Horizon 2020
European Union Funding
for Research & Innovation

European
Global Navigation
Satellite Systems
Agency

D2.3 SYSTEM REQUIREMENTS SPECIFICATION

Due date of deliverable: 01/06/2020

Actual submission date: 01/06/2020

Leader/Responsible of this Deliverable: Aleš Filip (UPA)

Reviewed (Y/N): Y

Document status		
Revision	**Date**	**Description**
01	01/06/2020	1st Official Release

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: 02/01/2020 Duration: 24 months

This project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No 870257

CONTRIBUTING PARTNER

Name	Company	Roles/Title
Aleš Filip	**UPA**	WP2 Leader & Contributor
Filip Holík	UPA	Contributor
Alessandro Neri	RDL	Contributor
Maurizio Salvitti	RDL	Contributor
Cesare Dionisio	RDL	Contributor
Panagiotis Xefteris	RDL	Contributor
Pietro Salvatori	RDL	Contributor
Roberto Capua	SGI	Contributor
Luca Gattuso	SGI	Contributor
Manuele Innocenti	SGI	Contributor
Marco Giangolini	SGI	Contributor
Anja Grosch	DLR	Contributor
Omar Garcia Crespillo	DLR	Contributor
Chen Zhu	DLR	Contributor
Ondrej Kutik	RBA	Contributor
Miroslav Krajíček	RBA	Contributor
Michael Loupis	ITC	Contributor
John Spanoudakis	ITC	Contributor

DISTRIBUTION LIST

Name	Company	Roles/Title
Alessandro NERI	RDL	Project Coordinator
Daniel LOPOUR	GSA	GSA Programme Officer
Aleš Filip	UPA	WP2 Leader
Anja Grosch	DLR	WP3 Leader
Ondrej Kutik	RBA	WP4 Leader
Pietro Salvatori	RDL	WP5 Leader
Roberto Capua	SGI	WP6 Leader

APPROVAL STATUS

Document Code	Rev.	Role	Approved	Authorised	Date
HELMET_D2.3	01	WP2 Leader	A.Filip (UPA)	-	01/06/2020
		Coordinator	A.Neri (RDL)	A.Neri RDL)	01/06/2020

EXECUTIVE SUMMARY

This document is the deliverable **D2.3 System Requirement Specifications** (with traceability matrix) which describes systems requirements for HELMET (High integrity EGNSS Layer for Multimodal Eco-friendly Transportation) solution from viewpoint of high-accuracy and high-integrity EGNSS applications in rail (RAIL) and automotive (AUTO) sectors. The HELMET is mainly focused on ERTMS and automated car driving and supported by Unmanned Aerial Vehicles and Systems (UAV, UAS) in terms of infrastructure inspection, infrastructure assets monitoring, traffic management, etc.

The main HELMET objectives are: 1) to develop a cyber-secured multimodal, multi-sensor integrity monitoring architecture based on EGNSS to introduce High Integrity Location Determination System (LDS) for trains, automobiles and Unmanned Aerial Systems (UAS/RPAS) automation with the later aggregating the demand of IMTM (Inspection, Monitoring and Traffic Management) for rail and road assets and operations, 2) to assess the system performance by a Proof-of-Concept (PoC), and finally 3) to draw a roadmap for exploitation and future standardization and certification of HELMET results in terms of (a) the designed multi-modal augmentation and integrity monitoring architecture, and (b) high integrity and accuracy OBU algorithms fully customized for land transportation (rail and road) and supporting aerial operations.

The system requirement specifications started from the HELMET WP2 CONOPS (Concept of Operations) delivered within the D2.2 document and used for definition and justification of high-level user requirements for RAIL, AUTO and UAV user groups. The purpose of the HELMET CONOPS was to describe the operational needs, views, visions, expectations and high-level requirements of the user's groups without provision of technical details on HELMET. On the contrary, the intention of this deliverable (D2.3) was to specify detailed technical requirements needed for the HELMET Architecture Design, which is the subject of the Work Package 3.

The System Requirements Specification process employed within the HELMET Task 2.2. was based on following activities:

- HELMET CONOPS development;
- High-level User Requirements specification (as a result of CONOPS);
- Identification of general constrains and limitations;
- Specification of Logical Concepts and Models for the User's groups;
- Safety analysis for the Logical Concepts for multi-modal applications;
- Development of Requirements Traceability Matrices (RTMs) for the maim HELMET User's groups (RAIL, AUTO, UAVs);
- Description and justification of individual Systems Requirements;
- Specification of Systems Requirements for High-Level HELMET architecture.

The Requirements Traceability Matrices for the individual user's groups were developed for mapping links and dependences between the high-level User Requirements (D2.1) and the System Requirements in order to facilitate, make transparent and justify the System Requirements Specification process.

The specified System Requirements are summarised in Section 5. Section 6 outlines a high-level HELMET architecture with the key safety measures. The architecture will be further developed in detail within WP3. The related RTMs for RAIL, AUTO and UAVs applications and GNSS Augmentation are included in Section 7.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

DEFINITIONS AND ABBREVIATIONS

Acronym	Description
ABAS	Air Borne Augmentation System
ACSF	Automatically Commanded Steering Functions
ADS-B	Automatic Dependent Surveillance—Broadcast
AEC	Airspace Encounter Category
AG	Air-Ground
AGL	Above Ground Level
AIMN	Augmentation and Integrity Monitoring Network
AL	Alert Limit (defined by user)
ALARP	As Low As Reasonably Practicable
ANSP	Air Navigation Service Provider
ARAIM	Advanced Receiver Autonomous Integrity Monitor
ARC	Air Risk Class
ASIL	Automotive Safety Integrity Level
AT	Along Track (or longitudinal)
ATC	Air Traffic Control
ATC/UTM	Air Traffic Control / Unmanned Aircraft System Traffic Management
ATM	Air Traffic Management
AWR	Airborne Weather Radar
BER	Bit Error Rate
BG	Balise Group
BHT	Balanced Histogram Thresholding
BLOS	Beyond Line-Of-Sight
BRLOS	Beyond Radio Line-Of-Sight
BVLOS	Beyond Visual Line Of Sight
BTM	Balise Transmission Module
BTX	Balise Transmission
CAA	Civil Aviation Authority
CAN	Controller Area Network
CENELEC	Comité Européen de Normalisation Électrotechnique
CCS	Control Command and Signalling
CCS TSI	Control Command and Signalling Technical Specifications for Interoperability
COM	Wider range communication / Communications
CON	Control
CONOPS	Concept of Operations
CoP	Codes of Practice
COTS	Commercial Off-The-Shelf
CNPC	Control and Non-Payload Communications
CS-LURS	Certification Specification for Light Unmanned Rotorcraft Systems
CSM	Common Safety Method
CSM-DT	Common Safety Method Design Targets
CSM-RA	Common Safety Method for Risk evaluation and Assessment

CST	Common Safety Targets
CT	Cross-Track (or lateral)
DAA	Detection And Avoidance
DB	Track Database
DEM	Digital Elevation Model
DMI	Driver Machine Interface
DOP	Dilution of Precision
DTE	Driving Technical and control Error
E/E/PE	Electrical/Electronic/Programmable Electronic
EASA	European Aviation Safety Agency
EC	European Commission
ECAC	European Civil Aviation Conference
EDAS	EGNOS Data Access Service
EGNOS	European Geostationary Navigation Overlay Service, i.e. European SBAS
EGNSS	European GNSS
EMI	Electro-magnetic interference
ENU	East-North-Up (A local geodetic east-north-up reference frame)
ENV	Environment
ERA	The European Union Agency for Railways
ERSAT GGC	ERTMS on SATellite – Galileo Game Changer
ERTMS	European Rail Traffic Management System
ESA	European Space Agency
ETCS	European Train Control System
EU	European Union
EVLOS	Extended Visual Line of Sight
FAA	Federal Aviation Administration
FAB	Function B (in composite fail-safety)
FCU	Flight Control Unit
FDIR	Fault Detection, Isolation and Recovery
FOV	Field of View
FTA	Fault tree Analysis
GA	General Aviation
GAD/TV	GNSS Augmentation Dissemination/ Trackside Verification
Galileo	European GNSS
GAMAB	Globalement Au Mois Aussi Bon
GBAS	Ground Based Augmentation System
GCP	Ground Control Points
GCS	Ground Control Station
GCS/RPS	Ground Control Station / Remote Pilot Stations
GEO	Geostationary Earth Orbit satellite
GIS	Geographic Information System
GIVE	Grid Ionospheric Vertical Error
GNSS	Global Navigation Satellite System
GNSS Rx (rx)	GNSS Receiver
GNSS SIS	GNSS Signal-in-Space

GNSS SoL	GNSS Safety of Life (service)
GNSS UCP	GNSS User Consultation Platform (organized by GSA in Prague)
GPS	Global Positioning System
GRC	Ground Risk Class
GSA	European Global Navigation Satellite Systems Agency
GSC	European GNSS Service Centre
GSM-R	Global System for Mobile Communications – Railway
HAP / HAPS	High-Altitude Platform(s)
HAS	High Accuracy Service
HD	High Definition
HELMET	High integrity EGNSS Layer for Multimodal Eco-friendly Transportation
HF	Human Factor
HNSE	Horizontal Navigation System Error
HPL	Horizontal Protection Level
HSV	Hue Saturation Value
HV-AL THR	High Vertical Alert Limit THR
HW	Hardware
LDS	Location Determination System
ICAO	International Civil Aviation Organization
I/F	Interface
IFR	Instrument Flight Rules
IGS	International GNSS Service
ILS	Integrated Logistic Support
IMC	Instrumental Meteorological Conditions
IMTM	Inspection, Monitoring and Traffic Management
IMTM-UA/RPA	Inspection, Monitoring and Traffic Management + Unmanned Aircraft/ Remotely Piloted Aircraft
IMTM UAS/RPAS-PIT	Inspection, Monitoring and Traffic Management + Unmanned Aircraft System / Remotely Piloted Aircraft Systems. In this PIT station the UA/RPA can land and refuel batteries based for instance on a non-contact equipment.
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
IOC	Intelligent Orientation Control
IP	Information Point (in ETCS)
IR	Integrity Risk
IRC	Inter RPAS Communication
ISM	Integrity Support Messages
IT	Information Technology
ITS	Information Transportation System
ITU	International Telecommunication Union
JARUS	Joint Authorities on Rulemaking for Unmanned Systems
LEO	Low Earth Orbit Satellite
LDS	Location Determination System
LiDAR	Light Detection and Ranging
LOC	Localization

LOS	Line of Sight
LR	Local Roads (scenario)
LV-AL THR	Low Vertical Alert Limit THR
MAP	Map (for automated car driving)
MEM	Minimum Endogenous Mortality
MOBU	Multi-sensor On-Board Unit platform
MTBF	Mean Time Between Failure
MTGW	Maximum Take-off Gross Weight
MTOM	Maximum Take-off Mass
NAVAIDS	Navigational Aids
NCR	Narrow & Curved Roads (scenario)
NGTC	New Generation Train Control
NLOS	Non-line-of-sight reception
NP	No Power
NPA	Non-Precision Approach
NRTK	Network RTK
NSE	Navigation System Error
NTRIP	Networked Transport of RTCM via Internet Protocol
OBU	On-Board Unit
OC	Odometry Calibration
OPS	Operational
OSO	Operational Safety Objectives
OTH	Other (functions)
PDE	Path Definition Error
PE	Position Error
PF	Probability of Failure (average) per 1 hour
PIT-Station	On ground Service Station
PL	Protection Level
PLA	Planning (route)
PoC	Proof-of-Concept
PoF	Probability of Fatality
POS	Position determination
PPP	Precise Point Positioning
PPS	Pulse Per Second
PSD	Power Spectrum Density
PVT	Position, Velocity, Time
RAC	Risk Acceptance Criteria
RAIM	Receiver Autonomous Integrity Monitor
RAM	Reliability, Availability, Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RBC	Radio Block Centre
RC	Remote Control
RCC	Regulatory Cooperation Council
RCP	Required Communications Performance
RF	Radio Frequency
RHINOS	Railway High Integrity Navigation Overlay System – H2020 project

RIMS	Ranging Integrity Monitoring Stations
RLOS	Radio Line-Of-Sight
RLP	Required Link Performance
RP	Remote Pilot
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft Systems
RPS	Remote Pilot Stations
RS	Reference Station network
RTS	Real-Time Service
RTCA	Radio Technical Commission for Aeronautics
RTCM	Radio Technical Commission for Maritime Services
RTH	Return-to-Home
RTK	Real Time Kinematics
RTM	Requirements Traceability Matrix
RTX	Radio Transmission (in ETCS)
SAIL	Specific Assurance and Integrity Levels
S&A	Sense and Avoid
SAR	Search and Rescue
SAT	Satellite
SBAS	Satellite Based Augmentation System: e.g.: EGNOS, WAAS, MSAT, SDCM, GAGAN
SDC	Self-Driving Car
SDR	Software-Defined Radio
SEN	Sensing (environment)
SESAR	Single European Sky ATM Research
SIL	Safety Integrity Level
SIS	Signal-In-Space
SOM	Start of Mission
SORA	Specific Operational Risk Assessment
SSR	State Space Representation
STK	Satellite Tool Kit
SYS	System
SW	Software
TFR	Traffic Fatality Rate
THR	Tolerable Hazard Rate
TI	Track Identification (discrimination)
TIR	Target Individual Risk
TLC	Telecommunications
TMPR	Tactical Mitigation Performance Requirements
TMS	Traffic Management System
TOT	Totally
TOW	Take off Weight
TS	Track Spacing
TSE	Technical System Error
TSI	Technical Specifications for Interoperability
TSO	Technical Standard Order

TTA	Time-To-Alert
TX	Transmission (in ETCS)
UA	Unmanned Aircraft
UA/ RPA	Unmanned Aircraft/ Remotely Piloted Aircraft
UAS	Unmanned Aircraft System
UAS/RPAS	Unmanned Aircraft System / Remotely Piloted Aircraft Systems
UAS/RPAS-PIT	Unmanned Aerial System/Remotely Piloted Aerial System-PIT Station(s). In this PIT station the UA/RPA can land and refuel batteries based for instance on a non-contact equipment.
UAV	Unmanned Aerial Vehicle
UAV/RPAS	Unmanned Aerial Vehicle / Remotely Piloted Aircraft Systems
UCP	User Consultation Platform
UIC	Union Internationale des Chemins de fer (International Union of Railways)
UDRE	User Differential Range Error
UPS	Uninterruptible Power Supply/Source
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VB	Virtual Balise
VBN	Visual Based Navigation
VBR	Virtual Balise Reader
VBTM	Virtual Balise Transmission Module
VBTS	Virtual Balise Transmission System
VCM (VMC)	Visual Meteorological Conditions
VLOS	Visual Line Of Sight
UTM	Unmanned Aircraft System Traffic Management; UAV Traffic Management
VFR	Visual F light Rules
VHF	Very High Frequency
VHL	Very High Level flights
VLL	Very Low Level
VTOL	Vertical Take-Off and Landing

1. INTRODUCTION

The purpose of the deliverable **D2.3 System Requirement Specifications** (with traceability matrix) is to define systems requirements for HELMET (High integrity EGNSS Layer for Multimodal Eco-friendly Transportation) solution from viewpoint of high-accuracy and high-integrity EGNSS applications in rail (RAIL) and automotive (AUTO) sectors. The HELMET is mainly focused on ERTMS and automated car driving and supported by Unmanned Aerial Vehicles and Systems (UAV, UAS) in terms of infrastructure inspection, infrastructure assets monitoring, traffic management, etc. The specified system requirements are needed for the HELMET Architecture Design, which is the subject of the Work Package 3.

The scope of the system requirements specification process performed within the HELMET WP2, task T2.2 is outlined in Figure 1. As it is evident from Figure 1, the system requirements result from User Requirements, Functional User Requirements and also from preliminary architectures and related functional and safety concepts for RAIL, AUTO and UAVs applications.

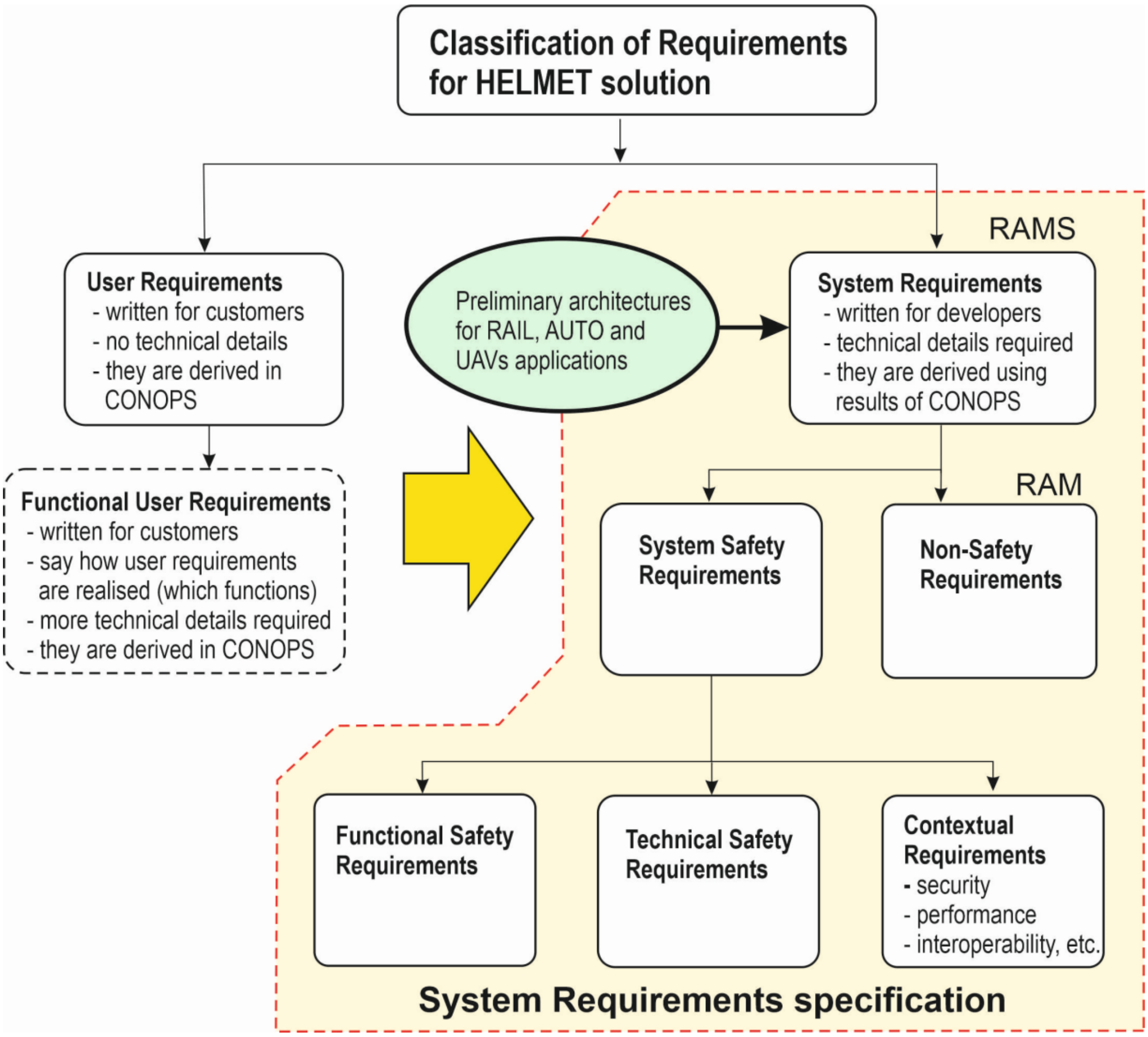

Classification of Requirements for HELMET solution
RAMS
User Requirements
- written for customers
- no technical details
- they are derived in CONOPS
Preliminary architectures for RAIL, AUTO and UAVs applications
System Requirements
- written for developers
- technical details required
- they are derived using results of CONOPS
Functional User Requirements
- written for customers
- say how user requirements are realised (which functions)
- more technical details required
- they are derived in CONOPS
RAM
System Safety Requirements
Non-Safety Requirements
Functional Safety Requirements
Technical Safety Requirements
Contextual Requirements
- security
- performance
- interoperability, etc.
System Requirements specification

Figure 1. Scope of System Requirements Specification process for HELMET

The specification process starts from the already elaborated User Requirements Specifications described in HELMET D2.1 [1] and HELMET CONOPS (Concept of Operations) described in HELMET D2.2 [2]. The purpose of the HELMET CONOPS was to describe the operational needs, views, visions, expectations and high-level requirements of the user's groups without provision of technical details on HELMET. On the contrary, the intention of this deliverable (D2.3) is to specify detailed technical requirements needed for the HELMET Architecture Design (in WP3) and Proof-of-Concept (in WP5).

The System Requirements Specification process applied within the HELMET Task 2.2. is based on following activities:

- HELMET CONOPS development;
- High-level User Requirements specification (as a result of CONOPS);
- Identification of general constrains and limitations;
- Specification of Logical Concepts and Models for the User's groups;
- Safety analysis for the Logical Concepts for multi-modal applications;
- Development of Requirements Traceability Matrices for the maim HELMET User's groups (RAIL, AUTO, UAVs);
- Description and justification of individual Systems Requirements;
- Specification of Systems Requirements for High-Level HELMET architecture.

The Requirements Traceability Matrices (RTMs) for the individual user's groups will be developed for mapping links and dependences between the high-level User Requirements (D2.1) and the System Requirements in order to facilitate, make transparent and justify the System Requirements Specification process.

The individual activities of the above proposed System Requirements Specification process applied for the Task T2.2 solution and achieved results are described in sections below.

2. INPUTS TO SYSTEM REQUIREMENTS SPECIFICATION PROCESS

2.1 USER REQUIREMENTS REVIEW

The fundamental starting point for the System Requirements Specification applied in HELMET is represented by the high-level User Requirements, which have been specified in in HELMET D2.1 [1] using the HELMET COONPS described in D2.2 [2]. The high-level User Requirements for HELMET RAIL and AUTO solutions are summarised in Table 1. The high-level User Requirements for speed accuracy related to RAIL and AUTO are described in Table 2. Finally, Table 3 shows a summary of the user requirements for UAS/RPAS as a segment supporting railway and automotive safety applications.

Table 1. Summary of high-level user requirements for HELMET [1]

Application	Operational scenario	Safety Integrity	Accuracy (2*sigma)	Alert Limit (AL)	Time to Alert (TTA)	Availability	Security		Notes	Requirement Code
RAIL	Track identification	Very high (SIL 4)	generally < 1 m across track; more precise estimate 0.7 m	1.785 m across track; AL ~ 5*sigma for GNSS with THR ~ 1e-6/hr assumed	from 10 s to 30 s	High	Very high		Integrity of vertical position not required; 7*sigma (i.e. AL) corresponds to THR of 2.558e-12/ hr [1])	**UR_001**
	Odometry calibration	Very high (SIL 4)	generally < 1 m along track; more precise estimate 0.7 m	1.7 m along track; AL ~ 5*sigma for GNSS with THR~1e-6/hr	< 1 s	High	Very high			**UR_002**
RAIL	Cold Movement Detection	Very high (SIL 4)	< 2 m along track	5 m along track; AL ~ 5*sigma for GNSS with THR~1e-6/hr	< 10 s	High	Very high			**UR_003**
AUTO	Automated driving on highway; velocity 80-130 km/hr	Very high (ASIL D)	< 34 cm lateral [2])	< 75 cm lateral	< 1 s; Timing accuracy < 1 µs	High	Very high		Integrity of vertical position required to confirm road level on multi-level crossing	**UR_004**
	Automated driving on local roads; velocity 60-90 km/ hr	Very high (ASIL D)	< 20 cm lateral [2])	< 45 cm lateral	< 1 s; Timing accuracy < 1 µs	High	Very high			**UR_005**

	Automated driving on narrow and curved roads; velocity 20-60 km/ hr	Very high (ASIL D)	< 9 cm lateral ^{2})	< 20 cm lateral	< 1 s; Timing accuracy < 1 µs	High	Very high			**UR_006**

Note: ^{1}) and ^{2}) are described in HELMET D2.1 [1], Section 4.

