VICE4RAIL

D2.3 – Certification Plan

Due date of deliverable: 31/07/2025

Actual submission date: 02/08/2025

Leader/Responsible of this Deliverable: Antonio Salvi (BVI), Alessandro Basili (BVI)

Reviewed (Y/N): Y

Document status		
Revision	**Date**	**Description**
0.1	13/06/2025	First internal release
1.0	21/07/2025	1st Official Release
1.1	24/07/2025	2nd Official Release for integrating comments received from VICE4RAIL
1.2	01/08/2025	3rd Official Release for integrating feedback received from EUSPA

Dissemination Level		
PU	Public	X
CO	Confidential, restricted under conditions set out in Model Grant Agreement	
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

Start date of project: 01/10/2024 Duration: 36 months

This project is funded by European Union's Horizon Europe programme
under grant agreement No 101180124

CONTRIBUTING PARTNER

Name	Company	Roles/Title
Antonio Salvi	BVI	Author
Alessandro Basili	BVI	Contributor/Reviewer
Ales Filip	UPCE	Contributor/Reviewer
Salvatore Vetruccio	ITCF	Contributor/Reviewer
Vittorio Cataffo	RFI	Contributor/Reviewer
Nerea Canales Sebastian	RFI	Reviewer
Alessia Vennarini	RDL	Reviewer
Roberto Capua	SGI	Reviewer

DISTRIBUTION LIST

Name	Company	Roles/Title
Daniel Lopour	EUSPA	EUSPA Programme Officer
Salvatore Sabina	Expert Advisor	General review of the document
Philippe Citroën	Expert Advisor	General review of the document
Nerea Canales Sebastian	RFI	Project Coordinator
Aleš Filip	UPCE	WP2 Leader
Roberto Capua	SGI	WP3 Leader
Alessandro Neri	RDL	WP4 Leader
Alessandro Basili	BVI	WP5 Leader
Alessia Vennarini	RDL	WP6 Leader

APPROVAL STATUS

Document Code	Rev.	Role	Approved	Authorised	Date
VICE4RAIL_D2.3	1.0	WP2 Leader	Aleš Filip	Aleš Filip	28/07/2025
		WP5 leader	Alessandro Basili	Alessandro Basili	28/07/2025
		Coordinator	Nerea Canales Sebastian	Nerea Canales Sebastian	27/07/2025
VICE4RAIL_D2.3	1.2	WP2 Leader	Aleš Filip	Aleš Filip	01/08/2025
		WP5 leader	Alessandro Basili	Alessandro Basili	01/08/2025
		Coordinator	Nerea Canales Sebastian	Nerea Canales Sebastian	01/08/2025

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

EXECUTIVE SUMMARY

VICE4RAIL aims to promote the adoption of GNSS technology for implementing efficient, resilient and competitive train localization within ERTMS systems. The main goal is to contribute to an industry-approved certification procedure of GNSS technologies by an innovative evaluation ecosystem coherent with the CENELEC norms. The focus is on scalability, cost-efficiency and flexibility to validate, as much as technically feasible, GNSS-based Train localization solutions, such as technology-agnostic 'Advanced Safe Train Positioning' (ASTP) or others; these key factors are crucial in addressing the gaps that currently hinder the widespread adoption of GNSS technologies.

The scope of the VICE4RAIL project, that is the validation and testing system referred to as 'HyVICE (Hybrid Virtualized Testing Certification Environment)', will include a baseline GNSS-based train localization simulator to facilitate a preliminary definition of the roadmap leading to a possible certification process; this process will rely on dedicated testing facilities on RFI's railway lines (Bologna San Donato), for testing GNSS-based train positioning solutions in operational scenarios, and ERTMS accredited laboratory of CEDEX.

The testing environment proposed in the VICE4RAIL project will represent the starting point for future test architecture to be used by manufacturers and system integrators for performance evaluation, optimization and preliminary verification of compliance with the applicable standards and by NoBo for future certification of GNSS-based train positioning devices.

The methodology proposed by the VICE4RAIL project aims to extend its coverage also to the automotive, maritime and avionic sectors in order to share know-how for virtual testing, safety concepts, principles, and standards and certification of safety functions for GNSS-based train localization.

This deliverable **D2.3 'Certification Plan'** has the objective to define a guideline and a roadmap for the verification and validation process of the HyVICE test platform to be adopted for future certification of GNSS-based train positioning solutions for ERTMS/ETCS applications, in order to contribute to achieve the following objectives:

1) contribute to establish a standardized methodology for future certification of GNSS-based train localization solutions (e.g. ASTP) and to develop a harmonized European framework for ensuring reliability, compliance and regulatory alignment.
2) the construction of a dedicated reference dynamic testing environment (i.e. the HyVICE test platform) based on the 'near zero-on-site' testing approach, to support future assessment and certification process for GNSS-based train localization solutions (e.g. ASTP)
3) provide guidelines for a preliminary verification of compliance of the HyVICE test platform with the applicable technical requirements defined in the Regulatory Standards, to be used by Notified Bodies (NoBo) and Assessment Bodies (AsBo) as a starting point for future certification of GNSS-based train localization solutions (e.g. ASTP).
4) proceed to quantifying and modelling the effects of electromagnetic environments on GNSS and IMU technologies included in the HyVICE validation and testing simulation environment

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Acronyms and definitions

Acronym	*Meaning*
AsBo	Assessment Body
ACSF	Automatically Commanded Steering Function
ADS	Automated Driving System
AL	Alert Limit
ASIL	Automotive Safety Integrity Level
ASTP	Advanced Safe Train Positioning
C	Continuity (GNSS)
CA	Consortium Agreement
CAB	Conformity Assessment Bodies
CAT I	Category I precision approach and landing
CENELEC	Comité Européen de Normalisation Électrotechnique
CoP	Code of Practice
CR	Continuity Risk
CSM-RA	Common Safety Method for Risk Assessment
DeBo	Designated Body
DH	Decision Height (in aviation)
DUT	Device Under Test
EC	European Commission
E/E	Electrical and/or Electronic (ISO 26262)
E/E/PE	Electrical and/or Electronic and/or Programmable Electronic (IEC 61508)
EGNOS	European Geostationary Navigation Overlay Service
EOTTI	Emergency Operation Tolerance Time Interval
ERA	European Union Agency for Railways
ERJU	Europe's Rail Joint Undertaking
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EU	European Union
EUSPA	European Union Agency for the Space Programme
FMECA	Failure Modes, Effects and Criticality Analysis
FTA	Fault Tree Analysis
GBAS	Ground Base Augmentation System
GNSS	Global Navigation Satellite System
HARA	Hazard Analysis and Risk Assessment
HW	Hardware
HyVICE	Hybrid Virtualized Testing Certification Environment
IC	Interoperability Constituent
ICAO	International Civil Aviation Organization
IM	Infrastructure Manager
IMO	International Maritime Organization
IMU	Inertial Measurement Units

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Acronym	*Meaning*
ISA	Independent Safety Assessor
MED	Marine Equipment Directive
MTBF	Mean Time Between Failures
MTBO	Mean Time Between Outages
N_C	Number of critical satellites
NoBo	Notified Body
NSA	National Safety Authorities
PES	Programmable Electronic Systems
PL	Protection Level
PMHF	Probabilistic HW Failure Rate per Hour (ISO 26262)
PVT	Position, Velocity and Time
RAMS	Reliability, Availability, Maintainability and Safety
RAMSS	Reliability, Availability, Maintainability, Safety and Security (automotive)
R&D	Research and Development
RNP	Required Navigation Performance
RU	Railway Undertaking
SaRA	Safety-Related Availability
SBAS	Satellite-based augmentation system
SIL	Safety Integrity Level
SIS	Signal-In-Space
SLA	Service Level Agreement
SOL	Safety of Life
SOLAS	Safety of Life at Sea
SOTIF	Safety of the intended functionality
SW	Software
THR	Tolerable Hazard Rate
TLS	Target Level of Safety
TRL	Technology Readiness Level
TSI	Technical Specifications for Interoperability
TTA	Time To Alarm
UIC	International Union of Railways
UNIFE	Union of the European Railway Industries
UNISIG	Union Industry of Signalling
V&V	Verification and Validation
VDB	VHF Data Broadcast
VICE4RAIL	Hybrid Virtualized Testing for Certification of EGNSS in Railway Train Positioning
WP	Work Package

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Table of contents

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

List of figures

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

1 Introduction

1.1 Scope of the project

VICE4RAIL project supports the integration of GNSS technology into ERTMS-ETCS applications in order to enhance system performance, reliability, Safety integrity and competitiveness. Rather than focusing on contributing to define a fixed certification process for future of GNSS-based train localization solutions (e.g. ASTP), the VICE4RAIL project aims to support and promote the development of future and flexible industry-recognized certification procedures by providing a robust and innovative evaluation, testing and validation environment aligned with CENELEC standards.

The approach adopted in this project emphasizes adaptability, affordability and scalability to contribute to assess and certify advanced GNSS-based train positioning solutions that are not tied to a specific technology; these aspects are essential to overcoming current barriers to the broader use of GNSS in rail applications.

VICE4RAIL project is fully aligned with the 'Horizon' objectives to promote innovative, interoperable and competitive railway systems across Europe; liaisons will be established with the RTCM SC 134 Standardization Group and other relevant projects related to satellite-based positioning funded by Europe's Rail, such as R2DATO, as well as the System Pillar standardization activities (see § 5 of this document for further details).

The main objectives of the VICE4RAIL project can be summarized as follows:

- **OBJECTIVE 1**: contribute to establish a comprehensive certification methodology to evaluate, verify and validate the future integration of GNSS and IMU technologies for train positioning into train control systems, ensuring compliance with the ERTMS/ETCS standard, to guarantee reliability, accuracy, and integrity of the train positioning systems.
- **OBJECTIVE 2**: design and develop a HyVICE system with associated facilities and tools, capable of executing tests outlined in Objective 1, and providing realistic and reliable representations of real-world effects in the railway environment.
- **OBJECTIVE 3**: create and maintain a repository of diverse scenarios and test patterns. These resources will be used to conduct the tests outlined in Objective 1, ensuring thorough evaluations of the train performance under various conditions.
- **OBJECTIVE 4**: carry out dedicated rail tests that integrate, within HyVICE platform environment, real and synthetic data to simulate a full range of operational scenarios.
- **OBJECTIVE 5**: carry out dedicated ERTMS lab tests, within HyVICE platform environment and perform a validation of the lab test results based on the comparison against onsite tests.
- **OBJECTIVE 6**: contribute to develop a system capable of generating standardized test patterns and accompanying documentation to support the future certification of GNSS-based train localization and positioning systems.

Further details of the scope of the VICE4RAIL project are provided in the 'Technical Proposal' [VC.1].

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

1.2 Scope of the document

The present document constitutes the deliverable **D2.3 'Certification Plan'** of the VICE4RAIL project (Horizon Europe Grant Agreement No 101180124) and is one of the output documents on the WP2 'Hybrid Virtualized Testing Certification Environment Requirements/Development of Certification Plan' / Task 'T2.2: Development of the certification plan for the VICE4RAIL solution' as defined in the 'Technical Proposal' [VC.1].

The scope of the 'Certification Plan' is to contribute to define a preliminary guideline for verifying and validating the HyVICE platform environment and to lay down a roadmap for future certification/assessment process of the GNSS-based safe train positioning (e.g. ASTP) for ERTMS/ETCS applications.

The contribution to a certification plan for virtualised GNSS-based positioning testing will build on the well-established certification process currently in place on European railways, as defined in the Interoperability directives and regulations, CENELEC standards, etc. where the certification process ensures that all essential ERTMS-ETCS requirements for safety and interoperability specified in TSIs are met.

The VICE4RAIL project aims to complement the activities being carried out in the framework of Europe Rail R2DATO project and to contribute to the roadmap to release the new TSI for introducing the GNSS-based train positioning technology into the ERTMS-ETCS standard.

Any "open point" highlighted in the process described above will be registered and properly evaluated.

In case any information reported in this document should be updated (e.g. due to more details or integrations/changes in the functional architecture definition of CEDEX laboratory and/or Bologna San Donato Test site, or in the hardware/software configurations of 'Device Under Test (DUT)', etc.) this document will be consequently updated as internal document for the project.

1.3 Structure of the document

The present document is organised as follow:

- Chapter 1: it describes scope of the project, the scope of the document and put in evidence the input/output relations between D2.3 (i.e. this document) and other VICE4RAIL WPs and deliverables
- Chapter 2: it reports the list of main reference documents that are considered or mentioned within D2.3, including both international/European norms and standards and other VICE4RAIL deliverables
- Chapter 3: it proposes some standardized definitions of terms in order to guarantee, within the VICE4RAIL project, a common understanding of specific concepts.
- Chapter 4: it provides a summary description of the objects involved in the overall future certification process, that are the DUT (i.e. the VICE4RAIL proposed solution for GNSS-based train localization) and the HyVICE testing environment ('Bologna San Donato' and 'CEDEX ERTMS Lab' facilities)
- Chapter 5: it provides a general survey about the other past and current European projects from which the VICE4RAIL project can achieve fundamental feedback
- Chapter 6: it compares assessment/certification procedures used in other transport sectors, such as automotive, avionic and maritime sectors, in order to identify common elements with the rail sector and to contribute to finalize a global process for future certification of multimodal solutions.
- Chapter 7: it illustrates, in general terms, the overall future certification process of the VICE4RAIL proposed solution for GNSS-based train localization (e.g. the 'ASTP' solution).
- Chapter 8: it provides a more detailed description of the future 'Interoperability Certification' process, 'Safety Assessment' process and 'Risk Management' process, properly 'tailored' to simulate roadmap and a preliminary guideline for future applications to GNSS-based train localization solutions.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

- Chapter 9: it illustrates general open points that can be anticipated in this preliminary definition of the Certification/Assessment process and provides recommendations for possible investigation areas.
- Chapter 10: it provides Conclusions about future Certification/Assessment process.

1.4 Relationship to other project outcomes

As described in the 'Technical Proposal' [VC.1], VICE4RAIL project is structured in dedicated Work Packages (WPs), many of which are interrelated each other as shown in Figure 1 here below:

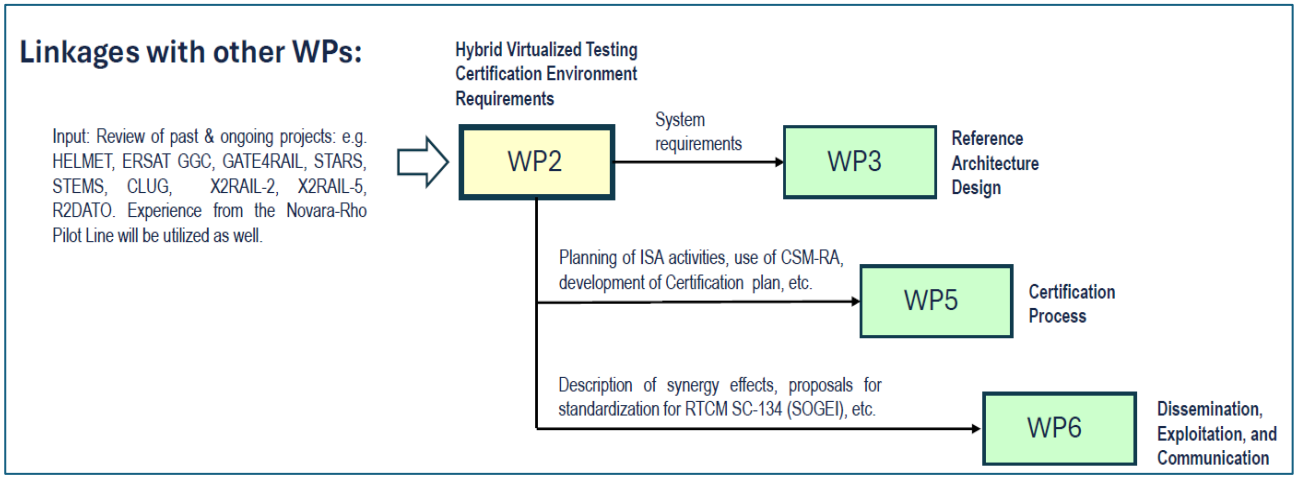

Figure 1 Linkages of WP2 with other WPs of VCE4RAIL project [VC.1]

With reference to the figure above, the VICE4RAIL technical WPs are summarized here below:

- WP2: has the aim of specifying requirements (user, functional, system safety and security requirements) for both the DUT (representing the future GNSS-based train localization solution, e.g. ASTP) and for the HyVICE platform (to be further developed in WP3) and developing an industry-accepted Certification Plan to be used as reference for HyVICE architecture validation. At the same time, comparison of assessment and certification procedures in rail, automotive and maritime sectors will be analyzed in order to identify common features and elements of the certification schemes.
- WP3: has the aim of designing the System Requirements, Overall Architecture, Detailed Architecture and Test Plan for the HyVICE platform environment, composed by both Laboratory Test Platform (CEDEX Laboratory) and the On field/Mixed Reality Testing Platform (Bologna San Donato Trial site of RFI).
- WP4: has the aim of implementing the designed architecture and performing Unit Test, Integration Test and executing Real Platform Test; based on the design of the architecture for the HyVICE platform carried out in WP3, WP4 is dedicated to the development of each subsystem and their integration and testing in laboratory and on-field.
- WP5: it reports results of both laboratory and field tests that are used in WP5 to conduct the final verification and validation of HyVICE platform. In WP5 the validation strategies are defined in order to allow VICE4RAIL project to issue a draft or a simple template (for demonstration use) of main validation documents/evidence. One of the other aims of WP5 is actually to simulate a possible future certification process by tentatively evaluating the conformity of the DUT requirements and functionalities to the Essential Requirements and the Technical Compatibility in accordance with current TSI CCS [NS.11].

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

VICE4RAIL deliverables that are interrelated with the **D2.3 'Certification Plan'** are:

- **D2.1 'Rail User & System Requirements'** [VC.2]: to provide an overview of the user and system requirements (including user, functional, system safety and security requirements) for the DUT with the aim of supporting the development of a hybrid virtualized testing and certification framework (HyVICE) specifically tailored for GNSS-based train localization solutions.
- **D2.2 'Risk Analysis Evaluation Report'** [VC.3]: to achieve fixation of the Requirements (as defined in deliverable D2.1 above) by applying the Common Safety Method for Risk Evaluation (at system level) Assessment ("CSM-RA") according to the regulation (EU) 402/2013 [NS.4].
- **D2.4 'Synergies in the Certification Process for Use in Multi-modal Transport'** [VC.4]: to compare standard certification procedures in rail, automotive and maritime sectors to identify common elements to make the future certification of multimodal transport solutions more efficient.
- **D3.1 'Overall Architecture Design Document'**: to design the high-level architecture for the HyVICE platform (starting from the analysis of the User Requirements defined in WP2). The functional decomposition of the overall HyVICE system for the full chain is carried out and all the relevant interfaces are identified. Main functional architectural blocks for the HyVICE platform are defined.
- **D3.2 'Detailed Design Document'**: to design the detailed architecture for the HyVICE platform. It defines the interfaces of each HyVICE architectural block of the Laboratory Testing Platform (CEDEX lab) and of the Real Testing Platform (Bologna San Donato).
- **D3.3 'System Requirement Document'**: to define the System Requirements Specification for the HyVICE Platform (starting from the analysis of the User Requirements defined into WP2); it contains the whole HyVICE System and Interface Requirements.
- **D3.4 'Test Plan'**: it defines the Unit and Integration Test Procedures and Plan for the Laboratory Test Platform (CEDEX laboratory) and the On field/Mixed Reality Testing Platform (Bologna San Donato Test site of RFI).
- **D4.2 'Development Report'**: to report about development of each HyVICE subsystem component and of the related testing interfaces and the final system integration for both the Real and the Laboratory testing platforms, including the Unit testing, the Interface testing, the System Integration testing and the integration of the DUT at CEDEX laboratory.
- **D4.3 'Test Report'**: to define test scenarios (GNSS Scenarios, ERTMS Scenarios, etc.) and to execute Tests on both the Real Testing Platform (Bologna San Donato) and the Laboratory Testing Platform (CEDEX laboratory). Tests execution and recording will be carried out according to the prescriptions of D3.4 'Test Plan'. It also includes results of comparison and analysis between the On-field and lab test records.
- **D5.1 'Validation Strategies'**: to propose Validation strategies to be adopted for validation, assessment and certification of the the future GNSS-based train localization solutions (e.g. ASTP), based on validation and test activities carried out by HyVICE platform.
- **D5.2 'Certification On-Board Subsystem'**: based on the DUT adopted in the project and the HyVICE testing and validation platform, a simulated analysis will be carried out in order to evaluate (for demonstration use) the conformity of the On-Board Subsystem to the TSI Essential Requirements, in relation to the validation activities performed in the previous tasks.
- **D5.3 'Certification on Track Subsystem and related System Integration'**: based on the DUT adopted in the project and the HyVICE testing and validation platform, a simulated analysis will be carried out in order to evaluate (for demonstration use) the conformity of the whole on-board system as integrated with the train/ground equipment to the TSI Essential Requirements, in relation to the validation activities performed in the previous tasks.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

In the Figure 2 here below it is illustrated the interrelation scheme among the aforementioned VICE4RAIL deliverables Dx.y respect to the **D2.3 'Certification Plan'** (this document).

