROLS

This standard defines the requirements for the functional safety of electrical, electronics and programmable machine controls. It also gives recommendations for the design, integration, and validation of safety-related electrical, electronics and programmable electronic control systems (SRECS) for machines.

EN 62061 consider the entire safety chain from the sensor to the actuator. This standard requires the user to follow the series of steps:

1. Assess the risks
2. Allocate the safety measures
3. Design architectures
4. Validate

EN 62061 Risk assessment

This standard has a quantified risk assessment that is taken from EN ISO 14121.

Impact/Consequence	Severity class
Irreversible injury Death, loss of eye or arm	4
Irreversible injury Broken limb, loss of a finger	3
Reversible injury Require further medical attention from doctor	2
Reversible injury Requires first aid on-site	1

Table 8:Severity classification (Se)

Frequency of exposure	Duration class <= 10 min	Duration class > 10 min
≥ 1 hour	5	5
< 1 hour to ≥ 1 day	4	5
< 1 day to ≥ 2 weeks	3	4
< 2 weeks ≥ 1 years	2	3
< 1 year	1	2

Table 9:Frequency and exposure time (F)

Probability of occurrence	Probability class
Often	5
Probably	4
Possible	3
Rare	2
Negligible	1

Table 10:Probability of occurrence of the hazard event (Pr)

Probability of avoiding	Avoiding class
Impossible	5
Possible	3
Probably	1

Table 11:Possibility of avoidance (A)

The sum of the F, P and A parameters determines the class of probability of harm (CI), this value is mapped against the severity score to give a target safety integrity level (SIL).

EN 62061 Safety integrity level – SIL

Safety integrity level (SIL) need to be defined by the functional performance required and as the probability of dangerous failure per hour (PFH_D).

Safety integrity level	Probability of a dangerous failure per hour (PFH_D)
3	≥ 10^{-8} to < 10^{-7}
2	≥ 10^{-7} to < 10^{-6}
1	≥ 10^{-6} to < 10^{-5}

Table 12:Probability of dangerous failure per hour - SIL

2.4.7 Applicable Document [AD-07]: EN 50657 RAILWAY APPLICATIONS – ROLLING STOCK APPLICATIONS – SOFTWARE ON BOARD OF ROLLING STOCK

This standard specifies the process and technical requirements for the development of software for programmable electronics systems for use in rolling stock applications. This standard does not support software that is part of the signalling equipment installed on board trains.

EN 50657 applies to safety related as well as non-safety related software including for example:

- Application programming
- Operating systems
- Support tools
- Firmware

Application programming can be said to high level programming, low level programming and special programming e.g., programming logic controller ladder logic. This standard can also be used on pre-existing software and tools.

This standard is not intended to be used retrospective. It therefore applies primarily to new development and only applies in its entirety to existing systems if these are subject to major modifications.

2.4.8 Applicable Document [AD-17]: EN 45545-2 – RAILWAY APPLICATIONS – FIRE PROTECTION ON RAILWAY VEHICLES – PART: REQUIREMNTS FOR FIRE BEHAVIOR OF MATERIALS AND COMPONENTS

This standard specifies the reaction to fire performance requirements for materials and products used on railway vehicles.

REQUIREMENTS

Essential fire safety objectives

It is important that the design of rolling stock and the products used shall incorporate the aim of limiting fire development should an ignition event occur so that an acceptable level of safety is achieved. There should be a high probability that in the event of a fire, a passengers and staff will be able to escape from the unaided and be able to reach a place of safety.

Hazard levels (HL 1 to HL 3) have been determined using a product of the relation between operation categories and design categories. Hazard level are used in the table below for material fire safety requirement classification.

Operation category	Design category			
	N: Standard vehicles	A: Vehicles forming part of an automatic train having no emergency trained staff on board	D: Double decked vehicle	S: Sleeping and couchette vehicles
1	HL1	HL1	HL1	HL2
2	HL2	HL2	HL2	HL2
3	HL2	HL2	HL2	HL3
4	HL3	HL3	HL3	HL3

Table 13:Hazard level classification

Grouping rules

No requirements apply to products with a combustible mass of < 10 g not in touching contact with another unclassified product. Products shall be considered as grouped if:

- The exposed area of each product is < 2.2 m^2
- The combustible mass of each product is > 10 g or they are in touching contact to another combustible product.

Rule 1

If the total combustible mass of the grouped products is

- < 100 g for inferior grouped products or < 400 g for exterior grouped products

No requirements apply to the products of this group.

Rule 2

If the combustible mass of the grouped products exceeds the limits stated in rule 1, but is

- < 500 g for inferior grouped products or < 2000 g for exterior grouped products

One combustible product of this group must be evaluated according to R24.

Listed products

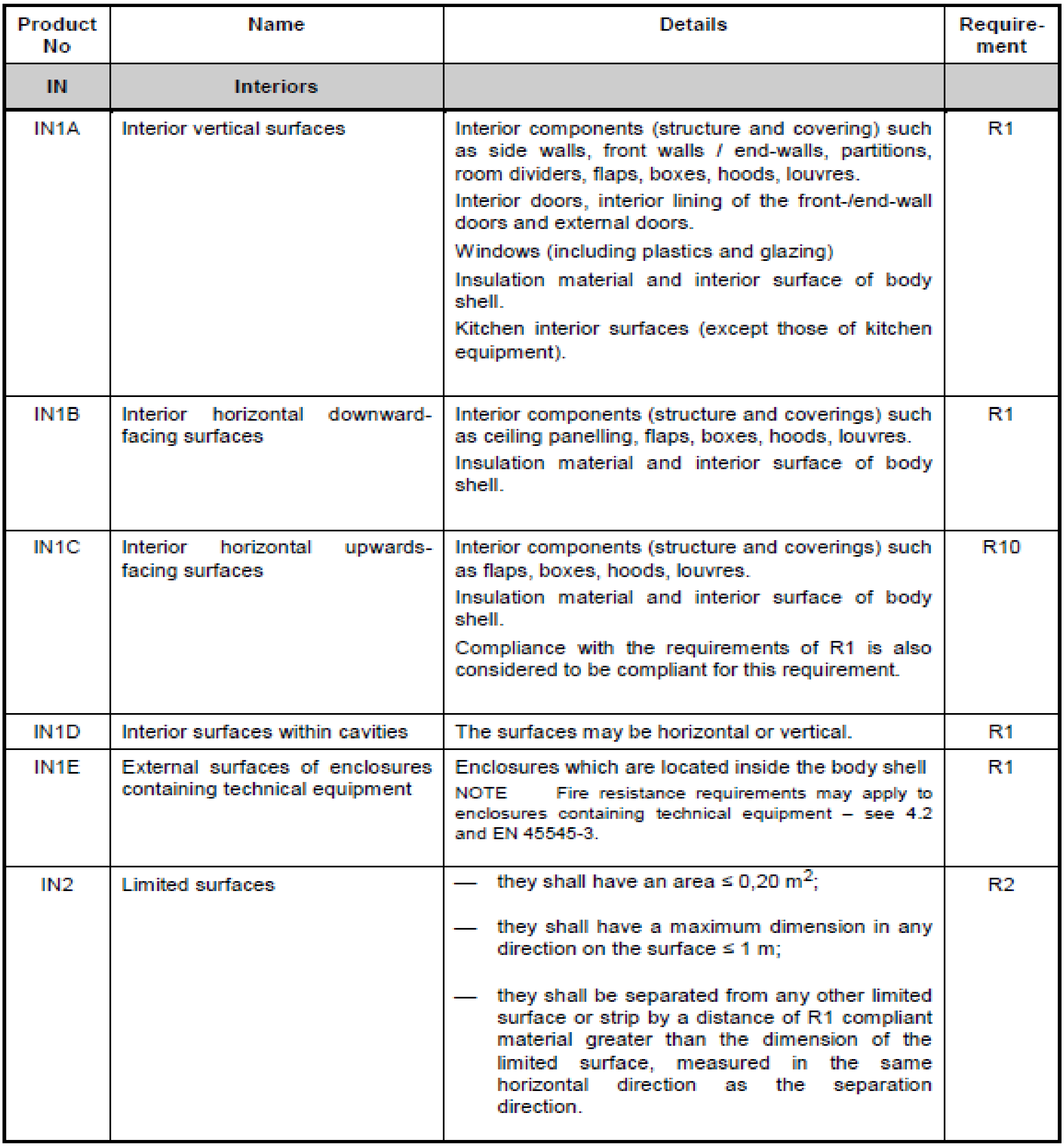
The reaction to fire performance requirements of materials and components depends on their intrinsic nature but also:

- on the location of the materials or components with the design
- on the surface exposed and the relative mass and the thickness of the materials

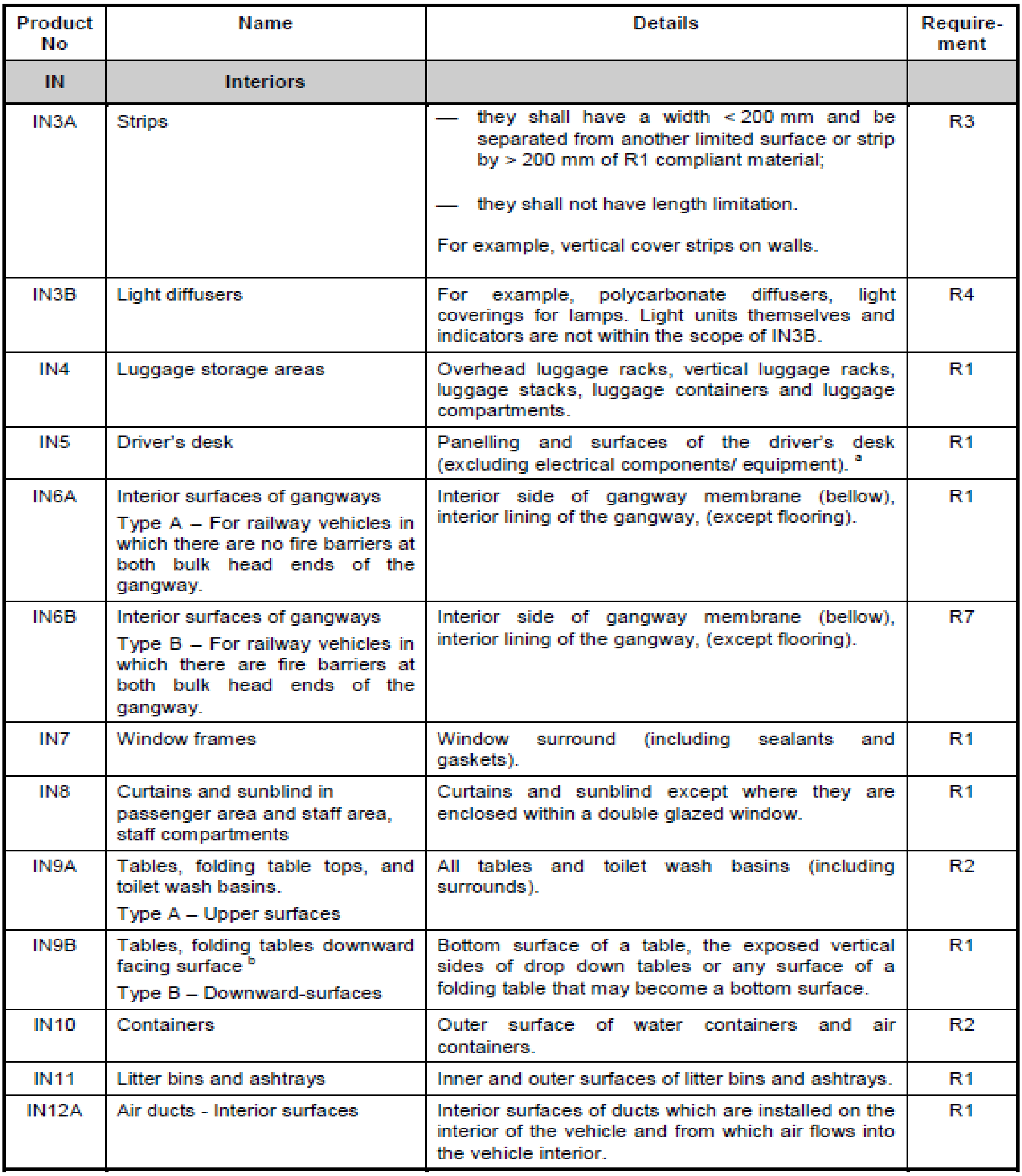
Based on the above, the listed products can be classified and further differentiated into subgroups as follows:

- their general location (exteriors or interiors)
- their specific use (furniture, electrotechnical equipment or mechanical equipment).

Within the sub groupings, for each of the listed products, a set of requirements has been given which defines the ability of the products to contain fire developments to an appropriate degree considering the location, the exposed surfaces, their geometry, and general disposition. The requirement sets for listed products are given in table 2 and are designated R1 to R26.



Product No	Name	Details	Require-ment
IN	**Interiors**		
IN1A	Interior vertical surfaces	Interior components (structure and covering) such as side walls, front walls / end-walls, partitions, room dividers, flaps, boxes, hoods, louvres. Interior doors, interior lining of the front-/end-wall doors and external doors. Windows (including plastics and glazing) Insulation material and interior surface of body shell. Kitchen interior surfaces (except those of kitchen equipment).	R1
IN1B	Interior horizontal downward-facing surfaces	Interior components (structure and coverings) such as ceiling panelling, flaps, boxes, hoods, louvres. Insulation material and interior surface of body shell.	R1
IN1C	Interior horizontal upwards-facing surfaces	Interior components (structure and coverings) such as flaps, boxes, hoods, louvres. Insulation material and interior surface of body shell. Compliance with the requirements of R1 is also considered to be compliant for this requirement.	R10
IN1D	Interior surfaces within cavities	The surfaces may be horizontal or vertical.	R1
IN1E	External surfaces of enclosures containing technical equipment	Enclosures which are located inside the body shell NOTE Fire resistance requirements may apply to enclosures containing technical equipment – see 4.2 and EN 45545-3.	R1
IN2	Limited surfaces	— they shall have an area ≤ 0,20 m^2; — they shall have a maximum dimension in any direction on the surface ≤ 1 m; — they shall be separated from any other limited surface or strip by a distance of R1 compliant material greater than the dimension of the limited surface, measured in the same horizontal direction as the separation direction.	R2



Product No	Name	Details	Require-ment
IN	Interiors		
IN3A	Strips	— they shall have a width < 200 mm and be separated from another limited surface or strip by > 200 mm of R1 compliant material; — they shall not have length limitation. For example, vertical cover strips on walls.	R3
IN3B	Light diffusers	For example, polycarbonate diffusers, light coverings for lamps. Light units themselves and indicators are not within the scope of IN3B.	R4
IN4	Luggage storage areas	Overhead luggage racks, vertical luggage racks, luggage stacks, luggage containers and luggage compartments.	R1
IN5	Driver's desk	Panelling and surfaces of the driver's desk (excluding electrical components/ equipment). [a]	R1
IN6A	Interior surfaces of gangways Type A – For railway vehicles in which there are no fire barriers at both bulk head ends of the gangway.	Interior side of gangway membrane (bellow), interior lining of the gangway, (except flooring).	R1
IN6B	Interior surfaces of gangways Type B – For railway vehicles in which there are fire barriers at both bulk head ends of the gangway.	Interior side of gangway membrane (bellow), interior lining of the gangway, (except flooring).	R7
IN7	Window frames	Window surround (including sealants and gaskets).	R1
IN8	Curtains and sunblind in passenger area and staff area, staff compartments	Curtains and sunblind except where they are enclosed within a double glazed window.	R1
IN9A	Tables, folding table tops, and toilet wash basins. Type A – Upper surfaces	All tables and toilet wash basins (including surrounds).	R2
IN9B	Tables, folding tables downward facing surface [b] Type B – Downward-surfaces	Bottom surface of a table, the exposed vertical sides of drop down tables or any surface of a folding table that may become a bottom surface.	R1
IN10	Containers	Outer surface of water containers and air containers.	R2
IN11	Litter bins and ashtrays	Inner and outer surfaces of litter bins and ashtrays.	R1
IN12A	Air ducts - Interior surfaces	Interior surfaces of ducts which are installed on the interior of the vehicle and from which air flows into the vehicle interior.	R1

Table 14:Requirements of listed products

2.5 Applicable Documents Related to Railway (Non-Safety)

The following chapter contains a briefly summary of available, applicable norms. For the further analysis, the complete norm was considered.

2.5.1 Applicable Document [AD-08]: ISO/TS 22163 – QUALITY MANAGEMENT SYSTEM-BUSINESS MANAGEMENT SYSTEM REQUIREMENTS FOR RAIL ORGANIZATIONS: ISO 9001:2015 AND PARTICULAR REQUIREMENTS FOR APPLICATION IN THE RAIL SECTOR.

The international standard ISO / TS 22163 is an initiative led by the Association of the European Railway Industry (UNIFE). It is based on the quality management standard ISO 9001 and supplements it with rail-specific requirements. ISO/TS 22163 aims to achieve global uniformity in language, assessment guidelines and audits.

ISO/TS 22163 fully adopts the structure of the ISO 9001:2015 quality management standard and has been extended to include requirements specifically for the railway industry. The expanded standard applies to all companies in the rail vehicle industry, including suppliers of infrastructure technology.

2.5.2 Applicable Document [AD-09]: EN 50125-1 RAILWAY APPLICATIONS – ENVIRONMENTAL CONDITIONS FOR EQUIPMENT

EN 50125-1 specifies the environmental conditions encountered within Europe. It covers the use of on board electrical, electromechanical and electronics equipment for rolling stock for the following parameters: Altitude, Temperature, Humidity, air movement, rain, snow and hail, ice, solar radiation, lightning, pollution, vibrations and shocks, electromagnetic interference environment, acoustic noise environment, supply systems characteristics. This standard defines the interface conditions between the vehicle and its environment.

This standard intends to define the interface conditions between the equipment and its environment and parameters to be used by designers when calculating RAMS and lifetime with respects to the environment effects. This standard applies to all signalling and telecommunication systems excepts those use in cranes, mining vehicles and cable cars.

Environmental Conditions:

1. Altitude
   The equipment shall perform as specified for the different classes of altitude range relative to sea level given in the table below.

Classes	Altitude range relative to sea level (m)
A1	Up to 1400
A2	Up to 1000
AX	More than 1400

Table 15:Classes of altitude range

For AX class, the maximum altitude shall be specified by the purchaser. Altitude is relevant, for air pressure level and its consequences on cooling systems.

2. Temperature

The equipment shall operate as specified for the different classes of temperature given in the table below.

Classes	Air temperature external to vehicle (°C)	Inside vehicle compartment temperature (°C)	Inside cubicle temperature (°C)
T1	-25 +40	-25 +50	-25 +70
T2	-40 +35	-40 +45	-40 +65
T3	-25 +45	-25 +55	-25 +70
TX	-40 +50	-40 +60	-40 +75

Table 16:Classes of air temperature

The values in columns (2) and (3) are temperatures that the plant or equipment designer must not exceed in a given part, because too much energy is dissipated with insufficient cooling. They are also the temperatures that the equipment manufacturer must take into account in the design.

A reference temperature of 25 °C is assumed to be the continuous temperature at which the influences on the ageing of the insulating material are the same as those caused by the climatic temperature during the service life temperature during the operating life.

3. Humidity

The external humidity level listed below shall be considered:

- yearly average: ≤ 75% relative humidity
- on 30 days in the year continuously: between 75% and 95% relative humidity
- on the other days occasionally: between 95% and 100% relative humidity
- maximum absolute humidity: 30g/m^3 occurring in tunnels

An operation caused infrequent and slight moisture consideration shall not lead to any malfunction or failure.

4. Wind

The maximum speed of wind shall be taken as 35m/s. Exceptionally higher wind speed, up to maximum 50m/s, may occur. In this case, the equipment or vehicle performance may be affected but no permanent damage may occur.

5. Rain

Rain rate of 6mm/min shall be considered. The effect of rain shall be considered depending on the equipment installation together with wind and vehicle movement.

6. Snow

Consideration shall be given to the effect of snow and all forms of snow which may occur.

7. Pollution

   Pollution effects shall be considered in the design of equipment and components. The severity of pollution will depend upon the location of the equipment. The effect of the following kinds of pollution needs to be considered:

   - Chemically active substances
   - Cleaning products specified by the purchaser.
   - Fire extinguishing means.
   - Biological active substance

8. Solar radiation

   Equipment exposed to the effect of solar radiation shall remain unaffected. For equipment directly exposed to solar radiation, the maximum level shall be considered as 120W/m2, and the maximum duration of the exposure shall be conventionally taken as 8h unless otherwise specified.

9. Large animals on tracks

   There is a possibility of large animal being present on track. Animal's strike are a common occurrence in inter-urban area. So, some mounted equipment is particularly susceptible to damage due to strikes and should be suitable protected.

2.5.3 Applicable Document [AD-10]: EN 50125-3 ENVIRONMENTAL CONDITIONS FOR EQUIPMENT: EQUIPMENT FOR SIGNALLING AND TELECOMMUNICATIONS

EN 50125-3 specifies the environmental conditions encountered within Europe. It covers the design and the use of equipment for signalling and telecommunication systems.

This standard intends to define the interface conditions between the equipment and its environment and parameters to be used by designers when calculating RAMS and lifetime with respects to the environment effects.

This standard applies to all signalling and telecommunication systems excepts those use in cranes, mining vehicles and cable cars. It does not define the specifications for train-borne signalling and telecommunication systems.

This standard relates to the environmental conditions.

Environmental Conditions

It is the current state of the environment. It is the duty of the customer to specify the required class for each environmental parameter in the technical specification. The specified values are maximum, or limit values and they may be reached.

Pressure

- **Altitude**

  Altitude is the distance above sea level. Altitude is related to air pressure. As altitude rise, air pressure drops.

  The table below gives the different classes of altitude relative to sea level at which the equipment shall perform as specified.

Classes	Altitude range relative to sea level
A1	Up to 1400
A2	Up to 1000
AX	More than 1400

Table 17:Altitude relative to sea level

Temperature

Temperature is the degree of hotness or coldness of an object. Temperature is usually measured in degree-Fahrenheit or degree-Celsius and it tells us how much heat an object has.

The table below shows the overall system air temperature parameters

Climatic classes	External ambient	In cubicle a b	In Shelter a b		In building a b	
			N.T.C. c	T.C. d	N.C.C. c	C.C. e
T1	(-25 + 40) °C	(-25 + 70) °C	(-5 + 55) °C	(+15 + 30) °C	(0 + 45) °C	(+18 + 27) °C
T2	(-40 + 35) °C	(-40 + 65) °C	(-20 + 50) °C	(+15 + 30) °C	(-5 + 40) °C	(+25 + 27) °C
TX	(-55 + 40) °C	(-55 + 70) °C	(-35 + 55) °C	(+15 + 30) °C	(-5 + 45) °C	(+18 + 37) °C

a – The temperature inside cubicle, shelter or building are values measured in free air not directly adjacent to heat emitting elements

b – The maximum temperature inside a cubicle, a shelter N.T.C. and a building N.C.C. are higher than max. ambient temperatures because of the effects of solar radiation and power dissipation of installed equipment.

c – The higher value of lowest temperature compared to those for external ambient are due to heat emitting equipment.

d – 3K2 of EN 60721-3-3

e – 3K1 of EN 60721-3-3

C.C.: with climate control N.C.C: without climate control	T.C: with temperature control N.T.C: without temperature control

Table 18:Temperature range at different sites

For the table above, open air temperature was measured 2m above ground.

For installation of equipment’s, the effect of the climatic or temperature control operating outside its specified parameters should be considered.

The yearly average temperature of each type of site (for R.A.M.S. calculation) to be used are the following:

- +40 °C for equipment housing, cubicle
- +30 °C for shelter N.T.C.
- +25 °C for shelter T.C. and building (N.C.C. and C.C.)

Wind

Withstanding of stress is especially important. Equipment exposed to air movement must be designed to withstand stress generated. There are two sources of stress cause by air movement. They are

1. Natural wind

$$F_w = q * c * A$$

Where F_w is the force produced by the natural wind.
q – is the pressure head (N/m^2)
c – is the form factor
A – is the equipment surface perpendicular to the direction of the wind (m^2)

2. Air movement produced in the area of the track by the passing of the train.
The customer shall advise the designer of the value of q to be used to calculate air movement pressure caused by train.

2.5.4 Applicable Document [AD-11]: EN 50155 TYPE APPROVAL TEST ON ELECTRONIC EQUIPMENT FOR RAILWAY APPLICATIONS

This standard applies to all electronic devices for control, regulation, protection, supply etc. installed on rail vehicles and connected to:

- either the battery of the vehicle or
- a low-voltage power supply with or without a direct connection to the mains voltage (transformer, voltage divider, auxiliary power supply)

Electronic equipment for railway applications must adapt to different operational environmental requirements such as temperature, humidity, shock, vibration, and electrical characteristic differences. Such electronic devices must comply with the EN50155 standard set of rigorous tests to ensure that the entire system can function properly in the harsh environment of the railway.

EN 50155 testing applies to all electronic equipment for control, regulation, protection, supply, etc., installed on rail vehicles and associated with either the accumulator battery of the vehicle or a low voltage power supply source with or without a direct connection to the contact system (transformer, potentiometer device, auxiliary supply). The exception is electronic power circuits, which conform to the EN 50207 test.

The EN 50155 test covers the conditions of operation, design, construction, and testing of electronic equipment, as well as basic hardware and software requirements considered necessary for competent, reliable equipment. For the purpose of this standard, electronic equipment is defined as equipment mainly composed of semiconductor devices and recognized associated components. These components will mainly be mounted on printed boards. It is important to note that sensors (current, voltage, speed, etc.) and firing unit printed board assemblies for power electronic devices are covered by this standard. Complete firing units are covered by EN 50207 testing.

EN50155 Type Approval Test and test methods for a typical railway component:

- EN 50155 Test 1 – Visual Inspection
  - The visual inspection must be conducted to ensure that the device work properly and corresponds to the system requirements. After each test, the visual inspection must also be conducted check if any damage or deterioration has occurred.
- EN 50155 Test 2 – Cooling
  - The cooling must not be done by blowing stifling air into the housing of the device. Where fan assisted cooling is used, the facility must be protected so that no damage occurs if the cooling system fails.
- EN 50155 Test 3 – Dry Heat
  - The dry heat test is conducted using natural ventilation, except when forced ventilation is provided for the facility. The temperature value in this test depends on the temperature range that is set by the user and the type of facility to be evaluated is determined. During the dry heat test, every heat emitting device is either switched on or reproduced.
- EN 50155 Test 4 – Radio frequency interference test
  - For this test, the arrangement of the device to be evaluated, including the associated wiring and all connections correspond to the installation conditions. The device under test must be in its housing to which all panel and access covers are attached.
- EN 50155 Test 5 – Insulation test
  - This test is to check that the assembly of components, their metal connections, the housing, and the routing of the wiring are not too tight surrounding metal parts or fastenings. The test consists of the insulation measurement and the dielectric strength test.
- EN 50155 Test 6 – Vibration, Shock and Bump
  - During this test, the complete cabinet or frame must be together with their auxiliary and assembly equipment.
- EN 50155 Test 7 – Water tightness
  - It is not necessary to conduct this test if the device is inside the vehicle or in boxes outside. Except cases that are determined by the user and manufacturer.
- EN 50155 Test 8 – Low Temperature Storage
  - If the device will be exposed to temperature below the lowest operating temperature, a storage testing can be conducted at low temperature.

2.5.5 Applicable Document [AD-12]: EN 50121-3-2 TYPE APPROVAL TEST ON ELECTROMAGNETIC COMPATIBILITY FOR RAILWAY EQUIPMENT.

This standard applies to emission and immunity aspects of electromagnetic compatibility (EMC) for electrical and electronic apparatus which are meant to be used on railway rolling stock. This standard clearly considers the internal environment of the railway stock and the external environment of the railway. It also considers the interference to the apparatus from equipment such as hand-held radio transmitters.

This standard cannot be applied to transient emissions when starting or stopping the apparatus.

The following definitions applies to this standard. They are:

- Rolling stock apparatus – A rolling stock apparatus is a finished product with an intrinsic function intended for implementation into the rolling stock installation.
- Port – Interface of the specific apparatus with the external environment e.g., d.c. power port, a.c. power port.
- Enclosure port – the physical boundary of the apparatus through which electromagnetic field may radiate.

Conditions during Testing

The manufacturer oversees deciding the conditions during testing in a test plan. The test shall be made at a typical operating mode considered by the manufacturer to produce the largest emission or maximum susceptibility to noise as appropriate in the frequency band being investigated consistent with normal applications.

The apparatus shall only be evaluated while connected to the minimum configuration of auxiliary apparatus necessary to exercise the port on the condition that the apparatus is part of a system or connected to auxiliary apparatus.

The test shall be conducted within the specified operating range for the apparatus and at its rated supply voltage.

Applicability

The measurement should be made on the relevant port of this apparatus. Some tests shall not be applicable, and this shall be determined from the consideration of the electrical characteristics, the connection, and the usage of a particular apparatus.

Emission tests and limits

The emission tests and limits for apparatus are given on a port-by-port basis. For disturbance, measurement shall be performed in well-defined and reproducible conditions.

The tables below describe the test, the test methods, and the test set-up.

	Port	Test specifications		Basic standards	Test set-up	Remarks
1.1	High voltage connection, input side before filter (port 3 on figure A.1, A.2, A.3)	Signalling and telecommunication frequencies	See EN 50121-3-1			
		9 kHz … 30 MHz	No limits			See note 1 & 2
NOTE 1: No conducted radio frequency limits are applied. The apparatus when installed with other surrounding equipment shall satisfy the radiated emission limits of EN 50121-3-1 for trains.						

NOTE 2: It is desirable but not possible to apply conducted radio frequency limits. No practical test method exists and the relationship between conducted emissions and radiated emissions is not possible to define.

Table 19:Emission-traction a.c. power ports

<table>
<tr><th></th><th>Port</th><th colspan="2">Test specifications</th><th>Basic standards</th><th>Test set-up</th><th>Remarks</th></tr>
<tr><td>2.1</td><td>High voltage connection, input side before filter (port 3 on figure A.4)</td><td>Signalling and telecommunication frequencies</td><td>See EN 50121-3-1</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td>9 kHz … 30 MHz</td><td>No limits</td><td></td><td></td><td>See note 1 & 2</td></tr>
<tr><td colspan="7">NOTE 1: No conducted radio frequency limits are applied. The apparatus when installed with other surrounding equipment shall satisfy the radiated emission limits of EN ETSI EN 303 446-2 -3-1 for trains.
NOTE 2: At present there is no agreed method or limit for conducted emissions on the traction supply from 9 kHz to 30 MHz Limiting conducted emissions from an apparatus connected to the traction supply prevent excessive radiation emissions from the supply system.</td></tr>
</table>

Table 20:Emission-traction d.c. power ports

Immunity tests and limits

The immunity tests and limits for apparatus are given on a port-by-port basis. The limits shall be applicable to all relevant apparatus to ensure the immunity of the complete vehicle. Tests shall be conducted in a well-defined and reproducible manner. The tests shall be conducted as single tests in sequence.

2.5.6 Applicable Document [AD-13]: IEC 61373 TYPE APPROVAL TEST ON SHOCK AND VIBRATION TESTS FOR RAILWAY ROLLING STOCK EQUIPMENTS.

This standard deals with the requirements for random vibration and shock testing items of pneumatic, electrical, and electronic equipment/components to be fitted on the railway vehicles. The only method to be used for equipment/component approval is random vibration.

The test contained here are specifically aimed at demonstrating the ability of the equipment under test to withstand the type of environmental vibration conditions normally experienced by railway vehicles.

This standard is not intended to cover self-induced vibrations.

Terms and definitions

- Random vibrations – a vibration the instantaneous value of which cannot be precisely predicted for any given instant of time.

- Accelerated spectral density (ASD) – Mean square value of that part of an acceleration signal passed by a narrow-band filter of a central frequency, per unit bandwidth, in the limit as the bandwidth approaches zero and the averaging time approaches infinity.
- Components – pneumatic, electrical, or electronic parts located inside a cubicle.
- Cubicle – whole equipment, including mechanical parts and especially the structure.

Order of testing

A possible order of testing is as follows:

Vertical, transverse, and longitudinal simulated long-life testing by increasing random vibration, followed by vertical, transverse, and longitudinal shock testing, followed by transportation and handling (when identified/agreed) and finally by vertical, transverse, and longitudinal functional random testing.

Method of mounting and orientation of equipment under test

The equipment under test shall be mechanically connected to the test machine by its normal devices of attachment, including any resilient mount, either directly or by utilizing a fixture. Unless otherwise agreed, it is preferred that the equipment shall be evaluated in its normal working orientation with no special precaution taken against the effects of magnetic interference, heat or any other factors upon the operation and performance of the equipment under test.

Fixing point

A fixing point is part of the equipment under test that is in contact with the fixture or vibrating testing surface at a point where the equipment is normally fastened in service.

Check point

A check point shall be as close as possible to a fixing point and in any case shall be rigidly connected to it. If four or less fixing point exist, each one is defined as a check point.