Table 2. User requirements related to speed accuracy for HELMET [1]

Application	Requirement for speed accuracy	Requirement Code
RAIL	± 2 km/h for speed lower than 30 km/h, then increasing linearly up to ± 12 km/h at 500 km/h.	**UR_007**
AUTO	• The indicated speed must never be less than the actual speed, i.e. it should not be possible to inadvertently speed because of an incorrect speedometer reading. • The indicated speed must not be more than 110 percent of the true speed plus 4 km/h at specified test speeds. For example, at 80 km/h, the indicated speed must be no more than 92 km/h.	**UR_008**

In order to specify the System Requirements for the multi-modal HELMET solution, it is also necessary (in addition to the above HELMET high-level User Requirements) to:

- identify general constrains and limitations,
- specify logical concepts, models and architectures for the main User's groups (RAIL, AUTO, UAVs),
- identify/ propose the relevant functional and safety concepts,
- perform safety analysis for the logical concepts and
- develop the Requirements Traceability Matrices (RTMs) for the main HELMET User's groups (RAIL, AUTO, UAVs) in order to facilitate, make transparent and justify the System Requirements Specification process.

It is generally known that there are significant differences in the maturity of the GNSS-based logical/ functional concepts for the RAIL (ERTMS), AUTO and UAVs applications including the related user/ functional and systems requirement. The ERTMS Virtual Balise safety concept is the most developed in respect to AUTO and UAVs safety applications. This railway experience is utilized for specifications of system requirements for self-driving cars, as it is shown in sections below.

Table 3. Summary of High-Level UAS/RPAS Requirements for HELMET [1]

UAV Typical Flight Operation (No Specific Mission)/Flight Phase	Accuracy Horizontal 95%	Accuracy Vertical 95%	Integrity	Time-to-Alert	Continuity	Availability	Requirement Code
En-route	3.7 km (2.0 NM)	N/A	1 – 1×10–7/h	5 min	1–1×10–4/h to 1–1×10–8/h	0.99 to 0.99999	**UR_009**
Arrival (Landing)	0.74 km (0.4 NM)	N/A	1 – 1×10–7/h	15 s	1–1×10–4/h to 1–1×10–8/h	0.99 to 0.99999	**UR_010**
Approach, Departure (Take-off)	220 m (720 ft)	N/A	1 – 1×10–7/h	10 s	1–1×10–4/h to 1–1×10–8/h	0.99 to 0.99999	**UR_011**
Field Approach Operations	16.0 m (52 ft)	20 m (66 ft)	1 – 2× 10–7 in any approach	10 s	1 – 8× 10–6 per 15 s	0.99 to 0.99999	**UR_012** **UR_013**
Precision Approach (PIT Station Approach)	16.0 m - 4m	6.0 m to 4.0 m (20 ft to 13 ft)	1 – 2× 10–7 in any approach	6 s	1 – 8× 10–6 per 15 s	0.99 to 0.99999	**UR_014**
SPECIFIC FLIGHT OPERATIONS (RAIL/AUTOMOTIVE)	**ACCURACY HOR**	**ACCURACY VER**	**INTEGRITY**	**TIME-TO-ALERT**	**CONTINUITY**	**AVAILABILITY**	
MONITORING MISSION (RAIL/AUTOMOTIVE)							
Position/Navigation (Urban/Non-Urban)	1 m /10m	1 m /10m	1 – 2× 10–7	1s (HOT)-6s (COLD)	1–1×10–4/h to 1–1×10–8/h	0.95-0.99	**UR_015**
GEO-Awareness	1m	1m	1 – 2× 10–7	1s (HOT)-6s(COLD)	1–1×10–4/h to 1–1×10–8/h	0.95-0.99	
INSPECTION MISSION (RAIL/AUTOMOTIVE)							**UR_016**
Position/Navigation (Urban/Non-Urban)	1 m /10m	1 m /10m	1 – 2× 10–7	1s (HOT)-6s(COLD)	1–1×10–4/h to 1–1×10–8/h	0.95-0.99	**UR_017**
GEO-Awareness	1m	1m	1 – 2× 10–7	1s (HOT)-6s(COLD)	1–1×10–4/h to 1–1×10–8/h	0.95-0.99	**UR_018**
TRAFFIC MANAGEMENT MISSION (RAIL/AUTOMOTIVE)							**UR_019**
Position/Navigation (Urban/Non-Urban)	10m / 30m	10m / 30m	1 – 2× 10–7	1s (HOT)-10s(COLD)	1–1×10–4/h to 1–1×10–8/h	0.95 to 0.99	**UR_020**
GEO-Awareness	1m	1m	1 – 2× 10–7	1s (HOT)-6s(COLD)	1–1×10–4/h to 1–1×10–8/h	0.95 to 0.99	**UR_021**

2.2 SERVICE LEVELS ANALYSIS

A preliminary service level classification has been performed, through the User Requirements analysis review, in order to derive basic Multimodal Service Levels to be provided by HELMET.

The generalized Service Levels are reported in Table 4. Relevant mapping to augmentation and sensor technology is highlighted. Explanations are given in Sections 2.3 and 2.4.

Table 4. Generalised Service Levels

Service Id	**Description**	**Achievable Accuracy 95%***	**Integrity**	**Availability**	**Application**
SL 1	GNSS Single/Multi-Constellation Single-Frequency DGNSS/GBAS, SBAS	2 m AT	THR_{GNSS}~1e-6/hr THR_{TOT}~1e-9/hr AL 5 m AT TTA < 10 s	High	*RAIL* Cold Movement Detection
SL 2	GNSS Multi-Constellation Single/Multi-Frequency RTK Float + GBAS (Galileo HAS****)	< 0.7 m AT/CT	THR_{GNSS}~1e-6/hr THR_{TOT}~1e-9/hr AL_{TI} 1.785 m CT AL_{OC} 1.665 m AT TTA_{TI} 10-30 s TTA_{OC} < 1 s***	High	*RAIL* Track Identification & Odometer Calibration
SL 3	GNSS Multi-Constellation Multi-Frequency RTK Fixed/Float + NRTK (Galileo HAS****)	< 48 cm AT < 34 cm CT	THR_{GNSS}~1e-5/hr THR_{TOT}~1e-8/hr AL_{CT} 75 cm AL_{AT} 1.4 m TTA < 1 s	High	*AUTO* Autonomous driving on highway

SL 4	GNSS Multi-Constellation Multi-Frequency RTK Fixed + NRTK + IMU + other sensors (odometer, camera, LIDAR)	< 22 cm AT (LR) < 20 cm CT (LR) < 10 cm AT (NCR) < 9 cm CT (NCR)**	THR_{GNSS}~1e-5/hr THR_{TOT}~1e-8/hr $AL_{CT/LR}$ 45 cm $AL_{AT/LR}$ 64.5 cm $AL_{CT/NCR}$ 20 cm $AL_{AT/NCR}$ 29 cm TTA < 1 s	High	*AUTO* Autonomous driving on local roads & Autonomous driving on narrow and curved roads

*: accuracy 95% for AT (along-track or longitudinal) and CT (cross-track or lateral)

**: LR stands for Local Roads scenario, NCR stands for Narrow & Curved Roads scenario

***: TI stands for Track Identification scenario, OC stands for Odometer Calibration scenario

****: Currently Galileo HAS is not available and GNSS receivers are not able to decode and apply relevant correction; it is anyway assumed that when available, such Service Level can be met through Galileo HAS if convergence time is suitable

2.3 GENERAL CONSTRAINTS

The most important identified constraint is related to autonomous driving scenarios on local and on narrow & curved roads. The assumed scenarios are: rural, sub-urban, wooded, urban and urban-canyons. Hence the satellite visibility/availability and the Ambiguity Resolution (AR) rate and stability are critical aspects on the OBU side.

This main consideration derived from the performed analysis is the need to integrate different technologies and to have several sensors on board the vehicle, in order to meet the HELMET requirements. Through current technologies, it is possible to meet the most stringent requirements with a maximum of 10 seconds on average in the cases of no correct RTK fix or GNSS outages [3], [4], [5], 6], [7], [8], [46].

Concerning fast convergence PPP-RTK, current technological limitations in terms of time for convergence and accuracy, as well as PPP-Integrity concepts, are still at a research level. Such limitations are a constraint for a massive implementation of such a technology.
Therefore, PPP-RTK will be analysed at theoretical level and relevant implementation not covered during the Pilot phase.

Concerning Galileo HAS (High Accuracy Service) can be considered as an implementation of a global PPP Service. It has to be underlined that a public ICD (Interface Control Document) is currently not available. Current specifications available by conference papers and official documents refers to an accuracy of 20 cm and the possible broadcasting of precise ephemeris, clocks and satellite biases. Relevant analysis is postponed to the availability of the relevant ICD, taking into account different design options for data broadcasting currently under analysis.

2.4 ASSUMPTIONS AND DEPENDENCIES

In order to map the performance achievable through Augmentation and OBU technologies to the HELMET User Requirements, an analysis has been conducted based on [9], [1]. Longitudinal AL (along-track, AT) and accuracies for HELMET scenario has been derived. GNSS technology is considered to be adopted for longitudinal positioning in autonomous driving scenarios, as reported in [1].

Assumptions on road geometry, car dimensions and vehicle velocities stated in [9] are in line with those derived in the HELMET User Requirements document.

For comparison, “Narrow & Curved Roads” has been linked to the “Local Roads” scenario from [9]. Assumptions have been made to meet specifications on Alert Limits and accuracies falling between the “Highway” and “Narrow & Curved Roads” scenarios, for both the longitudinal and lateral directions.

For analysing the achievable standard deviations and relevant accuracies, values of Root Mean Square Errors (RMSE) on the North and East directions derived from [6], [7] have been projected on Along-track and Cross-track directions. The guidelines specified in [9] have been used for deriving the level of accuracy to be guaranteed by HELMET with the relevant safety level through the different positioning solutions for each scenario.

Concerning SL 3 (Service Level), it has to be noted that the RTK fixed/float transition depends on the operational scenario. The highway scenario can be characterized by mainly open-sky conditions, with the obstacles identified in overpasses along the path and in correspondence of road intersections. Considering a vehicle velocity of 80-130 km/h, as done in [1], the obstacles are supposed to lead to tracking losses for a few seconds.

The performed analysis shows that GNSS Multi-Constellation Multi-Frequency integrated with IMU and other sensors (odometer, camera, LIDAR) is needed for meeting SL 4 requirements.

3. LOGICAL MODELS FOR RAIL, AUTO AND UAVs APPLICATIONS

This section contains the preliminary functional decomposition of the system into single high-level functions.

3.1 RAIL: ENHANCED ERTMS FUNCTIONAL ARCHITECTURE

The high-level logical model for RAIL applications considered in HELMET is represented by the enhanced ERTMS functional architecture developed for the Virtual Balise concept. The model is based on results that have been achieved by the H2020 ERSAT GGC consortium led by RFI in years 2018-2020 (http://www.ersat-ggc.eu/).

The Enhanced ERTMS/ETCS functional architecture is foreseen to integrate:

- The GNSS technology, to enable the Virtual Balise Concept for the ERTMS Train Position function;
- The IP-Based Public Mobile Radio Networks (Land and/or Satellite), to enhance the ERTMS On-board-Trackside communication.

The project Enhanced ERTMS/ETCS functional architecture, reported Figure 2, has been defined within Task 2.1 activities of ERSAT-GGC WP 2 [10] with the following approach:

- Identifying the interaction with the current ERTMS/ETCS functions;
- Minimizing the impact on the current ERTMS/ETCS specification;
- Avoiding unnecessary constraints in order to let each supplier designing its own new functional blocks.

The following subsections list and briefly describe the enhanced functional blocks relative to the Virtual Balise Concept and the IP-Based Radio communication. For major details, please refer to [10].

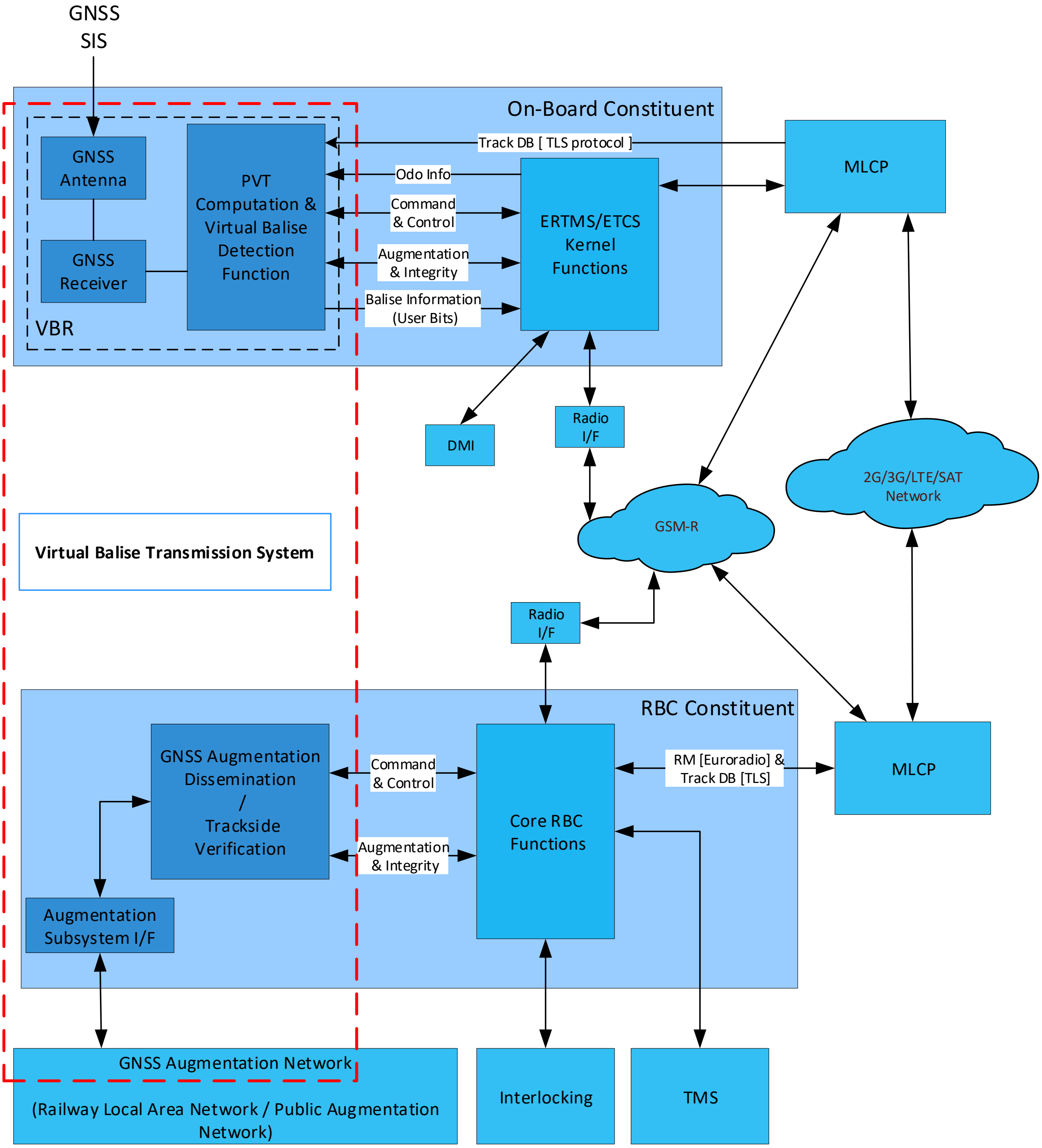

GNSS
SIS
On-Board Constituent
GNSS Antenna
GNSS Receiver
PVT Computation & Virtual Balise Detection Function
VBR
Track DB [TLS protocol]
Odo Info
Command & Control
Augmentation & Integrity
Balise Information (User Bits)
ERTMS/ETCS Kernel Functions
MLCP
DMI
Radio I/F
GSM-R
2G/3G/LTE/SAT Network
Virtual Balise Transmission System
Radio I/F
RBC Constituent
GNSS Augmentation Dissemination / Trackside Verification
Command & Control
Augmentation & Integrity
Core RBC Functions
RM [Euroradio] & Track DB [TLS]
MLCP
Augmentation Subsystem I/F
GNSS Augmentation Network
(Railway Local Area Network / Public Augmentation Network)
Interlocking
TMS

Figure 2. The ERSAT-GGC Enhanced ERTMS/ETCS Functional Architecture [10]

3.1.1 Virtual Balise Transmission System Functional Architecture

The enhanced functional architecture subject of this analysis is based on the ERTMS/ETCS reference functional architecture, including the existing Eurobalise Transmission System, Euroloop Transmission System and Radio Transmission System, which integrates the Virtual Balise Transmission System (VBTS), highlighted in Figure 2 (within the Red dashed line).

The VBTS is intended as a safe spot transmission system that aims at conveying balise information from the trackside infrastructure to the on-board equipment.

The on-board and trackside functional blocks, which constitute the VBTS, are described in the following sub-sections.

Please note that, according to the project strategy the modifications to the ERTMS/ETCS reference architecture should be reduced at minimum. For this reason, it has been assumed that the ERTMS/ETCS Kernel and the Core RBC module shall ensure:

- the compliance with the SUBSET-026 [11] ERTMS/ETCS functions;
- the gateway function between the VBTS On-board and Trackside components by means the Euroradio channel.

3.1.2 On-board VBTS functions

According to [10], the on-board VBTS equipment, Virtual Balise Reader (VBR) in the following, is comprised of the functional blocks represented in Figure 3 and described in the following:

- The **GNSS Antenna**, the device that receives the radio GNSS Signal In Space (SIS);
- The **GNSS Receiver (RX) Function**, fed by the Antenna module, periodically provides the code and the carrier phase measurements relative to the input GNSS SIS;
- The **PVT Computation Function,** fed with the computed code and carrier phase measurement (i.e. pseudorange information), mainly computes the Position, Velocity, Time (PVT) solution on the basis of GNSS information, Augmentation and other on-board information;
- The **Virtual Balise Detection Function,** fed with the computed PVT solution:
    - Compares the computed PVT information with the pre-known virtual balise positions stored in the on-board Track Database (DB), to enable the Virtual Balise detection;
    - In case of Virtual Balise detection, it communicates the following information to the ETCS on-board Kernel:
        - Time / odometer stamp (according to the Odometry data received from ERTMS/ETCS Kernel) of the detected virtual balise centre;
        - The detection error associated with the virtual balise detection accuracy;
        - Balise information for the detected virtual balise according to the on-board track Database.
- The **Railways FDE**, the on-board functional block that, executing the Fault Detection and Exclusion (FDE) algorithms, ensures an integrity check to cope with GNSS system and local feared events that may have impact on the PVT solution to be used for detecting the virtual balise.

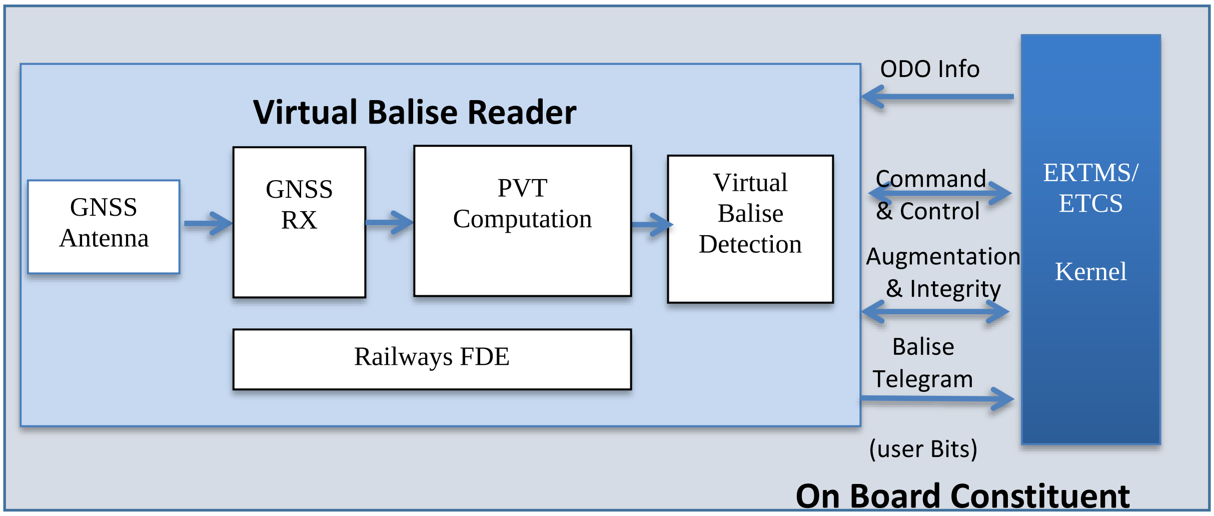


Figure 3. The On-board VBTS functional blocks

Referring to the Standard ERTMS/ETCS Functional Architecture, the VBR functional block should be added to the existing BTM in order to ensure the communication of both Virtual and Physical Balise information to the ERTMS Kernel.

3.1.3 The Trackside VBTS functions

According to [10], the Trackside VBTS equipment is comprised of:

- The **GNSS Augmentation Dissemination** functional block, responsible for:
  - disseminating the GNSS augmentation information;
  - timely computing and disseminating warning or alarms based on the information received from the “Core RBC Functions” block and the GNSS Augmentation system.
- The **Trackside Verification Function** responsible for carrying out additional railway verification checks on the Train Position by the combination of multiple information.

The whole of the two abovementioned functions are referred as the GAD/TV functional block. Regarding the GNSS Augmentation information, which is disseminated by the GAD/TV to the on-board by means of the existing Euroradio link, the interface between VBTS and an adequate Augmentation System (i.e. Railways compliant in terms of safety and performance) is foreseen.

3.1.4 The VBTS interfaces

As inferred from Figure 2, the project ERTMS Functional architecture foresees that VBTS is interfaced to the exiting ERTMS/ETCS On-board and Trackside functional blocks by means of the following logical interfaces:

The VBTS –ERTMS/ETCS Kernel Interfaces:

- **Command and Control:** this bidirectional interface addresses the management of the VBR equipment (e.g. equipment configuration, auto-test etc.)

- **Augmentation & Integrity:** this bidirectional interface is involved in the dissemination of the GNSS augmentation information forwarded from the Trackside GAD/TV block;
- **ODO Info:** this interface carries the ERTMS/ETCS Odometry information for time and odometer stamping of Virtual Balises (as per BTM, see Subset-036) as well as for crosscheck purposes;
- **Balise Information:** analogously to BTM for a Physical Balise, this interface carries the
    - User Bits,
    - The odometer time or space stamping,
    - The dynamic calculation of the accuracy (the only difference with respect the Physical Balise).

The VBTS –ERTMS/ETCS RBC Interfaces:

- **Command and Control:** this bidirectional interface addresses the management of the GNSS Augmentation Dissemination/Trackside Verification (GAD/TV) module within the RBC constituent;
- **Augmentation & Integrity:** this bidirectional interface enables the dissemination of the GNSS augmentation information received from the interfaced GNSS Augmentation System and optionally selected on the basis of the VBR estimated position, and the reception of VBR information / warnings.

3.1.5 The Trackside VBTS functions

Beside the Virtual Balise Concept, the future ERTMS/ETCS system includes the IP-based Radio Communication concept addressing the enhancement of the RBC-On-board communication (already investigated within NGTC project).

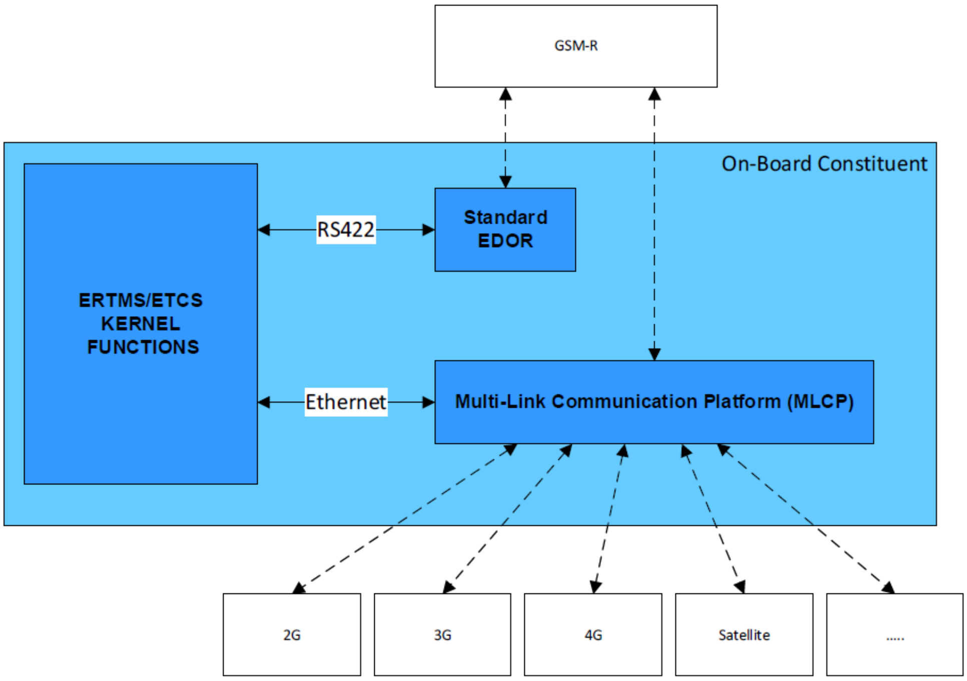


Figure 4. Multi-Bearer IP based Communication Network System [10]

A Radio Communication System based on a Multi-bearer public network (terrestrial and satellite communication) as represented in Figure 4, is potentially foreseen from rail stakeholders and ERA as ERTMS radio communication evolution.

