VICE4RAIL

D2.2 – Risk Analysis Evaluation Report

Preliminary Assessment Report

Risk management process developed by VICE4RAIL Consortium
pursuant to EU Reg. 402/2013 as amended
for EGNSS-based railway localization solutions

Due date of deliverable: 31/07/2025

Actual submission date: 02/08/2025

Leader/Responsible of this Deliverable: Salvatore Vetruccio (ITCF), Luigi Caccamo (ITCF)

Reviewed (Y/N): Y

Document status		
Revision	**Date**	**Description**
0.1	09/07/2025	First internal release
0.2	18/07/2025	Stable version for review
1.0	21/07/2025	First reviewed version
1.1	28/07/2025	1st Official Release
2.0	31/07/2025	2nd Official Release, receiving feedback 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
Salvatore Vetruccio	ITCF	Author
Luigi Caccamo	ITCF	Author
Antonio Salvi	BVI	Contributor/Reviewer
Alessandro Basili	BVI	Contributor/Reviewer
Ales Filip	UPCE	Reviewer
Vittorio Cataffo	RFI	Reviewer
Nerea Canales Sebastian	RFI	Reviewer
Alessia Vennarini	RDL	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_D2.2	1.1	WP2 Leader	Aleš Filip	Aleš Filip	29/07/2025
		Coordinator	Nerea Canales Sebastian	Nerea Canales Sebastian	29/07/2025
	2.0	WP2 Leader	Aleš Filip	Aleš Filip	01/07/2025
		Coordinator	Nerea Canales Sebastian	Nerea Canales Sebastian	01/07/2025

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

EXECUTIVE SUMMARY

The development of a Certification Process for virtualized GNSS-based positioning solutions which involve system-lifecycle and Lab/On-Site testing moves from current Certification Process on European Railways. This last is well defined inside European Directives and Regulations and ensures that all essential ERTMS-requirements for Safety and Interoperability, as specified in TSIs, are met. VICE4RAIL takes this as the starting point with the aim to define a clear methodology specifically applicable to innovative railway localization solutions.

In the scope of VICE4RAIL project, the proposed certification methodology is based on the procedures and methodology refined for GNSS-based train localization systems. The core of the work will be HyVICE platform and the proposed methodology, and the first part of this approach has been formalized in the document **D2.1 'Rail User & System Requirements'** [9].

In deliverable D2.2 the evaluation of the **Risk Management** process, as provided by the Applicant, in alignment with Reg. 402/2013/EU [1] relating the changing on 'Common Safety Methods' (CSM), will be carried out by the Inspection Organisation, because a change occurs in this way in the railway sub-system. We anticipate the discriminating factor on assessment activities is the impact of change: Relevant or Not Relevant. The Inspection Organisation review will include documentation of the Proposer's (VICE4RAIL Consortium) Risk Analysis, developed in accordance with the CSM-Regulation.

Any new technological solution proposed for ERTMS/ETCS (or in general within the signalling railway subsystem) 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:

- 'Risk Management', in accordance with Regulation 402/2013/EU;
- 'Safety Assessment', in accordance with CENELEC EN5012x standards;
- 'Interoperability Certification', in accordance with Decision 2010/713/EU and TSI CCS.

In the current activity, this process is going to be applied on the ASTP, as the ideal DUT to be proposed as guideline for verification, testing and validation performed by the HyVICE platform under the scope of the VICE4RAIL-project. The alignment to Full ASTP requirements as the primary basis for development is intended to ensure that VICE4RAIL can develop a platform (HyVICE) and related certification methodology capable of addressing the most advanced use cases aligning with the European standardization roadmap.

In the following the first sub-process (bullet "Risk Management") is addressed and analysed.

The Reg. EU 402/2023 can be seen as the backbone for the safety certification process for VICE4RAIL project, due to its ability to logically link the safety management process 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).

