VICE4RAIL

D2.4 – Synergies in the certification process for use in multimodal transport

Due date of deliverable: 31/07/2025

Actual submission date: 31/07/2025

Leader/Responsible of this Deliverable: Univerzita Pardubice (UPCE)

Reviewed (Y/N): Y

Document status		
Revision	**Date**	**Description**
01	22/11/2024	First internal release - Table of Contents defined; section on Significance of GNSS continuity for land transport described.
02	06/02/2025	Second internal release - the following sections were elaborated: Safety concepts; Review of safety standards; Safety-related availability
03	18/03/2025	Third internal release - SOGEI contributed by description of RTCM SC-104 / SC-134 standards and GNSS augmentation systems for rail; Introduction and section on Methodology for using synergies identified.
04	31/05/2025	Fourth internal release – Stable version for internal review.
05	14/07/2025	Fifth internal release – This version was internally reviewed.
06	17/07/2025	1st Official Release
07	26/07/2025	Final version

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
Aleš Filip	UPCE	Author
Roberto Capua	SGI	Contributor
Francesco Rispoli	RDL	Contributor
Alessia Vennarini	RDL	Reviewer
Alessandro Neri	RDL	Reviewer
Domenico DeLisi	BVI	Reviewer
Nerea Canales Sebastian	RFI	Reviewer
Vittorio Cataffo	RFI	Reviewer
Giacomo Labanca	RFI	Reviewer
Fabio Frittella	SGI	Reviewer
Daniele Antonetti	SGI	Reviewer
Camillo D'Amico	SGI	Reviewer
Veronica Tripodoro	BVI	Reviewer
Cristian Veglia	BVI	Reviewer
Antonio Salvi	BVI	Reviewer
Alessandro Basili	BVI	Reviewer
Emilie Cheneau-Grehalle	SNCF	Reviewer
Luigi Francesco Caccamo	ITCF	Reviewer
Salvatore Vetruccio	ITCF	Reviewer
Juliette Marais	UNI EIFFEL	Reviewer
Simon Collart-Dutilleul	UNI EIFFEL	Reviewer
Zdeněk Němec	UPCE	Reviewer
Tomáš Zálabský	UPCE	Reviewer

DISTRIBUTION LIST

Name	Company	Roles/Title
Salvatore Sabina	Expert Advisor	General review of the document
Philippe Citroën	Expert Advisor	General review of the document

APPROVAL STATUS

Document Code	Rev.	Role	Approved	Authorised	Date
VICE4RAIL_D2.4	07	WP2 Leader	Aleš Filip	Aleš Filip	24/07/2025
		Coordinator	Nerea Canales Sebastian	Nerea Canales Sebastian	26/07/2025

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

EXECUTIVE SUMMARY

The railway sector is undergoing significant digital transformation to meet growing demands for safer, more efficient, and sustainable transportation. The integration of Global Navigation Satellite System (GNSS) technology into the European Rail Traffic Management System (ERTMS) can improve safe train localization and bring significantly advantages to the entire sector. Despite the transformative potential of this technology to enhance safety, operational efficiency, and cost-effectiveness in railways, its deployment is hindered by the absence of a standardized and industry-accepted certification methodology tailored to the railway sector's specific requirements. The VICE4RAIL project addresses this critical gap by developing a hybrid virtualized testing and certification framework tailored to EGNOS and Galileo (EGNSS)-based railway localization solutions.

This D2.4 deliverable entitled “Synergies in the certification process for use in multimodal transport” describes a review of safety assessment and certification procedures in the rail, automotive and maritime sectors with the aim of identifying common elements to streamline the certification of GNSS-based positioning in multimodal transport. The practical application of the analysed synergies in the certification process is demonstrated in D2.4 by the example of the identified common element, which is GNSS continuity. It is shown what role GNSS continuity plays in achieving the required reliability or safety of positioning in land transport. It should be noted that the use of GNSS continuity has not been sufficiently explored in recent R&D projects on GNSS safety applications in rail or road transport – even though GNSS continuity in aviation significantly impacts the costs of GNSS infrastructure.

The main objective of this work was 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.

Since it is assumed that the analysis of the reliability of GNSS-based vehicle positioning is required not only in rail transport, but also in other transport sectors (aviation, maritime, automotive), it was necessary to carry out preparatory work before performing the analysis of the continuity attribute. This preparation consisted of 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 the given areas of application, and clarifying the terminology of safety and dependability – especially in the context of the recent introduction of the automotive safety standard ISO/TR 4808 on the dependability of automated driving systems (ADS). In connection with techniques for achieving the required ADS safety, the term Safety-related Availability (SaRA) was clarified, as well as the automotive concept of Safety of the Intended Functionality (SOTIF), which follows on from functional safety according to ISO 26262 and is achieved through the massive use of verification and validation techniques, including those based on extensive simulations.

One of the main findings obtained using Markov modelling is the improvement of the reliability of GNSS-based positioning systems in terms of the mean time to system failure ($MTTF_{sys}$). This can be significantly increased from approximately 521 hours, which corresponds to the aviation continuity for a Category I approach, to $5x10^5$ hours required for GNSS-based positioning for the ERTMS system. Finally, GNSS architecture and interfaces of GNSS augmentation for ERTMS were outlined, which will be designed within WP3 “Reference Architecture design” of the VICE4RAIL project.

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

List of tables

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

Abbreviations and Acronyms

Acronym	Meaning
A(t)	Availability
ACSF	Automatically Commanded Steering Function
ADS	Automated Driving System
AI	Artificial Intelligence
AL	Alert Limit
APV I, II	Approach with Vertical guidance I, II
ASIL	Automotive Safety Integrity Level
ASTP	Advanced Safe Train Positioning
BTM	Balise Transmission Module
C	Continuity (GNSS)
c	Coverage (diagnostic)
CAT I	Category I precision approach and landing
CCS	Control Command Signalling
CCS-OB	Control Command Signalling Onboard
CCS-TS	Control Command Signalling Trackside
CENELEC	European Committee for Electrotechnical Standardization
CoP	Codes of Practice
CR	Continuity Risk
CSF	Corrective Steering functions
CSM-RA	Common Safety Method for Risk evaluation and Assessment
CTI	Continuity Time Interval
DFMC	Dual-Frequency Multi-Constellation
DGNSS	Differential GNSS
DH	Decision Height (in aviation)
DPF	Dual Point Fault/Failure
EC	European Commission
ECAC	European Civil Aviation Conference
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
EGNSS	European GNSS
EOTTI	Emergency Operation Tolerance Time Interval
ERTMS	European Railway Traffic Management System
ETSI	European Telecommunications Standards Institute
EU	European Union
EUSPA	European Union Agency for the Space Programme
F(t)	Unreliability
FTA	Fault Tree Analysis
GA	GNSS Augmentation
GADF	GNSS Augmentation Dissemination Function

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

GA-OB	GNSS Augmentation Onboard
GAS	GNSS Augmentation System
GA-TS	GNSS Augmentation Trackside
GBAS	Ground Base Augmentation System
GNSS	Global Navigation Satellite System
HARA	Hazard Analysis and Risk Assessment
HAS	High Accuracy Service
HW	Hardware
ICAO	International Civil Aviation Organization
ICD	Interface Control Document
ILS	Instrument Landing System
IMO	International Maritime Organization
IMU	Inertial Measurement Unit
MSC	Maritime Safety Committee
IR	Integrity Risk (GNSS)
ISA	Independent Safety Accessor
ISO	International Organization for Standardization
LPV	Localizer Performance with Vertical guidance
MED	Marine Equipment Directive
ML	Machine Learning
MOPS	Minimum Operation Performance Standard
MTBF	Mean Time Between Failures
MTBO	Mean Time Between Outages
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair (restore)
NCSR	Navigation, Communications and Search and Rescue
NMEA	National Marine Electronics Association
NPA	Non-Precision Approach (aviation)
NRTK	Network RTK
Ntrip	Networked Transport of RTCM via Internet Protocol
OB	Onboard
OBU	Onboard unit
PES	Programmable Electronic Systems
PFH	Average frequency of dangerous failure per hour
PL	Protection Level
PMHF	Probabilistic HW Failure Rate per Hour (ISO 26262)
PPP	Precise Point Positioning
PVT	Position, Velocity and Time
R(t)	Reliability
RAM	Reliability, Availability, Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RAMSS	Reliability, Availability, Maintainability, Safety and Security (automotive)
R&D	Research and Development

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

RINEX	Receiver INdependent EXchange
RNP	Required Navigation Performance
RTK	Real Time Kinematics
RTCM	Radio Technical Commission for Maritime Services
SAE	Society of Automotive Engineers,
SaRA	Safety-Related Availability
SBAS	Satellite Based Augmentation System
SC	Special Committee
SDC	Self-Driving Car
SG	Safety Goal
SIL	Safety Integrity Level
SIS	Signal-In-Space
SoL	Safety-of-Life
SOLAS	Safety of Life at Sea
SOTIF	Safety Of the Intended Functionality (automotive)
SRS	System Requirements Specification
SW	Software
THR	Tolerable Hazard Rate
TFFR	Tolerable Functional Failure Rate
TLS	Target Level of Safety
t_{MT}	Mission duration (operational lifetime)
TS	Trackside
TSI	Technical Specification for Interoperability (ERTMS)
TTA	Time-to-Alert
U(t)	Unavailability
U(∞)	Steady state Unavailability
UN	United Nations
UN ECE	United Nations Economic Commission for Europe
V&V	Verification and Validation
VDB	VHF Data Broadcast
VICE4RAIL	Hybrid Virtualized Testing for Certification of EGNSS in Railway Train Positioning
VRS	Virtual Reference Station
WG	Working group
WP	Work package

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

1. INTRODUCTION

1.1 Scope of the document

This document constitutes Deliverable D2.4 “Synergies in the certification process for use in multimodal transport” as part of the Horizon Europe VICE4RAIL project (Grant Agreement No 101180124). It provides a comprehensive overview of synergies applicable in the safety assessment and certification in multimodal transport identified during Task 2.3 of Work Package 2 (“Hybrid Virtualized Testing Certification Environment Requirements/Development of Certification Plan”). The practical application of the analysed synergies in the certification process is demonstrated in D2.4 by the example of the identified common element, which is GNSS continuity. It is shown what role GNSS continuity plays in achieving the required reliability or safety of positioning in land transport. This issue is addressed in D2.4 mainly because the use of **GNSS continuity has often been neglected in recent projects on GNSS safety applications in rail or road transport** [82], [83], [21]. Other outputs associated with the review of safety assessment and certification were created to support the above solution. Although the presented outputs are the result of a comparative analysis related to safe GNSS based positioning in different transport sectors (aviation, rail, maritime, automotive), they will mainly guide the project’s development of a hybrid virtualized testing and certification framework tailored specifically for EGNSS-based railway localization solutions. Nevertheless, the synergies described in D2.4 can also be used for safety assessment and certification of GNSS safety applications in other modes of transport.

1.2 Motivation

Train positioning based on GNSS is a strategic priority for realising the Advanced Safe Train Positioning (ASTP) system to enhancing the performance and competitivity of the European Railway Traffic Management System ERTMS. For safe and efficient operation of ERTMS integrated with GNSS it is necessary to demonstrate not only the required integrity (i.e. correctness) of GNSS-based positioning, 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 approach.

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 due to applied redundancy. GNSS continuity analysis and methods to increase the reliability of GNSS-based train location are currently being used in the EU VICE4RAIL project to develop plans and procedures for the certification of train positioning solutions.

The aim of this research is to close this gap 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 deliverable, we focus on GNSS continuity - its correct interpretation

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

and use in land transport, especially in terms of meeting the requirement for reliability of position, velocity, and time (PVT) determination. The aim of this effort is to start with the 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 ground 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 (Reliability, Availability, Maintainability and Safety), as a variant to the aeronautical safety concept, in the RNP sense, for comparative analysis and further investigation.

One of the main objectives of introducing GNSS into ERTMS is to reduce the maintenance costs of physical balise while keeping the required operational availability of ERTMS. Availability is generally dependent on reliability and in the case of the aviation requirement for continuity of GNSS service, it can be expressed by reliability. In the field of automated driving of cars, where the performed driving functions cannot be interrupted for safety reasons (overtaking of car, lane changes, etc.), then Safety-Related Availability (SaRA) requirements must be defined for these functions. In maritime transport, as in aviation, GNSS continuity is one of the two main safety attributes (next to integrity). The criticality of continuity for safety, reliability and availability of GNSS applications has long been overlooked in automotive and rail transport. Therefore, the application output in this deliverable mainly consists in the use of GNSS service continuity in land transportation and related safety assessment and certification activities. The diversity and synergies associated with the use of GNSS in multimodal transport make it possible to form the necessary opinion on the possible use of aviation GNSS continuity in other transport modes as well.

Since it is assumed that the analysis of the reliability of vehicle positioning based on GNSS is also required in other transport sectors (aviation, maritime, automotive), not only in railways, 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 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 on dependability (RAMSS) for automated driving systems (ADS). It was also necessary to clarify the automotive term SaRA used to achieve the required ADS safety in this context. The outputs in this deliverable also include other synergy effects, such as the use of the automotive concept SOTIF (Safety of the Intended Functionality), verification and validation based on simulations in the sense of automotive safety standards and other methods.

These are just some of the reasons why it is useful in railway R&D projects not to focus narrowly on, for example, GNSS-based train localization tasks, but to look at possible localization solutions in other transport sectors as well, which can bring further useful results and ideas.

This is also related to the expectation that the GNSS infrastructure, including regional or local augmentation, will be used simultaneously for various safety applications in multimodal transport, where GNSS continuity may affect, for example, “only” the reliability of the transport application, e.g. on rail, or also safety, e.g. in maritime or automotive. For this purpose, main areas of research have been defined, an overview of which is given in the following section.

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

1.3 Structure of the document

The present document is organised as follows:

Chapter 1 - Introduction
Chapter 2 - Safety concepts used in transport
Chapter 3 - Review of applicable functional safety standards and related regulations
Chapter 4 - Clarification of dependability and RAMS terminology
Chapter 5 - Safety-related availability for automotive safety-critical systems
Chapter 6 - Significance of GNSS continuity and reliability in multimodal transport
Chapter 7 - GNSS Augmentation systems for rail
Chapter 8 - Conclusions
Chapter 9 - References

1.4 Methodology for using synergies in the certification process

This section outlines a methodology for leveraging synergies applied in the safety assessment and certification process for GNSS safety applications in multimodal transport. The individual steps of the methodology are described below and illustrated in Figure Introduction-1.

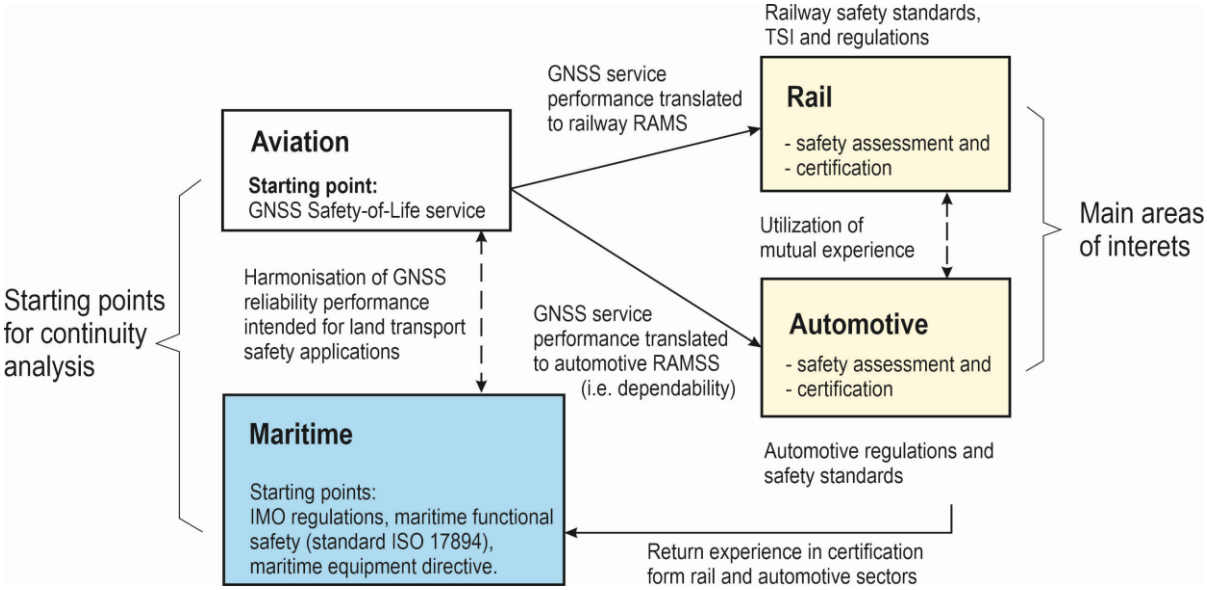

Figure Introduction-1: Methodology for exploiting synergies in the certification process of GNSS-based applications in multimodal transport.

The starting point is the GNSS SoL service developed for aviation. This is because aviation is the first transport sector where the GNSS SoL service started to be used for safety applications. GNSS performance in the sense of aviation requirements is then translated to performance indicators used in other modes of transport (maritime, rail, road). The maritime GNSS requirements in this methodology are used to verify the correct translation of the aeronautical GNSS requirements into GNSS attributes for use in the rail and automotive sectors. Therefore, the maritime GNSS requirements in this methodology are also considered as starting points. This entire solution is accompanied by analyses of safety concepts, safety assessment and certification

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

in multimodal transport. The practical applicability of synergies and related common elements in the certification process aims at the correct use of GNSS continuity, as the use of continuity in land transport has not been sufficiently explored in recent R&D projects.

GNSS applications and their required performance in civil aviation and maritime transport are used in this deliverable primarily to verify the correct meaning of GNSS continuity attributes in these two sectors and to harmonize them. The goal is to understand what GNSS performance can be expected for rail and automotive applications. This can be justified by the fact that continuity requirements are only defined in the aviation and maritime sectors. Verification and validation (V&V) and harmonization of GNSS performance across civil aviation and marine applications is possible because the safety concepts in these two sectors are similar. These are so-called safety-critical systems used in aviation and at sea - unlike, for example, safety-relevant systems used on railways. The difference between these two kinds of systems will be described in more detail in section 2. The safety of maritime GNSS-based applications depends on both GNSS safety integrity and GNSS continuity.

Regarding the use of GNSS for positioning of modern autonomous vessels, the maritime sector is looking for inspiration in the automotive sector, in the area of highly automated and autonomous vehicles [1]. One of the main reasons is that the maritime sector does not have new and detailed standards as the automotive standards and regulations for Automated Driving Systems. For example, the ISO 17894 standard [2] on marine applications of Programmable Electronic Systems (PES), which is an adaptation of the IEC 61508 functional safety standard was published in 2005 - although it is regularly reviewed and confirmed.

Automated driving system (ADS) of cars is currently one of the fastest growing fields in land transport. Similarly, efforts are underway to introduce the Advanced Safe Train Positioning (ASTP) [62] into ERTMS to make railway operations more efficient.

In both these transport sectors, appropriate regulations and updated safety standards are being developed. The railways can benefit from the experience of the automotive sector with ADS certification and the automotive sector can benefit from the experience of the railways with certification of safe train positioning. As indicated in Figure Introduction-1, the experience of the railroad and automotive sectors in certifying safe vehicle positioning based on GNSS can also be leveraged by the maritime sector.

1.5 Relationship with other project outcomes

In this development stage of the VICE4RAIL project, the inputs for the elaboration of deliverable D2.4 (Synergies in the certification process for use in multimodal transport) are mainly the reliability requirements of the ASTP solution defined in deliverable D2.1 (Rail user & system requirements) of the VICE4RAIL project developed within WP2 [63]– see Figure Introduction-2.

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

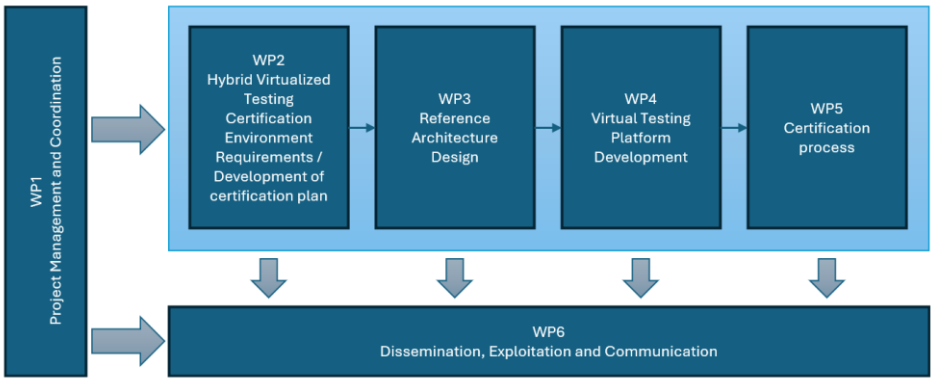

Figure Introduction-2: VICE4RAIL Study Logic.

The main outputs addressed by task VICE4RAIL T2.3 and described in deliverable D2.4 are synergies related to the use of aviation GNSS continuity to meet reliability and safety requirements in multimodal transport. In addition, other outputs in deliverable D2.4 supporting those main outputs are: description of safety concepts used in multimodal transport, review of applicable functional safety standards and other regulations for safety assessment and certification in different transport sectors, clarification of dependability and RAMS/RAMSS terminology and description of Safety-Related Availability (SaRA) in automotive safety-critical systems. A brief overview of the outputs from deliverable D2.4 is also provided in deliverable D2.3 (Certification plan).

It is expected that the outputs of deliverable D2.4 associated with the utilization of GNSS continuity in certification procedures in multimodal transport, whether to achieve the required reliability or safety of vehicle localization, will be subsequently utilised in solving the tasks of the VICE4RAIL project within the work packages WP3 (Reference Architecture Design), WP4 (Virtual Testing Platform Development), WP5 (Certification Process) and WP6 (Dissemination, Exploitation and Communication) - as indicated in the VICE4RAIL Study Logic in Figure Introduction-2.

2. SAFETY CONCEPTS USED IN TRANSPORT

Existing GNSS infrastructure and related safety services will be increasingly used in the coming years to ensure the safety and efficiency of operations in multiple modes of transport simultaneously. Not only for air traffic management, as evidenced by the preferred use of the original aviation requirements in the design and certification of GNSS-based safety services.

However, the 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 described below: (i) safety-related and (ii) safety-critical. This classification will, among other things, help to clarify how to properly exploit the aeronautical requirement for GNSS continuity in ground transport, which has been neglected in the past years. Perhaps the only exception has been the maritime sector, as the safety concepts in shipping and air transport are very similar. From the perspective of railways, but also automated car driving, the correct use of GNSS continuity is an urgent problem / open point [3]-[5] which needs to be solved as soon as possible.