The combination of intelligent routing algorithms and the IP-based solution enable the use of multiple technologies instead of a single one, thus the interoperability with the legacy GSM-R network will be guaranteed. Furthermore, the interoperability of multiple communication technologies will be supported by Multipath TCP (MP-TCP) protocol, which extend the traditional TCP protocol.

Concerning the Quality of Service (QoS), the Multi-Link Communication Platform (MLCP) integrating cognitive algorithms will follow the Euroradio protocol according to SUBSET-037 and SUBSET-093 to ensure the QoS requirement fulfilment.

3.2 AUTO: FUNCTIONAL MODEL FOR AUTOMATED CAR DRIVING

This subsection outlines a logical model related to automated car driving in order to identify main functional blocks, which will be further used for specification of system and sub-system requirements.

In general, the logical flow for an automated car driving can be summarized as follows: the environment/physical situation is observed by several sensors such as GNSS, IMU, camera etc. This hardware information is then analysed and processed in a software system to give a reliable feedback to the control functions of the automated car. How the software system is composed in detail depends highly on the set of hardware sensors and the required functionally of the system. An example of the autonomous driving pipeline is outlined in Figure 5 [12]. It consists of following modules: sensing, 3D map, localization, perceiving, planning and control. A similar architecture is shown in Figure 6 [9].

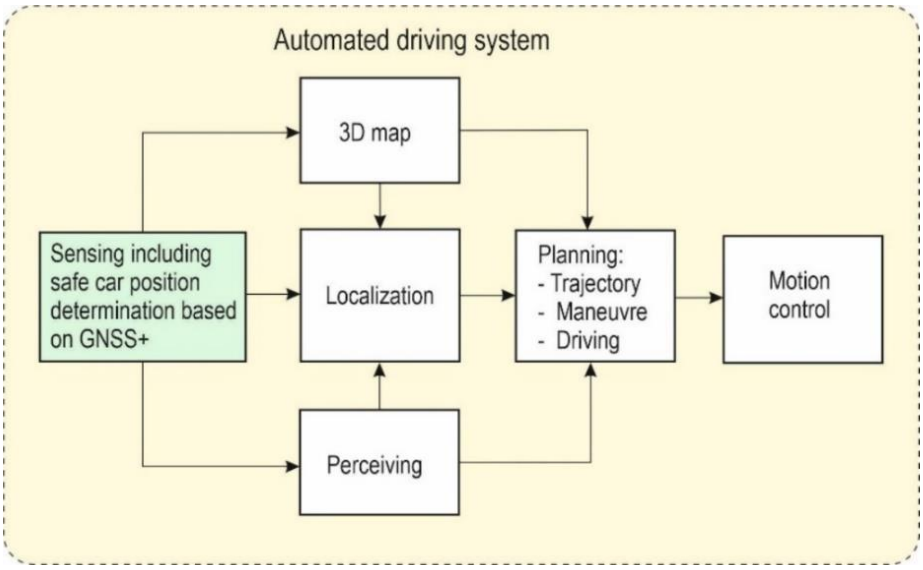


Figure 5. Autonomous driving pipeline according to NVIDIA [12]

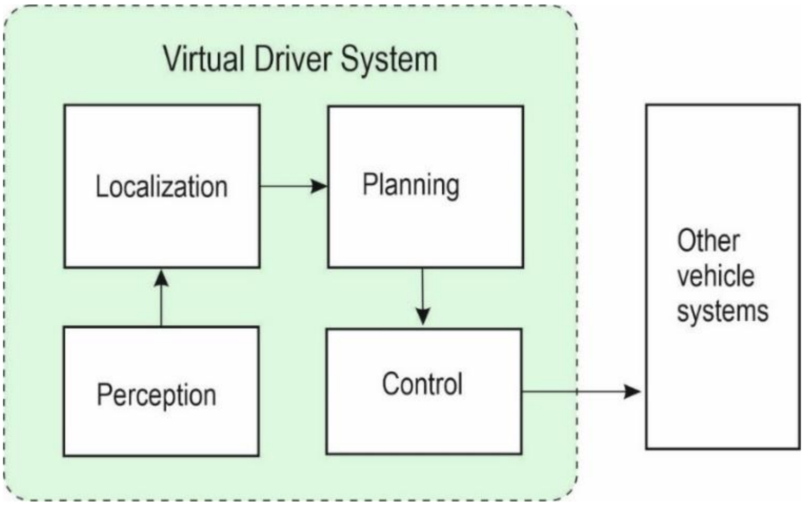


Figure 6. Autonomous driving pipeline according to FORD [9]

The high-level concept (logical model) for automated car driving consisting of the Virtual Driver System and further supported by a public Multi-modal GNSS augmentation network, advanced communications (including 5G, V2V, V2I) and other functions is outlined in
Figure 7.

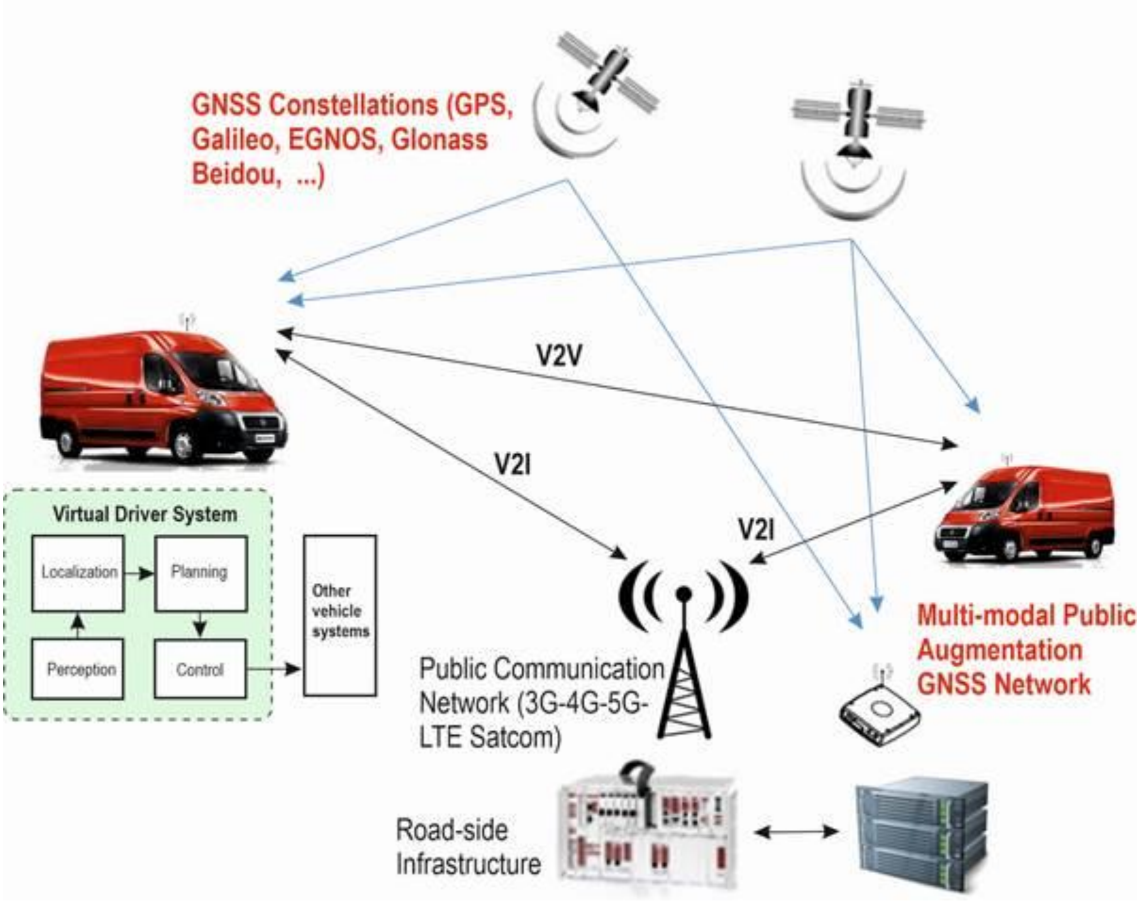

GNSS Constellations (GPS, Galileo, EGNOS, Glonass Beidou, ...)
V2V
V2I
V2I
Virtual Driver System
Localization
Planning
Perception
Control
Other vehicle systems
Public Communication Network (3G-4G-5G-LTE Satcom)
Multi-modal Public Augmentation GNSS Network
Road-side Infrastructure

Figure 7. High-level concept for automated car driving based on GNSS and advanced communications

The autonomous driving pipeline depicted in Figure 6 and included in

Figure 7 have been used for allocation of the automotive Harmonized Design Target (already specified in the HELMET deliverable D2.2 as the Probability of failure PF_{SYS} of 1e-7/ h) to SDC safety subsystems. The allocation process is described in Section 4.2. The high level and detailed On-Board Unit (OBU) architecture and system design for the automated car driving are key elements in HELMET WP3.

3.3 UAV: FUNCTIONAL CONCEPTS AND OPERATIONAL MODES

This section describes functional concepts and operational scenarios of Unmanned Aircraft Vehicles (UAVs) / Unmanned Aircraft Systems (UAS) in HELMET, which have impact on definition of system requirements.

3.3.1 Introduction

The use of UAVs/ UAS has grown exponentially in the past decade, driven by the needs of civil/commercial operations in a variety of industry sectors. Enabling this growth has been the accelerated development of UAS technology, Regulatory frame and the lower costs of operations/services offered in comparison to other systems such as manned aircraft and EO satellites. UAS capabilities that were unachievable only 3 to 4 years ago are now possible and highly competitive. Emerging global markets for UAS employment include emergency services, agriculture, insurance, energy product mining, and security with a wide range of data capture and infrastructure inspection activities being used in construction, utilities and transportation, including railroads, highways and roads. In the HELMET contest it was proposed to study, in addition of Rail and Road application, a complementary service based on UAV/RPAS.

In the HELMET contest we can identify the following objectives:

- Exploit the applicability of EGNSS for navigation and positioning with highly safety standards for UAV applications
- Identify common requirement among the three applications (Rail, Road UAV) for safety navigation
- Conceive a UAV ground infrastructure that can interface with Helmet core service and support UAV applications.

The aerospace applications need very stringent integrity requirement for mission and safety critical missions. These is even more for RPAS/UAV applications that are remotely piloted today in LOS and in future in BLOS even in non-segregated areas.

However current aircraft, and even more those in the future, are equipped with a variety of sensors and navigation equipment. Those in combination with external augmented information can provide additional integrity and accuracy to the RPAS operations and support the future UTM (UAV Traffic management).

In Figure 8 the overall picture of the UAV/RPAS functions required for their operation is reported. Since few years several strategies have been proposed for increasing level of integrity of positioning and navigation while accuracy is more assessed at various levels let’s consider PPP and RTK. In the contest EGNSS plays a fundamental role and therefore it is important to understand its limitations and operability in order to conceive a system capable to contribute to the UAV/RPAS navigation

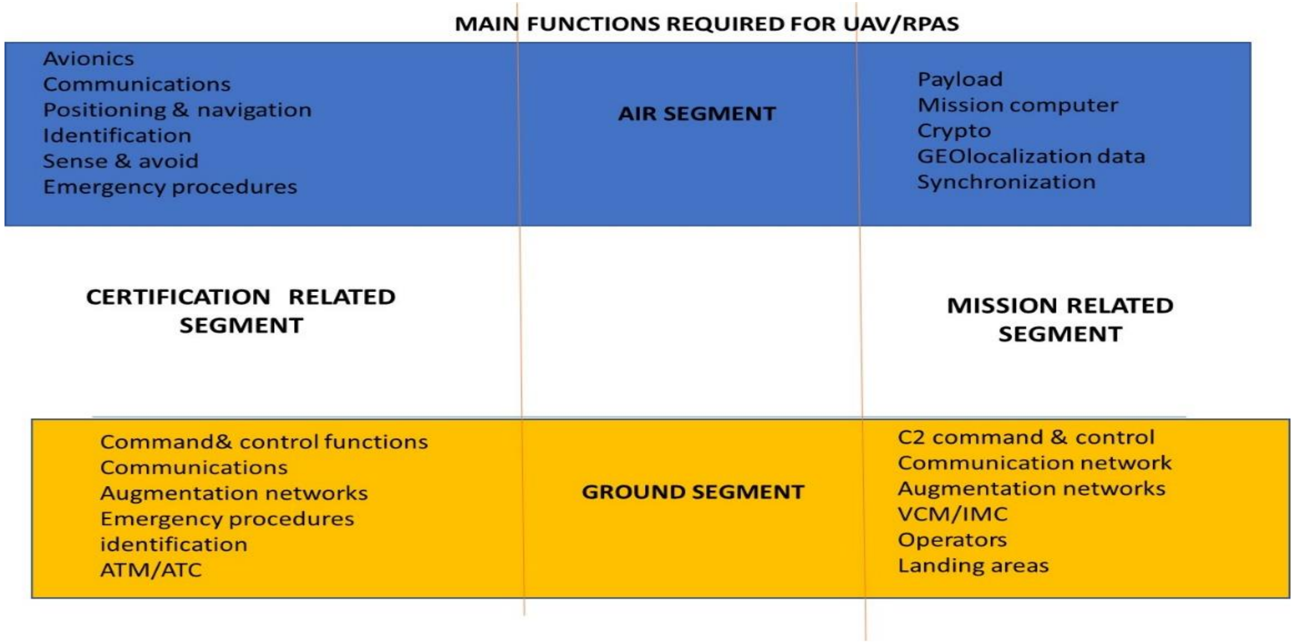


Figure 8. Main UAV/RPAS functions

and positioning requirement. In Figure 9 the future complex and multilayer communication and operation scenario of the UAV/RPAS is depicted.

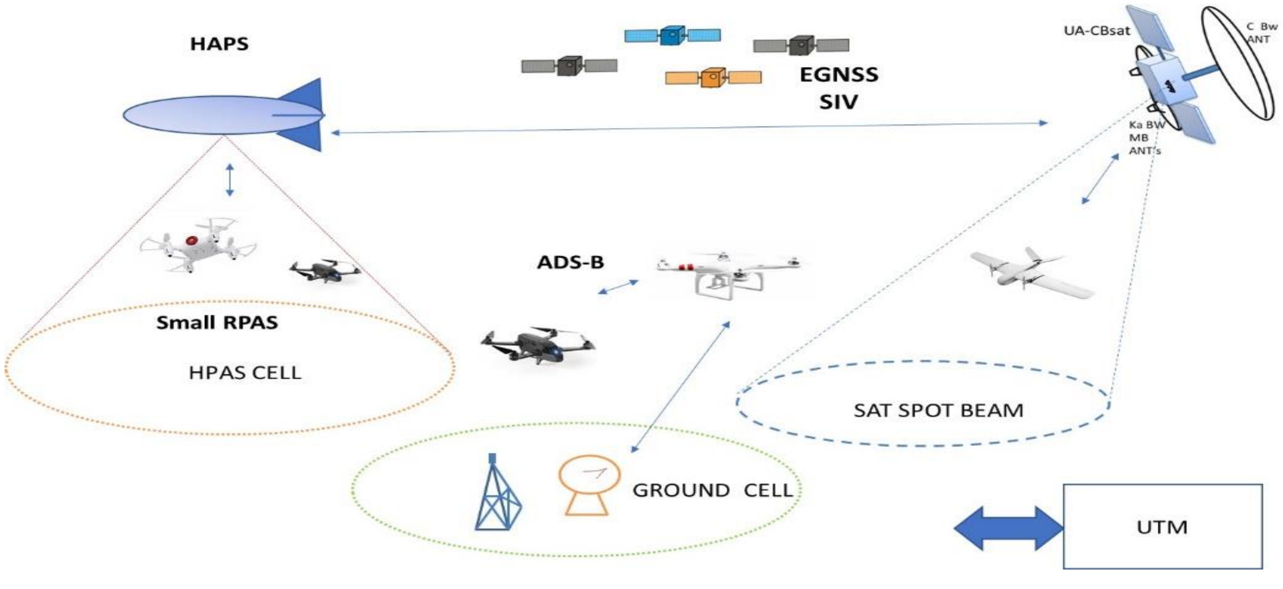


Figure 9. Overall future communication scenario for RPAS

Let’s note how communication will play a fundamental role not only to command and control but also to augment navigation and positioning. Ground stations, satellites and HAPS will create an infrastructure ubiquitous and resilient to allow UAV/RPAS operation even in BLOS. Then the integrity and safety of navigation data became of fundamental importance and this is the objective of this study.

From Figure 9 it is possible to distinguish four potential sources of communications:

- Space communications; by GEO sat (currently a new BW in C band is available for C2) or LEO constellation.

The smaller RPAS likely will not be able to embark a transponder for direct communication with sat in GEO orbit. So in case it was necessary to pass through a satellite it is better to use a relay a HAPS or a ground station.

- HAPS communications

HAPS are under developing and can provide not only communication pilot-RPAS but also additional navigation and positioning services.

- Inter RPAS communication (IRC)

This for the time being is considered a hypothesis but could be very effective in particular for SWARMS/FORMATION operations. IRC can useful also for providing positioning augmentation in same circumstances.

- Ground communications

In this case it is important to evaluate if the augmentation data that we derive from HELMET can be transferred via the C2/3 link or by a dedicated additional link. For instance, RTK are often delivered by a VHF link.

The communication link a general key issue of RAPS operation completely different form the other applications for the time being where we have autonomy or pilot embedded in the vehicle.
Communication lost is even more critical than EGNSS data or integrity degradation and can leads to immediate recovery actions. it is a common practice that if the radio link is lost, then the autopilot commands the aircraft to go to a predetermined waypoint (what is commonly known as return-to-home).

In this case of Navigation aid is lost the RPA usually enters an emergency state where the rotorcraft hovers and tries to land using other sensors such as an altimeter (in the case of fixed-wing aircrafts the engines are stopped and a parachute is launched).

Despite the scope of this study is not to design the communication infrastructure this is fundamental to guarantee RPAS command and control and can be complemented with other key functions such S&A and video. Only an integrated communication and navigation system can provide additional integrity to the aeronautic operations.

Of outmost importance in the future will be the capability to manage the traffic in air and establish a UAV Traffic Control System capable to coordinate the traffic and avoid collisions. The application description in the Helmet contest is in sections below.

3.3.2 Application description in HELMET contents

For the purpose of this project, UAS are considered as the platform by which to perform Rail, Highway/Road Asset Management, Monitoring and Surveillance for Planned and/or Unplanned Operations in cooperation with other systems utilizing the HELMET EGNSS Multi-Modal Augmentation Network Dedicated Services to UAS Applications.

In general, UAS technology is having a powerful and transformative impact on the railroad, highway and road environments and particularly suitable for highly cost-effective:

1) Structural monitoring, especially for critical assets like bridges and tunnels, and for fault detection (i.e. diagnostics/prognostics).
2) Photogrammetry and Railway and road Mapping
3) Environmental Safety Monitoring and Assessments of fire, explosions, earthquakes, floods and landslides along the railroad track and roads.
4) Fixed and Mobile Railway and Road Assets Accident and/or Incident Damage Assessment and Verification
5) Fixed and Mobile Railway and Road Assets Monitoring and Status Control.
6) Physical security monitoring. Detection of intrusions, objects stolen or moved, graffiti, etc.
7) Safety monitoring, e.g., to early detect failures on track elements/devices or obstacles on the track.
8) Situation assessment and emergency/crisis management. To monitor accident scenarios and coordinate the intervention of first responders.
9) Accident investigation and post-accident damage assessment and overall management.
10) Support to law enforcement services and patrol
11) Real Time Operational Support under Emergency Traffic Conditions
12) Potential implementation of uber like services for getting real time images and streaming from loitering UAVs along road and railways.
13) Support to law enforcement services and patrol
14) Wi-Fi Connectivity (Optional Application).

The UAV/RPAS operations require a complex control/ management environment that currently foreseen the presence of a pilot always in connection the air vehicle but in the future the autonomy will play a major role and the UAV will fly also in non-segregated areas in BLOS and finally autonomous. In order to get a better and safer service all along the road and railways, it is necessary to:

- Improve the safety and airworthiness of UAV operations from the navigation and communication point of view.
- Provide points of landing for UAV) for different purposes:
  - Allows safe landing in case of malfunctions of UAV or control network. the vehicles get disconnected, they must find a safe landing spot. We need to have contingencies in mind
  - Refurbish the UAV the smaller ones that because of electrical powering have a low operation time.

This “landing platform” (Fixed and/or Mobile) can then provide additional services to the UAV traffic management and control integrating the services of an EGNSS augmentation control will be later described.

One potential idea is to “create two-way communication” with air traffic controllers and the companies would use a 4G or 5G style of infrastructure for communications but it would need to study that solution for any latency that would become untenable as they scale up and look to remove pilots from the equation when of course the national rules will allow it. In this contest it is worthwhile to mention that ADS-B might be or not the right solution for small UAV traffic control management and in any case it should be complement by other non-cooperative system such radar or electronic recognition measurement (ESM in military language).

Finally, GNSS multi-constellations are also safety enablers in UAV-based SAR operations. In summary, the proposed UAS Rail, Highway/Road Operations of enhanced performance due to the HELMET Multi-Modal Augmentation Network Services offers a unique and Highly Integrated Support and Safety Management System mostly based on mature UAS technology and operational concepts with some novel technological additions to be developed under the proposed project so as to:

- Enhance railway/highway/road safety prevention, environmental and social benefits;
- Reduce overall infrastructural inspection and maintenance costs;
- Increase availability of the overall railway/highway/road assets; and in general
- Lower the safety related operational and economic risks so as to increase global transport business cost-effectiveness.
- Enhance the Embedded cybersecurity features.

3.3.3 System architecture for UAV/RPAS operation

In order to better focus an application, we concentrate our design with reference to the Rail application because it is legacy very well consolidated and presents the real chance to be implemented in a short time.

This for different reasons, but primarily because the air space above the railway lines can be easily segregated or easily georeferenced, giving the possibility to initiate and experiment a service based on a en-route BLOS and semiautomatic or automatic approach in a safety situation. Really Railway application may become the beginning opportunity from where to develop future innovative and via via more autonomous services. The system requirement for road application are however similar with higher complexity in the air space constraints and service management. The basic idea is to implement an architecture that exploit the specific characteristics of railways as that presented in Figure 10.