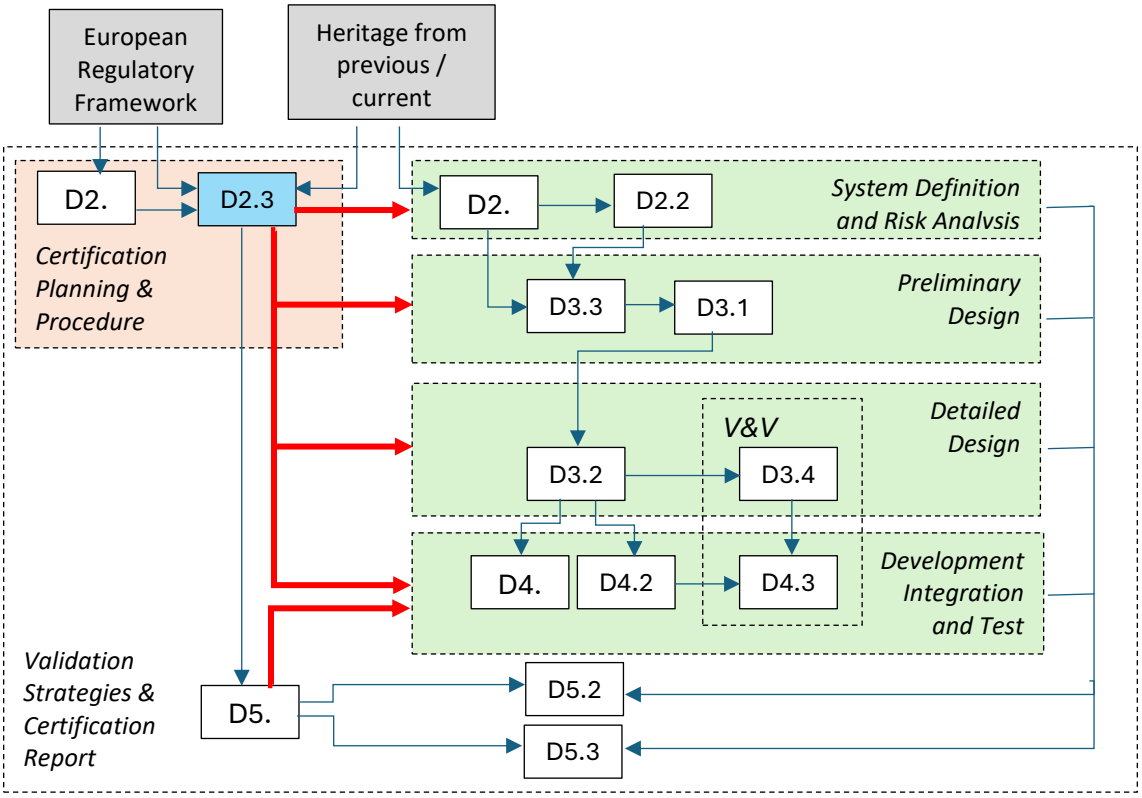

Figure 2 Linkages of D2.3 with other VCE4RAIL deliverables

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

2 Reference Documents

2.1 Regulations, Norms and Standards

[NS.1] Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways (Railway Safety Directive).

[NS.2] Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community

[NS.3] Commission Decision 2010/713/EU of 9 November 2010 on modules for the procedures for assessment of conformity, suitability for use and EC verification to be used in the technical specifications for interoperability adopted under Directive 2008/57/EC

[NS.4] Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009

[NS.5] Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC.

[NS.6] Commission Implementing Regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment

[NS.7] Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union

[NS.8] Directive (EU) 2016/798 of European Parliament and of the Council of 1/05/2016 on railway safety

[NS.9] Regulation (EU) 2018/762 of 8 March 2018 establishing common safety methods on safety management system requirements pursuant to Directive (EU) 2016/798 of the European Parliament and of the Council and repealing Commission Regulations (EU) 1158/2010 and (EU) 1169/2010

[NS.10] Regulation (EU) 2018/858 of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) 715/2007, (EC) 595/2009 and repealing Directive 2007/46/EC.

[NS.11] Commission Implementing Regulation (EU) 2023/1695 of 10 August 2023 on the technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union and repealing Regulation (EU) 2016/919

[NS.12] EN 50126-1: Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process. 2017

[NS.13] EN 50126-2: Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Guide to the application of EN 50126-1 for safety. 2017

[NS.14] EN 50128 Railway Applications: Communications, signalling and processing systems – Software for railway control and protection systems. 2020

[NS.15] EN 50716 Railway applications – Requirements for SW development. European CENELEC standard (2023).

[NS.16] EN 50129: Railway Applications - Safety related electronic systems for signalling. 2018

[NS.17] EN 50159-1 Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

[NS.18] EN 50125-1 - Railway applications - Environmental conditions for equipment - Part 1: Rolling stock and on-board equipment

[NS.19] EN 50125-3 Railway applications - Environmental conditions for equipment Part 3: Equipment for signalling and telecommunications

[NS.20] EN 50155 Type Approval Test on Electronic Equipment for Railway Applications

[NS.21] EN 62061 Safety of machines-functional safety of electrical, electronics and programmable machine controls

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

[NS.22] CEN/EN16803 “Use of GNSS-based positioning for road Intelligent Transport Systems (ITS)

[NS.23] ETSI TS 103 246 Satellite Earth Stations and Systems (SES) - GNSS based location systems (GBLS)

[NS.24] IEC 61508 (1-7): Functional safety of electrical/electronic/programmable electronic safety-related systems, 2010. European Standard

[NS.25] ISO/TR 4804 Road vehicles — Safety and cybersecurity for automated driving systems — Design, V&V. International Organization for Standardization (ISO), international standard (2018).

[NS.26] ISO 21448 Road vehicles. Safety of the intended functionality (SOTIF). International standard (2019).

[NS.27] ISO 26262 Road vehicles – Functional Safety. International Organization for Standardization (ISO), international standard (2018).

[NS.28] RTCM SC-104 / SC-134 papers

[NS.29] IMO SOLAS, 1974

[NS.30] ISO 17894:2005 - Ships and marine technology — Computer applications — General principles for the development and use of programmable electronic systems in marine applications (2005).

[NS.31] ISO/SAE 21434 Road vehicles — Cybersecurity engineering

[NS.32] IEC 60300-1 Dependability management – Part 1: Guidance for management and application. International standard (2014).

[NS.33] CEI IEC 300-3-4 Dependability management – Part 3: Guid to the specification of dependability requirements. International standard (1996).

[NS.34] UNISIG SUBSET-026 v3.3.0, “ERTMS/ETCS System Requirements Specification”

[NS.35] UNISIG SUBSET-036 v.3.0.0, “FFFIS for Eurobalise”

[NS.36] UNISIG SUBSET-040 v.3.2.0 “ERTMS/ETCS- Dimensioning and Engineering rules”

[NS.37] UNISIG SUBSET-041 v.3.1.0, “Performance Requirements for Interoperability”

[NS.38] UNISIG SUBSET-091 v.3.2.0, “Safety Requirements for Technical Interoperability of ETCS in L1 & L2”

2.2 VICE4RAIL Documents

Deliverables of Horizon Europe VICE4RAIL project - Hybrid Virtualized Testing for Certification of GNSS in Railway Train Positioning (2025).

[VC.1] Proposal template Part B: technical description - HYBRID VIRTUALIZED TESTING FOR CERTIFICATION OF EGNSS IN RAILWAY TRAIN POSITIONING - VICE4RAIL

[VC.2] D2.1 Rail User & System Requirements

[VC.3] D2.2 Risk Analysis Evaluation Report

[VC.4] D2.4 Synergies in the Certification Process for Use in Multimodal Transport

2.3 Other Documents

[OD.1] GSA Report - Rail-Report-on-User-Needs-and-Requirements, 2021 (outcome of EUSPA User Consultation Platform)

[OD.2] Smith, D. J. Reliability, Maintainability and Risk: Practical methods for engineers. Sixth edition, 263-264. (Butterworth Heinemann 2003).

[OD.3] Mauer, M. et al. Autonomous Driving: Technical, Legal and Social Aspects. 457-458 (2016).

This project is funded by European Union’s Horizon Europe programme under grant agreement No 101180124

[OD.4] Kilian, P. et all. Safety-Related Availability in the Power Supply Domain. *IEEE Access 10, 47869-47880 (2002).* Available: https://ieeexplore.ieee.org/document/9765464 (Accessed 4 Feb 2025).

[OD.5] Tiemeyer, B. Performance Evaluation of Satellite Navigation and Safety Case Development. *EUROCONTROL Experimental Centre - EEC Report No. 370 (2002)*. [Online]. Available: https://www.eurocontrol.int/sites/default/files/library/002_Satellite_Navigation_Performance.pdf (Accessed 1 Nov 2023).

[OD.6] Roturier, B., Chatre, E. & Ventura-Traveset, J. The SBAS Integrity Concept Standardised by ICAO: Application to EGNOS. *In book EGNOS – A Cornerstone of Galileo*, pp. 43-53 (ESA Publications Division, ESTEC, Noordwijk, 2006). [Online]. Available: http://www.egnos-pro.esa.int/Publications/GNSS%202001/SBAS_integrity.pdf (Accessed 1 Nov 2023).

[OD.7] Smith, D. J. Reliability, Maintainability and Risk: Practical methods for engineers. Sixth edition, 263-264. (Butterworth Heinemann 2003).

[OD.8] International Maritime Organization (IMO). *IMO Resolution A.860(20) Maritime Policy for a Future Global Navigation Satellite System (GNSS). UK* (1997). [Online]. Available: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.860(20).pdf (Accessed 24 Jan 2025).

[OD.9] International Maritime Organization (IMO). *IMO Resolution A915 (22) Revised Maritime Policy and Requirements for a Future GNSS. UK* (2001). [Online]. Available: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.915(22).pdf (Accessed 1 Nov 2023).

[OD.10] Radio Technical Commission for Aeronautics (RTCA). *Minimum Aviation System Performance Standards for the Local Area Augmentation System (LAAS).* RTCA standard DO-245 A, Washington DC (2004).

[OD.11] GNSS User Technology Report. GSA, Issue 3 (2020). [Online]. Available: https://prod5.assets-cdn.io/event/6041/assets/8361034923-231960e68d.pdf (Accessed 1 Nov 2023).

[OD.12] 25E046 version 1 dated 2025-04-10 'LOCALISATION WORKING GROUP (LWG) - EUG Position on BASTP'

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

3 Definitions

In order to guarantee, within the VICE4RAIL project, a common understanding of specific concepts, minimizing the risk of ambiguity and misunderstandings, in the table here below there is a list of standardized definitions of the terms that are commonly used in this document:

Term	*Definition*
Advanced Safe Train Positioning (ASTP)	[VC.2] CCS onboard interoperability constituent, separated from the ETCS on-board by fully standardized interfaces with all connected systems. ASTP shall perform functions for safety relevant applications and be the only source of odometry information in the CCS-OB.
Accuracy	[OD.1] 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. [ASTRail project] (Absolute) Accuracy: the degree of conformance between the estimated position and the true position of the craft (vehicle, aircraft, vessel) at a given time (95% 2σ). This definition is the most conservative to be used in the rail industry.
Assessment Body (AsBo)	[NS.4] the independent and competent external or internal individual, organisation or entity which undertakes investigation to provide a judgement, based on evidence, of the suitability of a system to fulfil its safety requirements [VC.2] its role is to evaluate the risk management processes required under the CSM-RA. AsBos ensure that hazards are identified, mitigated and managed effectively in safety-critical systems. AsBos must be accredited to ensure they meet regulatory requirements. Their assessments are broader in scope, covering not only signaling systems but also rolling stock and operational changes.
Authorization Process	[VC.2] Authorization ensures that certified subsystems and vehicles are safe and compatible with the railway network. This process, governed by the ERA and NSAs, involves detailed assessments of technical documentation and compliance with safety and interoperability requirements. Subsystems such as CCS and trackside infrastructure require an Authorization for Placing in Service (APIS)

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Term	*Definition*
	before deployment. This includes a review of the EC Declarations, safety documentation, and operational testing results. Similarly, vehicles must undergo an Authorization for Placing on the Market (APOM), confirming their compatibility with infrastructure and compliance with rolling stock TSIs. These authorizations are essential steps in achieving a fully interoperable and safe railway system.
Availability	[NS.12] ability of an item to be in a state to perform a required function under given conditions at a given time or over a given time interval, assuming that the required external resources are provided
Black Box (functional) testing	[NS.14] test to confirm that the component performs its intended functions
Certification Process	[VC.2] Certification verifies that railway subsystems and components meet the essential requirements of interoperability, safety, and reliability as defined by EU directives and TSIs. The process involves Conformity Assessment Bodies (CAB), which evaluate the design, production and performance of subsystems against relevant standards. EC verification is a structured process that assesses technical documentation, production methods, and operational tests. CABs are authorized to inspect and validate that the subsystem's performance aligns with the applicable TSIs and European standards. Upon successful completion, an EC Declaration of Conformity or EC Declaration of Verification is issued, demonstrating the readiness of the subsystem for integration into the railway system.
Common Safety Methods (CSMs)	[NS.8] methods describing assessment of safety levels, achievement of safety targets and compliance with other safety requirements
Conformity Assessment	[NS.3] Process demonstrating whether specified requirements relating to a product, process, service, subsystem have been fulfilled
Conformity Assessment Body	[NS.7] Body that has been notified or designated to be responsible for conformity assessment activities, including calibration, testing, certification and inspection; a conformity assessment body is classified as a 'notified body' following notification by a Member State; a conformity assessment body is classified as a 'designated body' following designation by a Member State (Article 2(42) of Directive (EU) 2016/797)
Continuity / Continuous Train Localization	[STARS project] Continuity: a specification of an intended operation named mission, during which the reference function must not be interrupted accidently (assuming that the function was available at the beginning of the operation). In the railway case the reference function is the train positioning function. [ASTRail project] Continuity: the ability of the total system (comprising all elements necessary to maintain aircraft position within the defined airspace) to perform its function without interruption during the intended operation. More specifically, continuity is the probability that the specified system performance will be maintained for the duration of

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Term	*Definition*
	a phase of operation, presuming that the system was available at the beginning of that phase of operation and was predicted to operate throughout the operation. Continuity (of a system): is the ability of the system to perform its function without interruption during the intended operation i.e. the probability that the specified performance will be maintained for the duration of a phase of operation. The continuity requirement should be applied as applying the average risk of loss of service. The continuity of the system is a critical performance parameter for aviation. It is defined as (ICAO 2006).
Designated Body	[VC.2] Operate within the framework of National Technical Rules (NTRs) to ensure subsystems meet specific national requirements not covered by TSIs. They are appointed by Member States to verify conformity against national regulations. Some DeBos also act as AsBos to avoid redundant assessment processes.
EC verification	[NS.3] the procedure referred to in Article 18 of Directive 2008/57/EC whereby a NoBo checks and certifies that the subsystem complies with Directive 2008/57/EC, relevant TSI(s) and with the other regulations deriving from the Treaty, and may be put into operation.
Essential Requirements	[NS.2] all the conditions set out in Annex III which must be met by the rail system, the subsystems, and the interoperability constituents, including interfaces;
Harmonised standard	[NS.3] any European standard adopted by one of the European standardisation bodies listed in Annex I to Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services (1) in connection with a mandate by the Commission drawn up in accordance with the procedure referred to in Article 6(3) of that Directive, which, by itself or together with other standards, provides a solution as regards compliance with a legal provision;
Independent Safety Assessors	[VC.2] Provide third-party assessments of the safety integrity of railway systems and their compliance with safety standards, including those defined by CENELEC (e.g., EN 50126, EN 50128, and EN 50129). ISAs ensure the robustness and reliability of GNSS applications in railways. Although ISAs are not required to be formally accredited, they must be accepted or licensed by a recognized safety authority. [NS.12] process to determine whether the system/product meets the specified safety requirements and to form a judgement as to whether the product is fit for its intended purpose in relation to safety
Integrity	[OD.1] 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.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Term	*Definition*
	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. [ASTRail project] Integrity: is a measure of the trust that can be placed in the correctness of the information supplied by the total system. It includes the ability of a system to provide timely and valid warning to the user (alerts) when the system must not be used for the intended operation (or phase of flight). Integrity: the measure of trust that can be placed in the information provided by the PNT system, including the ability to provide timely warnings when the system should not be used.
Interoperability	[NS.2] the ability of a rail system to allow the safe and uninterrupted movement of trains which accomplish the required levels of performance for these lines. This ability depends on all the regulatory, technical and operational conditions which must be met in order to satisfy the essential requirements. For control-command and signalling subsystems, essential requirements are set out in Annex III to Directive (EU) 2016/797 and then furtherly developed in the Regulation (EU) No 1695-2023 (TSI CCS).
Interoperability Constituent	[NS.3] any elementary component, group of components, sub-assembly or complete assembly of equipment incorporated or intended to be incorporated into a subsystem, upon which the interoperability of the rail system depends directly or indirectly. The concept of a 'constituent' covers both tangible objects and intangible objects such as software
Notified Body (NoBo)	[NS.2] the bodies which are responsible for assessing the conformity or suitability for use of the interoperability constituents or for appraising the 'EC' procedure for verification of the subsystems [VC.2] Appointed by member states and responsible for third-party assessment of interoperability constituents and structural subsystems, ensuring compliance with the applicable TSIs. Their role includes verifying EC conformity, issuing intermediate statements of verification, and checking the correctness of ETCS system compatibility reports
Risk Assessment	[NS.4] the overall process comprising a risk analysis and a risk evaluation (where 'risk analysis' means systematic use of all available information to identify hazards and to estimate the risk and 'risk evaluation' means a procedure based on the risk analysis to determine whether an acceptable level of risk has been achieved)
Risk Acceptance Criteria	[NS.4] the terms of reference by which the acceptability of a specific risk is assessed; these criteria are used to determine that the level of

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Term	*Definition*
	a risk is sufficiently low that it is not necessary to take any immediate action to reduce it further
Safety Acceptance	[NS.4] status given to the change by the proposer based on the safety assessment report provided by the assessment body (AsBo) [NS.17] safety status given to a product by the final user
Safety Approval	[NS.17] safety status given to a product by the requisite authority when the product has fulfilled a set of predetermined conditions
Safety Integrity	[NS.17] 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 duration
Safety Integrity (SIL)	[NS.17] one of a number of defined discrete levels for specifying the safety integrity requirements of safety-related functions to be allocated to the safety-related systems
Safety Requirements	[NS.4] the safety characteristics of a system and its operation (including operational rules) and maintenance necessary in order to meet legal or company safety targets
THR (Tolerable Hazard Rate)	[ASTRail project] In terms of rail applications, THR of positioning system is directly related to undetected faults that could lead to an accident, and the system must detect these hazardous faults in the underlying GNSS within known time before the navigation error is greater than a certain established amount. The faster is the detection, the smaller is maximum allowed error amount, the greater is the system availability (higher train speed and shorter headways). The maximum allowed THR (i.e. undetected hazardous faults) to achieve SIL4, required for train positioning, is $1e^{-8}$ per hour per function.
Validation Process	[NS.17] confirmation, through objective evidence, that requirements for a specific intended use or application have been fulfilled
Verification Process	[NS.17] confirmation, through the provision of objective evidence, that specified requirements have been fulfilled
White Box (structural) testing	[NS.14] test to check how the internal parts of the component interact to carry out the intended functions and to confirm that all parts of the component are tested

Table 1: List of Definitions

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

4 Definition of the scope of the Certification process

4.1 Definition of the 'Device-Under-Test' (DUT)

As explained in the document 'D2.1 Rail User & System Requirements' [VC.2], the ASTP (Advanced Safe Train Positioning) solution has been selected by 'Europe's Rail Joint Undertaking' (ERJU) as the solution for future standardization, being a modular/scalable component within the CCS on-board architecture that provides localization information to multiple on-board users (e.g. ETCS-OB) through standardized interfaces. In particular, the ASTP solution has been incorporated into the 1st version of the 'Standardization and TSI Input Plan' (STIP), that reports the indications that European Community (EC) and European Union Agency for Railways (ERA) should adopt to define priorities for the evolution of TSIs, as developed by the System Pillar of ERJU (see also [OD.12] for further details).