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

2.1 Classification of safety systems

A safety-related system ensures the safety of people who are in or around it. It is required for such applications in transportation, medicine, energy, industry, etc. that can cause injury or death to a person when they fail. 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 [6]. *From a safety point of view, it is not necessary to complete the safety operation.* In the event of a fault, for example, the system has a Fail-stop or Fail-soft / Fail-degraded behaviour. In the event of a dangerous failure, the saw motor (or vehicle, machine, lift) is immediately stopped by a safety mechanism. This is ensured by means of the safety functions.

A safety-critical system also protects people's lives, but in a different way than a safety-relevant system. *Here, safe completion of the operation is required in the event of a fault.* A dangerous fault here leads directly to an accident [6], [7]. 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. Examples: an aircraft must safely complete a landing without interruption; a running chemical process must not be stopped immediately, but safely regulated, otherwise there is a risk of explosion; a self-driving car must safely complete an overtake. Fail-safety is based on reliability, which is achieved through redundancy. This means that safety is supervised, for example, by a human operator (pilot) or another technical system.

2.2 Safety concepts in multimodal transport

2.2.1 Road versus Rail transport

The fundamental difference between the concept of safety in road and rail transport is as follows. The driver of a road vehicle can drive at any time, unless this is forbidden in any way, e.g. by a traffic sign or lights, by order of a traffic police officer, etc. Fail-safe design with fail-stop / fail-soft behaviour in many operational situations can be employed to achieve and maintain the required safety. On the other hand, some functionalities cannot be interrupted because it could lead to a hazardous situation. It is e.g. control of vehicle movement during overtaking or lane changing when automated driving system (ADS) is active. Such functionalities which must be completed due to safety reasons are characteristic properties of safety-critical systems. Fail-operational behaviour utilises a property (technique) called fault tolerance. It is based on redundancy. To summarize, an ADS can be considered a safety-related system in many cases because a fail-safe state can be defined, and in some cases, it can be considered a safety-critical system because it is required to complete an operation - not stop it - for safety reasons. Therefore, an important attribute is the reliability of the safety functionality.

In contrast, a train can only travel from point A to point B if it is allowed by technical system or dispatcher to do so – i.e. if it receives a Movement authority (MA). Fail-safe design with fail-stop (or fail-soft) behaviour is applied. Railway signalling is a safety-related system. High reliability of railway signalling systems is mainly required for economic reasons, to keep train delays and downtime to a minimum. Reliability has also an indirect effect on operational safety, because in the event of a failure of the signalling system, an emergency mode is activated with the involvement of the human factor. Any abnormality in the operation can reduce its safety.

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

2.2.2 Aviation

Avionics is generally considered to be a safety critical system because in the event of a system failure, it is not possible to define a safe state of the aircraft to ensure safety. However, it is possible to define a failure mode that leads to a safe state. Therefore, from the point of view of the use of GNSS for flight control, there are two important basic GNSS quality indicators: integrity and continuity. Integrity relates to the correctness of the position information provided during a given operational operation, while continuity relates to the provision of correct information (integrity) without interruption during a critical phase of the operation with duration of 15 s or 1 h. Continuity therefore corresponds to short-term reliability. An example of the allocation of integrity and continuity for SBAS APV I, II and Cat I operations is shown in Figure 1 in [8]. In this case the allocated Integrity Risk (IR) for Signal-In-Space (SIS) is $2x10^{-7}$/150 s and the Continuity Risk (CR) is $8x10^{-6}$/15 s.

It should be noted that the CR allocation is also fully compliant with aviation requirements for the Instrument Landing System (ILS) [27], [37], which was in use long before the introduction of GNSS. This compliance is based on the recommendation that the MTBO (Mean Time Between Outages) or MTBF (Mean Time Between Failures) of Localiser and Glide slope of ILS is 1000 h. Then, based on the reliability theory, it can be calculated that the ILS is required to determine a 3D position at least with an MTBF of 500 h. The corresponding CR values for Localiser and Glide slope are: CR(Localiser) = $4.1666x10^{-6}$/15 s $\approx$ $4x10^{-6}$/15 s, and CR(Glide slope) = $4.1666x10^{-6}$/15 s $\approx$ $4x10^{-6}$/15 s. The CR requirement for GNSS SIS for CAT I in total is $8x10^{-6}$/15 s. Since the duration of the precision approach phase of the airborne operation is short (15 s), the CR requirements can be met even with an MTBF of about 500 h. However, in ground transportation, the system requirements for MTBF are much higher than 500 h, e.g. on the order of 10^5 h. This fact has been often forgotten in previous projects. Therefore, a section on GNSS continuity has been included in this deliverable below.

2.2.3 Maritime

Maritime GNSS based navigation safety systems, similarly as the aviation ones, belongs to the category of safety-critical systems where safety is built simultaneously on safety integrity and reliability. At first reliability requirement for GNSS, not continuity, was specified by the maritime community in 1997 - see the IMO Resolution A.860 (20) [9] and paper [10]. In that time, the reliability of service was defined > 99.97 % during a time interval of 1 year. It was in fact a long-term reliability measure.

Four years later, the term GNSS reliability was replaced in IMO Resolution A.915(22) [11] by the term continuity, which had already started to be used in aviation. Continuity was defined for the duration of a critical maritime operation with a duration of 3 hours. Here, continuity represents a short-term measure of reliability. At that time, the duration of a maritime safety operation meant the duration of the ship's approach to port. When recalculating the continuity from the air service, it was found that the interval of 3 hours was too long and as a result the GNSS air service could not meet the continuity requirements of the maritime sector. An analysis of the duration of critical maritime operations was performed and it was found that a large vessel approach to port lasting approximately 3 hours consists of a series of sub-critical operations (e.g. course change, overtaking other vessels, enter/leave a Traffic Separation Scheme (TSS)) that do not last more than 15 minutes. Therefore, a time interval of 15 min was chosen to define continuity. Even so, this interval is long (relative to 15 s in aviation) and it is difficult to meet the maritime requirement for GNSS continuity, as will be shown below.

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

2.3 Clarification of notions as safe-life, fail-safe, fail-operational, fault-tolerant

In the past, the term fail-safe was and sometimes still is incorrectly used in the context of rail and air transport. Due to the rapid introduction of electronic safety systems also in self-driving cars, this and related terms need to be clarified. This is also important for the correct use of GNSS for safety applications in multimodal transport.

It is stated in the field of railway signalling that the fail-safe principle is used here, which is related to the fact that the train can stop or slow down in the event of a dangerous failure of the signalling system and thus reach a safe state. In contrast, in the context of air transport it was (and still often is) argued that in the event of a dangerous failure of the avionics or some other fault on the aircraft, the fail-safe principle cannot be applied and therefore the aircraft cannot be stopped because the aircraft must complete the flight safely. The following paragraphs will describe the behaviours and operational modes of safety architectures to clarify the relationship between fail-safe and other safety notions that affect the classification of safety architectures and the use of GNSS. The goal is to make the terminology consistently applicable to GNSS applications in multimodal transport.

2.3.1 Safe-life design

The safe-life (i.e. safety-by-retirement) design approach was applied in aviation when metal structures were introduced (1930s). Safe-life refers to the philosophy that a component or system is designed to not fail within a certain, defined period. Later, safe-life was replaced by fail-safe principle – see below.

2.3.2 Fail-safe design

It is a design feature which enables to enter or remain in a safe state (fail-stop, fail-soft) in the event of failure. Fail-safe design is not defined and explicitly required in the generic functional safety standard IEC 61508 [12] or in the automotive functional safety standard ISO 26262 [13]. On the other hand, fail-safety is a basic safety design used in railway signalling – see EN 50129 [14]. The allowed safety techniques for the design of a railway fail-safe system include a) inherent fail-safety, b) reactive-fail safety and c) composite fail-safety.

Besides railway signalling, fail-safe design has also been widely used e.g. in the process industry, civil aviation and nuclear power plants. In the 1950s, when problems with the safe-life design in aircraft structures occurred, mainly due to the limited service live of critical components, the fail-safe concept in aviation was introduced – i.e. safety-by-design. Fail-safety applied to the aircraft structure design was based on redundancy - e.g. the redundant number of screws attaching the wings to the fuselage. Another example of a fail-safe design used in aviation is a flight control system – e.g. manoeuvring characteristics augmentation system (MCAS) of the Boeing 737 MAX.

2.3.3 System behaviour

Fail-stop behaviour: This refers to stopping the system (vehicle/process) in the event of a system failure.

Fail-soft (Fail-degraded) behaviour: It is not directly stopping the system, but only limiting its performance, e.g. speed of vehicle.

Fail-safe behaviour: A system is able to enter or remain in a safe state in the event of a failure (EN 50129).

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

Fail-silent behaviour: A fail-silent system is a type of system that either provides the correct service, or provides no service at all (becomes silent). For example, the automotive Lane Assist (Lane Keeping System) provides no action in the case of a failure.

Fail-operational behaviour: Fail-operational systems continue to operate when their control systems fail [48]. This is the behaviour of a system without a safe stop state that could otherwise be reached fast enough in the event of a failure. The system must remain operational and provide a minimal amount of guaranteed service – e.g. airplane must safely continue in flight, self-driving car must safely finish overtaking, chemical process must safely continue to avoid a hazardous event, etc. To achieve the fail-operational behaviour of the system, fault-tolerance is required.

The relationship between the types of safety systems, system design concepts, and system behaviour is shown in Figure Safety concepts used in transport-3.

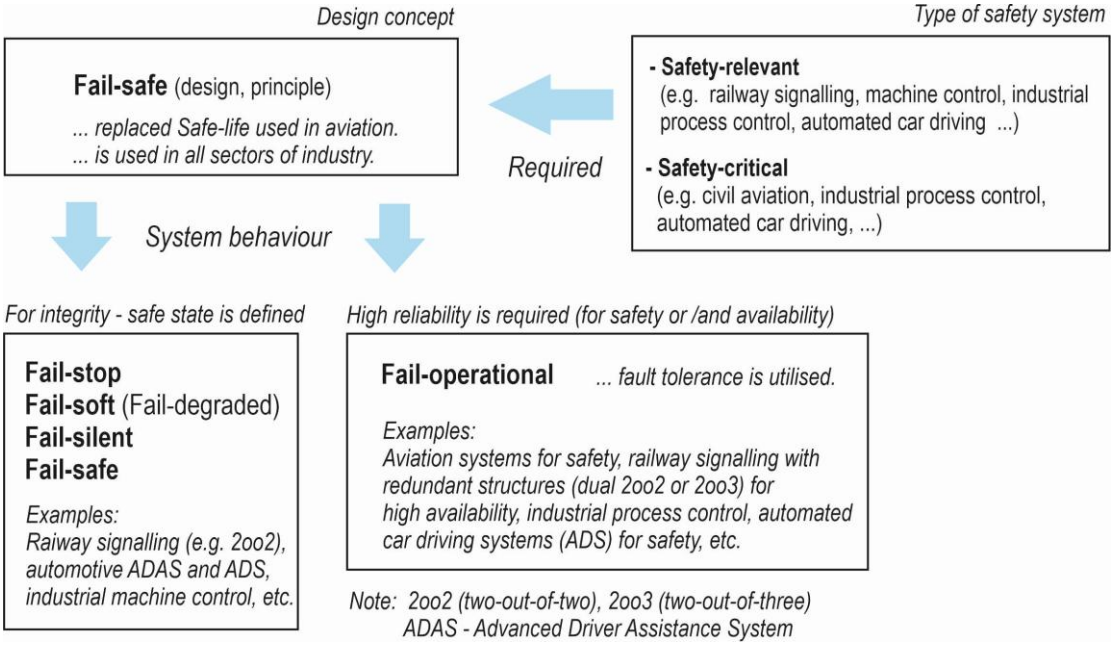

Figure Safety concepts used in transport-3: Relationship between the types of safety systems, system design concepts, and system behaviour.

Fault tolerance is a property (or technique) that enables fail-operational behaviour of a system in the event of a failure of any of its components. This is only possible with a redundant system design. To properly design fault-tolerance into a system, it is necessary to identify if the system items/ channels are redundant or not. According to the automotive standards ISO 26262, fault tolerance is the ability to deliver a specified functionality in the presence of one or more specified faults. Fault-tolerance and fail-operational behaviour are not explicitly defined in railway safety standards.

Nevertheless, in addition to high safety integrity, high availability of railway signalling is also required, because excessive number of signalling system interruptions may have in addition to financial losses also indirect impact on the overall safety of railway system. Therefore, fault tolerance and fail-operational behaviour are also critical for railway signalling, not only for aviation systems or self-driving cars.

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

3. REVIEW OF APPLICABLE SAFETY STANDARDS AND RELATED REGULATIONS

This section provides an overview of the basic safety standards and regulations required for safety applications in multimodal transport. The aim of the overview is to 1) harmonise the terminology/measures of reliability and safety, particularly with regard to the use of GNSS continuity to achieve the required reliability and safety in land transport, and 2) identify possible techniques and procedures used in non-rail sectors that could also be applicable for the safety assessment and certification of GNSS in land transport and could potentially be effective for the certification of the HyVICE platform within this project.

3.1 IEC 61508

IEC 61508 [12] 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/ EN 50716 [14]-[17] for railways, ISO 26262 [13] 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. This safety standard specifically covers hazards that occur when safety functions fail. The main objective of IEC 61508 is therefore to reduce the risk associated with a hazardous failure to an acceptable level. IEC 61508 is built on two fundamental pillars: i) the safety lifecycle intended to reduce or eliminate failures due to systematic causes during system development and operation, and ii) the probabilistic failure approach to address dangerous random HW failures via Safety Integrity Levels (SILs). This concept is strengthened by the fact that the system must be developed, validated and assessed according to specific requirements which result from the hazard identification and risk analysis. IEC 61508, on the other hand, does not cover the effects of human factors on safety during operation as this goes beyond functional safety.

Predictable behaviour of the system can be achieved in case of both systematic and random failures. A systematic failure is deterministically linked to a specific cause that can only be eliminated by modifying the design (rules) or method of the production process, operating procedures, documentation, or other relevant factors. In case of random failures, the required predictability of the system can be achieved through probabilistic description of the system behaviour. Deterministic means that each event or state is the result of previous events on the principle of causality and fixed rules. Causality and rules are necessary for the predictable behaviour of a system in the event of its failure.

3.2 Railway safety standards and regulations

The basic framework for ensuring the safety and dependability of railway systems is defined in EN 50126-1 [15] on the specification and demonstration of RAMS (Reliability, Availability, Maintainability and Safety). EN 50129 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

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

RAMS within the system life cycle. Safety shall be demonstrated by means of safety case and independent third-party assessment. The basic framework defined through RAMS can be imagined as an umbrella (Figure Review of applicable safety standards and related regulations-4) under which a safety-related system is subsequently developed and implemented according to the downstream standards EN 50129 [14] (safety-related system), EN 50716 [17] (software for safety-related system), and others. The attribute dependability on railway is defined by the acronym RAM and it will be analysed in more details in section 4.

A safety case and its independent assessment alone is still not enough to ensure safety on European railways. Technical interoperability must also be ensured (Figure Review of applicable safety standards and related regulations-4). In the case of ERTMS, e.g., this means that one manufacturer's on-board equipment works

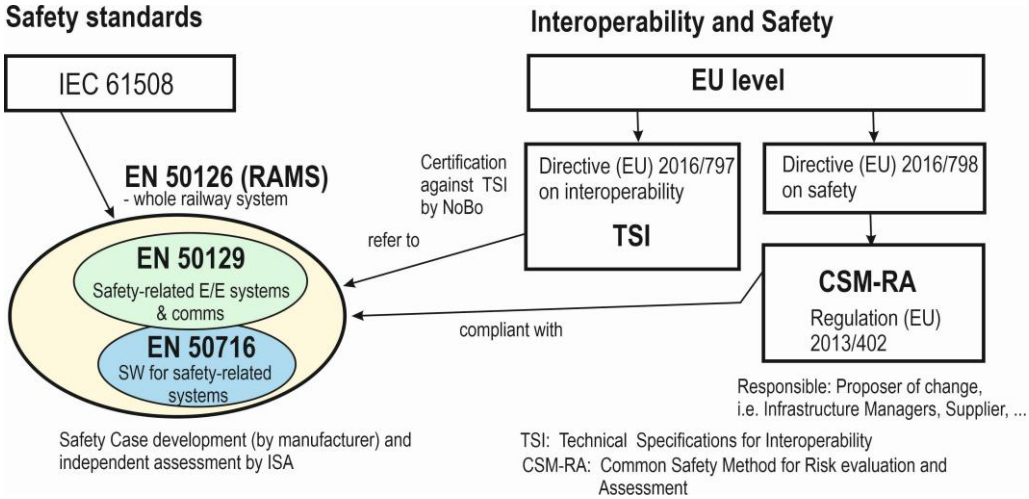

Figure Review of applicable safety standards and related regulations-4: Railway safety standards, interoperability and common safety method.

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 the Regulation (EU) 402/2013 [18] and its amendment (Regulation (EU) 2015/1136), which harmonises the risk assessment process and safety requirements, must be applied. The safety concept of EN 50129, as well as IEC 61508, is based on the predictable (safe) behaviour of the system in the event of a failure. A causal analysis, i.e. an analysis of the reasons how and why a particular hazard can come into existence, is therefore important part of hazard analysis.

A safety-relevant system is designed for a specific operating environment and therefore the rules for its operation and maintenance as well as external influences (such as climatic, mechanical, electrical, IT-security, etc.) must be clearly defined. The conditions, rules and constraints for the design, manufacture, installation, operation, and maintenance of the system (ensuring functional safety) and the way to verify them shall be contained in the document “Safety-related Application Conditions (SRACs)” according to EN 50129. The safety and reliability of system operation with external influences shall be demonstrated in the document “Operation with External Influences”. Both documents are part of the safety demonstration. The safety case

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

is valid only within the specified range of external influences, as defined in the system requirements specification.

The applicable railway safety standards and the assessment and certification processes are described in more details in deliverable D2.1 (Rail user & system requirements) of the VICE4RAIL project [63].

According to railway safety standards EN 50129/ EN 50126/ EN 50716 and IEC 61508, the cause of a failure due to the operational environment is a systematic fault in the system design. In contrast to the automotive ISO 26262, any malfunction of the intended functionality of an automotive system due to complex operating environment or gaps in the requirement specifications, is out of scope of ISO 26262 (functional safety) and should be covered by the standard ISO/PAS 21448 (SOTIF) [19]. It is discussed in more details below.

3.3 Automotive safety standards and regulations for vehicle type-approval

3.3.1 ISO 26262, ISO/PAS 21448 (SOTIF) and UL 4600

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 [13]. It is an adaptation of the IEC 61508 (1-7): 2010 [12] 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 life-cycle 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 [19] 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.

The system safety according to IEC 61508 or EN 50129/ EN 50126/ EN 50716 is based on the fact that the behaviour of the system in the event of a failure is predictable. However, this is not the case for ML algorithms, which are considered a black box, because by the nature of ML (Machine Learning) it is not easy to know what is going on inside. ML for ADS purposes is still under research and there is no technical solution for which the required (high) safety can be demonstrated.

Safety of the intended functionality (SOTIF) is the implementation of safety measures to prevent or mitigate hazardous events at the vehicle level caused by functional insufficiencies, insufficiencies in requirements specifications, unexpected operating conditions within the operational design domain (ODD) and incorrect

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

user behaviour. According to ISO/PAS 21448, four basic operational scenarios of are considered [19] – see Figure Review of applicable safety standards and related regulations-5:

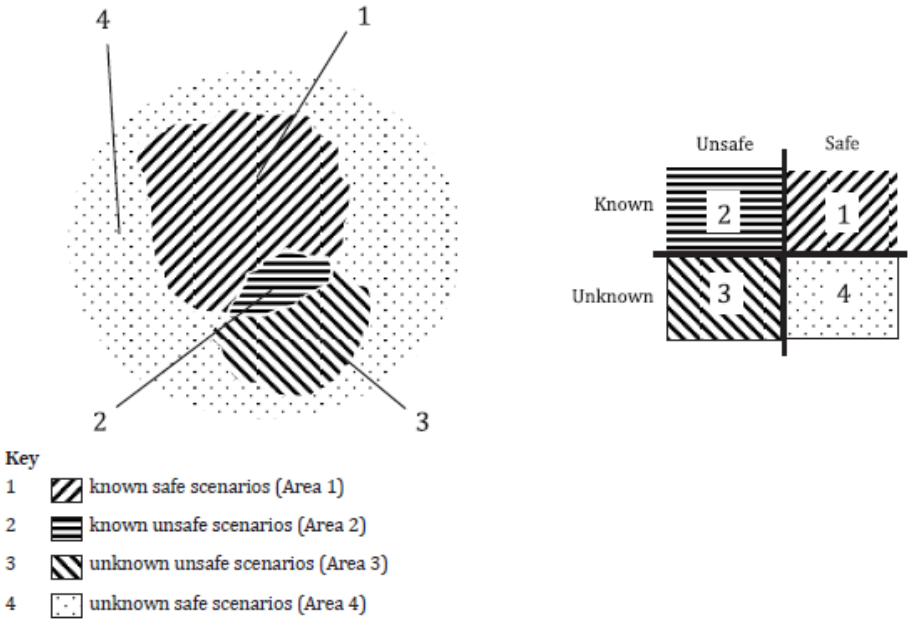

Figure Review of applicable safety standards and related regulations-5: Visualisation of the known/unknown and safe/unsafe scenario categories [19].

The goals of the SOTIF process with respect to Area 1, Area 2, and Area 3 and relevant scenarios are:

- Area 1: Maximize or maintain area, while minimizing Areas 2 & 3. This retains or improves safe functionality.
- Area 2: Minimize area with technical measures to an acceptably small level, with statistical significance of that level appropriate to the relative impact of the technical measure; evaluate the potential risk and, if necessary, move hazardous scenarios into Area 1 by improving the function or by restricting the use/performance of the function.
- Area 3: Minimize area (the risk of the unknown) as much as possible with an acceptable level of effort (every detected hazardous scenario is moved into Area 2).

SOTIF is mainly aimed at reducing risks in cases referred to as unknown/unsafe (Area 3). Unknown means a hardly anticipated operational situation and unsafe means the presence of hazards in the system due to limitations of the intended functionality under fault-free conditions.

ISO 26262 is intended to eliminate random and systematic failures. SOTIF is a complement to ISO 26262. The main difference is that SOTIF is focused on the intended functionality. A much bigger emphasis is on testing, verification, and validation and also increased statistical analysis when it comes to running virtual simulations - especially, when the unknown/unsafe cases shall be reduced. On the other hand, it is clear that for complex systems, even extensive testing and simulation for validation purposes will not help ensure 100% safety. The use of appropriate complementary analytical methods for hazard identification and risk analysis is required.