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

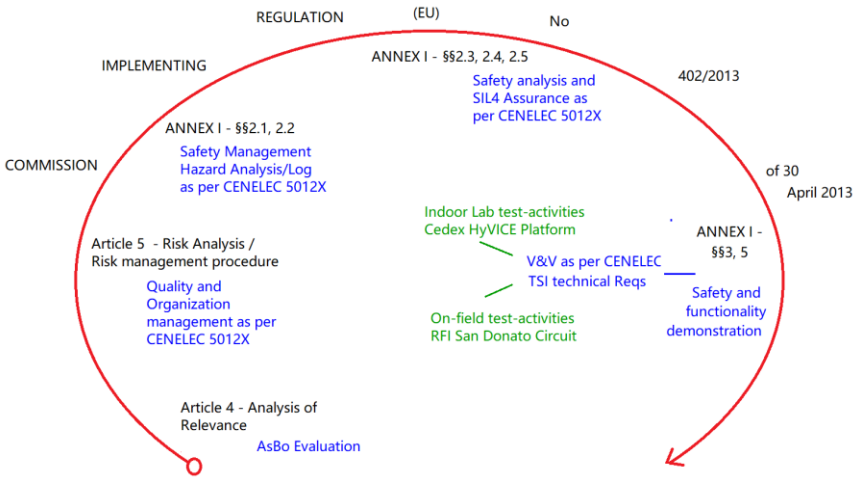

Figure 1: Schematic representation of the CSM-RA process flowchart.

Basically, Reg. EU 402/2013 [1] (throughout its analysis process) covers all relevant aspects of the project and collects all expected goals. More specifically, hereafter we want to better explain the five cornerstone in blue:

1. The analysis of relevance (article 4 of Reg. (EU) 402/2013) 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 analysis of quality management and organizational strategies of the involved companies, as required by EN 50126 and EN50129.
3. The risk analysis/risk management procedure and its evaluation: all relevant aspects contained in CENELEC Standards EN5012x are referenced to demostrate adequate coverage of ANNEX I of Reg. (EU) 402/2013 procedure ([1], 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.
4. The Risk Acceptance, which is obtained (Chapters from §2.3 to §2.5 of Reg. EU 402/2013 [1]) through adoption of good practice codes, CENELEC Standards and TSI, particularly thanks to the accurate risk estimation derived from quantifiable requirements such as the SIL 4 target and technical specifications in signalling TSI.
5. The Demonstration of conformity to the Safety Requirements, identified and registered throughout the previous points (Chapters §3, §5 of Reg. EU 402/2013 [1]). This demonstration has to be objective and well-documented, allowing for evidence of activities conducted both
    a. indoors (HyVICE simulation platform will be the perfect solution)
    b. on-site (RFI San-Donato test circuit is best way to proceed as well).

These activities will fulfill all requirements detailed in:

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.

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

Acronyms and definitions

Acronym	*Meaning*
AsBo	Assessment Body
ADS	Automated Driving System
ASTP	Advanced Safe Train Positioning system
ATO	Autonomous Train Operation
C	Continuity (GNSS)
CA	Consortium Agreement
CAB	Conformity Assessment Bodies
CAT I	Category I precision approach and landing
CE	European Community
CENELEC	Comité Européen de Normalisation Électrotechnique
CoP	Code of Practice
CR	Continuity Risk
CSM-RA	Common Safety Method for Risk Assessment
DeBo	Designated Body
DUT	Device Under Test
EC	European Commission
EGNOS	European Geostationary Navigation Overlay Service
EGNSS	European Global Navigation Satellite System
EUAR (or 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
EVC	European Vital Computer
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
IM	Infrastructure Manager
IMU	Inertial Measurement Unit
ISA	Independent Safety Assessor
ITCF	Italcertifer S.p.a.
LRBG	Last relevant balise group
MTBF	Mean Time Between Failures

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

Acronym	*Meaning*
MTBO	Mean Time Between Outages
NoBo	Notified Body
NSA	National Safety Authorities
OB	On-Board
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
RU	Railway Undertaking
SaRA	Safety-Related Availability
SBAS	Satellite-based augmentation system
SFA	Sensor fusing algorithms
SIL	Safety Integrity Level
SIS	Signal-In-Space
SLA	Service Level Agreement
SOTIF	Safety of the intended functionality
SW	Software
SRAC	Safety Related Application Condition
STB	On-board Technological Subsystem
TLS	Target Level of Safety
TRL	Technology Readiness Level
TSI (or STI)	Technical Specifications for Interoperability
UE	European Union
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

List of figures

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

1 Introduction

Whenever some changes (e.g. the adoption of the ASTP as the candidate solution for a GNSS-based train positioning system) are made to a Member State's railway sub-system, the Regulation (EU) 402/2013 [1] (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 reduce the risk to an acceptable level). 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, tools called Common Safety Targets (CSTs) and Common Safety Methods (CSMs) have been introduced in the Railway Safety management process.

Since the introduction of GNSS into ERTMS/ETCS context represents an important novelty within the European railway network, then CSM-RA process, according to EU legislation, must be applied.