ASTP deployment has been structured in 2-phase incremental approach:

- Phase 1 (Basic ASTP, planned for TSI 2027): focuses on enhancing odometry performance and defining interface between ASTP and EVC (European Vital Computer); standardization of GNSS augmentation or Digital Maps is not included yet (i.e. the use of virtual reference points is not yet possible).
- Phase 2 (Full ASTP, planned for TSI 2032): aims for a more comprehensive implementation, incorporating absolute positioning capabilities and the potential use of GNSS augmentation, including EGNOS. This phase may allow for the use virtual reference points.

The integration of ASTP in the STIP framework represents a significant institutional endorsement for GNSS-based train positioning in the European railway. This inclusion establishes ASTP as the officially recognized pathway toward standardization and incorporation of GNSS-based solutions into future TSIs by 2032.

According to STIP, 'Full ASTP with GNSS Augmentation and Digital Maps' is the satellite-based positioning solution under consideration for inclusion in the future TSI. Consequently, the VICE4RAIL project strategically aligns with this European standardization trajectory by adopting the Full ASTP requirements as the primary basis for its developmental baseline and so contributes to develop a HyVICE platform capable of addressing the most advanced Use Cases. Nevertheless, the flexible, modular and scalable approach used in designing and developing the HyVICE architecture will make that HyVICE platform can support also other relevant solutions for GNSS-based train localization such as solutions based on the 'Virtual Balise' paradigm. VICE4RAIL project's architecture and certification methodologies will be designed to demonstrate this flexibility.

At the current status of the VICE4RAIL project, the HW and SW configuration of the 'Device Under Test' (DUT) that will be used for in-lab tests (at CEDEX laboratory) and for on-site tests (at Bologna San Donato Test site) have not been defined and agreed yet; when the HW and SW features of the 'selected' candidate for DUT have been defined and agreed, the present document will be updated accordingly.

4.2 Definition of the 'HyVICE testing environment'

The VICE4RAIL project focuses on creating a flexible and scalable certification framework (HyVICE) that can accommodate the diverse operational environments in which GNSS-based train localization technologies are deployed, including complex urban and rural areas where GNSS signal performance can vary significantly.

By developing a robust testing environment that combines real-world data and advanced simulation techniques, VICE4RAIL project ensures that the future certification process of GNSS-based train localization solutions can reliably account for GNSS-specific issues like multipath interference and signal degradation.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

The HyVICE platform is envisaged as a comprehensive environment combining laboratory simulations (at CEDEX ERTMS Simulation Lab) and realistic on-field testing (at Bologna San Donato RFI Test Circuit), by also taking advantages from the experience accumulated in the RFI field campaign in the Novara-Rho Italian line in order to support future certification of GNSS-based train positioning systems, aiming to SIL4 (essential for safety-critical rail applications) for the whole system functional chain GNSS+ERTMS/ETCS.

4.2.1 CEDEX ERTMS Simulation Laboratory

CEDEX laboratory is an accredited lab for functional validation, integration and testing of ERTMS components, and has collected deep experience on testing ETCS trackside implementations and onboard integration into the line at operational level.

At the current status of the VICE4RAIL project, the proposed general definition level of the CEDEX ERTMS Test Lab architecture includes the equipment/components that are illustrated in Figure 3 here below; when the HW and SW features of the CEDEX ERTMS Test Lab architecture have been defined and agreed, the present document will be updated accordingly.

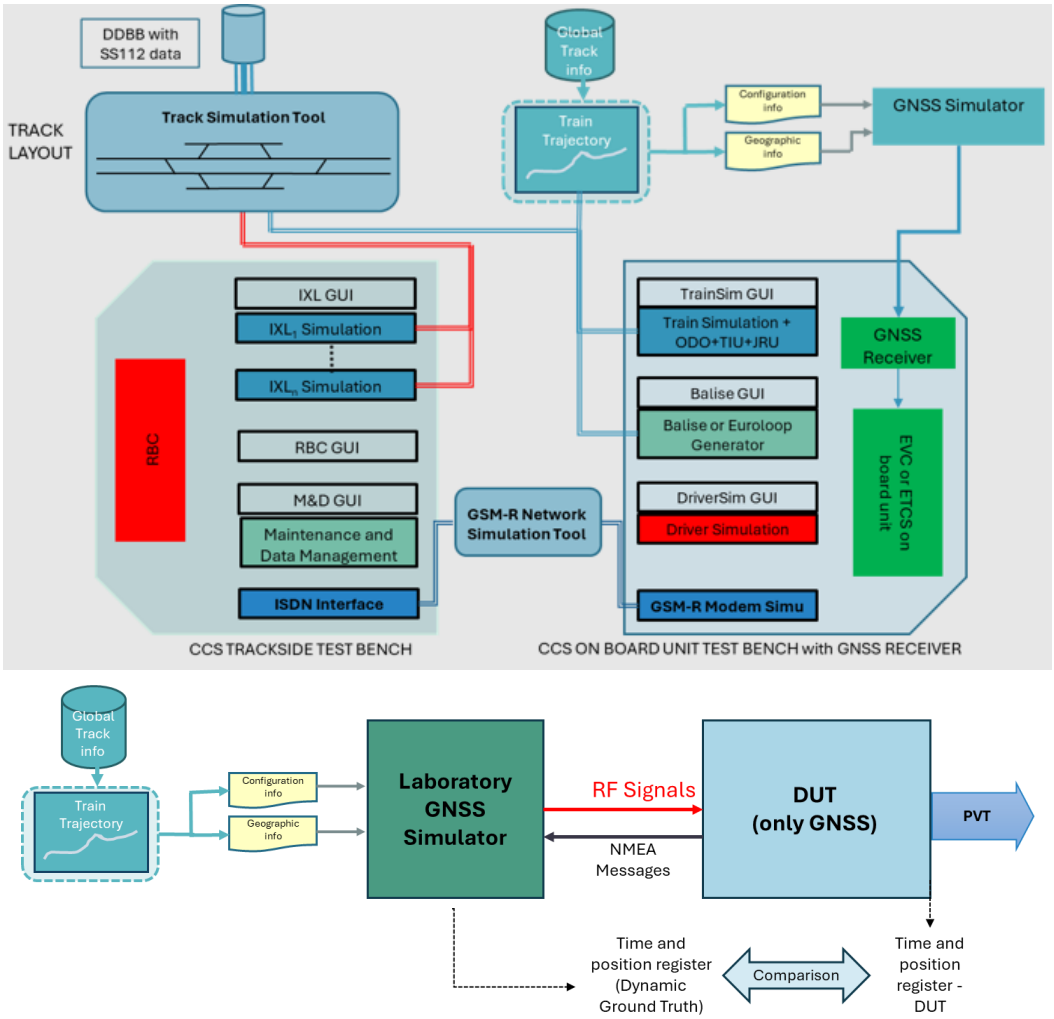

Figure 3 CEDEX ERTMS test lab (VICE4RAIL architecture)

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

The architecture of the CEDEX laboratory will be particularized for the VICE4RAIL project and the final blocks to be used will be defined according to the DUT provided for the tests.

As shown in the previous figure, CEDEX laboratory is equipped with a GNSS Signal Simulator, which allows to simulate the GNSS signals from different satellite constellations, having the possibility of adding effects such as multipath, signal power loss or interferences.

The GNSS simulator available at CEDEX laboratory is the GSG8+Skydel simulator. This simulator allows to generate the GNSS signals to be injected in a GNSS receiver or, in the VICE4RAIL case, an emulated DUT. The availability of this simulator allows to test a GNSS DUT, as shown in the scheme here below:

4.2.2 Bologna San Donato test circuit

In the context of the VICE4RAIL project, the integration of the 'Bologna San Donato test circuit' is a fundamental milestone in the execution of field tests on the selected DUT; the process involves the creation and validation of virtual models for the GNSS electromagnetic environment and it encompasses collaborative testing of GNSS and IMU technologies, exposing the GNSS to a blend of real and synthetic data while the IMUs navigate authentic real-world scenarios.

HyVICE field testing in Bologna aims to:

- Create and validate virtual models for the GNSS electromagnetic environment.
- Jointly test and certify GNSS + IMUs, through procedures for which GNSS receiver can receive either real or synthetic data, or a blend of them, while IMUs experience real train dynamics.
- Add interferences (jamming and spoofing) to real GNSS signals, to test vulnerability/resilience of both signal and data processing stages.

In the picture here below it is reported, at the current stage of the project, the functional architecture of the 'Bologna San Donato Testing Circuit'; when the HW and SW features of the 'Bologna San Donato Testing Circuit' have been defined and agreed, the present document will be updated accordingly.

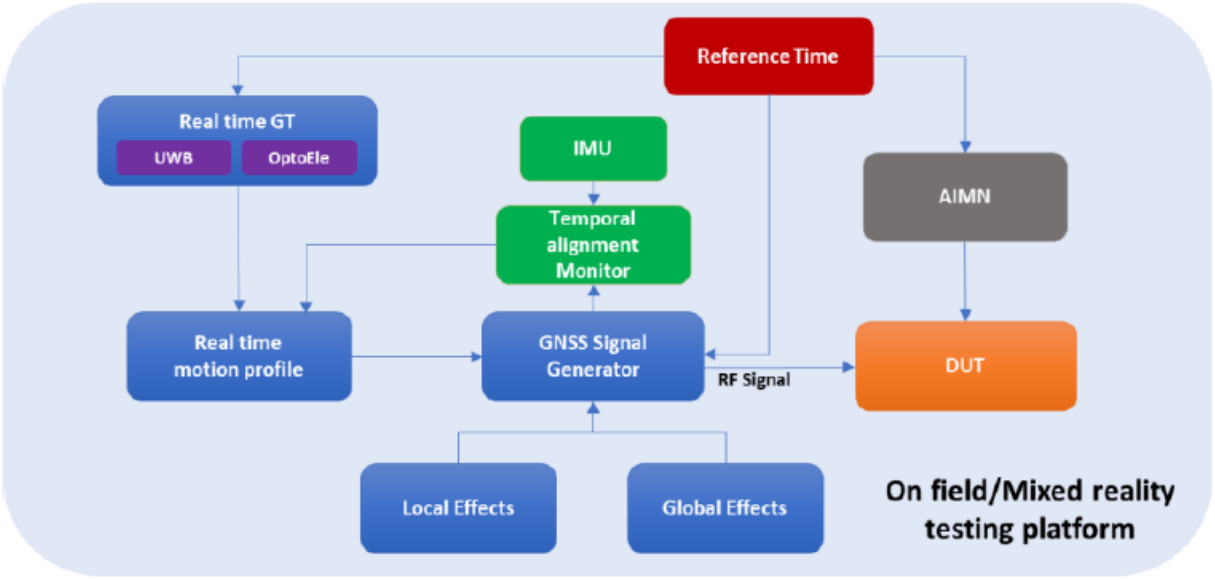

Figure 4 RFI Bologna San Donato Testing Circuit [VC.1]

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

4.2.3 Novara – Rho Pilot Line

The definition of the validation procedure for the HyVICE platform will benefit from the know how acquired by means of the 'Novara – Rho Pilot Line' activities; this line was funded by RFI to integrate GNSS positioning into the ERTMS system, including validation and certification of a specific GNSS solution and of a communication system integrating Satcom technologies with public cellular networks. Actually, the Novara-Rho line is the first example in Europe undergoing the validation and certification process of a GNSS-based ERTMS solution. VICE4RAIL project will exploit the contribution of the Novara - Rho pilot line to make a further step towards a standardizable approach in the Conformity Certification and Assessment process.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

5 Synergies with past and current projects

The VICE4RAIL project can exploit the expertise cultivated in various national research initiatives by leveraging insights from ongoing projects funded by entities such as EUSPA, ESA, and Shift2Rail. The starting point are the results of past and on-going projects which have demonstrated the feasibility of using GNSS applications in the context of the ERTMS namely, STARS, ERSAT EAV, ERSAT GGC, GATE4RAIL, HELMET, X2RAIL-2, X2RAIL-5, CLUG, VOLIERA, SBS, EGNSS MATE, RAILGAP, R2DATO, complemented by the results of the 'Pilot Line Novara-Rho' (commissioned by RFI for the assessment and certification of integration of the GNSS technology in the ERTMS L2 system) and of the 'Cagliari-S. Gavino' line.

In particular, activities to support the validation and certification phase of the "virtual balise" functionality were commissioned by RFI on the 'Pilot Line Novara-Rho', where ERTMS L2 is already activated and in operation. The aim of the assessment activities was to:

1) Assess that the specific solution (Reference Stations and Virtual Balise Reader) meets the safety requirements identified during the risk analysis (SIL4).
2) Ensure the additional GNSS-based solution functions do not lead to conflicts with implemented functions specified in CCS-TSI. The on-board and RBC Generic Application have been assessed according to the SIL4 level defined in the CENELEC standards.
3) At functional level, verify the non-intrusiveness of the additional satellite-related hardware with respect to signalling equipment already in service on the "Novara-Rho" Pilot Line.

The VICE4RAIL project aims to take advantage form past experience accumulated in previous projects related to GNSS-based ERTMS applications; NoBo(s) have been involved in similar projects to evaluate the application of virtual balises as:

1) ERSAT-EAV: virtual balises managed by satellite receiver, integrated into the ERTMS signalling system
2) Novara-Rho railway line: experimental ERTMS L2 variant with satellite positioning
3) Rail certification roadmap definition for the Contract No GSA/OP/07/13: provision of technical assistance in the GNSS market technology monitoring

The approach adopted by VICE4RAIL project will emphasize GNSS continuity and utilization of multi-modal augmentation network and certification paths by leveraging on Rail, Automotive and Maritime common user needs; to facilitate this, a liaison will be established with the RTCM SC 134 Standardization Group "Integrity for GNSS-based High Accuracy Applications".

VICE4RAIL project will also ensure synergies with the R2DATO project, by considering as input the strategy and general requirements for a common virtual assessment and certification process ("Testing, validation and certification" work packages WP34/35); actually, operational requirements, system capabilities and system architecture for 'Absolute Safe Train Positioning' systems as defined in the R2DATO project will be relevant to properly identify the potential systems under test and the test environments in VICE4RAIL.

Additionally, a specific liaison with the results of the GATE4Rail project will be pursued since the GATE4Rail project itself provided a laboratory test architecture capable of simulating railway scenarios for GNSS-based ERTMS applications that allows to move towards a zero-on-site testing paradigm.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

6 Certification process in multimodal transport

The aim of this section is to review safety assessment and certification procedures for GNSS-based positioning in the rail, automotive and maritime sector to identify common elements of certification schemes to make the certification of multimodal positioning solutions more efficient. The central idea of this part, and a common element to be used for the safety assessment and certification of GNSS-based positioning, is the continuity of the GNSS SoL service, originally developed for aviation, and its effective use in land transport. It is described below how to interpret GNSS continuity in terms of GNSS reliability, which is necessary for both safety system design and certification. The description is based on the deliverable 'D2.4 - Synergies in the certification process for use in multimodal transport of the VICE4RAIL project' [VC.4].

6.1 GNSS continuity: common element for safety assessment and certification in multimodal transport

For safe and efficient operation of ERTMS with GNSS-based train positioning, it is necessary to demonstrate not only the required integrity (i.e. correctness), but also reliability, which depends significantly on GNSS continuity. Continuity means the probability of providing a position with the required accuracy and integrity without unscheduled interruptions during the most critical phase of the operation - which is, e.g., during the 15 s before the aircraft descends to the decision height (DH of 60 m) in the case of a Category I (CAT I) precision approach and landing. In recent railway oriented GNSS R&D projects, railway stakeholders have not yet clearly specified how to properly exploit the guaranteed continuity of GNSS - although the aeronautical requirement for continuity significantly determines the cost of GNSS infrastructure. GNSS continuity analysis and methods for increasing the reliability of GNSS-based train localization and safety of positioning in maritime and advanced automotive applications are currently being used within the EU VICE4RAIL project to develop plans and procedures for the certification of GNSS-based positioning in multimodal transport.

6.2 Objectives and methodology used

One of the aims of this work is to close the gap regarding GNSS continuity issues by clarifying: 1) where the requirement for GNSS continuity comes from, 2) why GNSS continuity is needed in land transport, and 3) how GNSS-based applications can be made more reliable when needed. Using a comparative analysis, the continuity requirements in aviation, rail, maritime, and road transport have been investigated showing their importance for railways and automotive control.

Although GNSS meets very stringent aviation requirements, it does not necessarily mean that it is suitable for use in other transport sectors. In this section, we focus on GNSS continuity - its correct interpretation and use in land transport, especially in terms of meeting the requirement for reliability of position, velocity, and time (PVT) determination considering the Railway environment. The aim of this effort is to start with the aviation continuity requirement set for GNSS Safety-of-Life (SoL) service to evaluate potential benefits of reusing this GNSS continuity attribute in other modes of transport. The goal is to increase the reliability of GNSS positioning to the level required by land transportation. The methodology is based on (i) well-defined International Civil Aviation Organization (ICAO) required navigation performance (RNP) in terms of accuracy, integrity, continuity and availability for the GNSS SoL service, (ii) interpretation of these GNSS quality metrics in terms of failure modes and associated failure probabilities, and (iii) the use of the railway safety and dependability concept, in the sense of railway RAMS, as a variant to the aeronautical safety concept, in the RNP sense, for comparative analysis and further investigation.