ISO 26262 and ISO/PAS 21448 (SOTIF) prescribe how to design, verify and validate (V&V) a safety system. Important part of safety demonstration is safety case development and its assessment by an independent third party. More detailed information on V&V and safety case development can be found in the US national

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

standard UL 4600 (Evaluation of Autonomous Products) [20], which prescribes in particular what the safety case for autonomous products should focus on and how the safety case should be assessed. UL 4600 is based on previous automotive standards ISO 26262 and ISO/PAS 21448 and is intended for autonomous driving with SAE Levels from 3 to 5. UL 4600 does not prescribe which technologies or architectures should be used (although it considers the use of ML to be very promising), but on the other hand it does require that the safety case must convincingly argue for the safety claims of the ADS, especially based on analysis, simulation, laboratory testing, and testing on public roads.

3.3.2 ISO/TR 4804

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, a technical report ISO/TR 4804 (Road vehicles - Safety and cybersecurity for automated driving systems - Design, verification and validation) was developed [21] . 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. It considers safety and cyber security by design, as well as verification and validation methods for ADS with SAE Levels 3-4 (levels of car automation).

3.3.3 Regulations for certification of self-driving cars

3.3.3.1 Need for certification of self-driving cars

Safety certification and authorization process for road vehicles in Europe is historically based on a so called Type-approval process [64]-[66]. The National Safety Authority in a given EU Member State usually entrusts the national Technically Services to perform tests and other verification and validation of a vehicle prototype. After the tests have been successfully completed, the National Safety Authority issues the vehicle type-approval certificate to the vehicle manufacturer. On this basis the vehicle manufacturer issues the Certificate of Conformity (birth-certificate) [67] which must accompany each manufactured vehicle.

In recent years the development and type-approval process for automated vehicles is getting more complicated when Automatically Commanded Steering Functions (ACSF) are being introduced into operations [68]. Higher categories ACSF systems (*B2 - Hands-off lane guidance systems and E - Lane change system without driver input*) will require among others much higher safety levels for car position determination, as it is also common in aviation or railway sectors. For example, on railway, the compliance with Safety Integrity Level (SIL) 4 with THR < 1e-9/h is required for train position determination function. Furthermore, a clear certification and safety approval process for these high safety levels should be specified. Otherwise, it would be impossible to use cars with ACSF due to lack of trust from the passenger side.

To solve the above tasks, numerous activities have been performed within the UN ECE expert groups (United Nations Economic Commission for Europe) and other working parties. However, usable conclusions and recommendations on ACSF certification are still missing, although examples for such a process have also been searched in sectors with traditionally very high safety target levels like aviation, nuclear energy and railway – see [69] and [70]-[78].

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

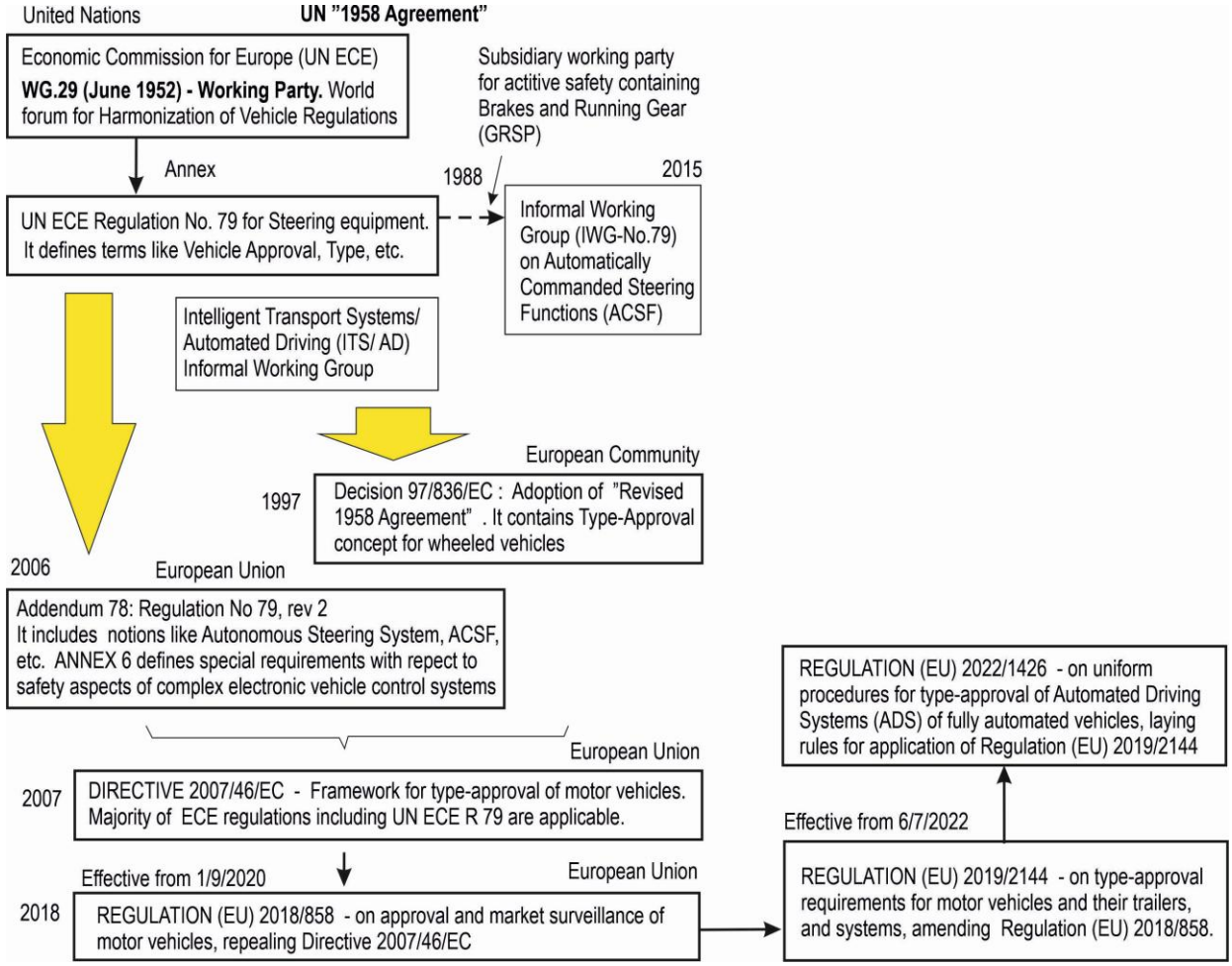

Figure Review of applicable safety standards and related regulations-6: Chronology of regulations towards type-approval process of cars with automated driving in Europe.

3.3.3.2 Shorter vehicle lifecycle on road-side digital infrastructure

Demonstration of compliance with regulations and standards for a large civil aircraft can take more than 5 years. Duration of safety authorization in case of complex railway signalling such as ERTMS is similar to the process duration for airplane. The situation in the automotive industry is different, because the conformity assessment process usually takes less than 1 year [69]. It is not expected it will take longer for cars with automated driving functions satisfying higher safety levels than existing car assistants. It is because the current trend is towards reducing the life cycle of cars to about 3 years. Furthermore, these cars will be much more dependent on a way-side communications-based infrastructure. It will be necessary not only to demonstrate the required safety of automated car, but all significant changes in future road automated transport systems must be safely managed as well – including road-side infrastructure for connected cars.

The absence of a widely acceptable methodology for management of relatively frequent safety-related changes in vehicles with implemented ACSF currently represents a significant gap in terms of safety for automated vehicles world-wide. Future SDC operating companies and road infrastructure managers will not simply be able without a suitable Risk Management Process to safely control system changes and enable to guarantee a high safety level which is e.g. common in aviation or on railway. The absence of such a clearly

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

defined process also has a negative impact in society. Every accident of not properly approved automated car due to technical failures contributes to the mistrust towards this new technology in society. Nevertheless, railway stakeholders know how to safely manage changes on European railways. That's why it is proposed to utilise this railway experience as an example and motivation for setting up the risk management process for SDCs.

3.3.3.3 Type-approval framework for cars in EU

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 of May 2018 [67], 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.

The above EU regulation has been formulated in accordance with the 1958 United Nations Economic Commission for Europe (UN ECE) agreement [64] and additional subsequent regulations as it is outlined in Figure Review of applicable safety standards and related regulations-6. The World Forum for Harmonization of Vehicle Regulations is a working party (WP.29) of the UN ECE. It is tasked with creating a uniform system of regulations, called UN Regulations, for vehicle design to facilitate international trade. WP.29 was established in June 1952 as the "Working Party of experts on technical requirement of vehicles", while its current name was adopted in year 2000. The forum works on regulations covering vehicle safety, environmental protection, energy efficiency and theft-resistance.

The approval of vehicles with regard to steering equipment is included in UN ECE regulation No. 79 [65] that is effective from 1988. This regulation is annexed to the UN 1958 agreement regarding adoption of technical prescriptions on equipment of wheel vehicles and mutual recognition of the approval.

However, the Regulation No. 79 did not cover primary steering transmissions purely based on electric means. In 1997 European Community adopted a so called Revised 1958 Agreement (97/836/EC) [66] concerning the adoption of uniform technical prescriptions for wheeled vehicles including mutual recognition of approvals (type-approvals).

In 2005 Annex 6 to the UN ECE Regulation No. 79 concerting special requirements to be applied to the safety aspects of complex electronic vehicle control systems was adopted. It very generally defines the design methodology for a vehicle safety system and requirements for documentation that shall be applied and also disclosed for the type-approval purposes containing verification and tests. The Annex 6 introduces Corrective Steering functions (CSF) and Automatically Commanded Steering Function (ACSF).

In 2007 the EU directive 2007/46/EC [79] establishing a harmonised framework for the approval of vehicles in EU Member States was adopted. No technical requirements are contained in the directive. However, it is stated in the Appendix IV, that the majority of ECE Regulations, including Regulation No. 79 are applicable. Regulation (EU) 2018/858 [38] on approval and market surveillance of motor vehicles repeals the Directive

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

2007/46/EC. Subsequently, Regulation (EU) 2018/858 was extended by Regulation (EU) 2019/2144 of 27 November 2019 on type-approval requirements for motor vehicles, which also includes requirements for automated and fully automated vehicles.

Finally in 2022, Regulation (EU) 2022/1426 laying down rules for the application of Regulation (EU) 2019/2144 [80] as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles was published [81] – see Figure Review of applicable safety standards and related regulations-6. This regulation is one of the key pieces of legislation which will eventually permit the European type-approval of fully automated vehicles. Annex III specifies a number of physical tests that the automated vehicle must be subjected to. These tests shall confirm the minimum performance requirements described in Annex II and the functionality of the ADS and the safety concept of the manufacturer.

Demonstrating the functional safety of ADS, according to automotive standards ISO 26262 [13], ISO/PAS 21448 (SOTIF) [19] and ISO/TR 4804 (Safety and cybersecurity for ADS – Design, verification and validation) [21], mostly depends on a series of simulations and field tests (as well as analytical work) that are part of the validation procedures. Simulation primarily serves two purposes: to assist the development of a (robust) function and to test and validate the function before release. Simulation introduces models to represent the behaviour of the system of interest, for example. Models are abstractions from the physical reality and rely almost on simplifications of the true complexity in the real world. Simulations can be accurate only to some degree. Understanding the accuracy offered by a simulation is key to determining and arguing its use during development and validation activities.

If the human driver is to be replaced by an ADS, then the ADS must cope with millions and millions of different operational situations due to the complex operating environment. Functional safety associated with all these operational scenarios cannot be naturally tested and validated during dedicated field tests. That would not be practically feasible. Instead, advanced simulators are used to validate and certify various ADS functions in different operational scenarios, including the so-called edge cases (rare dangerous events) that ADS must also handle. Simulation techniques and procedures used in the automotive industry for ADS development and validation can serve a source of inspiration for the GNSS error modelling and simulation within the VICE4RAIL project [21]. In the following work packages, a research will be carried out to see whether some of the simulation techniques for ADS purposes could also be used for simulation within the framework of the ASTP validation for ERTMS. This is despite the fact that the ERTMS simulator operated by CEDEX is already used within the framework of the VICE4RAIL project.

3.4 Maritime standards and regulations

To give an overview on normative requirements regarding safety applications in the maritime sector, this section presents the existing procedures for maritime equipment as it is given by the International Maritime Organization (IMO) regulations, EU regulations or standardization organization.

3.4.1 IMO conventions, regulations and resolutions

The IMO is the United Nations (UN) specialized agency. Its primary purpose is to develop and maintain a comprehensive framework of regulations for shipping and its responsibilities today includes maritime safety, environmental concerns, and legal matters, among other issues. The IMO work is carried out in specialised committees and one of which is the Maritime Safety Committee (MSC). The MSC includes different sub-

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

committee and also Sub-Committee on Navigation, Communications and Search and Rescue (NCSR). Matters relating to the use of GNSS at sea fall within the competence of the NCSR.

The work of the IMO has resulted in different treaty instruments and conventions and hundreds of other measures such as guidelines and codes of practice. Four main UN IMO conventions are recognised as the pillars of the international regulatory regime for shipping, the so called "four pillars of international maritime law", which are

- SOLAS (International Convention for the Safety of Life at Sea)
- MARPOL (International Convention for the Prevention of Pollution from Ships) and
- STCW (Standards of Training, Certification and Watchkeeping for Seafarers) at that time was
- MLC 2006 (Maritime Labour Convention).

The SOLAS convention regulates the equipment of maritime ships including their installation and use. The regulations within SOLAS are classified into 14 Chapters. For example, Chapter V of SOLAS contains regulations relating to Safety of navigation. A revised SOLAS Chapter V (Safety of Navigation), which entered into force in 2002, requires ships to carry a GNSS or terrestrial radionavigation receiver, to establish and update the ship's position by automatic means, for use at all times throughout the voyage.

From the perspective of using GNSS for safety applications at sea, IMO resolutions are also relevant [58]. These are in particular resolutions voted by the IMO Assembly (A), which is the highest Governing Body of the Organization. For example, in section 5 of this document, we have used IMO resolutions A.860 (20) [9], A.915(22) [11] , A.1046(27) [38] to analyse the relevance of GNSS continuity in land transport.

3.4.2 Marine Equipment Directive 2014/90(EU)

The enforcement of the international SOLAS convention is carried out in Europe by the Marine Equipment Directive (MED) 2014/90/EU [59], 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. However, MED does not provide information on which test methods or criteria are required for validation and verification (V&V) [59], [60].

3.4.3 ISO 17894 - Ships and marine functional safety standard

In the maritime sector, there is a standard for the development and use of shipboard electronic systems (HW and SW) based on functional safety. This is the ISO 17894:2005 [61] 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 [12]. 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 by the absence of unacceptable risk; Principle 13 states that the required level of PES safety must be

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

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 fulfil 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 [61]. 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 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).

In ISO 17894, dependability is also explicitly defined as – "*the extent to which a system can be relied upon to perform exclusively and correctly a task under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided"* [61]. However, this definition does not explicitly state what attributes the marine concept of dependability includes. Therefore, the analysis of the dependability concept was performed in the paragraph above. This analysis shows that dependability for marine applications corresponds to dependability for ADS in automotive transport (RAMSS). On the other side, the dependability attribute used in railways, which does not include safety (only RAM) is different from marine and automotive concepts. A detailed comparative analysis of dependability concepts is developed in section 4.

Efficient V&V methods are indispensable for both independent safety assessment and certification of interoperable systems. The maritime standard ISO 17894 has been published 20 years ago and is regularly revised - most recently in 2024. It mainly describes general principles and techniques for V&V, which doesn't sufficiently reflect rapid development of safety applications in land transport, such as in the field of automated car driving systems (ADS). Therefore, experts specialised in testing maritime assistance systems up to autonomous vessels are looking for inspiration regarding modern V&V methods also in standards and guidelines developed for automotive ADS purposes [60]. Similarly, the VICE4RAIL project is looking for inspiration regarding modern V&V methods in standards and regulations for self-driving cars that could be used for HyVICE certification.

3.5 RTCM SC-104 and SC-134

RTCM (Radio Technical Commission for Maritime Services) is the worldwide leading standard for GNSS High Accuracy System and Services.

RTCM is organised in Special Committees.

RTCM SC 104 "Differential GNSS (Global Navigation Satellite Systems) Services" deals with the definition of Protocol and Data formats, to be exchanged between an Augmentation System Provider and a user receiver for High Accuracy systems developments.

Started in the 90's, it is currently implemented in any GNSS receiver needing high accuracy. Messages are grouped by:

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

- OSR (Observation State Representation), covering augmentation methods based on the processing of satellite code and phase measurements, e.g. DGNSS, RTK/NRTK, VRS
- SSR (State Space Representation), covering augmentation methods based on single SIS error estimations (e.g. satellite orbits, clock, ionospheric errors, tropospheric errors) including PPP (Precise Point Positioning) and PPP-RTK.

The standard includes the definition of a protocol, based on htpp1.1., named NTRIP, "RTCM 10410.1 Standard for Networked Transport of RTCM via Internet Protocol (Ntrip)" and details the establishment of the connection between the user receiver, equipped with a mobile communication system, and an Augmentation System.

The standard is used in any kind of application, from Land Surveying, to Automotive and Maritime and is encapsulated in sectional standards (e.g. SAE J2735 – Data and message set dictionary).

Due to the need for High Integrity Services (e.g. for autonomous transport applications), in 2018 RTCM founded the RTCM SC 134 Committee, named "Integrity for GNSS-based High Accuracy Applications). The objective is to define a multimodal and multiservice standard for the delivery of High Integrity Augmentation services.

The following Working Groups (WGs) are in place:

- Working Group 1: Automotive
- Working Group 2: Rail
- Working Group 3: Maritime and other applications
- Working Group 4: Harmonization of Requirements and Metrics
- Working Group 5, dealing with Open Satellite Correction services

Working Groups 1, 2, and 3 are responsible for assessing the requirements for specific classes of applications: automotive, rail, and maritime, respectively. Working Group 4 aims to harmonize the requirements and parameters among different application sectors. Working Group 5 is a newer addition focused on publicly provided satellite high-accuracy augmentation services such as the European Galileo High Accuracy Service (HAS). In addition, ad-hoc Task Forces are set up as needed and currently include the Message Development Task Force, NRTK Task Force, and the Transition Mode Task Force.

The RTCM SC 134 Committee Chairman and the Chairman of the RTCM SC 134 WG 2 Rail are members of the VICE4Rail project.

The standard is agnostic with respect to the applied augmentation system. Overbounding parameters and time correlation parameters are transmitted to the rover for allowing the determination of the Protection Level.

A Safety Analysis has been conducted by the SC 134 Committee to define sectorial requirements and harmonise the Data Field contents.

The plan for the RTCM SC 134 standard release is end of 2025.

Several liaisons are in place with other standardisation organisations: SAE, NMEA, ETSI 3GPP, ISO/TC204, RINEX.

The standard is used in VICE4Rail for the Augmentation Service implementation.

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

4. CLARIFICATION OF DEPENDABILITY AND RAMS TERMINOLOGY

When considering safety assessment and certification of systems, it is essential to use the correct terminology/metrics. In individual transport sectors, the terminology used has become established and its meaning is clear. However, the terminology problem arises when considering safety applications of GNSS in multimodal transport, where the same terms can have different meanings in different sectors. An example of this inconsistency is the term dependability often used in railway signalling and the same term used for the automated driving system (ADS). Or it may be the case that a given term is used in one transport sector, e.g. GNSS continuity in aviation, and in another sector, such as rail, the term does not exist. And this could cause confusion and errors in demonstrating safety.

The European rail industry has been seeking to use GNSS safety services in signalling technology for more than 30 years. This long development shows that this is not an easy task, as it must firstly comply with the railway RAMS (Reliability, Availability, Maintainability, Safety) requirements according to EN 50126 and secondly technical interoperability in the sense of the CCS TSI must be ensured. In recent years, a rapidly developing area for the use of GNSS safety services in land transportation is automated driving systems (ADS) for autonomous vehicles, where ADS solutions must meet the automotive dependability requirements defined in the ISO/TR 4804 standard [21]. Here, dependability for ADS is abbreviated with the acronym RAMSS (Reliability, Availability, Maintainability, Safety, Security).

Dependability is a notion that has undergone a complex historical development and has a variety of interpretations. As mentioned above, it is used in different application areas including rail, aviation and now in the latest automotive ADS.

The aim is to explain the inconsistencies caused by the introduction of new definitions related to dependability in recent years. This is the focus of the following paragraphs. The term dependability is explained below in this chapter, while the term GNSS continuity is discussed in section 5.

4.1 Classical definition of dependability and RAMS

For many years the railways have traditionally used the notion of dependability, which is a collective term describing availability and its influencing factors such as reliability and maintainability (RAM) [50], [51].

Note: a more generic definition of dependability according CEI IEC 300-3-4:1996 [50] also inherently includes maintenance-supported performance. Therefore, the acronym RAMS is often used to specify dependability and safety, i.e. (RAM + S) = RAMS. Safety is considered here as complete safety - i.e. safety that is ensured by technical measures (i.e., control of hazards due to failures of the technical system), operational measures, as well as conditions for operation and maintenance.

4.2 Dependability according to prEN 50126:1995

The acronym RAMS first appeared in the disapproved draft railway standard prEN50126 [52] from 1995, entitled Railway applications: Specification and demonstration of Dependability - Reliability, Availability, Maintainability and Safety (RAMS). Note: This draft never came into effect. It is already clear from the title of this draft standard that the term dependability at that time included the attributes Reliability, Availability, Maintainability and Safety.

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

On railways, the acronym RAM is currently often used for dependability although the term dependability is practically absent in the current edition of EN50126:2017 [15], [16].

4.3 Generic definition of dependability (IEC 60300-1:2014)

Further confusion in relation to railway RAMS has been raised by the current definition of dependability according to the IEC 60300-1:2014 [53] standard, which includes availability, reliability, recoverability, maintainability, and maintenance support performance, and, in some cases, other characteristics such as durability, safety and security. This means that, as in the 1995 draft railway standard prEN50126, the currently valid generic definition of dependability (IEC 60300-1:2014) includes the attribute of safety.

4.4 Discrepancy between generic definition of dependability and railway RAMS (EN 50126:2017)

The question is whether there is any difference between the railway RAMS (EN 50129:2017) and the generic definition of dependability (IEC 60300-1:2014) [52]. The answer can be based on the generic definition of dependability, which states that it is the ability of an item to be in a state to perform as required. An item can be HW, SW, people or any combination of these. Dependability according to IEC 60300-1:2014 is a term used to describe the time-dependent characteristics (aspects) associated with the performance of an item. It is related to faults and failures within the life cycle of a technical system.

It is clear from the above that the concept of generic definition of dependability does not correspond to railway RAMS. This is because dependability includes only the part of safety that is affected by the occurrence of technical system failures. Dependability in the sense of IEC 60300-1 does not include safety that is ensured by operational and organisational measures, i.e. non-technical measures as specified in EN 50126 (RAMS):2017 [15], [16]. On railways, therefore, RAMS = RAM + S = Dependability and Safety. For the sake of completeness, it can be noted that railway cyber security is addressed in EN50129 and is part of safety.