The CSM-RA (Regulation (EU) 402/2013 [1]) sets out a harmonised framework to be applied by the proposer when making any change, significant or not significant (Article 4), 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 set out in Article 5 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). After that, the Independent Assessment is executed by CSM Assessment Body (AsBo).

'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 considered if the related risk can be considered as "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 "Acceptable", a Risk Evaluation activity shall be continued.

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 widely 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.

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

1.1 Scope of the document

This document is intended to assess compliance with Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 [1] and amendment on application of the common safety method for risk evaluation and assessment, formalised in the internal project document "Preliminary Hazard analysis-rev.06" linked to the output of Task 2.1, i.e. "VICE4RAIL D2.1 Rail user & system requirements-rev.7" [9].

The process has been developed by VICE4RAIL Consortium, which acts as Proposer of the introduction of standardized EGNSS-based localization solutions to be used in the framework of the European Rail Traffic Management System (ERTMS), which has to be intended as a research project.

We need to precise that even if VICE4RAIL Consortium acts as Proposer within the aims of VICE4RAIL, its scope is not to obtain final acceptance or authorisation for putting into service of a technological system. The tasks we are currently performing want to be considered as a guideline to explain and present the correct process to future users.

The Global Navigation Satellite System (GNSS) has emerged as a pivotal technology and innovative train localization systems. This technology is going to play a crucial role in the evolution of railway control and signalling systems, improving the economic sustainability and operational effectiveness of the ETCS-ERTMS signalling subsystem.

The analysis is aimed to identify and to assess the risks associated with the change and, if necessary, to assess as appropriate the identified safety measures.

1.2 Structure of the document

The current document is organised as follow:

- **Chapter 1: "Introduction"** with scope and structure of the document;
- **Chapter 2: "Standards and reference documents"** applicable**;**
- **Chapter 3: "Description of the change"** a brief description of EGNSS-based localization solutions to be used in the framework of the European Rail Traffic Management System (ERTMS);
- **Chapter 4: "Independent risk assessment plan"** a schematical presentation of the assessment tasks**;**
- **Chapter 5: "Analysis of impact and significance for safety"** and the subsequent explanation of the consequences derived from this introduction in railway subsystem; overview of the work conducted for D2.2;
- **Chapter 6: "Evaluation of the risk management process"** the description of the assessment activities on the risk management process conducted in conformity to the Regulation (EU) n.402/2013 and amendment;
- **Chapter 7: "Conclusion**" provides closing remarks on the document.

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

2 STANDARDS AND REFERENCE DOCUMENTS

2.1 Technical-methodological reference standards

Reference	Identifier	Title/Description	Issue
(1)	European Commission Regulation (EU) No 402 of 30 April 2013	Adoption of a common method for risk evaluation and assessment, repealing Regulation (EC) No 352/2009	30/04/2013
(2)	European Commission Implementing Regulation (EU) No 1136 of 13 July 2015	Amendment of Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment.	13/07/2015
(3)	Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016	On railway safety	11/05/2016
(4)	ERA Recommendation For Use nr. 1 – AsBo Cooperation	Working method of the Assessment Body	Version 2.0 16/04/2024
(5)	ERA Recommendation For Use nr. 2 – AsBo Cooperation	Harmonised template for the AsBo safety assessment report	Version 1.0 29/03/2023
(6)	ERA Recommendation For Use nr 03 – AsBo Cooperation	AsBo technical knowledge and competence requirements for the different areas	Version 1.1 30/03/2022
(7)	ERA Recommendation For Use nr 8 – AsBo Cooperation	Use by the AsBo of external experts and sub-contractors – Mutual recognition of reports from other conformity assessment bodies	Version 1.0 15/06/2022

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

(8)	ERA Recommendation For Use nr 11 – AsBo Cooperation	Tracking (identification, recording and closing) of issues and non-compliances by the AsBo	Version 1.0 05/11/2020
(9)	None	VICE4RAIL D2.1 Rail user & system requirements	07
(10)	None	Internal project-document Preliminary Hazard Analysis	0.2

3 Description of the change

The described changes in [10] concerns the introduction of standardized EGNSS-based localization solutions in the framework of the European Rail Traffic Management System (ERTMS). Hereafter a brief description of the change, on the basis of the relevant information contained in the documents of the proposer [9] and [10].

Global Navigation Satellite System (GNSS) is one of the key technology for supporting the full Advanced Safe Train Positioning (ASTP) concept. The ASTP system, as described in D2.1, is designed with the aim to enhance the European signalling system by providing more accurate, and reliable localization information. This evolution is strategic for increasing the capacity and efficiency of the railway network, reinforcing its role as a competitive and sustainable mode of transport for both passengers and freight.