Availability is generally dependent on reliability and in case of aviation requirement for continuity of GNSS service, it can be expressed in terms of reliability. In the field of automated driving of cars, where the performed driving functions cannot be interrupted for safety reasons, then Safety-Related Availability (SaRA)

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

[NS.27] requirements must be defined for these functions. In maritime transport, as in aviation, GNSS continuity is one of the two main safety attributes, i.e. next to integrity. The criticality of continuity for safety, reliability and availability of GNSS applications has long been often overlooked in automotive and rail transport. Therefore, the central idea in this section is mainly aimed at leveraging GNSS service continuity in land transportation and its inclusion in related tasks in the area of safety assessment and certification. The diversity and synergies associated with the use of GNSS in multimodal transport made it possible to form the necessary opinion on the possible use of aviation GNSS continuity in other modes of transport.

Since it is assumed that the analysis of the reliability of vehicle positioning based on GNSS is also required in other transport sectors, not only in railways (aviation, maritime, automotive), it was necessary to carry out preparatory work before performing this analysis. This preparatory work consisted in describing the basic differences in safety concepts in multimodal transport, analysing and comparing the relevant functional safety standards and regulations for safety assessment and certification in given application areas, and clarifying the terminology of safety and dependability - especially in connection with the recent introduction of the automotive safety standard ISO/TR 4808 [NS.25] on dependability of Automated Driving Systems (ADS). Note: in this standard the term dependability is referred to by the acronym RAMSS, which includes Reliability, Availability, Maintainability, Safety and Security. It was also necessary to clarify the automotive term SaRA used to achieve ADS safety in this context. The analysis in this section also includes other synergies, such as the use of the automotive concept SOTIF (Safety of the Intended Functionality) [NS.26], verification and validation based on simulations in the sense of automotive safety standards and other methods.

6.3 Certification of Safety systems in transport

Certification of safety systems in individual areas of surface transport is carried out according to specific regulations for the given area – see below.

Automotive: Before a new model of vehicle is to be placed on the EU market, it must pass through a so-called type-approval process, i.e. homologation. Within this process national authorities in EU Member states certify that the model of a vehicle (or its part) satisfies all EU safety, environmental and production requirements. This type-approval process shall be performed according to the Regulation (EU) 2018/858 [NS.10], which establishes the harmonised framework for approval of motor vehicles. The manufacturer shall submit according to the above regulation the application accompanied by the information folder to the *approval authority* in each Member State. If all relevant requirements are met, the national authority delivers an EC type-approval certificate to the manufacturer authorizing the sale of the vehicle type in EU. After that the manufacturer issues a Certificate of Conformity, which accompanies every produced vehicle.

The certification process is based on a mutual recognition, i.e. cross-acceptance of approvals by national approval authorities in EU Member States. A detailed chronology of different regulations towards type-approval process of road vehicles with automated driving in Europe and amendment of Regulation (EU) 2018/858 [NS.10] by Regulations (EU) 2019/2144 and 2022/1426 is outlined in Figure 13.

Maritime: The enforcement of the international SOLAS (Safety of Life at Sea) convention is carried out in Europe by the Marine Equipment Directive (MED) 2014/90/EU [NS.5], which repeals Council Directive 96/98/EC of 20 December 1996 on marine equipment. Through the directive the European Union has acted to harmonise testing standards and certification for marine equipment in the EU. The directive requires that equipment installed on the ship shall be certified by a type-approval leading to a certificate. The conformity assessment is carried out by specialised entities, known as Notified Bodies.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

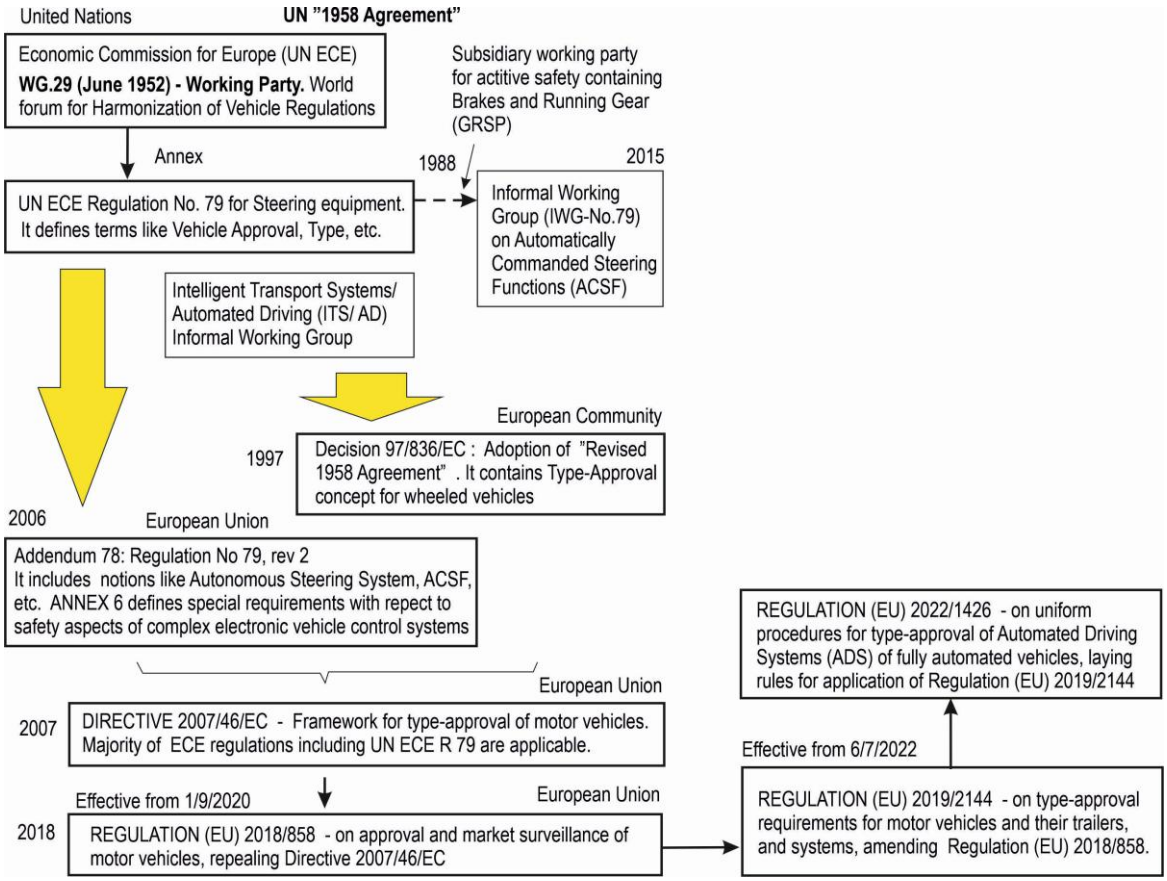

Figure 5 regulations towards type-approval process of vehicles with automated driving [VC.4]

Railway: The basic framework for ensuring the safety and dependability of railway systems is defined in EN 50126 (1-2) [NS.12], [NS.13] on the specification and demonstration of RAMS (Reliability, Availability, Maintainability and Safety). The framework can be imagined as an umbrella under which a safety-related system is subsequently developed and implemented according to the downstream standards EN 50129 [NS.16] (safety-related system), EN 50716 [NS.15] (software for safety-related system), and others. Safety shall be demonstrated by means of a safety case and independent third-party assessment. The safety case and its independent assessment alone is still not enough to ensure safety on European railways. Technical interoperability must also be ensured. In the case of ERTMS, e.g., this means that one manufacturer's on-board equipment works correctly with another manufacturer's track-side equipment. Therefore, certification according to the Technical Specifications for Interoperability (TSI) must be carried out. But even this may not be enough to ensure safety. In the case of a change in the railway system from a safety point of view, the so-called Common Safety Method for Risk Evaluation and Assessment (CSM-RA) according to Regulation (EU) 402/2013 [NS.4] and its amendment (Regulation (EU) 2015/1136), which harmonises the risk assessment process and safety requirements, must be applied.

The example of railways has shown that the safety of systems is proven based on a safety case, which is developed according to the relevant (railway) safety standards. The safety case supports certification. A similar procedure is required in the case of automotive or ship safety systems, where it is also necessary to develop and independently assess the safety case for the system according to the relevant safety standards for the given application area (automotive, marine).

From the above, it is clear that in order to exploit synergies and identify common elements in the certification process of GNSS-based systems for multimodal transport, it is also necessary to take into account the safety concepts used (types of safety systems) and to compare and analyze relevant safety standards, especially

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

with regard to the safety and reliability attributes used. Only then can one consider how effectively common elements can be used in the certification process for GNSS-based vehicle positioning in multimodal transport.

Correct and effective use of GNSS for safety applications in multimodal transport depends on the type of safety system for which GNSS will be used and the associated safety concept. Therefore, two basic types of safety systems are mentioned below: (i) safety-related and (ii) safety-critical [OD.2], [OD.3].

A safety-related system: Hazard as a dangerous system failure does not lead to an accident in a properly designed system. This is because the system is capable of entering or maintaining a safe state in the event of a hazardous failure. From a safety point of view, it is not necessary to complete the safety operation.

A safety-critical system: Safe completion of the operation is required in the event of a fault. A dangerous fault here leads directly to an accident. This is what we want to prevent, and that's why a human or machine supervises. We define an emergency operation to ensure safety after response to a dangerous fault. The emergency operation is not a safe state (in case of dangerous failure) but leads to a safe state. Following safety measures, which include safety mechanism as a technical solution, can be applied: (i) fault avoidance, (ii) fault forecasting and (iii) fault tolerance.

6.4 Functional safety standards

IEC 61508 [NS.24] is a basic functional safety standard applicable to safety-related systems in all industries that incorporate Electrical and/or Electronic and/or Programmable Electronic (E/E/PE) devices. It is also the parent standard that has been used to create application-specific safety standards such as EN 50129/ EN 50126 (1-2)/EN 50716 (from [NS.12] to [NS.16]) for railways, ISO 26262 (1-12) [NS.27] for automobiles, IEC 61511 for a process industry, etc. The fundamental safety concept according to IEC 61508 is that any safety-related system must work correctly or fail in a predictable (safe) way.

Automotive: ISO 26262, ISO/PAS 21448 (SOTIF) and ISO/TR 4804

A safe Automated Driving System (ADS) means that all hazards associated with ADS operation are fully under control using safety functions with the required safety integrity. The basic functional safety standard used for development and safety demonstration of ADS is ISO 26262 (1-12):2018 [NS.27]. It is an adaptation of the IEC 61508 (1-7): 2010 [NS.24] functional safety standard for automotive Electrical/Electronic (E/E) systems. ISO 26262 aims to eliminate potential hazards caused by malfunctioning E/E systems in vehicle. Malfunctioning behaviour of the system is caused by a failure or unintended behaviour of the system with respect to the intended design. Risk of hazardous operational situations is qualitatively assessed by means of Automotive Safety Integrity Levels (ASILs). Safety measures are defined to avoid or control systematic faults and to detect or control random hardware failures or mitigate their effects.

ISO 26262 covers functional safety of automotive E/E equipment in the event of HW failures and SW faults throughout the entire life-cycle of the equipment. However, this standard does not apply to vehicle safety in the absence of E/E equipment failure, e.g., in the event of ADS malfunction due to human driver error or unforeseen changes in a complex operating environment. This has led the automotive industry to start addressing hazardous behaviour of systems caused by insufficiencies in the system design and limitations in system performance. Therefore, the ISO/PAS 21448 standard [NS.26] was developed and is referred to as SOTIF (Safety Of The Intended Functionality). The purpose of SOTIF is to mitigate: (1) risk due to unexpected operating conditions including incorrect user (human driver) behaviour, and (2) insufficiencies in requirements specifications. This standard focuses mainly on design guidelines and procedures for validation and verification (V&V) to reduce the residual risk associated with hazards under fault-free (but not error-free) conditions. Safety issues are then resolved by functional modifications.

A function mitigating risk can be considered safe if ISO 26262 (functional safety) and ISO/PAS 21448 (SOTIF) standards are applied. However, vehicles cannot be in a safe state without secure operation. To cover the whole area of ADS safety, the ISO/TR 4804 standard (Road vehicles - Safety and cybersecurity for automated

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

driving systems - Design, verification and validation) was developed [NS.25]. The intention of ISO/TR 4804 is to put together standards ISO 26262 (functional safety), ISO/PAS 21448 (SOTIF) and ISO SAE 21434 (cyber security) under one risk-based approach and create the automotive dependability concept RAMSS (i.e. Reliability, Availability, Maintainability, Safety and Security). ISO/TR 4804 describes how the three dependability domains, i.e. functional safety, the safety of the functional functionality, and cybersecurity, work together and how to combine them to create a dependable system.

Maritime: ISO 17894

In the maritime sector, there is a standard for the development and use of shipboard electronic systems based on functional safety: ISO 17894:2005 [NS.30] standard entitled "Ships and marine technology - Computer applications - General principles for the development and use of programmable electronic systems (PES) in marine applications". It is an adaptation of the generic standard on functional safety IEC 61508:2010 [NS.24]. It also provides references to other standards that must be followed when developing PES.

ISO 17894:2005 provides a set of 20 mandatory principles, recommended criteria and associated guidance for the development and use of dependable marine PES for shipboard use. The principles for PES and related guidance cover the entire life cycle of the equipment. For example, Principle 1 generally defines PES safety defined by the absence of unacceptable risk; Principle 13 states that the required level of PES safety must be implemented throughout the life cycle; and Principle 15 states that verification and validation (V&V) activities must also be performed throughout the PES life cycle.

The ISO 17894 standard states that the overall ship system consists of interlinked PES and crew which work together to meet the operator's business goals for the ship. For this total system to be dependable, both the design of the PES and the management of its use have to support the safe and effective performance of the crew as a critical component of the total system [NS.30]. From the above statement, it follows that the highest quality attribute of a ship system is dependability, which includes safety and efficiency. The combination of the quality of PES and the skills of the crew is called a "human-centred" approach in this standard. Based on the analysis of ISO 17894, it can be assumed that obviously security is also part of maritime safety, and the concept of efficiency mainly includes availability and other attributes on which availability depends (reliability, maintainability and maintenance assurance).

Railway: EN 50126-1, EN 50126-2, EN 50716 and EN 50129

Basic railway safety standards have already been mentioned in section 6.3 of this deliverable. More detailed description of standards can be found in D2.1 of VICE4RAIL [VC.2].

6.5 Clarification of dependability and RAMS terminology

It was the release of the automotive standard ISO/TR 4804 [NS.25] in 2020 that caused confusion among the long-used railway terms dependability (RAM), RAMS and a newly introduced automotive dependability (RAMSS). To use these quality metrics correctly for GNSS applications in multimodal transport, it was first necessary to clarify discrepancies among them (see [VC.4]).

It has been found that both railway RAMS and automotive RAMSS includes all safety provisions (technical, operational and organizational including maintenance) to achieve and maintain full safety. Dependability in automotive industry corresponds to RAMSS (ISO/TR 4804:2020), but the railway RAMS (EN 50126:2017) doesn't correspond to the generic definition of dependability (IEC 60300-1: 2014) [NS.32], because the safety included in generic dependability doesn't contain safety that is ensured by operational and organisational measures, i.e. non-technical measures.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

These facts can be summarised as follows:

- Railway RAMS (EN 50126:2017 [NS.12], [NS.13]) ≠ dependability (IEC 60300-1: 2014 [NS.32])
- Railway RAMS = dependability (IEC 300-3-4:1996 [NS.33], IEC 60300-1: 2014) + (full) safety
- Automotive RAMSS = automotive dependability (ISO/TR 4804:2020 [NS.25])

GNSS performance specified in terms of service integrity and continuity for multimodal transport applications follows on from the above basic metrics in terms of RAMS or RAMSS. It is only necessary to correctly interpret the GNSS attributes for the given multimodal application. This interpretation will depend on the type of safety function for which the GNSS service will be used - whether it will be e.g. a safety-relevant function (with fail-safe state) for rail applications or a safety-critical function for automotive ADS, where emergency operation and Safety-Related Availability (SaRA) requirement, depending on reliability/ continuity, shall be defined.

As mentioned above, the central idea and common element for safety applications of GNSS in multimodal transport is the correct interpretation of GNSS service continuity. This is needed for system design, safety assessment and certification. However, for automotive ADS, the SaRA attribute is also important, which is described in the following section.

6.6 Safety-related availability for automotive safety-critical systems

Many functionalities in automated driving systems (ADS) of car cannot lead to hazard, because a fail-stop or fail-soft (reduced system performance) behaviour is activated if the system fails. However, in some cases hazard identification and risk assessment shows that a loss of a certain functionality can lead to a hazardous event. It is e.g. vehicle positioning based on GNSS during overtaking or lane changing when ADS is applied. Then the SaRA requirements must be defined for the functionality according to ISO 26262-10 [NS.27].

The need for SaRA requirements is determined based on Hazard Analysis and Risk Assessment [NS.27]. A SaRA requirement is initially derived for a system because HARA is generally performed on system level (see [OD.4]). The operational state of the vehicle determines whether the vehicle's functionality (or system) is considered as safety-critical. The vehicle operation state is defined as by the combination of the operational mode and the operational situation. If loss of the vehicle function cannot lead to hazardous event, then the function is deactivated, and thus safe state is achieved. In the opposite case a SaRA requirement must be defined to meet a safety goal (SG). SaRA is a requirement that can be met through implementation. To meet SaRA requirements, the following safety measures, which include safety mechanism as a technical solution, can be applied: (i) fault avoidance, (ii) fault forecasting and (iii) fault tolerance.

In the case of fault avoidance, no safe state is defined because the failure must not occur at all. Even in the case of failure forecasting, no safe state is defined because the fault is controlled before the critical failure occurs. Finally, in case of fault tolerance, the fault is tolerated during emergency operation until a safe state is reached. Fault tolerance measures leading to fail-active (i.e. fail-operational or fail-degraded) behaviour by implementing redundancy are used as an example to demonstrate the SaRA requirements in practice. The need to define the SaRA requirement for a system with fail-operational behaviour in case of a fault is explained in Figure 6, which shows the safety-relevant time intervals associated with emergency operation.

Figure 6 shows an example of a strategy where in case of a fault, a safety mechanism is implemented (e.g. by switching to a backup channel) and then an emergency operation with a limited duration, the so-called Emergency Operation Tolerance Time Interval (EOTTI), is used to meet the desired safety goal (SG). System functionality is maintained, and vehicle operation is not restricted. Therefore, upon detection of a fault, a transition to the emergency mode, which is an operational mode to ensure safety after the response to the fault, occurs until a safe system state is reached. Thus, by means of this emergency operation with a limited duration of EOTTI, the required safety is ensured. EOTTI corresponds to Time to repair in emergency mode. This is a safety-critical system because the emergency operation is used, even if for a limited time.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

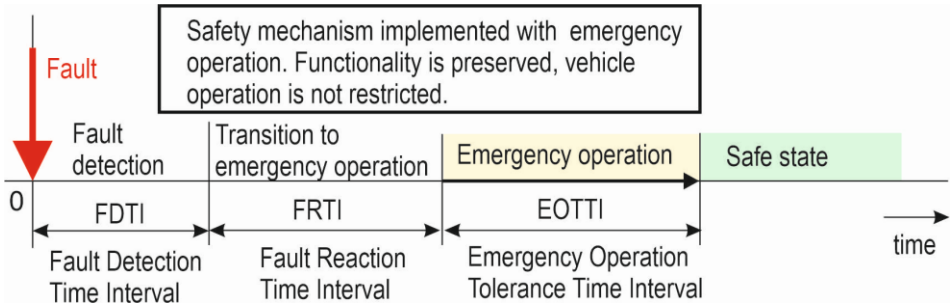

Figure 6 Safety-relevant time intervals for fail-operational systems with emergency operation [VC.4]

The SaRA requirement for the system according to Figure 6 needs to be specified. In this case, SaRA include: (1) a system availability requirement to ensure that the automotive PMHF (Probabilistic HW Failure Rate per Hour) [NS.27], which is the average probability of a hazardous failure over the lifetime of the item, corresponding to the Automotive Safety Integrity Level (ASIL) for a given SG, is met, and (2) an EOTTI requirement to be derived based on a reliability calculation for the ultimate safety layer. To meet the SaRA requirement for GNSS-based positioning, we need to know the probability of providing GNSS integrity without interruption, i.e. GNSS continuity (reliability).