4.5 Automotive dependability (ISO/TR 4804:2020)

Further confusion in the relation between dependability and RAMS that needed to be clarified with respect to GNSS safety applications in multimodal transport emerged in 2020 with the introduction of the automotive standard ISO/TR 4804 [21] entitled Road vehicles - Safety and cybersecurity for automated driving systems - Design, verification and validation.

Therefore, this paragraph will first introduce the purpose of this standard and then explain the relationship between railway RAMS and automotive RAMSS - with regard to the possible use of a single GNSS augmentation especially for both railway and road transport.

ISO/TR 4804 focuses on the systematic development of dependability to support safety by design. Dependability in the sense of this standard is defined as ability of a system to provide a service or function regarding the attributes of reliability, availability, maintainability, safety, and security (RAMSS). Dependability defined in this way for ADS purposes is based on two pillars, which are (i) Safety by design and (ii) Verification and validation.

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

The first pillar introduces the three domains for automated driving: safety of the intended functionality (ISO/PAS 21448 [19]), functional safety (ISO 26262:2018 [13]) and automotive cybersecurity (ISO/SAE 21434 [54]). The second pillar discusses the quantity of testing and simulation.

To clarify the relationship between automotive dependability defined in this way and automotive RAMSS, we are interested in whether automotive dependability defined in the sense of ISO/TR 4804 includes complete safety or only part of it, as was the case in the generic dependability definition (IEC 60300-1: 2014). The answer can be found in ISO/TR 4804 [21] in section 4.4.3, Principles of safety and cybersecurity for automated driving, because the safety of automated driving depends on the safety principles used.

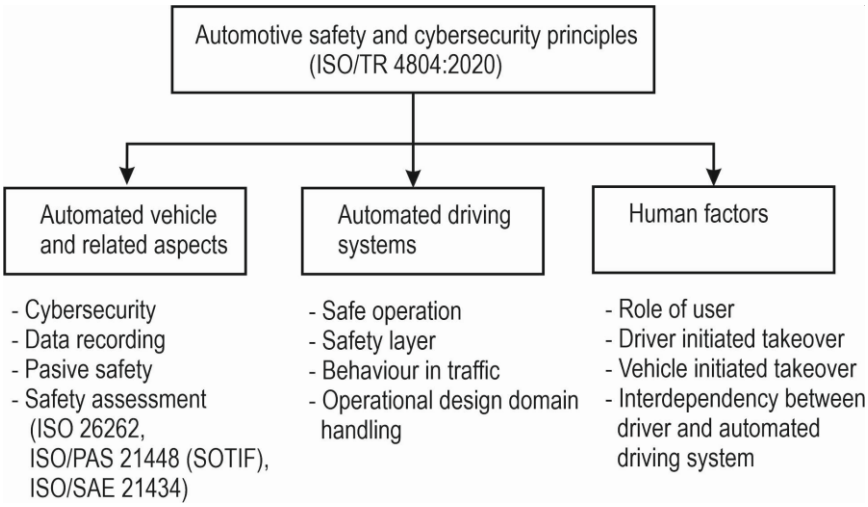

Figure Clarification of dependability and RAMS terminology-7: Safety and security principles used for automated car driving.

Safety principles can be divided into three main groups: 1) Automated vehicle and related aspects, 2) Automated driving system, and 3) Human factors. In Figure Clarification of dependability and RAMS terminology-7 an overview of each safety principle is then given in each group.

For example, safety assessment in Figure Clarification of dependability and RAMS terminology-7 includes verification and validation to ensure that the safety requirements (ISO 26262 and ISO/PAS 21448) and security requirements (ISO/SAE 21434) are met. Further, e.g. safe operation is dealing with degradation of driving function and application of two main capabilities - fail-safe behaviour (safe state defined) or fail-operational behaviour (emergency operation with SaRA requirements defined). And finally, the human factor includes the role of user under operational conditions. It can be concluded that the above safety principles will ensure full safety and cybersecurity for ADS. Then one can write that (automotive) dependability = RAMSS.

4.6 Commonalities between railway RAMS and automotive RAMSS

It was the release of the automotive standard ISO/TR 4804 [21] in 2020 that caused confusion between the long-used railway terms dependability and RAMS. To use these quality metrics correctly for GNSS applications in multimodal transport, it was first necessary to clarify discrepancies.

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

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 used in automotive industry corresponds to RAMSS (ISO/TR 4804:2020), but railway RAMS (EN 50126:2017) doesn't correspond to the generic definition of dependability (IEC 60300-1: 2014), because safety included in generic dependability doesn't contain safety that is ensured by operational and organisational measures, i.e. non-technical measures. These facts can be written as follows:

- Railway RAMS (EN 50126:2017[15], [16]) ≠ dependability (IEC 60300-1: 2014 [53])
- Railway RAMS = dependability (IEC 300-3-4:1996 [50], IEC 60300-1: 2014 [53]) + (full) safety
- Automotive RAMSS = automotive dependability (ISO/TR 4804:2020 [21])

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 application 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 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. This is because SaRA represents a requirement for the availability of some ADS functions that must be completed with a high probability for safety reasons. The basis for availability, and therefore also for SaRA, is reliability. And GNSS reliability, as will be shown in detail below, can be expressed in terms of GNSS continuity. Since SaRA is an important ADS safety requirement that significantly depends on GNSS continuity, it is described in the next section. Safety-related availability for automotive safety-critical systems

This section discusses a safety notion referred to as Safety-Related Availability (SaRA), which according to ISO 26262-10 is used for automotive safety-critical systems/functions with fail-operational behaviour - i.e. in operational situations where the loss of performance of a required ADS function could have fatal consequences for vehicle safety. The aim is to show that GNSS continuity, which is one of the two main safety measures in aviation, can also be effectively used for safety in road transport.

As mentioned in section 2.2.1, many functionalities in automated car driving systems (ADS) 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 show 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 so called the SaRA requirements must be defined for the functionality according to ISO 26262-10 [13].

The need for SaRA requirements is determined based on Hazard Analysis and Risk Assessment (HARA) [13]. A SaRA requirement is initially derived for a system because HARA is generally performed on system level – see [48]. The operational state of the vehicle determines whether the vehicle's functionality (or system) is considered as safety-critical (see sections 2.1 and 2.3.3). The vehicle operation state is defined as by the combination of the operational mode and the operational situation. If loss of the vehicle function do not 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

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

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 the 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 Safety-related availability for automotive safety-critical systems-8, which shows the safety-relevant time intervals associated with emergency operation.

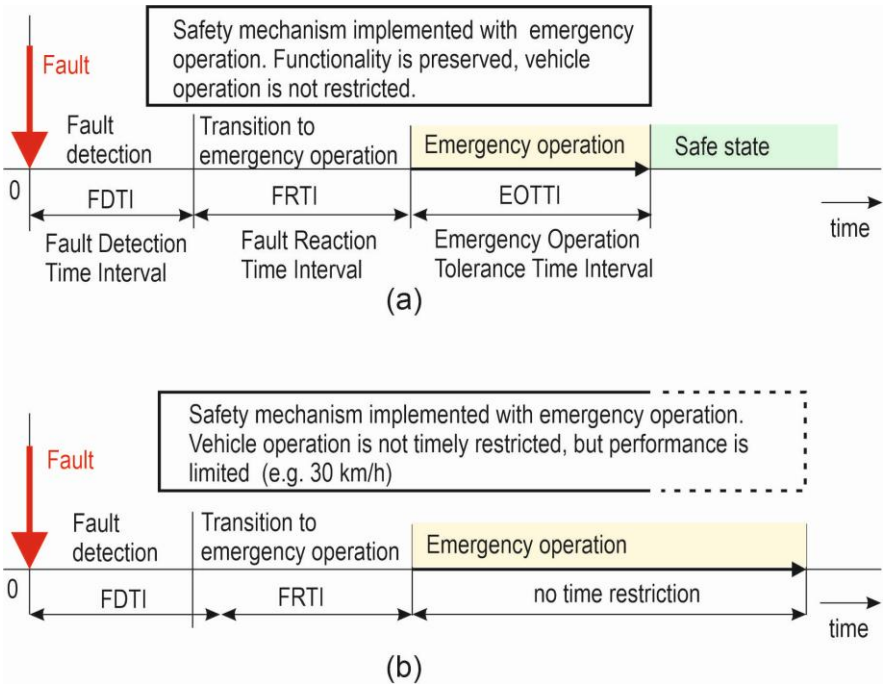

Figure Safety-related availability for automotive safety-critical systems-8: Safety-relevant time intervals for fail-operational systems with emergency operation: (a) with time restriction and without limitation of vehicle operation, (b) without time restriction and with limitation of vehicle operation.

Figure Safety-related availability for automotive safety-critical systems-8(a) 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.

For completeness, Figure Safety-related availability for automotive safety-critical systems-8(b) shows a strategy where a safety mechanism is also implemented in case of a fault, but an emergency

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

operation with unlimited duration is used. Vehicle operation is restricted, e.g. for a maximum speed of 30 km/h. When a fault is detected, the system switches to emergency operation - e.g. switches to a backup channel.

4.7 Elements of the SaRA requirement

The SaRA requirement for the system according to Figure Safety-related availability for automotive safety-critical systems-8(a) 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) [13], 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). The question may arise as to when to use unavailability U(t) and when to use unreliability F(t) for specifying SaRA requirements. This is explained in the section below.

4.8 Unavailability U(t) vs. unreliability F(t)

According to IEC 61508 [12], when the E/E/PE (Electrical/Electronic/Programmable Electronic) safety-related system is the ultimate safety layer, the average frequency of dangerous failure per hour (PFH) should be calculated from its *unreliability* F(t) = 1-R(t). When it is not the ultimate safety-related system (it is e.g. intermediate layer) its PFH should be calculated from its *unavailability* U(t). PFH approximations are given by F(T)/T and 1/MTTF in the first case and 1/MTBF in the second case. Reliability R(t) represents the probability of a failure occurring within a defined time interval. Availability A(t) represents the probability of a failure occurring within a certain time. If a safety function is not available within the required time, the system will not perform as required.

4.9 Example: strategies for specification of SaRA requirements

In this section, two safety strategies are considered to specify SaRA requirements. For this purpose, as an example, a redundant safety system with 1oo2 (one-out-of-two) architecture is used – see Figure Safety-related availability for automotive safety-critical systems-9. The 1oo2 system is composed of two sufficiently independent channels A and B. Channel A is working, performing a nominal function. Channel B is the backup channel. If channel A fails in such a way as to cause loss of system functionality, channel B is activated to prevent violation of the safety goal. Each of the A and B channels shall meet the systematic failure requirements for the required ASIL (e.g. ASIL D). Combining the probability of failure for channels A and B will meet the quantitative requirements for the ASIL (e.g. ASIL D) as far as random failures are concerned.

4.9.1 Repair within Emergency Operation Tolerance Time Interval (EOTTI)

This strategy corresponds to the situation depicted in Figure Safety-related availability for automotive safety-critical systems-8(a). Backup channel B alone will not meet the safety requirements for random HW faults regarding the required ASIL (e.g. ASIL D). When the loss of channel A is detected, the driver is alerted and prompted to repair the system within EOTTI. The probability of a channel B fault occurring during EOTTI is considered as part of the PMHF calculation.

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

4.9.2 Limited operation without time restrictions

This strategy corresponds to the situation depicted in Figure Safety-related availability for automotive safety-critical systems-8(b). Channel B alone will not meet the safety requirements for random HW faults at the required ASIL level (e.g. ASIL D). For example, it can only meet the safety requirements for random HW faults at ASIL A. Therefore, the speed is reduced to level v1 (e.g. 30 km/h) and this speed reduction function is an additional requirement for this system with e.g. ASIL D.

4.10 Example: Markov modelling of steady-state unavailability in 1oo2 architecture

In this section, the calculation of the system unavailability as one of the components of the SaRA requirement is shown using Markov modelling. By means of this technique, the time dependencies of the probabilities of the states in which the system is can be calculated, and using these probabilities, the reliability R(t) or availability A(t) of the system can also be determined. Similarly, the probability of failure of the entire system, called unreliability F(t) = 1 - R(t) or system unavailability U(t) = 1-A(t), which are quantitative measures of

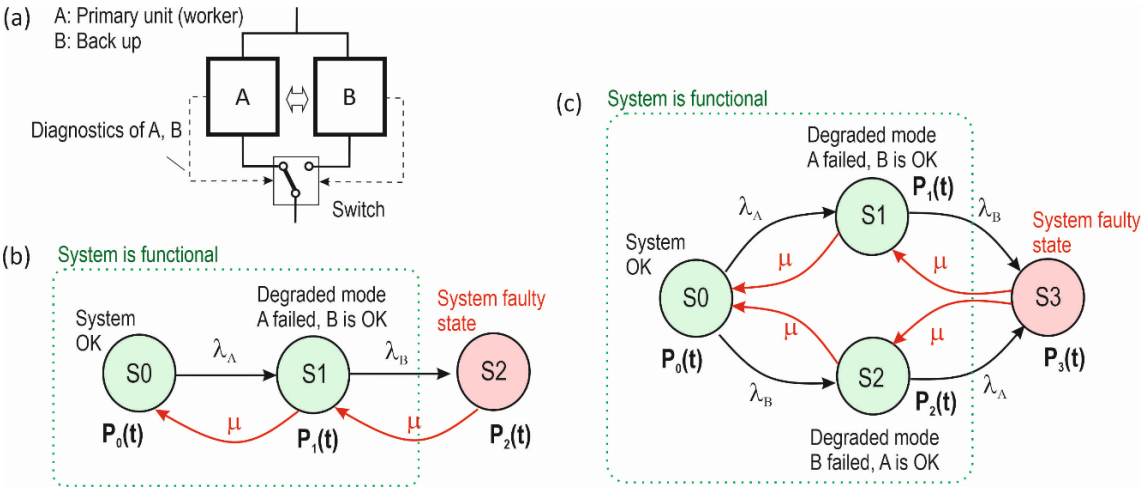

Figure Safety-related availability for automotive safety-critical systems-9: 1oo2 redundant architecture: (a) functional schema, (b) Markov model with primary channel/ unit A and cold standby B, and (c) Markov model with warm standby.

safety integrity for safety-critical systems. The quantities F(t) or U(t) are used according to IEC 61508 to calculate the average frequency of hazardous failure per hour (PFH) or according to the automotive standard ISO 26262-10 to calculate an automotive safety measure referred to as Probabilistic Measure of HW Failures per Hour (PMHF). Both PFH and PMHF are used as measures of safety integrity of safety systems.

An example of a 1oo2 system is shown in Figure Safety-related availability for automotive safety-critical systems-9. The behaviour of the system in terms of functional safety is described in 4.9. In general, this is a system with fail-operational behaviour, where the use of emergency operation (shown in Figure Safety-related availability for automotive safety-critical systems-8) is considered. The first dual point fault (DPF) does not yet cause a dual-point failure of the whole system, because the required functionality is performed by the second channel. A possible first DPF can be revealed by periodic testing.

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

The first safety layer (intermediate, not ultimate) is characterized by the probability of a system failure when a fault occurs simultaneously on channel A and B. The diagnostics tests both channels with a time interval T_{test}. Then the recovery rate $\mu = 1/T_{test}$. The required value of steady-state system unavailability $U(\infty)$ is calculated as the limiting probability of a non-absorbing system faulty state. A non-absorbing state means that the system faulty state is restored/repaired. The absorbing faulty state means that once the system enters it, it cannot be left until the system is properly restored.

The second safety layer (ultimate) is characterized by the probability of a system failure that occurs after the fault of the remaining functional channel. We consider that the remaining channel alone is not able to provide the required safety for an indefinite operating time due to a possible random failure of the remaining functional channel, and therefore the required safety is achieved by introducing emergency operation, i.e., a reduced time of use of the remaining functional channel.

In the case of the ultimate safety layer, the SaRA requirement, which is EOTTI, is calculated using the unreliability F(t). This can be justified by the fact that, for the ultimate layer, no recovery of the system from the absorption failure state is considered anymore. The following is a hazardous event. Whereas in the intermediate safety layer, testing is considered, hence the SaRA requirement is represented by unavailability. When the testing interval of the system equals the lifetime $T_{lifetime}$, then the unavailability U(t) equals the unreliability F(t).

The required steady-state unavailability for the first safety layer of the 1oo2 architecture can be calculated using the Markov models shown in Figure-9(b) and Figure-9(c). The Markov model in Figure-9(b) describes a system with cold standby, whereas the model in Figure-9(c) is for a system with warm standby.

4.10.1 Derivation of steady-state unavailability for the first safety layer of 1oo2 architecture with cold standby

The Markov model for cold standby is in Figure-9(b). The meaning of the system states S0 to S2 is as follows:

- S0 - the system is fully functional, channels A and B are without fault, the required function is performed by the primary channel A;
- S1 - only channel B is functional, the system is in emergency mode; and
- S2 - the system is in a faulty state, both channels have a fault. The transition between states is characterized by the failure rates λ_A and λ_B and the restore/repair rate μ.

The steady state unavailability $U(\infty)$ is calculated using the transition matrix of the system [T] and the system of equations for solving the limiting state probabilities P_0^L , P_1^L and P_2^L (0.1) [49] . Each row and each column of the transition matrix [T] represents one of the system states. In the transition matrix [T] (0.2), row 0 and column 0 represent state 0, while row 1 and column 1 represent state 1. Similarly, for faulty state 2. The numerical input in a given row and column is the probability of transition from the state represented by the row to the state represented by the column. For example, in the matrix [T] (0.2), the expression λ_A in row 0, column 1 represents the probability of transition from state 0 to state 1 during the next unit time interval (e.g., 1 hr). The expression in row 0, column 0 (1- λ_A) represents the probability of transition from state 0 to state 0, i.e. staying in state 0 during the next time interval. The elements in the main diagonal of the transition matrix are most easily obtained by subtracting the failure/repair frequencies leaving the state from 1. Following the above procedure, the other elements of the transition matrix [T] can also be determined.

$$[P_0^L \quad P_1^L \quad P_2^L] = [P_0^L \quad P_1^L \quad P_2^L] \cdot [T] \qquad (0.1)$$

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

$$T = \begin{matrix} \\ 0 \\ 1 \\ 2 \end{matrix} \begin{matrix} \begin{matrix} 0 & 1 & 2 \end{matrix} \\ \begin{bmatrix} 1-\lambda_A & \lambda_A & 0 \\ \mu & 1-(\lambda_B+\mu) & \lambda_B \\ 0 & \mu & 1-\mu \end{bmatrix} \end{matrix} \quad (0.2)$$

$$[P_0^L \quad P_1^L \quad P_2^L] = [P_0^L \quad P_1^L \quad P_2^L] \cdot \begin{bmatrix} 1-\lambda_A & \lambda_A & 0 \\ \mu & 1-(\lambda_B+\mu) & \lambda_B \\ 0 & \mu & 1-\mu \end{bmatrix} \quad (0.3)$$

We multiply the system of equations (0.3) and get 3 equations. However, the equations are linearly dependent. To solve the system of equations (0.3), we replace one of the equations (e.g., the second equation) with an equation formed from the initial conditions for the limiting probabilities of the states, i.e., $1 = P_0^L + P_1^L + P_2^L$. The resulting system of equations is as follows

$$\begin{aligned} P_0^L &= P_0^L \cdot (1 - \lambda_A) + P_1^L \mu + P_2^L \cdot 0 \\ P_2^L &= P_0^L \cdot 0 + P_1^L \cdot \lambda_B + P_2^L \cdot (1-\mu) \\ 1 &= P_0^L + P_1^L + P_2^L \end{aligned} \quad (0.4)$$

By solving the system of equations (0.4) we obtain the limiting probabilities

$$P_0^L = \mu / \left[\mu + \frac{\lambda_A}{\mu}(\lambda_B + \mu) \right] \quad (0.5)$$

$$P_1^L = \lambda_A / \left[\mu + \frac{\lambda_A}{\mu}(\lambda_B + \mu) \right] \quad (0.6)$$

$$P_2^L = 1 - (\mu + \lambda_A) / \left[\mu + \frac{\lambda_A}{\mu}(\lambda_B + \mu) \right] \quad (0.7)$$

The derived expression (0.7) for the limiting probability of system failure P_2^L is equal to the steady-state unavailability of the system U(∞).

4.10.2 Derivation of steady-state unavailability for the first (not ultimate) safety layer of 1oo2 architecture with warm standby

Following the procedure in the previous section, the steady-state availability solution for the Markov model of the system with warm backup can be calculated according to Figure-9(c), where the meaning of the system states S0 to S3 is as follows:

- S0 - the system is fully functional, channels A and B are fault-free;
- S1 - degraded state in case of channel A fault;
- S2 - degraded state in case of channel B fault; and
- S3 - faulty state of the system when both units have a fault.

The system of equations for calculating the limiting probabilities of the system states is as follows:

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

$$[P_0^L \quad P_1^L \quad P_2^L \quad P_3^L] = [P_0^L \quad P_1^L \quad P_2^L \quad P_3^L] \cdot \begin{bmatrix} 1-(\lambda_A+\lambda_B) & \lambda_A & \lambda_B & 0 \\ \mu & 1-(\mu+\lambda_B) & 0 & \lambda_B \\ \mu & 0 & 1-(\mu+\lambda_A) & \lambda_A \\ 0 & \mu & \mu & 1-2\mu \end{bmatrix} \quad (0.8)$$

In this case, deriving an analytical expression to calculate steady-state unavailability would be difficult. Therefore, after multiplying the vectors and matrices in (0.8), we obtain a system of equations of the form A*x = b, which is then solved numerically in Matlab using the notation x = A\b. Here, A is the matrix of coefficients of the system of equations after applying the equation arising from the initial conditions of the form $1 = P_0^L + P_1^L + P_2^L + P_3^L$ (similar to the previous example), the column vector b contains the coefficients on the right-hand side of the system of equations, and x is the column vector of variables being solved. The solution yields the values x(1), x(2), x(3) and x(4), which correspond to the limiting probabilities P_0^L, P_1^L, P_2^L a P_3^L. The steady-state unavailability U(∞) for model in Figure-9(c) corresponds to the variable x(4).

Using the above procedure, the matrix of coefficients A of the system of equations and the column vector b of coefficients on the right-hand side of the system of equations can be derived for the Markov model in Figure-9(c) in the form

$$A = \begin{bmatrix} -(\lambda_A+\lambda_B) & \mu & \mu & 0 \\ \lambda_A & -(\mu+\lambda_B) & 0 & \mu \\ \lambda_B & 0 & -(\mu+\lambda_A) & \mu \\ 1 & 1 & 1 & 1 \end{bmatrix}; \quad b = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad (0.9)$$

The vector of limiting probabilities for each system state is computed numerically using Matlab as described above. It holds that the system steady-state unavailability U(∞) is equal to x(4). The above numerical procedure is suitable for calculating U(∞) for more complex architectures.