Reference point

The reference point is the single point from which the reference signal is obtained to confirm the test requirements and is taken to represent the motion of the equipment under test. It may be a check point, or a fictitious point created by manual or automatic processing of the signals from the check points.

Measuring point

A measuring point is a specific location on the equipment under test at which data is gathered for the purpose of examining the vibration response characteristics of the equipment.

Functional test

The functional tests shall be specified by the manufacturer and agreed between manufacturer and customer prior to commencement of the tests. They shall be conducted during the vibration.

2.5.7 Applicable Document [AD-14]: EN 50153 TYPE APPROVAL ON PROTECTIVE MEASURES WITH REGARD TO ELECTRICAL HAZARDS FOR RAILWAY APPLICATIONS VEHICLES

This standard specifies several rules to be used in the design and manufacture of electrical equipment and equipment on vehicles to protect people against electric shock to protect.

This standard is applicable to vehicles used in rail transport, electrically powered road vehicles (e.g., trolleybuses), magnetic levitation trains and the electrical equipment installed on these vehicles. But it is not applicable to the following:

- Mine railways in underground mining
- Cableways
- Temporary structures
- Crane systems, transfer platforms and similar transport systems on rails.

Classification of the voltage ranges

- General specifications
  The voltages are according to their nominal values, as shown in the table below are divided into areas. Different installation regulations apply to each of these areas. The power supplies for the various circuits that are installed in rail vehicles are of diverse types, such as:
  - Batteries
  - Transformers
  - Voltage divider
  - Rotating machines
  - Capacitors
  - Special sources

- Connections between circuits
  Circuits operating at different nominal voltages, connected by a power conversion which do not have conductive connections between them, or circuits which only have been connected by a direct connection to the vehicle body (outside the power converters), must be classified individually according to their nominal voltage.
  If circuits are connected to a higher voltage source, e.g., via autotransformers or voltage dividers are connected, all circuits in the group must be treated as if they were supplied with the nominal voltage of this source, unless the requirements of exceptions are met. The common connection on the vehicle body is not considered as a connection.

Area	Nominal voltage U_n	
	AC voltage V	DC voltage V
I	U ≤ 25th	U ≤ 60
II	25 < U ≤ 50	60 < U ≤ 120
III	50 < U ≤ 1,000	120 < U ≤ 1,500
IV	U > 1,000	U > 1,500

Table 21:Voltage range

- Exceptions
  If the voltage conversion from one voltage range to another requires overvoltage detection which leads to a shutdown of the primary or secondary circuit, or other devices which prevent

an impermissible voltage in the secondary circuit, this secondary circuit must be of the highest voltage that causes the overvoltage detection to respond.
Circuits that are not connected to the vehicle body, e.g., ungrounded power supplies, must be classified in such a way as to ensure that the requirements of this standard are met, taking into account the possible potentials in these circuits in normal and fault conditions.

Protective measures against direct touch

Active parts that can cause an electric shock must be protected against direct contact. It must be possible to operate all equipment without losing protection against direct contact. Protection against direct touch must be conducted by at least one of the measures describes below.

- Protection through insulation
- Protection by preventing access
- Protection through application of area 1
- Warning signs

Protection measures at indirect contact

This section defines the procedures to be used to bring vehicles and their components to earth potential via the fixed railroad system.

- Protection connections
    - Equipotential bonding connections
    - Dimensioning of protective connections
    - Sliding contacts

2.5.8 Applicable Document [AD-15]: EN 50343 – RAILWAY APPLICATION – ROLLING STOCK – RULES FOR INSTALLATION OF CABLING

This standard specifies the requirements for the installation of electrical cables on rail vehicles, including within switch cabinets, including magnetic levitation trains. It can also be applied to the installation for the establishment of electrical connections between the equipment including cables, busbars, connections, and plugs/sockets, but does not include optical fibers.

Technical Requirements

General requirement

It is important that lines and installation materials must be type-tested and dimensioned and installed according to their function. Special stresses that are expected from rail vehicles must be considered when dimensioning and installing cables. Another important that must be considered is the material used and the method of laying the cables to avoid deformation.

Cables on railway vehicles can only be used for the transmission, distribution, and collection of electrical energy or for electrical control and monitoring systems. Components of the electrical installation must be selected, protected, used, and maintained to avoid hazards.

Selection of line type and cross – section

General

If or when a cable is selected, at least the following expected operating condition stated below must be considered.

- Tensions
- Amperage
- Overcurrent
- Voltage drops
- Short circuit current
- Current curve and frequency
- Characteristics of the electrical protective device
- Ambient temperature and temperatures due to load current
- Occurrence of rain, snow, steam or accumulation of condensation water, occurrence of corrosive
- Radiation such as sunlight

Selection of the conductor cross-section according to the load current for cables used for power distribution

The requirements allow the selection of conductor cross-sections with continuous maximum current flow depending on the type of installation and the ambient temperature to achieve the intended service life. In the case of newer insulation materials for which there is no long-term experience, it is based on acceptance tests.

- The load current
  The load current I_{Load} in amperes (A), which a cable must carry over extended periods of time during nominal operation, is a based value for the selection of the conductor cross-section. When the circuit that are supplied by the line are in continuous operation or in operation has a long-lasting cyclical course I_{Load} can be calculated using the formula below

$$I_{Load} = \sqrt{\frac{1}{t_1}\int i^2 \; dt}$$

Where t_1 in minutes (min) the time for a typical load cycle during operation.
i in amperes (A) is the instantaneous current

Bundling cables

When several lines are laid together as a bundle, the following requirement listed below must be meant.

- Heat-specific requirements
- EMC requirements
- Dielectric strength classes
- Mechanical aspects such as strength and weight of the bundle.

Use of green and yellow wire colors

For protective conductor used in rail vehicle, the color coding must be green / yellow. If there are already existing green / yellow multi-core cables, they must be used only for grounding or protective conductor.

Repositioning

Single-core and multi-core with nominal conductor cross-sections of up to 16 mm^2 installed in rail vehicles should be long enough at each connection point to enable them to be repositioned at least three times.

Busbars

Busbars must be made or copper or aluminum. To prevent contact resistance value, precaution on contact surfaces must be considered. On the account of dimensioning, the influence of ambient temperature must be considered.

Requirement of cable fastening

Mechanical fastening or locks must be used to secure lines that are not laid in pipes or closed ducts. Also, if the manufacturer does not specify any values for fastening, then the cables should be fastening at a maximum distance as follows:

- Power supply cables, multi-core cables and cable bundles:
  - 300 mm if the lines runs horizontally
  - 500 mm if the lines are vertical, single-core cables for low power.
- Individually
  - 150 mm between the fixings, if the lines are horizontally or vertically, also between a connection point and the first fixture.

For selection of cable fastening material, the following conditions must be followed.

- Cable fastening must be selected that do not damage the cables and their properties.

2.5.9 Applicable Document [AD-16]: IEC 60721 – CLASSIFICATION OF ENVIRONMENTAL CONDITIONS AND THEIR SEVERITIES – STATIONARY USE AT WEATHERPROTECTED LOCATIONS:

This standard classifies groups of environmental parameters and their severities to which products are subjected when installed for stationary use at weather protected locations.

The environmental conditions are limited to those which can directly affect the performance of products and only these environmental conditions are considered. Environmental conditions related to explosive hazards, microclimate within a product, fire extinction and ionizing radiation are excluded. Also, unforeseen incidents are also excluded.

General

A product may be subjected to a range of environmental conditions during its lifetime. These conditions have been separated into classes described in IEC 60721-3-0. The classes given may be used for defining the maximum short-term environmental stresses of a product.

Sometimes, a product may be exposed to several environmental parameters, for example, low air pressure and temperature, temperature, and humidity, as well as vibration and temperature change. So, combination of environmental parameters given may increase the effect on a product. Therefore, combined conditions should be considered when doing design and evaluation of a product. Product should be designed to survive and operate in different environments because they will be affected by the environmental influences in two ways.

- By the effect of short-term extreme environmental conditions which may directly cause malfunction or destroy the product.
- By the effect of the long-term subjection to the non-extreme environmental stresses which may slowly degrade the product and finally cause malfunction or destruction of the product.

Short-term extreme environmental conditions may occur at any time in the product’s life. A product sometimes may be unaffected by an extreme condition when it is new but fail when it is subjected to the same condition after being used for an extended period of time because of ageing.

It is important for the product specification, when referring to a certain class in IEC 60721-3, to define whether the product is required to be capable of operating or only to survive without permanent damage when exposed to the conditions described by the class. The environmental classes shall be used as a basis for the selection of design and test severities with respect to the consequence of failure.

Classification of groups of environmental parameters and their severities

This classification allows for several possible combinations of environmental conditions which bear upon products wherever in use. It represents the real situation in respect of world-wide conditions of use, due to local influence of open-air climate, construction of buildings, mounting, process conditions, etc.

Climate conditions

During the selection of appropriate classes, attention should be paid to the fact that the climatic conditions inside building may depend on the outside (open-air) conditions, especially air temperature and solar radiation, and the type of building construction. Walls with good thermal insulation or high thermal capacity can consistently smooth the peaks of the outside air temperature variation between day and night or those produce over a longer period. The effect of solar radiation can be increased by either heat-trap or greenhouse effects.

Chemical active substances

The contamination of the natural atmosphere is mainly caused by chemical emissions from industrial activities, motor-driven vehicles, and heating systems. Furthermore, chemical influence is also caused by aerosols of sea and road salts. Contamination may affect the function and materials of products.

Mechanical conditions

Mechanical conditions relate to the levels of vibration and shock that may exists at the location, for example because of normal operations, nearby vehicular movement.

2.5.10 Applicable Document [AD-18]: EN 61375-2 – RAILWAY APPLICATION – ELECTRIC RAILWAY EQUIPMENT – TRAIN BUS – TRAIN COMMUNICATION NETWORK CONFORMANCE TESTING

This standard can be applied to all equipment and devices implemented according to IEC 61375-1. It covers the procedures to be applied to such equipment and devices when the conformance should be proven.

Conformance requirements

The conformance requirements can be:

a. Mandatory requirements – these are to be observed in all cases
b. Condition requirements – these are to be observed if the conditions, set out in the clause apply
c. Options – these can be selected to suit the implementation, provided that any requirements applicable to the option are observed.

Static conformance requirements

Static conformance requirements and options in TCN parts can be of two varieties:

a. Those which determine the capabilities to be included in the implementation if the particular protocol
b. Those which determine multi-layer dependencies. E.g., those which place constraints on the capabilities of the underlying layers of the systems in which the protocol implementing resides.

Dynamic conformance requirements

They are those requirements and options which determine what observable behavior is permitted by the relevant TCN part in instances of communication. A system exhibits dynamic conformance in an instance of communication if its behavior is a member of the set of all behaviors permitted by the relevant TCN protocols part in a way which is consistent with the PICS.

2.5.11 Applicable Document [AD-19]: IEC 62443-1-1 Industrial communication networks - Network and system security -

This standard provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in IEC 62443-1-1 including defining the requirements for control capability security level, SL-C (control system). The seven foundational requirements are:

- Identification and authentication control (IAC).
- Use control (UC)
- System integrity (SI)
- Data confidentiality (DC)

- Restricted data flow (RDF)
- Timely response to events (TRE) and
- Resource availability (RA).

The seven FRs are then expanded into a series of SRs. Each SR has a baseline requirement and zero or more requirement enhancement (REs) to strengthen security. The baseline requirements are then mapped to the control system capability security level, SL-C (FR, control system) 1 to 4.

The seven FRs have a defined set of four SLs. The control system capability level 0 for a particular FR is defined as no requirements. The associated four SLs are defined as.

- SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
- SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills, and low motivation.
- SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

2.6 Other Applicable References and Papers

2.6.1 Applicable Document [AD-20]: ISO 26262 (1 – 10) SERIES – Road vehicle – Functional safety

To reduce the risk of hazards that are caused by a malfunctioning behavior of electrical /programable safety critical system 26262 addresses the safety-related aspects of the development activities and work products.

Part of these requirements cover the project management activities of all safety lifecycle phase and consist of project-independent requirements, project-dependent requirements to be followed during development, and requirements that apply after release for production.

Conforming to the requirements for RAMS w.r.t ISO 26262

During the development phase:

- Measures: include confirmation reviews, functional safety audits and functional safety assessments.
- Reviews: intended to check the compliance of the associated work products
    - to review the technical correctness of the associated work products, regarding functional safety.

Hazard analysis and risk assessment for RAMS w.r.t ISO 26262

The ISO 26262-3, identifies and categorize the hazards of the item and formulate the safety goals related to the prevention or mitigation of these hazards, in order to avoid unreasonable risk.

Hazard analysis, risk assessment and ASIL determination are concerned with determining safety goals for the item (device) such that an unreasonable risk is avoided. For this, the item is evaluated about its functional safety.

Hazard analysis and risk assessment is concerned with setting requirements for the item, such that unreasonable risk is avoided.

- determination of safety goals and their respective ASIL shall be conducted in accordance with the requirements
- The item without a safety mechanism shall be evaluated during the hazard analysis and risk assessment

Hazard Identification & Situational Analysis

The operational situation addresses the limits within which the item is expected to behave in a safe manner.

- A list of operational situations to be evaluated shall be prepared.
- The hazards of the item shall be determined systematically.
- Hazards shall be defined in terms of the conditions or events that can be observed at the vehicle (e.g., sensor failures).
- The consequences of hazardous events shall be identified for relevant operational situations and operating modes.

If hazards are identified during hazard identification, which are outside of the scope of ISO 26262, then the need for appropriate measures shall be indicated

Hazard classification

All hazards identified shall be classified, except for those that are outside the scope of ISO 26262.

Estimation of potential severity

The severity of potential harm shall be estimated for each hazardous event. The severity shall be assigned to one of the severity classes S0, S1, S2 or S3. If a hazard is assigned to severity class S0, no ASIL assignment is required.

Estimation of the probability of exposure in the operational situations

The probability of exposure of each operational situation shall be estimated. The probability of exposure shall be assigned to one of the probability classes E0, E1, E2, E3 and E4. If a hazard is assigned to exposure class E0, no ASIL assignment is required.

Estimation of controllability

The controllability of each hazardous event, by the driver or other traffic participants, shall be estimated. The controllability shall be assigned to one of the controllability classes C0, C1, C2 and C3. If a hazard is assigned to the controllability class C0, no ASIL assignment is required.

System Approach to Safety: assessment for RAMS w.r.t ISO 26262

Safety plan

- implementation of strategies, activities, and procedures for achieving functional safety

- the development interface agreement

- the supporting processes

- the hazard analysis and risk assessment

- the development, and implementation, of the safety requirements

- the analysis of dependent failures, and the safety analyses

- the verification and validation activities

Safety case

- The safety case shall be sufficiently complete to evaluate the achievement of functional safety of the item.

Initiation of Safety Life Cycle

Objective:

- To make the distinction between a new development and a modification to a previously existing item.
- To define the safety lifecycle activities

Modifications

- In the case of a modification the second objective is to define the safety lifecycle activities. An analysis shall be conducted to identify the intended modification applied to the item and its environment and to assess the impact of these modifications
- Include

  - Design modifications [requirements modifications, functional or performance enhancement or cost optimization.]
  - Implementation modifications [result from software fault corrections, or the use of new development or production tools, Implementation features]
  - Modifications to configuration data or calibration data are considered as modifications to the item if they impact the behavior of the item.
  - Changes to the environment of the item can result from the installation of the item in a new target environment.

- In the case of modifications to the item, the modifications shall be described, and the areas affected by the modifications to the item shall be identified. The implication of the modification on functional safety shall be described.
- In the case of changes to the environment of the item, the changes to the environment shall be described.
- The affected work products that need to be updated shall be identified.
- The results of the impact analysis shall be recorded.

Safety goals

- Safety goals and their assigned Automotive Safety Integrity Level (ASIL) are determined by a systematic evaluation of hazardous situations. It is based on the item’s functional behavior; therefore, the detailed design of the item does not necessarily need to be known.
- A safety goal shall be determined for each hazardous event evaluated in the hazard analysis
- The ASIL determined for the hazardous event shall be assigned to the corresponding safety goal
- If similar safety goals are combined into one, the highest ASIL shall be assigned to the combined safety goal.

Verification & Review of HARA & Safety goals

- The HARA and the safety goals shall be reviewed with regard to situations and hazards, compliance with the item (device) definition, and consistency with related hazard analyses and risk assessments
- This verification review checks the hazard analysis and risk assessment of the item for correctness and completeness, that is, considered situations, hazards, and parameter estimations (severity, probability of exposure and controllability).

Functional safety concept

Objective:

- To derive the functional safety requirements, from the safety goals, and to allocate them to the preliminary architectural elements of the item or to external risk reduction measures in order to ensure the required functional safety

Functional Safety requirements

The functional safety requirements shall be derived from the safety goals and safe states, considering the preliminary architectural assumptions, functional concept, operating modes, and system states. To comply with the safety goals, the functional safety concept specifies the basic safety mechanisms and safety measures in the form of functional safety requirements.

1. Fault detection and failure mitigation
   - Fault detection and driver warning to reduce the risk exposure time to an acceptable interval (repair request, stop request)
2. Transitioning to a safe state

- The transitions to and from a safe state and the conditions for transitioning (conditions to switch to the safe state and recovery conditions from the safe state) are described in terms of technical functions.
- If a safe state cannot be reached by immediately switching off, an emergency operation shall be specified.

3. Fault tolerance mechanisms

- where a fault does not lead directly to the violation of the safety goals, and which maintains the system in a safe state (with or without degradation)

4. Arbitration logic to select the most appropriate control request from multiple requests generated simultaneously by distinct functions.

2.6.2 Applicable Document [AD-21]: ANNEX VI OF THE DELEGATED REGULATION (DR) 2017/79

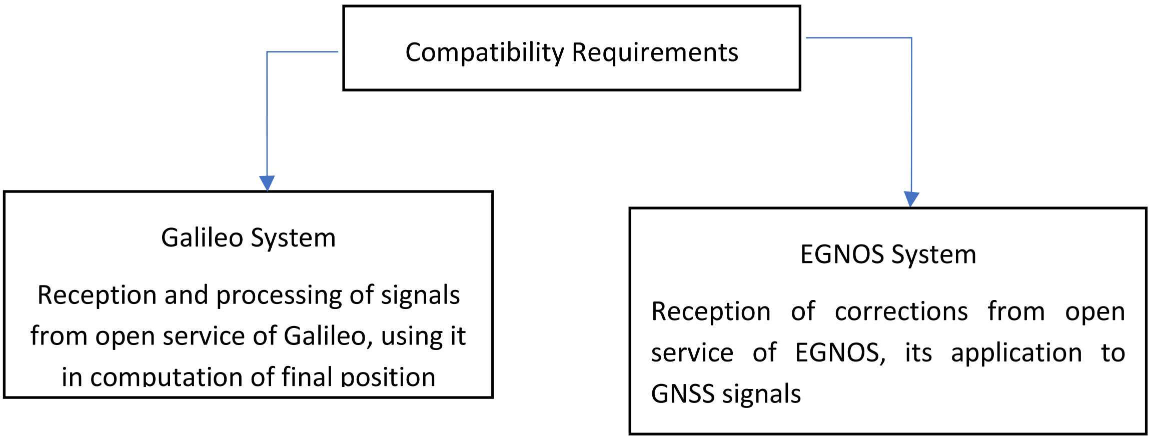
This standard mainly defines for the type of approval of eCall in M1/N1 vehicles with title Technical Requirements for compatibility of eCall-IVS with positioning services by the Galileo and EGNOS systems. As there are no regulations for the GNSS requirements in railway vehicles, this regulation can be a reference to identify validation methods for a later certification with the background of a safe localization under consideration of applicable standards

For GNSS requirements the relevant part is specified in annex VI of the Delegated Regulation (DR) 2017/79 is as follows:

- Compatibility Requirements
- Performance Requirements
- Test Conditions
- Test Procedures

Requirements

1. Compatibility of eCall IVS with the positioning services by Galileo & EGNOS with respect to positioning capabilities



Compatibility Requirements

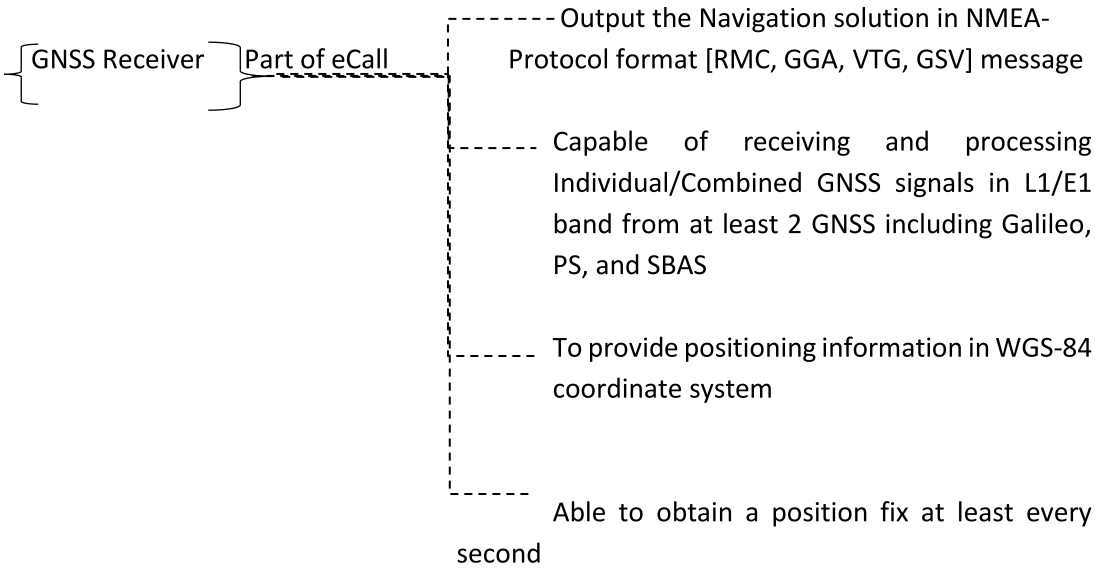
Galileo System

Reception and processing of signals from open service of Galileo, using it in computation of final position

EGNOS System

Reception of corrections from open service of EGNOS, its application to GNSS signals

Performance Requirements:



GNSS Receiver

Part of eCall

Output the Navigation solution in NMEA-Protocol format [RMC, GGA, VTG, GSV] message

Capable of receiving and processing Individual/Combined GNSS signals in L1/E1 band from at least 2 GNSS including Galileo, PS, and SBAS

To provide positioning information in WGS-84 coordinate system

Able to obtain a position fix at least every second

Test Procedures:

The Following are the test cases:

- NMEA-0183 Message's output Test
    - ○ Providing NMEA data minimum defined output rate
- Assessment of positioning accuracy in autonomous Static mode
    - ○ Static accuracy in open environment in combined and single constellation setup
- Assessment of positioning accuracy in autonomous Dynamic mode
    - ○ Dynamic accuracy in open environment with combined constellation setup
  - Movement in shadow areas of intermittent reception of navigation signals & urban canyons
    - ○ Dynamic accuracy in urban environment with combined constellation setup
- Cold start time to first fix test
    - ○ Time to first fix with two different signal levels
- Test of re-acquisition time of tracking signals after blocking out of 60 seconds.
    - ○ Reacquisition time
- Test of GNSS receiver sensitivity in cold start mode, tracking mode and reacquisition scenario
    - ○ Sensitivity testing (time to first fix, position holding, reacquisition) on low signal level

2.6.3 Applicable Document [AD-22]: CEN/EN16803 "USE OF GNSS-BASED POSITIONING FOR ROAD INTELLIGENT TRANSPORT SYSTEMS (ITS) SERIES

This standard mainly addressed the position performances, the relation between position quantities performances and End to End (E2E) performances, but only for road ITS applications. In particular, the GNSS-Based Position Terminals (GBPT) standardization activities. As there are no regulations for the GNSS requirements in railway vehicles, this regulation can be a reference to identify validation methods for a later certification with the background of a safe localization under consideration of applicable standards.

The CEN/EN16803-1 proposes to assess the end-to-end performances concerning road ITS applications. The physical architecture, process chain flow and the computed physical variables associated to the GBPT are depicted in Figure 4.

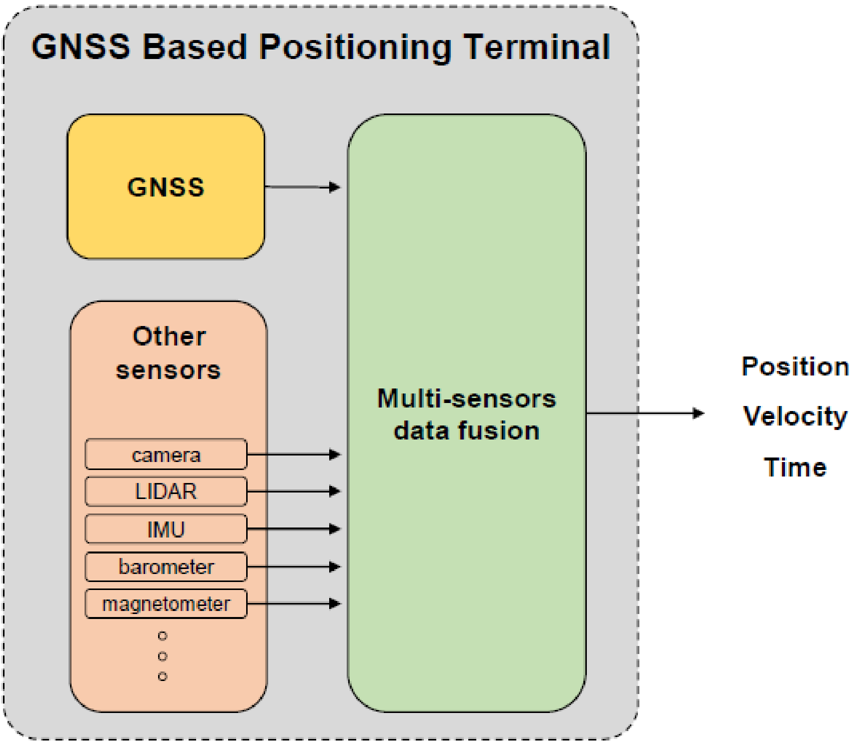


Figure 4: GNSS-Based Position Terminals. Source EN16803-1.

CEN/EN 16803-1 provides identification and definitions of positioning performance features and metrics that characterize the GNSS-Based Positioning Terminals (GBPT) performance requirements. These shall match a certain operational scenario, i.e., the conditions in which the GBPT is operating. These conditions may have an enormous impact on the GBPT performances. The adopted approach by CEN was to assess several metrics by conducting field test campaigns or by employing the Record and Replay (R&R) methodology.

The CEN/EN16803-1 has identified four performance metrics, namely,

- the accuracy associated to the position error, the velocity error, or the speed error
- the integrity determined by the protection level given an associated integrity risk
- the availability which refers to the percentage of time during which the SUT provides output data
- the timing performances, associated to the timestamp resolution, the output latency and time to first

The CEN/EN 16803-1 standard provides a generic procedure composed of a set of conditions to perform the testing (test requirements) and a test design specification. Pre-conditions defined to execute the test are:

- A system capable of providing a reference trajectory (ground-truth) the so-called reference trajectory measurement system (RTMeS)
- A GNSS receiver equipped with an antenna
- A data acquisition software capable of recording the outputs of both the RTMeS and the GNSS receiver under test
- A data processing software suitable to process the GNSS data and perform computations of the errors

The test design specification is composed of the following elements:

- Definition of the vehicle trajectory, i.e., the trajectory location, definition of the environment that best represents the environmental conditions upon which the system shall be evaluated. Equipment installation architecture procedure, i.e., antenna locations specifications (distance between antennas, height from the ground), equipment set-up and initialisation.
- Test time duration and output data rate, i.e., the journey time given a specified speed and output data rate of the two system (reference and GNSS systems).
- Repetitions of the tests using the same trajectory but at various times and with different time durations to be representative for the different satellite constellation geometries and environmental conditions, like ionosphere, troposphere, and multipath effects.
- Computation of the pseudo-range errors after processing the true ranges.
- Specification of which metrics to be used describing the errors, e.g., the 50th, 80th or the 95th percentiles representing the cumulative distribution function of the pseudo-range errors. The CEN EN 16803-1 standard proposes to use these metrics to define performance classes.

CEN/EN 16803 Part I defines six sky scenarios or environments. These are:

- “Flat Rural,” or “clear sky”: rural roads in a flat countryside with masking angles smaller than 10°, no mountains nor high hills,
- “Tree-lined Rural”: rural roads, with lines of trees with foliage on each side and a significant effect on signal reception due to the foliage,
- “Mountainous”: roads with sharp curves and high mountains around, on one side of a valley, with numerous tunnels and sometimes trees, masking angles between 10° and 80°,
- “European Peri-urban”: suburb or medium cities ring roads, with large streets and small to medium height buildings, masking angles up to 30°,
- “European Urban”: standard European “old” big cities with narrow streets, but sometimes large avenues or ring roads, with buildings from medium height to tall, masking angles up to 60° generating frequent multipath and Non-Line-Of-Sight (NLOS) phenomena,
- − “Modern Urban Canyon”: business centres with extremely high modern skyscrapers, large avenue, tunnel, masking angles often greater than 60° generating frequent NLOS phenomena.

The CEN/EN 16803-2 proposes a test methodology based on replay techniques in the laboratory of real data sets recorded during field test campaigns under the assumption that no security attack occurred during the test.

From the standardization point of view, since the record phase needs recognized skills and experience in GNSS metrology, this means that the work has to be performed by GNSS-specialized laboratories, i.e., ISO 17025 homologated and accredited for that purpose by an accreditation authority. The laboratories shall follow standardized procedures for recording the data sets that shall become themselves standardized scenarios to be replayed by a larger panel of homologated, but not GNSS-specialized, radio frequency (RF) test laboratories. This process is depicted in Figure 5.

The CEN/EN 16803-2 standard provides an informative section on how to proceed to record a scenario in standardized operational scenarios. The precise definition of operational scenarios is an issue that will be addressed by the CEN/EN 16803-4.

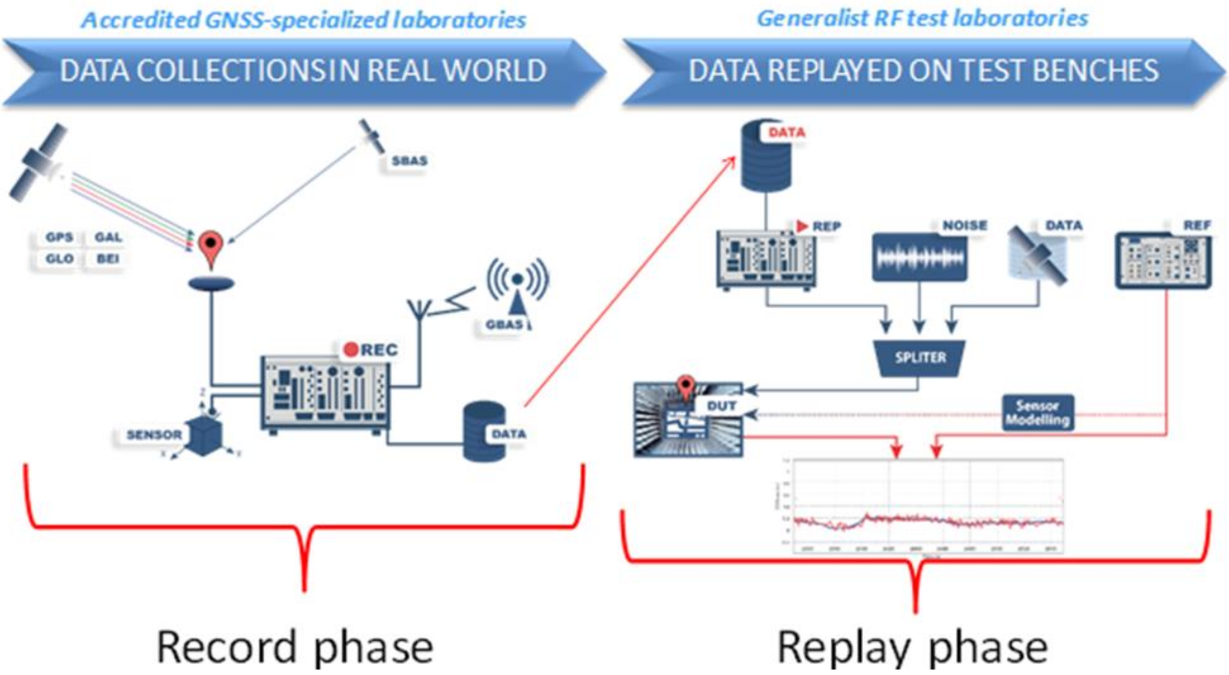

Accredited GNSS-specialized laboratories
DATA COLLECTIONSIN REAL WORLD
Generalist RF test laboratories
DATA REPLAYED ON TEST BENCHES
SBAS
GPS
GAL
GLO
BEI
GBAS
REC
SENSOR
DATA
DATA
REP
NOISE
DATA
REF
SPLITER
DUT
Sensor Modelling
Record phase
Replay phase

Figure 5:The principle of record and replay of GNSS RF signals. Source EN 16803-2

The CEN/EN 16803-3 proposes a complement to this test methodology to assess the performance degradation when the GNSS signal-in-space (SIS) is affected by intentionally radiofrequency (RF) perturbations such as jamming, spoofing or meaconing. This part of the standard is targeting mainly the generalist RF test laboratory in charge of assessing the performances of GBPTs for different applications. Figure 3 provides systematic scheme on how to classify the RF perturbation motivation and type.