6.7 Significance of GNSS continuity and reliability in multimodal transport

This section recapitulates the significance, need and utilization of service continuity for GNSS-based positioning in different transport sectors using the findings described in Deliverable D2.4 of the VICE4RAIL project, in section 6 of [VC.4]. It is the comparative analysis approach used in multimodal transport that has enabled the conclusions presented. Meeting aviation GNSS continuity requirements significantly determines the cost of the global GNSS infrastructure because it is based on redundancy. It is therefore reasonable to assume that the attribute of continuity may also be important for vehicle localization in other areas of land transport, including rail, although its significance has often been overlooked. The following chapters first provide an overview of recent research activities focused on the importance and use of GNSS continuity in transportation. And then it deals with the relationship and meaning of continuity with respect to the main sectors of multimodal transport (air, sea, rail and road).

6.7.1 Overview of research in the field of GNSS continuity within VICE4RAIL

Research activities focused on the use of GNSS continuity are described in Deliverable D2.4 of VICE4RAIL, section 6 of [VC.4].

The introduction in section 6.1 first mentions the concept of Required Navigation Performance (RNP), which was initiated by the International Civil Aviation Organization (ICAO) and includes the following 4 main attributes of GNSS: accuracy, integrity, continuity and availability. The origin of the GNSS continuity requirement for the aeronautical SoL service derived using the aviation Target Level of Safety (TLS) is explained in section 6.2. It is shown that the GNSS CAT I continuity attribute (C=1 - $8x10^{-6}$/ 15 s) can also be expressed in terms of reliability. The problem, however, is that the continuity of GNSS in terms of reliability is too small – MTBF of only about 520 hours. An overview of continuity requirements for GNSS in land transport follows in section 6.3. This includes the specification of GNSS continuity requirements for maritime transport, railway requirements for ERTMS reliability and finally a view on GNSS continuity for automated driving systems (ADS) of cars.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

For example, the MTBF requirement for GNSS-based train positioning for ERTMS is about $5x10^5$ hours. In section 6.4, an analysis of the reliability of GNSS positioning is performed, which focuses on improving reliability using redundant architectures. For this purpose, a 1oo2 architecture and Markov modelling are used. Based on the reliability calculation using 1oo2 architectures, it was found that using high-quality diagnostics and redundancy, positioning reliability with an MTTF of approximately $5x10^5$ h can be achieved, which is required in the case of ERTMS.

6.7.2 Discussion on GNSS continuity in multimodal transport in terms of reliability and safety

Aviation: continuity vs. reliability

In aviation, GNSS continuity is used as one of the two main safety attributes of GNSS, just along with GNSS integrity, which is derived from the acceptable aviation risk and the associated Target Level of Safety (TLS) (see [OD.5], [OD.6]). As mentioned above, GNSS continuity of SoL service is defined in terms of the probability with which GNSS accuracy and integrity is provided without unplanned interruption for the (short) duration of a critical operation phase. Thus, at first sight, continuity corresponds to short-term reliability. The question then arises as to why not use the term short-term reliability instead of continuity in aviation. Naturally, in the field of GNSS for aviation, the term reliability is also used - although reliability is not used to define a GNSS SoL service. The explanation could be as follows.

Reliability generally expresses the probability of success of a service or system function over a given time interval. In other words, it can be paraphrased as 'the probability of non-failure in a given period' (see [OD.7]). This means that reliability is associated with failure/fault - whether due to HW or/and SW. However, loss / interruption of GNSS SoL service provision or function with integrity can occur even in the absence of a fault. This is associated with the presence of GNSS integrity monitor. The integrity monitor can raise a true-alert or a false-alert (and thus the GNSS service/function interruption) even in the case of fault-free conditions.

Reliability is often measured in practice for repairable systems by Mean Time Between Failures (MTBF) or failure rate. Loss of GNSS continuity is measured by the loss of service/function over a given time interval in both the faulty and the non-faulty cases. Aviation continuity is an operational safety requirement. Continuity *explicitly defines* the critical time interval for which the service/function is to be correctly performed without interruption. In contrast, reliability need not be *explicitly defined* by a critical time interval – even though the definition of reliability includes a time interval. Often, only the MTBF is sufficient as a reliability requirement.

Continuity of GNSS depends on the reliability (MTBF) of system components - e.g. MTBF of GNSS reference receivers, GNSS satellites, CPUs, telecommunications, etc. (Figure 7). Therefore, the term GNSS continuity for aeronautical applications seems to be more appropriate than the term reliability.

Maritime

In the maritime sector, where safety-critical systems are used, as in aviation, the term reliability was first used as one of the main attributes of GNSS quality of service - see IMO Resolution A.860(20) adopted on 27 Nov 1997 (see [OD.8]). Here, reliability of GNSS service is defined as a probability of success of 99.97% over a period of 1 year. Thus, initially the term GNSS continuity was not used in the maritime sector, although the notion of continuity was already defined in [OD.8]. The term GNSS continuity started to be used in the maritime context in IMO Resolution A.915(22) adopted on 29 Nov 2001 (see [OD.9]).

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Railway

The railway safety and dependability concept based on the standard EN 50126 (1-2) (RAMS) [NS.12], [NS.13] does not directly specify continuity requirements for GNSS, but there are very demanding requirements for system reliability, e.g. for ERTMS, due to operational reasons. European railways aim to use the GNSS SoL service, in particular EGNOS, which was originally developed for aviation, and to benefit as much as possible from its high quality in the sense of a railway RAMS. An overview of railway requirements for the reliability of GNSS-based positioning for ERTMS is given in D2.4 of VICE4RAIL [VC.4], section 6.3.2. It is assumed that the MTBF of GNSS positioning should be about $5x10^5$ hours.

In general, a failure at the system level is caused by an error in the system. And the error in the system is due to a system fault (state). The fact that loss of GNSS service continuity can occur in the absence of a fault needs to be kept in mind when using the MTBF metric - because the MTBF is associated with the presence of a failure and fault as outlined above. However, it would be unpractical to think about using other measures for reliability in the sense of continuity in land transport that would be suitable for the fault-free case. One could mention, for example, the term MTBO (Mean Time Between Outages), which is also used in GNSS for aviation. But it would be useless as MTBO is not used within railway RAMS.

In railway or automotive transport, reliability is usually measured by MTBF, so we have to use MTBF also in the context of continuity. On the basis of the facts described above, it can be concluded that GNSS continuity designed for aviation can be utilised in the sense of GNSS reliability on railways and in road transport.

As shown in D2.4 of VICE4RAIL [VC.4], section 6.7, Signal-In-Space (SIS) reliability depends significantly on the MTBF of the satellite and the number of critical satellites in the position solution. If the most 4 critical satellites are considered (instead of 10 critical satellites – see Figure 7), than the total GBAS service continuity risk is 5.2x10-6/ 15 s and the corresponding MTBF is 801.3 h (instead of 520.8 h for 10 critical satellites). It's not that much difference between these (relatively small) MTBF values. We must not also forget that the real performance of the current EGNOS in terms of CR is 1e-4/ 15 s and the corresponding MTBF is only 41.66 h.

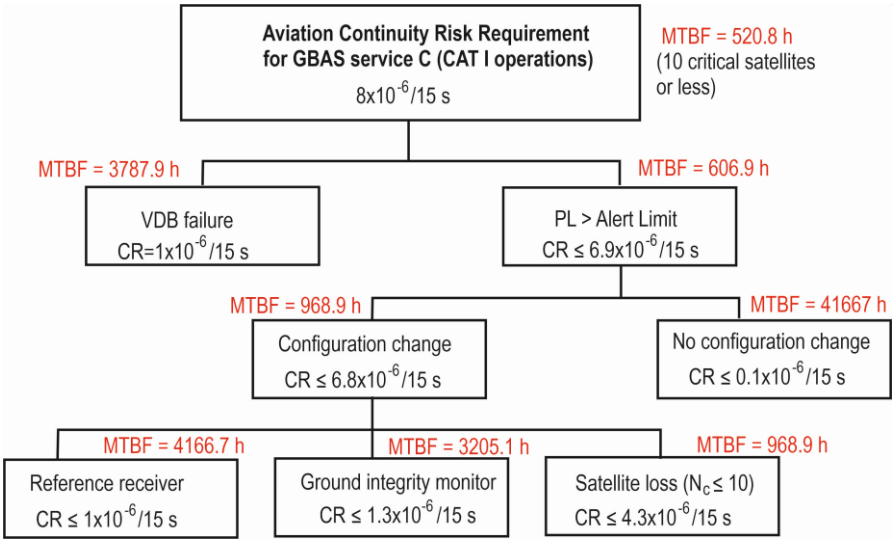

Figure 7 Example of continuity risk allocation for GBAS service C (CAT I operation) [OD.10]

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Automotive

It appears that there is no consensus in the automotive industry on the use of GNSS continuity. This is evidenced by the current umbrella safety standard for the automotive industry, ISO/TR 4804 [NS.25], which does not consider GNSS continuity as one of the main attributes of GNSS quality. The standard states the following: *"Continuity metric is no longer the main parameter of GNSS-based positioning with integrity*" [NS.25]. This is a needlessly rejecting statement, especially when continuity expresses GNSS infrastructure quality based on redundancy, which costs a lot of money. This statement is based on a misunderstanding of the GNSS continuity concept. This is justified by the fact that GNSS based positioning cannot have high continuity due to environmental obstructions of GNSS Signal-In-Space, such as bridges or tunnels. However, this statement conflicts with the definition of continuity, which is measured by unscheduled positioning outages. Loss of GNSS Signal-In-Space due to obstructions around a railway line or road can be well predicted and is therefore not related to loss of continuity of service.

Completely different views on the need for GNSS continuity for safety-critical applications in the automotive and other transport sectors are given in the GNSS User Technology Report (see [OD.11]), where GNSS continuity is considered a high priority requirement. Reliability (continuity) is the basis for the availability determination. GNSS continuity is therefore beneficial for meeting the Safety-Related Availability (SaRA) requirement [NS.27], which is needed where fail-operational system behaviour is required - e.g. for ADS when overtaking cars.

The above-mentioned views on the use of GNSS continuity in automotive transport are contradictory and therefore need to be monitored further.

Conclusions

GNSS continuity is a common element identified and analysed using synergies for vehicle positioning in multimodal transport. A consensus on the proper use of GNSS service continuity can significantly simplify the certification of vehicle positioning.

From the perspective of using GNSS continuity for safe vehicle positioning in multimodal transport, it follows that the requirements for continuity of GNSS SoL service are explicitly defined only in aviation and maritime standards and regulations.

In the field of railway safety-relevant systems, the attribute continuity is not used, as it is not included among the main RAMS attributes. However, in railways, the attribute continuity can be replaced by reliability in terms of MTBF. It is not enough for GNSS-based train positioning systems for ERTMS purposes to meet demanding safety integrity requirements (SIL 4). They are also required to meet high reliability requirements for localization, i.e. an MTBF of $5x10^5$ h, while the MTBF of the GNSS service derived from aviation requirements is only 520 h. It has been shown by means of reliability analysis in D2.4 of VICE4RAIL [VC.4] that the required reliability for train positioning for ERTMS can be achieved by means of redundant architectures with IMUs.

As far as automotive transport is concerned, the use of GNSS continuity as one of the main ICAO RNP attributes is not considered. The automotive standard ISO/TR 4804 on ADS dependability states that GNSS continuity is not required as a main parameter for positioning with integrity, although continuity significantly determines the cost of GNSS infrastructure. However, there are also conflicting/ opposite opinions in the professional literature on the need to use GNSS continuity for ADS purposes. Further attention needs to be paid to developments in this area.

The above facts must be taken into account when designing, assessing the safety and certifying a GNSS-based positioning system in multimodal transport. Certification is then carried out according to the relevant regulations and standards for the given transport sector.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

7 General overview of the Certification Process

The attempt of laying down the basis for a validation process of the HyVICE platform and future certification process for GNSS-based train positioning solutions will be based on the well-established Assessment and Certification process on European Railways, as defined in European Directives and Regulations (see § 2.1 of this document); the Assessment and Certification process ensures that all essential ERTMS requirements for Safety and Interoperability, as specified in TSI CCS, are met.

Actually, as any other safety-related railway system, before entering service, any future solution of GNSS-based ERTMS/ETCS application must be certified, by performing the planned process, by applying the applicable standards and by modifying or implementing what is necessary to consider due to the introduction of GNSS for train localization.

Basic steps to be carried out in accordance to what stated above are:

a) to identify any 'new' requirements for Certification Process that arise from the introduction of the GNSS-based positioning solutions in ETCS in place of physical balises

b) to identify any 'new' elements of documental evidence that NoBo and AsBo need for Interoperability Certification and Safety Assessment.

c) to apply the above-mentioned activities to a 'real case' in order to demonstrate the applicability of the 'new' Certification Process and to achieve a 'template' of CE Certificate

d) to submit the output/findings of the 'new' Certification Process to the Safety Agency for any comments/feedback.

7.1 Actors and roles

Refer to chapter 2.1 of [VC.2].

7.2 Railway Regulations and Standards

Refer to chapter 2.2 of [VC.2].

7.3 Certification Process overview

The VICE4RAIL project aims to contribute to establish a standard industry-accepted certification procedure, complying with CENELEC and ERTMS standards, covering the integration of GNSS-based train localization solutions in ERTMS-ETCS applications.

The certification procedure verifies that railway subsystems and components meet the essential requirements as defined by European Directives [NS.2], [NS.7] and TSIs [NS.11]. The process involves the 'Conformity Assessment Bodies' (NoBo, AsBo/ISA), which evaluate the design, production, and performance of subsystems against relevant harmonised standards.

A key element of Certification process is the 'EC Verification', a structured process that assesses technical documentation, production methods, and operational tests. NoBo/AsBo are authorized to inspect and validate that the subsystem's performance aligns with the applicable TSIs and European standards. Upon successful completion, an 'EC Declaration of Conformity' or 'EC Declaration of Verification' is issued, demonstrating the readiness of the subsystem for integration into the railway system.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

The process of **Interoperability Conformity Certification** is generally based on the 'Commission Decision 2010/713/EU' [NS.3], related to "Unit Verification" (Module SG) / "Type examination" + "EC verification based on quality management system of the production process" (Module SB + Module SD) to ensure that the subsystem satisfies the requirements of the applicable TSI(s) [NS.11], including the European mandatory standards for the following stages (as defined in the module).

In particular, the NoBo will assess the technical documentation and the 'requirements matrix' provided by the Applicant against the 'essential requirements' as defined in the applicable TSIs [NS.11]: Safety, Reliability and Availability, Health, Environmental Protection, Technical Compatibility and Accessibility.

If non-conformities are found, the NoBo will issue a detailed list of technical notes; when all non-conformities and technical notes are closed, and after a final and overall revision of the documentation of the Applicant, the NoBo will finalise the 'Technical NoBo File', in accordance with Directive (EU) 57-2008 [NS.2].

The Certification procedure includes appropriate examinations and tests, as set out in the relevant TSI(s), harmonised standards and/or technical specifications, to check the conformity of the subsystem with the requirements of the relevant TSI(s); the NoBo shall agree with the Applicant which tests and where the tests will be carried out and whether tests must be carried out and witnessed by NoBo. Where the subsystem meets the requirements of the TSI, the NoBo shall proceed to generate the 'Certificate of Conformity' to be submitted by the Applicant to the Supervisory Authority in the Member State.

In particular, within the process of Certification of Interoperability, for covering the essential requirement of 'Safety' it is necessary to activate, under the responsibility of the AsBo/IS, the **Safety Assessment** process, that will be carried out in accordance with CENELEC standards [NS.12], [NS.13], [NS.14], [NS.16].

For VICE4RAIL project, the Safety Assessment process includes DUT tests and validation by means of HyVICE platform; testing campaign will be carried out by taking into account several possibilities, such as:

- 'Black box' testing (functional testing): technique that ignores the internal mechanisms of the DUT and focuses only on the outputs generated in response to selected inputs and execution conditions. Actually, this approach is supposed to ensure that the functionality specified in the requirements works properly.
- 'White box' testing (structural testing): technique that considers the internal mechanisms of the DUT. 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 it is normally used for testing the SW or HW modules.

Both approaches complement each other and that will allow the observation of the system feedback to actions from the point of view of the user and looking into the system. Black box approach is more likely to detect conditions of failure as perceived by the user. 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.

Evaluation of the **Risk Management** process, in alignment with Reg. 402/2013/EU [NS.4] relating the changing on 'Common Safety Methods' (CSM), will be carried out by the AsBo in case of a changes in the railway system; the discriminating factor on assessment activities is based on considering the impact of change: Relevant or Not Relevant. The AsBo review will include: documentation of the Proponent's Risk Analysis, developed in accordance with the CSM Regulation, for the use of the subsystem in the railway system, analysis of the Risk Assessment document, a joint meeting on the Risk Analysis Assessment and preparation of Assessment Reports (see chapter 8.1 of this document for further details).

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

8 Certification Plan for VICE4RAIL project

Any new solution proposed for ERTMS/ETCS before entering into service must be validated, assessed and certified based on the applicable European Regulatory framework; the assessment/certification process can be considered as the integration of the following sub-processes, to be applied to the future candidate solution for GNSS-based train localization, when verified, tested and validated by the HyVICE platform:

- 'Risk Management', in accordance with Regulation 402/2013/EU [NS.4]
- 'Safety Assessment', in accordance with CENELEC EN5012x standards (from [NS.12] to [NS.16])
- 'Interoperability Certification', in accordance with Decision 2010/713/EU [NS.3] and TSI CCS [NS.11]

In the following chapters the above sub-processes will be addressed and analysed (see also contribution from: 'D2.1 Rail User & System Requirements' [VC.2] and 'D2.2 Risk Analysis Evaluation Report' [VC.3]).

8.1 Risk Management process

Whenever changes (i.e. the adoption of a new solution for a GNSS-based train positioning system e.g. ASTP) are made, the Regulation (EU) 402/2013 [NS.4] (including its amendments) shall be applied; this Regulation describes Common Safety Method for Risk Evaluation and Assessment (CSM-RA) and provides a structured process to evaluate the significance of these changes, identify associated risks, and develop mitigation strategies (e.g. operational procedures and rules to apply with the aim to avoid hazards or, at least, reduce the risk). Prior to the Safety acceptance of the change, fulfilment of the safety requirements resulting from the risk assessment procedure shall be demonstrated.

In principle, each change in railway signalling represents a risk, which could endanger safety; in order to manage risks at an acceptable level, methods as Common Safety Targets (CSTs) and Common Safety Methods (CSMs) have been introduced in the Railway Safety Directive (EU) 2004/49/EC [NS.1] and also in the revised Directive 2016/798 [NS.8]. Since the introduction of GNSS-based train localization functionality into ERTMS/ETCS represents a significant change within the European railway network, then CSM-RA process, according EU legislation, must be applied.

The CSM-RA (Regulation (EU) 402/2013) [NS.4] sets out a harmonised framework to be applied by the proposer when making any change, significant or not significant, to the railway system in a Member state. Depending on the classification of the change the process could be justified with an adequate documentation for a not significant change up to a specific process in case of a significant change. The CSM-RA shall be applied by the 'Proposer' (RUs, IMs, entity in charge of maintenance, manufacturers, etc.) that proposes the change under assessment.