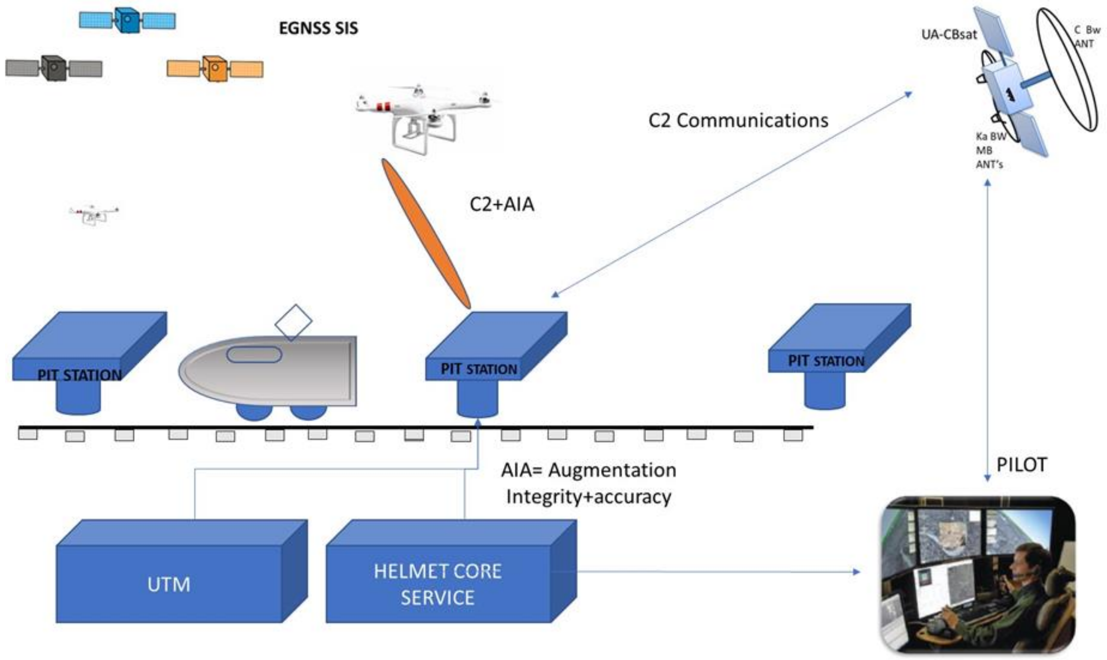


Figure 10. Proposed architecture for UAV/RPAS operation

From Figure 10. we can identify the novelty proposed configuration that see as innovative element the presence of the station for UAV/RPAS operation and control.

The so called PIT station will be deployed all along the rails lines in such a way to allow a seamless coverage of the UAV/RPAS operative areas.

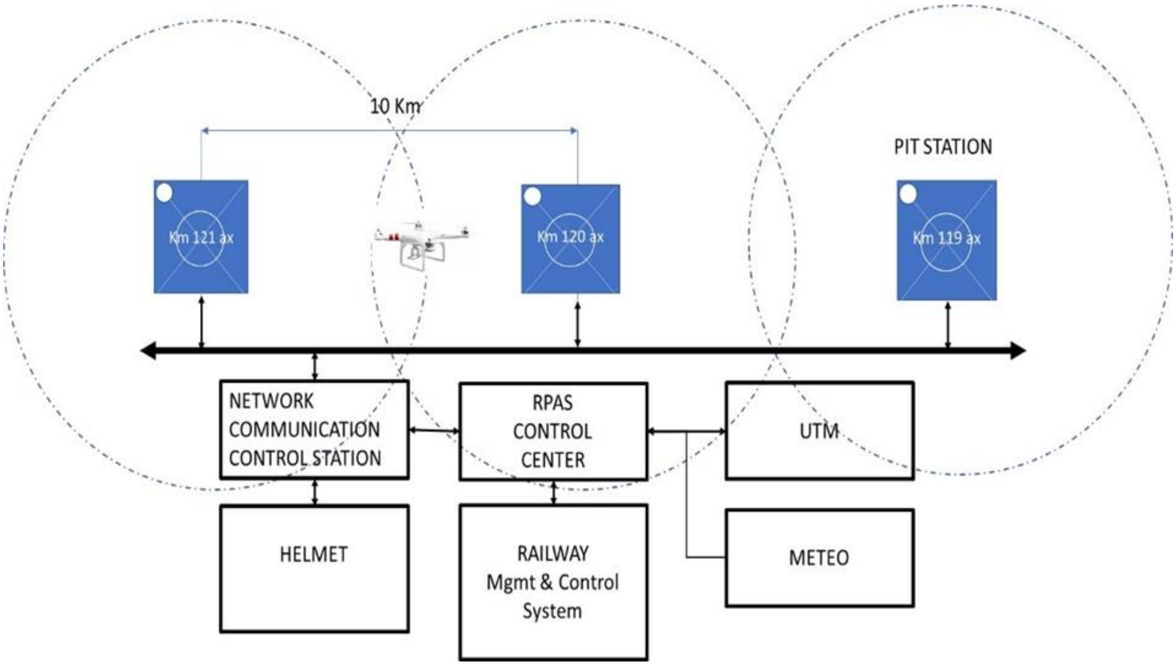


Figure 11. Overall proposed system architecture station functions

In Figure 11 the functional block diagram of the complete architecture is provided.

As such the UAS/RPAS-PIT Station Highly Integrated System Network Segment within the HELMET infrastructure shall be composed of the following main functional Operational Elements, namely:

1) The Operating UAS/RPAS Center which encompasses the Unmanned Aircraft (UA)/Remotely Piloted Aircraft (RPA) in a specific Configuration and Remote Pilot Stations (RPS) operating in LOS and/or BLOS mode by means of a Control and Non-Payload Communications (CNPC) Link (UP and DOWN Data and Voice Link) and Navigation Aid Components utilizing for this purpose a Terrestrial and/or Satellite based Network for Command, Control, Communications, Sense and Avoid (or Detect and Avoid) services covering all appropriate UTM airspace classes for railway and automotive related assets , in all integration cases and flight phases. This element shall include the operational services and capabilities provided by each PIT Station system but from this is excluded the UAS Logistic Support element.

2) The UAS dedicated PIT Integrated Logistic Support (ILS) Element: which shall guarantee UAS/RPAS supportability, operational availability and safety throughout its Operational Life-Cycle.

3) The HELMET Augmentation Network Element dedicated to UAS/RPAS Ground and Aerial Operations this shall encompass the physical connectivity of the UAS/RPAS Navigation

subsystem with the GNSS Gallileo and potential Augmentation Services by the HELMET multi-modal Augmentation and Integrity Monitoring Network

4) The communication networks: we can distinguish the communication among the ground infrastructure to exchange data and commands up to the PIT station and the communication link among PIT station or by satellite/HAPS and UAV/RPAS.

The benefits of introducing PIT station concept are:

- Improved UAV resilience by local fast refuelling
- Improved range autonomy by multiple refuelling
- BLOS operations even for small UAV
- Higher data rate remote communications
- Multiple UAV operations
- Higher position accuracy and integrity for navigation.

Depending on the application the PIT station became the local augmentation station for UAV operations in particular for supporting BLOS operations of small UAV. Based on PIT station will be possible for a UAV operate for a long path same time refuelling/recharging or execute specific tasks such transport of emergency goods.

In addition along the path the UAV can collect telemetry data that can be damped in a PIT station and then transmitted to the control centre. To same extent this procedure may result more economic and effective than transmit data o a ground collector unit or directly via satellite.
In case of rail than it is possible to complement navigation data simply painting the railways sleepers with a code indicating positioning (kilometres) . In case of Highway specific ground items can be geolocalized in order to be detected by the on board optical sensors.

Other items could consist of signal of opportunity present in a specific areas (frequency, BW, etc.) those can be recognized by the on board communication system based on SDR technology.
The possibility to implement a multi-constellation approach is of outmost importance, in rough terms, the more satellites in view (as will be the case in future GPS/Galileo, GLONASS/Compass . . .), the better the accuracy and precision (as already seen in the simulations presented earlier) of platforms using them to navigate. In addition in a multi-constellation system is possible to adopt a ARAIM algorithms.

Commonly, UAV navigation is performed with differential GNSS processing, for same application even in the form of RTK, which however lacks integrity measures.

In RTK mode (Real-Time Kinematic) the UAV or Drone calculates its position in relation to the Base position location (GCS). The base station sends corrections to the GPS/GNSS air module. This allows improving the relative accuracy between both devices, eliminating the errors introduced by the atmosphere and other factors. With RTK positioning activated the relative accuracy improves until to the centimeters scale. Depending on the operation needs, RTK positioning can be activated during the entire flight or automated so that the drone starts receiving RTK corrections when it is in a critical flight phase. An example could be the landing phase. Ensuring a centimeters accuracy at the touchpoint time (in fixed wings cases), landing on an exact point (in multirotor cases) or activate advanced modes (in case of landing on a network or moving vehicles).

One drone application that takes advantage of RTK mode is photogrammetry. Photogrammetry with drones makes possible to model a 3D surface, create plans and perform measurements. Therefore, achieving high accuracy is a fundamental factor. Drone camera positions with RTK are calculated in real-time. This allows correcting camera positions of a few precision centimetrs, both vertically and horizontally

For a few applications where non real time very high accuracy is requested we intend to follow the PPK approach.
Hence, integrity is (or should be) of high interest for UAV platform operators, as it might even be mandated when demonstrating compliance with future safety regulations. In this regard, two key statements define integrity: precision is below tolerances, and no faulty measurements are used. To perform autonomous UAV missions Beyond Visual Line-Of-Sight (BVLOS) or in low-altitude airspace safely, achieving high accuracy and reliability of navigation solutions is required.

This motivates the development of a cost-effective local-area UAV network that utilizes a Local-Area Differential Global Navigation Satellite System navigation solution. The PIT station operate as bridge for this task and achieves a level of integrity comparable to that of Ground Based Augmentation System (GBAS) Category I operations by monitoring navigation faults at the ground station and by broadcasting integrity information to the UAV . in addition the PIT station will monitor the surrounding EM environment to identify potential dangerous interferences.

The architecture of this system involves space-conserving hardware configurations and several simplified GBAS integrity monitoring algorithms to reduce both the cost and the complexity of the system. PIT station/Helmet is designed to support UAVs with a minimum operating altitude of either 50 ft plus obstacle height (within 5.10 km of the ground facility) or 200 ft (within 20 km of the ground facility) by providing an accurate position solution and a tight uncertainty bound on its position error. One notable characteristic our design is the utilization of a two-way datalink between the ground facility and the airborne user, which provides a major improvement in system flexibility. The two-way datalink enables the system not only to allocate integrity risk to each fault hypothesis dynamically to obtain the minimum safe protection level but also to simplify the geometry screening needed to mitigate ionospheric anomalies by computing the maximum error in vertical position only for the satellites known to be tracked by each UAV. Specifically, each UAV can continuously sends its GNSS measurements to the ground station, so that error corrections and integrity information can be generated by the ground station just for this known satellite geometry. This information is then broadcast back to the UAV to allow it to compute its position solution. The integrity status of each UAV, including its current protection levels, is maintained by the ground facility and is used to guide each vehicle while maintaining safe separation from nearby obstacles and other UAVs.

Despite the PIT station and its background infrastructure in our specific missions is of paramount importance to embed in the UAV/RPAS a suitable on board integrity mechanism that can operate even irrespectively from SBAS and GBAS support with acceptable degree of safety.

So, other navigation sensors are required to provide reliable navigation in case of GNSS signal interference or blockage. In this study, the idea is to incorporate multiple sensors to assure complete UAV navigation system safety. In addition, even more parallel layer of integrity will be deployed and operated in function of the specific mission or mission phase as later described.

With the inclusion of multiple sensors, a new fault hypothesis, which is a multi-sensor failure, is added to the existing ground support integrity fault tree. The onboard module integrates Inertial Measurement Unit (IMU) sensor output with the Ground Support solution using a Kalman filter (KF). In addition, optimal protection levels are computed by allocating the newly introduced multi-sensor integrity risk dynamically together with the Ground Support (combination of PIT station and Helmet central node) integrity risk. The sensor failures depend on sensor type and quality. However, a FDIR (Fault Detection Isolation and Recovery) SW module embedded in the system shall identify fault in the HW and will be able to reconfigure the system even in a graceful degradation mode or initiate the recovery procedure in case of loss of communications link or position data.

Another important requirement to fulfil is the estimation of heading that with a dual-antenna GPS receiver can be estimated with an accuracy of less than 0.5º. This system is much more reliable than a stand-alone magnetometer and corrects the typical sensitivity issues caused by electromagnetic sources like the RPA engine through a continuous and automatic calibration of the magnetometer using the data provided by the dual antenna GPS receiver.

Finally, the issue of authentication is very important because can generate a protection against the spoofing that can have dangerous consequences, it can be managed at different levels:

- Open service message authentication
- Commercial authentication services (based on E6)

Important is also the possibility to authenticate the RPAS position and timing for different purposes such assurance but also for police and law enforcement assessment.

The system we are defining will embedded the capabilities currently requested to operate in a safety way such (see Figure 12):

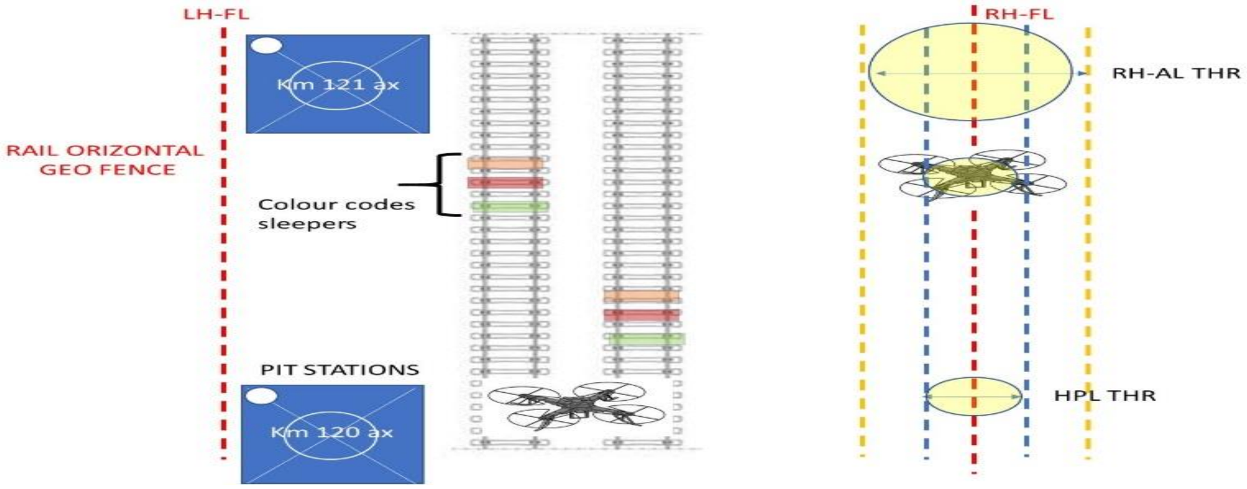


Figure 12. UAV Rail scenario with operational area constrined by virtual fences

- Geo fencing

Virtual barriers will be defined for RPAS/UAV operations in the railway sector.

- Waypoint navigation

Those define the trajectory to be followed by drones from moving for instance form PIT station A to B.

- Geotagging

Geographical information, ground refence point and emergency locations will be loaded into the UAV on board avionic navigation system before each mission to improve safety and utilize information for camera or other sensors for navigation augmentation – see Figure 13.

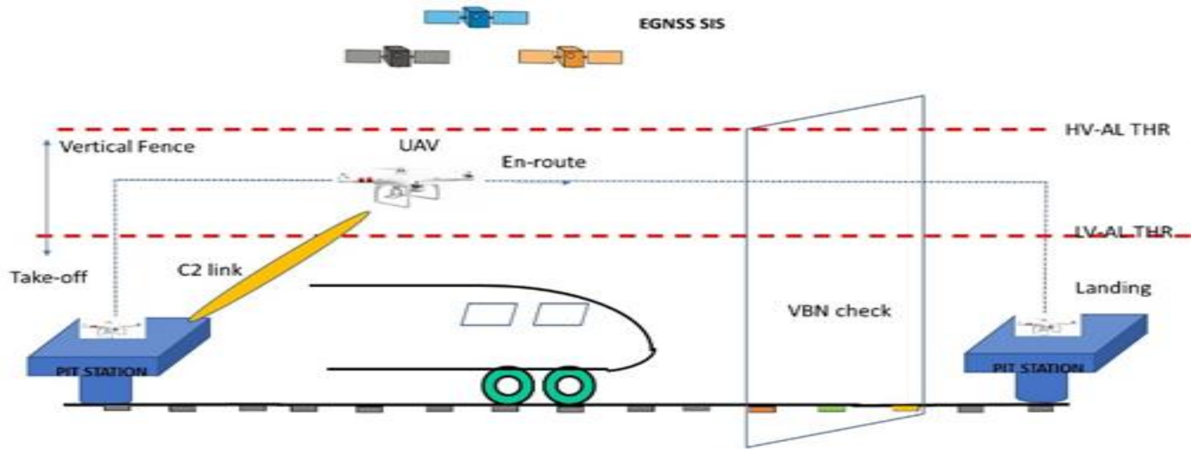


Figure 13. Geo tagging operation for VBN. The action can be performed during operation to verify system safety

Other capabilities that the system architecture and the relative aircraft will embed are:

- Drone telemetry/tracking position reported to pilot via PIT station or satellite link
- Detect & avoid by additional sensors or ADS-B or UTM data. Basically PIT station will embed a ADS-B sensor to detect UAV and /or Aircraft flying all around.
- Drone Identification: only identified aircraft will be authorized to fly in the future aerospace so our system will communicate each planned mission to UTM just before initiation.
- Recovery actions will be planned and setup every mission by :
  - Return to home
  - Altitude hold
  - Loiter on an area

Now for what we have said above we believe that a suitable augmentation infrastructure can be conceived to support the Helmet applications, that are:

- Railway

In this case the RPAS application has several advantages:

  - The area above the railways can be segregated and are easy to virtual fenced
  - The rails itself may constitute a reference item to refer RPAS localization
  - The presence of staggered small stations allows good location for RPAS augmentation /recovery/ maintenance/operation
  - Stations may become area of emergency landing

- Highway
  - Here segregation space is likely not achievable however the large paths are still a good reference for navigation
  - The lack of station should be compensated additional dedicated infrastructure.

So we propose to implement an infrastructure that:

- improve small UAV capabilities, resilience and integrity and permit their operations even in BLOS supported even by space communications.
- consist of a network of PIT stations that includes UAV landing area, a communication package and a GNSS integrity monitoring and improvement system.

In this PIT station the UAV can land and refuel batteries based for instance on a non-contact equipment.
The PIT station is also autonomous form energy point of view because of embedded solar cells.
With HELMET the idea is to make the recovery action in case of GNSS loss more effective and keep the on-board unit always calibrated so that the RPAS can reach the area where PIT station provide autonomous landing service.

For instance, it is possible to anticipate to the situation of a complete loss of GPS signal using the integrity information included in EGNOS messages or compute this information on ground and transmit it to the RPAS and pilot and take some countermeasures. EGNOS-capable receivers can use the integrity data included in EGNOS messages to calculate the so-called protection limits which are related to the reliability level of the GNSS measurements. A dedicated on ground PIT station can in addition evaluated the surrounding environment and provide better protection limit computation with information about the status of EM environment in terms of interferences or spoofing. Basically, we can have different situations:

- GNSS data are reliable and can be integrated by satellite augmentation EGNOS. These results can be integrated and complemented with ground data to improve reliability, integrity and accuracy
- Same situation as above with additional data form ground (differential, PPP or RTK) to get needed accuracy for the specific application
- Satellite augmentation (EGNOS) signals are not being received from the EGNOS satellites so the corrections are not being applied to improve GPS positioning and there is not an integrity service for calculating the protection levels. However the ground augmentation data are received and replace EGNOS data.
- GNSS signals are not reliable enough. This is detected when the protection levels are higher than user-fixed alarm limits that are set depending on the application. In this case the avionics should state if on board sensors can support degraded navigation accuracy for completing mission or enter in correction or recovery action
- GNSS receiver is not able to calculate a position solution.

So the main concept here is to use integrated integrity information (space & ground) to detect degradation in GNSS signal and anticipate to a possible loss of a GNSS position solution. For this purpose, it is necessary to identify new states in the on board avionics, communicated to pilot and UTM, that lead to enter in dedicated operative modes of RPAS avionic.

The states will be defined based on the values of the protection levels and the stated alarm levels. When the protection levels are higher than the alarm limits, then GNSS signals cannot be reliable and the autopilot may decide to try to land the aircraft before further signal degradation or even complete signal outage is experienced. The presence of a ground augmentation system can contribute to reduce those situations of emergency and continuously calibrate the on board IMU that in case of completely loss of navigation and link operativity can try to reach the planned area of landing where operation are in loco assisted.

UTM Constraints and operation

The UAV/RPAS particularly in the BLOS operation should withstand inside and AIR traffic system that present risks and challenges, the UTM complexity is shown in Figure 14 for different classes of traffic depending on its density and location.

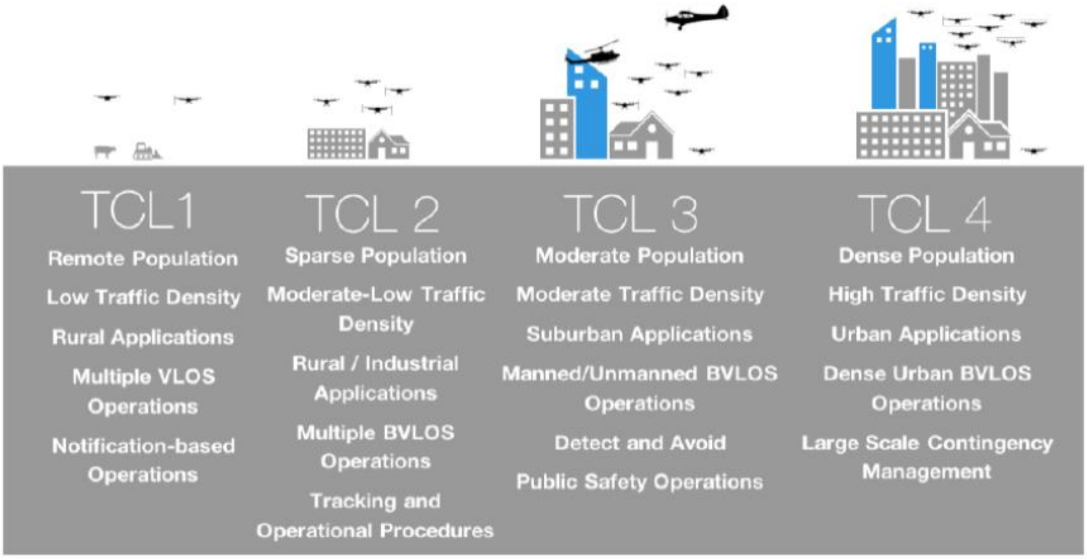


Figure 14. UAV traffic categories

The system major critical issue consists in detection of emergency situation and act properly procedure.

The basic idea is to communicate every mission trajectory to the UTM and embark an ADS-B transmitter in order to communicate UAV position.

On the other hand each (or only a few) PIT station might own and ADS-B receiver. This from one side is an addition equipment to control the UAV position in case the main communication path fails but permits also to control aero traffic all around the mission operation paths. The UTM for its own can provide information about potential trajectory conflicts.

When a conflict is detected (Figure 15) all the info are transmitted to the operator that act or supervision the recovery trajectory computed by the operator master station and sent to the UAV.
In case of lack of reprogramming but the UAV is still aware of emergency it is possible to conceive automatic procedure based on position of the danger target from sent from the PIT stations.

All this of course need a cooperative action from the intruder to further improve the traffic would be necessary to embark an autonomous S&A system on the UAV or foreseen a non-cooperative airspace control system like radars.

Basically, the UAV operation area is thought not accessible for other UAV or aircraft however an ADS-B tx only transmitter will be added to avionics. In principle only cooperative S&A are expected in the area and intrusions are communicated via UTM to the PIT stations that can estimate collision risk and communicate them to pilot together with potential avoidance trajectories.

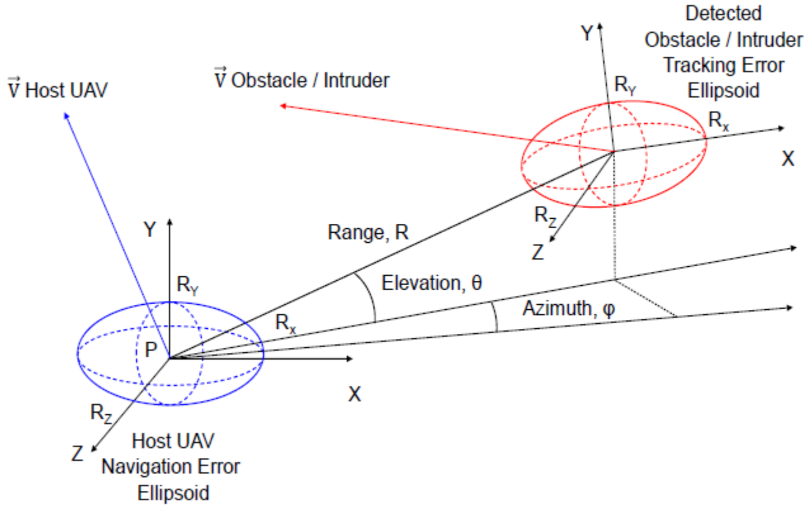


Figure 15. Trajectories computation for obstacle avoidance

The System will follow the UTM principles even with additional points:

- Only authenticated operations will be launched
- Avoid impacts among any other UAV entering in the georefenced air space
- Avoid impacts with aircraft entering in the georefenced air space
- Avoid exiting from mission planning operation unless emergency or replanning activity with immediate communication to UTM
- When initiated and during mission operators should have awareness of any constraints from traffic and all kinds of environments
- Keep Public safety as priority wrt any activity.