The CEN/EN 16803-4, still in development, intends to propose a methodology for the recording of the real data sets and is targeting, mainly, the GNSS-specialized test laboratories that will be in charge of elaborating the test scenarios.

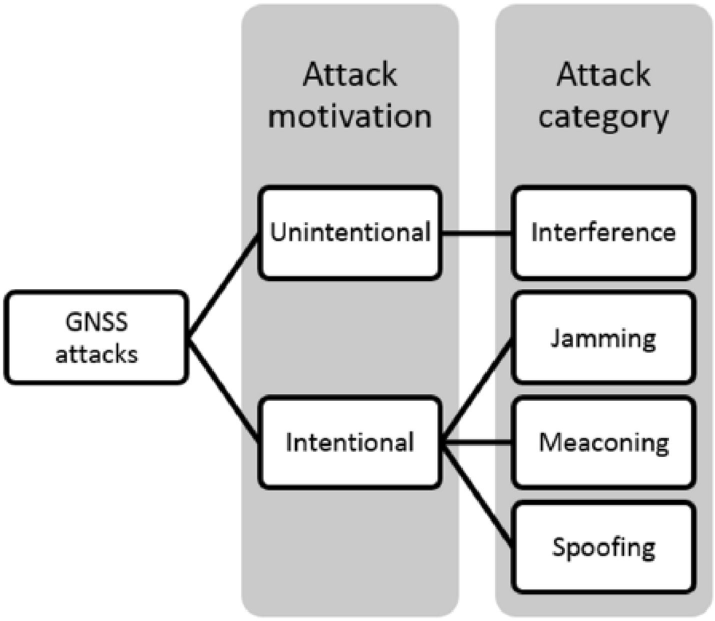


Figure 6: Systematisation scheme of the RF perturbations motivation and type (GNSS attacks taxonomy). Source EN16803-3.

2.6.4 Applicable Document [AD-23]: ETSI TS 103 246-1 ACTIVITIES FOR THE GNSS-BASED LOCATION SYSTEMS (GBLS)

The ETSI 103 246:2017 standard has been conceived with the purpose of testing GNSS system subjected to radio-frequency interferences. ETSI 103 246-5 part addresses the robustness of the GBLS to jamming interference. In the standard two infrastructures are proposed to conduct the testing. The general architecture of the position module is depicted in Figure 7. As there are no regulations for the GNSS requirements in railway vehicles, this regulation can be a reference to identify validation methods for a later certification with the background of a safe localization under consideration of applicable standards.

One infrastructure for system testing is based on performing the RF interference tests of the SUT in an anechoic chamber. Another infrastructure for system testing is based on performing the RF interference tests by connecting the SUT to the RF interference system via a wire. These infrastructures set ups are shown below in Figure 7.

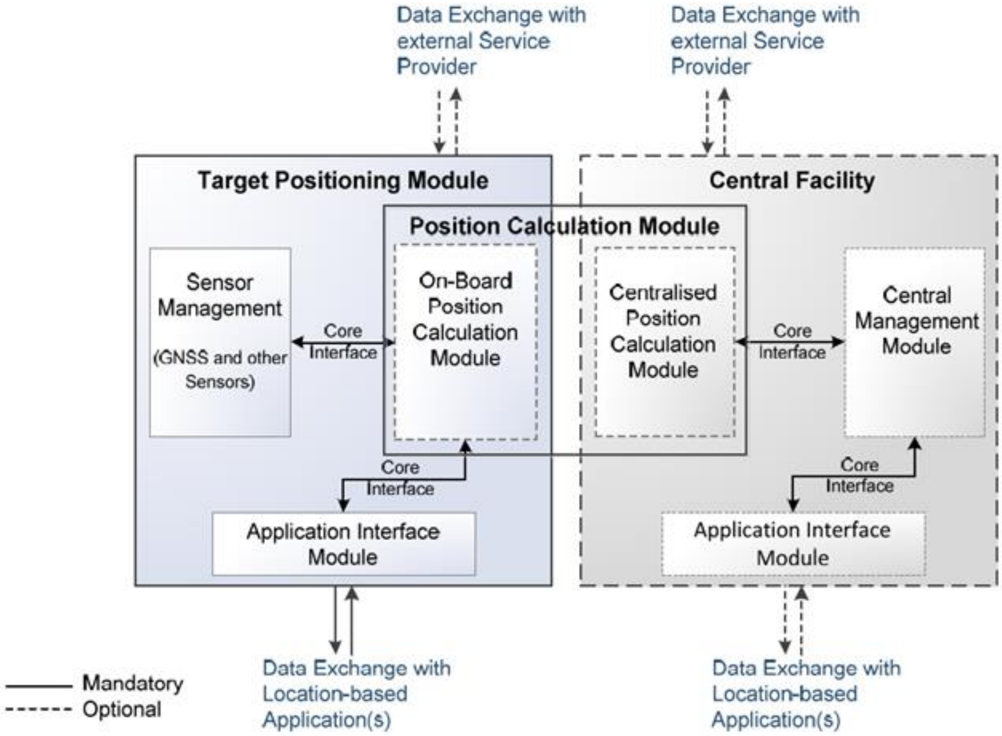

Data Exchange with external Service Provider
Data Exchange with external Service Provider
Target Positioning Module
Central Facility
Position Calculation Module
Sensor Management
(GNSS and other Sensors)
Core Interface
On-Board Position Calculation Module
Centralised Position Calculation Module
Core Interface
Central Management Module
Core Interface
Core Interface
Application Interface Module
Application Interface Module
Mandatory
Optional
Data Exchange with Location-based Application(s)
Data Exchange with Location-based Application(s)

Figure 7:GNSS based location system architecture. Source ETSI 103 246-2.

The ETSI TS 103 246-1 standard provides functional requirements divided in mandatory and optional requirements. The mandatory requirements are associated to positioning techniques, location related data delivery and the associated location system policies. The GBLS shall provide location data in a coordinate reference system and a time stamp in a reference time scale with respect to the positioning techniques. For the location related data delivery, the GBLS shall provide an external interface to convey information for monitoring and control of the data. For the location system policies, the GBLS shall implement a privacy protection policy, a service authentication policy, and a security policy. The requirements for optional features are associated to positioning techniques, location related data content and location related data delivery.

It means that The GBLS may use multiple sensors to complement GNSS and augmented methods such as assisted or differential GNSS positioning methods with respect to the positioning techniques. For the case of location related data delivery, it means that the GBLS may provide location target speed, acceleration, heading angular and angular acceleration. In terms of integrity the GBLS may also provide accuracy, protection level and authenticity flag.

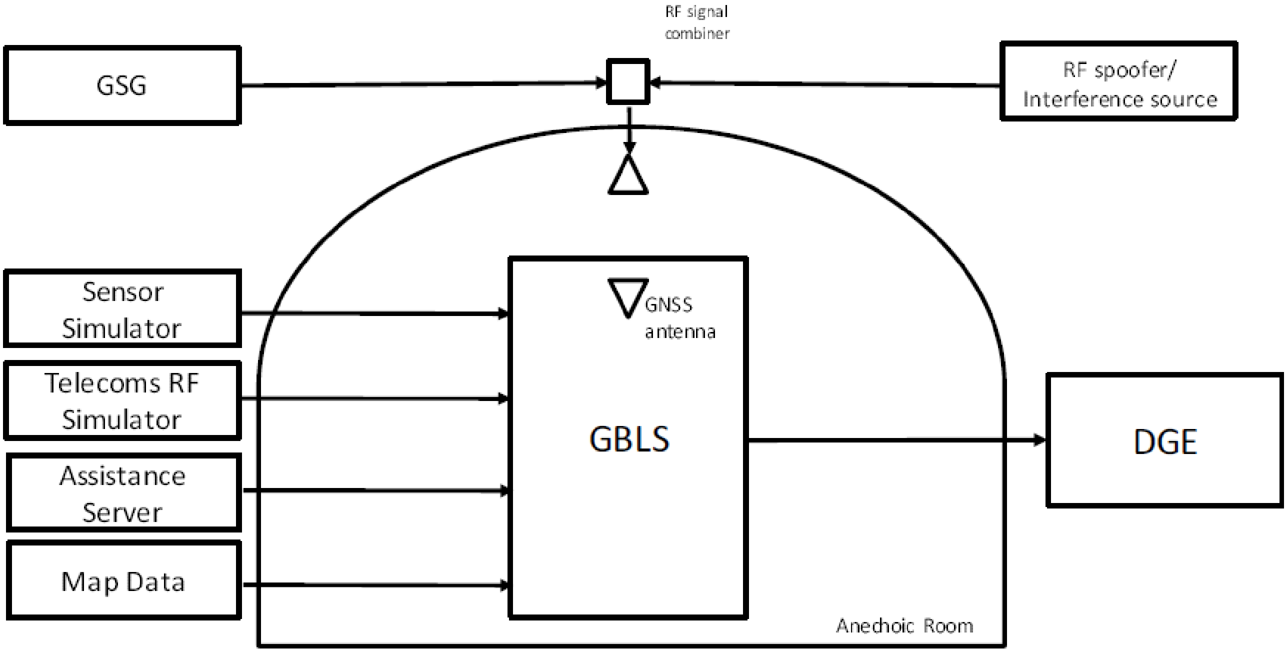


Figure 8: ETSI 103 246-5 systems set up for testing RF interference. Source ETSI 103 246-5.

The ETSI TS 103 246-2 addresses the functional architecture of the GBLS. The standard defines the system in terms of discrete functional elements connected to other internal or external functional elements via logical interfaces. The standard identifies three main components associated to the GBLS mainly, the sensor management module, the position calculation module, and the central management module. Extrinsic to the GBLS there are components providing positioning information (GNSS or other external positioning systems).

The standard adopts a top-down approach in describing the architecture starting at architecture level 1. The architecture levels 2 and 3 describe the several physical components, from level 1, with an increasing level of detail or granularity. In level 1 the overall architecture of the GBLS is defined as shown in Figure 9:

The ETSI TS 103 246-3:2017 standard defines several GNSS sky scenarios. The ETSI TS 103 246-3:2017 standard, defines the open sky as the sky region above an elevation mask of 5° for which no GNSS signal attenuation occurs. Figure 10 portraits the sky view situation which allows the acquisition and tracking of all visible satellites above the elevation mask of 5°, assuming that the GNSS receiver does not have acquisition and tracking restriction on the number of tracking satellites.

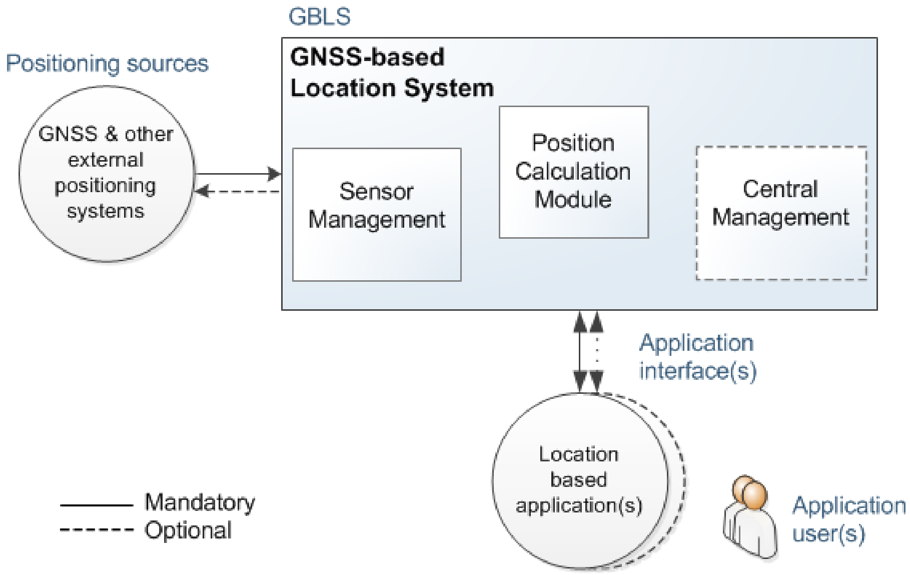
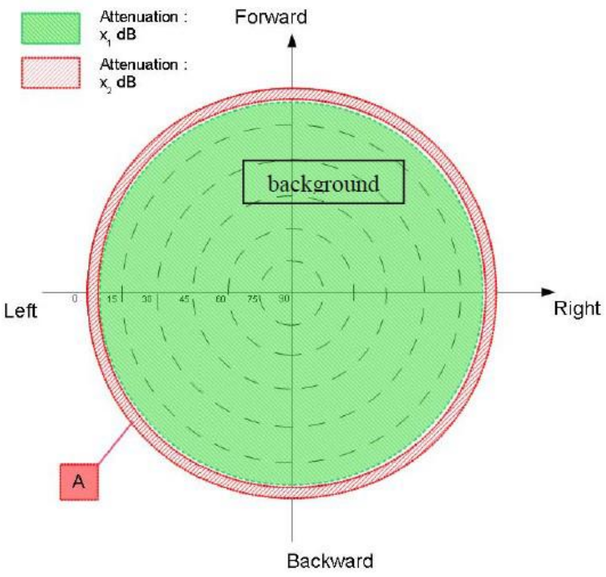

GBLS
GNSS-based Location System
Positioning sources
GNSS & other external positioning systems
Sensor Management
Position Calculation Module
Central Management
Application interface(s)
Location based application(s)
Application user(s)
Mandatory
Optional

Figure 9: GBLS architecture high-level or level 1. Source ETSI 103 246-2.

The above sky scenarios may be used for static or kinematic users. The ETSI TS 103 246-3 standard defines three position horizontal accuracy performance requirement classes for a moving vehicle in an open sky condition. These different class performances are provided in Table 22 for the case of a kinematic situation in an open sky environment as defined in the class defined in the ETSI TS 103 246-3:2017



Zone	Elevation range (deg)	Azimuth range (deg)	Attenuation (dB)
A	0 to 5	0 to 360	x_2 = 100
Back-ground	Angles out of Zone A		x_1 = 0

Figure 10: Urban canyon asymmetric sky view scenarios. Source ETSI 103 246-3

Horizontal Accuracy Metric	Maximal position error [m]		
	Class A	Class B	Class C
Mean error	1,0	4,0	8,0
Standard deviation	0,7	2,0	7,0
95% percentile	2,0	10,0	17,0

Mean cross track error	1,4	5,5	11,0
Cross track error – 95% percentile	2,8	14	24,0
Mean along track error	1,4	5,5	11,0
Along track error – 95% percentile	2,8	14,0	24,0

*Table 22:*Performance requirements for the horizontal accuracy

The Classes of performance (A, B and C) are defined in order to categorize the performance level of the GBLS for a given performance feature. In all cases Class A is the highest performance class and C is the lowest.

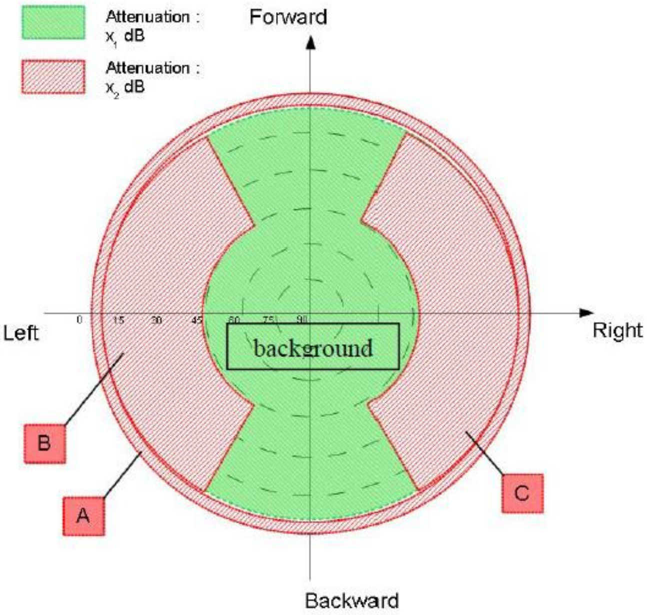


Figure 11: Urban canyon asymmetric sky view scenarios. Source ETSI 103 246-3.

The ETSI TS 103 246-5 defines the test procedures required to test conformance with the performance figures defined. The performance figures are:

1. Horizontal position accuracy
2. Vertical position accuracy
3. Time-to-first fix (TTFF)
4. Position authenticity
5. Robustness to interference
6. GNSS sensitivity
7. Position integrity (protection level)
8. Position day-to-day repeatability
9. Time-to-fix ambiguity

The standard defines the common test conditions required for all tests. The conditions range from environmental conditions, GNSS signal conditions, operational conditions, assistance and differential data and the test configurations.

The context of the VMPS from the GNSS signal conditions are a relevant aspect. In this regard, the ETSI TS 103 246-5 defines the GNSS signal at the antenna connector of the GNSS-Based Location System (GBLS). For a GBLS system equipped with an integral GNSS antenna it is assumed that the antenna has a gain of 0 dB. The standard also defines the reference input signal power level conditions. The reference power and relative signal power levels for each GNSS signal type are provided in the following table.

	Galileo		GPS		GLONASS	
Reference Power (dBm)	-130.0		-128.5		-131.0	
Signal power level relative to reference power level (dB)	E1	0	L1 C/A	0.0	G1	0.0
	E6	+2	L1C	+1.5	G2	-6.0
	E5	+2	L5	+3.6		
NOTE 1: The GNSS signal power levels in the table represent the total signal power per channel for pilot and data channels.						

Table 23:Power level conditions.

2.6.5 Applicable Document [AD-24]: REPORT ON RAIL USER NEEDS AND REQUIREMENTS - OUTCOME OF EUPSA USER CONSULTATION PLATFORM-

This report aims to provide the segmentation of Rail Applications on to the analysis of GNSS user requirements for Rail with definition and classification of applications focused on GNSS usage (not device-based).

This document provides performance and quality levels of positioning and movement vector reporting functions required in railway applications when using the GNSS navigation services.

Location unit for the railway applications

The location unit is a device fulfils specific functions for location, which is provide the information on position and if necessary, speed, direction of movement and acceleration of the device.

Satellite positioning receivers cannot be used as stand-alone technology to satisfy positioning requirements in the railway environment because of it being unavailable sometimes due to the landscape surrounding the moving vehicle, masking, shadowing, and canyon effects.

Specific concepts and definitions

This provides definitions and explanations of specific concepts referred to in the requirements.

Accuracy

It is defined as the degree of conformance between the position indicated at the location unit output and the true position, at a given level of confidence at any instance in time and at any location in the coverage area. Accuracy can also be said to be the position error at 95% confidence level. There is different variant of accuracy, and they are used by different applications.

- **Predictable accuracy** – The accuracy of the navigation unit position with respect to a mapped solution when the user evaluates the position related to a map.

- **Absolute accuracy** – The accuracy of the position related to the geodetic coordinates of the earth. It is used for positioning requiring high accuracy.
- **Relative accuracy** – The accuracy to which a user can determine its position relative to another user of the same navigation systems at the same time.

It should be noted that the accuracy requirement of a location unit used in train control system depend on the position of the train.

Integrity

Integrity is said to be the trust that can be placed in the correctness of the information supplied by the location unit to the application. There are two parameter that describe integrity.

1. **Threshold value or alert limit** – It is the maximum allowable error in the measured position before an alarm is triggered.
2. **Time-to-alarm** – The maximum allowable time between an alarm condition occurring and the alarm being present at the output.

The Rail scenarios/ use cases are much more complex that the aviation ones as because, if a failure occurs the train has to stop immediately. Therefore, the notion of Time-To-Alarm in the railway domain dissents from the aeronautical one. It cannot be expected from the rail community exclusively to define the GNSS requirements by applying the approach taken by aviation.

According to the [AD-24], the performance (time to alarm) for the safety related requirements, such as cold movement detection, Level crossing protection, the maximum allowable time between the occurrence of the failure in the PNT solution and its presentation to the user shall be less or lower than 10s.

According to the [AD-24], the performance (time to alarm) for the non-safety related requirements, such as odometer calibration, the maximum allowable time between the occurrence of the failure in the PNT solution and its presentation to the user shall be less or lower than 10s, and for management of emergencies, hazardous cargo monitoring, it shall be between 10s and 30s.

According to the [AD-24], the performance (time to alarm) for the non-safety related requirements, such as Infrastructure surveying, location of GSM reports, gauging surveys, structural monitoring, Fleet management, cargo monitoring, energy and Infrastructure charging, the maximum allowable time between the occurrence of the failure in the PNT solution and its presentation to the user shall be 30s or even more.
The results presented within [AD-24] and the associated stated requirements represent the most recent Rail User Requirements expressed for a representative sample of Rail applications. Those requirements are mostly expressed by ranges of value or qualitative requirements and tend to simplify the reality. But as of today, they are the only ones recognized by the Rail community– except for the Time to Alarm requirement. The Rail community is indeed not able to express any requirement in terms of TTA. Thus the [AD-24] reference to [ESSPTN- 12586 v01- 00 "EGNOS V3 requirements for the rail domain] , the performance (time to alarm) for the safety related requirements, such as train Integrity and train length monitoring, track identification, door control supervision and trackside personnel protection, the maximum allowable time between the occurrence of the failure in the PNT solution and its presentation to the user shall be 10s and 30s.

Integrity risk

This occur when the true location error is out of tolerance limit, but the location unit still reports information available, and no alarm is triggered within the time to alarm.

Integrity risk of the location unit strongly depends on the implementation and therefore system design.

For safety relevant applications, the integrity risk can be described by the tolerable hazard rate which is derived from a risk analysis per application. A safety integrity level can be then allocated.

Requirements and applications

The relevant railway applications have been grouped into three classes.

1. Safety related applications
2. Mass commercial / information and management – operational applications
3. Professional applications and infrastructure.

According to the [AD-24], the GNSS requirements for the Rail from the GNSS Rail Advisory Forum are as follows:

No	Application	Requirement					
		Accuracy	Integrity		Availability	Service interrupt threshold	Continuity
		Horizontal (m)	Alert limit (m)	Maximum time to alarms (s)	% Of mission time	(seconds)	
Safety related applications							
I	ex: ATC on high density lines/ stations/ parallel track	(1)	2.5	< 1.0	➢ 99.98	< 5	➢ 99.98
II	ex: Train control on medium density lines	(10)	20	< 1.0	➢ 99.98	< 5	➢ 99.98
III	ex: Train control on low density lines	(25)		< 1.0	➢ 99.98	< 5	➢ 99.98
Mass commercial / information and management – operational application							
IV	Tracing and tracking of vehicles	50	125	< 10	99.9	N/A	N/A
V	Cargo monitoring	100	250	< 30	99.5	N/A	N/A
VI	Dispatching	50	125	< 5	99.9	N/A	N/A

VII	Passenger information	100	250	< 30.0	99.5	N/A	N/A
Infrastructure and civil engineering, professional applications							
VIII	Positioning of machines	1 cm	N/A	< 5	99.5	N/A	N/A
IX	Infrastructure survey	1 cm	0.1 cm	< 10	99	N/A	N/A
X	Fix point applications	5 mm	N/A	< 30.0	99	N/A	N/A

Table 24:Requirements for safety-related, operational. infrastructural and professional applications.

2.6.6 Applicable Document [AD-25]: ETSI EN 303 413 V 1.2.0: GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS) USER EQUIPMENT (GUE)

This standard specifies technical characteristics and methods of measurements for Global Navigation Satellite Systems (GNSS) user equipment (GUE).

A GUE receives radio signals from one or more GNSS constellation for the purpose of radiodetermination of the position, velocity and/or other characteristics of an object or the obtaining of information relating to those parameters, by means of the propagation properties of radio waves.

Technical requirements specifications

- Environmental profile

  The technical requirements apply under the environmental profile for operation of the GUE, which shall be in accordance with its intended use. The GUE shall comply with all the technical requirements of this document at all times when operating within the boundary limits of the operational environmental profile defined by its intended use.

- Conformance specifications

  Receiver blocking is a measure of the capability of the GUE to receive a wanted signal without exceeding a given degradation due to the presence of an unwanted input signal operating in accordance with the allocation table of the ITU Radio Regulations in frequency bands adjacent or near adjacent to the relevant RNSS band.

  - Specification

    The C/N0 metric reported by the GUE for all GNSS constellations and GNSS signals given in table below and supported by the GUE shall not degrade by more than the value given in equation below when a blocking signal is applied.

$$\Delta \frac{C}{N_o} = \leq 1dB$$

GNSS Constellation	GNSS Signal Designations	RNSS Frequency Band (MHz)
BDS	B1I	1 559 to 1 610
	B1C	1 559 to 1 610
Galileo	E1	1 559 to 1 610
	E5a	1 164 to 1 215
	E5b	1 164 to 1 215
	E6	1 215 to 1 300
GLONASS	G1	1 559 to 1 610
	G2	1 215 to 1 300
GPS	L1 C/A	1 559 to 1 610
	L1C	1 559 to 1 610
	L2C	1 215 to 1 300
	L5	1 164 to 1 215
SBAS	L1	1 559 to 1 610
	L5	1 164 to 1 215

Table 25: GNSS constellation, GNSS signals and RNSS frequency bands

Frequency band (MHz)	Test point centre frequency (MHz)	Blocking signal power level (dBm)	Comments
1 518 to 1 525	1 524	-65	MSS (space-to-Earth) band
1 525 to 1 549	1 548	-95	MSS (space-to-Earth) band
1 549 to 1 559	1 554	-105	MSS (space-to-Earth) band
1 559 to 1 610	GUE RNSS band under test		
1 610 to 1 626	1 615	-105	MSS (Earth-to-space) band
1 626 to 1 640	1 627	-85	MSS (Earth-to-space) band

Table 26: Frequency bands, blocking signal test point centre frequencies and power level

- Conformance
- A GUE utilizing the RNSS band 1559 MHz to 1 610 MHz shall be presumed to conform to this technical requirement specification if the C/N0, as reported by the GUE for each declared GNSS constellation and GNSS signal, does not degrade by more than the value given in equation above in the presence of the blocking signals in table 16.

- Receiver spurious emissions

  Receiver spurious emissions are emissions at any frequency when the GUE is active.

  - Specification

    The receiver spurious emissions of the GUE shall not exceed the values given in table below.

Frequency range	Maximum power	Bandwidth
30 MHz to 1 GHz	-57 dBm	100 kHz
1 GHz to 8,3 GHz	-47 dBm	1 MHz

Table 27:Receiver spurious emission limits

Testing for conformance with technical requirements

- Environmental conditions for testing

  Where technical performance varies subject to environmental conditions, tests shall be conducted under sufficient variety of environmental conditions (within the boundary limits of the operational environmental profile defined by its intended use) to give confidence of compliance for the affected technical requirements.

  Unless otherwise declared, the temperature and humidity conditions for tests shall be any convenient combination of temperature and humidity within the following ranges:

  - Temperature: +15 °C to +35 °C
  - Relative humidity: 20% to 75%

- EUT Configuration

  For an equipment under test (EUT), detachable antenna, the EUT shall be connected to a test bed by means of the antenna port. For an EUT with integrated antenna, the antenna element is removed and a connection from the antenna to the test bed shall be made in place of the antenna element. The diagram for conducted measurement is shown below.

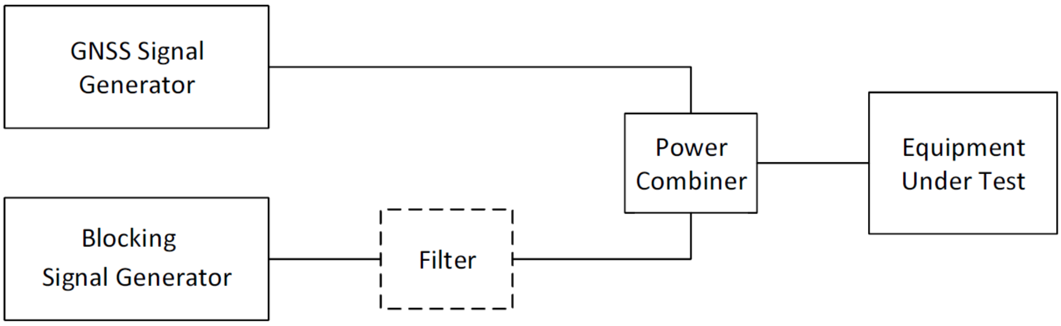


Figure 12:Conducted measurement setup for EUT receiver blocking.

- Test setup for radiated measurements

  Radiated measurements require additional test elements and equipment in addition to those specified for conducted measurements.

- EUT configuration

  The orientation of the EUT with respect to the transmitting antennas (normally boresight) shall be declared in the test report. The test bed shall be calibrated so that the blocking signal power levels are incident upon the antenna of the EUT.

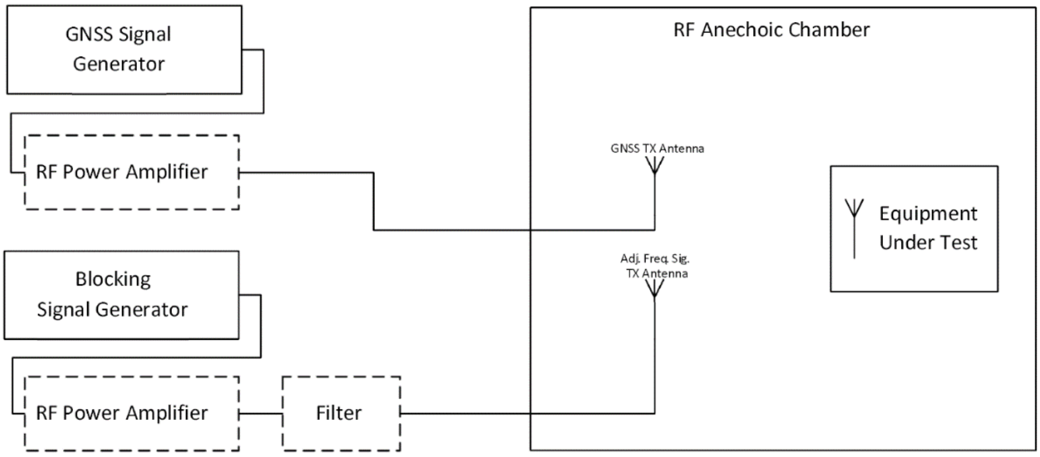


Figure 13:Radiated measurement setup for EUT receiver blocking

2.6.7 Applicable Document [AD-26]: IEC 61508 – FUNCTIONAL SAFETY OF ELECTRICAL / ELECTRONIC / PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS

This standard covers those aspects to be considered when electrical/electronic/programmable electronic systems are used to conduct safety functions.

Conformance to this standard

To conform to this standard, it shall demonstrate that the equipment has been satisfied to the required criteria specified. The standard specifies the requirements for E/E/PE safety-related systems and has been developed to meet the full range of complexity associated with such systems.

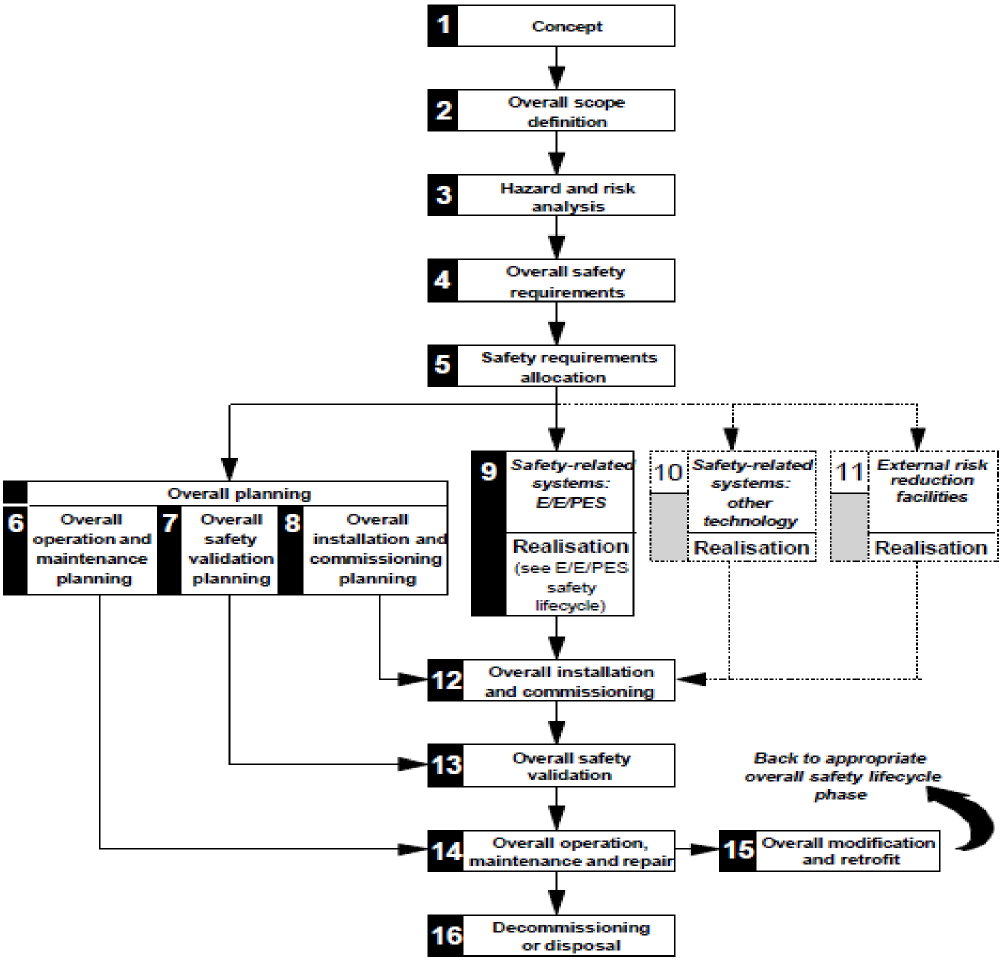
Management of functional safety Requirements

Those organizations or individuals that have overall responsibility for one or more phrases of the overall, E/E/PES or software safety lifecycles shall in respect of those phases for which they have overall responsibility, specify all management and technical activities that are necessary to ensure that the E/E/PE safety-related systems achieve and maintain the required functional safety. The following should be considered.

a. The policy and strategy for achieving functional safety, together with means for evaluating its achievement.
b. The overall, E/E/PES or software safety lifecycle phases to be applied
c. The way in which information is to be structured and the extend of the information to be documented.
d. The functional safety assessment activities.