Introduction, harmonization and technical integration of ASTP System is the change this report is going to assess. The safe and efficient operation of ERTMS, thanks to the change, is expected to benefit from GNSS subsystems and information with the following main aspects:

- provides continuous absolute train positioning in 3D coordinates (and so longitudinal speed, relative distance from a reference point);
- combines multiple sensor inputs;
- computes the distance providing 1D-orientation.
- Potentially replaces embedded odometry device.

The ASTP system to be introduced is a modular, scalable component that provides localization information to multiple on-board users (e.g., ETCS-OB, ATO-OB) through standardized interfaces, making independence from specific train configurations.

ASTP can utilize various supporting information to achieve performance requirements:

- **Map Data**: Digital representation of track layout and topological information, used for sensor fusion and absolute positioning.

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

- **Augmentation Data**: GNSS augmentation data (e.g., EGNOS) to improve accuracy and integrity of positioning information. The augmentation data may be provided to the ASTP through Signal in Space (SiS) or by the trackside augmentation system.
- **Routing Information**: Point status according to the safe train path uniquely assigned to a train/vehicle, useful for track selectivity determination.
- **Eurobalise Telegram**: Information from physical balises on the track, serving as reference points. This information is provided from the ETCS.
- **Last Relevant Reference Location**: Reference point information (LRBG or virtual reference point) for establishing relative positions.
- **Cold Movement Status**: Information about whether a train has moved during power-off conditions.

ASTP should be able to meet the new localization user requirements pursuing the following main objectives:

1. Reducing the train confidence interval, improving both safety and performance by preventing confidence intervals from increasing indefinitely with travelled distance.
2. Mitigating skidding and slipping effects, which are common issues affecting legacy odometry accuracy, particularly in adverse weather conditions.
3. Significantly reducing systematic errors, such as those caused by incorrect wheel diameter calibration.
4. Reducing the need for physical repositioning reference points, thereby reducing infrastructure costs.
5. Supporting the transition to an on-board-centric approach by enabling the migration of track occupancy functions from trackside to onboard systems.
6. Facilitating the integration of future technologies through a modular safety architecture.
7. Reducing the distance that trains operate in ETCS mode with restricted supervision when a valid and unambiguous train position cannot be ensured, either after Start of Mission or following a recovery from a failure, thereby improving train operation efficiency.

4 Independent risk assessment plan

As described in Annex III of Regulation (EU) 402/2013, as amended, the Assessor's assessment report must be based on an independent assessment plan; this plan has been applied in the development of this assessment and is based on what is stated and required in the regulations referenced in §3.1 of this report and specifically in:

- Regulation (EU) 402/2013 (1);
- Regulation (EU) 2015/1136 (2) (3);
- Recommendation for Use ERA nr.01 (6), 03 (7), 8 (8) and 11 (9).

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

The application of the above assessment plan for the modification (introduction of standardized EGNSS-based localization solutions in the framework of the European Rail Traffic Management System-ERTMS) enabled to assess the compliance of the risk management process, developed by the Proposer, with the requirements of Regulation (EU) 402/2013 as amended and to define the aspects to be analysed.

The above assessment plan is shown below, indicating for each stage of the assessment the planned activities to be developed, that is:

I. Verification of the execution of the analysis of incidence and safety relevance of the sub-system change (developed by the Proposer), in accordance with the provisions of Art.4 of Regulation (EU) 402/2013 as amended;

II. evaluation of the risk management process developed by the Proposer in the document in accordance with Art. 5, Art. 6 and Annex I of Reg. (EU) 402/2013, as amended, which consists of the verification of:

- the coherence of the documentation referenced in §3. 2 of this report for the purpose of defining the system under analysis;

- the identification, classification, and evaluation of hazardous events;

- the coherence of the risk acceptance criterion(s) used;

- the identification of any safety measures and requirements to be implemented to manage the risks associated with the change;

- the evidence of the system's compliance with the safety measures and requirements individuated by the Proposer including verification of the acceptance of the conditions and limitations of use resulting from the Notified/Designated Bodies' assessments;

- verification of the Proposer's acceptance of the residual risk associated with the change.

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

5 Analysis of impact and significance for safety

5.1 Impact of the change on safety

The Proposer, just as properly explained later in the chapter, considers the change with an impact of safety, as follow from the analysis of significance reported in [Ref 1].