In this contest the UAV operator station should be able in collaboration with UTM centre:

- Recognize proximity alert (based on GEO fencing, etc)
- Recognize intruders (via ADS-, UTM or other sensors)
- Management of contingency alert
- Replan flight in 4D for emergency management
- Manage priorities

The management of priorities should also embed in the PIT station network control.

1. System Operative modes

In order to better identify the navigation requirement, we need to define:

- Mission classes
- Mission operation modes
- Mission operation control typologies

MISSION CLASSES

Potential mission classes of general utilization are:

- **Routine mission**

It consists of a surveillance mission with flight path from a PIT station to another one. Basically, the mission is operated in a semiautomatic way with pilot supervision. During this mission is however possible for emergency or needs change the flight path based on pilot control command.

The en-route phase requests not stringent accuracy requirement but very good integrity in particular when the UAV is operated in BLOS. The main recovery action is based on VBN assistance.
The routine mission definition, being repetitive, may follow a learning curve activity where ground feature are stored in an on board data base that is used as complementary on board navigation method. This can be very useful for PIT station automatically landing. The process can be portable and stored in other similar UAV performing the same mission. More in general in case of routine operation a dedicated activity will consist in geo localization of ground elements and point of interest that can be associated with maps. This activity can be also performed with a specific UAV operating with camera (even 3D) and RTK.

- **Specific/Critical operation mission**

In this mission a few flight phases will be automatic or semiautomatic (landing/take off , approach) but pilot takes control of the UAV for the specific operation time interval. In this mission mode the navigation accuracy is very important and should be sent to the operator screen in a short latency time. In addition even the map should be referenced with high degree of accuracy so that the pilot can get a good awareness of relative position of UAV and target under observation.

- **Special mission**

These missions are devoted to specific activities that need pilot directly operating the UAV in loco.
As for Bridge or galleries inspections where UAV distance form obstacles can't be guaranteed by autonomous or remote controls unless very sophisticated S&A mechanism are embarked. And additional external systems are implemented to facilitate the operation in those missions.

In Figure 16 the sketch of UAV operations when galleries are found. Even in this case PIT station may play a role connecting additional equipment inside the gallery for operation especially in particular situations like the emergency's ones. However, this aspect will be not further discussed in this contest.

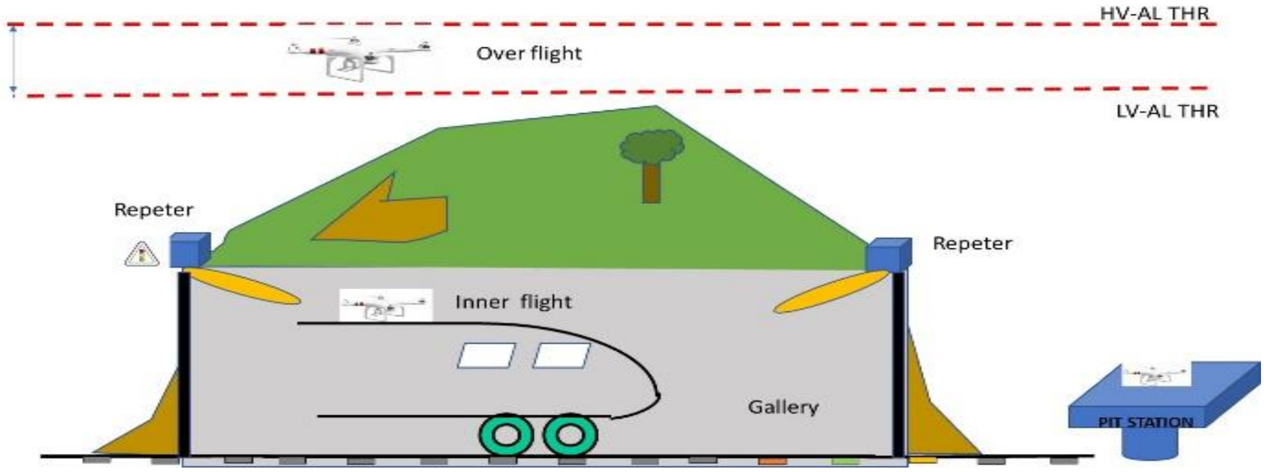


Figure 16. Gallery inspection procedure

For the scope of Helmet we will concentrate on the first type of mission mode above described. The UAV in our application will operate in a “controlled “ airspace with expected “exemption “ from local Aviation Authority. Currently rules vary from country to country and things are more difficult for manufacturers and operators. Nevertheless, even slowly same progress, is running. The main issues to cope with in the UAV application process deployment are:

- Autonomous mission management with human supervision
- Contingency /emergency management
- UTM/ATM system reliable management
- System Health monitoring system (ground, on board, telecommunication)
- High navigation and communication integrity
- Certification of system and functions.

For the time being we propose a study case of a UAV that operate in semi-automatic way with pilot supervision that could be accepted for initial service experimentation form designed institutions.

The UAV class taken in consideration belong to the 25 Kg and below following the rules of :
“Specific’ (medium risk) UAS/RPAS operation category that, considering the risks involved.

It requires an authorization by the competent authority before the operation takes place and considers the mitigation measures identified in an operational risk assessment, except for certain standard scenarios where a declaration by the operator is sufficient; this is achieved by communication each mission to ATM/UTM authority.

It requires a risk assessment, which should follow the JARUS Specific Operations Risk Assessment (SORA) methodology, performed by the operator. Thus, the Regulation in this category considers the following:

a) Increased risk operations
b) Safety risk assessment
c) Approved by NAA possibly supported by Qualified Entities unless approved operator with privilege
d) Operation authorisation with operations manual
e) Concept of accredited body
f) Airworthiness of drone and competence of staff based on risk assessment
g) The CONOPS assumes that most of the professional flying in VLL will be considered Specific operations.

MISSION OPERATION MODES

In terms of general operative modes for each single flight we can see in Figure 17 the various phases. Each phase presents same specific requirement in terms of navigation accuracy and integrity.

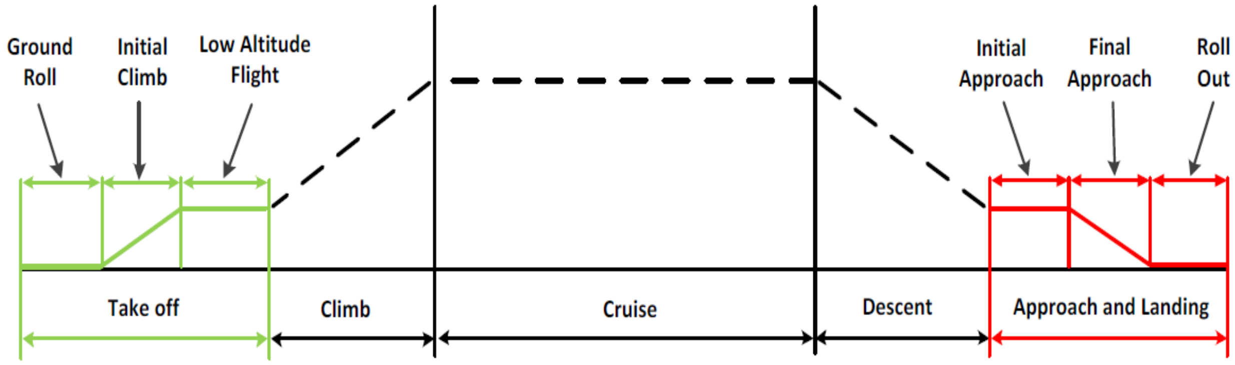


Figure 17. UAV operation PIT to PIT flight as mission reference

The specific operations done during the phases are:

Take-Off at PIT station A

- Check and confirm the UAV identifier
- Refuel/Recharge UAV
- Set local coordinate and target PIT coordinate
- Set UAV heading
- Select altitude and speed
- Compute trajectory
- Select positioning accuracy AL and PL (for each phase)
- Set fence box vertical and horizontal limits
- Set emergency/ recovery actions
- Set alternative reference positioning and navigation objects. (i.e. geo localized sites that can be recognized by VBN)
- Set mission operative modes (i.e. observation, data gathering, etc.)
- Set communication operative frequencies and encryption keys
- Verify communication links operations
- Communicate flight plan to UTM
- Take-off on pilot command through local authorization (and UTM).

All those activities can be done in autonomy but under the supervision and confirmation of the operator.

En-route

Then the UAV takes off and reach the operative altitude. The trajectory is controlled by the on board auto-pilot. Any displacement from the trajectory is timely compensated by the navigation system based on integrated avionics sensors including GNSS rx. The positioning error is verified through the integrity mechanism. During the en-route the PIT station transmit to the UAV integrity data and augmentation data for improving accuracy. The PIT station can be also the bride for controlling and commanding the UAV as alternative to other systems. Because of small UAV can't communicate directly with satellite the PIT station can operate as relay. The augmentation data comes from

HELMET core service centre. In case there is a real time link between pilot and RPAS then it is possible to replan operation or take direct control of the RPAS.

Then the UAV reach the PIT station B.
Initialize the landing procedure automatic or assisted by pilot. In case of automatic the procedure foreseen speed reduction, attitude acquisition, reference signal acquisition form PIT station. (i.e. augmentation for attitude and heading or RTK data).

Landing -PIT station B

- Hand over of communication links form PITA to PITB
- Acquire reference signal or data for landing (supported by optical or RF augmentation)
- Precision approach category I/II/III and/or visual assisted landing
- Augment Landing and attitude control (if requested)
- Landing
- Communicate flight plan to UTM
- Refuelling/Recharging
- Dump acquired data for tx to Pilot or users via ground or space networks
- Check-up health status
- Reprogram operation as for station A
- Goes next PIT stations

As said PIT stations tx to the UAV and pilot the integrity levels of position accuracy and receive back current position of UAV that is then tx to the UTM.
Any violation of trajectory or non-planned actions are immediately tx to the pilot.
Any other activity in the operational aerospace shall be communicated to the pilot for flight (re) planning.

In Figure 12 above the UAV application scenario for railway with indicated the PIT stations and the operative area bordered by the virtual fences in horizontal and vertical levels. Another potential improvement for positiong awareness is the colour code of the sleepers.

MISSION CONTROL TYPOLOGIES

Mission control typologies will be:

- Direct LOS

In this typology the operator controls the UAV in visual mode

- Direct via PIT station

Here the operator uses the optical equipment in addition of the on board accommodations to control the UAV. This is typical for landing and take-off.

- BLOS via PIT station

The most innovative and challenging. The operator supervise or control the UAV operation via PIT station link. Note that this link may pass via ground communication network or via satellite so allowing the UAV control in safety way even in remote areas. In practice

- Autonomous

Possible autonomous operation will be mainly operated during the en-route phase.The landing can be also autonomous with the support of a VBN system like what presented in Figure 18. As alternative in case of poor visibility a RF landing system may be implemented based of on board autonomous or on ground assistance.

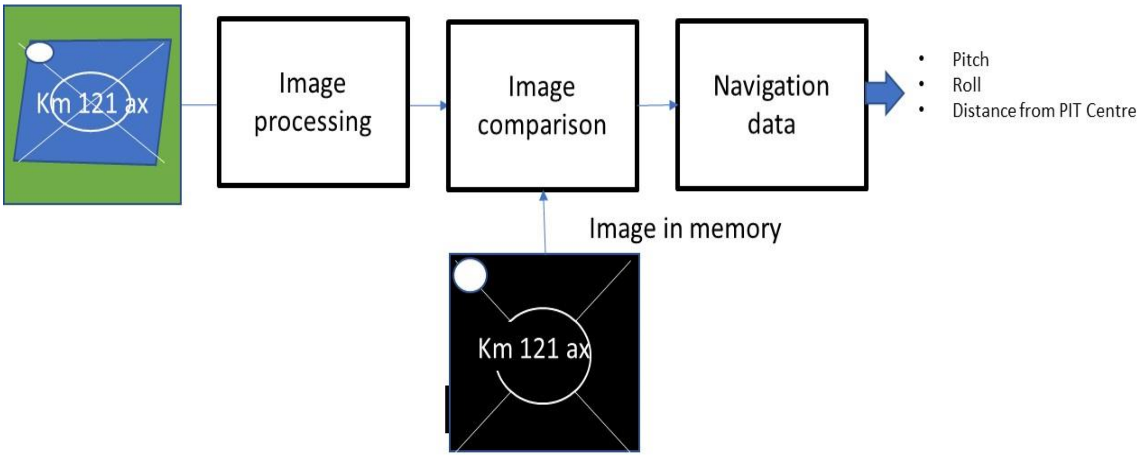


Figure 18. Landing autonomous by optical support principle of operations

In order to specify requirement for safety and operation here-in we will adopt the concept of Performance–Based Navigation (PBN). PBN is a method of defining aircraft performance requirements independent of the specific equipment. In other word with this approach we move from sensor-based navigation to performance-based navigation. This leave the system designer free to select and even update equipment according to other requirement or simply to their evolution. Then as already mentioned in the user requirement and CONOPS we refer to Required Navigation Performance (RNP) to define performance requirement in terms of accuracy, availability, continuity and integrity and are independent of equipment capabilities.

The HELMET architecture should provide a contribution to merge those different sources of integrity for improving mission and safety critical operations and systems. Not forgetting the meteo data that will be part of mission analysis, planning and final authorization.

The in order to improve safety the following functions should be introduced according to literature (Sabatini et al.) but here extended in their meaning, in the overall system design:

- Prediction (caution flags)

Prediction is mainly based on Space augmentation but more on ground augmentation system that only can provide status of integrate navigation and communication safety of the area where it is placed. This allows a better plan of the RPAS mission and the overall UTM traffic management.
One specific case might be the PIT station detect interference and communicate this situation to the operator station signalling the risk in entering in that areas. Or simply the PIT station signal its malfunctions.

- Avoidance optimal flights path guidance

The availability of good integrity data allows to optimize flight path and to define potentially dangerous situation anticipating correction manoeuvring or flight reprograms. This of course in our system based on UTM or ABS-B/PIT station but in the future with assistance of on-board S&A process.

- Reactions (warnings flags)

When a warning is detected then the action should be performed. It is important to minimize the false warnings. The action may consist in a redefinition of UAV mission, trajectory or mode of operation just reconfiguring on board HW and SW.

-   Corrections (recovery path guidance)

Correction are needed in case of emergency situations. In this case it is important to get awareness of situation around RPAS for optimizing escape or avoidance manoeuvres.

For the time being this activity is done under the operator supervision but could be fully automatized. It is important to emphasize here the difference of actions in case of emergency wrt other applications like Rail or Auto. If the communication links are lost or the navigation assistance is not supported, then the correction actions may consist of:

1. The RPAS autonomously (or assisted by local augmentation system or operator) land in a pre-defined area pre-planned before mission start
2. The RPAS remains in flight possibly loitering over a pre-planned area.
3. The RPAS is reprogrammed with new trajectory
4. The RPAS is reprogrammed in a redundant or degraded operation mode to conclude the mission

Depending on the status of communication and on board functionality action can be automatic or executed from the operator on pre-defined procedure that can start automatically to reprogram trajectory and send data to the UAV. In practice the operator just assists to the machine functioning.

3.3.4 Augmentation and Integrity approach

The overall functional block diagram of RAPS operation integrity is provided in Figure 10 above.

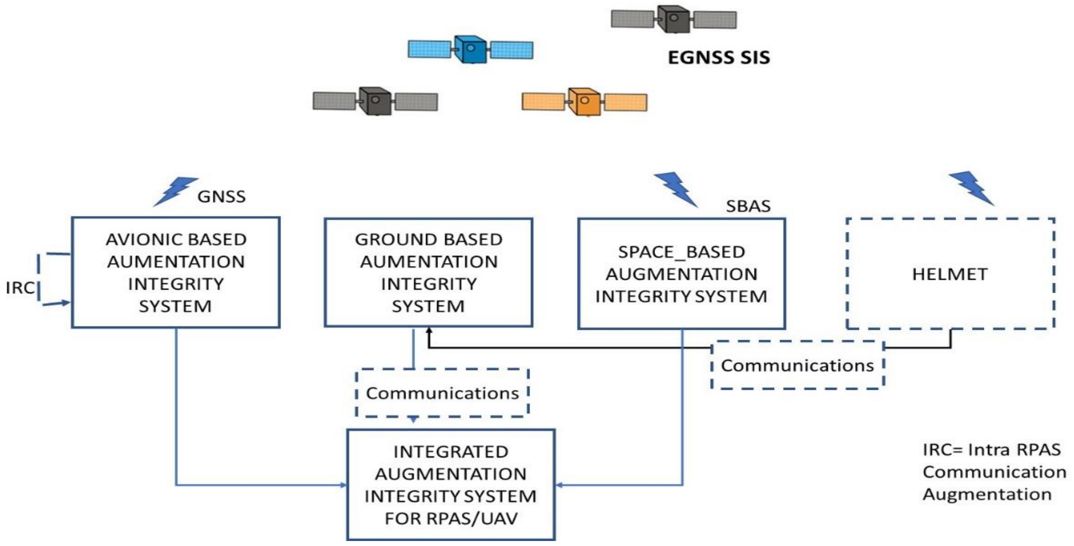

EGNSS SIS
GNSS
SBAS
IRC
AVIONIC BASED AUMENTATION INTEGRITY SYSTEM
GROUND BASED AUMENTATION INTEGRITY SYSTEM
SPACE_BASED AUGMENTATION INTEGRITY SYSTEM
HELMET
Communications
Communications
INTEGRATED AUGMENTATION INTEGRITY SYSTEM FOR RPAS/UAV
IRC= Intra RPAS Communication Augmentation

Figure 19. The overall contest of improved integrity for RPAS/UAV and in general aeronautic

From Figure 19 we have:

- On board augmentations (ABAS) provided by avionics and specific applications such ARAIM.

Integrated avionics allow to estimate integrity from the diverse source and provide internal FDIR capability. Decision can be taken on board or remote pilot depending on the on-board autonomy.

- Space based augmentation

This is provided by SBAS system, EGNOS for us in Europe. However, EGNOS presents same limits in terms of local integrity and accuracy that can be improved only by dedicated ground augmentation systems.

- Ground based augmentation

This provides differential correction and integrity. This is a key issue for RPAS operators for landing and take-off in absence of other mechanism. Of interest are the situation where a landing area is used form more RPAS and then as for small airport it is necessary to adopt specific procedures with priority rights. Current SBAS/GBAS play an important role in improving navigation performance both in terms of accuracy and integrity.

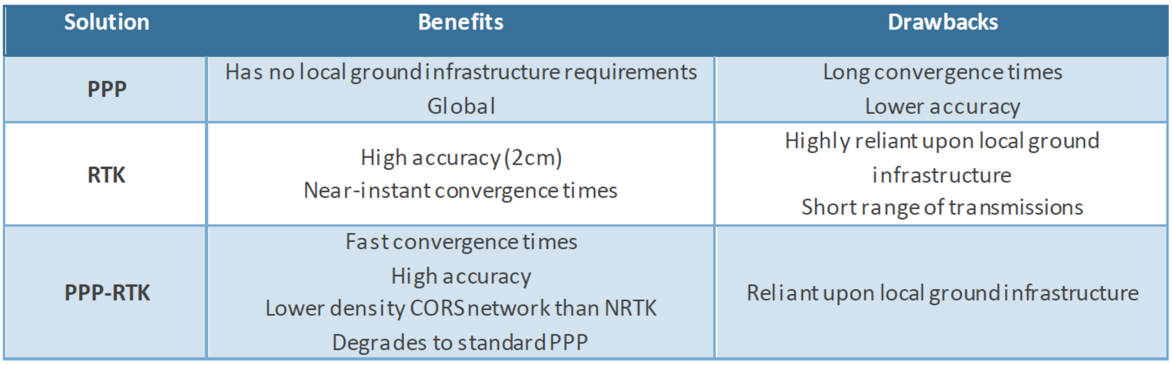
However, it is fundamental to design and implement a properly designed on board integrity system that can introduce a safety critical standard in UAV applications in particular in precision approach and landing. So the idea is to explore the concept of integrated space, ground and on board architecture where Helmet can provide essential services.

The on-board unit (OBU) design and functions will be designed to cope with the different missions and phases of flight in order to comply with the specific current requirement in terms of accuracy/integrity with a layered configuration that allows timely failure detection and system reconfiguration.

The UAV accuracy requirement currently well recognized have been conceived for large UAV remotely piloted and not for autonomous small UAV applications likely autonomous. Here in we will also try to understand how to tailor those requirements for our application on the basis of the PIT specific architecture.

We intend to exploit new possibility coming from PPP-RTK – see Figure 20. This seems a good compromise between RTK complexity, high data rate and long PPP convergence time. Let’s consider that the FWD data rate for the UAV should not allow large BW. The availability and density of PIT stations makes the PPP-RTK a viable solution. Other possibility may consist in tx pseudoranges to the PIT station and rx back the corrected data. That’s a viable solution to be further investigated for landing approximation. For very high accuracy geolocalization the intention is to adopt the PPK approach that consist in a post processing of the data.

In this view the PIT station can be assimilate to COR (Continuous Operation Stations) proposed in literature.



Solution	Benefits	Drawbacks
PPP	Has no local ground infrastructure requirements Global	Long convergence times Lower accuracy
RTK	High accuracy (2cm) Near-instant convergence times	Highly reliant upon local ground infrastructure Short range of transmissions
PPP-RTK	Fast convergence times High accuracy Lower density CORS network than NRTK Degrades to standard PPP	Reliant upon local ground infrastructure

Figure 20. High accuracy methodologies

GNSS integrity concept has been firstly developed and formalized in the aviation field for Safety-of-Life (SoL) applications it is necessary and important to bound the errors and to ensure that the probability of errors not properly bounded is below a certain limit in order to reduce the probability of the harmful effects and to guarantee the correctness and fairness of the decision.

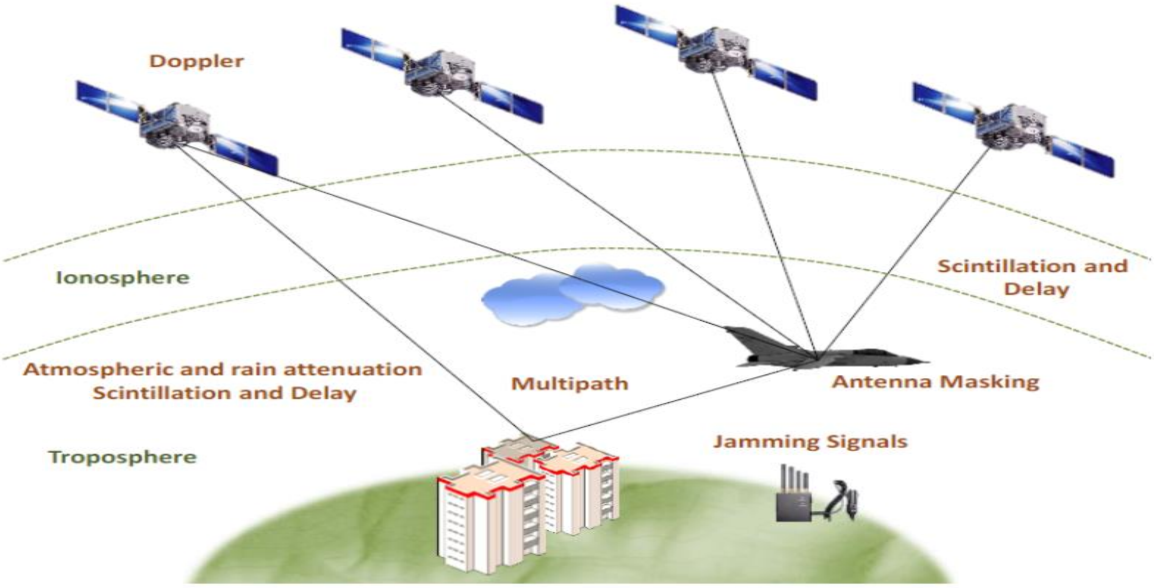


Figure 21. Major causes of EGNSS degradation

The Major causes (Figure 21) of errors outages and severe performance degradations are:

- Obscuration of satellite signals during manoeuvring (Antenna obscuration)
- Bad satellite geometries (DOP)
- Fading so low C/N0
- Doppler shift
- Multipath
- Interference or jamming

These causes of integrity reduction are not well represented in RAIM approach while they are affecting the UAV navigation integrity in particular when operating at low altitude.