Overall safety lifecycle requirements

To deal in a systematic manner with all the activities necessary to achieve the required safety integrity level for the E/E/PE safety-related systems, the standard adopts an overall safety lifecycle as the technical framework.


1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 Safety-related systems: E/E/PES
Realisation (see E/E/PES safety lifecycle)
10 Safety-related systems: other technology
Realisation
11 External risk reduction facilities
Realisation
12 Overall installation and commissioning
13 Overall safety validation
Back to appropriate overall safety lifecycle phase
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
16 Decommissioning or disposal

NOTE 1 Activities relating to ***verification***, ***management of functional safety*** and ***functional safety assessment*** are not shown for reasons of clarity but are relevent to all overall, E/E/PES and software safety lifecycle phases.

NOTE 2 The phases represented by boxes 10 and 11 are outside the scope of this standard.

NOTE 3 Parts 2 and 3 deal with box 9 (realisation) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

Figure 14:Overall safety lifecycle AD-25

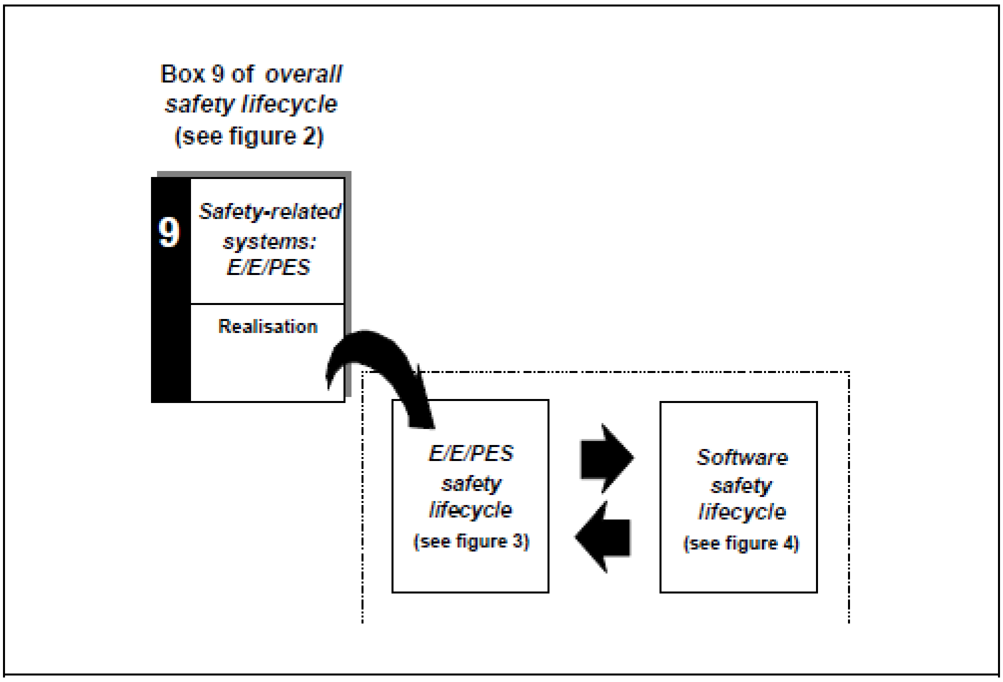


Figure 15: Relationship of overall safety lifecycle to E/E/PES and software safety lifecycles AD-26

2.6.8 Applicable Document [AD-27]: CEN/TR 17603 11: TECHNOLOGY READINESS LEVEL (TRL) GUIDELINESS

This document is used to support application of the TRL and provides guidelines to its use in projects and its independent verification within each specific project context.

TRL and assessment basic principles

Technology readiness assessment allows for the assignment of a measure of the maturity of a technology. It is important to make clear that undertaking a TRA is not a method to develop technologies.

The measure provided by TRL assessment is valid for a given element, at a given point in time, and a given defined environment. It changes if the conditions (such as operational environment) that prevailed at the time of the assessment are no longer valid.

TRL is used during preliminary Phases (0, A, B) as a tool supporting the decision whether or not to use or integrate specific technology in a space mission and allowing such decision to be taken with sufficient knowledge of any risk relating to the degree of maturity.

The intermediate levels of maturity (typically TRLs 4, 5 and 6) are sometimes called “valley of death” since some technologies are developed until TRL 4 or below, however they are not developed beyond this achieved level (i.e., in the absence of a project “pull”), noting that projects are normally interested in TRL 6 or above.

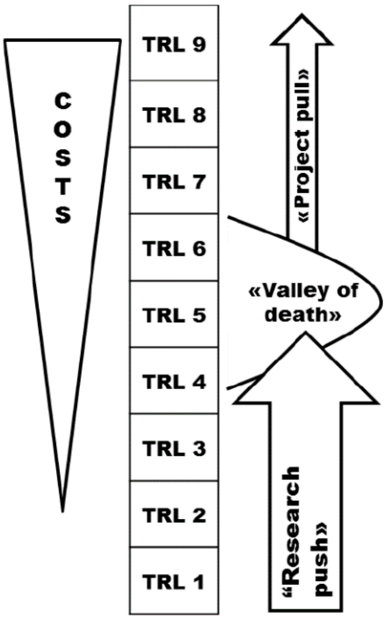


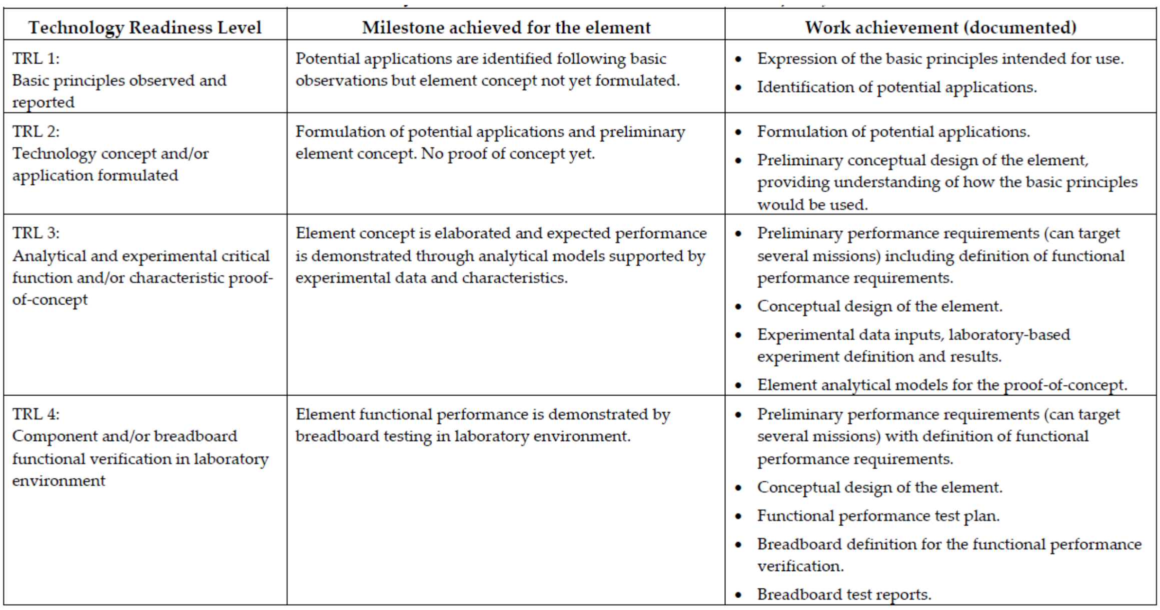
Figure 16: Evolution technology maturity

Technology readiness assessment (TRA) guidelines

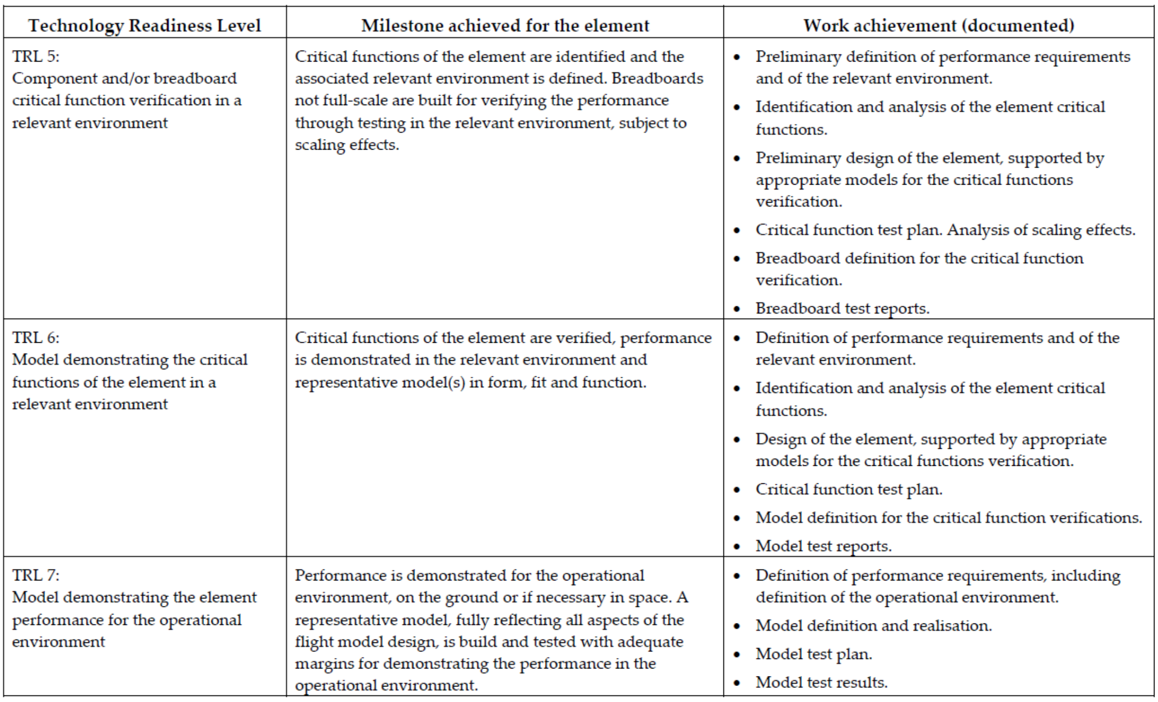
The value of a technology readiness assessment (TRA) exercise is to inform new programmes about the work already achieved on modern technologies and optimize synergies between programmes. Technologies are often developed in the frame of institutional programmes, or through R&T&D activities to prepare commercial programmes.

- TRL standard
  A TRA implements the requirements of TRL Adoption Notice ECSS-E-AS-11 (which adopts the definitions and criteria of assessment of ISO 16290) which are provided in the table below.

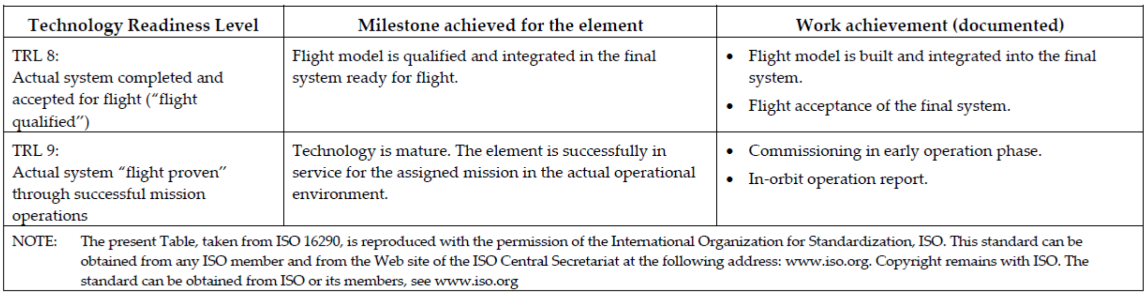
- Independent verification of the TRL
  The following below ensure the independent verification of the TRL
  - To ensure that a TRA of an element is objective, it is completed by independent expertise in the discipline.
  - Principle of independence in TRA process is like any review process.
  - Access for TRA team, to the necessary information and data concerning the technology and level to be assessed is ensured by the entity requesting the TRA.



Technology Readiness Level	Milestone achieved for the element	Work achievement (documented)
TRL 1: Basic principles observed and reported	Potential applications are identified following basic observations but element concept not yet formulated.	• Expression of the basic principles intended for use. • Identification of potential applications.
TRL 2: Technology concept and/or application formulated	Formulation of potential applications and preliminary element concept. No proof of concept yet.	• Formulation of potential applications. • Preliminary conceptual design of the element, providing understanding of how the basic principles would be used.
TRL 3: Analytical and experimental critical function and/or characteristic proof-of-concept	Element concept is elaborated and expected performance is demonstrated through analytical models supported by experimental data and characteristics.	• Preliminary performance requirements (can target several missions) including definition of functional performance requirements. • Conceptual design of the element. • Experimental data inputs, laboratory-based experiment definition and results. • Element analytical models for the proof-of-concept.
TRL 4: Component and/or breadboard functional verification in laboratory environment	Element functional performance is demonstrated by breadboard testing in laboratory environment.	• Preliminary performance requirements (can target several missions) with definition of functional performance requirements. • Conceptual design of the element. • Functional performance test plan. • Breadboard definition for the functional performance verification. • Breadboard test reports.



Technology Readiness Level	Milestone achieved for the element	Work achievement (documented)
TRL 5: Component and/or breadboard critical function verification in a relevant environment	Critical functions of the element are identified and the associated relevant environment is defined. Breadboards not full-scale are built for verifying the performance through testing in the relevant environment, subject to scaling effects.	• Preliminary definition of performance requirements and of the relevant environment. • Identification and analysis of the element critical functions. • Preliminary design of the element, supported by appropriate models for the critical functions verification. • Critical function test plan. Analysis of scaling effects. • Breadboard definition for the critical function verification. • Breadboard test reports.
TRL 6: Model demonstrating the critical functions of the element in a relevant environment	Critical functions of the element are verified, performance is demonstrated in the relevant environment and representative model(s) in form, fit and function.	• Definition of performance requirements and of the relevant environment. • Identification and analysis of the element critical functions. • Design of the element, supported by appropriate models for the critical functions verification. • Critical function test plan. • Model definition for the critical function verifications. • Model test reports.
TRL 7: Model demonstrating the element performance for the operational environment	Performance is demonstrated for the operational environment, on the ground or if necessary in space. A representative model, fully reflecting all aspects of the flight model design, is build and tested with adequate margins for demonstrating the performance in the operational environment.	• Definition of performance requirements, including definition of the operational environment. • Model definition and realisation. • Model test plan. • Model test results.



Technology Readiness Level	Milestone achieved for the element	Work achievement (documented)
TRL 8: Actual system completed and accepted for flight ("flight qualified")	Flight model is qualified and integrated in the final system ready for flight.	• Flight model is built and integrated into the final system. • Flight acceptance of the final system.
TRL 9: Actual system "flight proven" through successful mission operations	Technology is mature. The element is successfully in service for the assigned mission in the actual operational environment.	• Commissioning in early operation phase. • In-orbit operation report.

NOTE: The present Table, taken from ISO 16290, is reproduced with the permission of the International Organization for Standardization, ISO. This standard can be obtained from any ISO member and from the Web site of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with ISO. The standard can be obtained from ISO or its members, see www.iso.org

Table 28:TRL summary-milestones and work achievement

2.6.9 Applicable Document [AD 28]: CEN/JTC N150 – SPECIFICATION OF THE TEST FACILITIES; DEFINITION OF TEST SCENARIOS; DESCRIPTION AND VALIDATION OF THE PROCEDURES FOR FIELD TESTS RELATED TO SECURITY PERFORMANCE OF GNSS – BASED POSITIONING TERMINALS

This document is applied for the test procedures for assessment of robustness to security attacks.

GNSS threats overview

The analysis is focused on the intentional RF threats scenarios since they represent a worst case with respect to unintentional interference. Furthermore, intentional attacks encompass a wide variety of cases that allow a more flexible, representative, and controllable analysis.

The possible attacks on GNSS can be divided in two (2) areas:

- Denial of service (DoS)
    - Jamming
- Deception of service
    - Spoofing
    - Meaconing

Jamming threat is based on the transmission of an interfering signal on the GNSS bands.

Deception of service attacks are instead focused on making a receiver computing a false PVT solution.

- Denial of service: Jamming

  Jamming signals are disturbing signals developed to prevent the correct operation of a receiver. Commercial jammers can be categorized in:
    - Continuous wave (CW) signal (class I)
    - Chirp signal with 1 (one) saw-tooth function (class II)
    - Chirp signal with multi saw-tooth functions (class III)
    - Chirp jammer with frequency bursts (class IV)
- Deception of service: spoofing and meaconing.

  Several types of attacks to GNSS can be grouped under the spoofing label, aimed at impacting various aspects of the GNSS system such as data or signals:
    - Channel spoofing
    - Trajectory spoofing
    - Data level spoofing

Security metrics

Security metrics are necessary to assess the robustness of the receiver against jamming and spoofing threats. Jamming attacks are brute force attacks intended for Denial of Service (DoS), being it a loss of accuracy below a certain threshold or a complete loss of lock and, consequently, loss of PVT estimation. These kinds of attacks therefore can impair accuracy, and if strong enough, they can disrupt availability and continuity. A typical jammer performs little or no concealment countermeasure at all to avoid detection by the receiver. The transmission of high-power signals can probably cause the disruption of service and it is necessary to assess how the receiver reacts to these threats.

In summary, jamming and spoofing attacks impact the accuracy, availability, integrity, and continuity of the GNSS service. These attacks can also impact Time to First Fix. The degradation analysis is based on comparison of statistical estimates under attack with respect to the ones estimated in basic scenarios.

The most meaningful information requested for the degradation analysis are:

- Reference trajectory for the whole recording time
- Reference velocity for the whole recording time
- Performance assessment in the basic case

Integrity

Integrity measures the reliability of the information returned by the navigation system. This metric has been defined in the aviation domain and is currently highly exploited to ensure the airworthiness safety.

The parameter related to integrity are the following:

- Alert limit (AL)
- Position error (PE)
- Protection level (PL)
- Integrity risk (IR)

2.6.10 Applicable Document [AD 29]: CEN/TR 17475 – TEST PROCEDURES FOR ASSESSMENT OF ROBUSTNESS TO SECURITY ATTACKS:

The CEN 17475 has identified the following performance metrics, namely:

- Accuracy
- Integrity
- Availability and continuity
- Timing performance

Accuracy

Accuracy metrics as defined in FprCEN/TR 17448:2019 is the baseline metric for assessing security performance and identifies the receiver capabilities of correctly estimating the position and velocity. The accuracy is evaluated through CDF computation.

Let us assume that the metric is computed processing data points where the GNSS PVT is available at the receiver. This approach avoids the introduction of dummy data in the performance computation, which could bias the degraded calculus.

A jamming threat can heavily impact the CDF:

- Medium jamming: jamming be an error source, spreading the CDF toward higher values.
- Intense jamming: in case of intense jamming, the PVT is lost to all, and if the number of remaining points is too low, no CDF can be computed at all.

In the case of spoofing attack, two cases can happen:

- Spoofing attack failed
- Spoofing attack successful

Integrity

- Integrity from aviation domain

  Integrity measures the reliability of the information returned by the navigation system. This metric has been defined in the aviation domain and is currently highly exploited to ensure the airworthiness safety. The degradation of these metrics depends on the reaction to jamming and spoofing of the protection level computation unit. Figure below shows the standard diagram that illustrates all the integrity failures concepts. The same concept sketched here for position (horizontal or vertical) can be applied to velocity.

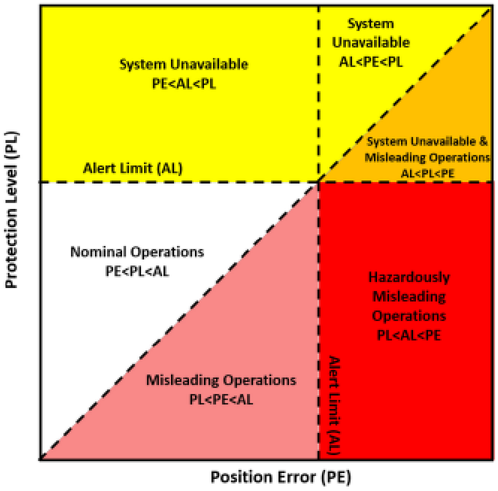


Figure 17:Stanford diagram

The simplest algorithm for protection level calculation accounts for the following 3 (three) factors:

$$PL = k_{IR} * \sigma_{UERE} * GDOP$$

Where k_{IR} is a factor accounting for integrity risk requirements, σ_{UERE} is a term accounting for the overall user equivalent ranging errors, i.e., the noise on receiver measurement, and GDOP is the geometric dilution of precision, a factor accounting for geometry of the satellites.

- Integrity from ITS
  Intelligent transport system sector has defined a simplified version of integrity, and in particular the concept of Alarm limit is not used. For the sake of simplicity, the Stanford plot above describe can still be used to represent graphically the relation among protection level and position error (and the same as for velocity plots), since many software analysis tools are capable of deriving such plots by default. The classical Stanford plot can be used, by considering only two regions above and below the line PL = PE in the plot, as visible in figure 16.

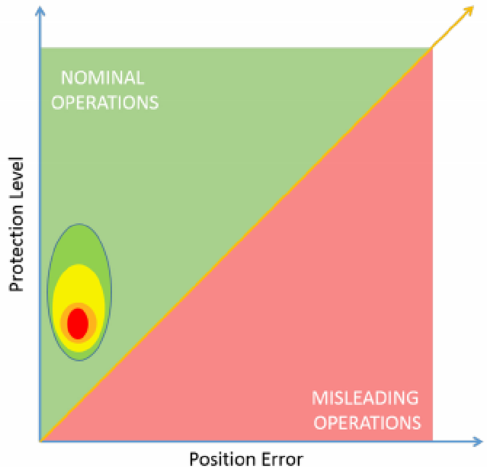


Figure 18:Integrity plot in ITS

Availability and continuity

The **availability** is a simple dimensionless quantity, i.e., according to two definitions:

- The ratio of the number of samples with valid PVT over the total number of samples.

- Position availability (T) is the percentage of operating time intervals of length T during which the positioning terminal provides at least one position output. In this case also the observation period is considered, but the two definitions are equivalent of the time interval is taken equal to the length of the PVT period, i.e., 1 (one) second in the worst case.

Continuity is defined as the percentage of time intervals of length T during which the positioning terminal provides valid outputs at the expected rate and without interruptions. A possible procedure for continuity estimation, according to this definition is the following:

- Start from the sample validity, i.e., for each valid sample assign a value 1 and assign instead a value 0 to each invalid (or not present) PVT sample.
- Fix a time interval of length T (i.e., window of T contiguous samples).
- Perform a sliding window on the data, summing at each instant the number of valid samples in the window. The outcome spans from 0 to T. In practice the continuity signal is set to 0 if at least one sample in the window is equal to 1, while the continuity signal is set to 1 only if all samples in the window are equal to 1.
- Apply the thresholds, obtaining run-length estimates for availability and continuity.
- Evaluate availability and continuity as the ratio of the number of 1 obtained over the total number of sliding-window samples.

Time to first fix (TTFF)

Time to First Fix: TTFF measures the time of first fix, so for each run 1 (one) sample is collected. It is very time consuming to build a CDF. It is hence suggested to evaluate TTFF as an average, not a CDF, averaging 10 to 30 test runs. It seems better to reuse the same scenarios considered for the other security metrics, for the sake of homogeneity of the testing procedure. It is clear why TTFF needs fields tests. It seems also TTFF can be assessed, as the other metrics, i.e., with a record (or generation) and replay of specific scenarios with jamming and spoofing superimposed to authentic GNSS signal.

2.6.11 Applicable Document [AD 30]: PAPER ON GALILEO FOR RAILWAY OPERATIONS ABOUT THE POSITIONING PERFORMANCES ANALOGY WITH THE RAMS

This paper deals with the question of the RAMS evaluation of the satellite-based location function delivered to a railway safety application, as recommended by railway standards, and presents a methodology to transpose GNSS specifications into RAMS

Failure cause analysis of the positioning function

The position failure is a feared event for the user, i.e., a hazard for the safety-related railway application. It may result from software or hardware failures that occur in any of the three GNSS segments (ground control, satellite, and user segments).

Errors that are not due to intrinsic failure of the system can also be the result of specific causes that are not common in RAMS evaluation methods: errors that affect satellite signals (or SIS).

In this paper these errors are classified in two categories:

- Errors due to perturbations in signal propagation. Indeed, pseudo-ranges (estimation of the satellites/
  receiver distances by the receiver) used to calculate a position rely on propagation time measurements
- Errors in signal data (navigation message). These data (ephemeris, satellite clock correction) used for satellite location can be corrupted.

	Level A requirements	Level B requirements	Level C requirements
SIS integrity risk	2.0 e-7 in any 150 sec	1.0e-7/ 1 h	1.0e-5/ 3 h
Continuity risk	8.0e-6 in any 15 sec	1.0e-4 to 1.0e-8 / 1 h	3.0e-4 / 3 h
Availability of service	99.5 %	99.5 %	99.5 %
Time to alarm	6 sec	10 sec	10 sec
Accuracy (95%) H / V	4 m / 8 m	220 m / NA	10 m / NA
HAL / VAL	40 m / 20 m	556 m / NA	25 m / NA

Table 29: Performance requirements for the Galileo SoL service

In the case of the railway community, the needs for safety applications are expected to be covered by the level associated to the more constrained requirements: level A.

It is obvious, that GNSS service performance is defined by means of notions that came from aviation sector. Railway sector can employ them with respect of their specific meaning according to railway standards.

GNSS availability quality criterion

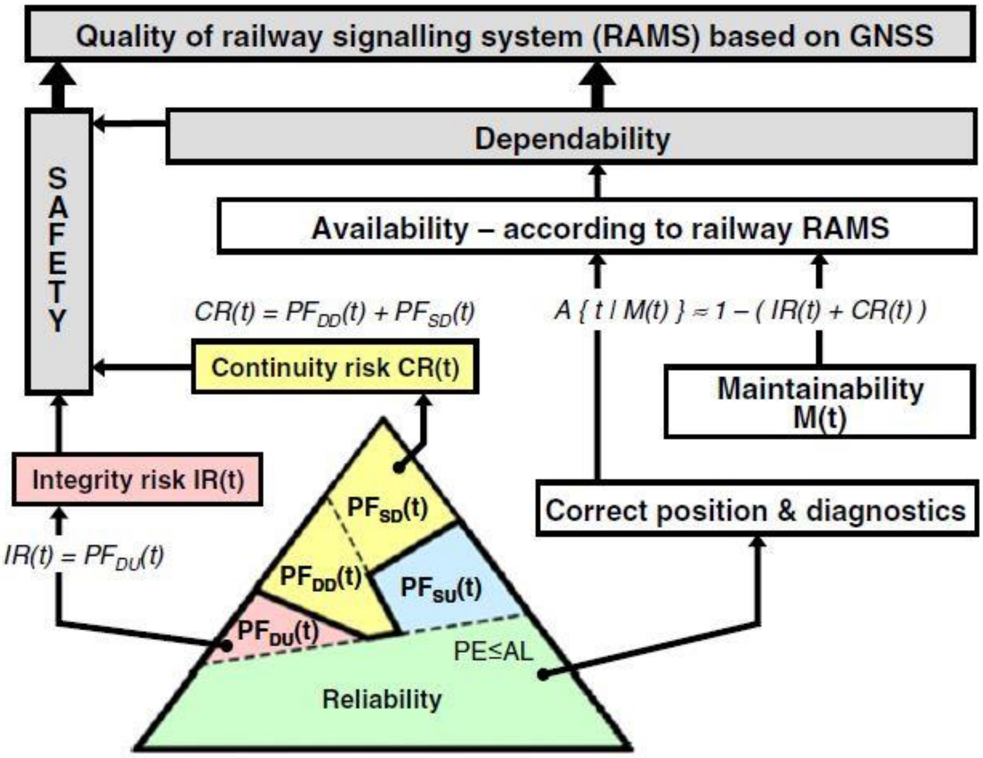

Quality of railway signalling system (RAMS) based on GNSS
SAFETY
Dependability
Availability – according to railway RAMS
$CR(t) = PF_{DD}(t) + PF_{SD}(t)$
$A\{t\,|\,M(t)\} \approx 1 - (IR(t) + CR(t))$
Continuity risk CR(t)
Maintainability M(t)
Integrity risk IR(t)
Correct position & diagnostics
$IR(t) = PF_{DU}(t)$
$PF_{SD}(t)$
$PF_{DD}(t)$
$PF_{SU}(t)$
$PF_{DU}(t)$
PE≤AL
Reliability

Figure 19: GNSS quality criteria within railway RAMS

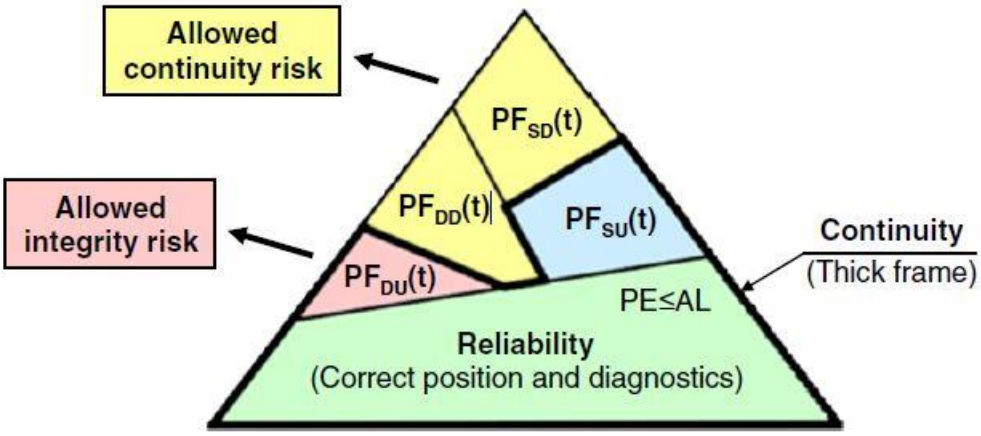


Figure 20:Detailed illustration of the analogy between GNSS criteria and the safety of the position

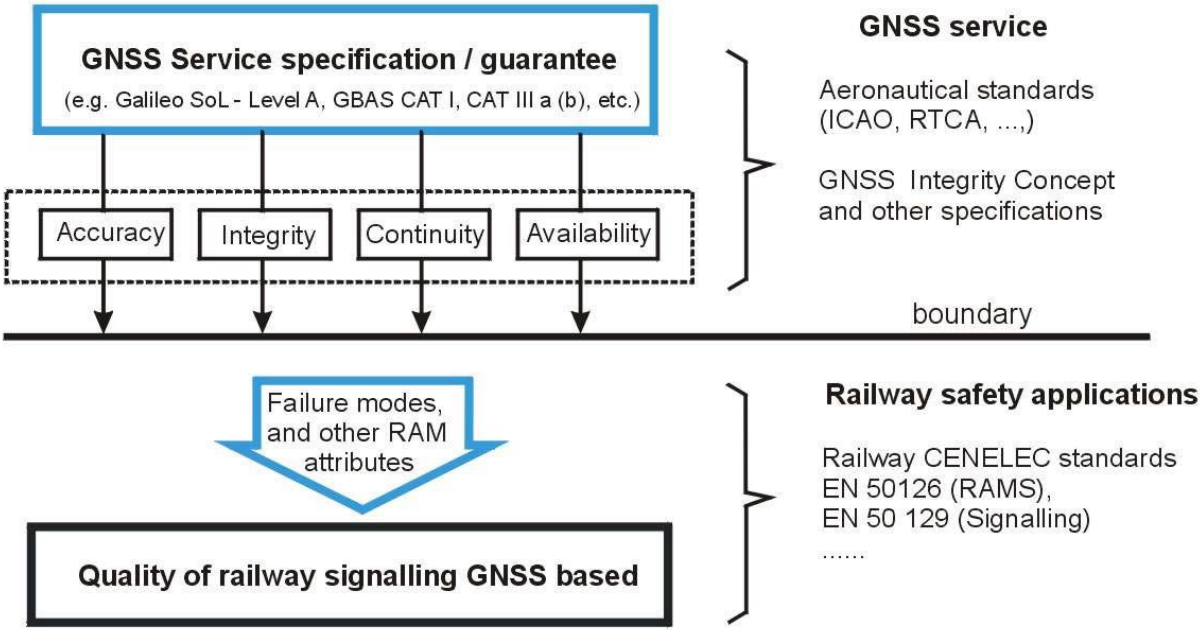

GNSS Service specification / guarantee
(e.g. Galileo SoL - Level A, GBAS CAT I, CAT III a (b), etc.)
Accuracy
Integrity
Continuity
Availability
GNSS service
Aeronautical standards
(ICAO, RTCA, ...,)
GNSS Integrity Concept
and other specifications
boundary
Failure modes, and other RAM attributes
Quality of railway signalling GNSS based
Railway safety applications
Railway CENELEC standards
EN 50126 (RAMS),
EN 50 129 (Signalling)
......