4.10.3 Example: calculation of PMHF for Markov model 1oo2 with cold backup

The corresponding Markov model is shown in Figure-9(b). PMHF is the Probabilistic HW Failure Rate per Hour according to ISO 26262 [13] and corresponds to the Automotive Safety Integrity Level (ASIL).

- A maintenance-free system is being considered. The mission duration t_{MT} = 8000 hours. Then the system renewal frequency $\mu = 1/t_{MT}$.
- Channel A (GNSS service continuity) and B failure rates: λ_A = 1.92e-3/h; λ_B = 5e-6/h.
  Note: Failure rate of channel A (λ_A = 1.92e-3/h) represents reliability corresponding to the aviation GNSS continuity risk CR = 8e-6/15 s, i.e. MTBF of 520.83 h, which is derived in section 5.2 .
- The expression (0.7) gives the steady state unavailability U(∞) = 3.619e-2 [-].
- PMHF = $U(\infty)/t_{MT}$ = 3.619e-2/8000 = 4.5244e-6/h.

4.10.4 Example: numerical solution of PMHF for Markov model 1oo2 with warm standby

The corresponding Markov model is shown in Figure-9(c).

- A maintenance-free system is being considered. The mission duration t_{MT} = 8000 hours. Then the system renewal frequency $\mu = 1/t_{MT}$.

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

- Channel A (GNSS continuity of service) and B failure rates: λ_A = 1.92e-3/h; λ_B = 5e-6/h.
- By solving x = A\b with consideration of A and b according to (0.9) we obtain

  x =
  0.058773744592816
  0.902764716945646
  0.002350949783713
  0.036110588677826

- The limiting probability x(4) corresponds to steady-state availability, i.e. U(∞) = 3.611e-2 [-]
- PMHF = U(∞)/t_{MT} = 3.611e-2/8000 = 4.5137e-6/h.

Conclusion: the steady-state unavailability of a 1oo2 system with a cold backup is generally larger than the unavailability of the system with a warm backup, because the cold backup (B) is only used after the main channel (A) fails, whereas in the case of warm backup, in the event of a random failure of channel A or B, the other channel can operate practically immediately. However, in the above examples is $\lambda_A << \lambda_B$, and therefore the calculated unavailability for cold and warm backup are approximately equal.

4.10.5 Confirming the correctness of the steady-state unavailability calculation U(∞) using the unreliability F(t)

In this section, calculations of U(∞) performed in the sections 4.10.3 and 4.10.4 are verified using the same input data. The unreliability F(t) of a parallel system 1oo2 consisting of independent channels A and B can be calculated as

$$F(t) = F_A(t) * F_B(t) = \left(1 - e^{-\lambda_A * t}\right) * \left(1 - e^{-\lambda_B * t}\right) \quad (0.10)$$

When t = t_{MT}, then the steady-state unavailability U(∞) is equal to the unreliability F(t_{MT}). In general, the U(t) is not greater than the F(t). This can be proved numerically as follows:

- A maintenance-free system is being considered. The mission duration t_{MT} = 8000 hours.
- Channel A (GNSS continuity of service) and B failure rates: λ_A = 1.92e-3/h; λ_B = 5e-6/h
- Then expression (0.10) gives F(t_{MT}) = 3.921055e-02 and PMHF = F(t_{MT})/t_{MT} = 4.90131e-06/h.
- It is evident that F(t_{MT}) = 3.921055e-02 calculated according to (0.10) is greater than U(∞) = 3.619e-2 calculated according to (0.7), which is correct.

4.10.6 Derivation of the SaRA requirement for the ultimate safety layer

This section focuses on deriving the SaRa requirement for the ultimate layer of a safety-critical system. As mentioned above, safety in these systems is achieved using a technique called fault-tolerance, which is based on redundancy.

As soon as the system completes its response to the first fault, the system is in operational mode without redundancy. If the ASIL of the system with such operating mode does not meet the ASIL derived from the vehicle operating state, the amount of time allowable to stay in this vehicle operating state must be limited to reduce the risk of a second fault. In other words, this SaRA requirement is related to the calculation of the maximum allowed emergency mode time, called the Emergency Operation Tolerance Time Interval (EOTTI),

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

for which the system's ultimate layer must operate correctly (without degrading vehicle performance - e.g. speed reduction) in order to meet safety objectives.

To derive EOTTI, we use the assumption that the target probability of system failure during the actual vehicle usage time must equal the actual (i.e. degraded) probability of system failure (e.g. back up channel B) during emergency operation. Let the actual vehicle usage time be equal to the $T_{lifetime}$. Further, let:

- λ_{target} is the target PMHF (derived in accordance with ISO 26262-5:2018, 9.4.2.2) corresponding to the ASIL rating of the system.
- λ_{degr} for the system state after the occurrence of the fault or loss of redundancy, corresponding to the average probability per hour over the Emergency Operation Tolerance Time Interval (EOTTI) of a failure that results in a violation of the safety goal.

Then

$$EOTTI \leq T_{lifetime} \times \lambda_{target} / \lambda_{degr} \quad (0.11)$$

and

$$EOTTI \leq T_{lifetime} \times PMHF / \lambda_{degr}$$

The specific formula for EOTTI calculation depends on the system architecture and detailed design.

5. SIGNIFICANCE OF GNSS CONTINUITY AND RELIABILITY IN MULTIMODAL TRANSPORT

5.1 Introduction to GNSS continuity

Over the last two decades, civil aviation has demonstrated through numerous examples that the GNSS Safety-of-Life SoL (SoL) service is an efficient means to manage air safety operations, including the most demanding ones such as precision approach and landing. This has undoubtedly become a good example and motivation for the use of GNSS SoL service also in land transport - e.g. within the European Railway Traffic Management System (ERTMS) for safe train positioning [28], in maritime or river transport for navigation of vessels [29] or more recently on roads for automated driving of cars [30]. As the GNSS SoL service was originally developed for aviation, the requirements for the GNSS Signal-in-Space (SIS) provided by the GNSS SoL service were specified in terms of quality attributes used in aviation.

In the 1990s, the International Civil Aviation Organization (ICAO) defined the so-called Required Navigation Performance (RNP) concept [31], which includes aircraft positioning system requirements for in-flight operations (e.g. departure, en-route and approach) including the most critical operations, which are Category I, II and III precision approaches and landings [23], [27]. Within the RNP, ICAO has proposed to specify the requirements for the entire navigation system using the main quality attributes: accuracy, integrity, continuity, and availability. The meaning of the above RNP attributes can be briefly described as follows:

- *Accuracy* is a statistical value that characterizes the positioning error in 95% of the time (2σ).
- *Integrity* means the ability of the system to warn the user when the system due to failures or other abnormal conditions cannot be used for safety applications. It is associated with the correctness of

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

the provided position needed for the entire duration of the operation - which is e.g. 150 s in the case of a Category I precision approach [23].

- *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, for example, during the 15 s before the aircraft descends to the decision height (DH of 60 m) in the case of Category I [25]. The pilot needs to decide, based on the continuous provision of (correct) PVT information during the 15 s, whether to continue the approach and landing or, e.g. due to poor SIS visibility or its failure, to perform a backup manoeuvre (missed approach) - e.g. to fly to another airport.
- *Availability* represents the percentage of time that the system provides service within given limits - i.e., meets the requirements for accuracy, integrity and continuity.

Although GNSS meets very stringent aviation requirements [25], [27], it does not necessarily mean that it is suitable for use in other transport sectors. In this section, we will focus on GNSS continuity - its correct interpretation and use in land transport, especially in terms of meeting the requirement for reliability of PVT determination.

The aim of this analysis is to start from the continuity requirement set for GNSS 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 ground transportation. The methodology is based on (i) well-defined aeronautical RNP requirements (accuracy, integrity, continuity and availability) for the GNSS SoL service [23]-[26], (ii) the interpretation of these GNSS quality metrics in terms of failure modes and associated failure probabilities [32], [33], and (iii) the use of the railway safety and dependability concept, in the sense of railway RAMS (Reliability, Availability, Maintainability and Safety) [15], [16], as a variant to the aeronautical safety concept, in the RNP sense, for comparative analysis and further investigations.

5.2 Origin of continuity requirement for GNSS SoL service

The existing safety requirements for the GNSS SoL service were primarily derived from the needs of civil aviation. This is because civil aviation was the first of all modes of transport to use GNSS for traffic management. The GNSS integrity and continuity requirements, which are the main safety requirements for air navigation, were therefore directly derived from the aviation Target Level of Safety (TLS) measured by the risk of loss of the aircraft hull over the duration of the mission [31]. The derivation of safety requirements from TLS is briefly described below.

The TLS comes from ICAO historical statistical data on commercial aircraft accidents in the period 1959-1990 and was defined as a probability of hull loss (i.e. risk) of 1.5×10^{-7} per aircraft mission, i.e. per 1.5 hours. The TLS was then allocated to each phase of the flight as well as to the final approach with a value of 1×10^{-8} per approach, which takes about 150 seconds. Since GNSS integrity and continuity are the main metrics of aviation safety with respect to navigation, the TLS per approach was equally divided between integrity risk (IR), i.e. loss of integrity, and continuity risk (CR), i.e. loss of continuity, as shown in [8] in Fig. 1.

In general, however, not every incident leads to an accident, and also in the case of loss of integrity or continuity, the pilot may be able to prevent an accident in some cases. Based on these assumptions, supplemented by specific risk reduction factors, it was derived using fault tree analysis (FTA) for non-airborne systems, i.e. GNSS SoL service, that CR is 8×10^{-6} per 15 s and IR is 2×10^{-7} per approach (i.e. 150 s) [8]. CR is equal to the continuity (C) complement to 1, i.e. C = 1 - CR, and IR is equal to the integrity (I)

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

complement to 1, i.e. I = 1- IR. The same FTA shows that the CR requirement for airborne equipment, i.e. GNSS receiver and accessories, is $2x10^{-6}$ per 15 s.

Continuity is the ability of the system or service to provide navigation accuracy and integrity (integrity is monitored) throughout the intended operation, given that the navigation accuracy and the integrity are provided at the start of the operation [34]-[36], [10]. Continuity is a quality measure whether the system is functioning when it is really needed. This corresponds to the reliability (i.e. probability of correct functioning) of the system, which is related to a specific operation of usually short duration - e.g. 15 s or 1 h in aviation. Therefore, e.g. the continuity requirements for the provision of GNSS Signal-In-Space (SIS) for typical air operations can be considered as a short-term reliability of service [10]. For comparison, the railway standard EN 50126-1 [15] defines reliability as follows: '*ability to perform as required, without failure, for a given time interval, under given conditions'*. So how the aviation continuity differs from reliability on railways? Railway reliability does not refer to the duration of a typical operation because on rail, unlike aviation, the duration of an operation would be difficult to determine.

The reliability of an item (system) may be measured in different ways, depending on the situation, e.g. as: mean time to failure (MTTF) for non-repairable items, mean time between failures (MTBF) for repairable items, failure rate (λ) or the probability of correct item functioning $R(t) = \exp(-\lambda t)$ as a function of time t. The mean time to restore (MTTR) is usually much smaller than the lifetime of the item, then the values of MTTF and MTBF are practically the same, because MTBF ≈ MTTF + MTTR. With this simplification, one can also write for constant failure rate that $\lambda = (\text{MTTF})^{-1} = (\text{MTBF})^{-1}$. The assumption of a constant failure rate is often used in reliability analyses of technical systems.

Continuity means the reliable operation of the system during a certain continuity time interval (CTI). As GNSS is a repairable system, then the SoL service continuity can be expressed as [34], [36]

$$C = \exp\left(-\frac{CTI}{MTBF}\right) \tag{5.1}$$

This is the standard expression for reliability and excludes scheduled outages (i.e. uses random parameter MTBF) assuming that planned outages will be notified, and the operation will not take place. If $\text{CTI} \ll \text{MTBF}$, then

$$C \cong 1 - CTI/MTBF \tag{5.2}$$

Continuity risk (CR) is the probability that the GNSS system will be unintentionally interrupted and will not provide navigation outputs with the required quality over the intended period of time (CTI), assuming that the outputs were present with specified quality at the beginning of a given operation. This occurs when the integrity monitor of SBAS or GBAS triggers a true alert, a false alert, or does not have enough information to make a decision. CR here refers to unplanned interruptions of GNSS service. Loss of GNSS Signal-In-Space (SIS) due to obstructions along a railway line or road is not a loss of continuity because correct functioning of GNSS positioning can be well predicted from the profile of the surrounding environment. Since CR equals the continuity complement to 1, the expression (5.2) yields

$$CR = CTI/MTBF \tag{5.3}$$

The aviation GNSS SoL service CR requirement of $8x10^{-6}$ per 15 s for a Category I precision approach can be converted to an MTBF of 520.83 h using (5.3). For the sake of completeness, this continuity requirement was not introduced only with the coming of GPS technology, but before that for the so-called Instrument Landing

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

System (ILS) [27], [37]. Current GNSS receivers integrated with GNSS antennas achieve MTBF > 50 000 h, therefore, in further considerations below in section 5.4, we neglect the GNSS receiver reliability with respect to much worse SoL service reliability. The primary focus on assessing the impact of GNSS SoL reliability can also be justified by the fact that the quality of service affects many GNSS users, whereas the quality of the GNSS receiver affects only one user. Although continuity is always related to the accuracy and integrity of positioning, this section focuses on GNSS SoL service continuity and its impact on the reliability of positioning in land transport.

5.3 Continuity requirements for GNSS in land transport

In Europe, the strategy to adopt GNSS for the transport sector is based on the use of EGNSS: the Galileo satellite navigation system and the EGNOS SoL service certified for aviation. In that scenario, in addition to the integrity of accuracy, the key to the efficient operational use of the EGNOS SoL service becomes the continuity of the service provided. Early warning to the user that the GNSS SoL service is not able to provide the required accuracy of the positioning function (and thus ensure integrity) will not help if unplanned service outages do not allow its intended use - e.g. GNSS-based ASTP in the case of ERTMS or continuous positioning of a self-driving car in the overtaking phase. Maritime transport is the only surface transport sector that has historically set requirements for continuity of GNSS SoL service [11], [38]. It is also the sector that has the most similar safety concept to air transport - as maritime safety is directly dependent on both safety integrity and reliability (and availability). This section therefore first analyses the importance of GNSS SoL service continuity for maritime navigation purposes. This is followed by an analysis of the applicability of continuity from a railway perspective. The railway has very well-defined safety and dependability requirements (RAMS) for safety-related systems. However, the requirement for GNSS SoL continuity is not explicitly required on the railway [15], [16], [39]. Finally, a brief mention is made of the possible need for GNSS SoL service continuity in the area of self-driving cars, which is currently the most dynamically developing area of transport.

5.3.1 Continuity requirements for maritime

User requirements for GNSS-based maritime navigation were specified in IMO Resolution A.915(22) [11] two decades ago. Most of the requirements for the categories of navigation in oceans, coastal waters, harbour approaches and restricted waters specify an accuracy of 10 m (95 %). Accuracy of 1 m or less is required for port operations - e.g. 0.1 m accuracy for automatic docking. Practically the same approach for the specification of GNSS-based navigation requirements as is applied in aviation has been implicitly used in the maritime sector. This means that maritime GNSS requirements are defined for each category of operation in terms of accuracy, integrity, continuity, and availability.

Integrity and continuity are defined in the maritime sector over the duration of an operation, i.e. a specific manoeuvre such as entering a port or docking. It should be reminded here that in aviation, integrity is defined for the duration of the entire operation, e.g. 150 s for a precision Category I approach, and continuity is defined for the most critical phase of that operation, e.g. 15 s before reaching the decision height. For some flight operations, e.g. en-route or non-precision approach (NPA), both integrity and continuity are defined on a one-hour basis because it is not possible to simply estimate the average duration of flight operations. In maritime the problem is that, unlike aviation, IMO A.915(22) [11] completely lacks a rationale for how the maritime requirements for GNSS were derived. A broadly acceptable maritime safety goal for this derivation is missing. It is not explained how the risk of integrity (IR) and continuity (CR) in terms of the

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

failure probability and the associated duration of operation were derived, i.e. IR of $1x10^{-5}$ per 3 h and CR of $3x10^{-4}$ per 3 h (i.e.

continuity of 99.97% per 3 h according to the original IMO format [11]). In terms of correctness, however, it should be noted that an attempt was subsequently made to retrospectively justify the derivation of the IR and CR attributes using the TLS defined for maritime operations [32], but this attempt has not been adopted by the maritime community.

Over time it became apparent that the initial maritime requirement for continuity ($1\text{-}3x10^{-4}$ per 3 h) was very strict due to very long continuity time interval (CTI) and not achievable by GNSS technology. Translating the maritime continuity requirement in terms of a CR of $3x10^{-4}$ per 3 h for the CTI of 15 s used in aviation gives a CR of $4.2x10^{-7}$ per 15 s. For comparison, e.g. the actual EGNOS SoL service performance in terms of continuity for localizer performance with vertical guidance (LPV-200/ CAT I) and approach with vertical guidance I (APV-I) flight operations is better than $1\text{-}1x10^{-4}$ per 15 s in the core of ECAC (European Civil Aviation Conference) region [25]. It is therefore clear that the initial maritime requirement for GNSS continuity is unrealistic. For this reason, the CTI was implicitly reduced from 3 hours to 15 minutes – as stated in IMO resolution A.1046(27) [38]. The updated maritime CR requirement of $3x10^{-4}$ per 15 minutes and translation to a 1-hour basis gives a CR of $1.2x10^{-3}$ per 1 h. This according to (5.3) equals to an MTBF of 833.33 h. If a CTI of 15 s is used, then the translation of this new maritime requirement for continuity is $1\text{-}5x10^{-6}$ per 15 s. This corresponds roughly to the aeronautical requirement for GNSS continuity, i.e. $1\text{-}8x10^{-6}$ per 15 s. The new multi-constellation and multi-frequency EGNOS V3 is expected to meet aviation continuity requirements and therefore the new maritime GNSS continuity requirement can be considered realistic.

5.3.2 Reliability requirements for rail

The basic framework for ensuring the safety and dependability of railway systems is defined in the CENELEC standards EN 50126-1 [15] and EN 50126-2 [16] on the specification and demonstration of RAMS. These standards consider 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 operating and maintenance conditions. The safety of the railway signalling system is based on three main pillars: 1) functional safety – i.e. mainly safety integrity (S) of each safety function designed to mitigate a specific hazard, 2) technical safety – i.e. a prescribed safe behaviour of the system in case of a dangerous failure, and 3) high dependability – i.e. reliability, availability and maintainability (RAM), because occasional irregularities in train operations due to degraded operational mode of signalling system with participation of a human factor may indirectly compromise railway safety.

As the safety concepts in aviation and on railways are different, in general the aviation requirements for GNSS SoL services cannot be directly applied to the design and approval of safety-related systems on railways. The opposite approach should be taken, i.e. first define the requirements for a safe and reliable train positioning function based on the GNSS SoL service for the application in terms of the railway RAMS and safety standards EN 50129/ EN 50126/ EN 50716 and other regulations, and then use the relevant GNSS service (e.g. EGNOS and/or GBAS) and other sensors and techniques to meet these railway requirements. The key to success is the correct interpretation and assurance of the aeronautical RNP attributes for GNSS in terms of railway RAMS [28], [33].

As evident from above, continuity as a quality measure of safety systems or service is not contained in the railway EN 50126 RAMS framework as a safety attribute. Nevertheless, continuity is an important quality

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

attribute of GNSS SoL service performance, which also significantly affects cost of GNSS SoL service, and therefore continuity cannot simply be omitted when designing GNSS-based railway systems.

EN 50126 [15], [16] prescribe a well-developed method to specify system requirements based on a risk assessment process. The following principles for risk acceptance can be used: codes of practice (CoP), similar reference systems or explicit risk estimation. If there is sufficient experience with a given railway safety-related system, which is also the case of ERTMS, then CoP (i.e. CENELEC standards, ERTMS Technical Specifications for Interoperability (TSI), EU and national regulations and other documents) can be used to specify the requirements for ERTMS based on GNSS. The ERTMS TSI contain, among others, the RAMS requirements for the on-board and trackside part, including requirements for the track balise and onboard balise transmission module (BTM) used for safe train position determination. ERTMS TSI have been used to specify the safety requirements for GNSS-based virtual balise detection [39], [40]. Similarly, ERTMS specification [41] can be used to determine the reliability requirements for virtual balise detection.

	Reliability of ERTMS in MTBF [hours]		
Type of failure	On-board equipment	Central track-side equipment	Line-side equipment
Immobilizing failures	$2.7x10^6$	$3.5x10^8$	$1.2x10^5$
Service failures	$3.0x10^5$	$4.0x10^7$	$1.4x10^4$
Minor HW failures	$8.0x10^3$	$1.0x10^5$	$3.6x10^2$

Table Significance of GNSS continuity and reliability in multimodal transport-1: Reliability requirements for the European Railway Traffic Management System [41].

The ERTMS mission reliability targets [41] consist of qualitative and quantitative requirements. The quantitative requirements are expressed in MTBF and are differentiated according to the criticality (immobilising, service or minor) of the considered failures, as shown in Table Significance of GNSS continuity and reliability in multimodal transport-1. In the ERTMS context, immobilising failures are identified as all the ERTMS failures, which cause two or more trains to be switched in on-sight mode (i.e. driver's responsibility). Service failures cause the nominal performance of one or more trains to be reduced and/or at most one train to be switched in on-sight mode. A minor hardware (HW) failure is a failure which results in excessive unscheduled maintenance and cannot be classified as immobilising or service failure.

It is stated in the ERTMS/ETCS Subset 36 [42] that the minimum operational lifetime of a track balise should be 30 years. ERTMS tenders often contain MTBF values of 50 000+ h for a complete ERTMS on-board subsystem and MTBF of 50+ years for ERTMS balises [39]. In the reliability analysis of the ETCS L2 on-board subsystem [43], the BTM, which reads the physical balises, is assumed to have a failure rate of $0.2x10^{-5}$/h (i.e. an MTBF of $5x10^5$ h) and a similar reliability analysis [44] assumes that the MTBF of both the BTM and the single balise is $4.4x10^5$ h – i.e. approximately MTBF of $5x10^5$ h.

In the Europe's Rail R2DATO project [62], the occurrence of sudden variation or loss of the GNSS-based Advanced Safe Train Positioning (ASTP) shall be less than $2x10^{-6}$/h, corresponding to a MTBF of $5x10^5$ h. In addition, the occurrence of not operational ASTP (no output) shall be less than 1 event every 10 years, corresponding to a MTBF of more than $1x10^5$ h. These R2DATO reliability ASTP targets are very similar to the targets coming from [39].