In Figure 22 the interface of an integrity on board system are shown. In particular it is pointed out the presence of the waning messages that can be generated internally from the sensors analysis or from the FDIR function or externally by the combination of PIT sensors, HELMET core centre and UTM centre.

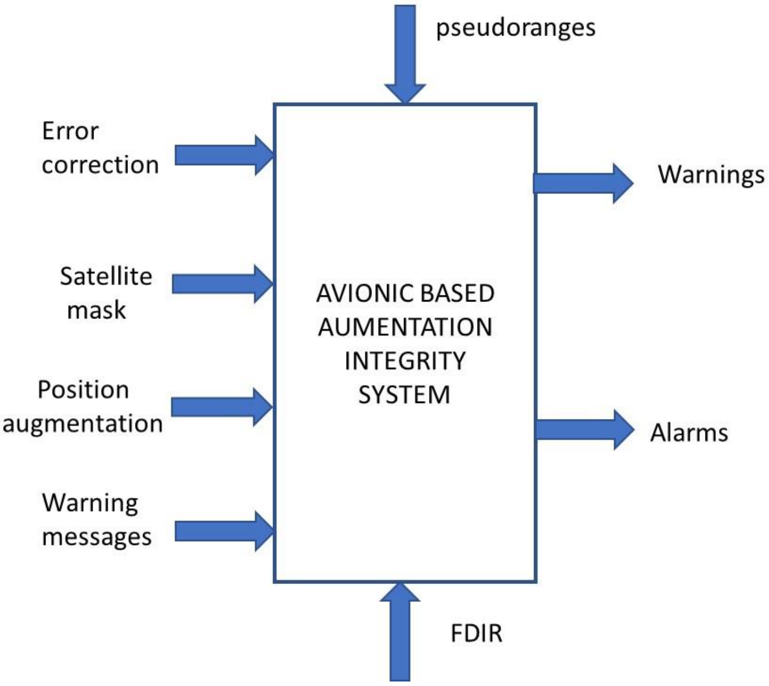


Figure 22. Avionic based integrity functional system interfaces

In Figure 23 the main functional components that participate in the decision process related to assess integrity and in case that is not compatible with the specific flight phase then a recovery action is adopted.

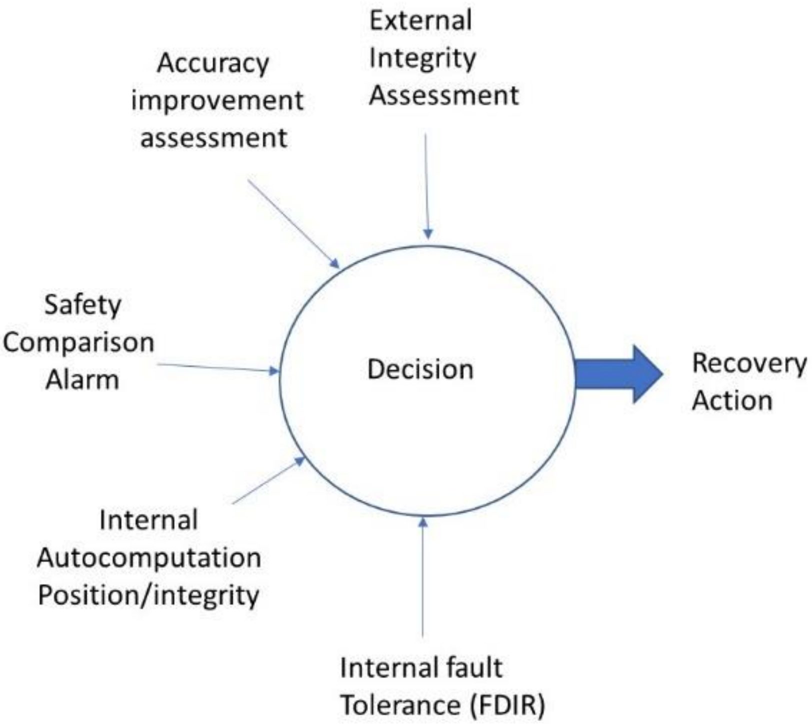

Accuracy improvement assessment
External Integrity Assessment
Safety Comparison Alarm
Decision
Recovery Action
Internal Autocomputation Position/integrity
Internal fault Tolerance (FDIR)

Figure 23. Integrity computation process on board

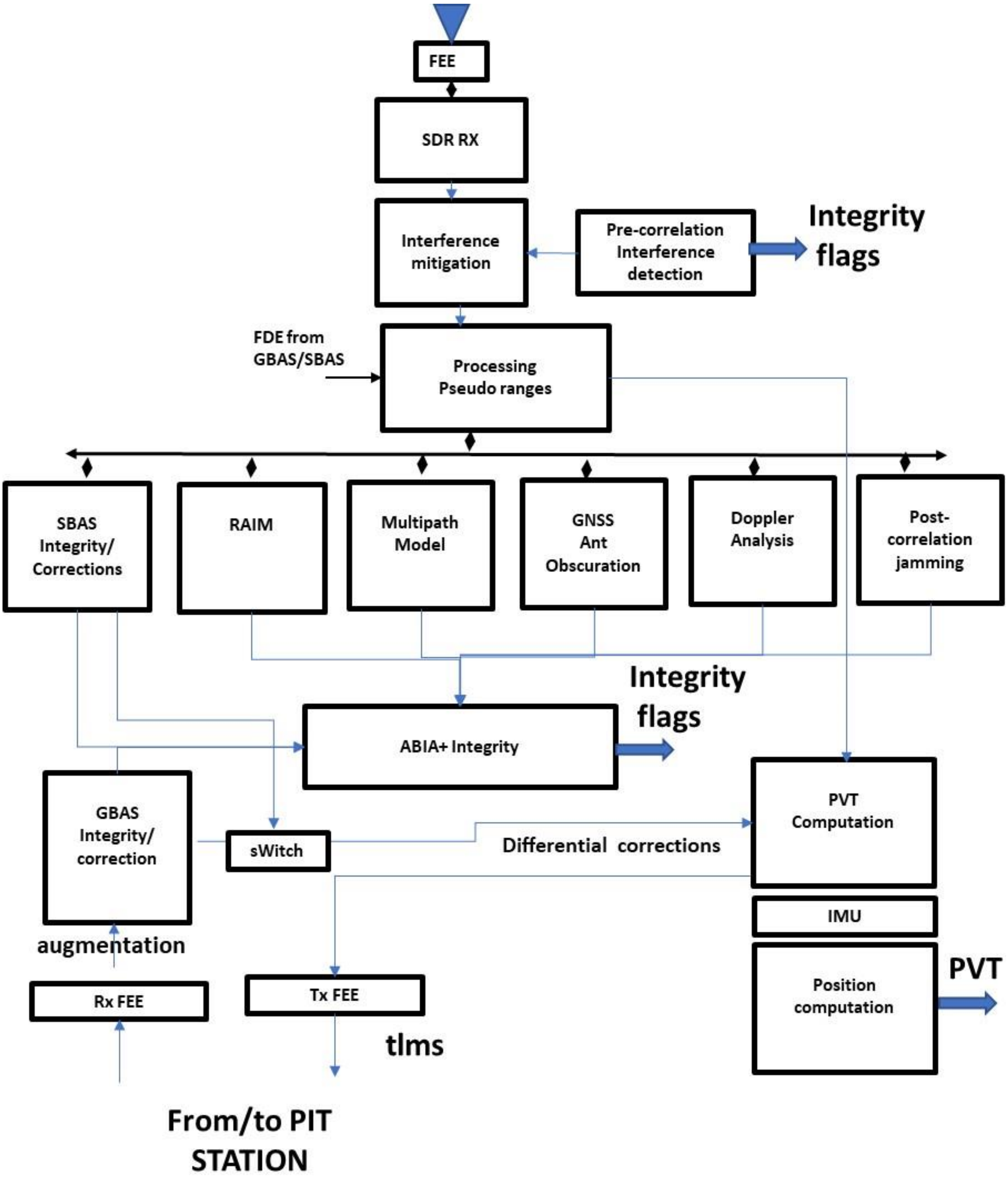


Figure 24. Avionic integrated integrity functional block diagram according to ABIA principle and legacy standard ARAIM

According to the characteristic of the UAV and the selected mission the on-board system can be properly tailored to respond to requirement in terms of:

- Cost/complexity
- Mission phase
- Available support for external sources (space/ ground)

In this case of Navigation aid is lost the UAV/RPAS usually enters an emergency state where the rotorcraft hovers and tries to land using other sensors such as an altimeter (in the case of fixed-wing aircrafts the engines are stopped and a parachute is launched).

The augmentation of GNSS benefits aviation domain in many respects:

- Increase the access to the landing areas
- Allows direct en route flight paths
- Improved and innovative approach services
- Reduced or simplified on board equipment

With HELMET and PIT stations we:

- Improve PVT integrity (see Figure 24)
- Provide accuracy services
- Improve safety and security of flights
- Aid emergency operations
- Improve mission plan and control
- Allows BLOS operations

Communication integrity issues

Moreover we should recognize the key importance of communications for bringing the augmentation ground data to/from the RPAS. Clearly the integrity, availability and continuity of communications should have even better performance of the GNSS itself in order to be effective.

This link can be either a line of sight (LOS) air-ground (AG) link between the two entities or a beyond line-of-sight (BLOS) link using another platform such as a satellite or high-altitude platform (HAP). Data rates for such links are expected to be modest (e.g., a maximum of 300 kbps for compressed video, which would not be used continuously).

In this respect another important function of GNSS is to provide data for the ADS-B equipment that likely will be mounted in same configuration in all the future system if operated in BLOS.

The ADS-B can provide the useful information for UTM. This can provide for instance sequencing and de-conflict constraints (see landing) , flight plan/mission objectives, separation assurance and collision avoidance and of course environmental constraints.

In this case it is important to evaluate if the augmentation data that we derive from HELMET can be transferred via the C2/3 link or by a dedicated additional link.

The communication link a general key issue of UAV/RAPS operation completely different form the other applications for the time being where we have autonomy or pilot seated in the vehicle.

Communication lost is even more critical than EGNSS data or integrity degradation and can leads to immediate recovery actions. it is a common practice that if the radio link is lost, then the autopilot commands the aircraft to go to a predetermined waypoint (what is commonly known as return-to-home).

3.3.5 General system operational requirement

General system operation requirement for out specific applications are:

1) The integration of UAS/RPAS shall not imply a significant impact on the current users of the airspace;
2) UAS/RPAS shall comply with existing and future Civil Aviation Regulations and Procedures;

3) UAS/RPAS integration shall not compromise existing aviation safety levels, nor increase risk: the way UAS/RPAS operations are conducted shall be equivalent to manned aircraft, as much as possible;

4) UAS/RPAS shall comply with the SESAR trajectory management process;

5) All UAS/RPAS shall be able to comply with ATM/UTM air traffic control rules/procedures;

6) UAS/RPAS shall comply with the capability requirements applicable to the airspace within which they are intended to operate.

7) If the UAV/RPAS loses communications or loses its GNSS NAV signal, it must enter in the emergency mode and implement suitable recovery actions

8) If UTM or other sensor recognise potential collision probability the system shall implement recovery procedure in order to avoid obstacle.

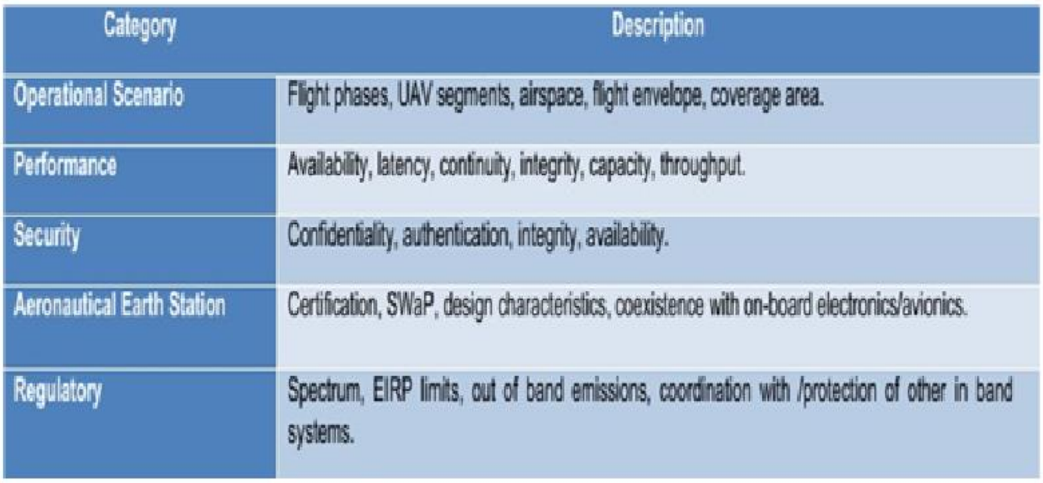
9) Overall system position accuracy and integrity will be such to guarantee the accomplishment of all the above points according to the std UAV aviation requirement.

10) All the system will be synchronized at UTC time

11) All communication interfaces will be designed with high std of integrity and security.

3.3.6 Requirement categorization and functionality description

The overall system requirement categorization will follow what presented in Figure 25.



Category	Description
Operational Scenario	Flight phases, UAV segments, airspace, flight envelope, coverage area.
Performance	Availability, latency, continuity, integrity, capacity, throughput.
Security	Confidentiality, authentication, integrity, availability.
Aeronautical Earth Station	Certification, SWaP, design characteristics, coexistence with on-board electronics/avionics.
Regulatory	Spectrum, EIRP limits, out of band emissions, coordination with /protection of other in band systems.

Figure 25. Requirement categorization

Detailed requirement specification are provided in Section 5.

OBU general Description

UAV avionics will include the following equipment / functions:

- EGNSS rx Galieo/ GPS two frequencies
- IMU (accelerometer, gyro)
- Magnetic compass, barometer
- SW for position and navigation integration based on Kalman filter

- Autopilot
- On board SW controller with FDIR
- Remote C2 communication link with navigation Augmentation
- VBN (visual based navigation) based on PIT station reference, loaded maps and sleeper coded, used for navigation check point and attitude calibration.
- ADS-B transmitter (to be confirmed)
- Antennas for GNSS and communication
- TCXO oscillator for on board frequencies and timing generation with synchronization capability with GNSS pps.

Protection mechanisms to assurance communication integrity will be also implemented.

A representative block diagram of OBU for UAV is given in Figure 26.

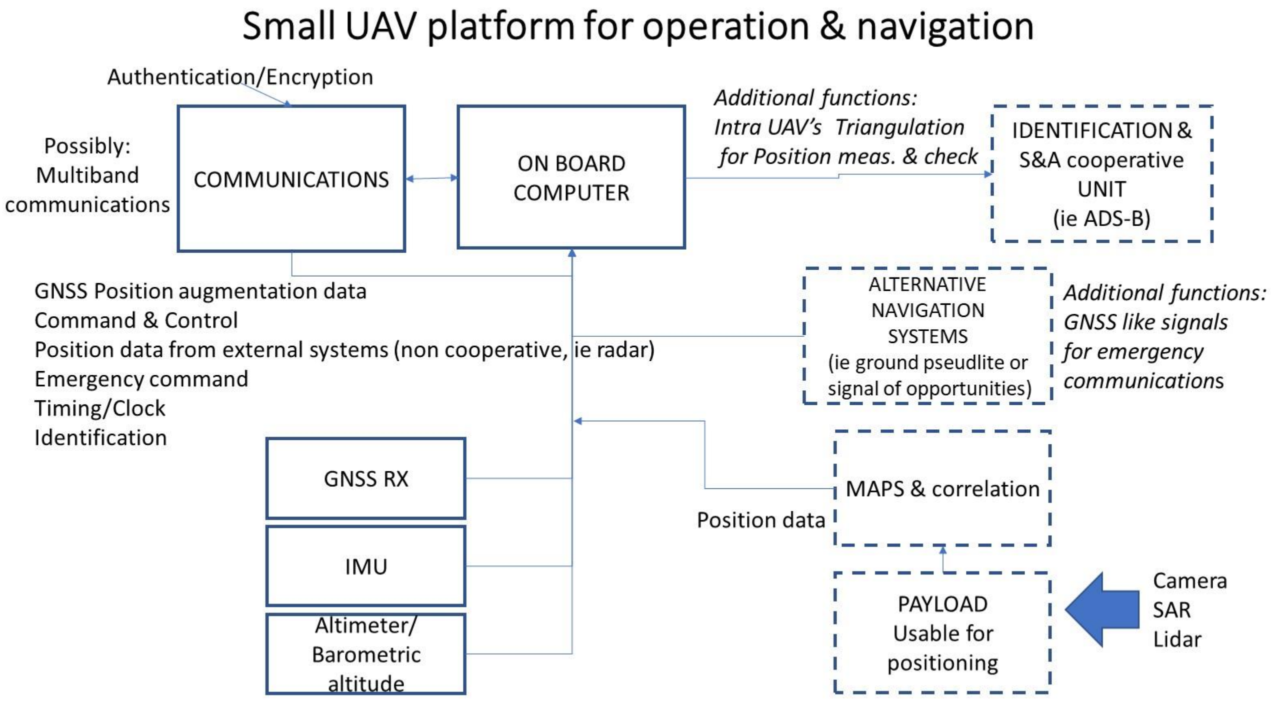
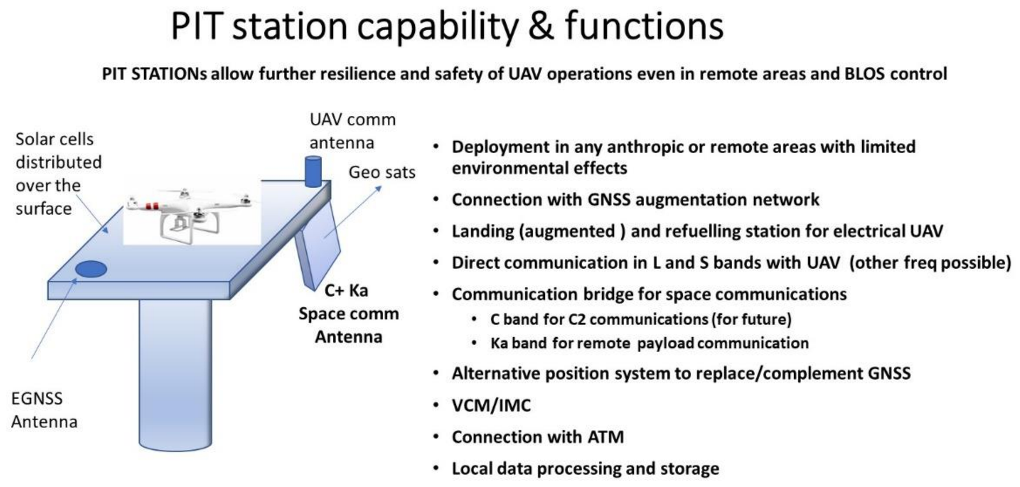


Figure 26. UAV OBU functional block diagram

PIT station general description

PIT station consist of a ground terminal characterized by a UAV landing areas and a number of equipment including sensor and communication unit to support the UAV missions – see Figure 27. PIT stations will be deployed all along the mission path at a suitable inter-distance such to allow the complete coverage of the mission areas.



PIT station capability & functions

PIT STATIONs allow further resilience and safety of UAV operations even in remote areas and BLOS control

- Deployment in any anthropic or remote areas with limited environmental effects
- Connection with GNSS augmentation network
- Landing (augmented) and refuelling station for electrical UAV
- Direct communication in L and S bands with UAV (other freq possible)
- Communication bridge for space communications
  - C band for C2 communications (for future)
  - Ka band for remote payload communication
- Alternative position system to replace/complement GNSS
- VCM/IMC
- Connection with ATM
- Local data processing and storage

Figure 27. PIT station functions

The PIT station functions are:

- Deployment capability in any anthropic or remote areas with limited environmental effects
- Landing (augmented and automated) site with wireless refuelling/recharging station for electrical UAV
- Direct communication in L ,S or C bands with UAV (TBD)
- Communication relay for space and ground C2/3 communications
- Communication relay for space for mission data tx in Ka band
- GNSS local integrity station (including interference monitoring and position accuracy augmentation) with communication messages in contact with HELMET augmentation station
- Local data processing and storage
- Local access to LOS UAV control
- Support for ATMUTM by ADS-B rx
- Provide georeferenced site for optical navigation augmentation sensor
- Internal BITE and autocalibration capability
- Local capability to connect directly an operator to a UAV

PIT station equipment/systems:

- EGNSS tri frequencies antennas
- Omnidirectional communication antenna
- High gain directional antennas
- ADS-B antenna
- WIDE FOV optical arrangement for surrounding and landing areas monitoring
- Satellite antenna (optional)
- Remote communication network modem

As option local radar for UAV control will be implemented in critical areas- The PIT station can also determine the UAV heading by connecting the PIT station antenna with the UAV antenna as for Figure 28. The PIT station internal receiver computes the heading also with support of UAV gyros.

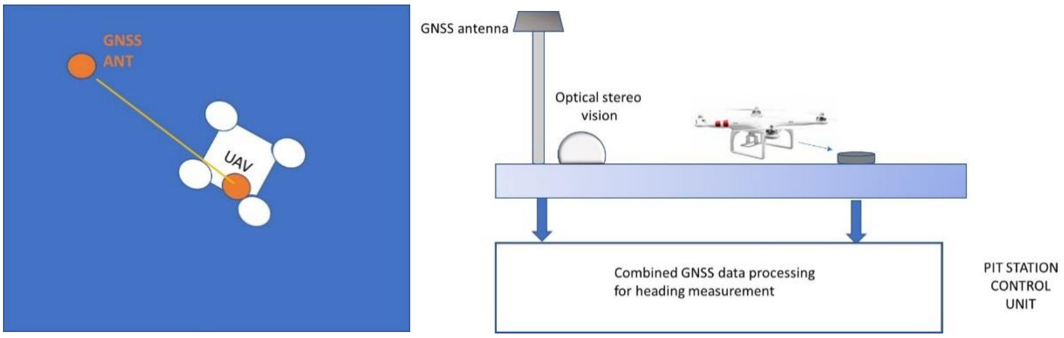


Figure 28. Determination of UAV heading by combined processing of PIT station and on board GNSS Rx

Communication links requirement

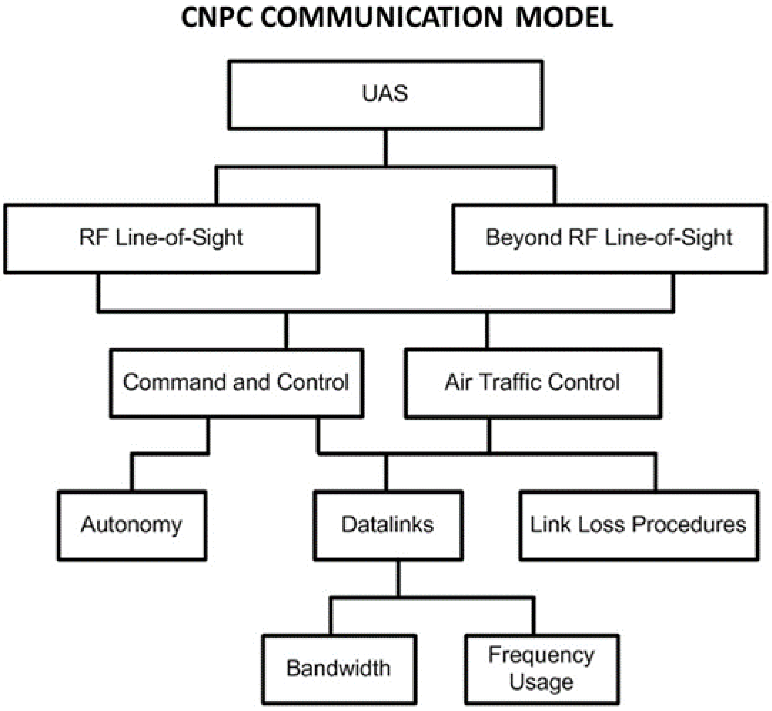


Figure 29. UAV Communication model

In Figure 29 the UAV/RPAS communication model is provided. Note that in our case the BLOS and LOS communications pass both through the PIT stations even if satellite communication can be directly used if the UAV embark a suitable terminal.