5.2 Significance of the Change

The Proposer analysed, only for the changes with impact on safety, the significance according to Art. 4 of the Regulation (1):

> *1. If there is no notified national rule for defining whether a change is significant or not in a Member State, the proposer shall consider the potential impact of the change in question on the safety of the railway system.*
>
> *If the proposed change has no impact on safety, the risk management process described in Article 5 need not be applied.*
>
> *2. If the proposed change has an impact on safety, the proposer shall decide, by expert judgement, on the significance of the change based on the following criteria:*
>
> *(a) failure consequence: credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system under assessment;*
>
> *(b) novelty used in implementing the change: this concerns both what is innovative in the railway sector, and what is new for the organisation implementing the change;*
>
> *(c) complexity of the change;*
>
> *(d) monitoring: the inability to monitor the implemented change throughout the system life-cycle and intervene appropriately;*
>
> *(e) reversibility: the inability to revert to the system before the change;*
>
> *(f) additionality: assessment of the significance of the change taking into account all recent safety-related changes to the system under assessment and which were not judged to be significant.*
>
> *3. The proposer shall keep adequate documentation to justify its decision.*

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

The Proposer assessed the significance of the changes pursuant of Art. 4 of the Regulation (1).

Below are showed the results of this analysis only for the changes significance on safety:

Criteria of Significance pursuant to the Regulation (UE) 402/2013	DESCRIPTION OF CRITERIA	RESULTANTS OF ANALYSIS	
	Failure consequence	**YES**	*"The primary function of ASTP is to provide accurate and reliable localization data to safety-critical applications. A failure of the ASTP to perform this function correctly (e.g., providing an erroneous safe position or velocity) has the potential to directly lead to hazardous situations, such as collisions or derailments. The potential severity of these consequences is considered high".* The change is significant for the "Failure consequence"
	Innovation	**YES**	*"The reliance on GNSS as a primary or significant source for safety-critical train localization, along with the associated sensor fusion algorithms, integrity monitoring techniques for space-based signals, and dependencies on external systems (GNSS constellations, augmentation services), introduces a significant degree of technological and operational novelty compared to traditional ERTMS localization methods (balise/odometry). The change is assessed as having high novelty"* The change is significant for the "Innovation"
	Complexity of the change	**YES**	*"The ASTP system, encompassing multi-sensor data acquisition, advanced real-time processing and fusion algorithms, sophisticated integrity monitoring, and interfaces with multiple systems, presents a substantial level of inherent complexity. This complexity extends to its design, implementation, verification, validation, and maintenance. The change is assessed as having high complexity"* The change is significant for the "Complexity of the change"

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

	Monitoring	**NO**	*"The system is integrated and highly interconnected with the others train on-board systems and the change does not involve the modification, or removal of existing monitoring processes or performance indicators intended to track operational safety metrics post-implementation. Accordingly, it does not influence the determination of the change significance."* The change is not significant for the "Monitoring"
	Reversibility	**YES**	*"In an operational deployment, a full reversion from an ASTP-based localization to a purely legacy system could be complex and may not always be feasible without impacting operational performance or requiring significant infrastructure re-adaptation. Reversibility in an operational context is considered limited".* The change is significant for the "Reversibility"
	Additionality	**NO**	*"ASTP does not constitute an additional or supplementary safety measure to an existing system. Rather, it represents a fundamental transformation of the core train localization architecture. Consequently, this criterion does not contribute to the significance assessment."* The change is not significant for the "Additionality"
	CLASSIFICATION OF THE CHANGE	The Proposer VICE4RAIL Consortium affirmed that the change is **SIGNIFICANT** for safety pursuant to the Regulation (UE) 402/2013	

Therefore, the change under consideration described in §4 of this report, is classified by the Proposer in [10] as relevant to the safety of the rail system, in consideration of the following criteria:

- Failure consequence
- Innovation
- Complexity of the change
- Reversibility

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

5.3 Result of the assessment of impact analysis and significance

On the basis of the above analysis, the Proposer proceeded to determine in [10] the incidence and safety significance of the change under consideration using the criteria set forth in Article 4 of Regulation (EU) 402/2013 as amended, as stipulated in the aforementioned regulation.