If the change in signalling system is significant, then the Proposer has to evaluate the associated risk according to the six criteria (as defined in the Regulation (EU) 402/2013 [NS.4]):

1) Failure consequence: credible worst-case scenario;
2) Novelty: innovative or new to organization;
3) Complexity: the complexity of the change;
4) Monitoring: the inability to monitor the implemented change throughout the system life cycle & intervene appropriately;
5) Reversibility: the inability to revert to the original system;

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

6) Additionality: assessment of the significance of the change taking into account all recent safety-related changes which were not judged to be significant.

When the change is evaluated as 'significant', an AsBo must be appointed by the Proposer.

CSM-RA covers the following activities (see also Figure 8, extracted from the document 'D2.1 Rail User & System Requirements' [VC.2], that is a simplification of the scheme illustrating CSM-RA in Appendix of Regulation (EU) 402/2013 [NS.4]):

1) Risk assessment process and demonstration of compliance with the Safety requirements,

2) Hazard Management (performed within Safety Management Systém in operations)

3) Independent Assessment by CSM Assessment Body (AsBo)

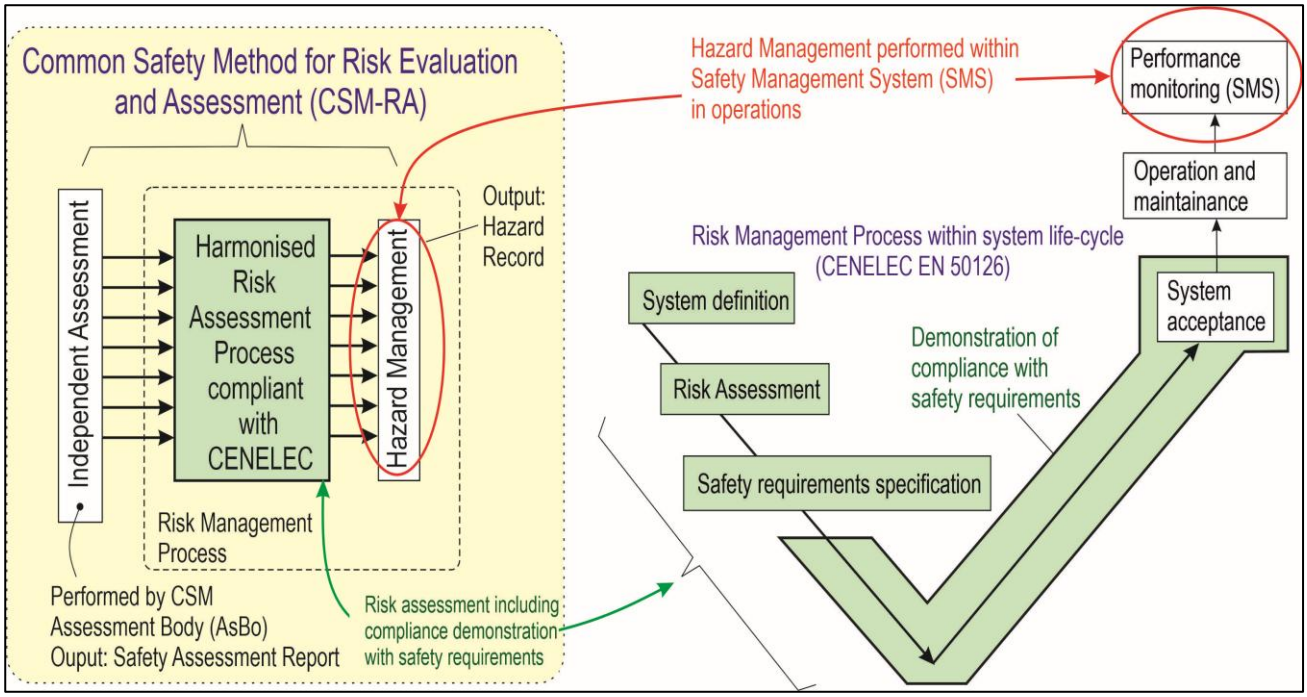

Figure 8 Compliance of CSM-RA with CENELEC safety life cycle [VC.2]

In the figure above, the compliance of CSM-RA with CENELEC EN50126 ([NS.12], [NS.13]) is outlined as well.

The safety monitoring during system operations is not covered by the harmonised Risk Assessment within CSM-RA. In order to be 'CSM-RA compliant' with the CENELEC life cycle, CSM-RA requires a separate Safety Management System (SMS) to be implemented and provided within activities of the Proposer of the significant change.

Figure 9 here below, extracted from the document 'D2.1 Rail User & System Requirements' [VC.2] (that is a simplification of the scheme illustrating CSM-RA in Appendix of Regulation (EU) 402/2013 [NS.4]), represents harmonization of risk acceptance and safety requirements using CSM-RA:

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

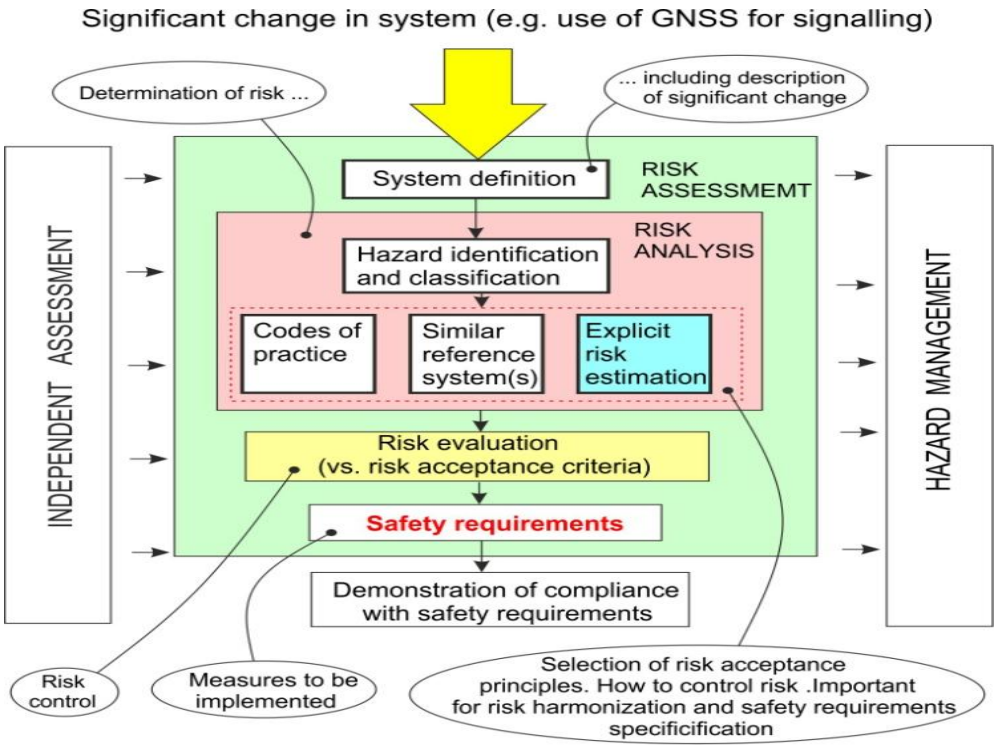

Figure 9 Harmonization of risk acceptance and safety requirements using CSM-RA [VC.2]

CSM-RA is an iterative process that is considered to be completed when it is demonstrated that all safety requirements are fulfilled, and no additional reasonably foreseeable hazards have to be considered. The Proposer shall systematically identify all reasonably foreseeable hazards for the whole system under assessment, its functions where appropriate and its interfaces. Widely acceptable Codes of Practice (e.g. CCS TSI, CENELEC standards, etc.) enable to harmonise risk and thus also safety requirements across Europe. Both Code of Practice and similar Reference Systems can be considered at the same time.

In case of GNSS application for railway signalling including ERTMS, Code of Practice (i.e. ERTMS TSI) have been utilized for derivation of safety requirements for Virtual Balise Detection (see as reference 'Project H2020 ERSAT GGC - ERTMS on Satellite Galileo Game Changer. Deliverable 3.2: GNSS Quantitative Study for ERSAT GGC Project, rev. 03, 22/11/2019').

RUs and IMs shall establish a Safety Management System (SMS) in accordance with Directives 2004/49/EC [NS.1] and 2016/798 [NS.8] in order to ensure the control of all risks associated with activities of IM and RU, including Maintenance. The Risk Management process can be represented within the EN50126-1 [NS.12] V-Cycle (life cycle) that starts with the preliminary system definition and finishes with the System Acceptance.

However CSM doesn't cover Performance Monitoring, and Operation and Maintenance and these two phases shall be covered by the RUs and IMs Safety Management System (SMS) (see Figure 8 above).

'Risk Assessment' means the overall process comprising a Risk Analysis and a Risk Evaluation; the CENELEC Risk Assessment process is compliant with the Risk Assessment employed within CSM-RA. For each identified hazard, it shall be decided if the related risk can be considered as "Broadly Acceptable" on the basis of the related consequences (e.g. no injury to human, no consequences on safety but only on availability, etc.). In these cases, requirements for RAM can still apply.

If the Risk Analysis identified cases with risk "Broadly Acceptable" there is no need to specify Safety Requirements for those cases; if the Risk Analysis identified that the risk is not "Broadly Acceptable", a Risk Evaluation activity shall be continued.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Risk Evaluation consists in comparing the determined risk against an associated RAC, including:

- use of Code of Practice (CoP);
- comparison with a similar system as a reference;
- explicit risk estimation (qualitative or quantitative).

Widely acceptable CoP such as CCS TSI, CENELEC standards, etc. have been elaborated on the basis of a long-term experience with designing of railway safety-related systems. Reference systems can be used in a very similar way as Codes of Practice because a reference system is a system that has been proven in practice to have an acceptable safety level. If a sufficient experience with the specific safety system design and assessment is missing, then explicit risk estimation must be applied.

Risk Assessment process is described in detail in EN 50126-1 [NS.12], EN 50126-2 [NS.13] and also in Regulation EU No. 402/2013 [NS.4] on CSM-RA. The expectation is that CSM-RA would be applied to assess changes introduced by GNSS-based localization solution in ERTMS.

For the VICE4RAIL project, the output of the Risk Management process will be addressed by the deliverable D2.2 'Risk Analysis Evaluation Report' [VC.3]; the objective of this deliverable is to fix the requirements in order to initially consolidate the certification process of the VICE4RAIL test platform for GNSS-based safe train positioning. To achieve the requirements fixation, the Common Safety Method for Risk evaluation (at system level) Assessment ("CSM-RA") according to the regulation (EU) 402/2013 [NS.4] will be applied; the requirement fixation will be the basis to demonstrate compliance and related certification of conformity, with detail to the new requirements defined in relation to the GNSS-based safe train positioning.

As considered in the deliverable D2.2 'Risk Analysis Evaluation Report' [VC.3], the Reg. EU 402/2023 [NS.4] can be seen as the backbone for the safety certification process for VICE4RAIL project, due to its ability to logically link the safety management project flow (CENELEC Standards), technical specifications (CCS, TSI and technical project requirements) and the demonstation of safety/functional conformity (i.e., engineering evidences of validation , testing activities both on-field and in laboratory).

Basically, Reg. EU 402/2013 [NS.4] (throughout its analysis process) covers all relevant aspects of the project and collects all expected goals, more specifically (see also Figure 10 as reference):

1. The analysis of relevance (article 4 of Reg. (EU) 402/2013 [NS.4]) and its evaluation provide the benefit of covering the project description. It defines the perimeter of interest and clarifies what is truly new in this innovative project, as well as its relationship with the operational context.
2. The risk analysis/risk management procedure and its evaluation: all relevant aspects contained in CENELEC Standards EN5012x (from [NS.12] to [NS.16]) are referenced to demostrate adequate coverage of ANNEX I of Reg. (EU) 402/2013 [NS.4] procedure (Chapters §2.1, §2.2), i.e quality aspects about organization, role independence, Hazard Log maintenance, and Safety Assurance in accordace with recognized norms at European level, including the Signalling TSI, application-conditions to be exported, environmental influences.
3. The Risk Acceptance, which is obtained (Chapters from §2.3 to §2.5 of Reg. EU 402/2013 [NS.4]) through adoption of good practice codes, CENELEC Standards and TSI, particularly thanks to the accurate risk estimation derived from quantifiable SIL4 requirements and technical specifications in signalling TSI.
4. The Demonstration of conformity to the Safety Requirements, identified and registered throughout the previous points (Chapters §3, §5 of Reg. EU 402/2013 [NS.4]). This demonstration has to be objective and well-documented, allowing for comprehensive evidence of V&V activities conducted both
    a. indoors (using Cedex HyVICE simulation platform)
    b. on-site (using RFI San-Donato test circuit)

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

These activities should directly link to the detailed test documentation, which can be produced according to

1. CENELEC guidelines, keeping in mind the test-plan, procedures and report models;
2. TSI guidelines, leveraging example provided by “reference test facilities” technical documents.

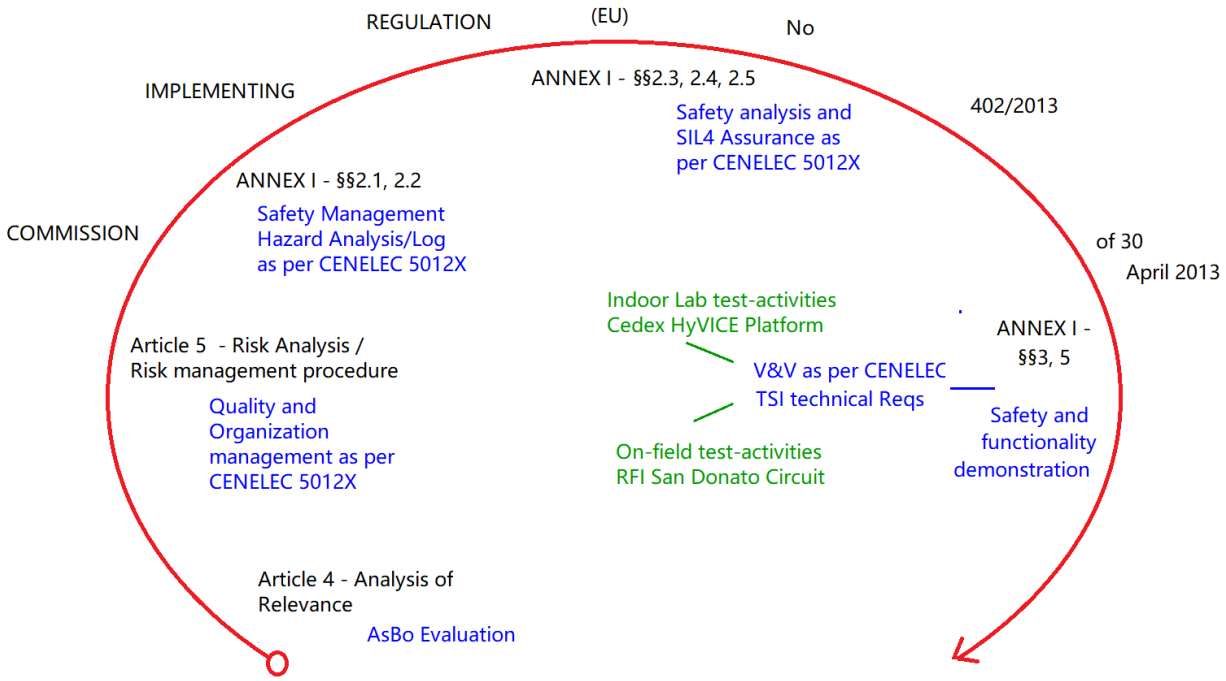

Figure 10 schematic representation of the CSM-RA process flowchart [VC.3]

8.2 Safety Assessment process

The basic framework for ensuring safety of railway systems is defined in CENELEC standard EN50126 ([NS.12], [NS.13]) on the specification and demonstration of RAMS. EN50126 considers the railway system in a given physical and operational environment, i.e., including human operators, as well as the factors that influence the railway RAMS - in particular the technical system and the operational and maintenance conditions. The standard specifies in detail the different phases of the system life cycle, i.e. including the role of the human factor in them and also prescribes methods for managing the RAMS within the system life cycle. Safety shall be demonstrated by means of ‘Safety Case’ and independent third-party assessment (ISA Assessment). The basic framework defined through RAMS can be imagined as an umbrella (Figure 11) under which a Safety-related system is subsequently developed and implemented according to the downstream standards EN50129 [NS.16] (safety-related system), EN50128 [NS.14] / EN 50716 [NS.15] (software for safety-related system), and others. (Note: EN 50716 replaces EN 50128 from 30/10/2026).

This project is funded by European Union’s Horizon Europe programme under grant agreement No 101180124

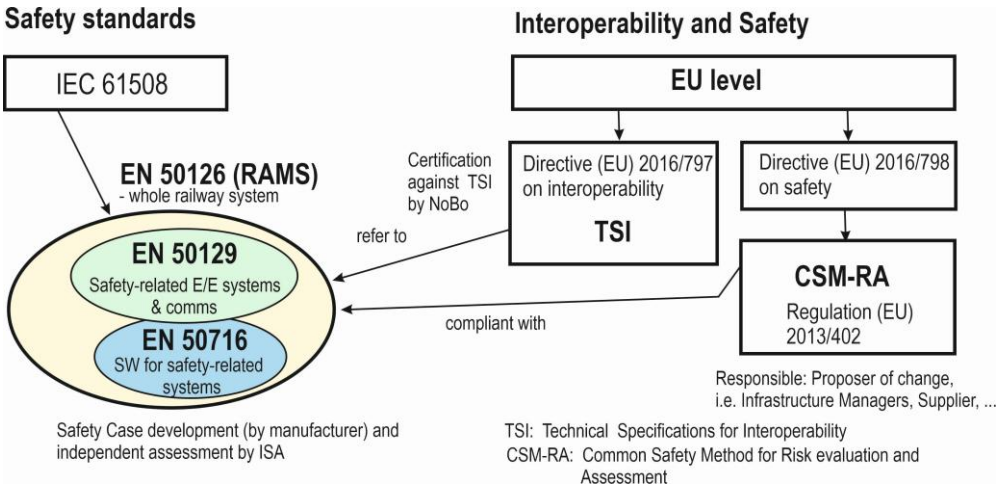

Figure 11 Railway safety standards, interoperability and common safety method [VC.2]

The EN50129 [NS.16] defines the conditions that shall be satisfied in order that a safety-related electronic railway system/sub-system/equipment can be accepted as adequately safe for its intended application. All of these conditions shall be satisfied, at equipment, sub-system and system levels, before the safety-related system can be accepted as adequately safe.

The documentary evidence that these conditions have been satisfied shall be included in a 'Safety Case' that forms part of the overall documentary evidence to be submitted to the relevant Safety Authority in order to obtain Safety Approval for a Generic Product, a Generic Application or a Specific Application.

The safety management process shall consist of a number of phases and activities, which are linked to form the safety life cycle; this should be consistent with the system life cycle defined in EN 50126-1 [NS.12] and in EN50129 [NS.16]. Before an application for Safety approval according to EN 50129 [NS.16] can be considered, an Independent Safety Assessment of the system/sub-system/equipment and its Safety Case shall be carried out under the responsibility of an Independent Safety Assessor (ISA), to provide additional assurance that the necessary level of safety has been achieved.

Its results should be presented in an Independent Safety Assessment Report (see Figure 12 here below); the Report should describe the activities carried out by the ISA to determine how the system / sub-system / equipment (hardware and software) have been designed to meet its specified requirements and, possibly, specify some additional conditions for the operation of the system/sub-system/equipment (namely, Safety-related Application Conditions).

The overall documentary evidence according to EN50129 [NS.16] shall consist of:

- the System (or sub-system/equipment) Requirements Specification,
- the Safety Requirements Specification,
- the Safety Case
- the Safety Assessment Report.