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

Reliability requirements for ASTP are also defined in deliverable D2.1 of the VICE4RAIL project [63]. According to them, ASTP should have an MTBF value at least comparable to the odometry solution for ETCS. In addition, ASTP reliability target (MTBF) shall be defined according to the impact on operation of the failure: minor (no impact), reduced service, immobility [41] . Furthermore, ASTP life cycle shall be at least 30 years [42].

As indicated above, MTBF values of $5x10^5$ h for balise and BTM can be considered as minimum to meet the MTBF requirement of 50 000+ h for an ERTMS on-board system. In addition, there are other non-redundant components of the ERTMS on-board subsystem, e.g. the BTM antenna under the vehicle, which must have an even higher MTBF value (e.g. 1.43 $x10^6$ h [43]) to meet the MTBF requirement of 50 000+ h for the on-board subsystem.

The result of the above analysis of the reliability requirements for the ERTMS balise and BTM is that the MTBF target for ASTP for ERTMS should be approximately $5x10^5$ h. This value exceeds the MTBF of GNSS SIS service (520.83 h) by three orders of magnitude. Both these two MTBF values are used as inputs in the reliability analysis in section 5.4.

5.3.3 GNSS continuity for automated car driving

In the field of automated driving systems (ADS) for cars there is currently still no consensus on the need to use the GNSS continuity. Therefore, only two opposing views on the applicability of continuity for ADS are presented below.

Let's first take a closer look at the problem in terms of the relevant automotive safety standards. A safety function mitigating risk can be considered safe if ISO 26262 (Automotive functional safety) [13] and ISO/PAS 21448 (Safety of the intended functionality - SOTIF) [19] standards are used for its design and implementation. However, vehicles cannot be in a safe state without secure operations specified in the standard ISO SAE 21434. To cover the whole area of ADS safety, standard ISO/TR 4804 (Road vehicles - Safety and cybersecurity for automated driving systems - Design, verification and validation) [21] was recently developed. The intention of ISO/TR 4804 is to put together standards ISO 26262, ISO/PAS 21448 and ISO SAE 21434 under one risk-based approach. ISO/TR 4808, which is the umbrella for all other automotive safety standards, states that *"the continuity metric is no longer the main parameter of GNSS-based positioning with integrity"*. This is justified in ISO/TR 4808 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 [22] , where GNSS continuity is considered a high priority requirement. The importance of GNSS continuity is considered here for safety and liability-critical applications such as autonomous cars, trains, mobile robots (autonomous things), agricultural machinery with GNSS-based automated steering. As mentioned above, the conflict of opinion regarding the importance of GNSS continuity for ADS is due to the fact that ISO/TR 4808 has a different understanding of the meaning of continuity - it does not only consider unplanned satellite signal outages, but also planned (known in advance) outages. This is incorrect. In any case, the above-mentioned views on the use of GNSS continuity in automotive transport are quite different and therefore need to be monitored further.

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

5.4 Reliability analysis of GNSS-based positioning

The aim of the analysis is to show how to meet the strict railway (ERTMS) requirement for reliability of GNSS-based train positioning in terms of MTBF of $5x10^5$ h (as it was specified above) although the reliability (continuity) of the GNSS SoL service is relatively very low. At the same time, this analysis can be seen as a guide to improve the reliability of GNSS-based positioning in other land transport applications. In maritime, e.g., resilient positioning solutions based on GNSS and other diverse sensors have been investigated for continuity and integrity using fault tree analysis (FTA) [45]. The disadvantage of the FTA method is that it does not include time analysis of system faulty states, which is required for rail applications. Therefore, for the reliability analysis in this section, Markov analysis was used [46], which, unlike FTA, allows to efficiently solve the time dependencies of the probabilities of fault or fault-free states of the system, including the calculation of the MTTF.

For this purpose, redundant 1oo2 (one-out-of-two) architectures with primary unit A and standby B are used – as shown in Figure Significance of GNSS continuity and reliability in multimodal transport-10(a) and Figure Significance of GNSS continuity and reliability in multimodal transport-11(a). Unit A is based on GNSS and provides an absolute position. Backup B is an inertial measurement unit (IMU) that provides a relative position. Fault diagnostics is critical, as it ensures the correct switchover of operation from the failed primary unit A to the backup B. When the correct function of unit A is restored, the operation is switched from standby B to unit A.

For simplicity, assume that the EGNOS V3 (dual-frequency and multi-constellation) service meets the aeronautical continuity requirement for a Category I precision approach in terms of a continuity risk (CR) of $8x10^{-6}$ in 15 s, which according to (5.3) corresponds to an MTBF of 520.83 h and a CR (i.e. also failure rate) of $1.92x10^{-3}$ in 1 h. Therefore, let the MTBF of unit A ($MTBF_A$) be 520.83 h. The MTBF of the B unit ($MTBF_B$) will be variable to meet the reliability requirement for ASTP (MTBF of $5x10^5$ h).

The reliability analysis is demonstrated using two examples of redundant architectures and the corresponding Markov models in Figure Significance of GNSS continuity and reliability in multimodal transport-10(b) and Figure Significance of GNSS continuity and reliability in multimodal transport-11(b). Markov models describe the system through system states, e.g. S0, S1, S2 etc., with transitions between them depending on failure rates (λ) and restore/ repair rates (μ). The states must be mutually exclusive and collectively exhaustive. Based on the state model, the time dependencies of the probabilities of each state, e.g. $P_0(t)$, $P_1(t)$, $P_2(t)$ etc., in which the system is found, are calculated. Using these probabilities, reliability, availability, failure rate, and other system attributes can be determined.

The goal in this analysis is to calculate the mean time to failure ($MTTF_{sys}$) for the system architecture using Markov models [46]. Although a GNSS-based positioning system for transport applications is considered to be repairable, the resulting calculated reliability is reported in this analysis in terms of $MTTF_{sys}$ and not $MTBF_{sys}$. This is because, as shown below in section 5.4, the output attribute when analysing the reliability of systems using Markov models is the MTTF. However, as shown above, the values of MTTF and MTBF are almost identical. For the architectures in Figure Significance of GNSS continuity and reliability in multimodal transport-10 and Figure Significance of GNSS continuity and reliability in multimodal transport-11, the function of the primary unit A is assumed to be superior to that of unit B. These are therefore Markov models with priority of operation. The examples are given below.

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

Example 1: Redundant system with priority operation of unit A, cold standby B, imperfect diagnostics of unit A, and online restoration of unit A. The architecture of the basic redundant system with priority operation of one of the units is shown in Figure-10(a). The primary unit A is GNSS-based and provides absolute positioning. The standby B provides a relative position. Units A is assumed to have imperfect diagnostics with diagnostic coverage c (probability of fault detection). Diagnostics of the standby B is performed only off-line in this example.

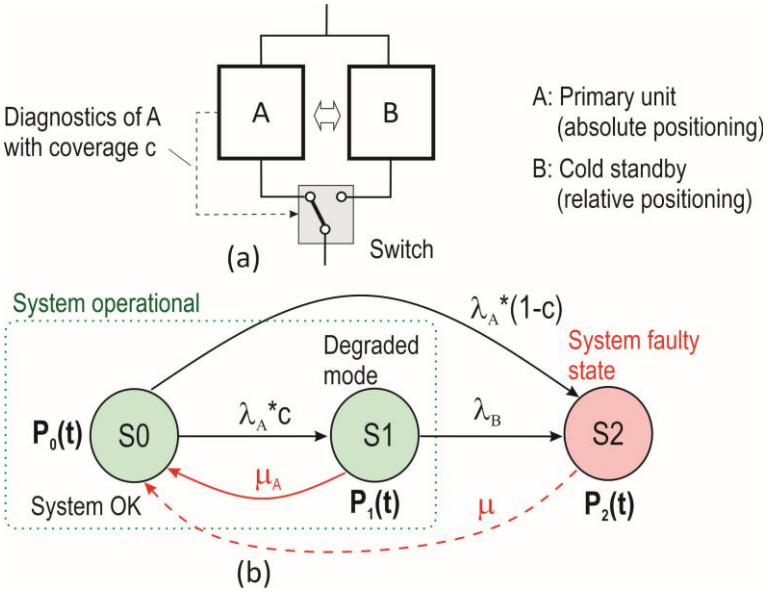

Figure Significance of GNSS continuity and reliability in multimodal transport-10: Redundant system with priority operation of unit A, cold standby B and imperfect diagnostics and switching: (a) schema of the system, (b) Markov model.

For the Markov model of the architecture in Figure-10(b), the following three system states are defined:

- S0: Fully functional system state. Primary unit A is operating according to specifications. Standby unit B is fault-free and not operational.
- S1: Degraded operational mode. It is still functional state. Primary unit A is faulty. Fault on unit A is detected by imperfect online diagnostics and is restored with a frequency of μ_A. Switchover to standby unit B is successful. Standby B is operational.
- S2: System faulty state. It is the result of a fault on standby B or when the diagnostics of faulty unit A fails. Recovery of the system with a frequency μ will bring the system from state S2 to S0.

The corresponding time-dependent state probabilities according to the Markov model in Figure-10(b) are $P_0(t)$, $P_1(t)$ and $P_2(t)$. The intention is to determine the $MTTF_{sys}$. It can be calculated by integrating the system reliability $R(t) = P_0(t) + P_1(t)$ over time t from zero to infinity for non-absorbing states S0 and S1. A prerequisite for a correct system reliability calculation is that the faulty state of the system S2 must be an absorbing state. The absorbing faulty state means that once the system enters it, it cannot be left until the system is properly restored. Therefore, in the case of $MTTF_{sys}$ calculation according to Figure-10(b), the (dashed) directional arc indicating the system restoration with frequency μ must be omitted. Mean time to restore/ repair (MTTR), which is indirectly proportional to μ (μ = 1/MTTR), can be used to calculate system availability as $A = MTTF_{sys}/(MTTF_{sys} + MTTR)$. Thus, $MTTF_{sys}$ characterizes, besides reliability, also the availability of the system. Online restoration of primary unit A with frequency μ_A can bring the system from degraded state S1 to the

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

fully operational state S0. Therefore, online diagnostics and restoration is the key to increase system reliability and MTTF. The Markov model for the system according to Figure-10(b) can be described by the system of linear differential equations as

$$\begin{pmatrix}\dot{P}_0(t)\\ \dot{P}_1(t)\\ \dot{P}_2(t)\end{pmatrix}=\begin{pmatrix}-[\lambda_A c+\lambda_A(1-c)] & \mu_A & 0\\ \lambda_A c & -(\mu_A+\lambda_B) & 0\\ \lambda_A(1-c)] & \lambda_B & 0\end{pmatrix}\cdot\begin{pmatrix}P_0(t)\\ P_1(t)\\ P_2(t)\end{pmatrix} \quad (5.4)$$

with the initial conditions for the state probabilities [$P_0(0)$, $P_1(0)$, $P_2(0)$] = (1,0,0). To calculate the mean time to system failure ($MTTF_{sys}$), we use the Laplace transform (marked as *) and the limit theorem as follows

$$MTTF_j=\int_0^\infty P_j(t)dt=\lim_{s\to 0}\int_0^\infty P_j(t)e^{-st}dt=P_j^*(0)\ \Rightarrow MTTF_{sys}=\sum P_j^*(0) \quad (5.5)$$

where j represents the non-absorbing states. The system of equations (5.4) after the Laplace transform and application of the initial conditions is

$$\begin{pmatrix}sP_0^*(s)-1\\ sP_1^*(s)-0\\ sP_2^*(s)-0\end{pmatrix}=\begin{pmatrix}-[\lambda_A c+\lambda_A(1-c)] & \mu_A & 0\\ \lambda_A c & -(\mu_A+\lambda_B) & 0\\ \lambda_A(1-c)] & \lambda_B & 0\end{pmatrix}\cdot\begin{pmatrix}P_0^*(s)\\ P_1^*(s)\\ P_2^*(s)\end{pmatrix} \quad (5.6)$$

Since the complex frequency domain parameter s → 0, then $sP_j^*(s)\to 0$. For the $MTTF_{sys}$ calculations, only the equations for the non-absorbing states (j = 0, 1) are used from (5.6) as follows

$$\begin{pmatrix}-1\\ 0\end{pmatrix}=\begin{pmatrix}-[\lambda_A c+\lambda_A(1-c)] & \mu_A\\ \lambda_A c & -(\mu_A+\lambda_B)\end{pmatrix}\cdot\begin{pmatrix}P_0^*(0)\\ P_1^*(0)\end{pmatrix} \quad (5.7)$$

Solving the system of equations (5.7) gives

$$P_0^*(0)=\frac{\mu_A+\lambda_B}{\lambda_A\cdot[\lambda_B+\mu_A(1-c)]} \quad (5.8)$$

$$P_1^*(0)=\frac{c}{\lambda_B+\mu_A(1-c)} \quad (5.9)$$

and using (5.5) the mean time to (first) system failure is

$$MTTF_{sys}=P_0^*(0)+P_1^*(0)=\frac{\mu_A+\lambda_B+\lambda_A\cdot c}{\lambda_A\cdot[\lambda_B+\mu_A(1-c)]} \quad (5.10)$$

Note: The diagnostic coverage c in (5.10) refers only to the primary unit A. In section 5.5 (Results of reliability analysis), for clarity, this coverage is denoted as c(A).

Example 2: Redundant system with priority operation of unit A, warm standby B, imperfect diagnostics of units A and B, online restoration of unit A. The system architecture in this example is shown in Figure-11(a) and the corresponding Markov model is shown in Figure-11(b). The difference of this architecture with respect to the architecture in Figure-10 is that both units (A and B) are equipped with online diagnostics. Since the diagnostics of faulty standby B with coverage c can fail, the Markov model additionally contains state S2 - latent fault of standby B.

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

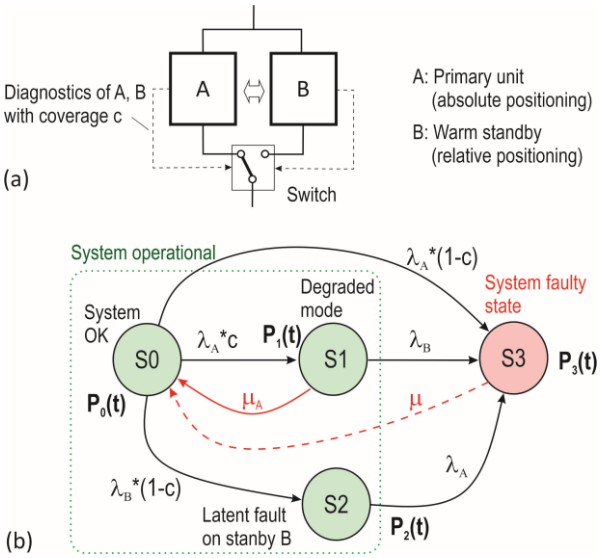

Figure Significance of GNSS continuity and reliability in multimodal transport-11: Redundant system with priority operation of unit A, warm standby B and imperfect diagnostics and switching: (a) schema of the system, (b) Markov state model. Note: P – probability, S – system state, c – coverage, λ – failure rate, μ – repair rate.

For the Markov model in Figure-11(b), the following four states of the system can be defined:

- S0: Fully functional system state. The GNSS-based primary unit A is operating according to specifications. Fault-free standby B (e.g. IMU) is not operational.
- S1: Degraded mode of operation, but functional system state. Fault of unit A is detected by diagnostics with coverage c and is recovered online with a frequency of μ_A. The switchover to standby B was successful. Standby unit B is operational.
- S2: Standby B has a latent fault.
- S3: System faulty state. This occurs when: i) a fault of primary unit A is not detected, ii) unit A fails and then standby B fails, or iii) standby B has a hidden fault and then unit A fails.

The Markov model in Figure-11(b) can be described by the system of linear differential equations as

$$\begin{pmatrix} \dot{P}_0(t) \\ \dot{P}_1(t) \\ \dot{P}_2(t) \\ \dot{P}_3(t) \end{pmatrix} = \begin{pmatrix} -[\lambda_A c + \lambda_A(1-c) + \lambda_B(1-c)] & \mu_A & 0 & 0 \\ \lambda_A c & -(\mu_A + \lambda_B) & 0 & 0 \\ \lambda_B(1-c) & 0 & -\lambda_A & 0 \\ \lambda_A(1-c) & \lambda_B & \lambda_A & 0 \end{pmatrix} \cdot \begin{pmatrix} P_0(t) \\ P_1(t) \\ P_2(t) \\ P_3(t) \end{pmatrix} \qquad (5.11)$$

with the initial conditions for the state probabilities $[P_0(0), P_1(0), P_2(0), P_3(0)] = (1,0,0,0)$. Solving the mean time to system failure using (5.11) and the Laplace transform described in Example 1 gives

$$MTTF_{sys} = \frac{(\mu_A+\lambda_B)\cdot\frac{[\lambda_A+\lambda_B(1-c)]}{\lambda_A^2\cdot c}+1}{\{[\lambda_A+\lambda_B(1-c)]\cdot\frac{\mu_A+\lambda_B}{\lambda_A\cdot c}-\mu_A\}} \qquad (5.12)$$

Note: The diagnostic coverage c in (5.12) refers to units A and B. In section 5.5 (Results of reliability analysis) this coverage is denoted as c(A, B) for clarity.

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

5.5 Results of reliability analysis

This section describes the reliability calculations and discusses the results achieved in terms of $MTTF_{sys}$ for systems based on the aviation GNSS SoL service and intended for vehicle positioning in land transport. The calculations are performed according to the expressions derived for redundant architectures in the previous section. In particular, the aim of these calculations is to show how the relatively low reliability (continuity) of the GNSS SoL service-based positioning can be increased to the level of reliability acceptable in rail transport. The railway case is considered because the reliability requirements for positioning of trains are the highest of all the surface transport modes mentioned.

The following symbols are used in the tables below:

- CR_A – is the required aviation continuity risk or real performance for GNSS SoL service considered in channel A of the redundant architecture,
- $MTBF_A$ – is the mean time between failures of unit A corresponding to the continuity risk CR_A,
- λ_A – is the failure rate per 1 h of unit A corresponding to the continuity risk CR_A ($\lambda_A = 1/MTBF_A$),
- $MTBF_B$ – is the selected mean time between failures of unit B,
- μ_A – is the recovery frequency of unit A per 1 h,
- λ_B – is the failure rate per 1 h of unit B corresponding to the $MTBF_B$,
- c(A) – is the diagnostic coverage (probability of failure detection) of unit A, and
- c(A, B) – is the diagnostic coverage of units A and B.

For the sake of simplicity in this section, we assume that the MTBF and MTTF values are practically identical for relatively short MTTR, because MTBF = MTTF + MTTR. The input reliability values of units A and B are considered in terms of MTBF and associated failure rates per 1 h.

CR_A [per 15 s]	$MTBF_A$ [h]	λ_A [per h]	$MTBF_B$ [h]	λ_B [per h]	μ_A [per h]	c (A) [-]	$MTTF_{sys}$ (5.10) [h]
$8x10^{-6}$ Aviation requirement	520.83	$1.92x10^{-3}$	1000	$1x10^{-3}$	1	1	$5.22x10^5$
						0.99999	$5.17x10^5$
						0.9999	$4.75x10^5$
						0.999	$2.61x10^5$
						0.99	$4.75x10^4$
$1x10^{-4}$ EGNOS performance	41.66	$2.40x10^{-2}$	1000	$1x10^{-3}$	1	1	$4.27x10^4$
						0.99999	$4.23x10^4$
						0.9999	$3.88x10^4$
						0.999	$2.14x10^4$
						0.99	$3.88x10^3$

Table Significance of GNSS continuity and reliability in multimodal transport-2: Effect of diagnostic coverage c(A) of unit A on $MTTF_{sys}$ according to Example 1.

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

Table-2 contains the calculated $MTTF_{sys}$ values according to (5.10) for the architecture in Figure-10. The main objective here is to show the effect of diagnostic coverage c(A) of the primary unit A on the overall system reliability. Unit A represents the GNSS-based positioning and unit B represents the IMU-based backup relative positioning. Thus, the operation of unit A is prioritized over the operation of standby B. In the calculation of $MTTF_{sys}$, only the continuity of the GNSS SoL service is considered, which is measured by the continuity risk CR_A in terms of (5.3). Since continuity is one of the most demanding quality attributes of GNSS SoL service to achieve, in Table-2 we consider both the aviation continuity risk requirement for safety operations, e.g., APV I/ LPV-200/ CAT I – i.e., $8x10^{-6}$ per 15 s, and the actual EGNOS SoL service performance in terms of achieved continuity risk – i.e., $1x10^{-4}$ per 15 s in the core of ECAC region [25]. The CR_A value is converted to $MTBF_A$ using (5.3) and also to λ_A using the expression $\lambda_A = 1/MTBF_A$. The CR_A of $1x10^{-4}$ per 15 s corresponds to the $MTBF_A$ of 41.66 h. For standby B, a $MTBF_B$ of 1000 h was first selected, which is approximately twice the MTBF value for the GNSS SoL service. The average duration of a train mission is 1 hour [47], and therefore the corresponding minimum recovery frequency of unit A (μ_A) is 1 recovery per 1 h. The calculated $MTTF_{sys}$ values strongly depends on the diagnostic coverage c(A) of unit A. Table-2 shows that the system in Example 1 is unable to meet the railway MTBF requirement of $5x10^5$ h for a real CR performance of EGNOS. The railway MTBF requirement can be met, e.g., for the following input values: a CR_A of $8x10^{-6}$ per 15 s, an $MTBF_B$ of 1000 h, μ_A of 1 restoration per 1 h, and a high diagnostic coverage c(A) of 0.99999.

CR_A [per 15 s]	$MTBF_A$ [h]	λ_A [per h]	$MTBF_B$ [h]	λ_B [per h]	μ_A [per h]	c (A, B) [-]	$MTTF_{sys}$ (5.12) [h]
$8x10^{-6}$	520.83	$1.92x10^{-3}$	1000	$1x10^{-3}$	1	0.9999	$4.53x10^5$
						0.999	$2.07x10^5$
						0.99	$3.24x10^4$
			1000	$1x10^{-3}$	10	0.9999	$2.07x10^6$
						0.999	$3.22x10^5$
						0.99	$3.42x10^4$
			10000	$1x10^{-4}$	1	0.9999	$2.54x10^6$
						0.999	$4.53x10^5$
						0.99	$4.92x10^4$
			10000	$1x10^{-4}$	10	0.9999	$4.52x10^6$
						0.999	$4.90x10^5$
						0.99	$4.95x10^4$
			20000	$5x10^{-5}$	1	0.9999	$3.42x10^6$
						0.999	$4.85x10^5$
						0.99	$5.06x10^4$
						0.9999	$4.84x10^6$

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

			20000	$5x10^{-5}$	10	0.999	$5.05x10^5$
						0.99	$5.08x10^4$

Table Significance of GNSS continuity and reliability in multimodal transport-3: Effect of diagnostic coverage c(A, B) of primary unit A and standby B on $MTTF_{sys}$ according to Example 2.