6 Evaluation of the risk management process

6.1 Overview of the evaluation of the risk management process

The Proposer, following the significance outcome of the change under consideration, as required by Regulation (EU) No. 402/2013, as amended, has developed a risk management procedure (required in Annex I of the aforementioned regulation) in order to identify and manage the hazards related to the system under analysis. Specifically, the Proposer, in its risk analysis and assessment in [10], should define and describe the main steps of the risk management procedure and specifically:

1) the definition of the system as required in §2.1.2 of Annex I of [1] (§7.1);
2) the identification and classification of hazards with related initial risk assessment as required in §2.2 of Annex I of [1] (§7.2);
3) the selection of risk acceptance criteria as required in §§2.3, 2.4 and 2.5 of Annex I of [1] (§7.3);
4) the identification of safety measures to be applied as required in §§2.3, 2.4 and 2.5 of Annex I of [1] (§7.4);
5) the demonstration of the implementation of safety measures as required in §3 of Annex I of [1] (§7.5);
6) the management of hazards and related risks as required in §4 of Annex I of [1] and the acceptance of residual risk (§7.6)

6.2 System Definition

The system and modification under analysis are described in §3.2 of [9] (see §4 of this report).

Against the above, the system has been defined by the Proposer in accordance with the requirements of §2.1.2 of Annex I of Regulation (EU) 402/2013 as amended.

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

6.3 Identification and Classification of Hazards

The Proposer, at §2.1.6 of [10] has proceeded to identify the potential high-level hazards associated with the system detailed above. Said this, the initial risk, associated with each hazard, has been associated thanks to the well-accepted considerations about severity and frequency of related consequences; considerations directly obtained from CENELEC Standards EN50126:2017 and EN50129:2018.

Just to remind the most important aspects of this practice, we recall from D2.1 [10] the analysis done to identify and list all potential failure modes, causes, and operational issues, and the consequent synthesis of high-level system hazards, coming from the introductions of GNSS technology into signalling subsystem (with the already discussed benefit to the railway ecosystem).

With this premises, the severity of the potential consequences of a hazard is classified according to the following categories (refer to [10]):

Level	Category	Description
S1	Catastrophic	Affecting a large number of people and resulting in multiple fatalities, and/or extreme damage to the environment
S2	Critical	Affecting a very small number of people and resulting in at least one fatality, and/or large damage to the environment
S3	Marginal	No possibility of fatality, severe or minor injuries only, and/or minor damage to the environment
S4	Insignificant	Possible minor injury

The frequency of occurrence of hazardous events is classified according to the following qualitative categories [10]:

Level	Category	Description
F1	Frequent	Likely to occur frequently. The event will be frequently experienced.
F2	Probable	Will occur several times. The event can be expected to occur often.
F3	Occasional	Likely to occur several times. The event can be expected to occur several times.
F4	Rare	Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur.
F5	Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.
F6	Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.

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

The risk level for each hazard is determined by combining its severity and likelihood using the Risk Matrix in §2.3 of [10]. The matrix also defines risk acceptance levels (e.g. Intolerable, Undesirable, Tolerable, Acceptable).

Risk Acceptance Category	Actions to be applied
Intolerable	The risk shall be eliminated.
Undesirable	The risk shall only be accepted if its reduction is impracticable and with the agreement of the railway duty holders or the responsible Safety Regulatory Authority.
Tolerable	The risk can be tolerated and accepted with adequate control (e.g. maintenance procedures or rules) and with the agreement of the responsible railway duty holders.
Negligible	The risk is acceptable without the agreement of the railway duty holders.

Frequency of occurrence of an accident (caused by a hazard)	Risk Acceptance Categories			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Rare	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Undesirable
Highly improbable	Negligible	Negligible	Negligible	Tolerable
	Insignificant	**Marginal**	**Critical**	**Catastrophic**
	Severity of an accident (caused by a hazard)			

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

Keeping this in mind, the list in the table below appear clear, which is an extract of table at §2.1.6 of [10]

Hazard ID	Name	Description	Initial risk acceptance level
HAZ-01	*Provision of Hazardously Misleading Information (HMI)*	*ASTP provides localization data (1D position/ distance travelled, speed, acceleration) to a safety-critical consumer (i.e., ETCS-OB) that is incorrect (outside its reported confidence interval) but is flagged as safe/valid. The integrity of the information is compromised, but the system erroneously claims it is trustworthy.*	*Intolerable*
HAZ-02	*Unavailability of Localization Function*	*ASTP fails to provide valid and safe localization data to its consumers, forcing the consuming system (e.g., ETCS-OB) into a fallback state.*	*Undesirable*
HAZ-03	*Late Provision of Localization Data (Latency)*	*ASTP provides correct and high-integrity localization data, but the end-to-end delay (from measurement to consumer reception) exceeds the maximum specified latency, causing the consumer to operate on obsolete information.*	*Undesirable*
HAZ-04	*Malicious Compromise of Localization*	*A deliberate and malicious attack compromises the integrity or availability of the ASTP system or its data, with the intent to cause a hazardous event or a denial of service.*	*Undesirable*

Against the above, the hazards have been identified and classified by the Proposer in accordance with the requirements of §2.1.3 of Annex I of Regulation (EU) 402/2013 as amended, provided that they must be confirmed and refined at later stage when a more detailed analyse will be possible.