Provided all the conditions for Safety Acceptance have been satisfied, as demonstrated by the 'Safety Case', and subject to the results of the Independent Safety Assessment, the system/ sub-system/equipment may be granted Safety Approval by the relevant Safety Authority.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

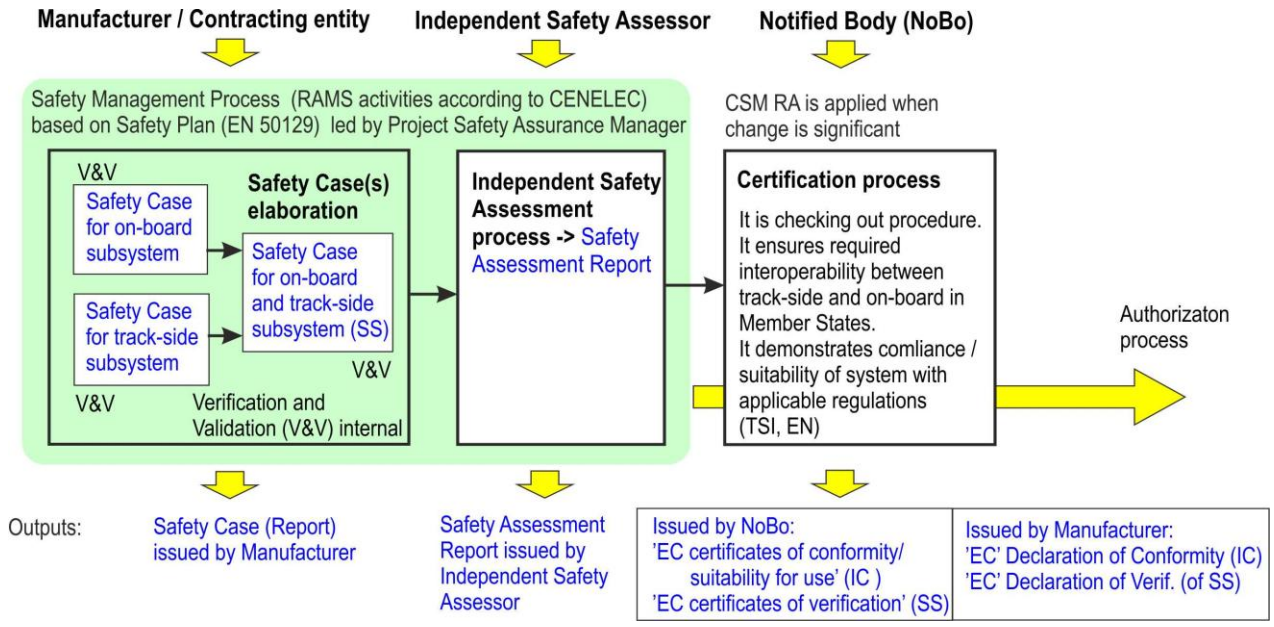

Figure 12 Activities within Safety Assessment / Approval process [VC.2]

Here below is the decomposition of the box indicated as 'Safety Management Process' in the figure above.

Verification and Validation

Verification is the process of evaluating system during development phase and saying whether it meets the specified requirements for that phase; in other words, if the element or system was built correctly in accordance with the applicable specification for that phase. Validation checks for errors in the specification and demonstrates that the system works as it required. Because requirements on safety, security and reliability in railway signalling can be complex, and because they use many concepts from multiple domains, in order to ensure that such requirements are satisfied, Formal/Semi-Formal Methods can be used in verification and validation phase. Those methods provide techniques and tools to define and precisely analyse such concepts and relationships, and to verify requirements exhaustively. Formal methods can also improve requirement quality and reliability. The V&V activities are to be carried out by Verifiers and Validators in accordance with the recommendations given by CENELEC EN50128 [NS.14] / EN 50716 [NS.15] and EN50129 [NS.16] to guarantee the required independence.

Safety Case

The application of V&V process, as alone, does not still provide sufficient evidence that the Safety requirements for the system have been met. Actually, CENELEC EN50129 [NS.16] and EN50126 [NS.12], [NS.13] require that this evidence is described in documents named Safety Case (for the Generic Product, for the Generic Application and for the Specific Application); moreover, when the integration of subsystems is required, the Safety Case of the Integration of subsystems is also required.

The Safety Case shall include a structured argument, supported by analytical and experimental evidence including simulations, that provides a comprehensive and valid case that a Generic Product / system is safe for the intended application in the given operational environment; its content are specified in details in EN50126-1 [NS.12] and in the EN50129 [NS.16].

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Independent Safety Assessment (ISA) Report

The Safety Case, as elaborated by the Manufacturer, shall be assessed by the ISA or AsBo.

In the Safety Case, the Independent Safety Assessor verifies that safety requirements have been met, all potential safety hazards have been identified, risks associated with them have been carefully evaluated that appropriate safety mitigations have been designed as protection against the hazards. In addition, the Safety Case must also demonstrate that the quality and safety management controls adopted within the life cycle are suitable for the required SIL, and appropriate development techniques have been adopted and that they have been implemented correctly. The ISA elaborates the 'Independent Safety Assessment Report'.

8.3 Interoperability Certification process

In order to apply the GNSS-based solution for safe train positioning as integrated in the ERTMS-ETCS system, it is necessary to certify the new solution according to the relevant European standards and regulations. It means that it is possible that a new subsystem has to be integrated into the Interoperability Constituent (IC) within ERTMS/ETCS environment and has also to be incorporated into the ERTMS TSI CCS [NS.11]; if this is the case, the new IC should pass through all the expected phases of the safety and conformity assessment processes according to the applicable European norms and standards.

The interoperability certification process covers all the conformity assessment activities based on the requirements set out in applicable TSI (e.g the TSI CCS [NS.11]) which defines the technical and operational standards which must be met by each subsystem (or part of it) in order to meet the essential requirements and ensure the interoperability of the railway system of the EU. Moreover, in case of change in the railway system from a Safety point of view, the so-called Common Safety Method for Risk Evaluation and Assessment (CSM-RA) according to the Regulation (EU) 402/2013 [NS.4], which harmonises the risk assessment process and safety requirements, must be applied (see chapter 8.1 of this document for further details).

The basic framework applicable for the safety/risk assessment and interoperability certification of the ERTMS based on GNSS is illustrated in the picture here below:

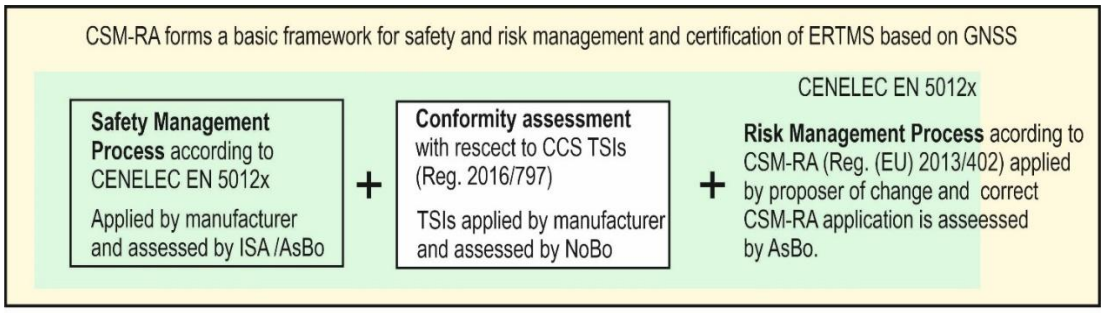

Figure 13 Basic framework for safety assessment and certification of ERTMS based on GNSS [VC.2]

The Risk Management process follows the Safety Management process according to CSM-RA as for Reg. 402/2013/EU [NS.4] (as amended by 1136/2015/EU [NS.6]) and to CENELEC standards ([NS.12] - [NS.16]); in turn, the Safety Management process is linked to the Interoperability Certification process according to the TSI CCS [NS.11], in the sense of Reg. (EU) 2016/797 [NS.7], because list of mandatory standards EN 5012x are referred in the TSI CCS [NS.11]. The Interoperability Certification process ensures that the required interoperability among on-board and track-side ERTMS-ETCS subsystems, while meeting the requirements of the CENELEC standards (from [NS.12] to [NS.16]), is shared among many independent actors, mainly IMs and RUs; the corresponding Interoperability Certificate comprises the assessment of the conformity of an IC (Interoperability Constituent), considered in isolation, to the technical specifications to be met.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

The relation between the Interoperability Certification process and the Safety Management process according to CENELEC standards is illustrated in Figure 11 and Figure 12 of this document; the safety management according to CENELEC will ensure the required safety and reliability/availability of the safety-relevant system, while the Interoperability Certification process will verify the fulfilment of the ERTMS requirements according to the TSI CCS [NS.11].

The Interoperability Certification process for Railway Safety-related systems includes 3 steps:

- Review reports on all evidence elaborated by system Manufacturer;
- Issue/review Technical Report detailing requirements to be met by the system and how they are fulfilled;
- Issue of the Interoperability Certificate as top level summary.

For ERTMS applications based on the GNSS positioning both Safety Authorization (IM) and Vehicle Authorization (RU) must be obtained; therefore, the Certification and Authorisation for placing in service new IC, e.g. GNSS-based train positioning system, is expected to include three main activities (see Figure 12):

- EC declaration of Conformity issued by Applicant/Manufacturer with respect to specifications (e.g. new interoperable specification that will also include such a new technology) - i.e. certification of IC's conformity assessed by NoBo;
- EC declaration of verification of a subsystem (SS) issued by Applicant/ Manufacturer – i.e. certification of verification assessed by NoBo;
- Authorisation for the placing in a service of a new system/subsystem by Member State.

In particular, for the process of Certification of Conformity for Interoperability, the activities that will be carried out in the process for each project phase are as follows:

Design Assessment:

- Checking of completeness and compliance to applicable legislation (TSI, European Harmonized standard, additional requirements, etc.) to verify the list of specifications and technical standards that the Applicant intends to use for demonstrating the compliance of the subsystem with the relevant TSI CCS [NS.11].
- Examination of design methods, tools, and design results to assess compliance with the TSI CCS [NS.11].
- Checking of the correctness of values/parameters against applicable TSI CCS [NS.11] requirements related to the final design.
- Checking if the ICs used are appropriate to the railway system and application.
- Issuance of Conformity Report for design stage.

Assembled, before putting into service:

- Checking that subsystems comply with the relevant design parameters set out in the TSI CCS [NS.11].
- Examination of construction methods, review test documentation and perform site inspection to assess compliance with the requirements of the TSI CCS [NS.11] based on the verification modules selected.
- If necessary, request appropriate examinations and tests, which haven't been carried out by Client, to ensure that the relevant harmonized standards and/or TSI CCS [NS.11] have been applied correctly.
- If necessary, Assess the test reports to verify that checks and tests have been performed according to the relevant TSI CCS [NS.11] procedures.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

8.4 HyVICE document delivery roadmap

Based on the contents of the 'Technical Proposal' [VC.1], and in accordance with the the V-model of the System life-cycle as for CENELEC EN50126-1 standards [NS.12] (see picture here below):

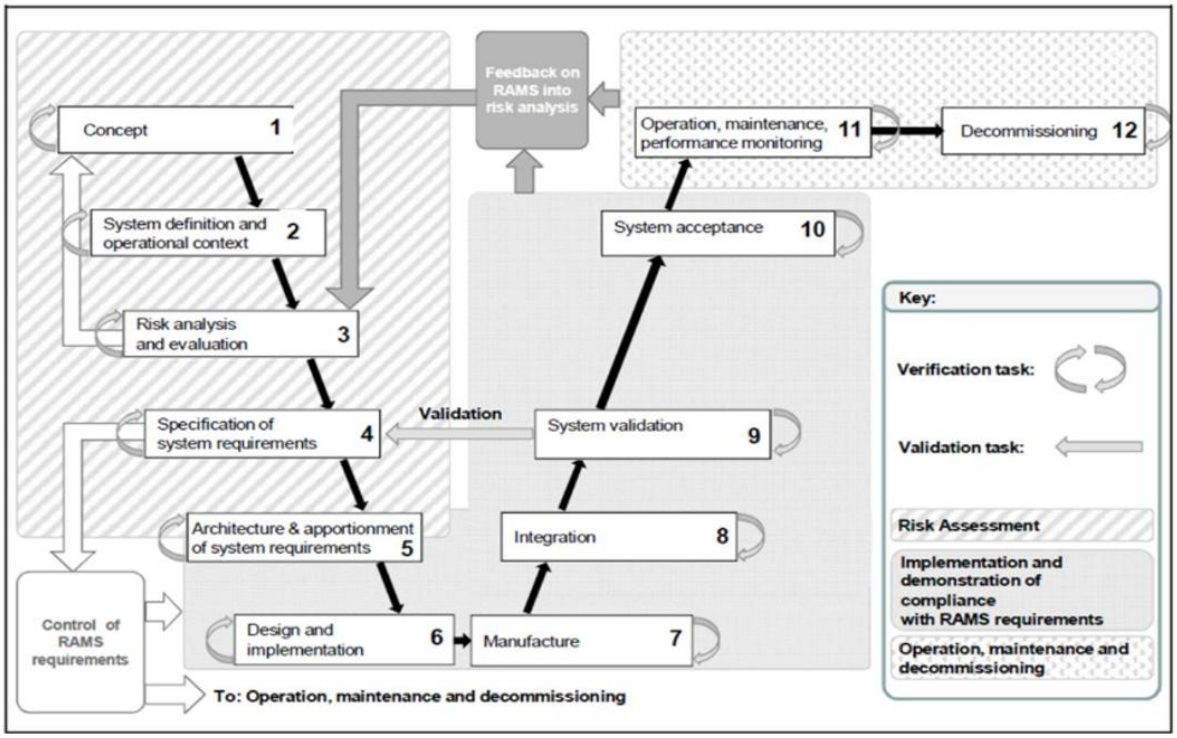

Figure 14 EN50126-1 V-model of the System life-cycle [NS.12]

the following documents will be delivered within the VICE4RAIL project; those documents are cross-referenced to the main phases/areas of concern of CENELEC EN50126-1 standards [NS.12], Regulation (EU) 402/2013 [NS.4] and TSI CCS [NS.11] as it is shown in the table here below:

VICE4RAIL deliverable	Reference to European regulatory framework
D2.1 'Rail User & System Requirements' [VC.2]. Its scope is to provide an overview of the user and system requirements (including user, functional, system safety and security requirements) supporting the development of a hybrid virtualized testing and certification framework (HyVICE) tailored specifically for GNSS-based railway solutions. Well-developed procedures have been used to derive harmonised requirements used on European railways to guarantee both interoperability and transport safety. Input for the derivation of the railway requirements were also the outputs of previous similar projects such as the ERSAT GGC, RHINOS, GATE4RAIL, HELMET, EUSPA UCP, ERJU R2DATO and ESA projects.	Phases '1. Concept' and '2. System Definition and Operational Context' of EN20126-1 [NS.12]
D2.4 'Synergies in the Certification Process for Use in Multi-modal Transport' [VC.4]. Its scope is to compare and assess certification procedures in rail, automotive and maritime sectors to identify common elements of the certification schemes to make the certification of multimodal transport solutions more efficient. For further details see also chapter § 6 of this document.	

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

VICE4RAIL deliverable	Reference to European regulatory framework
D2.2 'Risk Analysis Evaluation Report' [VC.3]. Its scope is to achieve fixation of the Requirements by applying the Common Safety Method for Risk evaluation (at system level) Assessment ("CSM-RA") according to the Regulation (EU) 402/2013 [NS.4] for harmonisation of risk assessment. The requirement fixation will be the basis to demonstrate compliance to the requirements defined in relation to the GNSS-based train localization approach. For further details see chapter § 8.1 of this document.	Phase '3. Risk Analysis and Evaluation' of EN20126-1 [NS.12] ANNEX I of Regulation (EU) 402/2013 [NS.4]: RISK MANAGEMENT PROCESS
D3.3 'System Requirement Document'. Its scope is (starting from the analysis of the deliverable **D2.1 'Rail User & System Requirements'** [VC.2]) to define the System Requirements Specification for the HyVICE platform; it contains the whole HyVICE System and Interface Requirements. A review of the state of the art of GNSS-based positioning solutions is carried out to identify the simulation platform blocks required and beside to be developed in the project for simulation. These blocks shall represent the context of use of the testing platform that will impact sensors, thus system behaviour: train trajectory, environments crossed and their effects on the embedded sensors, dynamic of the vehicle and information required by the ERTMS on-board. Special tasks will be devoted to local effects modelling: from state of the art of existing error models, complementary investigations will be carried out, investigating the use and opportunity to use 3D models and ray tracing as a complementary data-driven modelling solution. About RAMS requirements to be applied to the HyVICE platform, at the current stage of the VICE4RAIL project, being the architecture and the functionalities of both CEDEX laboratory and Bologna San Donato not finalized yet, and also considering the state-of-the-art of the regulatory framework where the VICE4RAIL project is moving, it can only be anticipated that whereas SIL/THR concepts appears not to be directly applicable to a Testing and validation platform such as HyVICE, some RAM requirements, such as Availability, Testability and Maintainability of the platform, more in qualitative that in quantitative sense, can be extracted from the prescriptions reported in the CENELEC EN50128 [NS.14] / EN 50716 [NS.15]. Further details about contents of D3.3 deliverable can be provided in the future up-dates of this document once the HW and SW features of the HyVICE platform architecture have been defined and agreed.	Phase '4. Specification of System Requirements' of EN20126-1 [NS.12]
D3.1 'Overall Architecture Design Document'. Its scope is (starting from the analysis of the deliverable **D2.1 'Rail User & System Requirements'** [VC.2]) to design the Overall Architecture for the HyVICE platform, based on Field Testing and Virtualised Simulation Platform. The functional decomposition of the overall system for the full chain is carried out and relevant interfaces identified. The following aspects will be integrated: • Integration of designed systems in ETCS and full chain testing modelling • Integration of existing functional ERTMS and PVT simulation tools • Interoperability with Odometry and the other Rail On-Board equipment • Local Effects modelling Main functional architectural blocks for the HyVICE platform are defined.	Phase '5. Architecture and apportionment of System Requirements' of EN20126-1 [NS.12]

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

VICE4RAIL deliverable	Reference to European regulatory framework
D3.2 'Detailed Design Document'. Its scope is (starting from the analysis of the deliverable **D3.1 'Overall Architecture Design Document'**) to design the detailed architecture for the HyVICE platform. It defines the interfaces of each HyVICE Architectural block and it includes the design of the HyVICE Communication System, of the Laboratory Testing Platform and of the Real Testing Platform. Further details about contents of D3.2 deliverable can be provided in the future up-dates of this document once the HW and SW features of the HyVICE platform architecture have been defined and agreed.	Phase '6. Design & Implementation' of EN20126-1 [NS.12]
D3.4 'Test Plan'. It defines the DUT Test Procedures for the Laboratory Test Platform and the On field/Mixed Reality Testing Platform. Relevant Interfaces between architectural components for GNSS+ERTMS implementation are designed (e.g. between the DUT and the GNSS Augmentation System). Based on the System Requirements (see **D3.3 'System Requirement Document'**) and Interface definition (see **D3.1 'Overall Architecture Design Document'** and **D3.2 'Detailed Design Document')**, the HyVICE platform, based on On-field measurements and the identified Simulation tools, is designed. The definition of a testing process shall consider aspects like: • definition of the test architecture (i.e. DUT and its interfaces) • definition of the test requirements (i.e. Test Specification, with description of each Test step and uniquely pass and fail criteria) • definition of the test implementation (i.e. Test Procedure) • definition the proper test results documentation (i.e. Test Report) Further details about contents of D3.4 deliverable can be provided in the future up-dates of this document once the HW and SW features of the HyVICE platform architecture have been defined and agreed.	
D4.1 'Procurement List Document'. Its scope is to activate the procurement of the full set of HW, SW and services needed for HyVICE implementation.	Phase '7. Manufacture' of EN20126-1 [NS.12]
D4.2 'Development Report'. Its scope is to report about the development of each HyVICE component and related testing interfaces and the final system integration for both Real and Laboratory testing platforms, including Unit testing, Interface testing, System Integration testing and integration of the DUT at CEDEX laboratory. Final system integration for both the Real and the Laboratory testing platforms includes: • Unit testing. Each developed module will be tested against the established requirements. The test results will be collected in a test report • Interface testing • System integration testing • The DUT (EVC including Train Positioning Module) to be integrated at CEDEX laboratory, according to the architecture shown in Figure 3.	Phase '8. Integration' of EN20126-1 [NS.12]