Table-3 contains the $MTTF_{sys}$ values calculated using (5.12) for the architecture with priority operation of unit A with warm standby B shown in Figure-11. The main objective is to show to what extent the system reliability is affected when both units of the system are equipped with online diagnostics with diagnostic coverage c(A, B), which is shown in Table-3, compared to a system where only unit A is equipped with online diagnostics with coverage c(A), which is shown in Table-2. For example, from comparing the calculated $MTTF_{sys}$ value of $2.07x10^5$ h in Table-3 and the $MTTF_{sys}$ value of $2.61x10^5$ in Table-2 for the identical input values, including diagnostic coverage (0.999), the imperfect diagnostics with coverage c(A, B) in Example 2 slightly reduces the $MTTF_{sys}$ value relative to the applied diagnostics with coverage c(A) in Example 1. This is understandable because perfect diagnostics is replaced with imperfect diagnostics. A further increase in $MTTF_{sys}$ can be achieved by increasing the input values of $MTBF_B$ and μ_A, as can be seen in Table-3.

Based on the calculated $MTTF_{sys}$ values shown in Table-2 and Table-3, it can be concluded that the reliability of the position determination function based on the aviation GNSS SoL service can be significantly improved by using a standby unit such as an IMU. In this case, it is a redundant system with priority operation of unit A providing absolute positioning and standby unit B providing relative positioning. To achieve the required $MTTF_{sys}$, e.g. $5x10^5$ hours, which is the railway reliability requirement for ERTMS, the system based on GNSS SoL service must be equipped with a reliable standby unit B (e.g. $MTBF_B$ of 10 000 h or more) and high-quality online diagnostics and unit switching.

5.6 Impact of the reliability analysis

According to reliability theory, the MTTF of systems can be increased by using redundant architectures. Therefore, in this section, simplified 1oo2 (one-out-of-two) architectures have been analysed, where channel A is represented by the GNSS SoL service with guaranteed continuity for aviation (corresponding to an MTBF of 520.83 h) and channel B is implemented by e.g. IMU. The reliability of the GNSS receiver and antenna, which is several times greater than the reliability of the SoL service, has been neglected for simplicity in this analysis. Systems of differential linear equations based on Markov models of the corresponding architectures, the Laplace transform, and the limit theorem were used to numerically solve the mean time to system failure ($MTTF_{sys}$). The numerical results of $MTTF_{sys}$ presented in section 5.5 demonstrate that redundant architectures when using aviation GNSS SoL service will enable to meet the high reliability requirements of railways for safe GNSS-based train localization. However, having high diagnostic coverage is a prerequisite.

5.7 Example of continuity risk allocation for GBAS - for CAT I

The causes of the loss of continuity and the magnitude of the individual contributions to the overall loss of continuity can be seen from the example of the continuity risk allocation for the airborne GBAS service level C shown in Figure Significance of GNSS continuity and reliability in multimodal transport-12 [27]. This service

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

is designed for a Category I precision approach (CAT I). In this example, the continuity risk is expressed both in terms of the probability of unexpected failure (service interruption) during a 15 s interval, and also as continuity expressed in terms of MTBF - and this is due to the use of GNSS in multimodal transport.

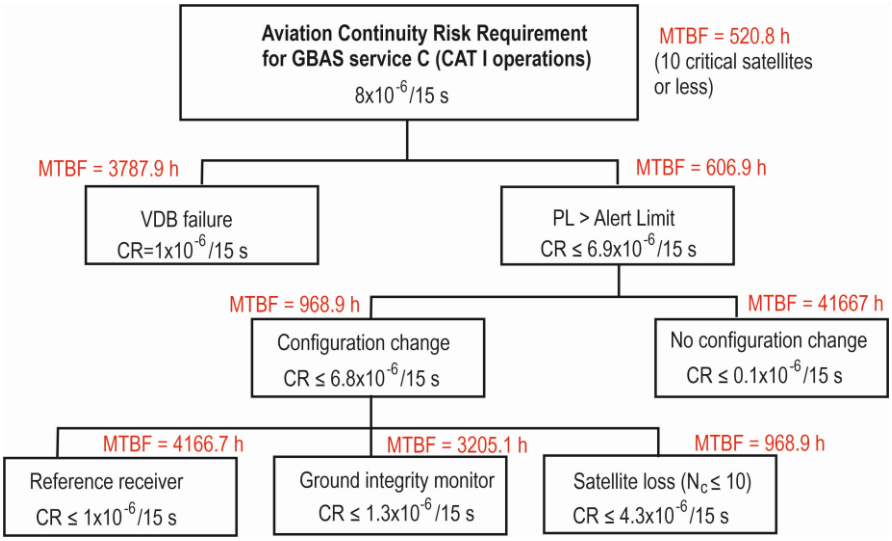

Figure Significance of GNSS continuity and reliability in multimodal transport-12: Example of continuity risk allocation for GBAS service C (CAT I operation) [27].

The overall GNSS SIS continuity requirements are sub-allocated among two basic sources of continuity risk: loss of the VHF data broadcast (VDB) and the possibility of a protection limit (PL) exceeding the required alert limit (AL), i.e. PL > AL. In terms of the use of GNSS continuity in land transport, the second source is more interesting now. Unscheduled occurrences of PL > AL cases are also subdivided into two categories: those that involve 'configuration changes' and those that do not. Configuration changes are defined to be unexpected events that cause the loss of one or more ranging sources or reference receivers. PL can also exceed AL without any configuration change due to data sent by the ground – such as increase in bias values and/or sigma values for one or more ranging corrections.

As can be seen from Figure Significance of GNSS continuity and reliability in multimodal transport-12, configuration changes, and in particular SV loss, contribute most to the loss of continuity. Conservatively, the MTBF of the satellite is considered to be 9740 hour (1 year). Further, it is conservatively assumed that the critical satellites (which can cause continuity loss after its exclusion from the position solution in the sense of PL > AL) are at most 10, i.e., Nc $\leq$ 10. The corresponding continuity risk is 4.3×10^{-6}/15 s. In addition to satellite loss, configuration changes can occur due to reference receiver failures and integrity alerts from ground monitoring under fault-free conditions.

If the most 4 critical satellites are considered, then the total GBAS continuity risk is 5.2×10^{-6}/15 s and the corresponding MTBF is 801.3 h. We must not forget that the performance of the current EGNOS in terms of CR is 1×10^{-4}/15 s and the corresponding MTBF is 41.66 h.

The continuity risk allocated to the reference receiver is 1×10^{-6}/15 s and this corresponds to an MTBF of 4167 h. If we consider that GBAS uses for SIS integrity monitoring 4 reference receivers (M = 4) [27], then based

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

on reliability the theory, it can be determined that each of the reference receivers must have an MTBF of 16667 h. Remaining CR is the allocated to the “no configuration change”.

In aviation, the duration of the critical phase of an operation is short (e.g. 15 s for CAT I), and therefore GNSS can be used to achieve the required low probability of loss of continuity (e.g. $8x10^{-6}$/15 s). However, this corresponds to a small MTBF value, which is used as a measure of fault-free performance in ground transportation. To further increase the MTBF to the required level in transport, redundant systems need to be used, as discussed in section 5.4.

Note: In aviation and telecommunications, the term Mean Time Between Outages (MTBO) is also used as a measure of uptime. It is intended among others for systems with short outages (e.g. 1 s) and for describing continuity. MTBO is a related metric that focuses on the average time between outages, which may or may not be caused by failures, e.g. due to SW issues, geometry of satellite constellation, etc. On the other hand, MTBF is the average time a system or component operates reliably before a failure occurs. Since the term MTBO is not used in transportation, we will continue to use MTBF to describe continuity/reliability, with the understanding that not all service/function outages are caused by a failure or fault.

5.8 Discussion on the meaning of GNSS continuity in multimodal transport

This section recapitulates the need and utilization of GNSS service continuity in different transport sectors using the findings presented in section 5 above. It is the comparative analysis approach used in multimodal transport that has enabled the conclusions presented.

The starting point of the analysis is the need for GNSS continuity in aviation, which was already well justified more than 30 years ago on the basis of a relevant risk analysis – see e.g. [31]. General considerations on reliability are subsequently added. The similarity between short-term reliability and continuity in terms of probability of success over a critical time interval, i.e. phase of operation, is shown. It is also shown why it is preferable to use the term GNSS continuity in aviation rather than (short-term) reliability. This is demonstrated by an example from maritime transport, where the reliability requirement for GNSS was first defined and then replaced by a requirement for GNSS continuity. Finally, the need to utilise aviation continuity in the rail and automotive sectors within a single GNSS infrastructure for multimodal transport applications is being defended.

Aviation: continuity vs. reliability

In aviation, GNSS continuity is used as one of the two main safety attributes of GNSS quality (along with GNSS integrity), which is derived from the acceptable aviation risk and the related Target Level of Safety (TLS) [31], [8]. As mentioned above, GNSS continuity of SoL service is defined in terms of the probability with which GNSS accuracy and integrity are provided without unplanned interruption for the (short) duration of a critical operation phase. Thus, at first sight, continuity corresponds to short-term reliability. This poses the question of why the term short-term reliability is not used in aviation instead of the term continuity. 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' [6]. 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 project is funded by European Union’s Horizon Europe programme under grant agreement No 101180124

This is associated with the presence of GNSS integrity monitor. The integrity monitor can raise a true-alert or a false-alert (and thus cause 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 does not need to 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. 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 [9]. 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 [9]. The term GNSS continuity started to be used in the maritime context in IMO Resolution A.915(22) adopted on 29 Nov 2001 [11].

Railway

The railway safety and dependability concept based on the standard EN 50126 (RAMS) [15], [16] 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 service, in particular EGNOS, which was 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 section 5.3.2. It is assumed that the MTBF of GNSS positioning should be $5x10^5$ 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 section 5.7, GNSS 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 Significance of GNSS continuity and reliability in multimodal transport-12), then the

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

total GBAS service continuity risk is 5.2×10^{-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 performance of the current EGNOS in terms of CR is 1×10^{-4}/15 s and the corresponding MTBF is only 41.66 h.

Automotive

It appears that there is no consensus in the automotive industry on the use of GNSS continuity. Witness is the current automotive umbrella safety standard ISO/TR 4804 [21] that does not consider GNSS continuity to be one of the main GNSS quality attributes. The standard states the following: *"Continuity metric is no longer the main parameter of GNSS-based positioning with integrity*" [21]. 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. Reliability (continuity) is the basis for the availability determination. As the railway has the most stringent requirements for system reliability in surface transport, the MTBF value of 5×10^5 hours, which is required for ASTP, was chosen as the reliability target for the analysis described in section 5.4. and also as GNSS reliability target in multimodal transport. In the field of self-driving cars, GNSS continuity is beneficial for meeting the Safety-Related Availability (SaRA) requirement, which is needed where fail-operational system behaviour is required - e.g. for ADS when overtaking cars.

6. GNSS AUGMENTATION SYSTEMS FOR RAIL

6.1 GNSS Augmentation within ERTMS

High Accuracy and High Integrity GNSS services for Rail and Automotive are based on Augmentation Systems.

As reported in [55], within ERTMS, the GNSS augmentation dissemination framework to be adopted for Rail has to be designed to be agnostic with respect to the Augmentation System.

Concerning integrity, a relevant point concerns the PL calculation based on the OBU algorithms (e.g. Kalman Filter) where estimated covariance matrix may not allow bounding the position error.

This can be due to the assumptions of uncorrelated errors and deviation from the Gaussian distribution.

While in this case it is recommended to leave to the manufacturer the responsibility to address such point, the Augmentation System can estimate time correlation parameters and distribute to the user receiver. It can implement state augmentation parameters and apply through Gauss-Markov models.

To apply such solution, the system shall rely on multimodal standards. RTCM SC-134 is currently foreseeing the transmission of time correlation parameter Data Fields into [56].

The general ERTMS architecture, including GNSS Augmentation, is shown in Figure GNSS augmentation systems for rail-13. The GAS (GNSS Augmentation System) is interfaced to the Trackside Subsystem (CCS-TS) through interfaces defined into the GA-TS MOPS. Communication function, e.g. the GADF (GNSS Augmentation Dissemination Function).

RTCM SC-104 and RTCM SC-134 can be adopted for this interface.

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

The Augmentation Messages are transmitted to the On-board Subsystem (CCS-OB) through protocols and data formats defined into the GA-OB/GA-TS ICD. Such data exchange format shall allow encapsulation of external multimodal messages (e.g. RTCM SC-104 [57] and RTCM SC-134 [56]) into the existing protocol and data format.

Therefore, the GA-TS within the CCS-TS Trackside subsystem acts as an adapter between the external GNSS Augmentation System and the GA-OB.

The CCS-OB also receives, through a safe communication system, GNSS signals and SBAS Augmentation messages through the relevant standard specifications (SBAS MOPS [26] and GNSS SIS ICDs).

Temporary communication losses are also considered through a resume message stream. The communication of messages between the GA-TS and the GA-OB implies an acknowledge to be sent from the user to the Trackside.

It has to be underlined how the proposed architecture allows a complete decoupling between external GNSS Augmentation, the Trackside and the On-Board Unit.

Integrity is ensured with a reactive fail-safe design, where the TTA is the time elapsed from the onset of the alert condition to its detection and negation in the GA-OB.

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

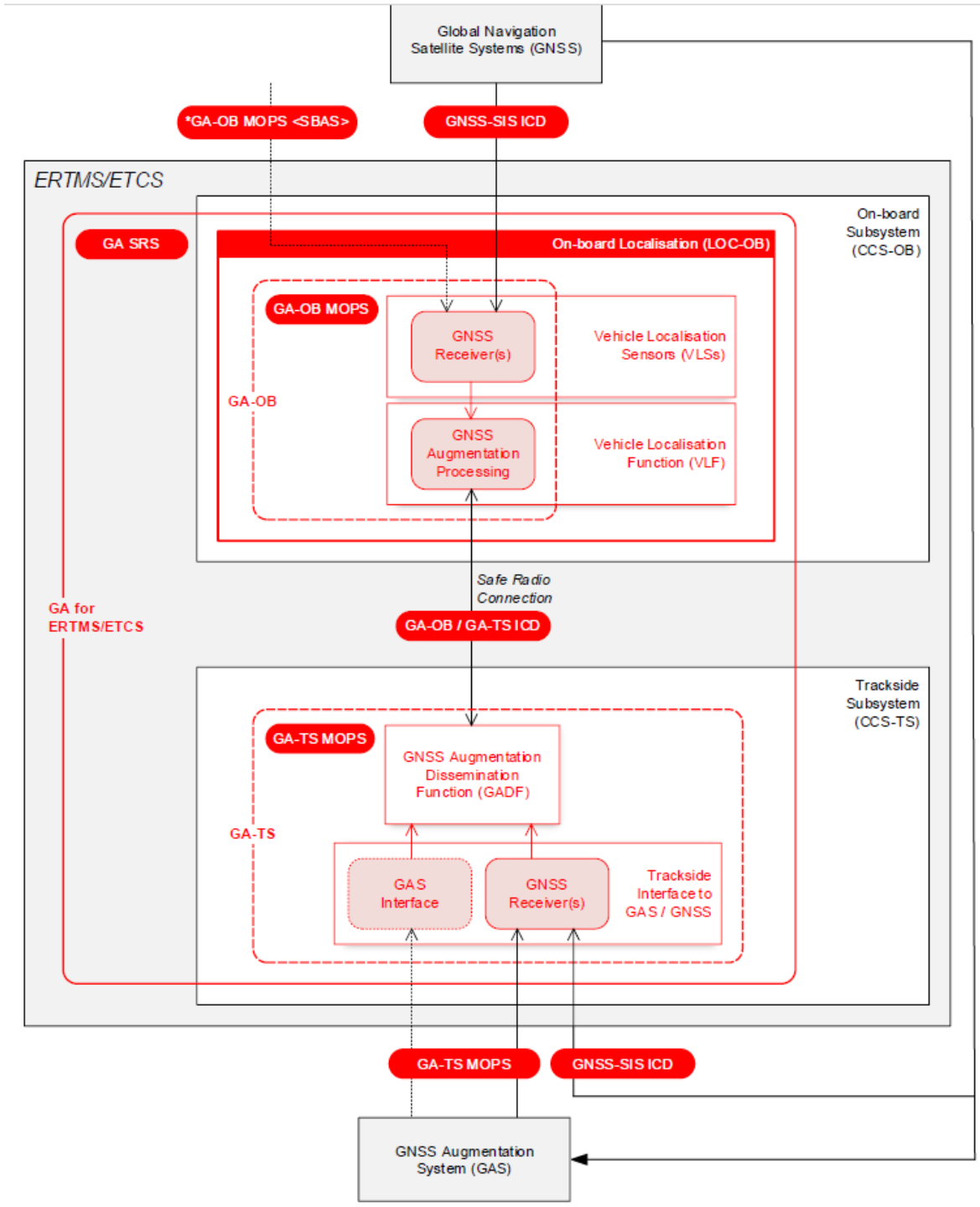

Figure GNSS augmentation systems for rail-13: Architecture and Interfaces of GNSS Augmentation for ERTMS (Source [55]).

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

The System includes the rebroadcasting of SBAS messages and the management of the TTA, including Ground, Space and Receiver latency.

The GA Maximum TTA (T_NVGAMAXTTA) has been defined as a national value for the GNSS augmentation system.

The Core constellations are GPS and Galileo, while others are optional.

Furthermore, two parallel Augmentation message streams are allowed to be processed by the GA-OB. A clear State Transition matrix is defined for the GA-OB, with relevant priority levels assigned.

A clear list of GA-TS operational states is defined:

- NP (No Power)
- SB (Standby)
- OP (Operational)
- FA (GA-TS Failure)

The Railway SoL Service concept is expected to be quasi-independent of the user concept of operations, using GNSS augmentation in a technology-neutral manner.

The GNSS Augmentation System shall also be independent from receiver suppliers.

A Minimum Operational Performance Standard for GNSS Augmentation On-board Equipment (GA-OB MOPS) is recommended to be developed.

It has to be noted that it is foreseen only the use of Pseudorange and Carrier Smoothing processing at the GA-OB.

As well known, the Kalman Filter can underestimate the covariance matrix elements or not able to manage time correlated error, as well as not able to deal with non-Gaussian error distribution. The management of such topics is left to the manufacturer's responsibility.

The computation of the Protection Level depends on the availability of a safety-related interoperable digital track map and error models (Tropospheric corrections, receiver noise, multipath, code-phase Ionospheric divergence).

EGNOS Railway SoL Services have been also defined and are shown in Table GNSS augmentation systems for rail-4.

It is noted the need for an upper bound for time correlation and biases, to be provided by an alternative channel. It has to be remembered that RTCM SC-134 (RTCM, 2024) incorporates such broadcast parameters into the standard.

A similar approach for EGNOS Augmentation Architecture is defined (see Figure GNSS augmentation systems for rail-14), including a GA-MOPS.

The following Open points, of relevance for VICE4Rail, have to be taken into account:

- Development of guidance on the computation of protection levels (along-track and horizontal)
- Degraded modes management
- Support for more than 2 GA message streams
- Validation of SRS.

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

These Open points will be further discussed in the framework of the WP3 solution.

		Hypothetical Service Levels			
Hypothetical commitments on SIS performances		**SL1**	**SL2**	**SL3A**	**SL3B**
Integrity	Detection of fault conditions (Note 1 and 12)	1-2.4E-6 /h	1-2.4E-6 /h	1-2.4E-6 /h	1-2.4E-6 /h
	Bounding of pseudorange error residuals (orbit, clock and ionospheric delay) under fault-free conditions (Note 2 and 3)	1-2.4E-6 /h	1-2.4E-6 /h	1-2.4E-6 /h	1-2.4E-6 /h
	Bounding of pseudorange-rate error residuals (orbit, clock and ionospheric delay) under fault-free conditions (Note 2 and 3)				1-2.4E-6 /h
	Time-to-alert (SBAS to GA-TS) (Note 4)	5.2s	5.2s	5.2s	≤ 5.2s
Accuracy	Pseudorange accuracy (95%) (Note 5)		TBC (pr_acc_1)	TBC (pr_acc_1)	TBC (pr_acc_2)
	Pseudorange-rate accuracy (95%) (Note 6)				TBC
Continuity	Pseudorange continuity risk (Note 7)				TBC
	Pseudorange-rate continuity risk (Note 8)				TBC
Availability	Pseudorange availability (Note 9)			TBC	TBC
	Pseudorange-rate availability (Note 10)				TBC
Enhanced Support for Kalman filtering	Provision of bias values (Note 11)			TBC	TBC
	Pseudorange residual error time correlation bound (Note 11)			TBC	TBC
	Pseudorange-rate residual error time correlation bound (Note 11)			TBC	TBC
Hypothetical mapping of Service Levels to potential future EGNOS Railway SoL Services					
EGNOS L1 Railway SoL Service		X			
EGNOS DFMC Railway SoL Service		X	X		
EGNOS DFMC+ Railway SoL Service		X	X	X	
EGNOS Next Railway SoL Service		X	X	X	X

Table GNSS augmentation systems for rail-4: Hypothetical EGNOS Railway SoL Services (source [55]).