In Figure 30 the PIT station communication arrangement is provided.

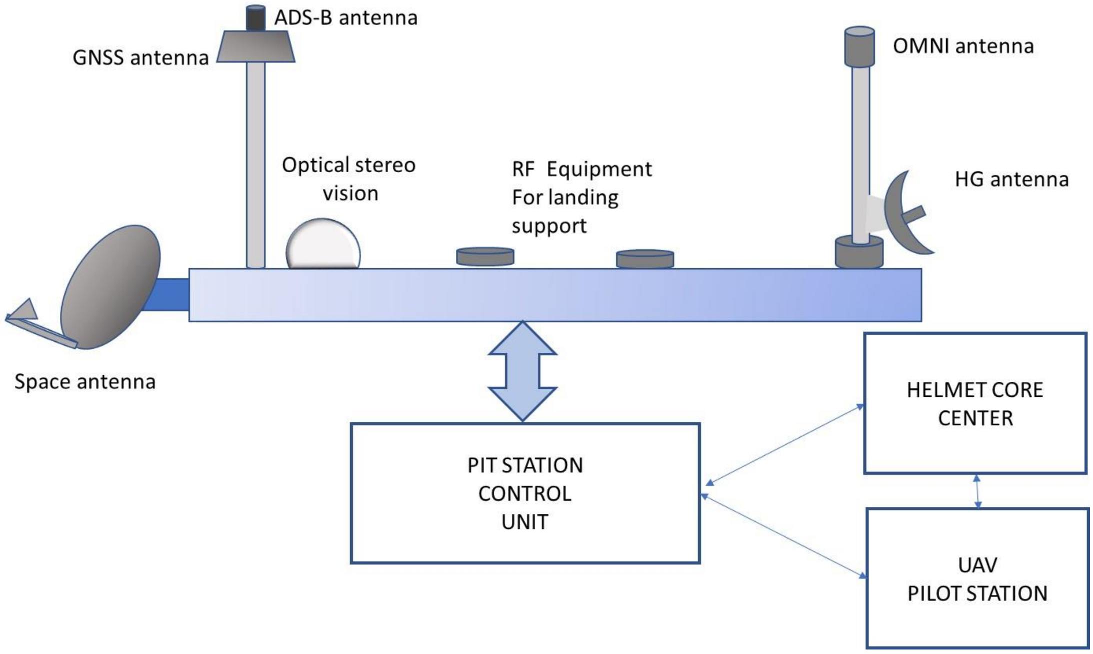


Figure 30. PIT station communication link arrangement

The PIT stations by omni antenna will be capable to:
• Fix communications by the omni antenna that operates on dedicated frequency channels, that change cell by cell
• determine the UAV position by its GNSS data
• determine frequency value, frequency doppler, power levels of the link with UAV
• on the basis of above points to send the link characteristic to the steerable antenna and UAV to initialize the operative connection
A steerable antenna in a first assumption is devoted to control only a single UAV.

The key parameters are:

- Latency
- Frequency and relative BW
- Data Rate
- FEC

Major communication requirement are:

- **UAV/PIT stations C2 full duplex**

C2 and augmentation data rate:
Up: 10 Kbits/s
Down: 300 Kbits/s
BER: 10-5

- **UAV/Pit station data (unidirectional)**

Down: 1-2 Mbits
By HGA antenna

- **PIT station-intra network (with operator)**

Data Rate: 100MBits/s bidirectional
QoS: selectable with minimum latency (<100msec) in case of emergency
BER: 10-7 (10-9 for non-emergency data)

- **PIT station Satellite**

For C2
FWD: 10 Kbits/s
RETURN: 300 Kbits/s
For Mission data
FWD: 10 Kbits/s
RETURN: 10 Mbits
By dedicated space antenna vs GEO satellite.
PIT Station data to Helmet core centre

- EM status
- EGNSS local rx data

PIT Station data to UTM via Operator station

- Local visibility status
- ADS-B data

PIT Station data to Operator station

- PIT station health status
- All the data acquired by its sensors

- **Remote augmentation system (Helmet)**

The remote augmentation system will provide to operator centre:

- EGNSS Satellite mask
- PPP-RTK data
- DGNSS data
- SBAS data via internet

All the links will be characterized by high degree of integrity achieved by encryption authentication and acknowledge.

The loss of a data link must be addressed by a link-loss procedure. It is important that the aircraft always operates in a predictable manner. From the survey, it was revealed that the most common link-loss procedure is for the aircraft to fly to a predefined location. Once at the predefined location, the UAS can either loiter until the link is restored, it can autonomously land, or it can be remotely piloted via secondary data link and/or redundant main data link at cold or semi-hot condition(s) (Depending on the RPAS category, complexity and operational/mission capabilities).

For additional secure communication proof, one approach is for the UAV to acknowledge or echo all commands it receives. This will ensure the operator that all commands sent are received and acknowledged. Such an approach will also notify the operator if the aircraft receives commands from an unauthorized entity.
In case the commands can be simultaneously received from both BLOS and LOS links, a priority setting will define priorities.

3.4 OVERALL FUNCTIONAL ARCHITECTURE FOR HELMET

In the following, the overall Multimodal System Architecture is reported – see Figure 31.

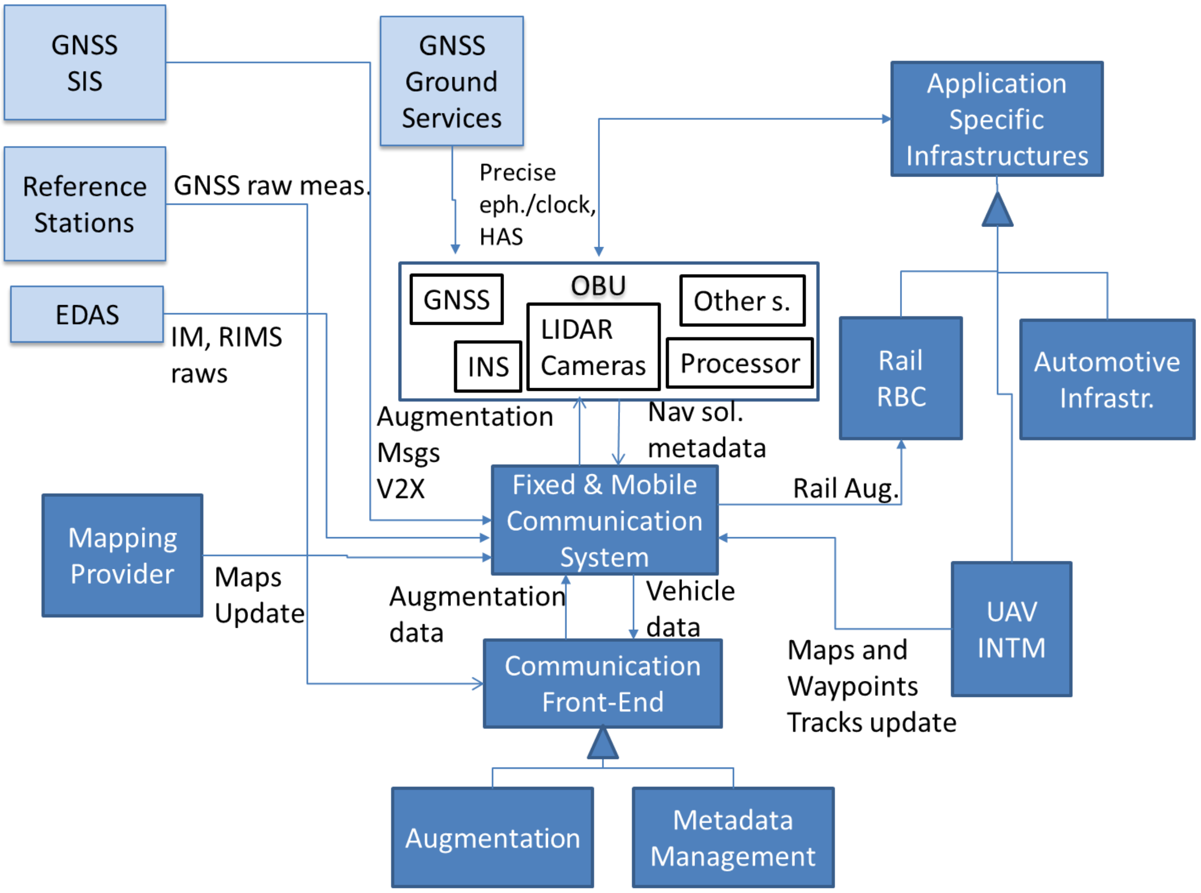


Figure 31 Overall HELMET High Level Architecture

OBU: it is installed within trains, cars and UAV and it is based on GNSS receivers, tightly or loosely coupled with Inertial Sensors, LIDAR and Communication router. A processor is in charge of managing communication with the Augmentation System and the other specific applications processing.

Mobile Communication System: it is the fixed and mobile communication system in charge of implementing the link between the Augmentation Communication Front-End and the Reference Stations, as well as the Mapping Provider and Augmentation System and the Rail Radio Broadcasting Centre (RBC). It also implements also the link between the Communication Front-End and the OBU for transmitting Augmentation data and receiving relevant ancillary data (e.g. sensors).

Communication Front-End: it implements the Gateway for Augmentation data broadcasting and Reference Stations data gathering.

Augmentation: it is the Augmentation system in charge of generating Augmentation data.

Metadata Management: it manages ancillary data coming from on-field sensors.

Mapping Provider: it is in charge of providing Maps and Maps update to the OBU.

Rail RBC: it is the ERTMS Radio Broadcasting Centre in charge of communication between Rail trackside and the train.

Automotive Infrastructure: it implements the Road Infrastructure for V2I.

UAV INTM: it is the UAV tracking monitoring system.

For the Augmentation system, the logical functions decomposition is defined as in Figure 32.

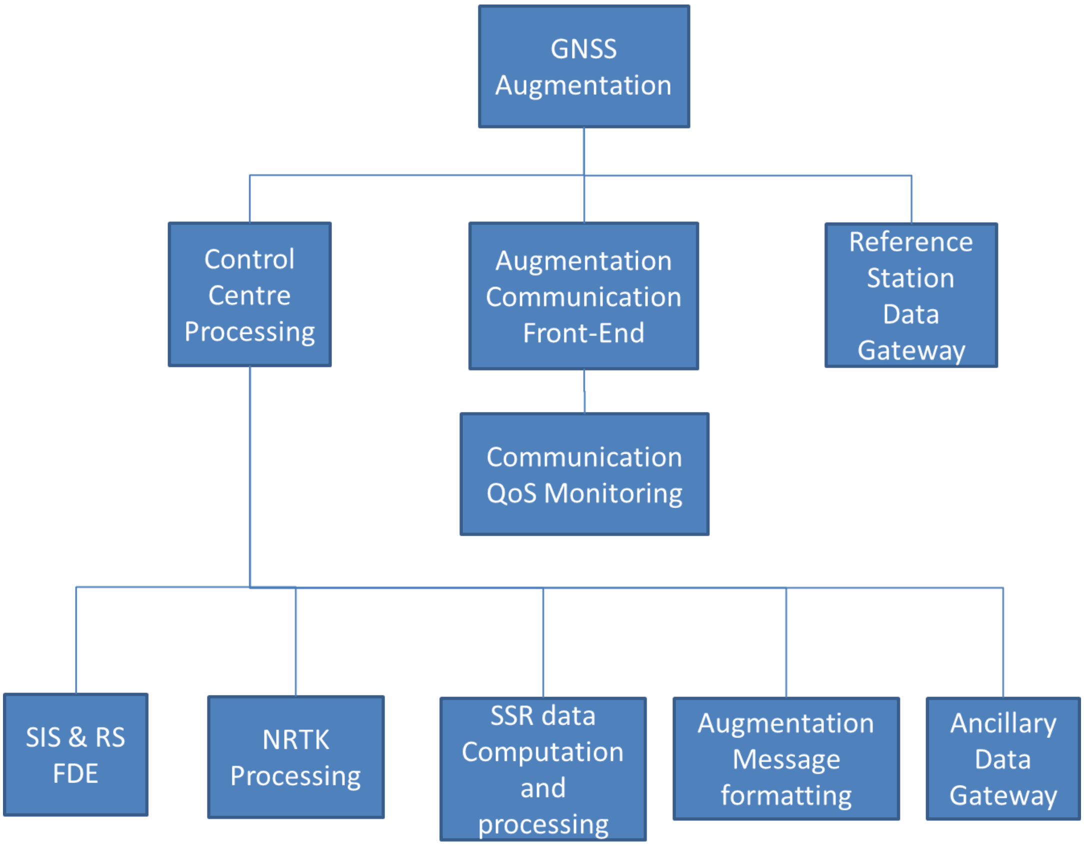

GNSS Augmentation
Control Centre Processing
Augmentation Communication Front-End
Reference Station Data Gateway
Communication QoS Monitoring
SIS & RS FDE
NRTK Processing
SSR data Computation and processing
Augmentation Message formatting
Ancillary Data Gateway

Figure 32 Augmentation Functional Logical Components

GNSS Augmentation is composed by the following main functions:

Augmentation Communication Front-End: it is the gateway for Augmentation messages broadcasting to the user receiver or single applications broadcasting centre through Standard protocol and data formats.

Communication Q0S Monitoring: it implements the monitoring of Communication systems for Fault Detection and Exclusion.

Reference Station Data Gateway: it is in charge of Reference Stations data streams acquisition by the High QoS Communication system through a standard protocol.

Control Centre Processing: it implements the Augmentation data processing through the following sub-functions:

- **SIS & RS FDE**: it implements the Reference Stations and GNSS Signal In Space Fault detection and Exclusion.
- **NRTK Processing**: it implements the RTK and NRTK processing; NRTK implies the processing of clusters of Reference Stations and processing through Single Reference Stations ambiguity fixing and Ionospheric interpolation techniques.
- **SSR data computation and processing**: it implements precise ephemeris, satellite clocks and satellite biases data calculation or gathering from available sources (e.g. IGS RTS); if PPP-RTK is implemented, precise Local ionospheric and tropospheric errors are developed
- **Augmentation Messages Formatting**: it implements message formatting through the most diffused protocol and data format (currently RTCM NTRIP and SC-104 format and SC-134 for Integrity Monitoring purposes).

Ancillary Data Gateway: it collects data from external sensors for reference data gathering, e.g. sensors data and waypoints.

4. SAFETY AND DEPENDABILITY ANALYSIS

Due to the relevance of safety requirements for the present project, a preliminary and dependability safety analysis is needed for deriving safety requirements allocation to each safety functions, to be inserted within safety requirements, is performed.

4.1 RAIL: SAFETY ANALYSIS FOR ERTMS VIRTUAL BALISE CONCEPT

Railway safety analysis related to HELMET is performed for the ERTMS Virtual Balise concept, which enhances the baseline ERTMS in order to reduce operational costs and further improve interoperability. The related Enhanced ERTMS architecture with its main functions has been outlined in Section 3.

Train Position, Velocity and Time (PVT) represent the vital information for railway signalling. Physical balises installed on a track (i.e. ETCS Information Points) are used for train position determination and reporting to the track-side Radio Block Centre (RBC). Virtual Balises detected by GNSS on board of a train efficiently substitute ETCS track balises and thus the investment and maintenance costs can be reduced.

The intention of the safety analysis it is to specify system requirements for the HELMET solution from the railway point of view. The main attention in this safety analysis is focused on the most demanding ERTMS operational scenario, which is Start of Mission in Staff Responsible without a priori known position of train and especially when it is necessary to determine one which of parallel tracks (e.g. in station) the train is located. This Track identification / discrimination function cannot be solved using standalone EGNOS, because Alerts Limits guaranteed for aviation safety operations are larger than required for RAIL. Safety requirements for odometry calibration and train cold movement detection functions, both required also for ERTMS, are also considered.

4.1.1 Allocation of ETCS Core Hazard Rate to Balise Subsystem

During years 1996 to 1998 a group of six European railways under the name of ERTMS Users Group (DB, FS, NS, Railtrack, RENFE and SNCF) were engaged in drafting the ERTMS/ETCS specifications. The safety analysis was based on statistical data from the participating railways. The National Safety Agencies in an ESROG (ERTMS Safety Requirements and Objectives Group) meeting have agreed on a harmonised safety target for ERTMS/ETCS, based on DB and SNCF results and the assessment report. It was et the end of 2001. This overall target is expressed as a quantitative target of 2e-9 hazardous HW failure per 1 hour and per train (1e-9/ hr for onboard and 1e-9/hr for trackside), which corresponds to SIL 4.

In the HELMET project, the ERTMS/ETCS safety target of 2e-9/ hr/ train is considered as a high-level safety requirement for ERTMS/ETCS. Figure 33 shows the allocation the ETCS Core Hazard Rate to the ETCS balise subsystem – see ETCS/ERTMS SUBSET-088, Part 3 [13].

It is evident in Figure 33 that ETCS Core hazard rate is split into the following contributes:

- transmission hazard (THR allocated by UNISIG SUBSET 091 = 0.67e-9/h);
- on board hazards (THR allocated by UNISIG SUBSET 091 = 0.67e-9/h);
- trackside hazards (THR allocated by UNISIG SUBSET 091 = 0.67e-9/h).

According to the SUBSET 091 setup the ‘transmission’ hazard is intended to collects all the contribution due to the ‘non-trusted parts’ (i.e. not safe) of the trackside <-> on-board communications to the ETCS failure rate. Therefore, the TRASMISSION hazard (THR-TX in Figure 33) receives contributions from: the radio sub-system (THR-RTX) and from the balise sub-system (THR-BTX).

The balise THR-BTX is further allocated to following hazardous events:

- **TRANS-BALISE-1: ETCS Balise Corruption:** $THR_{BTX\ Corruption} < 1.0e\text{-}11\ hour^{-1}$.
- **TRANS-BALISE-2: ETCS Balise Deletion:** $THR_{BTX\ Deletion} = 3.3e\text{-}10\ hour^{-1}$;
- **TRANS-BALISE-3: ETCS Balise Insertion:** $THR_{BTX\ Insertion} = 3.3e\text{-}10\ hour^{-1}$;

TRANS-BALISE-1: ETCS Balise Corruption - is related to the corruption of a BG message during its transmission from track-side to on-board.

TRANS-BALISE-2: ETCS Balise Deletion - means an event when no Information Point (IP) is detected due to a track balise or Balise Transmission Module (BTM) failure. Any missed detection of a single IP cannot lead to a hazard. There is no safety requirement in respect of not being able to detect an information point when IP linking by odometry is active (ERTMS/ETCS subset-088). If two expected consecutive IPs announced by linking are not detected, the on-board vital computer shall consider the linking command of the second IP as a command to apply the service brake. ETCS balises are fixed on track in known positions. If the balise is not detected by on-board in the anticipated (expectation) window, measured from the Last Relevant Balise Group (LRBG), then linking reaction is applied and a safe state of train is maintained.

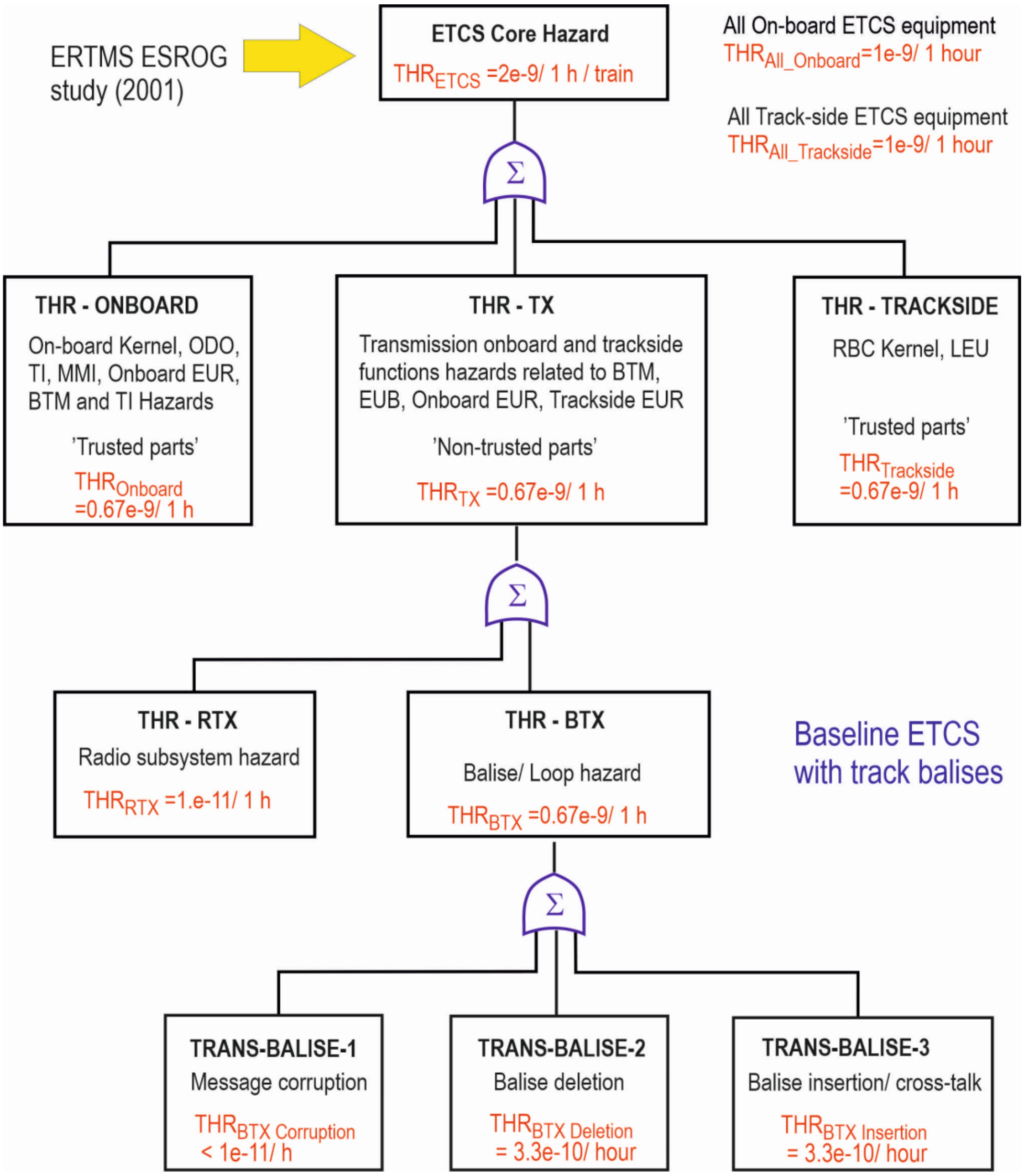

ERTMS ESROG study (2001)
ETCS Core Hazard
THR_ETCS =2e-9/ 1 h / train
All On-board ETCS equipment
THR_All_Onboard=1e-9/ 1 hour
All Track-side ETCS equipment
THR_All_Trackside=1e-9/ 1 hour
Σ
THR - ONBOARD
On-board Kernel, ODO, TI, MMI, Onboard EUR, BTM and TI Hazards
'Trusted parts'
THR_Onboard =0.67e-9/ 1 h
THR - TX
Transmission onboard and trackside functions hazards related to BTM, EUB, Onboard EUR, Trackside EUR
'Non-trusted parts'
THR_TX =0.67e-9/ 1 h
THR - TRACKSIDE
RBC Kernel, LEU
'Trusted parts'
THR_Trackside =0.67e-9/ 1 h
Σ
THR - RTX
Radio subsystem hazard
THR_RTX =1.e-11/ 1 h
THR - BTX
Balise/ Loop hazard
THR_BTX =0.67e-9/ 1 h
Baseline ETCS with track balises
Σ
TRANS-BALISE-1
Message corruption
THR_BTX Corruption < 1e-11/ h
TRANS-BALISE-2
Balise deletion
THR_BTX Deletion = 3.3e-10/ hour
TRANS-BALISE-3
Balise insertion/ cross-talk
THR_BTX Insertion = 3.3e-10/ hour

Figure 33. Allocation of ETCS Core hazard to balise subsystem hazards

TRANS-BALISE-3: ETCS Balise Insertion - means detection of a wrong IP (balise group) or erroneous order of reported track balises due to a balise failure (too strong up-link signal) or on-board BTM failure. Balises can be inserted from adjacent tracks (e.g. single and double antenna effect, etc).