Figure 21: Relation between GNSS service specification and railway RAMS

2.6.12 Applicable Document [AD 31]: PAPER ON PERFORMANCE EVALUATION OF GNSS FOR TRAIN LOCALISATION

This paper demonstrates the performance of the GNSS receiver for train localization. This paper has shown a method to evaluate GNSS performances according to standards, particularly RAMS. A stochastic Petri net model is established to illustrate the GNSS receiver location states, i.e., up, degraded, and faulty states. The states are then related to the migrated four properties providing the bridge for quantitative evaluation of the characteristics for each property as shown in the Figure 22.

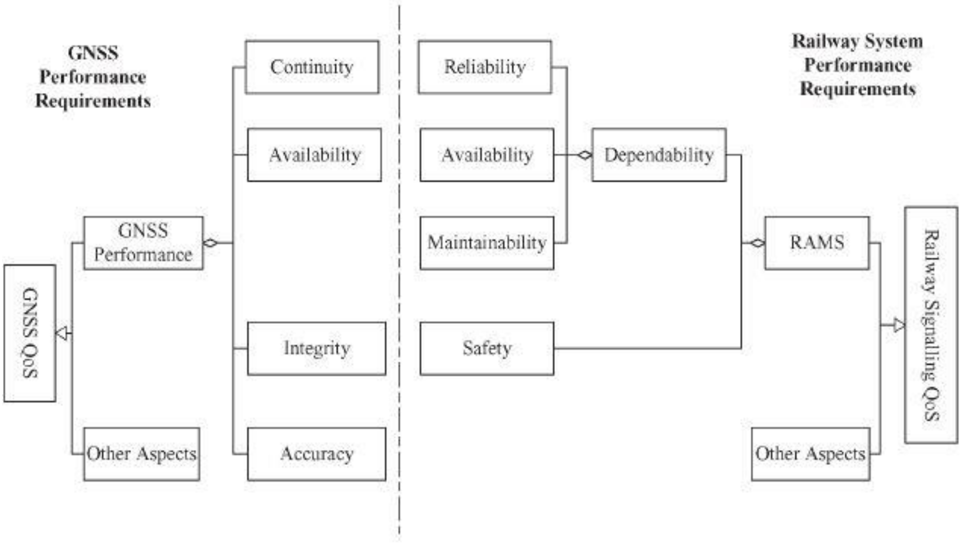


Figure 22: GNSS and railway performance requirements comparison.

Accuracy can be represented by two characteristics, i.e., trueness and precision. Trueness tells the deviation between the measured value and the true value; the true value is represented by a value measured by a multisensory reference system. The mean value of the deviations is denoted by μ. Precision is normally calculated through dispersion of measurement samples, called standard deviation, denoted as σ. Normally, μ ± 2σ (95% if normally distributed) is used to express the accuracy level of the measurement system.

The methodology for performance evaluation according to standards and the setup of a reference system together can promote a standardized test scenario and procedure for GNSS quantitative assessments.

2.6.13 Applicable Document [AD 32]: ISO/IEC 27000 INFORMATION TECHNOLOGY-SECURITY TECHNIQUES - INFORMATION SECURITY MANAGEMENT SYSTEMS-OVERVIEW AND VOCABULARY

This standard explains the overview and the vocabulary of information security management systems, which form the subjects of the ISMS family of standards and defines related terms and definitions.

Information security management systems

Organizations of all types and sizes:

a. collect, process, store, and transmit information.
b. recognise that information, and related processes, systems, networks, and people are important assets for achieving organization objectives.
c. face a range of risks that may affect the functioning of assets and
d. address their perceived risk exposure by implementing information security controls.

As information security risks and the effectiveness of controls change depending on shifting circumstances organizations need to:

a. monitor and evaluate the effectiveness of implemented controls and procedures.
b. identify emerging risks to be treated and
c. select, implement, and improve appropriate controls as needed.

What are an ISMS?

An information security management system (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. The following fundamental principles also contribute to the successful implementation of an ISMS.

a. Awareness of the need for information security
b. Assignment of responsibility for information security
c. Incorporating management commitment and the interests of stakeholders
d. Enhancing societal values

Why an ISMS is important

Risks associated with an organization’s information assets needs to be addressed. Achieving information security requires the management of risk, and encompasses risks from physical, human and technology related threats associated with all forms of information within or used by the organization.

An ISMS is important to both public and private sector businesses. In any industry, an ISMS is an enabler that supports e-business and is essential for risk management activities. The interconnection of public and private networks and the sharing of information assets increases the difficulty of controlling access to and handling of information.

Identifying information security requirements

Within the overall strategy and business objectives of the organization, its size and geographical spread, information security requirements can be identified through and understanding of:

a. Identified information assets and their value.
b. Business needs for information processing, storage, and communication
c. Legal, regulatory, and contractual requirements

2.6.14 Applicable Document [AD 33]: PAPER ON RAMS EVALUATION OF GNSS RAILWAY LOCALISATION

This paper demonstrates model GNSS RAMS aspects according to EN50126, using a petri net to model the states of the GNSS locations as a formal method. The availability and reliability Figure 23 aspects are analyzed as the basis for safety evaluation.

The beautiful aspect about the GNSS location is that the GNSS receiver is giving positioning results independently. The localization accuracy varies according to the movement of the train. This is cause by changes in the environment, mask angle, etc.

The reference system is said to be accurate location at the timestamps compared with GNSS receiver output.

Modelling of Reliability and Availability

Reliability means the ability of an item to perform a required function under given condition for a given time interval and availability is the ability of an item to be in a state to perform a required function under given conditions at a given instance of time.

Reliability and availability mean almost same thing, but reliability denotes the function itself and availability shows the result of the function.

Reliability of a repairable system is represented as the mean time to failure (MTTF) and availability is represented as the relationship between MTTF and mean failure time (F).

$$Availability = \frac{MTTF}{MTTF + F}$$

Three states of the GNSS receiver are defined.

1. Up state – The GNSS receiver is powered up, the location is reliable.
2. Degraded state – the GNSS receiver is powered up, the location may cause risks for train localisation.
3. Faulty state – the GNSS receiver is powered up, the location is unavailable due to GNSS signal loss or bad satellite geometry.

Modelling of Safety

Freedom from unacceptable levels of risk of harm is known as safety. Safety integrity is defined as the ability of a safety-related system to achieve its required safety functions under all the stated conditions within a stated operational environment and within a stated period. Safety is related to operational environment.

A model based on stochastic Petri net according to standard IEC62551 is shown in Figure 23, the model, the faulty state contains dangerous failures and safe failures which lead to failed state. The transition from up state to faulty state means the error of GNSS location is large enough for safety consideration and appropriate alarm notification. The transition between faulty state and the other two states means both up state and degraded state can go to unavailable situations, vice versa.

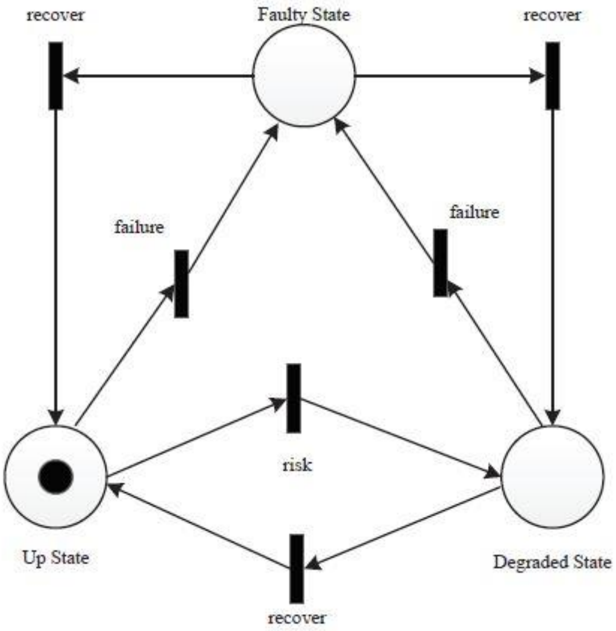


Figure 23: Petri net Model for State Transition (Reliability and Availability)

2.6.15 Applicable Document [AD 34]: CEN/TR 17465: Space-Use of GNSS-based positioning for road Intelligent Transport Systems (ITS)-Field tests definition for basic performance

This document constitutes the part of the technical report on metrics and performance levels detailed definition and field test definition for basic performances regarding the field tests definition.

Definition of the general strategy: kind of tests, GBPT characterization, hybrid and heterogenic system, Test combinatory explosion, Stakeholders and responsibilities, Roles and responsibilities, Main criteria for testing strategy,

Potential test Methods : Historically, only two types of tests were carrier out in the Domain of GNSS-based positioning : simulations in lab. tests with a GNSS signal generator and field tests, record, and replays.

Definition of the metrics and related tools : Accuracy metrics for along Track, Cross track,3D Vector, Horizontal, Easting, Northing, Integrity metrics, availability metrics, continuity metrics,

Field tests for recording the in-file data of the standardized operational scenario: test plan, test bench preparation and good functioning verification, field test execution, data analysis and archiving

Definition of the validation procedures : how to be sure of the results ? several points are of interest to be sure of the tests results : the quality of the reference trajectory, the availability, regularity of the of the DUT's outputs for the metrics computations, the statistic representability of the results : Numbers of points, correlation time, etc. For the replay, the stability of results along several replays.

Definition of the synthesis report: Identification of the DUT with brand, model, Serial number, SW part or release, any interesting features cable or alignments.

To Identify of a test, one must record test with test date and location of test, used a test bench and material including, test bench devices, serial number of devices, software release.

Personal responsible of test, report on test conditions, identification of file including the test data, Identification of tools used in post processing for computing the metrics.

Results analysis should be based on per metric identification in the standards, class per environment, company file number, logo, contact details, convenient justification, qualification (ISO/IEC 17025, etc.).

For Synthetic reporting tests are defined for various transverse combinations for GNSS error propagation environments. These are open sky area, urban area, asymmetry area using operational scenario mode called static measurement or dynamic measurements mode.

2.6.16 Applicable Document [35] ISO 17025: General requirements for the competence of testing and calibration laboratories

This document demonstrates models (EN ISO/IEC 17025:2017) prepared by Technical Committee ISO/CASCO "Committee on conformity assessment" in collaboration with Technical Committee CEN/CLC/JTC 1 “Criteria for conformity assessment bodies” .

Terms and definitions in this document

- Impartiality of tests: Objectivity means that conflicts of interest do not exist or are resolved so as not to adversely influence subsequent activities of the laboratory.
- Complaint: expression of dissatisfaction by any person or organization to a laboratory, relating to the activities or results of that laboratory, where a response is expected, Interlaboratory comparison: Organization, performance and evaluation of measurements or tests on the same or related items by two or more laboratories in accordance with predetermined conditions
- Interlaboratory comparison: organization, performance and evaluation of measurements or tests on the same or related items within the same laboratory in accordance with predetermined conditions.
- Proficiency testing: evaluation of participant performance against pre-established criteria by means of interlaboratory comparisons.
- laboratory: Person/body that performs one or more of the following activities: testing, calibration of device, and sampling, associated with subsequent testing or calibration.
- Resource requirements: Personal, Facilities and environmental conditions, equipment, metrological traceability, externally provided products and services.

Process requirements: The laboratory shall have a procedure for the review of requests, selection, verification, and validation of methods, tenders and contracts.

Management system requirements: As part of minimum requirement in management, the management system of the laboratory shall address the following: Management system documentation, control of management system documents, control of records, actions to address risks and opportunities, improvement to be performed, corrective actions, internal audits, management reviews.

2.6.17 Applicable Document [36] ISO 17065: Conformity assessment – Requirements for bodies certifying products, processes, and services

This documents defined requirements for the competence, consistent operation and impartiality of product, process, and service certification bodies. In this International Standard, the term “product” can be read as “process” or “service.”

Resource requirements for [ISO17065]: Certification body includes personnel those normally working for the certification, as well as persons working under an individual contract or a formal agreement that places them within the management control and systems/procedures of the certification body

The personnel shall be competent for the function the perform, including technical judgement qualification, to define policies and implementing them. The Personnel including any committee members, external bodies, personnel acting behalf of certification body should keep confidential information obtained

Personnel, including any committee members, personnel of external bodies, or personnel acting on the certification body's behalf, shall keep confidential all information or certification activities.

As part of documentation the certification body shall maintain the following records on the personnel involved in the certification process name and address of personnel, employer(s) and position held, educational qualification and professional status, experience and training, the assessment of competence, performance monitoring, authorizations held within the certification body, date of most recent updating of each record.

Requirements for management system: The certification body shall establish and maintain a management system that can achieve the consistent fulfilment of the requirements of this International Standard in accordance with either Option A or Option B according to ISO 17065.

- Option A : should include the management system of the certification body shall address the Following: General management system documentation (e.g., manual, policies, definition of responsibilities, control of documents, control of records, management review, internal audit, corrective actions, prevent) .

- Option B :certification body established and maintains a management system, in accordance with the requirements of ISO 9001, and that is capable of supporting and demonstrating the consistent fulfilment of the requirements of this International Standard, fulfils the management system clause requirements.

2.6.18 Applicable Document [37] JCGM 100: Evaluation of measurement data - Guide to the expression of uncertainty in measurement

Evaluation of measurement data document establishes general rules for evaluating and expressing uncertainty in measurement that are intended to be applicable to a test measurement.

Scope: This document guideline establishes general rules for evaluating and expressing uncertainty in measurement that can be followed at various levels of accuracy and in many fields from the shop floor to a fundamental research project.

Therefore, the principles of this guideline are intended to be applicable to a broad spectrum of measurements, including those required for: quality control and quality assurance in production, to comply with enforcing law and regulations, conducting basic research and applied research in science and engineering, to achieve a traceability and repeatability of national standard, instrument calibration must use during test execution. Moreover, physical reference standard and reference material should maintain national and international standard.

Basic concepts of uncertainty measurements: Measurement, errors, effects, corrections, uncertainty, and practical considerations should be taken.

Evaluating standard uncertainty: Modelling the measurements, Type A evaluation of standard uncertainty, Type B evaluation of standard uncertainty, graphical illustration of evaluating standard uncertainty.

- Determining combined standard uncertainty: Correlated input quantities and uncorrelated input quantities must be combined.

- Determining expanded uncertainty: Expanded uncertainty, choosing a coverage factor.

Reporting uncertainty: To report any uncertainty one must follow general guidance, specific guidance.

Summary of procedure for evaluating and expressing uncertainty: There are several annexes regarding this topic. These are :

- Annex A: Recommendations of Working Group and CIPM,
- Annex B. General metrological terms,
- Annex C: Basic statistical terms and concepts,
- Annex D: True value, error, and uncertainty,
- Annex E. Motivation, and basis for Recommendation INC-1 (1980),
- Annex F: Practical guidance on evaluating uncertainty components,
- Annex H: Examples, Annex J: Glossary of principal symbols

3 METHODOLOGY ADJUSTMENT AND ENHANCEMENT

The certification of the developed safety relevant train localization system within the CLUG project thorough validation and testing is essential for the later exploitation plan. For this the applicable test methods and standards discussed in the chapter state-of-the-art need to be adapted so that they can be used under consideration of the input from the deliverables D2.1 High-level mission requirements definition, D2.2 Operational Scenarios, D2.3 High Level System Requirements and D2.4 Preliminary Hazard Analysis.

In the following sections the general methodology and the specific methods are described. The general methodology provides an overview of the defined KPIs, and the methods based on the existing methodology as defined in the state of the art and from the existing standards which is extended. The section specific methods detail the methodology by describing the testing methods for certification of the developed safety relevant train localization system (TLS).

3.1 GENERAL METHODOLOGY

This section explains how the general methodology for prototypical certification for the CLUG project is defined. The process takes the applicable standards from various domains into account as well as input from the other CLUG deliverables.

The general testing and certification process with the referring QM standards is defined in Figure 24.

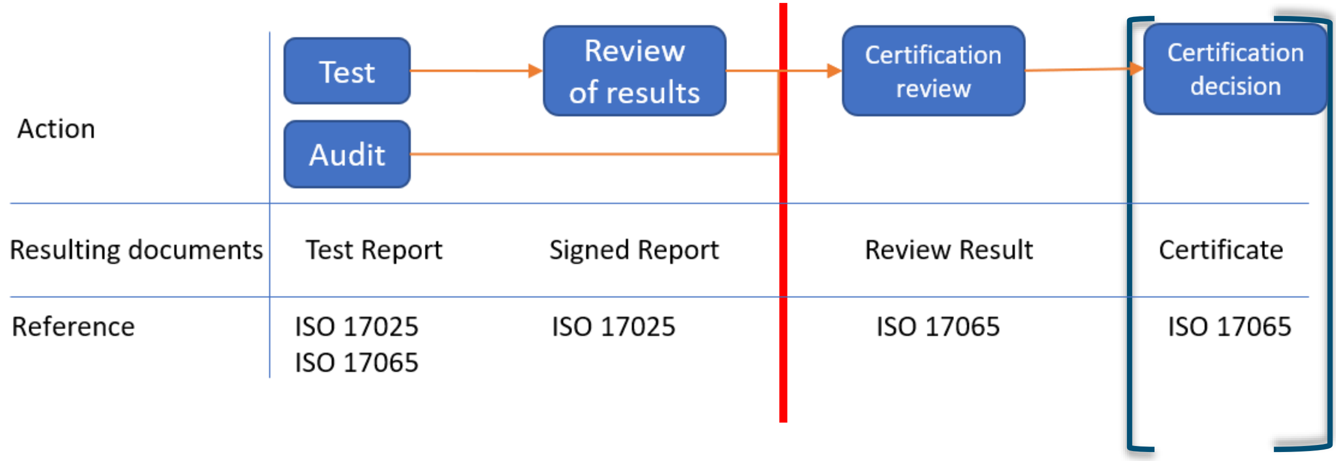


Figure 24 Overview of general testing and certification process

This process is described in more details in section 3.1.1 for the testing part (in the figure before the red line) and 3.1.2 for the certification process (in the figure after the red line).

3.1.1 General process for testing

The following section describes the evaluation and test process general objectives and methodology to be adopted for the CLUG testing.

In general, two test methodologies exist for a system, black box, and white box testing. The first step in the test process for both black box and white box testing is the definition of the System Under Test (SUT), which can be either the complete system, or only a subsystem. Since the SUT and the type of tests to be executed influence each other, it is crucial to provide a clear definition of the SUT from the beginning. To be more precise, a given test may reflect just one part of the system (this part is the SUT in this case). However, the choice of a given SUT (part of the system) simply implies the execution of specifically designed tests. The conditions of the SUT are to be known before the start and after the end of each test. In the context of CLUG, both black box and white box tests will be performed.

Black box testing (also called functional testing) is a technique that ignores the internal mechanisms of a system or component and focuses solely on the outputs generated in response to selected inputs and execution conditions. In other words, this approach is supposed to ensure that the functionality specified in the requirements works. This technique will be applied, for instance, to the products or solutions of the CLUG partners that are being extended. It can also be applied to external services, or the open-source components being used in the project and whose internal structure is not mandatory to be understood partially or entirely. In black box testing, the "reactions" of the SUT to "actions" are observed by means of the testing environment (e.g., counters of the testing tools).

White box testing (also known as structural testing) is a technique that considers the internal mechanisms of a system or component. When this approach is used, the testers will verify that the code that was written does what it is intended to do at an exceptionally low structural level. This technique will be mainly used for testing the software or hardware modules being developed by the project partners.

Both approaches complement each other. Therefore, it is foreseen in the CLUG project to combine black box and white box testing. This will allow the observation of the system feedback to actions from the point of view of the user (external observation) and looking into the system (observation of the internal parts of it). In fact, the black box approach is more likely to detect conditions of failure as perceived by the user, no matter what the internal detection instruments may claim. The white box technique could be easier, because of the knowledge of the internal structure, and the less time and steps it requires.

Combining both approaches provide the advantage that some internal observation of the system may allow the detection of defects that, otherwise, should be detected through the execution of exceptionally long tests.

This combined approach can be considered and inherited from the [AD-21], i.e. the eCall testing from the DELEGATED REGULATION (EU) 2017/79-Annex 1, where the test procedures and requirements are designed in such a way, where the DUT (device under test) is tested as black box to verify the sustainable functionality of the DUT and in the Part of Annex VI, where the test procedures and compatibility requirements are designed in such a way, where the DUT(device under test) is tested as white box via verifying the specifying navigation characteristics and features of the tested system.

Additionally, for the general test process the following distinctions must be included:

Simulation tests:

Simulation tests are in general lab test for which the software or hardware components under test are stimulated with simulated signals to test within a well controllable environment critical scenario. Additionally, this environment is also used to perform tests with a well-defined not changing input to achieve a repeatable and comparable testing. As well-known example tests using a GNSS signal simulation can be mentioned here.

Record & replay tests

This type of tests is a mixture between simulation tests and field tests. In such defined tests the sensor output and/or environment (for example RF) are recorded. For these records are reference is defined. The recording and the reference are analyzed by a laboratory so that it can be verified that both fulfil stated requirements. Afterwards the recorded signals can be "replayed" in the laboratory to evaluate hardware and/or software under consideration of the defined reference.

Field test

A usual definition for this test type is that the system under test is evaluated under defined requirements in a representative manner in an up to certain level uncontrolled and unknown environment.

A detailed definition for these test types can be found in CEN/TR 17465:2019 on the example of GNSS tests.

These test methodologies which can be found in the named references will also be considered to define the best possible, all-encompassing test plan.

The test methodology in CLUG spans various levels. In fact, it is crucial to have a system that is stable and provides the service according to the specifications and requirements. However, if this system does not interoperate in a seamless way with existing solutions and products, its deployment might not be possible.

3.1.2 General process for Prototypical Certification

This section describes the process of a prototypical certification using test reports of laboratories. Generally, for testing a laboratory needs to be accredited by a National Accreditation Body in the scope of ISO/IEC 17025 for performing the defined tests and audits. For the certification, the certification body needs to be accredited by a National Accreditation Body in the scope of ISO/IEC 17065. The certification process is divided into two parts, the certification review, and the certification decision.

Certificates are based on relevant directives, standards, or other criteria valid on the date of issue of the certificate. A certificate can be issued if all technical and quality management requirements in connection with the test have been fulfilled.

As the full certification requires a fully developed and mature product that is evaluated against valid standards, in the scope of the CLUG project only a prototypical certification will be performed. For a prototypical certification, the first part of the certification process comprising the certification review is conducted but the final formal certification decision will not result in issuing a real certificate.

This certification phase is divided into a technical and a formal part. Within the project as part of the project team NavCert will perform all work associated with the technical certification phase. The formal certification, which is excluded from the project due to the background of prototypical certification, would be conducted by an accredited certification body like NavCert.

Certifications are based on standards and as no specific standard exists in the project, an internal "standard" will be defined. Prerequisite for the development of a standard is a test mark. Both test mark and test plan have to be approved in the final phase by the certification body. Thereafter the first phase of the certification – the test laboratory work - will start with a validation based on the developed test plan.

The laboratory work will cover several activities each dealing with one specific aspect of the product as mentioned above for example:

- Detecting spoofing and jamming attacks
- trustworthiness of position
- Affectability in regard to critical scenarios (e.g., multipath)
- security from the PVT computation up to the final usage of the PVT data.

Full certification, which requires a fully developed and mature product, is not in the scope of this project, therefore this work package aims at achieving a 'Prototypical Certification.' Due to the existing restrictions, the activities of the previous work packages will be closely analyzed to identify suitable ones for the certification process in the deployment phase.

After successful completion of product testing, a certificate will be awarded to the certificate holder. Hereby the Certificate holder:

- shall comply with the requirements of the Certification Body with respect to referencing their certification status in communication.
- upon certificate suspension, expiry, revocation, or withdrawal, shall discontinue use of their advertising materials containing reference to their certification status, in line with the instructions of the Certification Body.
- shall not make or permit any misleading statements about their certifications.
- shall not use any certification documentation or parts thereof in a misleading manner or permit such use.
- shall not make or permit an implication that certification applies to activities outside the certification scope.
- keeps records of all complaints made known to it relating to compliance with the certification requirements and makes these records available to the Certification Body when requested.
- takes appropriate action with respect to such complaints and any deficiencies found in products that affect compliance with the requirements for certification.
- documents the actions taken.
- informs the Certification Body, without delay, of changes that may affect its ability to conform with the certification requirements.

3.2 Specific Methods

The goal of this section is to define specific methods to validate the prototypical system. The definition, development, implementation of tests and the verification of concepts depends greatly on the complexity of the system or subsystems to be analyzed and depends on the required effort to verify the requirements compliance. and is structured as following:

1. Identification of the TLOBU performance requirements
2. Define measuring metrics for the identified TLOBU requirements
3. Define tests for the identified TLOBU requirements
4. Establishment of a test procedure for the identified tests

3.2.1 Identification of the TLOBU performance requirements

Within this section an overview of the TLS performance requirements for the tests is given. This section takes input from the CLUG deliverables:

- [RD-7] D2.1 High-Level Mission Requirements Definition
- [RD-8] D2.2 Operational Scenarios
- [RD-9] D2.3 High Level System Requirements

Railways do not have a special requirement for duration of a specific operation like aviation or maritime, since generally it is very difficult to estimate a duration of railway operation. The identified requirements shall be met on all European rail environments including:

- meteorological environments according to [AD-11] EN50155 (including temperature variations, condensation, high rail temperature, low adherence conditions such as the presence of ice, snow, leaves, etc.

- physical environments (e.g., tunnels, mountains, underground stations, presence of metal masses around rail, forests, stations in urban areas, etc.)
- ionospheric and tropospheric conditions
- railway infrastructures (e.g., tunnels, bridges, concrete track, ballast track, etc.)

TLOBU solution is needed under all environmental conditions for a safe operation of the train. All normal events including but not limited to ionospheric scintillation, snow on tracks among others are considered as normal environmental conditions.

In order to apply GNSS for train localization, the GNSS performance properties need to be migrated to be identical with railway performance properties. The GNSS performance properties have been concluded as accuracy, continuity, availability, and integrity. The railway quality of service has been introduced as reliability, availability, maintainability, and safety.
In this section, the most fundamental performance requirements for the Train Localization Unit (TLOBU) from the initial project phase, are identified and collected under the Table 30.

According to the [RD-9] D2.3 "High level system requirements" for a fail-safe, multi-sensor train localization system, based on GNSS technology. During the operation, Minimum and Maximum Safe Front End positions can be used to trigger safety reactions, when required and if deemed necessary. Therefore, the performance requirements are identified using MCI (interval bounded by Minimum Acceptable Front End for Operations and Maximum Acceptable Front End for Operations).Hence the TLOBU shall provide the following safe and precise performance requirements.

The non-functional requirements are derived from using the applicable documents defined under chapter 2 the state of art. The TLOBU position terms and function names referred in the following Table 30 and in this document are described in the [RD-9] D2.3 "High level system requirements.

Note: When the confidence interval exceeds the MCI, the punctuality of operations may not be guaranteed anymore

Train Localization On-Board Unit Performance Requirements	
Parameter	**Value in Units**
Availability	
Safe position information (estimated, min and max front end) with an availability(within boundaries) of	≥ 99,998%
Safe velocity (estimated, min and max front end) Information with an availability (within boundaries) of	≥ 99,998%
Safe Acceleration information (estimated, min and max along track) with an availability (within boundaries) of	≥ 99,998%
Safe Heading (estimated, min and max front end) Information with an availability (within boundaries) of	≥ 99,998%
Safe Standstill (estimated, min and max front end) Information with an availability (within boundaries) of	≥ 99,998%
Reliability	

Train Localization On-Board Unit Performance Requirements		
Parameter	**Value in Units**	
The CLUG subsystem shall meet a total rate as a Reliability Target		
For all failures (incl. combined ones) leading to the "immobilizing" category at a total rate of	≤ 1.0E-6/h-	
For all failures (incl. combined ones) leading to the "operation impacting" category at a total rate of	≤ 4E-6/h	
For all failures (incl. combined ones) leading to the "operation transparent" category at a total rate of	≤ 1.5E-5/h	
Single component failures of CLUG subsystem leading to "immobilizing" or "operation impacting" category shall be classified as Reliability Critical Item.		
Maintainability		
The TLOBU design and maintenance concept shall meet Mean Time to Restore		
The system shall provide diagnosis information of each individual sensor component	MTTR ≤ 1 h	
Safety		
The TLOBU shall detect		
Detect a GNSS jamming attack within	Undefined value in [RD-9] refer to D5.8	
Detect a GNSS spoofing attack within	Undefined value in [RD-9] refer to D5.8	
Accuracy	**Precise**	**Normal**
Formal accuracy is a measure of the uncertainty of the estimates, according to the statistical characterization of the errors and the linear model used for the position estimate		
Position with an accuracy of (velocities lower or equal)	0.5 m. Distance run in 1sec if v = [40-600 km/h]	10 m. Distance run in 1sec if [36-600 km/h]
	The range depends on the length of the Track Edge and therefore no limits have been defined for the CLUG project	
Velocity with an accuracy of	○ 2 km/h for speed lower than 30km/h. ○ 1 km/h if v < 100 km/h ○ Linear increase up to 14 km/h at 600 km/h	

Train Localization On-Board Unit Performance Requirements	
Parameter	**Value in Units**
Along track estimated and safe acceleration with an accuracy of	Not quantified in the context of CLUG [RD-10]
Heading with (estimated Yaw, Pitch and Roll Angles)an accuracy of	Not quantified in the context of CLUG [RD-10]
Update Rate	
Safe position and confidence interval with a minimum update rate of	1/second
Safe Velocity and confidence interval with a minimum update rate of	1/second
Safe acceleration and confidence interval with a minimum update rate of	1/second
Latency	
Calculated safe front end position and confidence interval with a maximum latency	< 200 ms
Calculated safe accurate front-end position and confidence interval with a maximum latency	< 100 ms
Calculated velocity and confidence interval with a maximum latency	< 200 ms
Calculated acceleration (along -track) and confidence interval with a maximum latency	< 200 ms

Table 30: Train localisation on board unit requirements

For the test performance analysis several phases should be contemplated. These include the definition of the metrics to be employed in the performance analysis. The localization performance requirements are independent of any technical solution used. Combinations of different measurement technologies is expected to reach them. Based upon this context, the use case methodology is as follows:

- Analysing the Performance requirements for each of the use cases
- Analysis of use cases included the safety and operational criticality impact evaluation from a qualitative point of view
- Clustering the use cases in different performance profiles targeting similar performance localisation requirements and similar safety/operational criticalities.

The reliability assessment shall include:

- The possible modes of normal operation and of failure.
- The resulting effect on the considering the operating conditions.
- Failure detection capabilities and maintenance procedures; and
- The likelihood of the failure condition.

These performance requirements are analyzed for the testing under the consideration of the operational scenarios and environmental conditions defined in D2.2. These scenarios include standard situations, but also challenging environments and situations which might define design parameters and impact the key performance of the localization system. However, for the purpose of deriving test cases, individual operational scenarios and multiple environmental conditions and operations can be considered together.

Test cases are therefore to be derived by combination of operational scenarios in specific sequences (e.g.
standstill, acceleration, constant speed, and deceleration in a tunnel). The sum of all test cases shall then cover all individual operational scenarios, as far as possible.

3.2.2 Measuring metrics for the identified TLOBU requirements

The train localization on-board unit TLOBU is complex and susceptible to failures imposing large challenges for verifying that stringent accuracies and protection levels apply, as is largely acknowledged in the railway environment.

The Key Performance Indicators (KPI's) should be identified to measure the performance of the components and processes. For the TLOBU, the performance of the GNSS system delivering the position is critical along with additional sensors. This section clearly focuses on the measured variables and requirements for train location.