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

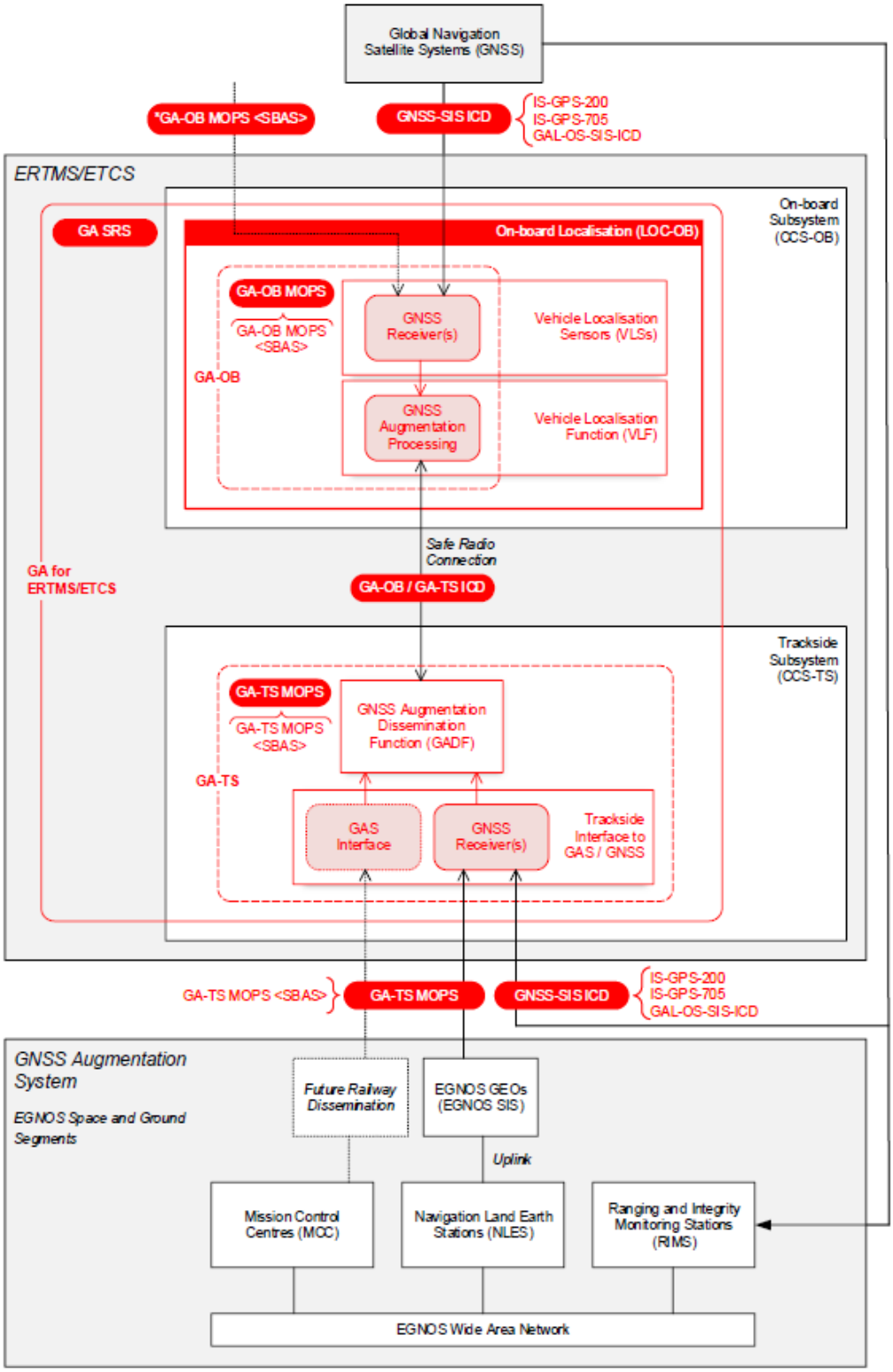

Figure GNSS augmentation systems for rail-14: Architecture and Interfaces of EGNOS Augmentation for ERTMS (source [55]).

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

6.2 The development of an Agnostic System through a Multiple-Tier Approach

A system able to work with multi-layered augmentation data has to be implemented at the augmentation and Receiver side in order to implement the foreseen agnostic concept.

The RTCM SC-134 is currently foreseen an approach that is technology agnostic and allows the calculation of the Protection Level through generalized integrity overbounding parameters and integrity flags.

The Integrity Monitoring Systems are divided by the following classes:

- User-Based approach: the user is in charge of Integrity Monitoring and can integrate Augmentation System information
- Missed Integrity Approach: the user integrates Local Integrity Monitoring, through its own algorithms, and Augmentation driven data
- Augmentation-Centric approach: the user has not Integrity Monitoring capabilities and fully relies on Integrity Flags (e.g. constellation, satellite and frequency alerts) transmitted by the Augmentation System

Such an approach allows meeting user receiver technology for High accuracy and High Integrity positioning and implementing several Rail constraints described into section 6.1.

Transmitted Integrity Parameters include:

- Overbounding standard deviation
- Overbounding biases
- MFD (Mean Fault Duration)
- Time correlation
- Visibility Maps and Local Multipath Model parameters

Continuity parameters are linked, through appropriate ranges, to the same parameters.

Starting from such an approach, a multiple service level system can be derived. The possible allocations are shown in Table GNSS augmentation systems for rail-5.

Tier Id	Technology	Scope	Accuracy	Integrity
4	Galileo HAS SL1, PPP	Integrity Monitoring	10 cm (20-20 min convergence)	10^{-4}/h
3	EGNOS	High Accuracy, Global Integrity Monitoring	< 1m	10^{-7}/150 s
2	DGNSS	High Accuracy, Global Integrity Monitoring	< 1m	10^{-7}/h
1	RTK, NRTK, PPP-RTK, Galileo HAS SL2 (TBC)	High Accuracy, Local Integrity Monitoring	< 10 cm	10^{-9}/h

Table GNSS augmentation systems for rail-5: Multitier Technology Allocation.

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

For the Protection Level calculation, a generalized definition and approach can be derived from the ARAIM upper bound equations. The communication protocol is TCP/IP, through the NTRIP definition. The messages transmitted by the Augmentation System can therefore by transmitted to the GA-TS through RTCM NTRIP protocol and RTCM SC 104 and RTCM SC 134 standards.

The GAS/GA-TS adapter has therefore to be based on the GA-TS-MOPS definition, containing RTCM general messages on the GAS side. IT is responsible to take such message, extract relevant information and encapsulate them into the rail standard message through the GA-TS/GA-OB interface.

Through this process any COTS receiver can be adapted for working in the VICE4Rail context.

The agnostic GNSS augmentation system for multimodal use will be designed within the framework of WP3 of the VICE4RAIL project entitled “Reference Architecture Design”. Subsequently, the augmentation system will be implemented within the framework of WP4 of the VICE4RAIL project entitled “Hybrid Virtualised Testing Certification Environment Development”. This augmentation system will be used for field testing and laboratory tests of the ASTP like emulator DUT, which will be carried out within the framework of the same WP4.

7. CONCLUSIONS

The main conclusions arising from the comparative analysis described in deliverable D2.4, which should be considered in the safety assessment and certification process in multimodal transport, are as follows.

The railway safety and dependability concept based on the standard EN 50126 (RAMS) does not directly specify continuity requirements for GNSS, but there are very demanding requirements for system reliability, e.g. for ERTMS, as reliability indirectly affects railway safety. European railways aim to use the GNSS 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. Further, it appears that there is no consensus in the automotive industry on the use of GNSS continuity. For example, the current automotive standard ISO/TR 4804 does not recommend using GNSS continuity as the main quality attribute for GNSS-based positioning with integrity. We show in sections 5.3.3 and 5.8 that this recommendation is based on a misunderstanding of the GNSS continuity concept. As railways have the most stringent requirements for system reliability in surface transport, then an MTBF value of $5x10^5$ h, which is required for Advanced Safe Train Positioning (ASTP) for ERTMS, was chosen as the reliability target for GNSS-based positioning – see section 5.3.2.

According to reliability theory, the MTTF of systems can be increased by using redundant architectures. Therefore, in this deliverable, simplified 1oo2 (one-out-of-two) architectures have been analysed, where channel A is represented by the GNSS SoL service with guaranteed continuity for aviation (corresponding to an MTBF of 520.83 h) and channel B is implemented by e.g. IMU. The reliability of the GNSS receiver and antenna, which is several times greater than the reliability of the SoL service, has been neglected for simplicity in this analysis. Systems of differential linear equations based on Markov models of the corresponding architectures, the Laplace transform, and the limit theorem were used to numerically solve the mean time to system failure ($MTTF_{sys}$). The numerical results of $MTTF_{sys}$ presented in section 5.5 demonstrate that redundant architectures when using aviation GNSS SoL service will enable to meet the high reliability requirements of railways for safe GNSS-based train localization.

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

8. REFERENCES

[1] Brinkmann, M., Bode, E., Lamm, A., Maelen, S. V. and Halm, A. Learning from Automotive: Testing Maritime Assistance Systems up to Autonomous Vessels. In *Proc. of OCEANS 2017, Aberdeen, UK, 19-22 June (2017)*. Available: https://www.researchgate.net/publication/318983781_Learning_from_Automotive_Testing_Maritime_Assistance_Systems_up_to_Autonomous_Vessels (Accessed 10 March 2025).

[2] ISO 17894 Ships and marine technology — Computer applications — General principles for the development and use of programmable electronic systems in marine applications. International standard (2005). Note: This publication was last reviewed and confirmed in 2024.

[3] D2.7 Identification of the validation certification methods. Deliverable of the H2020 project CLUG – Certifiable Localisation Unit with GNSS in the railway environment (2021). Available: https://clugproject.eu/en/deliverables (Accessed 24 Jan 2025).

[4] D5.4 EGNSS Services Evolution for railways and ETCS impacts. Deliverable of the H2020 project STARS – Satellite Technology for Advanced Railway Signalling (2018). Available: https://www.stars-rail.eu/results-publications/ (Accessed 24 Jan 2025).

[5] D3.1 System Requirement Specification of the Fail-Safe Train Positioning Functional Block. Deliverable of the Shift2Rail project X2RAIL-2 - Enhancing railway signalling systems based on train satellite positioning, on-board safe train integrity, formal methods approach and standard interfaces, enhancing Traffic Management System functions (2020). Available: https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-2 (Accessed 24 Jan 2025).

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

[7] Mauer, M. et al. *Autonomous Driving: Technical, Legal and Social Aspects*. 457-458 (Springer Open 2016).

[8] 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).

[9] 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).

[10] Moore, T. & Monteiro, L. S. Maritime DGPS: Ensuring the Best Availability and Continuity. *J. of Navigation*, **55**, 485-494 (2002).

[11] 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).

[12] EN IEC 61508 1-7 (2010): Functional safety of electrical/ electronic/ programmable electronic safety-related systems, European standard.

[13] ISO 26262 (1-12) *Road vehicles – Functional safety.* International Organization for Standardization (ISO), international standard (2018).

[14] EN 50129 *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling.* European CENELEC standard (2019).

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

[15] EN 50126-1 *Railway Applications: The Specification and Demonstration of Dependability Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process.* European CENELEC standard (2017).

[16] EN 50126-2 *Railway Applications: The Specification and Demonstration of Dependability Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety.* European CENELEC standard (2017).

[17] EN 50716 *Railway applications – Requirements for software development.* European CENELEC standard (2023).

[18] 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.

[19] ISO/PAS 21448 *Road Vehicles – Safety of the intended functionality (SOTIF).* International standard (2019).

[20] UL 4600: Standard for safety – Evaluation of Autonomous Products. *American National Standard*, 2020.

[21] ISO/TR 4804 *Road vehicles – Safety and cybersecurity for automated driving systems - Design, verification and validation.* International Organization for Standardization (ISO), technical report (2020).

[22] 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).

[23] Report on Aviation User Needs and Requirements. Outcome of the EUSPA User Consultation Platform. Reference: EUSPA-MKD-AV-UREQ-250287 (01/08/2021). [Online]. Available: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Report_on_User_Needs_and_Requirements_Aviation.pdf (Accessed 1 Nov 2023).

[24] Pullen, S. Augmented GNSS: Fundamentals and Keys to Integrity and Continuity. ION GNSS tutorial (2012). [Online]. Available: http://www-leland.stanford.edu/~spullen/ION12_tutorial.pdf (Accessed 1 Nov 2023).

[25] EGNOS Safety of Life (SoL) Service Definition Document. EUSPA, Issue 3.4 (2021). [Online]. Available: https://egnos-user-support.essp-sas.eu/sites/default/files/documents/egnos_sol_sdd_in_force.pdf (Accessed 1 Nov 2023).

[26] Radio Technical Commission for Aeronautics (RTCA). *Minimum Aviation System Performance Standards for Global Positioning System / Wide Area Augmentation System Airborne Equipment*. RTCA standard DO-229 D, Washington DC (2006).

[27] 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).

[28] Report on Rail User Needs and Requirements. Outcome of the EUSPA User Consultation Platform. Reference: GSA-MKD-RL-UREQ-250286 (2021). [Online]. Available: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Report_on_User_Needs_and_Requirements_Rail.pdf (Accessed 1 Nov 2023).

[29] Report on Maritime and Inland Waterways User needs and Requirements. Outcome of the EUSPA User Consultation Platform. Reference: GSA-MKD-MAR-UREQ-229399 (2021). [Online]. Available: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Report_on_User_Needs_and_Requirements_Maritime.pdf (Accessed 1 Nov 2023).

[30] Report on Road User Needs and Requirements. Outcome of the EUSPA User Consultation Platform. Reference: GSA-MKD-RD-UREQ-250283 (2021). [Online]. Available: https://www.gsc-

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

europa.eu/sites/default/files/sites/all/files/Report_on_User_Needs_and_Requirements_Road.pdf (Accessed 1 Nov 2023).

[31] 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).

[32] Klepsvik, J. O., Ober, P. B. & Baldauf, M. A critical look at the IMO requirements for GNSS. In *Proc. of the ION GNSS 20th Int. Technical Meeting,* 1931-1942, Fort Worth, Texas, USA, 25-28 Sept (2007). [Online]. Available: https://www.researchgate.net/publication/270898744_A_critical_look_at_the_IMO_requirements_for_GNSS (Accessed 1 Nov 2023).

[33] Filip, A., Beugin, J. & Marais, J. Interpretation of the Galileo Safety-of-Life Service by Means of Railway RAMS Terminology. *Trans. Transp. Sci.* **1**(2), 61-68 (2008). [Online]. Available: https://tots.upol.cz/pdfs/tot/2008/02/02.pdf (Accessed 1 Nov 2023).

[34] Kovach, K. Continuity: The Hardest GNSS Requirement of All. In *Proc. of the ION GPS-98*, 2003-2020, Nashville, Tennessee, USA, 5-18 Sep (1998).

[35] Petovello, M. & S. Pullen. GNSS Solutions: Quantifying the performance of navigation systems and standards for assisted-GNSS. *Inside GNSS*, 20-22, Sept/Oct (2008). [Online]. Available: https://www.insidegnss.com/auto/sepoct08-gnsssolutions.pdf (Accessed 1 Nov 2023).

[36] Porretta, M., Banos, D. J., Crisci, M., Solari, G. & Fiumara, A. GNSS Evolutions for Maritime: An Incremental Approach. *Inside GNSS*, 54-62, May/June (2016). [Online]. Available: https://insidegnss-com.exactdn.com/wp-content/uploads/2018/01/mayjune16-WP.pdf (Accessed 1 Nov 2023).

[37] Specification for ILS - Instrument Landing System. Specification of NAVAIDS High Standard (2006). [Online]. Available: https://www.etenders.gov.za/home/Download/?blobName=15405005-43e5-41b0-9263-5e7ae4267505.pdf&downloadedFileName=Appendix%20A%20-%20ILS%20Spec.pdf (Accessed 1 Nov 2023).

[38] International Maritime Organization (IMO). *IMO Resolution A.1046 (27) Worldwide Radionavigation System*. UK (2011). [Online]. Available: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.1046(27).pdf (Accessed 1 Nov 2023).

[39] D5.3 EGNSS Target Performances to meet railway safety requirements. *Deliverable of the H2020 project STARS – Satellite Technology for Advances Railway Signalling* (2017). [Online]. Available: http://www.stars-rail.eu/wp-content/uploads/2018/07/STR-WP5-D-ANS-034-07_-_D5.3_-_EGNSS_Target_Performances_to_meet_railway_safety_requirements_.pdf (Accessed 1 Nov 2023).

[40] Deliverable 3.2. GNSS Quantitative Analysis for ERTMS GGC Project. *Deliverable of the H2020 project ERSAT GGC - ERTMS on Satellite Galileo Game Changer* (2018). [Online]. Available: https://hal.science/hal-02096596/document (Accessed 5 Nov 2023).

[41] ERTMS/ETCS RAMS Requirements Specification. Chapter 2 – RAM. ERMTS Users Group, UIC Reference No.: 96S126 (1998). [Online]. Available: https://www.yumpu.com/en/document/read/47232494/ertms-etcs-rams-requirements-specification-chapter-2-ram (Accessed 1 Nov 2023).

[42] Subset-036. ERTMS/ETCS FFFIS for Eurobalise. UNISIG, Issue 3.1.0 (2015). [Online]. Available: https://www.era.europa.eu/system/files/2023-01/sos3_index009_-_subset-036_v310.pdf (Accessed 1 Nov 2023).

[43] Mahboob, Q. & Zio, E. *Handbook of RAMS in Railway Systems: Theory and Practice.* 414-418 (CRC Press Taylor and Francis Group, 2018).

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

[44] Kalvakunta, R. G. Reliability Modelling of ERTMS/ETCS. Norwegian University of Science and Technology (NTNU), Master Thesis (2017). [Online]. Available: https://extendsim.com/images/downloads/academic/grants/kalvakunta-paper.pdf (Accessed 23 Jan 2025).

[45] Hargreaves, C. & Williams, P. Maritime Integrity Concept. In *Proc. of the European Navigation Conference ENC 2018*, 120-127, Gothenburg, Sweden, 14-17 May (2018).

[46] Rausand, M. & Hoyland, A. *Markov Processes in System Reliability Theory: Models, Statistical Methods, and Applications*, 2nd ed., 301-359 (John Wiley & Sons, 2024).

[47] Subset-088. ERTMS/ETCS – Class 1, ETCS Application Levels 1 & 2 – Safety Analysis, Pert 3 – THR Apportionment. UNISIG issue 3.7.0 (2019). [Online]. Available: https://www.era.europa.eu/era-folder/informative-set-specifications-3-etcs-b3-r2-gsm-r-b1 (Accessed 1 Nov 2023).

[48] Kilian, P. et all. Safety-Related Availability in the Power Supply Domain. *IEEE Access 10, 47869-47880 (2022).* Available: https://ieeexplore.ieee.org/document/9765464 (Accessed 4 Feb 2025).

[49] Goble, W. M. *Controls Systems Safety Evaluation & Reliability*. 2nd ed., 151-173 (ISA – The Instrumentation, Systems, and Automation Society, 1998).

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

[51] EN 60300-1 Dependability management – Part 1: Dependability management systems. The European standard (2003).

[52] prEN50126 Railway Applications: The specification of Dependability – Reliability, Availability, Maintainability and Safety (RAMS). Draft European standard (1995).

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

[54] ISO/SAE 21434 Road vehicles — Cybersecurity engineering. International standard (2021).

[55] EEIG ERTMS Users Group, GNSS Augmentation for ERTMS/ETCS – System Requirements Document, EUG Solution for Enhanced Onboard Localisation Change Request (CR1368) – GNSS Augmentation for ERTMS/ETCS, (ERTMS 2023).

[56] RTCM SC-134 “Integrity for GNSS-based High Accuracy Applications” v 0.1”, draft release.

[57] RTCM 10403, “Differential GNSS (Global Navigation Satellite Systems) Services” (2006).

[58] Yamada, H. IMO and the GNSS. Inside GNSS, pp. 40-44, Sept/Oct (2017). Available: https://insidegnss.com/imo-and-the-gnss/ (Accessed 24 March 2025).

[59] 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.

[60] Brinkmann, M., Böde, E., Lamm, A., Maelen, S. V. and Hah, A. Learning from Automotive: Testing Maritime Assistance Systems up to Autonomous Vessels. In Proc. of the OCEAN ‘2017 MTS/IEEE conference, Aberdeen, UK (2017). Available: https://www.researchgate.net/publication/318983781_Learning_from_Automotive_Testing_Maritime_Assistance_Systems_up_to_Autonomous_Vessels (Assessed: 21 March 2025).

[61] ISO 17894 Ships and marine technology - Computer applications - General principles for the development and use of programmable electronic systems in marine applications. International standard (2005). Note: This publication was last reviewed and confirmed in 2024. Therefore, this version remains current.

[62] D21.1 Operational needs and system capabilities of an ASTP system (Use Cases). Deliverable of the Europe’s Rail FP2-R2DATO project, p. 88, November 15, 2024.

[63] D2.1 Rail user & system requirements. Deliverable of the Horizon Europe VICE4RAIL project, 31/03/2025.

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

[64] United Nations Regulation No. 79 on Uniform provisions concerning the approval of vehicles with regard to steering equipment, with effect from 29 January 1989. Annexed to the Agreement of 20 March 1958 concerning the adoption of uniform conditions of approval and reciprocal recognition of approval for motor vehicle equipment and parts - done at Geneva, on 20 March 1958.

[65] Addendum 78: 'Regulation No. 79 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of vehicles with regard to steering equipment Revision 2'. Date of entry into force: 4 April 2005, Corrigendum 20 January 2006, 51 pages.

[66] 97/836/EC 'Revised 1958 Agreement'. UN ECE Agreement concerning the adoption of uniform technical prescriptions for wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles and the conditions for reciprocal recognition of approvals granted on the basis of these prescriptions.

[67] 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) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC.

[68] Frost, B.: 'Automated Driving UNECE International Harmonization'. Presentation 2018, 12 slides.

[69] Edwards, M., Seidl, M., Tress, M. et al.: 'Study on the assessment and certification of automated vehicles'. European Commission Final Report, published by EU (EC Unit C.4 – Automotive and mobility Industries) in 2017, 111 pages.

[70] Report 'Assessment of Safety Standards for Automotive Electronic Control Systems'. U.S. Department of Transportation, NHTSA, Ref. No. DOT HS 812 285, June 2016.

[71] Koopman, P., Wagner, M.: 'Transportation CPS Safety Challenges'. NSF Workshop on Transportation Cyber Physical Systems, Arlington, Virginia, USA, Jan 23-24, *2014*, 3 pages.

[72] Parent, M., Tona, P., Csepinszky, A. et al.: 'Legal issues and certification of the fully automated vehicles: best practices and lessons learned'. Project EU CityMobil2, 7th FP, Deliverable No. D26.1, June 11, 2013, 59 pages.

[73] Koopman, P. and Wagner, M.: 'Autonomous Vehicle Safety: An Interdisciplinary Challenge'. IEEE Intelligent Transportation Systems Magazine, Vol. 9, No. 1, 2017, pp. 90-96.

[74] International Transport Forum. Report 'Automated and Autonomous Driving, Regulation under uncertainty'. OECD /ITF 2015, 33 pages.

[75] Lång, K. E: 'Collaborative Approach Needed For Big Business'. Innovation Bazaar, RISE Viktoria, Vehicle ICT Arena 2018-02-08, 20 slides.

[76] Lutz, L., S.: 'Automated Vehicles in the EU: Proposals to Amend the Type Approval Framework and Regulation of Driver Conduct'. General Reinsurance AG, March 2016, 7 pages.

[77] Hommes, V. E.: 'Assessment of safety standards for automotive electronic control systems'. Report No. DOT HS 812 285. Washington, DC: National Highway Traffic Safety Administration, June 2016, 30 pages + Appendix.

[78] Canis, S.: 'Issues in Autonomous Vehicle Deployment'. Congressional Research Service, Sept 5, 2017,10 pages. https://fas.org/sgp/crs/misc/R44940.pdf

[79] Directive 2007/46/EC of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles.

[80] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems.

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

[81] Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles.

[82] Final Book. *Deliverable of the H2020 project STARS – Satellite Technology for Advances Railway Signalling* (2017). [Online]. Available: https://www.stars-rail.eu/wp-content/uploads/2019/08/D7.5_Final-Book.pdf (Accessed 23 July 2025).

[83] D3.1 System Requirement Specification of the Fail-Safe Train Positioning Functional Block. Deliverable of the Shift2Rail project X2Rail-2 (2017). Available: https://projects.shift2rail.org (Accessed 23 July 2025).

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