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

6.4 Selection of Risk Acceptance Criterion

The Proposer identifies, the risk acceptance criterion as required by §2.1.4 of Annex I of Regulation (EU) No. 402/2013 as amended.

More specifically the Proposer used the following principles:

- Codes of Practice (CoP): the Proposer declares that ASTP development must adhere to CENELEC standards (e.g., CENELEC EN 50126/50129/50716) and shall be compliant to Technical Specification for Interoperability (TSI);
- Explicit Risk Estimation (ERE): the Proposer points out that the safety of the system should be demonstrated by defining explicit safety targets for each critical function (e.g., a THR of $< 10^{-9}$ failures per hour for SIL4 functions contributing to hazards).

Against the above, the risk acceptance criteria were selected by the Proposer in accordance with the requirements of §2.1.4 and §2.1.5 of Annex I of Regulation (EU) 402/2013 as amended, provided that they must be confirmed and refined at later stage when more details will be available.

6.5 Identification of Safety Measures/Requirements

Based on the chosen risk acceptance criterion (discussed in §7.4 of this report), the Proposer has identified in §2.1.6 of [10] a preliminary list of safety measures to be implemented. Safety requirements from VICE4RAIL D2.1 [9] are applicable in order to better understand the link between deliverable in this WP2). As already stated in [9], the safety measures in the list are designed to control or mitigate the risk, towards an acceptable level, and we chose to maintain the same ID-codes presented in [9] to reiterate the logical connections between these two documents, so we have:

- MAN-01: The ASTP shall implement self-diagnostic functions to detect hardware and systematic failures of its internal sensors.
- REL-01, AR-01: The ASTP shall meet reliability (MTBF) and availability targets at least equivalent to existing ETCS odometry solutions.
- SAF-03: The system's safety is to be ensured and demonstrated according to CSM-RA and EN 50126. This implies a rigorous development lifecycle.
- SAF-04, SAF-05, SAF-06: The true value of position, speed, and acceleration shall be contained within the computed confidence interval with a probability compliant with the specified Tolerable Hazard Rate (THR) for SIL4.
- FR-12: The ASTP shall use a common and safe time synchronization technique compliant with standards like EN 50159, ensuring temporal data consistency across all interfaces.
- FR-15: The ASTP shall be robust to train track adherence phenomena (slip/slide).
- PER-06: The ASTP dataset time validity shall not exceed 200 ms. This provides a hard, verifiable requirement for latency.
- SEC-01, SEC-02: The ASTP shall be designed following a systematic, standards-based (e.g., CLC/TS 50701) cybersecurity risk management process.

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

- SEC-03: The security of the ASTP shall be ensured by implementing technical and procedural measures as defined in a dedicated project security plan.
- SEC-04: The ASTP shall be resilient to signal spoofing and jamming attacks. Appropriate detection measures of such conditions and mitigation measure to counter such attacks shall be addressed to keep the integrity of the ASTP.
- INS-02: Requirements for an easy installation process.

Against the above, the security measures to be implemented have been defined by the Proposer in accordance with the requirements of §2.1.6 of Annex I of Regulation (EU) 402/2013 as amended, provided that they must be confirmed and refined at later stage when more details will be available.

6.6 Demonstration of compliance of Safety Measures/Requirements

The Proposer did not identify the entities in charge of controlling hazardous and managing the related risks, and did not provide evidence of either correct implementation or the correct transfer to third parties, as indicated in § 2.1.7 of Annex I of Reg. (EU) No. 402/2013 as amended

The Assessor will evaluate the evidence of Safety Measures/Requirements implementation at a later stage of the project.

6.7 Hazards Log and Acceptance of Residual Risk

The Proposer created the “Hazard Log” as required in §4 of annex I of reg. 402/2013 as amended (see § §2.1.3 of [10]), and in it declared the residual risk as tolerable and therefore acceptable, provided that it must be confirmed and refined at later stage through more detailed analyses.