Performance requirements are generally stated as requirements on the outputs of a given system component, assuming that the other components feeding it with input information do respect their own performance requirements.

Standard for assessing GNSS performance in the context of Train transport systems are not ready currently. Therefore, the existing standards which are initially defined for other domains which provides identification and definitions of positioning performance features and metrics can be adopted accordingly.

The above goals have led to consider the following Key Performance Indicators with considering the requirements from the preliminary work and metrological, reliability-related and railway technical standards and conditions

- Position
- Speed
- Accuracy
- Reliability

Performance metrics are precise definition of the means of measuring a given performance feature of a given output of a system. This section provides the definition of the positioning metrics related to position, velocity, and speed from the existing standards.

At these performance profiles the probability of a hazardous train unit effect arising from the TLOBU shall be predicted to be not greater than 10^{-9}per Train Unit operating hour. There are a variety of challenges in this context:

- The stringent level
- system components behaviour
- physical characteristics of the system components
- characterisation of the errors affecting the system components
- proper detection and mitigation strategies of the errors

- realistic driving scenarios

Track selectivity is mandatory for all performance profiles, understanding track selectivity as the TLOBU ability to discern in which track the train is located. A more detailed information can be found in [RD-8] D2.2 operational scenarios

The [AD-22] standard CEN/EN 16803-1:2019, provides identification and definitions of positioning performance features and metrics. These need to match a certain operational scenario, i.e., the conditions in which the positing system is operating that may have an enormous impact on its performances. The following Table 31 : presents the definitions of potential metrics:

Output	Component	Accuracy Metric
Position	3D vector	3D position accuracy is defined as the set of three statistical values given by the 50th, 80thv and 95th percentiles of the cumulative distribution of the 3D position errors
	Horizontal	Horizontal position accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the horizontal position errors.
	East	East position accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the east position errors
	North	North position accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the north position errors
	Along-track	Along-track position accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the along-track position error
	Cross-track	Cross track position accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the cross-track position errors.
	Vertical	Vertical position accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the vertical position errors.
Velocity	3D vector	3D velocity accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the 3D velocity errors
	Horizontal	Horizontal velocity accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the horizontal velocity errors.
	East	East velocity accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the east velocity errors.
	North	North velocity accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the north velocity errors
	Along-track	Along-track velocity accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the along-track velocity errors.
	Cross-track	Cross-track velocity accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the cross-track velocity errors

Output	Component	Accuracy Metric
	Vertical	Vertical velocity accuracy is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the vertical velocity errors.

Table 31: Accuracy metrics according to DIN EN 16803-1:2019

Output	Component	Protection Level Performance Metric	Integrity Risk Metric
Position Protection Level	3D vector	3D position protection level performance for a given(e.g., 10^{-6}) 10^{-6}target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the 3D position protection levels computed for that target integrity risk.	The 3D position integrity risk is the probability that the 3D position error exceeds the 3D position protection level
	Horizontal	Horizontal position protection level performance for a given (e.g., 10^{-6}) target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the horizontal position	The horizontal position integrity risk is the probability that the horizontal position error exceeds the horizontal position protection level
	East	East position protection level performance for a given (e.g., 10^{-6}) target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the east position protection levels computed for that target integrity risk.	The east position integrity risk is the probability that the east position error exceeds the east position protection level.
	North	North position protection level performance for a given (e.g., 10^{-6}) target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the north position protection levels computed for that target integrity risk	The north position integrity risk is the probability that the north position error exceeds the north position protection level.
	Along-track	Along-track position protection level performance for a given (e.g., 10^{-6}) target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the along-track position protection levels computed for that target integrity risk.	The along-track position integrity risk is the probability that the along track position error exceeds the along-track velocity protection level.
	Cross-track	Cross-track position protection level performance for a given (e.g., 10^{-6})	The cross-track position integrity risk is the probability that the

Output	Component	Protection Level Performance Metric	Integrity Risk Metric
		target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the cross-track position protection levels computed for that target integrity risk	cross-track position error exceeds the cross-track velocity protection level
	Vertical	Vertical position protection level performance for a given (e.g., 10^{-6}) target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the vertical position protection levels computed for that target integrity risk.	The vertical position integrity risk is the probability that the vertical position error exceeds the vertical position protection level.
Velocity Protection Level	3D vector	3D velocity protection level performance for a given (e.g., 10^{-6}) target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the 3D velocity protection levels computed for that target integrity risk	The 3D velocity integrity risk is the probability that the vertical velocity error exceeds the 3D velocity protection level.
	Horizontal	Horizontal velocity protection level performance for a given (e.g., 10^{-6}) target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the horizontal velocity protection levels computed for that target integrity risk.	The horizontal velocity integrity risk is the probability that the vertical velocity error exceeds the horizontal velocity protection level
	East	East velocity protection level performance for a given (e.g.,10^{-6}) target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the east velocity protection levels computed for that target integrity risk.	The east velocity integrity risk is the probability that the vertical velocity error exceeds the east velocity protection level.
	North	North velocity protection level performance for a given (e.g., 10^{-6}) target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the north velocity protection levels computed for that target integrity risk.	The north velocity integrity risk is the probability that the vertical velocity error exceeds the north velocity protection level.
	Along-track	Along-track velocity protection level performance for a given (e.g., 10^{-6}) target integrity risk is defined as the set	The along-track velocity integrity risk is the

Output	Component	Protection Level Performance Metric	Integrity Risk Metric
		of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the along-track velocity protection levels computed for that target integrity risk.	probability that the vertical velocity error exceeds the along-track velocity protection level.
	Cross-track	Cross-track velocity protection level performance for a given (e.g., 10^{-6}) target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the cross-track velocity protection levels computed for that target integrity risk.	The cross-track velocity integrity risk is the probability that the vertical velocity error exceeds the cross-track velocity protection level
	Vertical	Vertical velocity protection level performance for a given (e.g.,10^{-6}) target integrity risk is defined as the set of three statistical values given by the 50th, 80th and 95th percentiles of the cumulative distribution of the vertical velocity protection levels computed for that target integrity risk.	The vertical velocity integrity risk is the probability that the vertical velocity error exceeds the vertical velocity protection level.

Table 32: Security metrics according to DIN EN 16803-1:2019

According to the [RD-14] localization working group of the EEIG ERTMS Users Group ‘Railways Localization System Localization Performance Requirements from use cases’ the localization Performance Requirements based on analysis of use cases and operational scenarios were adapted for CLUG’s TLOBU. Wherever necessary, the requirements have been expanded and made clearer by building on-top of the work already carried out in the EUG Localization Working Group.

Hence the associated train localization performance requirements associated to performance profiles are stated in the following tables i.e. Table 33, Table 34, Table 35 and Table 36 under consideration of the in D2.1 High-Level Mission Requirements defined four main performance profiles:

High Safety High Impact on Operations and Speed Dependent	
HHSD Front	
Description	Provide train front position and train speed (including direction) for track occupancy notification and for speed supervision.
Safety Critical	Yes
Mission critical	Yes
½ MCI	10 m for speed lower that 40 km/h then the distance run in 1 s at higher speed
Speed ½ MCI	2 km/h for speed lower than 30 km/h, then increasing linearly up to

	12 km/h at 500 km/h.
Operational Examples	Train control while running, speed supervision, train control in ATO
HHSD Rear	
Description	Provide train rear position for track occupancy notification.
Safety Critical	Yes
Mission critical	Yes
½ MCI	10 m for speed lower that 40 km/h then the distance run in 1 s at higher speed
Operational Examples	Track occupancy notification

Table 33 : Safety High Impact on Operations and Speed Dependent

High Safety High Impact on Operations and Precise Location)	
HHPLOC Front	
Description	Provide train front position and train speed (including direction) for track occupancy notification and for speed supervision in missions that require high accuracy at low
Safety Critical	Yes
Mission critical	Yes
Front Position ½ MCI	1m
speed ½ MCI	2 km/h for speed lower than 30 km/h
Operational Examples	Train control in parking areas, stopping, coupling
HHPLOC Rear	
Description	Provide train rear position for track occupancy notification at low speed and high accuracy
Safety Critical	Yes
Mission critical	Yes
Rear Position ½ MCI	1m
Operational Examples	Train control in parking areas,

Table 34: Safety High Impact on Operations and Precise Location

Low Safety High Impact on Operations and Precise Location	
LHPLOC Front	
Description	Provide train front position, train speed (including direction), train acceleration for ATO while the train is stopping at a platform
Safety Critical	No
Mission critical	Yes
Front Position 3 * SD	0.5 m
Speed SD	2 km/h
Acceleration SD	
Operational Examples	Parking in ATO, stopping in ATO, Guidance and control of the ATO
LHPLOC Rear (Low Safety High Impact on Operations)	
Description	Provide train rear position for ATO while the train is stopping.
Safety Critical	No
Mission critical	Yes
Rear Position SD	
Operational Examples	parking, stopping in ATO

Table 35: Safety Low Impact on Operations and Precise Location

LH Front	
Description	Provide train front position, and train speed (including direction) for TMS, passenger information and location-based services
Safety Critical	No
Mission critical	Yes
Front Position SD	10 m up to 40 km/h, distance run in 1 s at higher speed
Speed SD	2 km/h for speed lower than 30 km/h, then increasing linearly up to ± 12 km/h at 500 km/h.
Operational Examples	Location for passenger information system, input for the train management system, information for fleet management

LH Rear	
Description	Provide train end position for TMS, passenger information and location-based services.
Safety Critical	No
Mission critical	Yes
Rear Position SD	10 m up to 40 km/h, distance run in 1 s at higher speed
Operational Examples	Location for passenger information system, input for the train management system, information for fleet management

Table 36: Safety High Impact on Operations

3.2.3 Define tests for the identified TLOBU requirements and establish a test procedure for the identified tests

The above defined requirements and metrics for the TLOBU encompass many model assumptions which need to be verified in the areas of the performance key performance indicators (KPI) like the accuracy, the availability, the convergence time, the service coverage area, and the target integrity risk. The strategy is to conduct testing for these.

There are many alternative methods to characterize the TLOBU ’s performance. The TLOBU ’s testing can be performed according to the standards applicable in various domains in simulation mode with simulators, record and replay mode reproducing the test conditions, or field test according to test behavior specified.

To comply with EN 50126 (reliability, availability, maintainability, and safety; RAMS) standards, the demonstration of GNSS quality of service (QoS) should be evaluated in consistent with RAMS. As ascribed in section 2.1, Standard for assessing GNSS performance evaluation methods in the context of train localization are not ready. Therefore, the following test methods stated here are collection from various existing standards and the methodology is adjusted and enhanced for the needs for various TLOBU’s test use cases. The exposition and the format of the results mainly depend on the KPI analysis within the tests.

3.2.3.1 *CTP/QOS/1*

CTP/QOS/1	Availability of positioning solution
DUT Test Objective	To verify if the system is correctly operating at time t and service is available
Focus	Uninterrupted service
Test Definition	The availability of a PVT system is the percentage of time that the services of the system are usable. Availability is an indication of the ability of the system to provide a usable navigation service within a specified coverage area. Availability is a function of both the physical characteristics of the environment and the technical capabilities of the transmitter facilities. So, the characteristic of availability is defined as a

<table>
<tr><td></td><td colspan="3">percentage function. The characteristic of availability can be interpreted as:
Availability here describes the time PVT service is usable in relation to the total time within the specified coverage area</td></tr>
<tr><td><b>KPI</b></td><td colspan="3">○ TLOBU- 3D Position-Accuracy (true position)
○ TLOBU- Speed -Accuracy</td></tr>
<tr><td><b>CTP Reference</b></td><td colspan="3">○ EN 50126 [AD-01], [AD-02]
○ ETSI 103 246-1 [AD-23]
○ CEN 17475[AD-29]
○ Metrics assessed according to EN 16803[AD-22]</td></tr>
<tr><td><b>Performance Requirements</b></td><td colspan="3">The TLOBU shall meet an availability of 99,998% for service-affecting failures if service-affecting failures persist on average for operating hours.
The availability A(t) according to EN 50126 is a combination of reliability and maintainability. The safety attribute is not included in the railway availability even if both are dependent. If the system is correctly operating at time t, service is available.
○ Availability of GNSS SIS means the percentage the system is usable with a good signal reception environment
○ Availability of TLOBU locations is the percentage of the locations that are acceptable for train localisation in a defined test run.
System is said to be available when:
○ Accuracy requirements are met
○ PL < AL (if there is an alert limit requirement)</td></tr>
<tr><td rowspan="3"><b>PVT Requirements</b></td><td colspan="3">PVT Requirements Advisory for Railway Applications-Availability
According to [RD 17], GNSS Rail user forum</td></tr>
<tr><td>Train on High density Line</td><td>Train on Medium density</td><td>Train on low density line</td></tr>
<tr><td>&gt;99.98%</td><td>&gt;99.98%</td><td>&gt;99.98%</td></tr>
<tr><td><b>Background:</b></td><td colspan="3">The availability A(t) according to EN 50126 is a combination of reliability and maintainability. The safety attribute is not included in the railway availability even if both are dependent. If the system is correctly operating at time t, service is available.
The positioning system is available if services of the system are within the required limits. That is requirements for accuracy, integrity and continuity of service/ function are met. According to a RAM’S point of view, service is available if the system is correctly operating at time t. No requirement for successful operation at a specific moment of time is directly involved in GNSS availability. Besides there is also an effect to safety because unavailability causes the use of fault back modes which are not as safe as the normal operation and therefore the “average” safety of the system decreases.</td></tr>
</table>

Requirements	Availability requirements for signalling equipment results from safety and operational requirements for entire railway transport system. For example, if a system based on GNSS should replace ERTMS/ ETCS odometry, then unavailability less than $10^{-7}$is required. It means downtime for odometry subsystem should be less than 3.15 seconds per year. According to the GALILEO SoL service - Level A specification SIS should be available at 99.5% of time. It means that SIS for SoL Level A may not be available 43.8 hours per year. Note that possible SIS interruptions due to objects along track and landscape profile are not included in this specification of availability. In some cases, due to SIS shadowing mainly on urban or mountain lines, conditions for utilization of the GALILEO service can be much worse. A guarantee of EGNOS SIS service is much worse: it is not available at 5% of time, i.e., 438 hours per year, i.e., approximately 18 days.
Test description	
Test Dynamics	○ DYN
Test Mode	○ CS ○ WS ○ HS
Test Environment	○ GRES available in multi-frequency spectrum (L1+L2+L5) ○ SIM (optional) ○ LIV - Open Sky Railway Operational Environment - Restricted Railway Operational Environment - Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply ○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.
Quality Indicator	For applicable conditions see ETSI TS 103 246 -5 v1.3.1 (2020-10), chapter 5.3
Test Procedure	
1	Verify GNSS availability under different operating conditions considering street width, building heights and receiver location.
2	Synchronize the same timestamp of TLOBU location and reference location.
3	Calculate the deviation between TLOBU location and reference location.
4	Count the total samples of the measurement time as T.

5	Count the samples when there are deviations without zero sign.
6	Calculate the percentage of time a signal fulfils the above accuracy, integrity, and continuity criteria.
7	Calculate Availability(A) = MTTF/MTTF + F Whereas MTTF- as mean time to failure, F- as mean failure time
8	Repeat the test a number of times in order to draw statistics.
Required Inputs	○ reference location ○ reference location time ○ TLOBU location ○ TLOBU location time ○ Number of visible satellites ○ PDOP
Required Output	Availability (%)
Adjustment/Enhancement	The position authenticity is required for safe position information availability. So according to input CTP- Applicable References, this methodology can be adjusted, and enhanced for the needs of validating CLUG for Availability.
Test Result	Availability results will be presented in tables including percentage of valid position with respect to the total test time.
Pass Condition	
Availability Target	○ The CLUG subsystem shall meet a (asymptotical) mean intrinsic availability (A) ≥ 99.973%. ○ Position/Speed CI (Protection Level) < Position/Speed MCI (Alert limit)

3.2.3.2 CTP/QOS/2

CTP /QOS/2	**Reliability**
DUT Test Objective	To verify how reliable the TLOBU is in holding a GNSS signal and how able to perform as required without failure for an interval of time.
Focus	probability of a failure event over the mission time
Test Definition	The reliability of a PVT system is a function of the frequency with which failures occur within the system. It is the probability that a system will perform its function within defined performance limits for a specified period of time under given operating conditions. Formally, reliability is one minus the probability of system failure. The characteristic of reliability is also defined as a probability function. The mathematical interpretation for reliability characteristic is: Reliability = 1 - P(system/ failure)|specified function & time

KPI	○ Time to First Fix : TLOBU time begin tracking satellites and outputting data ○ Acquisition : the minimum signal level needed to obtain a PVT ○ Tracking Sensitivity: : the minimum power level needed to track and maintain a position fix ○ Reacquisition Time: the interval between the signal's reintroduction and the TLOBU re-establishing an acceptable position reading
CTP Test Reference	○ EN 50126 [AD-01], [AD-02]
Performance Requirements	According to the D2.1 Safety critical and mission critical performance profiles the TLOBU is a Safety Critical Part when operating at the HSHIO Speed Dependent and Precise Location Performance Profile. At these Performance Profiles the probability of a Hazardous Train Unit Effect arising from the TLOBU shall be predicted to be not greater than 10^{-9} per Train Unit operating hour. The reliability assessment shall include: ○ The possible modes of normal operation and of failure/degradation. ○ The resulting effect on the total rate target ≤ 1.0E-6/h for all failures cconsidering the operating conditions. ○ Failure detection capabilities and maintenance procedures; and ○ The likelihood of the failure condition.
GNSS Requirements	GNSS Requirements Advisory for train Localization Performance requirement According to [RD 17], GNSS Rail user forum Reliability_ failure rate < 2 *10^{-4} /hour
Background:	Reliability is required by railway RAMS and the definition is inherited from IEC 60050 as the ability of an item to perform a required function under given conditions for a given time interval. According to the Applicable reference 16 The characteristic of reliability can be denoted as R(T). R(T)=P(required function)|time interval & given condition. - Reliability of position determination R(t) is a measure of success and is a function of operation time interval (0, t). - Unreliability F(t) of provided service or function is a measure of failure in time interval (0, t). It represents PE exceeding AL or/ and a diagnostic failure. Unreliability F(t) is one complement of R(t). For non-safety applications the strict specification of operation time is not critical. For safety-related applications the operation (mission) time is specified. For the location function, the ERTMS Control/Command RAMS specifies the mission duration as 1 hour.

	Integrity measures the reliability of the information returned by the navigation system.
Reference Requirement	The ERTMS RAMS specification may indirectly lead to identification of such a time when specifying the maximum time for recognition of a component failure (5s). It can be expected that any active repair duration shall be in the same range (max. 5 s).
Test description	
Test Dynamics	○ STA (static) ○ DYN (dynamic)
Test Mode	○ CS (cold start) ○ WS (warm start) ○ HS (hot start)
Test System	○ GRES (GPS + GLONAS + Galileo + EGNOS)
Test Environment	○ SIM (simulated) ○ LIV (live) - Open Sky Railway Operational Environment - Restricted Railway Operational Environment - Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply ○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.
Operational Scenarios	○ Low Speed ○ High Speed ○ Acceleration ○ Standstill
Quality Indicator	○ DOP ○ Signal Level
Test Procedure	
1	Observe all possible system failure modes in the specified application and environment and the consequences of each failure mode
2	Determine the frequency of occurrence or the likelihood of each failure mode
3	Synchronize the same timestamp of reference location and TLOBU location
4	Calculate the deviation between TLOBU location and reference location
5	When timestamps of TLOBU locations are missing, mark a zero sign. It means a faulty state" measurement.
6	When the deviation > degraded state threshold, mark a zero sign. It also means a faulty state measurement

<table>
<tr><td>7</td><td colspan="3">When the HDOP > 6, mark a zero sign. It means a faulty state "measurement”</td></tr>
<tr><td>8</td><td colspan="3">Count each sample time span when there starts and ends with zero signs</td></tr>
<tr><td>9</td><td colspan="3">Count the numbers of the time spans in TTFi.</td></tr>
<tr><td>10</td><td colspan="3">Calculate mean time to failure (MTTF)
i.e., the individual time to failure (TTF) is estimated as
TTFi = tk − tj + 1/f (k > j,j _ 2).</td></tr>
<tr><td>11</td><td colspan="3">Calculate the mean value of the time spans according to mean time to failure (MTTF), this represents MTTF of a test.</td></tr>
<tr><td><b>Required Input</b></td><td colspan="3">○ reference location
○ reference location time
○ TLOBU location,
○ TLOBU location time
○ Number of visible satellites
○ PDOP</td></tr>
<tr><td><b>Required Output</b></td><td colspan="3">○ Mean Failure Time</td></tr>
<tr><td><b>Adjustment/Enhancement</b></td><td colspan="3">So according to input CTP Applicable Reference the methodology can be adjusted, and enhanced for the needs of validating CLUG for positioning</td></tr>
<tr><td><b>Test Result</b></td><td colspan="3">Reliability results will be presented in tables including percentage of valid position with respect to the total test time.</td></tr>
<tr><td colspan="4"><b>Pass Condition</b></td></tr>
<tr><td><b>Reliability Target</b></td><td>Category</td><td>Operation</td><td>Target [defined in RD 9}</td></tr>
<tr><td></td><td>1</td><td>Impacting</td><td>The CLUG subsystem’s design shall meet a total rate ≤ 4E-6/h for all failure (incl. combined ones)</td></tr>
<tr><td></td><td>2</td><td>Impacting</td><td>90% of the operation impacting failures (failure rate) shall not cause an additional delay ≥ 6 minutes to the train service</td></tr>
<tr><td></td><td>3</td><td>Transparent</td><td>The CLUG subsystem shall meet a total rate ≤ 1.5E-5/h for all failures</td></tr>
</table>

3.2.3.3 *CTP/QOS/3*

CTP /QOS/3	Maintainability
DUT Test Objective	To verify the performance of the TLOBU in terms of maintainability to measure the repair process including fault diagnosis, localization isolation plus repair or replacement
Test Definition	The probability that a given active maintenance action, for an item under given conditions of use can be conducted within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources. Maintainability is based on the idea that the system is repairable. So, the Mean Time to Repair (MTTR) is normally used to express the performance of maintainability. Normally, MTTR = 1/µ
KPI	○ Time to First Fix : TLOBU time begin tracking satellites and outputting data

	○ Reacquisition Time: the interval between the signal's reintroduction and the TLOBU re-establishing an acceptable position reading
CTP Reference	○ EN 50126 [AD-01], [AD-02] ○ IEC 61508 [AD-26]
Performance Requirements	Maintainability performance requirements influence: ○ Maintenance and repair policy associated with the GNSS sub-system. ○ GNSS subsystem availability requirements. ○ The current most severe requirements are derived from the ETCS FRS: • Maximum time to detect a module failure: 5 seconds • Maximum time to replace the module: 5 minutes • Maximum time to restart the system: 15 seconds ○ Maximum additional time to substitute a traction unit after a failure requiring maintenance in a workshop: 3 hours
GNSS Requirements	GNSS maintainability is operated by the master control station belonging to the control segment. From user segment, we cannot maintain GNSS.
Background:	The TLOBU shall be able to self-diagnose when accuracy targets are not fulfilled, and the relevant mitigation/measure shall be identified without affecting safety. Servicing information should cover maintenance details regarding servicing points, inspections, adjustments, tests, and replacements of components if required. MTTR is the basic measure of the maintainability of repairable items and represents the average time required to repair a failed component or device. Expressed mathematically, it is the total corrective maintenance time for failures divided by the total number of corrective maintenance actions for failures during a given period of time
Requirements	○ For safety related applications the service interrupt threshold shall be no longer than the requirement for detection of the TLOBU failure.
Test description	
Test Dynamics	○ STA (static) ○ DYN (dynamic)
Test Mode	○ CS (cold start) ○ WS (warm start) ○ HS (hot start)
Test System	GRES (GPS + GLONAS + Galileo + EGNOS)
Test Environment	○ SIM (simulated, optional) ○ LIV (live) - Open Sky Railway Operational Environment - Restricted Railway Operational Environment - Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply

	○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.
Operational Scenario	- Low Speed - High Speed - Acceleration - Standstill
Test Procedure	
1	Verify that TLOBU set to receive GNSS Signals
	Measure the time between the point at which a downing event is first discovered until the point at which the GNSS satellites return to normal operating condition
2	Calculate the Mean Time to Restore (MTTR)
3	$MTTR = Total\ Actual\ Downtime\ (hrs)/Total\ Satellite\ Outages\ (number)$
4	Calculate Mean Repair Time
	Calculate Mean Down Time
Adjustment/Enhancement	So according to CTP Applicable References, the methodology can be adjusted, and enhanced for the needs of validating CLUG for positioning
Required Output	Restoration Time
Test Result	Maintainability results will be presented in tables including mean time to restore, mean repair time mean time to maintain with respect to the total test time.
Pass Condition	
Maintainability Target	The CLUG subsystem’s design and maintenance concept shall meet a Mean Time to Restore (MTTR) ≤ 1 h

3.2.3.4 *CTP/QOS/4*

CTP /QOS/4	**Safety**
DUT Test Objective	To verify the performance of the TLOBU in the terms of safety specifications with safety evaluation and verification process using GNSS performing the main localization function and also obeying the safety requirements.
Focus	the actual risk is below the acceptable risk
Test Definition	The necessity to estimate safety quantitatively calls for the safety function and safety integrity level definitions in EN 50129, i.e., Freedom from unacceptable risk of harm
KPI	○ Safety integrity ○ Time to First Fix: TLOBU time begin tracking satellites and outputting data ○ TLOBU- 3D Position -Accuracy true position) ○ TLOBU- Speed -Accuracy
CTP Reference	o EN 50126 [AD-01], [AD-02] o EN 50128 [AD-03]

<table>
<tr><td></td><td>○ EN 50129 [AD-04]
○ IEC 61508 [AD-26]</td></tr>
<tr><td><b>Performance Requirements</b></td><td>Safety Analysis can be conducted from the point of view of the user, identifying a Tolerable Hazard Rate (THR) for the function to be performed by the GNSS Location Subsystem.

From the point of view of the provider, a SIL is allocated to the different sub-functions and components, analyzing causes of failure for each of them and proposing mitigation strategies.

Safety assessment needs to identify the hazard and also the risk of the localization unit, particularly the safety integrity level needs to be allocated:
○ Tolerable Hazard Rate and SIL Relation
<table>
<tr><th>Tolerable Hazard Rate (THR)</th><th>Safety Integrity</th></tr>
<tr><td>$10^{-9} \leq THR < 10^{-8}$</td><td>4</td></tr>
<tr><td>$10^{-8} \leq THR < 10^{-7}$</td><td>3</td></tr>
<tr><td>$10^{-7} \leq THR < 10^{-6}$</td><td>2</td></tr>
<tr><td>$10^{-6} \leq THR < 10^{-5}$</td><td>1</td></tr>
<tr><td>$THR \geq 10^{-5}$</td><td>0</td></tr>
</table></td></tr>
<tr><td><b>GNSS safety related Requirements</b></td><td>GNSS Requirements Advisory for Railway Applications
According to [RD 16] Rail advisory forum requirements
○ GNSS SoL service performance
○ EGNOS SoL service performance
<table>
<tr><th></th><th>Train on High density Line</th><th>Train on Medium density</th><th>Train on low density line</th></tr>
<tr><td>Time to Alarm (sec)</td><td>&lt;1.0</td><td>&lt;1.0</td><td>&lt;1.0</td></tr>
<tr><td>Alarm Limit (m)</td><td>2.5</td><td>20</td><td>50</td></tr>
</table></td></tr>
<tr><td><b>Background</b></td><td>The safety concept of railway has a significant impact on terms of safety and integrity that normally defines the hazard rate in the time span of one hour.
The safety integrity is defined as the likelihood of a system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

○ w.r.t to localisation, railway domain concerns more horizontal accuracy.</td></tr>
</table>

	○ Different environments are analysed for the safety integrity property, GNSS parameters such as number of visible satellites and Dilution of Precision (DOP) are inputs for the evaluation ○ Among the different environments, two environmental scenarios such as safe and dangerous failures of GNSS for train localisation and the corresponding safety integrity level are considered. ○ To apply GNSS for train localisation, the safety aspects of these environments need to be analysed individually For safety, the decision choice failures can be categorized as : ○ dangerous failures ○ safe failures - The safe failures, whether detected or undetected, have no influence on the technical safety function. - Dangerous failures in the safety function lead on the other hand to a dangerous state of the system. - The detection failure probability analysed in the time interval can be expressed as failure rate. - Safety integrity is the summary of all the related characteristics: hazard rate, alarm limit, time to alarm, as well as protection limit
Reference Requirement	○ TLOBU ability to receive TLOBU's PVT in required time limit ○ TLOBU's successful indication of GNSS localisation deviation under required value. ○ Self-diagnosis of the localisation unit, the integrity information, whether the data can be trusted or not ○ GNSS information being accurately one after another as the time sequence and successfully matched the map.
Test description	
Test Dynamics	○ STA (static) ○ DYN (dynamic)
Test Mode	○ CS (cold start) ○ WS (warm start) ○ HS (hot start)
Test System	○ GRES (GPS + GLONAS + Galileo + EGNOS)
Test Environment	○ SIM (simulated) ○ LIV (live) - Open Sky Railway Operational Environment - Restricted Railway Operational Environment - Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply ○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model

	According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.
Operational Scenario	○ Low Speed ○ High Speed ○ Acceleration ○ Standstill
Test Procedure	
1	Identify the dangerous failures with consideration of the environmental scenarios.
2	The dangerous failure rate evaluation process is environmental scenarios related
3	Select a railway related environment
4	Mark the starting point of the environment and the end point of the environment
5	Synchronize the same timestamp to both TLOBU location and reference location.
6	Calculate the deviation between TLOBU location and reference location
7	Identify the clip of the GNSS receiver location inside the environmental scenario
8	Calculate the time of this environmental scenario as Ti.
9	Calculate the dangerous failure number in this test run
10	Calculate the number of dangerous failures in this test run.
11	Repeat the process with n times of test in this environmental scenario.
12	Estimate the dangerous failure rate in this environmental scenario
13	Dangerous failure rate per hour per train localization function in an environment is estimated as: $\frac{\text{dangerous failure numbers per environment}}{\text{samples per environment})/(\text{sampling rate})}$
Adjustment/Enhancement	So according to input CTP Applicable References the methodology can be adjusted, and enhanced for the needs of validating CLUG for Positioning
Required Output	○ hazard rate ○ horizontal accuracy
Test Result	Safety Results will be presented in tables including THR, SIL level with dangerous failure rate per hour per train localisation with respect to the total test time.
Pass Condition	
Safety Target	The TLOBU shall comply to the safety requirements (incl. TFFR) defined to each function.

3.2.3.5 *CTP/QOS/5-Optional*

Continuity and reliability properties are related to their definitions. Continuity is required by GNSS performance as the ability of the total system to perform its function without interruption during the intended operation as it is evident from railway RAMS standard [AD-01] and [AD-02], no continuity requirement is needed for railway safety systems. Hence the following CTP /QOS/5 need not to be followed but as Continuity of position is important, because in the future systems number Balise systems reduced, the train systems.