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

VICE4RAIL deliverable	Reference to European regulatory framework
Further details about contents of D4.2 deliverable can be provided in the future updates of this document once the HW and SW features of the HyVICE platform architecture have been defined and agreed.	
D4.3 'Test Report'. Its scope is to define test scenarios (GNSS Scenarios, ERTMS Scenarios, etc.) and to execute Tests on both the Real Testing Platform and the Laboratory Testing Platform; operational scenarios shall be defined to determine which operational limitations result, if any, for the ETCS application. Tests execution and recording will be carried out according to the prescriptions of deliverable **D3.4 'Test Plan'**. It also includes results of comparison and analysis between the On-field and lab test records. On-field tests execution is devoted to test execution on the Real Testing Platform. It includes the following activities: • On field tests execution according to the deliverable **D3.4 'Test Plan'**. • On field tests results will be collected in a 'Test Report' • After execution of each Test session, detection of eventual critical anomalies will be performed and HyVICE revised as necessary. Laboratory ERTMS tests execution is devoted to the test execution on the Laboratory Testing Platform. It includes the following activities: • Laboratory ERTMS tests execution according to the deliverable **D3.4 'Test Plan'**. Laboratory tests results will be collected in the 'Test Report' • Comparison and analysis between the On-field test and lab test. • Validation of the lab based on the comparison between on field and lab tests	Phase '9. System Validation' of EN20126-1 [NS.12] TSI CCS [NS.11] Table 6.1.1. 'Conformity assessment requirements of an interoperability constituent or a group of interoperability constituents' Table 6.2.1. 'Conformity assessment requirements for an On-board Subsystem or for groups of Parts'
D5.1 'Validation Strategies'. Its scope is to conduct the validation of the DUT + other track side/on board systems based on validation activities performed with support of the HyVICE platform, to evaluate the degree of compliance with requirements set in deliverables **D2.1 'Rail User & System Requirements'** [VC.2] and **D3.3 'System Requirement Document'**; additionally, to conduct the DUT - on board - trackside integration test and to issue a draft/template of main validation evidence.	
D5.2 'Certification On-Board Subsystem'. Its scope is to simulate a process where the conformity of the ERTMS DUT/On-Board Subsystem functionalities and performances is evaluated against the TSI CCS [NS.11] Essential Requirements, based on all the verification and validation activities performed in the previous tasks. The above activity could imply the following additional tasks: • 'example' of analysis of the requirement matrix for the TSI CCS [NS.11] • issuing of Technical Notes containing findings about deviations from standards • Test Witnessing on field into the circuit of Bologna San Donato • Issuing of a 'template' of No-Bo file/CE certificate based on the modules defined in the Decision 713/2010 EU [NS.3]	
D5.3 'Certification on Track Subsystem and related System Integration': to simulate a process where the conformity of the ERTMS Trackside Subsystem functionalities and performances is evaluated against the TSI CCS [NS.11] Essential Requirements, based on all the verification and validation activities performed in the previous tasks, including related system integration with DUT/On-Board Subsystem. Additional tasks that could be implied in the process are the same as for **D5.2 'Certification On-Board Subsystem'**.	

Figure 15 HyVICE document delivery roadmap

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

In order to adhere at the maximum extent to documental request from CENELEC EN50126-1 standards [NS.12] for SIL4 applications, the table reproduced in Annex A (chapter 11 of this document), as extracted from the document 'D2.1 Rail User & System Requirements' [VC.2], represents a high-level general guideline for all the technical documents/arguments (including VICE4RAIL contractual deliverables) to be considered within this project. The documental list of the table will be monitored all along the VICE4RAIL project and, if necessary, it will be reviewed/updated in the following updates of the D2.3 'Certification Plan'.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

9 Open points and investigation areas

Adopting GNSS-based railway solutions for train localization in ERTMS-ETCS applications represents a critical challenge that, as already confirmed from what reported in the previous chapters of this document, can imply some open points / investigation areas, at least in this initial stage of the VICE4RAIL project. In the chapters here below a preliminary list of open points / investigation areas is listed; this preliminary list will be constantly monitored all along the VICE4RAIL project until all open points have been addressed and, possibly, resolved or mitigated to an acceptable level/extent.

9.1 Missing references for GNSS-based train localization in European regulatory framework

Considering that the existing Railway Regulatory framework, centred on the current version of the TSI CCS [NS.11], was not originally designed to accommodate satellite-based positioning systems, the fact of introducing the GNSS into Railway operations requires a comprehensive revision of the current version of TSI CCS (and of all the Railway Technical Specification referenced therein, such as UNISIG subsets) to identify and review the main functional ERTMS requirements that are impacted by the introduction of GNSS position technology in order to include satellite-based technologies. This normative alignment must define clear, standardized requirements for accuracy, reliability, safety and interoperability, while also establishing robust validation methodologies for assessing GNSS performance under real-world railway conditions.

Changes to ERTMS specifications (e.g. TSI CCS) are regulated with the “Change Control Management” (CCM) procedure, under the responsibility of ERA (which is the system authority for ERTMS). More specifically, ERA has established and is responsible for managing and updating a register of ERTMS specification Change Requests (CR) and their status. Furthermore, ERA lay out the functional and technical requirements, including indications and parameters for possible subsystem renewals and upgrades, and the procedures to assess the conformity for ICs and subsystems.

Part of ERA decision will be if the proposed ETCS enhanced architecture (e.g. ASTP or other possible solutions for GNSS-based train localization) is introducing a new interoperability constituent and if the functions in charge of the proposed ETCS enhanced architecture (i.e. ASTP) are independent from the other functions allocated to the ETCS interoperability constituents.

Moreover, decision shall be taken if there is the need for ‘type approval’ of HW components of GNSS-based train localization device and, in case of positive response, proper Regulations are needed for the type of approval; then the installation itself of the device should also be approved.

9.2 How to fulfil highest safety integrity requirements typical of ERTMS-ETCS applications

Another critical challenge in GNSS-based railway solutions for train localization is how to meet the highest safety integrity requirements (SIL4) that are typically requested when considering ERTMS-ETCS applications; the fact of demonstrating certifiable SIL4 compliance requires:

- GNSS augmentation systems designed to support safety-critical applications, mitigating risks associated with signal interference, multipath effects, Non Line-Of-Sight (NLOS) reception, Radio Frequency Interferences (RFI), GNSS signal attenuation and integrity failures.

This project is funded by European Union’s Horizon Europe programme under grant agreement No 101180124

- development of advanced fault detection and mitigation strategies to prevent positioning errors that could impact train operations and passenger safety
- methods for assessing the safety performance of the algorithms in charge to validate the integrity of the GNSS system and in charge to calculate the current position accuracy.
- defining a standardized GNSS augmentation framework that ensures consistent and reliable performance across different railway environments.
- establishing standard digital maps with a uniform format, ensuring compatibility across rail networks and signalling technologies.

9.3 User and System Requirements for Assessment and Certification

As already anticipated in chapter 4.1 of this document, and as fully described at § 3.3 of the document 'D2.1 Rail User & System Requirements' [VC.2], User and System Requirements derivation for GNSS-based train localization has been performed by taking as inputs the deliverables D21.1 and D21.2 from 'ERJU Flagship Project 2 (FP2) R2DATO' and, more in general, the results of the Europe's Rail System Pillar activities.

The general approach that is intended to be followed in the VICE4RAIL project about the 'object' of future Assessment/Certification is that while the 'ASTP' solution should represent the primary and most relevant use case, the HyVICE platform and its associated tools and methodologies shall be designed to be capable of assessing/certifying any future GNSS-based location system, considering the ASTP as a core case study (being the flagship solution promoted in Europe's Rai) but not exclusively.

In particular, the aim of the VICE4RAIL project is to develop the HyVICE platform in such a way to be capable to assess performance of different customised GNSS-based train localization systems and to operate independently of the specific technology/architecture used for the GNSS-based train localization by the signalling system provider. This will contribute to reduce the risk of over-reliance on a still evolving solution such as ASTP.

Actually, ASTP solution is the one that implies the most demanding set of requirements for the VICE4RAIL certification framework, whereas the HyVICE platform, in line with the open vision of the VICE4RAIL project, should be as much as possible designed to support not only 'absolute positioning' systems but also alternative solutions such as e.g. virtual balise-based approaches, in order to develop a process capable of assessing a wider spectrum of GNSS-based solutions.

Using the ASTP as the 'primary reference' is a strategic choice that will allow to establish a forward-looking baseline for the VICE4RAIL project's activities, ensuring alignement with the most advanced evolution of GNSS-based positioning for ERTMS.

9.4 Relying on services provided by entities outside the Railway domain

As any safety-related railway system, before entering into service also this GNSS-based train positioning solution for ERTMS/ETCS applications has to pass through future Certification process, by performing the planned process and applying the foreseen standards and by modifying or implementing what is necessary to take into account the introduction of GNSS for train localization. As mentioned, any GNSS-based train localization solution is foreseen to evaluate the train position function by using the satellite constellations. This means that it will be provided by a system "external" to the railway and then out of the Infrastructure Managers' control. Therefore, it is mandatory to evaluate possible added risks coming from this new situation and to eliminate/reduce them as foreseen from the rail safety criteria.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Liability and regulatory clarity regarding the use of GNSS satellite constellations and augmentation services, must be established, as these services are provided by third-party organizations (out of the Infrastructure Managers' and Railway Undertaking's control), raising concerns about accountability and possible risks in case of system failures or inaccuracies.

In the particular case of the GNSS-based train localization, errors occur and can be mitigated not only in the user segment (user equipment on board and on ground), but also in space and ground segments which by their nature cannot be controlled by the Railways end user. This means that the initial integrity level of the Signal-In-Space (SIS) is given by an external entity respect to railways system and shall be trusted and assumed to be an input data for further improvement. For this reason, the SBAS integrity (space segment, out of control of end user) shall be analysed to compute and to justify the initial integrity of the system which is to be improved in the user segment (e.g. by Odometry Diagnosis).

When considering GNSS-based train positioning as well as the ERTMS-ETCS overall SIL4 requirement to be fulfilled, it should be noticed that significant contributor to the safety concept is EGNOS; however, if EGNOS data is sent to the train via geostationary satellites it is sent unprotected, and coverage is very poor. That's why other means of delivering of EGNOS messages to the on-board constituent will be required, such as sending it via the secure radio link between RBC and train. This will likely require an EDAS (EGNOS Data Access Service) type of service suitable for railways applications (i.e. compliant with CENELEC 50159 [NS.17] and with guaranteed safety level and availability); or other similar solutions to be defined.

The role of ERA and EUSPA in the authorization process needs to be clearly defined; in the future VICE4RAIL deliverables (e.g. D5.1, D5.2, D5.3 as for Figure 15) further clarifications will be provided about those aspects.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

10 Conclusions

The VICE4RAIL project aims to contribute to a standard industry-accepted, flexible and scalable certification and assessment procedure, in accordance with with CENELEC and ERTMS standards, covering the integration of possible solutions for GNSS-based train localization into the ERTMS train control system, with a support of a testing and validation system, the 'HyVICE (Hybrid Virtualized Testing Certification Environment)', capable of independently assessing the performance of different train position and velocity determination systems.

The HyVICE platform will leverage on a GNSS-based train location solution to promote the correctness and effectiveness of future assessment/certification process; this will rely on dedicated testing facilities on RFI's railway lines (Bologna San Donato) for evaluating GNSS-based multi-sensor positioning solutions in operational scenarios and in the accredited laboratory of CEDEX, in order to evaluate the end-to-end performance chain using GNSS-based positioning devices in operational scenarios.

The present document constitutes the deliverable **D2.3 'Certification Plan'** of the VICE4RAIL project (Horizon Europe Grant Agreement No 101180124) and is one of the output documents on the WP2 'Hybrid Virtualized Testing Certification Environment Requirements/Development of Certification Plan' Task 'T2.2: Development of the certification plan for the VICE4RAIL solution' as defined in the 'Technical Proposal' [VC.1].

Considering the technical and regulatory background where the VICE4RAIL project is operating, given by:

- Key institutions (main actors and their roles) at European and national levels that regulate compliance with safety, interoperability, and operational standards (see chapter 7.1 of this document)
- European regulations and standards that govern safety, interoperability and certification, that are essential for ensuring safe operation of railway systems (see chapter 7.2 of this document)
- Expertise cultivated in past and on-going projects which have demonstrated the feasibility of using GNSS applications in the context of the ERTMS namely, STARS, ERSAT EAV, ERSAT GGC, GATE4RAIL, HELMET, X2RAIL-2, X2RAIL-5, CLUG, VOLIERA, SBS, EGNSS MATE, RAILGAP, R2DATO, complemented by the results of the 'Pilot Line Novara-Rho' line (see chapter 5 of this document)
- Synergies between rail (CENELEC EN5012x, CCS TSI, etc.), automotive (ISO 26262, ISO/PAS 21448 (SOTIF) and UL 4600), avionics and maritime (RTCM SC-104 and SC-134) standards that have been investigated to identify common elements for assessment/certification (see chapter 6 of this document).

and focusing on:

1) developing a guideline for a certification/assessment framework by relying on the HyVICE platform to be used as testing/validation environment (see chapter 4.2 of this document),
2) defining a possible roadmap for applying the above framework to an 'ASTP' solution, seen as the primary candidate for GNSS-base train localization, but also for other possible alternative solutions such as 'virtual-balise' approach (see chapter 4.1 of this document)

in the chapter 8 of this document the main aspects to be taken into account when setting up future complementary processes such as:

- Risk Management process
- Safety Assessment process
- Interoperability Certification process

have been sketched, by indicating main requested tasks and by cross-referencing documental evidence as requested by regulatory framework with technical deliverables already defined in the VICE4RAIL programme (with possible document integration as suggested in the Annex A – chapter 11 of this document).

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Finally, given that adopting GNSS-based railway solutions for train localization in ERTMS-ETCS applications represents a critical challenge, a preliminary list of open points / investigation areas highlighted in this initial stage of the VICE4RAIL project has been provided at chapter 9 of this document; this preliminary list will be constantly monitored all along the VICE4RAIL project until all open points have been addressed and resolved or mitigated to an acceptable level/extent.

'Risk Management', 'Safety Assessment' and 'Interoperability Certification' process will be applied based on the current Regulatory framework (see chapter 2.1 of this document), on the best compromise between real / simulated functions of GNSS-based train localization (e.g. ASTP) and its interfaces with 'ETCS on-board' / Rolling Stock and with the support of the HyVICE environment (Lab Tests + real Tests in Railway Test Track) properly adapted to the technical/functional features of the selected DUT.

A final review will be accomplished in order to evaluate at which level of extent the compliance of the GNSS-based train localization (as integrated in the ERTMS-ETCS and GNSS environment), with the support of the HyVICE platform, with all the applicable standards and norms can be achieved, and any 'open-point' or 'investigation areas' highlighted in the process will be registered in the final documentation and properly analyzed for suitable follow-up until its resolution.

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

11 Annex A - Guideline for technical documentation/arguments for Certification

The table reproduced here below (extracted from the document 'D2.1 Rail User & System Requirements' [VC.2]) represents a high-level general guideline for all the technical documents/arguments (including VICE4RAIL contractual deliverables) to be considered within this project; the list here below will be monitored and, if necessary, reviewed/updated in the following updates of the D2.3 'Certification Plan'.

In the table here below 3 levels of System Architecture are defined:

1) Component Level: ASTP as individual component

2) Sub-system Level: ASTP as integrated with EVC (ETCS-OB)

3) System Level: ASTP as integrated with complete CCS On-board, CCS Track-side and GNSS

Document/Argument	***System Level***	***Sub-system Level***	***Component Level***
Documentation Plan (this table)	x		
Quality Plan	x		
Safety, Verification and Validation Plan	x		
Certification Plan [NoBo/DeBo/AsBo]	D2.3 Certification Plan D2.4 Synergies in Certification Process for Use in Multimodal Transport		
Specification of User Requirements	D2.1 Rail User & System Requirements		
Preliminary Hazard Analysis	x	x	x
Differences Analysis / Impact Analysis	x	x	x
Analysis of Relevance / Risk Analysis against Reg. 402/2013	x	x	x
Independent evaluation of Analysis of Relevance / Risk Analysis against Reg.402/2013 [AsBo]	D2.2 Risk Analysis Evaluation Report		
System Requirements Specification (Functional, RAM, Safety Requirements)	D3.3 System Requirement Document		
Preliminary System Specification / System Architecture	D3.1 Overall Architecture Design Document		

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Document/Argument	*System Level*	*Sub-system Level*	*Component Level*
Interface Specification	x	x	--
HW Components Requirements Specification	--	--	x
SW Components Requirements Specification	--	--	x
SW Coding Regulations	--	--	x
Detailed System Architecture Specification (including HW and SW)	D3.2 Detailed Design Document	x	x
HW Configuration and SW Release Notes	--	--	x
Hazard/Safety Analysis & Hazard-Log (including Fault Tree Analysis / FMECA: Failure Modes, Effects and Criticality Analysis.)	x	x	x
RAM Report	--	--	x
Test Plan	D3.4 Test Plan		
HW Components Tests Specification/Procedure (including Type Tests / Fault Tests)	--	--	x
SW Modules Tests Specification/Procedure	--	--	x
HW-SW Integration/Validation Test Specification/Procedure	--	--	x
Interface Test Specification/Procedure	x	x	--
System Requirement Tests Specification/Procedure	x	--	--
Design Verification Table (traceability between Req Specs and Test Specs)	D5.1 Validation Strategies	x	x
Development/Manufacturing Documents	D4.1 Procurement List Document D4.2 Development Report		
HW Components Test Report (including Type Tests / Fault Tests)	--	--	x

This project is funded by European Union's Horizon Europe programme under grant agreement No 101180124

Document/Argument	*System Level*	*Sub-system Level*	*Component Level*
SW Modules Test Report	--	--	x
Static Analysis Report / Source Code Verification Report	--	--	x
HW-SW Integration/Validation Test Report	--	--	x
Interface Test Report	x	x	--
System Requirement Test Report	D4.3 Test Report	--	--
System / HW / SW Verification Reports	x	x	x
System Validation Report	x	x	x
User & Maintenance Manuals	--	--	x
Safety Case (including Application Conditions)	x	x	x
Independent Safety Assessment [AsBo]	x	x	x
Safety Acceptance Dossier against Reg. 402/2013	x	x	x
Certification Documents [NoBo/DeBo/AsBo]	D5.2 Certification On-Board Subsystem D5.3 Certification on Track Subsystem and related System Integration		

In the table above the character ‘x’ indicates a document/argument not directly associated to a VICE4RAIL contractual deliverable; in this case it will be considered, within VICE4RAIL project, if a dedicated document has to be produced.

This project is funded by European Union’s Horizon Europe programme under grant agreement No 101180124