6.8 Results of the Assessment

Based on the documents reviewed and the previous paragraphs, the Proposer has proceeded, preliminarily, to:

- define the system;
- identify high-level hazards for the ASTP system;
- identify corresponding safety measures;

in a manner consistent with the provisions of Annex I of Regulation (EU) 402/2013 as amended provided that:

- when not in the preliminary-stage, the Proposer will provide evidence of actually implemented Safety Measures, and of related covered requirements;
- the results of the analyses in [10] must be confirmed and refined at later stage through more detailed analyses.

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

7 Conclusions

7.1 Conclusion related to the assessment

The Proposer, in the preliminary analysis in [10], applied the common safety method for the determination and assessment of risks in accordance with Regulation (EU) 402/2013 as amended in order to determine and assess the risks associated with change inherent in §4.

In [10] the Proposer declares that "*These preliminary conclusions must be confirmed and refined at later stage through more detailed, quantitative analyses.*"

In particular, in this preliminary analysis the Proposer has proceeded to carry out:

- the classification of the modification as significant on safety of the railway system, using the criteria set out in Article 4 of Regulation (EU) 402/2013 as amended, as provided by the said Regulation;
- a preliminary definition of the system under analysis, based on the provisions of §2.1.2 of Annex I of Regulation (EU) 402/2013 as amended (§7.1 of this report);
- a preliminary identification and classification of high-level hazards for the ASTP system resulting from the introduction of the change under consideration, based on what is indicated in §2.1.3 of Annex I of Regulation (EU) 402/2013 as amended (§7.2 of this report);
- identification of the risk acceptance criteria, based on what is indicated in §2.1.4 and §2.1.5 of Annex I of Regulation (EU) 402/2013 as amended (§7.3 of this report).
- a preliminary identification of safety measures to be implemented in order to adequately manage the previous high-level hazards:
- the classification of the level of residual risk following the introduction of the change, identified as "Tolerable";

Regarding the application of the Common Safety Method for risk management process in accordance with Regulation (EU) 402/2013 as amended and supplemented, in order to determine and assess the risks associated with the system that is the subject of this report, the Proposer has completed the Preliminary Risk analysis.

During the following stages of the project, the Proposer shall proceed to:

- define the system with any additional detail coming from next phases, according to §2.1.2 of Annex I of Reg. (UE) n.402/2013 and amend;
- identify any additional hazards that will not only be high-level and classify these hazards resulting from the introduction of the change under consideration, based on what is indicated in §2.1.3 of Annex I of Regulation (EU) 402/2013 as amended;

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

- define any additional safety measures to be implemented and the respective persons in charge of their implementation, based on what is indicated in §2.1.6 of Annex I of Regulation (EU) 402/2013 as amended (§7.4 of this report);
- identify and track, the evidence of implementation of the identified safety measures on the basis of what is indicated in §2.1.7 of Annex I of Regulation (EU) 402/2013 as amended (§7.6 of this report).
- always monitor in the later stages the level of residual risk following the introduction of the change, for all hazard it shall be "Acceptable".

All previous points are mandatory to demonstrate full compliance to Reg. (EU) 402/2013 [1] at the final stage of the Lifecycle (as per EN5012X) of the system implementing the change. However, as the VICE4RAIL project is a research initiative, it does not encompass the complete execution of all product lifecycle phases. Therefore, the points are provided to offer a comprehensive view of the overall process. For the purposes of the VICE4RAIL project, these points serve as references for updating related information and documentation (including this report), which may support the project's development and progression. Nonetheless, they are not considered mandatory within the scope of this research project.

7.2 Conclusion about task D2.2

Thanks to the deliverables submitted within the deliverable D2.2, the VICE4RAIL project has achieved important results that can be summarized as follow:

- Common safety methods (CSMs) have been implemented and assessed to ensure that a high level of safety is maintained and, where necessary, improved, strictly following the guidelines defined by the European Commission.
- Within this preliminary stage, the assessment has been conducted in strict coherence with Reg. (EU) 402/2013 [1], in order to improve clarity and avoid differences in application. Great importance has been given to well describe and applicate roles and relations between contributors, and also between certification/authorization procedures in the whole railway sector.
- The assessment has been performed by an independent body, recognized and which fulfils the criteria required in Reg. (EU) 402/2013 [1].
- The risk analysis and the related assessment provided in the D2.2 are able to demonstrate that the risk management process and independent assessment procedure adhere, in this preliminary stage, to the activity-flow, which we here recall from the Appendix of the Reg. (EU) 402/2013 [1].
- The application of this common approach for specifying and demonstrating compliance with safety levels and requirements of the railway system constitutes, from now on, a guideline for the implementation of novel EGNSS-based railway localization solutions in the railway sector, representing an important contribution to the liberalization of the railway market.

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