CTP /QOS/5	Continuity
DUT Test Objective	To verify the performance of the TLOBU in the terms of Continuity
Test Definition	The continuity of a system is the ability of the total system (comprising all elements necessary to maintain the TLOBU position within the defined railway environment) to perform its function without interruption during the intended operation. Continuity is defined as the ability of the total system, which is represented by the probability of a function. Mathematically the characteristic of continuity is defined as: Continuity = P(maintained system performance)Phase of operation & duration
KPI	○ TLOBU- 3D Position-Accuracy (true position)

<table>
<tr><td></td><td>○ TLOBU- Speed -Accuracy</td></tr>
<tr><td><b>CTP Reference</b></td><td>○ EN 50126 [AD-01], [AD-02]
○ EN 50128 [AD-03]
○ EN 50129 [AD-04]
○ IEC 61508 [AD-26]
○ CEN 17475 [AD-29]</td></tr>
<tr><td><b>Performance Requirements</b></td><td>continuity is defined in an intended operation which also has a time constraint. continuity is related to detected failures</td></tr>
<tr><td><b>GNSS Requirements</b></td><td>GNSS Requirements Advisory for Railway Applications-Availability
According to [RD 17], GNSS Rail user forum
<table>
<tr><td>Train on High density Line</td><td>Train on Medium density</td><td>Train on low density line</td></tr>
<tr><td>&gt;99.98%</td><td>&gt;99.98%</td><td>&gt;99.98%</td></tr>
</table>
GNSS Performance Requirements
○ Continuity Risk $1 * 10^{-4}/h$ to $1 * 10^{-8}/h$</td></tr>
<tr><td><b>Background</b></td><td>Continuity for a healthy GNSS SIS is the probability that the GNSS SIS will continue to be healthy without unscheduled interruption over a specific time interval.
According to railway standards, and currently in both GNSS the continuity is always used instead of reliability. GNSS performance also includes continuity risk and protection limit. The continuity property is stated by all requirements. The characteristic for continuity is the continuity risk.
Continuity risk is the probability that the system will not provide guidance information with the accuracy and the integrity required for the intended operation
The Horizontal Protection is the radius of a circle in the horizontal plane (the local plane tangent to the WGS-84 ellipsoid), with its center being at the true position, which describes the region assured to contain the indication horizontal position
The continuity can also be decomposed identically with the reliability definition into three elements as:
○ perform a required function
○ without interruption
○ during the intended operation</td></tr>
<tr><td colspan="2"><b>Test description</b></td></tr>
<tr><td><b>Test Dynamics</b></td><td>○ STA (static)
○ DYN (dynamic)</td></tr>
<tr><td><b>Test Mode</b></td><td>○ CS (cold start)
○ WS (warm start)
○ HS (hot start)</td></tr>
<tr><td><b>Test System</b></td><td>○ GRES (GPS + GLONAS + Galileo + EGNOS)</td></tr>
<tr><td><b>Test Environment</b></td><td>○ SIM (simulated)
○ LIV (live)
- Open Sky Railway Operational Environment
- Restricted Railway Operational Environment</td></tr>
</table>

	- Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply ○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.
Operational Scenario	- Low Speed - High Speed - Acceleration - Standstill
Test Procedure	
1	No test required
	This eventuality is covered by CTP /QOS/2
	Conduct test CTP /QOS/2
Enhancement	For the certification of GNSS solutions for safety-related applications, railway standards have to prove that, even in case of failures, the system studied is able to guarantee a given level of performances expressed in the railway domain in terms of RAMS attributes (Reliability, Availability, Maintainability and Safety) As it is evident from railway RAMS standard, no continuity requirement is needed for railway safety systems. Railways do not have a special requirement for duration of a specific operation like aviation or maritime, since generally it is very difficult to estimate a duration of railway operation. Furthermore, in case of continuity it is difficult to specify „the most critical phase" of railway operation, as it was done for aeronautical operations in airport in particular airspace without interruption of operation. Continuity requirement significantly determine cost of navigation system due to its parameters constrain. It is one of the most demanding quality measures of satellite system. Railway sector should declare how the continuity measure should be correctly used for safety application (as no continuity requirement needed for railway) and how much the continuity requirement service meets the railway needs .As in case of safety applications of GNSS it is necessary to consider continuity of Accuracy, Continuity of Integrity of Accuracy, and both Continuity of Service /Function which impacts the scope of CLUG.
Pass Condition	
	○ Pass CTP /QOS/2 ○ MCI (PL>AL)

3.2.3.6 RAMS and GNSS Performance Properties to Train Localization Unit (TLOBU)

The performance of GNSS for the TLOBU can be treated as the combination of both GNSS and RAMS performance properties. In order to apply GNSS for the TLOBU, the GNSS performance properties need to be migrated to be identical with railway performance properties.

The TLOBU'S, availability, reliability, maintainability, safety, and continuity are required by GNSS performance, and the characteristic values are all based on the accuracy performance properties. Hence the GNSS performance tests are as follows:

3.2.3.7 CTP/PP/1.1

CTP/PP/1.1	**Conformance of Position Authenticity**
Related QOS	Availability
Test Objective	To authentic GNSS signals, in order to deceive the TLOBU into erroneously estimating pseudo-ranges and computing false PVT solutions
Test Purpose	to verify the performance of the GBLS in: 1) avoiding false alarms under nominal GNSS signal conditions and no interfering signals (Clear scenario). 2) detecting a spoofing attack (Threat scenario 9)

Metrics	○ Probability of false alarm (PFA) ○ Probability of detection (PD) of spoofing attack
Performance Requirements	The TLOBU shall meet a requirement for PFA and PD (probability of direction of spoofing attack) in both the test dynamics and operational scenarios The position authenticity performance is defined by the ability of TLOBU to provide authentic positioning data via - processing true GNSS signals to detect spoofing - detection of false GNSS signals intentionally transmitted to TLOBU
Test Reference	○ ETSI TS 103 246-3 v1.3.1[AD-23] ○ ETSI TS 103 246-5 v1.3.1[AD-23]
Background:	Position Authenticity gives a level of assurance that the data for a location target has been derived from real signals relating to the location target. - Probability that the TLOBU falsely detects spoofed GNSS signals when there is no RF spoofing attack - Probability that the TLOBU detects spoofed GNSS signals during an RF spoofing attack
Requirements	According to [RD 6], the TLOBU shall comply to the requirements to provide safety relevant communication between safety relevant equipment that is connected to a transmission system. According to CLUG System requirements in D2.3, the TLOBU should inform the consumers if it was able to detect a GNSS spoofing attempt directed towards it.
Test description	
Test Dynamics	○ STA (static) -location ○ DYN (dynamic) -Moving location
Test Mode	○ CS (cold start) ○ WS (warm start) ○ HS (hot start)
Test System	○ GRES (GPS + GLONAS + Galileo + EGNOS)
Test Environment	○ SIM (simulated) ○ LIV (live) - Open Sky Railway Operational Environment - Restricted Railway Operational Environment - Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply ○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.

Operational Scenario	○ Clear scenario: avoiding false alarms under nominal GNSS signal conditions and no interfering signals ○ Interference scenario: detecting a spoofing attack
Quality Indicator	○ PDOP ○ Signal Level
	Test Procedure
1	Generate the operational scenario in both the test environment and dynamics
2	Start the GNSS scenario with location target at a random point within a 3 km radius of the reference location with an altitude randomly between 0 and 500 m to continue moving along the trajectory
3	scenario start time shall be randomly delayed by 0 to 30 s from start time
4	Collect 1000 authentication data samples at the output of the TLOBU at intervals of 1 s
5	If statistically independent authentication data measurements cannot be guaranteed at 1 s sample intervals, this interval shall be increased to 30 s.
6	Calculate Probability of false alarm (PFA) with measurement data collected as in % $PFA = \frac{N_k}{K}.100$ Where N_k is number of authentication data detections collected Where K is total number of observations.
7	Set the RF spoofer to generate false GNSS signals
8	Repeat the steps from 1 to 6
9	Calculate Probability of detection (PD) with measurement data collected as in % $PD = \frac{N_D}{K}.100$ Where N_D is the number of authentication data detections collected
10	Verify the latency to provide authenticity shall not exceed 5 s.
11	Repeat the test a number of times in order to draw statistics.
Adjustment/Enhancement	So according to input Applicable References ETSI 103 246 series standards, the defined standard methodology can be adjusted and enhanced for the needs of validating CLUG for Position Authenticity w.r.t Availability.
Required Output	○ TLOBU- PVT data
Test Result	Position authenticity results will be presented in tables including is number of authentication data detections with respect to the total number of observations.
	Pass Condition
Target	“pass" for each metric is if:

	- calculated Probability of False Alarm is lower than the values of Probability of False Alarm defined for TLOBU - calculated Probability of Detection is higher than the values of Probability of Detection defined for TLOBU

3.2.3.8 CTP/PP/1.2

CTP/PP/1.2	**Conformance of Position Integrity**
Related QOS	Availability
Test Objective	To verify the position integrity performance of the GBLS i.e., TLOBU
Test Purpose	The purpose of this test is to verify the Position Integrity performance of the TLOBU in terms of: - Horizontal Protection Level (HPL) expressed as the horizontal position error (HPE) at 95 %; and - Integrity Risk expressed as the probability that the position error exceeds the HPL.
Performance Requirement	The integrity performance is defined by: - The Position Integrity expressed in terms of Protection Level expressed in metres at 95th percentile. - The Integrity Risk, expressed as the probability that the position accuracy exceeds the position protection level.
Test Reference	○ ETSI TS 103 246-3 v1.3.1[AD-23] ○ ETSI TS 103 246-5 v1.3.1[AD-23]
Background:	Position Integrity is the ability of the TLOBU to measure the trust that can be placed in the accuracy of the location target position. It is relevant to Safety- and Liability here undetected large position errors can generate legal or economic consequences. It is expressed

	through the computation of a protection level associated to a predetermined integrity risk In terms of integrity algorithms, they can be based on Receiver Autonomous Integrity Monitoring (RAIM), on ground monitoring approach with a GNSS integrity channel (GIC, e.g., EGNOS) or a combination of them
Requirements	This integrity risk associated to the Protection Level on along-track position and along-track speed domains is 5×10^{-10}/h for each
Test description	
Test Dynamics	○ STA (static) -location ○ DYN (dynamic) -Moving location
Test Mode	○ CS (cold start) ○ WS (warm start) ○ HS (hot start)
Test System	○ GRES (GPS + GLONAS + Galileo + EGNOS)
Test Environment	○ SIM (simulated) ○ LIV (live) - Open Sky Railway Operational Environment - Restricted Railway Operational Environment - Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply ○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.
Operational Scenario	Integrity threat scenarios are: ○ Non-LoS (Line of Sight) tracking. ○ Pseudo-range Ramp errors.
Test Procedure	
1	Generate the operational scenario in both the test environment and dynamics
2	Start the GNSS scenario with location target at a random point within a 3 km radius of the reference location with an altitude randomly between 0 and 500 m
3	Collect consecutive TLOBU horizontal position reports and calculate the horizontal position error (HPE).
4	Stop GNSS scenario and TLOBU after a running time of 24 hours (because of the periodicity of integrity threats)
5	Calculate, the HPL value as the cumulative 95 percentile of the HPE distribution

6	Calculate, the Integrity Risk as the cumulative probability of HPE being greater than HPL
Adjustment/Enhancement	So according to input Applicable References ETSI 103 246-series and as here the TLOBU is a Ground based localization unit, this test can be adapted, and the methodology can be adjusted and enhanced for the needs of validating CLUG for Position Integrity.
Required Output	TLOBU- PVT data
Test Result	Position Integrity results will be presented in tables including probability of HPE with respect to the success rate
Pass Condition	
Target	"pass" for metric is if: ○ Protection Level in metres(xx) at 95 percentiles ○ If position error does not exceed the position protection level

3.2.3.9 *CTP/PP/1.3*

CTP/PP/1.3	**Conformance Test for Resilient PVT (GNSS Interference)**
Related QOS	Availability
Test Objective	To verify if the TLOBU is able to detect a GNSS spoofing and jamming attacks
Test Purpose	The purpose of this test is to verify the Performance of TLOBU in terms of the maximum Jammer-to-GNSS signal power ratio (J/S) at TLOBU antenna that allows a position fix.
KPI	○ Accuracy's ○ Availability
Performance Requirement	○ Position fix accuracy (horizontal) with degradation under interference conditions ○ Position fix availability as a function either of the jammer distance or the jamming-to-GNSS signal power ratio (J/S) ○ The performance of TLOBU can be determined by the interference power it tolerates for a given Horizontal accuracy error and not directly by the error resulting from the interference power.
Test Reference	○ ETSI TS 103 246-3 v1.3.1[AD-23] ○ ETSI TS 103 246-5 v1.3.1[AD-23] ○ EN 50126 [AD-01], [AD-02]

Background:	Resilient against interference characterizes the ability of the TLOBU to operate under interference conditions and maintain an appropriate level of performance in terms of PVT degradation. Resilient against is the PVT degradation caused by interference sources and is defined in terms of: ○ increase of the horizontal position error ○ decrease of availability of the position fix The robustness to interference is characterized by the maximum tolerable J/S, which is defined as that providing a position fix availability greater than 90 % with a maximum horizontal error of 100 m. The horizontal position error statistics provided are based on position fixes satisfying the condition of a maximum horizontal error of 100 m. J/S (dB) characterize the interference power applied to the TLOBU and are expressed in term of Jamming to Signal Ratio. Maximum Horizontal Position Error (m) values characterize the GBLS maximum Horizontal accuracy error that can be tolerated when applying the corresponding J/S to the TLOBU.
Requirements	○ TLOBU might be required to operate in RF environments subject to interference, in the GNSS frequency bands. ○ The TLOBU shall inform the consumers if it was able to detect a GNSS spoofing attempt directed towards it. ○ The TLOBU shall be able to detect GNSS jamming attacks directed towards it and inform the consumers of the same. GNSS spoofing and jamming impact TU's safety and detection is necessary to minimize the consequences of failure of accuracy and integrity targets would have on the TLOBU consumers. The [AD-02] is important for design and verification of railway safety related systems. With onboard localization technology, trains communicate their location, length, acceleration, and velocity together with a confidence interval that respects a certain probability determined by the confidence level, i.e., SIL4. In other words, an estimated position, velocity, and acceleration comes with a confidence interval for a given hazard rate. Safety integrity requirements often have to be apportioned from the higher level to the related functions at the lower subsystems. This has to be done very carefully, and the respective rules must be followed. From the input [AD-02], those rules are laid down in EN 50126-2. This standard is valid for all application areas of railways, which are signalling, rolling stock, and fixed installations.
Test description	
Test Dynamics	○ STA (static) -location ○ DYN (dynamic) -Moving location

Test Mode	○ CS (cold start) ○ WS (warm start) ○ HS (hot start)
Test System	○ GRES (GPS + GLONAS + Galileo + EGNOS)
Test Environment	○ SIM (simulated) ○ LIV (live) - Open Sky Railway Operational Environment - Restricted Railway Operational Environment - Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply ○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.
Operational Scenario	○ Open Area - Railway Environment
Quality Indicator	- HDOP and PDOP ○ Signal Level
Test Procedure	
1	Generate the operational scenario in both the test environment and dynamics
2	Start the GNSS scenario with location target at a random point within a 3 km radius of the reference location with an altitude randomly between 0 and 500 m to continue moving along the trajectory
3	Scenario start time shall be randomly delayed by 0 to 30 s from start time
4	Configure the Interference Generator to achieve the lowest J/S
5	Start the TLOBU in Cold Start and wait for the first position fix.
6	Collect consecutive position reports, with one good result and bad result and its J/S value
7	Calculate, the Integrity Risk as the cumulative probability of HPE being greater than HPL
8	Repeat the test a number of times in order to draw statistics
9	Stop the testing if Jammer power has achieved the maximum J/S
Adjustment/Enhancement	So according to input Applicable References ETSI 103 246-series standard, the following methodology can be adjusted, and enhanced for the needs of CLUG positioning for Safety w.r.t GNSS Spoofing and Jamming.
Required Output	○ TLOBU- PVT data ○ Jamming Signal Level

Test Result	Resilient against Interference results will be presented in tables including horizontal position error, position fix, with maximum tolerable J/S, and maximum Jammer distance.
Pass Condition	
Target	"pass" for metric is if: ○ statistical requirements of a 95 % success rate record a Pass ○ otherwise record a Fail at the snooted J/S level ○ maximum tolerable error is 100 m whatever is the applied J/S.

3.2.3.10 CTP/PP/2.1

CTP/PP/2.1	**Conformance Test for Time to First Fix**
Related QOS	Reliability
Test Objective	To verify the performance of TLOBU in terms of TTFF within a given positional accuracy.
Test Purpose	The purpose of this measurement is to evaluate how quickly the TLOBU can obtain a first position fix.
KPI	○ Accuracy ○ Time to fix
Performance Requirement	○ The TTFF is an important performance parameter since it strongly impacts the usability of the TLOBU
Test Reference	○ ETSI TS 103 246-3 v1.3.1[AD-23] ○ ETSI TS 103 246-5 v1.3.1[AD-23] ○ EN 50126 [AD-01], [AD-02]
Background:	The TTFF is evaluated in terms of response time of the TLOBU. The response time is defined as the time starting from the moment that the GNSS sensor is reset (Autonomous Cold start) to the time of issue of the TLOBU measurement report containing the first position estimate. TTFF is the time taken by the TLOBU to provide location-related data, starting either from the reception of a request, or from

	another triggering event (for instance for periodic or geo-dependent reporting). ○ The TTFF is defined for a cold-start condition, defined as the TLOBU having: ○ no prior information such as ephemeris, almanac, time, position available on unit ○ inaccurate estimates of its position, velocity, and time; or ○ inaccurate positions of any of the GNSS satellites. ○ In this case, the TLOBU will systematically search for all satellites For the Cold start mode with assistance ○ Max time error: the time difference between the GNSS time provided in assistance data and the real GNSS time. ○ Max Position error: the difference between the estimated position of the receiver provided by the assistance server and the real position of the receiver
Requirements	According to D2.1 "High-Level Mission Requirements Definition, the train has to continue the commercial operation until the end of service. Hence this TTFF test is required for verification.
Test description	
Test Dynamics	○ STA (static) -location ○ DYN (dynamic) -Moving location
Test Mode	○ Assisted cold start with fine time assistance. ○ Assisted cold start with coarse time assistance. ○ Cold start without assistance.
Test System	○ GRES (GPS + GLONAS + Galileo + EGNOS)
Test Environment	○ SIM (simulated) ○ LIV (live) - Open Sky Railway Operational Environment - Restricted Railway Operational Environment - Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply ○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.
Quality Indicator	○ PDOP ○ Signal Level
Test Procedure	
1	Verify that TLOBU set to receive GNSS Signals

<table>
<tr><td>2</td><td>Generate the operational scenario in both the test environment and dynamics</td></tr>
<tr><td>3</td><td>Start the GNSS scenario with location target at a random point within a 3 km radius of the reference location with an altitude randomly between 0 and 500 m to continue moving along the trajectory</td></tr>
<tr><td>4</td><td>Scenario start time shall be randomly delayed by 0 to 30 s from start time</td></tr>
<tr><td>5</td><td>Start the TLOBU from a "cold-start" state: the TLOBU GNSS sensor shall discard any stored GNSS reference time, location, and any other assistance data obtained or derived during a previous test instance (e.g., expected ranges and Doppler)</td></tr>
<tr><td>5</td><td>Delete all position, velocity, time, almanac, and ephemeris data from the TLOBU</td></tr>
<tr><td>6</td><td>By means of a stopwatch, measure time interval between signal start and the first navigation solution result.</td></tr>
<tr><td>7</td><td>Repeat the test 10 number of times in order to draw statistics.</td></tr>
<tr><td>8</td><td>Calculate average time to first fix in cold start mode based on measurements</td></tr>
<tr><td><b>Adjustment/Enhancement</b></td><td>Using references ETSI 103 246-series, defined standard methodology can be adjusted and enhanced for the needs of CLUG positioning for Safety w.r.t Reliability</td></tr>
<tr><td><b>Required Output</b></td><td>○ TOBLU- PVT data
○ Satellites in View</td></tr>
<tr><td><b>Test Result</b></td><td>○ Time to first fix results will be presented in tables including average and maximum values</td></tr>
<tr><td colspan="2"><b>Pass Condition</b></td></tr>
<tr><td><b>Time to first fix Target</b></td><td>“pass" for metric is if:
○ the horizontal and vertical position errors, calculated from the difference between the measured and true position, are less than 100 m
<table>
<tr><td rowspan="3">Average Values of Time to First Fix
[TTFF]</td><td>Does Not Exceed</td><td>For Signal Value</td></tr>
<tr><td>60 Seconds</td><td>-130dBm</td></tr>
<tr><td>300 Seconds</td><td>-140 dBm</td></tr>
</table>
</td></tr>
</table>

3.2.3.11 CTP/PP/2.2

CTP/PP/2.2	**Conformance Test of Acquisition**
Related QOS	Reliability
Test Objective	To verify the Performance of TLOBU in terms of acquisition
Test Purpose	The purpose of this test is to measure the TLOBU acquisition performance with a set of GNSS signals
KPI	○ Accuracy ○ Time to first fix ○ Sensitivity
Performance Requirement	○ Acquisition tests shall be executed for all the start modes permitted by the TLOBU
Test References	o ETSI TS 103 246-3 v1.3.1 o ETSI TS 103 246-5 v1.3.1 o EN 50126ss
Background:	Acquisition defines the minimum level of satellite signal power for TLOBU to acquire the signal and keep hold of it. Many conditions affect the power level of already-weak satellite signals including other electrical noise in the environment and it is important to know which conditions TLOBU will cope with, and which it will not. Acquiring a signal is more difficult than maintaining one due to low GNSS signal levels, so a simulator, of accuracy many factors greater than the device under test, is needed to achieve precise signal attenuation at low dB levels.

Requirements	According to the D2.3 System requirements, The TLOBU shall reach full operational capability including for safety-related applications within 600 s after powering up and able to initialize itself and provide the localization report for safety applications also when no initial position and track ID is provided as an input
Test description	
Test Dynamics	○ STA (static) -location ○ DYN (dynamic) -Moving location
Test Mode	○ CS (cold start) ○ WS (warm start) ○ HS (hot start)
Test System	○ GRES (GPS + GLONAS + Galileo + EGNOS)
Test Environment	○ SIM (simulated) - Open Sky Railway Operational Environment - Restricted Railway Operational Environment - Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply ○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.
Quality Indicator	○ PDOP ○ Signal Level
Test Procedure	
1	Verify that TLOBU set to receive GNSS Signals
2	Generate the operational scenario in both the test environment and dynamics
3	Start the GNSS scenario with location target at a random point within a 3 km radius of the reference location with an altitude randomly between 0 and 500 m to continue moving along the trajectory
4	Scenario start time shall be randomly delayed by 0 to 30 s from start time
5	Increase the power by steps in order to determine at which power level the TLOBU is able to gain a fix within the timeout
6	Set the (in simulation mode) the minimum signal level to -170dBm for the most powerful satellite For other satellites decrease the power by steps of 1.5dB for a duration of 5 minute or less in case a position fix achieved.
7	Repeat the above steps for a power level step of 3dB in Cold/Hot/warm start modes.
8	Test is repeated a number of times in order to draw statistics
Adjustment/Enhancement	So according to input Applicable Reference ETSI 103 246-series standard, the following methodology can be adjusted, and enhanced for the needs of CLUG positioning for accuracy
Required Output	TLOBU- PVT data, Satellites in view

Test Result	The Acquisition results will be presented in tables including Mean power level for a valid fix (and standard deviation), mean positioning error at the first fix (and standard deviation) ,Mean time to first fix (and standard deviation)
Pass Condition	
Acquisition Target	“pass" for metric is if: ○ at dedicated power level the TLOBU is able to gain a fix within the timeout.

3.2.3.12 CTP/PP/2.3

CTP/PP/2.3	**Conformance Test of Sensitivity**
Test Parameter	Reliability
Test Objective	To verify the performance of TLOBU in terms of maximum masking (attenuation) values tolerated by the TLOBU whilst still allowing the provision of location-related data in cold start mode, tracking mode and reacquisition scenario
Test Purpose	The purpose of this measurement is to find out the minimum satellite signal power at which the TLOBU is still able to either acquire or track the satellite signals and consequently establish or maintain a valid position fix.
KPI	○ Accuracy
Performance Requirement	○ Tracking Sensitivity: maximum attenuation (dB) which allows the receiver to provide a position. ○ Acquisition Sensitivity: maximum attenuation (dB) which allows the receiver to have a first position fix within a given time.
Test Reference	○ ETSI TS 103 246-3 v1.3.1 ○ ETSI TS 103 246-5 v1.3.1 ○ EN 50126
Background:	GNSS Sensitivity is defined in terms of the maximum masking (attenuation) values tolerated by the TLOBU while still allowing the provision of the required location-related data. It is respectively specified for Tracking and Acquisition.

Requirements	According to the D2.3 System requirements, The TLOBU shall reach full operational capability including for safety-related applications within 600 s after powering up and able to initialize itself and provide the localization report for safety applications also when no initial position and track ID is provided as an input
	Test description
Test Dynamics	○ STA (static) -location ○ DYN (dynamic) -Moving location
Test Mode	○ CS (cold start) ○ WS (warm start) ○ HS (hot start)
Test System	○ GRES (GPS + GLONAS + Galileo + EGNOS)
Test Environment	○ SIM (simulated) - Open Sky Railway Operational Environment - Restricted Railway Operational Environment - Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply ○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.
Operational Scenario	○ Open Area - Railway Environment ○ Asymmetric Area - Railway Environment
Quality Indicator	○ PDOP ○ Signal Level
	Test Procedure
1	Generate the operational scenario in both the test environment and dynamics.
2	Start the GNSS scenario with location target at a random point within a 3 km radius of the reference location with an altitude randomly between 0 and 500 m to continue moving along the trajectory.
3	Scenario start time shall be randomly delayed by 0 to 30 s from start time.
4	Adjust the GNSS reference input signal power level according to defined requirements.
5	Clear the TLOBU GNSS receiver RAM such that could start mode of GNSS receiver of TLOBU is achieved.
6	Check position, velocity and time information is reset.
7	Use the Vector Network Analyzer to set signal path attenuation on attenuators.
8	Measure frequency response for a given signal path in E1/L1 band of Galileo/GPS.

<table>
<tr><td>9</td><td>Record the average path transmission factor in dB in this frequency band</td></tr>
<tr><td>10</td><td>Disconnect GNSS antenna from the TLOBU and connect it again after 20 sec.</td></tr>
<tr><td>11</td><td>With stopwatch watch determine time interval between cable connection moment, restoration of satellites and calculation of navigation solution.</td></tr>
<tr><td>12</td><td>Generate a position report with the max. TTFF response time of 300s</td></tr>
<tr><td>13</td><td>Calculate the horizontal error from the difference between the measured and true position.</td></tr>
<tr><td>14</td><td>Test is repeated a number of times in order to draw statistics until the statistical requirements of a success rate of 90 %.</td></tr>
<tr><td><b>Adjustment/Enhancement</b></td><td>So according to input Applicable Reference ETSI 103 246-series standard, the following methodology can be adjusted, and enhanced for the needs of CLUG positioning for accuracy.</td></tr>
<tr><td><b>Required Output</b></td><td>○ TLOBU- PVT data</td></tr>
<tr><td><b>Test Result</b></td><td>The Sensitivity results will be presented in tables including power thresholds, signal strength at position fix.</td></tr>
<tr><td colspan="2"><b>Pass Condition</b></td></tr>
<tr><td><b>Sensitivity Target</b></td><td>Test of TLOBU sensitivity in cold start mode, tracking mode and reacquisition scenario
“pass" for metric is if:
<table>
<tr><td></td><td>Does Not Exceed</td><td>For Signal Value</td></tr>
<tr><td>Values of [TTFF] in cold start mode</td><td>3600 seconds</td><td>144 dBm</td></tr>
<tr><td>GNSS Navigation Solution available</td><td>600 seconds</td><td>155 dBm</td></tr>
<tr><td>Reacquisition of GNSS signals & Calculation of Navigation Solution</td><td>60 seconds</td><td>150 dBm</td></tr>
</table>
</td></tr>
</table>

3.2.3.13 CTP/PP/2.4

CTP/PP/2.4	**Conformance Test of Reacquisition Time**
Test Parameter	Reliability
Test Objective	To verify the performance of the TLOBU in terms of reacquisition time.
Test Purpose	The purpose of this measurement is to evaluate how quickly the TLOBU can reacquire the satellite signals after it has lost all signals for a brief period of time.
KPI	○ Accuracy ○ Sensitivity ○ Time to Fix
Performance Requirement	○ Re-acquisition tests shall be executed for all the start modes permitted by the TLOBU
Test Reference	○ ETSI TS 103 246-3 v1.3.1 ○ ETSI TS 103 246-5 v1.3.1 ○ EN 50126
Background:	For example, after leaving a tunnel where all satellite signals were blocked, the TLOBU should be able to quickly get a valid position fix and restore navigation services The TLOBU is fed with signal coming from a set of simulated SVs. The signals are switched off for a while (1s). This is done at different power levels in order to determine at which power level the TLOBU is able to regain a fix within the timeout.

Requirements	The reacquisition time is a performance parameter especially important for TLOBU.
Test description	
Test Dynamics	○ STA (static) -location ○ DYN (dynamic) -Moving location
Test Mode	○ CS (cold start) ○ WS (warm start) ○ HS (hot start)
Test System	○ GRES (GPS + GLONAS + Galileo + EGNOS)
Test Environment	○ SIM (simulated) - Open Sky Railway Operational Environment - Restricted Railway Operational Environment - Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply ○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.
Operational Scenario	○ In Cold start Mode ○ Tracking Mode
Quality Indicator	○ PDOP ○ Signal Level
Test Procedure	
1	Generate the operational scenario in both the test environment and dynamics.
2	Start the GNSS scenario with location target at a random point within a 3 km radius of the reference location with an altitude randomly between 0 and 500 m to continue moving along the trajectory.
3	Verify that TLOBU set to receive GNSS Signals.
4	Wait for 15 min to check if TLOBU has the PVT solution
5	Turn the signals off for a time at least one second at different power levels in order to determine at which power level the TLOBU is able to regain a fix within the timeout.
6	With stopwatch watch determine time interval between cable connection moment, restoration of satellites and calculation of navigation solution.
7	Repeat the above procedure for 10 times
8	Calculate the average value for acquisition time of satellite

Adjustment/Enhancement	Using references ETSI 103 246-series defined standard methodology can be adjusted and enhanced for the needs of CLUG positioning for accuracy.
Required Output	○ TLOBU- PVT data
Test Result	The Re-acquisition results will be presented in tables including Mean power level for a valid fix (and standard deviation), mean positioning error at the first fix (and standard deviation), mean time to first fix (and standard deviation).
Pass Condition	
Target	"pass" for metric is if: ○ If re-acquisition time of tracking signals after block out of 60 seconds does not exceed 20 seconds.

3.2.3.14 CTP/PP/3

CTP/PP/3	**Conformance of horizontal and vertical position accuracy**
Related QOS	Reliability, Availability, Maintainability, Safety
Test Objective	To verify the performance of the TLOBU in terms of Accuracy in estimating the location target position in both horizontal and vertical planes.
Test Purpose	The purpose of this measurement is to evaluate how accurately the TLOBU can determine its true position
KPI	○ Horizontal Position Accuracy ○ Vertical Position Accuracy ○ GNSS Time Accuracy
Performance Metrics	The metric used to characterize Horizontal/Vertical Position Accuracy is the Horizontal/Vertical Position Error over a specified time interval in terms of its: ○ Mean value ○ Standard deviation ○ 95th percentiles distribution ○ The deviation between TLOBU location and reference location indicates the accuracy level
Test Reference	○ ETSI TS 103 246-3 v1.3.1 ○ ETSI TS 103 246-5 v1.3.1

	○ EN 50126
Background:	The most direct reflection of a GNSS-based system performance is the measurement accuracy, no matter time accuracy or location accuracy. Accuracy is defined as the degree of conformance of the measured location with conventional true position of the TLOBU at the given time. In general, PVT accuracy performance depends on the quality of the pseudorange and carrier phase measurements as well as the broadcast navigation data. ○ The Horizontal Position Accuracy is the difference (error) between the position of the location target reported by the TLOBU and its true position projected onto the horizontal plane, at a given time (i.e., with a given timestamp). ○ The Vertical Position Accuracy is the difference (error) between the position of the location target reported by the TLOBU and its true position projected onto the vertical plane, at a given time (i.e., with a given timestamp). ○ GNSS Time Accuracy is the difference between the true GNSS time (reference time of the GNSS system), and the time computed by the TLOBU ○ Along-track error is the projection of the position error on the axis tangential to the location target trajectory, determined at the location target true position at the time the position was sampled by the TLOBU ○ Cross-track error is the projection of the position error on the axis orthogonal to the location target trajectory, determined at the location target true position at the time the position was sampled by the TLOBU. Both of these errors are characterized by their mean value, and the 95th percentiles values
Requirements	Horizontal position error shall not exceed: – Under open sky conditions: 0.5 metres at confidence level 0,95 probability with Position Dilution of Precision (PDOP) in the range from 2,0 to 2,5 – In urban canyon conditions: 10 metres at confidence level 0,95 probability with Position Dilution of Precision (PDOP) in the range from 3,5 to 4,0. 1.2.6. The performance requirements in [RD-8], for the associated requirements for Accuracy with specified ranges of for the speed and acceleration are summarised as follows: ○ Acceleration: weak ≈0,02m/s2 to ≈0,1 m/s2 ○ Acceleration: strong ≈0,1m/s2 to ≈0,7m/s2 (≈1,2m/s2) ○ Speed: slow >0km/h (different to standstill) to ≤25km/h ○ Speed: normal >25km/h to ≤160km/h ○ Speed: fast >160km/h to max. speed (500km/h)

	According to [RD-8], For all TLOBU outputs, erroneous output is analysed systematically by starting from specified performance Related requirements. The associated requirements for safe speed estimated too high and too low are : ○ 2 km/h if v < 30 km/h ○ Linear increase up to 14 km/h at 600 km/h The associated requirements for estimated speed are : ○ km/h if v < 100 km/h ○ One percent * v if v = [100-600 km/h] The associated accuracy requirements for estimated acceleration are not quantified in the context of CLUG.
Test description	
Test Dynamics	○ STA (static) -location ○ DYN (dynamic) -Moving location
Test Mode	○ CS (cold start) ○ WS (warm start) ○ HS (hot start)
Test System	○ GRES (GPS + GLONAS + Galileo + EGNOS)
Test Environment	○ SIM (simulated) - Open Sky Railway Operational Environment - Restricted Railway Operational Environment - Urban Railway Operational Environment
Environmental conditions for testing	According to [AD-25], considering the GNSS user equipment the following conditions apply ○ Temperature: +15 °C to +35 °C ○ Relative humidity: 20% to 75% ○ For simulation: standard atmospheric simulation model According to [AD-09], and [AD-10] the environmental conditions within Europe are given at which the TLOBU shall function are specified.
Operational Scenario	○ Along Track ○ Cross Track
Quality Indicator	○ HDOP, VDOP, PDOP ○ Signal Level
Test Procedure	
1	Generate the operational scenario in both the test environment and dynamics.
2	Start the GNSS scenario with location target at a random point within a 3 km radius of the reference location with an altitude randomly between 0 and 500 m to continue moving along the trajectory.
3	Verify that TLOBU set to receive GNSS Signals.
4	Set up TLOBU to output messages according to GNSS Data formats, i.e., RINEX OR NMEA-0813

5	Reset and start the TLOBU
6	The horizontal and vertical accuracy tests can be combined since each position measurement can be used to derive both parameters.
7	Collect 200 TLOBU position data samples at a rate of one per 120 s (to guarantee statistically independent PVT samples).
8	Extract coordinates: latitude and longitude contained in data format or samples
9	Calculate the systematic inaccuracy of coordinate's determination on stationary intervals
10	Calculate horizontal position error as Error = Π = $\sqrt{\boldsymbol{dB^2(m) + dL^2(m)}} + \boldsymbol{2}\sqrt{\boldsymbol{\sigma\_B^2(m) + \sigma\_L^2(m)}}$ where: dB(M) & σ_B are for Latitude; dL(M) & σ_B are for Longitude
11	The position accuracy test shall be repeated for all the combinations of location target environments and motion types
Adjustment/Enhancement	So according to input Applicable Reference ETSI 103 246-series standard, the methodology can be adjusted, and enhanced for the needs of CLUG positioning for accuracy.
Required Output	○ TLOBU- PVT data
Test Result	The Accuracy results will be presented in tables including average value at different power levels
Pass Condition	
Target	“pass" for metric is if: ○ If the position accuracy requirement is met ○ If the confidence level for the estimated percentiles is higher than 90 %.

3.2.4 System Safety Assessment & Audit

The safety assessment is a methodology to evaluate CLUG's TLOBU functions and the design of systems performing these functions to determine that the associated hazards for those functions have been properly addressed.

Objective of Safety Assessment Process

For the certification of GNSS solutions for safety-related applications that the system studied is able to guarantee a given level of performances expressed in the railway domain in terms of RAMS attributes (Reliability, Availability, Maintainability and Safety.

To verify if the TLOBU Performance of TLOBU in terms of accuracy in estimating the location target position in both horizontal and vertical planes.

Criteria

Before including new equipment or functions in a railway safety-related system, the RAMS attributes of these equipment or functions need to be quantified at the design level of the life cycle, as demanded in the EN 50126 standard.

Background:

Implementation of failure detection mechanisms can improve both safety and reliability. Subsequent refinement of failure modes will help to clarify exact meaning of GNSS integrity and continuity risks, and it will help to find a way how to describe them by means of railway RAMS terms according to EN 50126 safety requirements are derived from the preliminary Hazard analysis as well as from norms and regulatory requirements. GNSS application in the domain of safety, for TLOBU, a much better understanding of GNSS behavior is needed. For the use of GNSS in standardized applications, the performance of GNSS receivers must be harmonized in order to achieve standardized, guaranteed performance and thus interoperability between on-board unit.

Performance Metrics

- Failure causes and failure modes of the system
- Failure states of the system) by means of dependability methods like fault tree method FMECA (Failure Mode, Effects, and Criticality Analysis

Documentaion Requirements

- According to WP2.4, Preliminary Hazard Analysis (PrHA) for the targeted Train Localization Unit", an initial study was performed at initial stages of system design and focuses on identifying apparent hazards, assessing the severity of potential accidents that could occur involving the hazards, and identifying safeguards for reducing the risks associated with these hazards

Safety Assessment

- Documentation that shows to origin of hazards identified
- Documentation that shows to source of the hazards identified i.e., contribution from the sender (e.g., GNSS satellites, Balises, Augmentation satellites)
- Documentation that shows, to source of the hazards identified from the air gap between the sender and the receiver
- Documentation that shows to source of the hazards identified from the on-board receiver functionality (e.g., GNSS and SBAS receiver, BTM
- Documentation that shows to source of the hazards identified from the contributions from elements external to the senders (e.g., GNSS/SBAS ground segment, Radio Block Control, GSM-R

Audit & Assessment

Audit & Assessment that includes the following documentation to qualify according to EN 50126
- Preliminary Hazard Analysis Report for TLOBU

  - Hazard and Risk Assessment
  - Feared events associated with the defined localisation system

The end expectation of a safety assessment is that a judgement is made about the system safety conformance and safety integrity achieved by every safety instrumented function within the system(s) being assessed.

The goal is for an audit of procedures and records to determine whether an appropriate system safety management system is in place, and it is being followed.

An audit alongside a safety assessment activity is an entirely valid prospect for an installation.

3.2.5 Definition of test acronyms

Topic	Reference	Description
DYN	Based on ETSI TS 103 246 Series	- trajectory of the vehicle: its location in the world, and its cinematic impacting the capability to correct or filter any sensor's defaults - Low Speed - High Speed - Acceleration - Standstill
SIM (simulated, optional)	Based on CEN/EN16803 Series	Simultaneous simulation of the GNSS signals by a signal generator with realistic representative
LIV (live)	ETSI TS 103 246 Series	In Real time, i.e., Live sky in minimal test coverage
Open Sky Railway Operational Environment	ETSI EN 303 413 V 1.2.0 Series	the environmental conditions impacting the sensing measurements
Restricted Railway Operational Environment	Based on CEN/EN16803 Series	the environmental conditions impacting the sensing measurements

Urban Railway Operational Environment	Based on CEN/EN16803 Series	the environmental conditions impacting the sensing measurements
CS (cold start)	Based on CEN/EN16803 Series	no time, almanac, ephemeris, or position data
WS (warm start)	Based on CEN/EN16803 Series	knows the time, almanac, and rough position, but no ephemeris.
HS (hot start)	Based on CEN/EN16803 Series	the time, almanac, and ephemeris, plus a rough position
PDOP	Based on CEN/EN16803 Series	the actual PDOP target value can be understood as the one observed when having in visibility a single GNSS constellation, which is either the GPS or Galileo constellation, separately
Signal Level	Based on CEN/EN16803 Series	GNSS signal is defined at the GNSS antenna connector of the TLOBU

Table 37: Definition of test acronyms

3.2.6 Requirements Traceability Matrix

This section provides the high-level overview to map and trace the defined requirements and metrics for the TLOBU with the tests identified according to the standards applicable in various domains in simulation mode with simulators, record and replay mode reproducing the test conditions, or field test according to test behavior specified.

The process to review all the test cases that are defined for any requirement is called Traceability. Traceability enables to determine which requirements spawned the greatest number of defects during the testing process.

According to the [RD-19], the bi-directional traceability ensures that all the Test cases can be traced to requirements and each and every requirement specified has accurate and valid Test cases for them. Whereas show in the Figure 25:Bi-Directional Traceability below, a good traceability matrix has references from test cases to requirements and vice versa (requirements to evaluate cases).

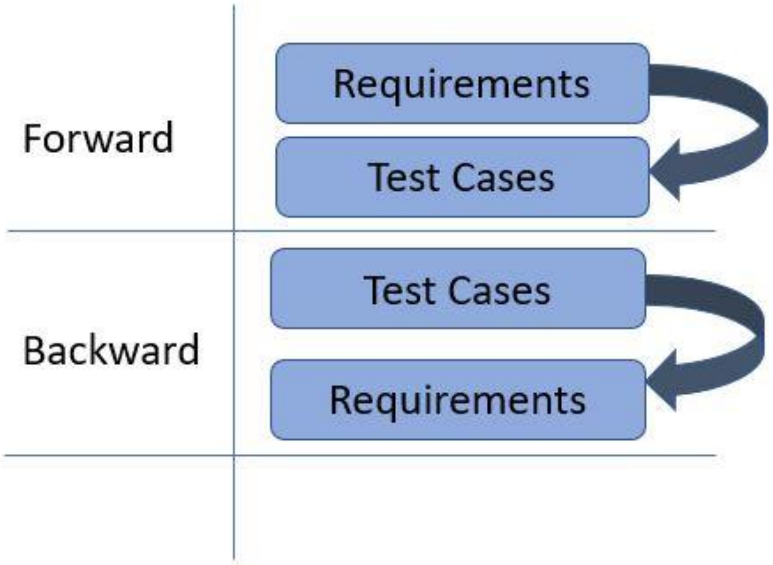


Figure 25:Bi-Directional Traceability

Note : The safety requiremets ID' s are acciording to [RD-10] and system requiremet ID's are according to [RD-09]

The following Table 38 shows the Traceability matrix of TLOBU requirements versus TLOBU identified test cases

Parameter/KPI	System/Function Requirement ID	Test Method	Performance Property	KPI- TLOBU
Availability	SR_R94 SR_R126 SR_R94 SFUNC-01 SFUNC-15	CTP/QOS/1	CTP/PP/1.1 CTP/PP/1.2 CTP/PP/1.3 CTP/PP/3	3D Position-Accuracy (true position) Speed -Accuracy
Reliability	SR_R94 SR_R127 SR_R128 SR_R129 SR_R130 SR_R131	CTP/QOS/2 CTP/QOS/5	CTP/PP/2.1 CTP/PP/2.2 CTP/PP/2.3 CTP/PP/2.4 CTP/PP/3	Sensitivity Time to Fix Acquisition Reacquisition Time
Maintainability	SR_R94 SR_R132	CTP/QOS/3	CTP/PP/3 CTP/PP/4	Time to Fix Reacquisition Time
Safety	SR_R101 SR_R107	CTP/QOS/4	CTP/PP/1.3	Safety integrity

	SR_R109 SR_R110 SR_R112 SR_R114 SR_R142 SR_R143 SR_R144 SR_R145 SR_R148			3D Position - Accuracy true position) Time to First Fix Reacquisition Time Speed -Accuracy
Position	SFUNC-10 SFUNC-03	CTP/QOS/1 CTP/QOS/2 CTP/QOS/3 CTP/QOS/4 CTP/QOS/5	CTP/PP/1.1 CTP/PP/1.2 CTP/PP/3	Position accuracy
Speed	SFUNC-04 SFUNC-05	CTP/QOS/1 CTP/QOS/2 CTP/QOS/3 CTP/QOS/4 CTP/QOS/5	CTP/PP/1.2 CTP/PP/3	Speed accuracy
Accuracy	SR_R38 SR_R43 SR_R50 SR_R57 SR_R68 SR_R121	CTP/QOS/1 CTP/QOS/2 CTP/QOS/3 CTP/QOS/4 CTP/QOS/	CTP/PP/2.1 CTP/PP/2.2 CTP/PP/2.3 CTP/PP/2.3 CTP/PP/1.3 CTP/PP/3	Horizontal Position Error Vertical Position Error

Table 38:Traceability Matric with Tests versus TLOBU requiremet

4 VALIDATION OF CERTIFICATION METHODOLOGY

This section highlights and provides the introduction to the validation and verification concepts. The approach is to provide validation of test schemes for the test identified under section 3.2.3. The goal is to validate the defined tests and procedures in compliance to the TLOBU identified requirements.

Validation is intended to ensure that identified test procedures and methodology for the TLOBU requirements that meets TLOBU identified requirements. Therefore, it relates to the process implemented to confirm that the system fulfils the TLOBU requirements. A set of validation requirements identified for the TLOBU, specifications, and regulations are considered as a base for qualifying the TLOBU system.

Verification is intended to check that TLOBU meets a set of design specifications. The verification of the concepts depends on the complexity of the system or subsystems to be analysed and depends on the required effort to verify the requirements compliance.

Verification procedures involve regularly repeating tests devised specifically to ensure that the system continues to meet the initial design requirements, specifications, and regulations. The strategies defined under the section 3.2.3 which encompass many model assumptions need to be verified, at least in some degree of confidence for Key Performance Figures like the accuracy, the availability, the convergence time, the service coverage area and the target integrity risk. Hence in this section the major focus is on Validation.

A more detailed description on the validation process, to perform the verification and validation activities to ensure the proper and correct function of the testing methods and tools. will be given in the deliverable for work package 5.3.

Additional validation procedures also include those that are designed specifically to ensure that modifications made to an existing qualified development flow or verification flow will have the effect of producing a product, service, or system (or portion thereof, or set thereof) that meets the initial design requirements, specifications, and regulations, these validations help to keep the flow qualified.

The validation phase of the certification is a crucial step. It will demonstrate the proposed prototypical certification process is a valid certification process. The validation of certification methodology involves process and topics from the related standards and regulations for accreditation bodies as well as laboratories.

In the scope of CLUG, the validation of the certification methodology is based on the identified test procedures and methodology for the TLOBU requirements from various existing standards that are defined under section 3.2.

The performance characteristics can be validated through the proposed validation methodology with a clear interpretation from performance concept to quantifiable characteristics on the basis of Reliability, Availability, Maintainability, and safety. The validation of the schemes depends on the complexity of the CLUG system and TLOBU subsystems to be analyzed and also on the required effort to validate the requirements compliance.

The here proposed method (see chapter 3.2.3) will potentially enable a future, final TLOBU to be certified and finally applicable for certifiable localization unit in railway environment. Within the CLUG project due to the development of only a prototype or similar only a prototypical certification is in the scope.

The assessment procedures, such as testing, inspection, and certification, offer assurance that TLOBU fulfil the requirements specified. In the scope of the Validation of certification methodology, therefore, the adopted conformity methodology will be as follows:

- the definition of tests according to standards or regulations
    - with the possibility to include other relevant standards,
    - with the possibility to include other relevant regulations,
    - extend the test procedure to include other aspects based on the expertise and experience of the consortium
- the definition of a testing process to perform the defined test procedure by considering aspects like,
    - definition of the test architecture and equipment,
    - definition of the test requirements,
    - definition of the test implementation, and
    - definition the proper test results documentation

In the test procedure, the test cases to be performed are uniquely defined with uniquely pass and fail criteria. As defined in the section 3.2, the test procedure process requires the identification of key performance indicators (KPI's), associated metrics and the minimum performance levels taken from the standard recommendations or regulations. The test cases used for testing or certification will encompass different situations (system architecture or module dependent) which are not all reflected in a unique standard. As several different standards have considered to define more tests.

The identified and adjusted test procedures describe testing methodology procedure required to execute the testing by defining responsibilities, defining the required test architecture and equipment, testing requirements, test implementation and test results documentation.

The test scheme should be validated to assess that test procedure provide the expected results and is correct. The assessed test procedure specifies requirements for test equipment (measurement devices), environmental conditions (ambient temperatures) and location of the test (in an accredited laboratory in the respective scope of GNSS).

During the development of a method, it is continuously validated that the test method can be executed and that it will achieve the required performance. If the method is revised, the validation is repeated to the extent necessary.

Testing focuses on the system's general functionality and if it meets following requirements:

- complete recording of all data
- documentation of subsequent changes
- complete and prompt recording

Validation of Test Method

All the test methods that are adjusted, enhanced including the standard methods are validated for the intended use. The validation is as extensive as it is necessary to meet the needs of the TLOBU requirements.

Following criteria for validation may be considered:

- Calibration or evaluation of bias and precision using reference standards or reference materials,
- Systematic assessment of all factors influencing the result,
- Comparison with results achieved with other valid methods,
- Testing method robustness through variation of controlled parameters, such as incubator temperature, volume dispensed,
- Assessment of measurement uncertainty

Performance characteristics can include, but are not limited to, measurement range, accuracy, measurement uncertainty of the results, limit of detection, limit of quantification, selectivity of the method, linearity, repeatability or reproducibility, robustness against external influences or cross sensitivity against interference from the matrix of the sample or test object, and bias.

The validation will be documented by:

- The used validation procedure,
- Specification of the requirements,
- Determination of the performance characteristics of the method,

- Obtained results,
- Statement on the validity of the method, detailing its suitability for the intended use.

TLOBU Validation Scheme

On an elevated level for the assessment of the CLUG system it is required to include the overall TLOBU architecture. According to [RD-11], the onboard localization can be envisaged as being comprised by three segments i.e., space segment (GNSS and SBAS), On board segment (sensors: Receivers, Train Equipment, Telecom, IMU) and trackside segment (trackside equipment: Digital Maps). These system elements should be validated as follows:

- The TLOBU shall be verified to demonstrate the compliance to identified performance requirements
- GNSS correction service shall be verified to demonstrate compliance to the TLOBU requirements
- The GNSS and Telecom receiver integrated in the TLOBU has to be validated
- The complete system shall be validated to demonstrate compliance to requirements

Classes of Validation

The activities for test validation can be categorized in two types of classes

- **Type I Validation:** The validation test class of Type I will be associated with theoretical approaches, i.e., derived from theoretical analysis and/or derived from simulation prototypes tools (SPT), might be further necessary to refine the information and define the way for the implementation of the system
- Theoretical analysis on Validation of CLUG methodology starts with error identification, impact analysis, measurement uncertainty analysis, etc. of course, the sensors are different, but the type is comparable.
- **Type II Validation:** The validation test class of Type II will be associated with field test to assess the quality of the system(s) under test. One example of the type II validation is the record and replay of GNSS data technique.
- The validation of the identified test schemes for CLUG are executed in a GNSS accredited test laboratory, based on the underlying the test methodology defined.

The preparation of the standard-compliant tests according to section 3.2 can already be integrated in the context of the experiments of the CLUG to examine the various measuring systems. In this way, the framework conditions of the test procedures can be defined at an early stage and appropriate preparations can be made.

With these methods, the first measured values of the investigated measuring systems can already be determined. This means that the conditions for a successful evaluation are met, and it is much faster than if these preparations have to be made at a later stage or if preparations that have already been made have to be corrected. The preparation of the standard-compliant examination includes the error analysis and statistical analysis which are specified in the following sections.

4.1 Error Identification Analysis

According to [RD-7], [RD-8], [RD-7] the CLUG System, i.e., the TLS consist of TLOBU which is embedded into the larger system. The CLUG system contains several other systems that have a need for the information produced by the CLUG System to support their own functions and that have their respective functional and non-functional requirements on the output provided by the CLUG System. Hence the output of the CLUG system i.e., the TLS output is of high importance for multiple topics like also definition of references. Hence an error analysis on the TLS evaluation is needed and this section identifies the error analysis on the TLOBU. Based on these findings, risks, and requirements for the CLUG system validation are considered.

TLOBU consist of a navigation core to provide continuous position, velocity, time, and other dynamics of the train, where the functionality is interfaced with the following elements:

- GNSS/EGNOS signals,
- EGNOS via TELECOM receiver
- Balise
- IMU
- Digital maps
- Reference points on the track
- Speed sensors / Tachometers

The error analysis is limited in this document to a high-level analysis for the GNSS and IMU sensor-based errors and conducted process upon the error analysis that is used to qualitatively evaluate and analyse the conformance procedure and methodology. Each identified fault can threaten a security or safety concept. Further analysis can be found in the deliverables of work package 2 and 3.

Proof of their suitability for this purpose is a necessary condition for the assessment and approval of TLOBU. The proof must provide proof of correct functional behavior and provide qualitative and quantitative proof of the handling of individual errors and systematic errors as well as their disclosure of errors. The proof benefits from a standard-compliant qualification by an accredited testing body. The qualification includes the metrological examination, the verification, i.e., the proof that the required conditions are being met and finally their certification.

The error analysis consists of the identification of impacting factors in the measurement process, of a quantification and severity analysis of these impacts, as well as, of an analysis of the remaining impact factors by using the error propagation or propagation of uncertainty of the measurement process.

For the error analysis, we need to identify the source of error, whether it is systematic error or random error.

- Random error arises from unpredictable variations of impacting factors. The effects of such variation give rise to variations in repeated observations of the measurand. Random errors cannot be compensated but only reduced by increasing the number of observations.
- Systematic error arises from faulty equipment or a flawed experimental design. This is usually caused by measurement instruments that are incorrectly calibrated or are used incorrectly. Systematic error cannot be eliminated but often may be reduced.

For the error analysis, the impacting factors and how they affect the test are analyzed. The impacting factors can be the equipment, the device under test, an operator, the measurement methodology and the environment, for instance. A severity analysis helps to identify the errors or risks with high impact or to be avoided, those that should be transferred or reduced.

The TLOBU is split in two parts:

- Sensor’s part: representing all data collected, in real time or not, that are injecting into the TLOBU algorithms for localization and safety purpose,
- Algorithm’s part: representing all data evaluations (FDE: Fault Detection and Exclusions), transformations and computations to provide TLOBU outputs in real time.

TLOBU subsystem is functionally interfaced with the following elements:

- Traffic Management,
- Train Control (indirectly),
- Train Protection,
- Train Control and Management System – TCMS,
- Automatic Train Operation,
- Train Integrity Monitoring / Train Rear End Localisation (indirectly),
- Incident Management / Perception,
- Passenger Information System

The above-mentioned elements relay on the TLOBU outputs very frequently and accurately to know the position, speed, acceleration, and movement of direction. The TLOBU outputs are:

- TUFE/ TURE position
- TUFE / TURE speed
- TUFE / TURE movement direction
- TUFE / TURE acceleration

The use of GNSS systems supporting the TLOBU is complex and susceptible to failures imposing large challenges for verifying that stringent accuracies and protection levels apply, as is acknowledged in the railway environment.

In this section, the error analysis is considering the TLOBU sensor part. The railway environment where the TLOBU operates has also a high impact for the error evaluation. Hence the errors such as defects of sensors and errors due to railway environmental conditions are considered.

According to the [RD-8], the environmental conditions affecting a sensor such as GNSS or IMU are leading to specific sensor errors in the end such errors lead to measurement error. Effect cause diagrams (also known as fishbone diagrams) have been used as a tool, as shown in the generic, complete example Figure 23 below.

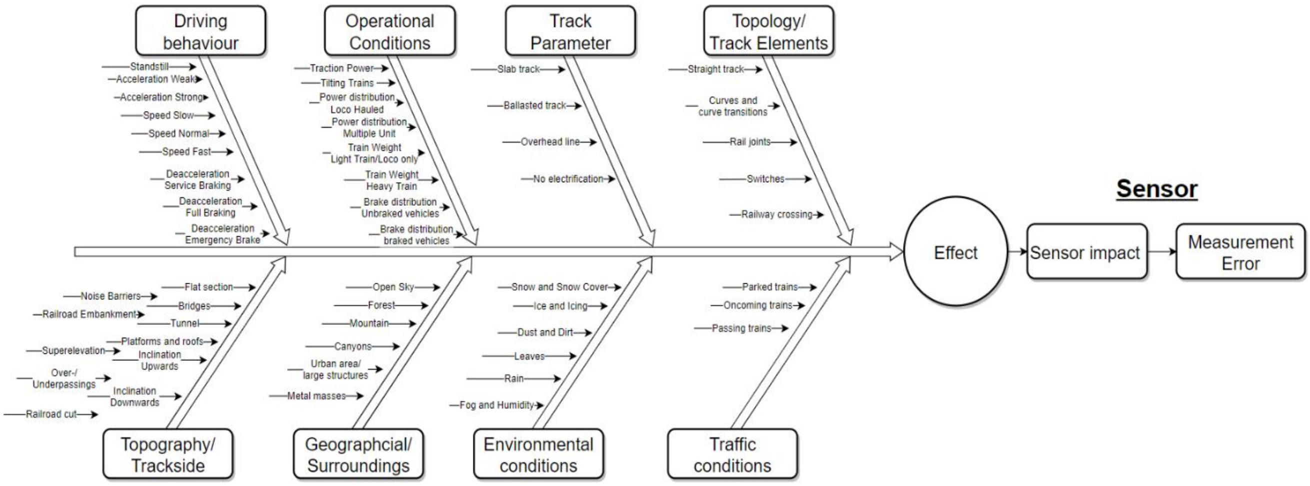


Figure 26: Generic effect cause diagram with all conditions

4.1.1 Operational Dependencies

The performance of TLOBU supporting will depend on factors below and thus lead to specific errors

- Dependency upon GNSS and IMU systems

- Dependency GNSS correction service (PPP/RTK/SBAS/EGNOS -based)
- Dependency on the implemented algorithms such as sensor fusion GNSS and IMU quality, receiver, and antenna characteristics
- Temperature conditions or electromagnetic conditions
  - Elevated temperature
  - Low temperature
  - Humidity
  - Shock
  - Vibration
  - Electromagnetic compatibility

In [RD-10] Preliminary Hazard Analysis and Safety Requirements, a quantitative analysis was performed at to identify all potential hazards and events and mitigation measures for reducing the associated risks.

Any hazard related to failures of the localization system arises from the combination of the CLUG TLOBU with the systems that decide and act on the train movements in the railway system, introduced in D2.1 Chapter 2

As defined in D3.1, that CLUG system aims to reduce the use of trackside balises, odometers and Digital Map data, as not in the scope of CLUG, the sensors such as GNSS receiver, EGNOS data receiver, are only analyzed. In this section, the following are the railway environments which lead to specific errors:

4.1.2 GNSS Error Analysis

The measurement performance of a TLOBU is characterized by the accuracy of its data output under the intended condition of operation. Accuracy can be defined as freedom from error and so is characterized by the magnitude and other properties of the error in the output data. The purpose of error analysis is to provide a description of the error that will permit its magnitude to be estimated for any set of operating conditions, without the necessity of running calibration or test for all combination of conditions. For the error analysis, there are many sources of GNSS measurement error that must be considered. In accordance with the D2.1 High level mission requirements [RD-7] and Preliminary External Interface Definition D2.6, this chapter presents the TLOBU Subsystem in its environment.

- GNSS denied environments such as TLOBU under
  - tunnel for several kilometres
  - under station roofs and bridges.
  - noise barriers
  - urban areas
  - Forests and vegetations
  - Mountains and canyons
- GNSS augmentation data unavailability
- TLOBU under Global and local atmospheric effects (Ionospheric, scintillation and tropospheric)
- TLOBU Coverage area, the provision of the GNSS correction service in earth sheltered situations
- TLOBU under RF interference effects (Jamming, meaconing, and spoofing)
- TLOBU under Masking and Multipath effects
- Reflecting environments, e.g., snow or rain on trees in forests or by metal structures.

For the GNSS detailed error analysis, referrer Section 3 of the [RD-16], D3.1.4 - Integrity Concepts & Algorithms In this subsection, a high-level analysis of the factors capable of impacting the observables, variables and processes are identified. This requires a knowledge of the underling system model or working principle in order to identify the factors influencing the performance of the observed system

4.1.3 IMU Error Analysis

The measurement performance of a TLOBU is characterized like described before by the accuracy of its data output under the intended condition of operation. For the error analysis, there are many sources of IMU measurement error that must be considered. In accordance with the D2.1 High level mission requirements [RD-7] and Preliminary External Interface Definition D2.6 [RD-12] this chapter presents the TLOBU Subsystem in its environment:

Vehicle maneuvers and dynamics such as

  - strong acceleration or deceleration
  - slope, inclination
  - elevation
  - drift
  - Parked or passing trains
  - Switches
  - Slab track or Railway crossing

- Track topography i.e., curve radius, inclinations, and superelevation

For the IMU detailed error analysis, referrer Section 3 of the [RD-16], D3.1.4 - Integrity Concepts & Algorithms. In this subsection, a high-level analysis of the factors capable of impacting the observables, variables and processes are identified. This requires a knowledge of the underling system model or working principle in order to identify the factors influencing the performance of the observed system

4.2 Error and Statistical Analysis

The certification procedure requires generally that the tests be executed using the equipment in accordance with standard test procedure and other laboratory requirements like validation prior usage, calibration of reference equipment. This is extended by further requirements originating from error and statistical analysis of the device/system under test, here TLBU. Thus, based on chapter 4.1 for GNSS typically and exemplary error and statistical analysis is done to define requirements for the reference, validate the independence in the measurements of the tester, of the specific unit, of the specific measurement method and other specific aspects. This process is detailed in the deliverable for work package 5.3

According to the [RD-11], the estimated or to be calculated parameters are TU 3D-position, velocity, acceleration, time, altitude with their respective standard deviation. According to the [RD-9] D2.3 "High level system requirements, the TLOBU localization solution is a software simulation of the TLOBU, evaluated using raw data collected during measurements trip.

In the first step, a measurement uncertainty analysis is conducted for the TLOBU. This draws on background knowledge about the errors that occur, which were identified in CLUG Feared events analysis. One goal is to determine the accuracy of what is required for the reference system. Another objective is to adapt the procedure for testing appropriately. The overall goal of all these steps is to adapt the test methodology for verifying the performance of the TLOBU.

In second step, clear understanding of the results of the measurement is achieved. This implies knowledge which observable(s)/variable(s)/process(es) shall be measured, what are the expected minimum and maximum ranges, and the accuracy. This information is obtained from the TLOBU sensors. The following are the list of observables from the measurement campaign:

- GNSS data in real time at 1Hz rate,
- SBAS (EGNOS DFMC) safe augmentation data in real time at 1Hz rate,
- Inertial data in real time at up to 100Hz rate
- Digital map safe data before the mission (so non real time but up to date) accessible at up to 100Hz rate,
- Speed data providing in real time at up to 20Hz rate: could be tachymeters, radars or "light odometer" solutions.
- Balise data

4.2.1 Definition of Error

Navigation System Error is the difference between the real position and the estimated one, defined based on general laboratory definition from JCGM 100:2008 or similar standards. The error (x) in each measurement is defined as the difference between the value indicated by the measuring instrument and the true value of the measured quantity.

$$x = U_{measured} - U_{true}$$

The error will vary with the time at which the measurement is made, the value of the quantity to be measured, and with environmental conditions.

Errors are commonly divided into systematic (bias) and random (accidental or noise) components. The value x_i of the error will lie within a limited range centered about a mean error $\bar{x}$, defined by

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

The standard deviation of the error measures the dispersion of the data in relation to the mean error $\bar{x}$, defined by

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n-1}}$$

where $\bar{x}$ is the mean error and n is the size of the vector $\bar{x}$. The error can be described with further statistical values, like percentiles. This topic is addressed in the deliverable for work package 5.3 and here in chapter 3.2.

4.2.2 Mathematical model and standard deviation

In general, the standard deviation is defined as follows:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n-1}}$$

But for this analysis, the standard deviation is defined as follows:

$$\sigma = \sqrt{\sum (x)^2}$$

where x represents the errors affecting the GNSS signal and receiver.

The standard error (SE) gives the accuracy of a sample by measuring the sample-to-sample variability of the sample means. The formula for the standard error (SE) is written below.

$$\sigma_{\bar{x}} = \frac{\sigma}{\sqrt{n}}$$

For the precision, the standard deviation will be used. The formula used is stated below.

$$\sigma = \sqrt{\sum (x)^2}$$

As an example, this is done here for a GNSS receiver in stand-alone mode with expected error margins:

$$\sigma = \sqrt{Sat.clock\ err.^2 + \ Sat.orbit\ err.^2 + \ Multipath^2 + \ Rec.clock\ err.^2 + \ Rec.ant.PCV^2}$$

$$\sigma = \sqrt{0.5^2 + 0.5^2 + \ 0.5^2 + \ 0.5^2 + \ 0.03^2}\ [m]$$

$$\sigma = \sqrt{0.25 \ + 0.25 + 0.25 + 0.25 + 0.0009}\ [m]$$

$$\sigma = \sqrt{1.0009}\ [m]$$

$$\sigma = 1.0018\ m$$

4.2.3 Measurement Uncertainty Analysis

This section explains the processes to assess the measurement uncertainty. One parameter of interest is the width of the margin, or interval. The other is the confidence level, which states how sure one can be that the ‘true value’ is within that margin.

The measurement uncertainty analysis distinguishes between the following uncertainties:

- physical uncertainty (material, construction, assembly, energy supply, ...)
- Uncertainty due to numerical-computational aspects and duration (rounding, resolution, conversion, computing time, ...)
- Uncertainty due to methods and algorithms for determination (e.g., correlation function, maximum determination, filtering, ...)

4.2.4 Determination of measurement uncertainty

According to Section 3.2, with already existed, enhanced, and adjusted methodologies are defined are used to a to analyze and evaluate the performance of the TLOBU system, by using the observables (outputs), variables (derived from outputs), or the processes. Therefore, an investigation might be adequate to check whether there are already standards existing for this test and if the observables or variables are already defined in these standards. At the end of this step a clear description of the observables and the related variables and eventually of the process is available. Subsequently, to the knowledge or identification of the observable(s)/variable(s)/process(es) to be measured, the measurement/process method is defined

5 CONCLUSION

The main focus of this document within the CLUG project is the preparation for the prototypical certifiability of the developed safety relevant train localization system. Hence in this document identified the current state of the type of approval with existing norms in the scope of localization with GNSS background in different fields.

Based upon that with respect to TLOBU performance requirements, and considerations from the WP2.3 preliminary hazard analysis and WP2.6 architectural properties of the system into account, the existing methodology from the existing norms are modified, adjusted, and enhanced and defined conformity test procedures according to the TLOBU requirements.

In addition to that, for the prototypical certification, the general process with methodology, including the conformity assessment, process for testing, and validation for such certification methodology are also defined.

This preliminary identification of the validation certification methods are served as input to WP5.3 for the prototypical certification for the train localisation system.

End of document