In case of ERTMS Virtual Balise concept it is necessary to correctly assign hazardous GNSS-based train position determination failures to the above balise subsystem hazardous invents. It is explained in next Section.

4.1.2 Allocation of ETCS Core Hazard Rate to Virtual Balise detection

Adopting the concepts of trusted and non-trusted parts, the components of the Virtual Balise Transmission System introduced in the proposed architecture (see Section 3.1) can be characterized as follows:

- Trusted (safe) parts:
  - Virtual Balise Reader Functions
  - GNSS Augmentation Dissemination / Trackside Verification
- Non-trusted parts:
  - Global Navigation Satellite System, i.e. the combined ground and airborne subsystems in its role as a source of positioning errors (failures and feared events originating from the system)
  - Airgap as the set of interfaces among SVs and on-board train GNSS Antenna. Therefore, the airgap refers to the GNSS signal in space as a source of positioning errors (feared events originating from the propagation environment)
  - On-board GNSS antenna.

In the Virtual Balise concept (see Figure 34), the TRASMISSION hazard (THR-TX) receives contributions from: the radio sub-system hazard THR-RTX with $THR_{RTX} < 1e\text{-}11/\ h$, and the Virtual Balise sub-system hazard THR-VBTX with $THR_{VBTX} = 6.7e\text{-}10/\ h$. Since the Virtual Balise insertion TRANS-VBALISE-3, i.e. cross-talk due to the incorrect GNSS-based train position determination, is much dangerous than the Virtual Balise deletion (TRANS-VBALISE-2) – see Figure 34, then risk due TRANS-VBALISE-2 is also allocated to TRANS-VBALISE-3.

Then the total value of THR corresponding to the Virtual Balise insertion (TRANS-VBALISE-3) is $THR_{VB\_Insertion} = 6.6e\text{-}10/\ h$. Since it is also necessary to detect Virtual Balises on parallel tracks, then the TRANS-VBALISE-3 event with $THR_{VB\_Insertion} = 6.6e\text{-}10/\ h$ is equally split between event H7 (Erroneous localisation of a VB, with reception of valid balise information, i.e. VB Insertion along track) with $THR_{H7} = 3.3e\text{-}10/\ h$, and event H9 (Erroneous reporting of a VB in a different track, i.e. VB Insertion across track) with $THR_{H9} = 3.3e\text{-}10/\ h$ [14] – see Figure 34.

The $THR_{H9} = 3.3e\text{-}10/\ h$ together with Alert Limit of 1.785 m [1] required for the Track discrimination function represents the most demanding requirement on HELMET solution from railway point of view.

The TRANS-BALISE-1 with $THR_{VB\ Corruption}$ < 1e-11/h (see Figure 34) corresponds to the safety requirements for communications associated with the GNSS based position determination function.

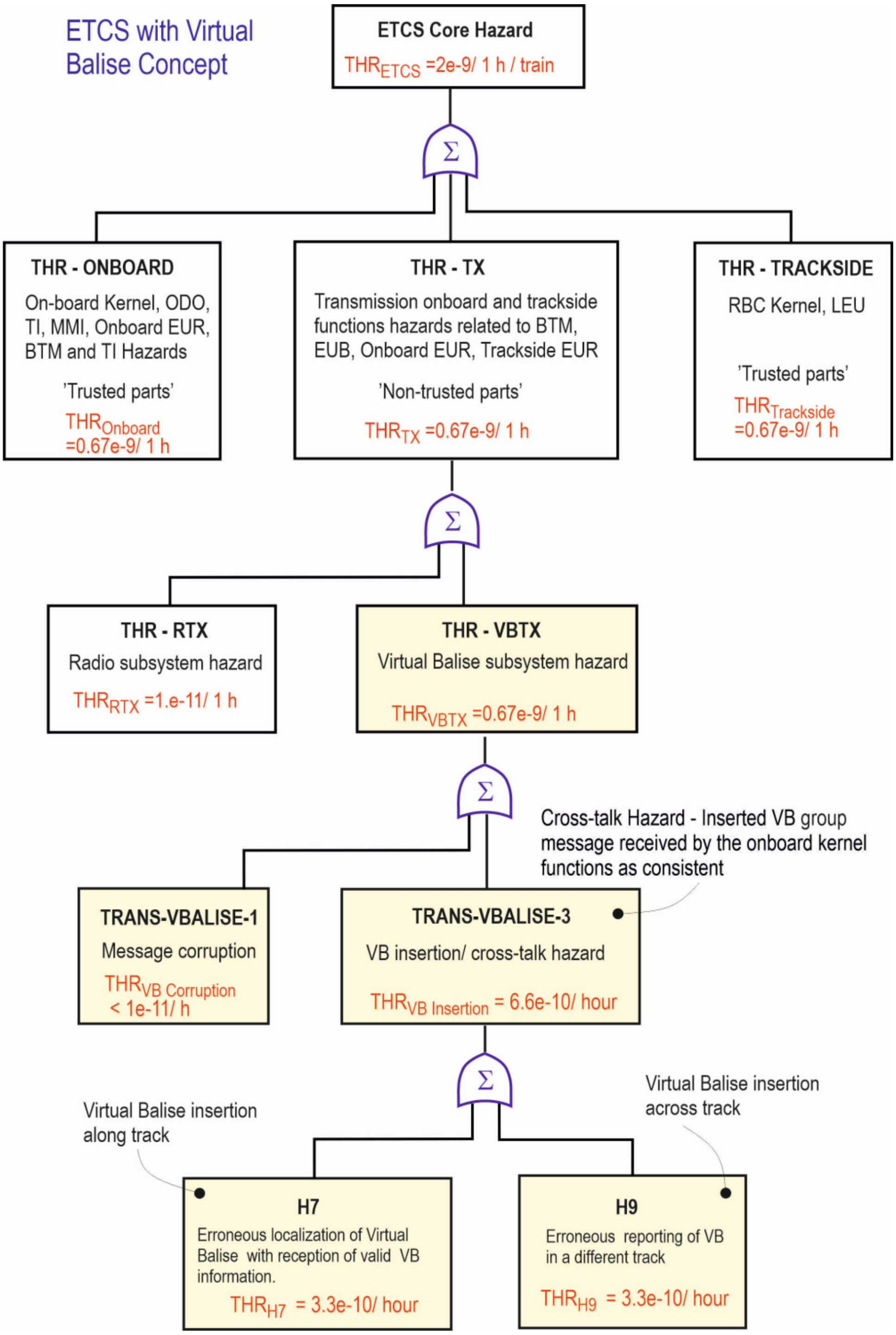

ETCS with Virtual Balise Concept
ETCS Core Hazard
THRETCS =2e-9/ 1 h / train
Σ
THR - ONBOARD
On-board Kernel, ODO, TI, MMI, Onboard EUR, BTM and TI Hazards
'Trusted parts'
THROnboard =0.67e-9/ 1 h
THR - TX
Transmission onboard and trackside functions hazards related to BTM, EUB, Onboard EUR, Trackside EUR
'Non-trusted parts'
THRTX =0.67e-9/ 1 h
THR - TRACKSIDE
RBC Kernel, LEU
'Trusted parts'
THRTrackside =0.67e-9/ 1 h
Σ
THR - RTX
Radio subsystem hazard
THRRTX =1.e-11/ 1 h
THR - VBTX
Virtual Balise subsystem hazard
THRVBTX =0.67e-9/ 1 h
Σ
Cross-talk Hazard - Inserted VB group message received by the onboard kernel functions as consistent
TRANS-VBALISE-1
Message corruption
THRVB Corruption < 1e-11/ h
TRANS-VBALISE-3
VB insertion/ cross-talk hazard
THRVB Insertion = 6.6e-10/ hour
Σ
Virtual Balise insertion along track
Virtual Balise insertion across track
H7
Erroneous localization of Virtual Balise with reception of valid VB information.
THRH7 = 3.3e-10/ hour
H9
Erroneous reporting of VB in a different track
THRH9 = 3.3e-10/ hour

Figure 34. Allocation of ETCS Core hazard to Virtual Balise subsystem hazards

4.1.3 Justification of THR allocation to Virtual Balise Insertion

This section deals with the justification of THR requirement for Virtual Balise insertion (TRANS-BALISE-3, $\text{THR}_{\text{VB Insertion}}$ of 0.66e-9/ h) and clarifies some assumptions in SUBSET-088, Part 3, Annex A, Section 7 with regard to the Virtual Balise concept.

The derivation is performed for the most demanding operational scenario, which is Start of Mission (SOM) in Staff Responsible (SR) with the UNKNOWN train position status – when linking of Balise Groups (BGs) by ETCS odometry cannot be applied.

The cross-talk effect causing insertion of wrong Balise Group (BG), which represents a system hazard, is considered in this THR derivation. For the purpose of the derivation two following scenarios are compared: 1) cross-talk in case of base-line ETCS with track balises, and 2) “cross-talk” in case of ETCS Virtual Balise (VB) detection by means of GNSS. Differences in possibilities of cross-talk mitigation in case of baseline ETCS with physical balises and in case of “cross-talk” effects on Virtual Balise detection are taken into account.

The fundamental question is whether there are available some operational provisions in respect to the ETCS Virtual Balise Concept, which could be utilised for hazard mitigation due to VB insertion as it is applied in case of cross-talk in the baseline ETCS with track BGs.

THR requirement for insertion of ETCS BG due to cross-talk effect

Derivation of the ETCS requirement for incorrect insertion of track BG due to cross-talk is derived in the SUBSET-088, Part 3, Annex A, Section 7 [13]. The corresponding scenario is depicted in Figure 35(a). The cross-talk effect can cause insertion of incorrect BG due to e.g. the two antennae problem. The vulnerability of the system depends on the duration that the system is in Staff Responsible (SR) and the likelihood that there is an adjacent information point during this time period.

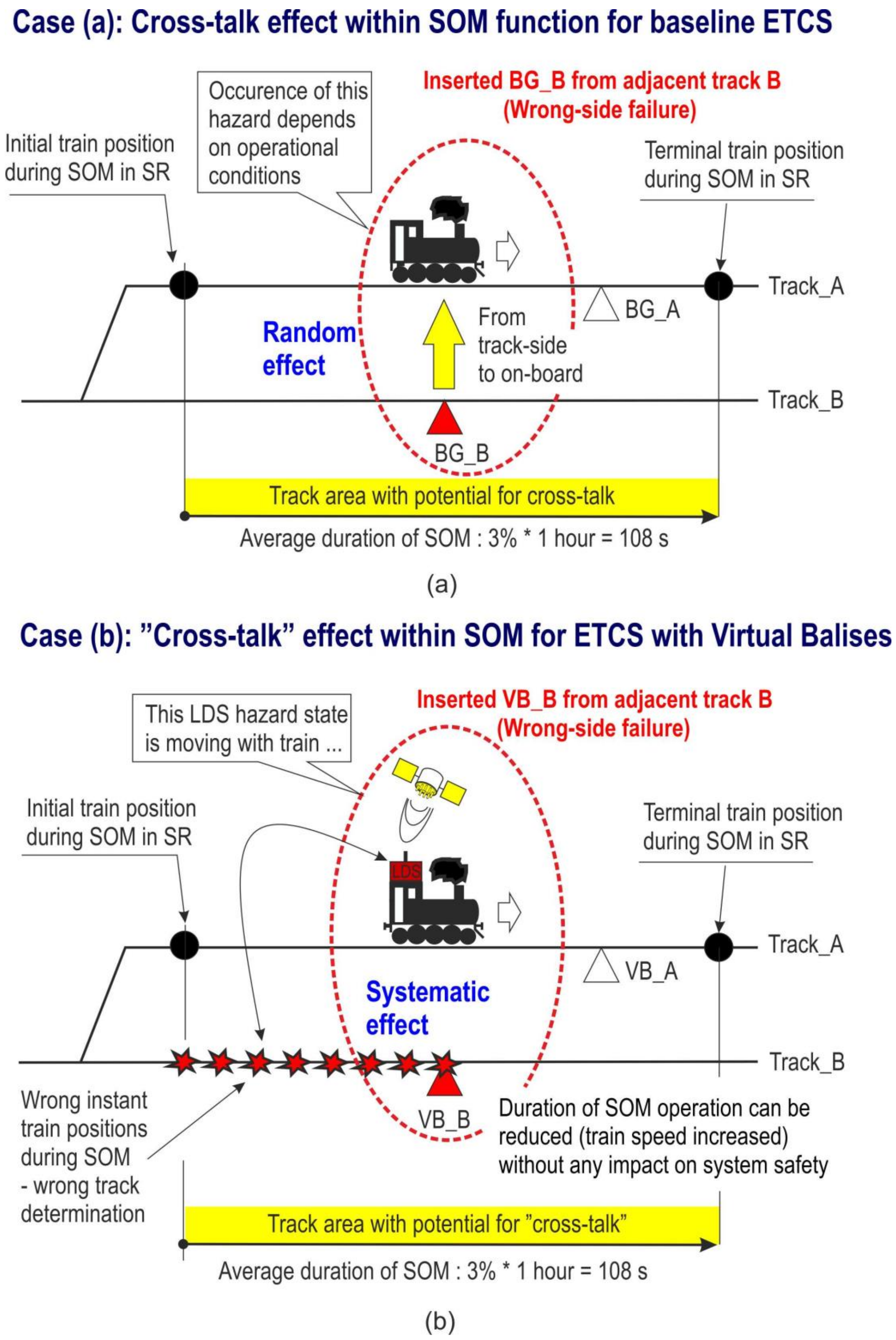
It is evident from the ETCS Level 2 Mission profile that the time spent in SR is 3% of the mission (1 hour), i.e. 108 seconds. Further, it is assumed that about 50% of the information points are encountered with cross-talk because of the traffic conditions (SUBSET-088, Part 3, Annex A, Section 7.2.1.5) [13]. Due to the above reasons it is possible to derive THR target for cross-talk during SOM as follows

$$\text{THR}_{\text{Cross-talk}} = \text{THR}_{\text{Trans-Balise-3}} * 100/(0.5*3) = 3.3\text{e-}10/\ \text{hr} * 100/1.5 = 2.2\text{e-}8/\ \text{hr}$$

The Risk Reduction Factor (RRF) corresponding to the cross-talk mitigation can be expressed as

$$\text{RRF} = \text{THR}_{\text{Cross-talk}} / \text{THR}_{\text{Trans-Balise-3}} = (2.2\text{e-}8\ \text{hr}^{-1})\ /\ 3.3\text{e-}10\ \text{hr}^{-1} = 66.\ 66$$

It can be justified by: 1) shortening of duration of train operation with potential cross-talk occurrence, i.e. shortening of duration of train operation from 1 hour (duration of the whole mission) to 108 seconds for SOM, and 2) reduction of number of balise groups encountered with cross-talk depending on train operational conditions – i.e. low traffic vs. high traffic and related the two antennae effect causing cross-talk.


Case (a): Cross-talk effect within SOM function for baseline ETCS
Occurence of this hazard depends on operational conditions
Inserted BG_B from adjacent track B (Wrong-side failure)
Initial train position during SOM in SR
Terminal train position during SOM in SR
Track_A
BG_A
Random effect
From track-side to on-board
Track_B
BG_B
Track area with potential for cross-talk
Average duration of SOM : 3% * 1 hour = 108 s
Case (b): "Cross-talk" effect within SOM for ETCS with Virtual Balises
This LDS hazard state is moving with train ...
Inserted VB_B from adjacent track B (Wrong-side failure)
Initial train position during SOM in SR
Terminal train position during SOM in SR
LDS
Track_A
VB_A
Systematic effect
Track_B
Wrong instant train positions during SOM - wrong track determination
VB_B
Duration of SOM operation can be reduced (train speed increased) without any impact on system safety
Track area with potential for "cross-talk"
Average duration of SOM : 3% * 1 hour = 108 s

(a)

(b)

Figure 35. Derivation of THR requirement for: (a) Physical Balise Group insertion, and (b) Virtual Balise insertion / detection considering cross-talk effect during Start of Mission with a priori train position status UNKNOWN

Such risk reduction / hazard mitigation resulting from operational characteristics AND technical system features is justifiable due to the fact that the erroneous data (i.e. inserted BG) due to a limited number of BGs on a track cannot be continuously transmitted to on-board during SOM operation. Thus cross-talk coming from track-side can be considered as a random effect (failure) for which mitigation can be justified and the RRF estimated.

Due to a possible greater train traffic, which can increase the likelihood for cross-talk, it was finally decided (SUBSET-088, Part 3) to choose a conservative target for cross-talk as

$$THR_{Cross\text{-}talk} = 1e\text{-}9/\ hr$$

The risk mitigation scheme for baseline ETCS:

$$THR_{Trans\text{-}Balise\text{-}3} \text{ of } 3.3e\text{-}10/\ hr \xrightarrow{RRF = 66.66} THR_{Cross\text{-}talk} \text{ of } 2.2e\text{-}8/\ hr \sim 1e\text{-}9/\ hr$$

Derivation of THR for detection of ETCS Virtual Balise considering “cross-talk” effect

The corresponding scenario related to the derivation of the THR requirement for Virtual Balise detection / insertion (THR_{VB}) by means of SOM scenario with train position UNKNOWN is outlined in Figure 35(b).

Virtual Balise insertion (i.e. detection of wrong VB) is more dangerous than VB deletion (i.e. VB missed detection) and thus most of ETCS core hazard rate is allocated to ETCS balise group, i.e. THR_{BTX} of 0.67e-9/ hr (ERTMS/ETCS SUBSET-088 2008; [13]).

Train position is (almost) continuously determined by means of GNSS-based LDS on train. It also means that estimated rate of incorrectly determined train position, corresponding e.g. to wrong track number (Figure 35(b)) doesn’t only depend on operational rules/ conditions and train traffic in a given GNSS service volume with nominal GNSS SIS reception conditions. Detection of wrong VB can depend on many other effects (SIS propagation, local effects, etc.). These effects must be considered as systematic hazard causes in case of VB in contrast to physical BG – see Figure 35(a). Due to these reasons it is not possible to mitigate the “cross-talk” (insertion of wrong VB) by means of specific train operational rules - such as shortening of operation duration (from 1 hour to 108 s in case of SOM in SR), which should otherwise result in less cross-talk occurrence or reduction of number of cross-talk effects depending on train traffic conditions, as it has been employed for the base-line ETCS in section above.

It is assumed that at the beginning of SOM the initial train position is determined by GNSS-based LDS at stand-still. This initial train position can be wrong (due to systematic multipath effect) and the related hazard cannot be mitigated by operational rules during the movement phase of SOM operation. One can imagine that the wrong train position determined by GNSS-based LDS is “moving with the train”, i.e. it is linked to the train and doesn’t depend on relatively spars independent track Information Points (i.e. physical balises), and consequently a wrong VB can be detected – see Figure 35(b). It is evident that shorter time interval for SOM (108 s) may not be helpful for the cross-talk risk reduction in the way, which is otherwise efficient in case of spatially distributed physical BGs. Thus THR of VB detection/ insertion $THR_{VB\ insertion}$ shall be 0.66e-9/ hr.

Risk mitigation scheme for ETCS with virtual balises:

$$THR_{VBTX}\text{ of }0.67\text{e-}9/\text{ hr}\ \xrightarrow{\text{RRF = 1 (no risk mitigation)}}\ THR_{Cross\text{-}talk} = THR_{VB\ Insertion} = 0.66\text{e-}9/\text{ hr}$$

Note: The TRANS-BALISE-1 with $THR_{VB\ Corruption}$ < 1e-11/h is also considered in the VB concept. Therefore $THR_{VB\ Insertion}$ + $THR_{VB\ Corruption}$ = THR_{VBTX} 0.67e-9/ hr.

Conclusions

- There are no applicable operational provisions with respect to the ETCS with Virtual Balises during Start of Mission in SR, which could be applied for justification of cross-talk reduction since it must be considered its systematic nature and not only its randomness;

  It is due to the fact that the absolute train position is (in contrast to the base-line ETCS with track balises) nearly continuously determined by GNSS-based LDS on board of train, and it doesn't make possible to apply operational provisions for such systematic hazard mitigation due to “cross-talk” effect (i.e. incorrect VB insertion);

- THR_{VBTX} of 0.67e-9/hr should be used for SOM in SR instead of 1e-9/hr (specified in SUBSET-088, Part 3, Annex A, Section 7). It is not question of the (small) difference between these two values. The justification is more relevant;

  It corresponds to THR_{BTX} of 0.67e-9/ hr that is nearly completely (except $THR_{VB\ Corruption}$) allocated to VB insertion in the ETCS VB concept. It is because all VBs are assumed linked by the ETCS odometry and thus VB insertion seems more dangerous than VB deletion;

- Benefit: The way of $THR_{VB\ Insertion}$ derivation and justification enables national ceiling speed limit increasing, e.g. above 30 km/ hr if required ;

  This higher speed limit during short SOM is justifiable via more demanding $THR_{VB\ Insertion}$ requirement. It will enable increasing a line capacity as it was originally intended in the H2020 ERSAT EAV project. It is possible due to the fact that derivation of $THR_{VB\ Insertion}$ of 0.66e-9/hr is performed independently of the SOM duration;

  In other words, the increasing of line capacity is paid by the more demanding requirement for $THR_{VB\ Insertion}$;

- Complementary track-side subsystems such as track circuits, axle counters, track balises can be subsequently used in combination with GNSS-based LDS for demonstration of system compliance with the required $THR_{VB\ Insertion}$ - but not for the $THR_{VB\ Insertion}$ requirement relaxation. It is necessary to distinguish between the requirement specification and the compliance demonstration with the requirement.

4.1.4 Difference between position estimation and decision making

This subsection clarifies major differences between two fundamental position determination tasks, which are required for safety applications in land transportation. These tasks are following:

- position determination along track / road lane, and
- track/ lane discrimination.

The clarification is mainly focused on safety characteristics related to design of safety-related systems which are critical for the above tasks. It has a direct impact on the system requirements specification.

Position determination along track/ lane

Position determination along track/ lane is a position estimation problem. In this case, it is usually possible to define a FAIL-SAFE STATE in case of a hazardous failure – i.e. train can stop, slow-down, etc. Therefore, the reduction of Time to Fault Detection and Negation (i.e. Safe Down Time (SDT) according to EN 50129) can enable a significant relaxation of safety requirements (i.e. THR increasing) for subsystems such as GNSS and independent diagnosis– see Figure 36. This Figure shows a fail-safe 2oo2 (two-out-of-two) structure composed of GNSS (Function A) and independent diagnosis (Function B).

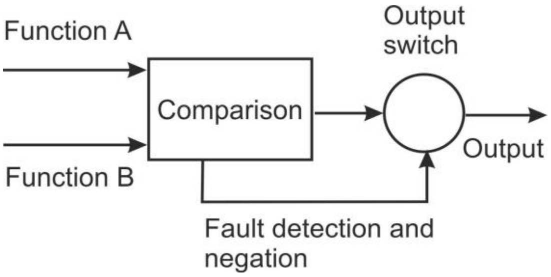


Figure 36. Composite fail-safety

Fast independent diagnosis (Function B) can significantly reduce the safety integrity requirement for GNSS. It can be demonstrated using the formula below for the system FFR (Functional Failure Rate) calculation (EN 50129)

$$FFR \approx \frac{FR_A}{SDR_A} \times \frac{FR_B}{SDR_B} \times (SDR_A + SDR_B) \qquad (1)$$

where FR_A is failure rate of function A (e.g. GNSS), FR_B is failure rate of function B (e.g. independent diagnosis of GNSS) and SDR_A and SDR_A are the relevant values of safe down rates for the functions A and B. In case of 2oo2 structure with comparison, SDR_A equals to SDR_B (i.e. SDR) and then

$$FFR \approx \frac{2 \times FR_A \times FR_B}{SDR} = 2 \times FR_A \times FR_B \times SDT = 2 \times FR_A \times FR_B \times (T_D + T_N) \qquad (2)$$

where SDT is safe down time, T_D is failure detection time and T_N is time to negation. If SDT is e.g. 1 second, then the total system FFR is reduced by 1: 3600. The ratio of 1/ 3600 is in fact a risk reduction factor. This is valid under the assumption that a fail-safe state can be defined (e.g. vehicle stopping). In addition, a very detailed Common Cause Failure/ Common Mode Failure (CCF/CMF) analysis must be performed to demonstrate the required SIL. It is evident that SDT is limited from below by system and operational characteristics.

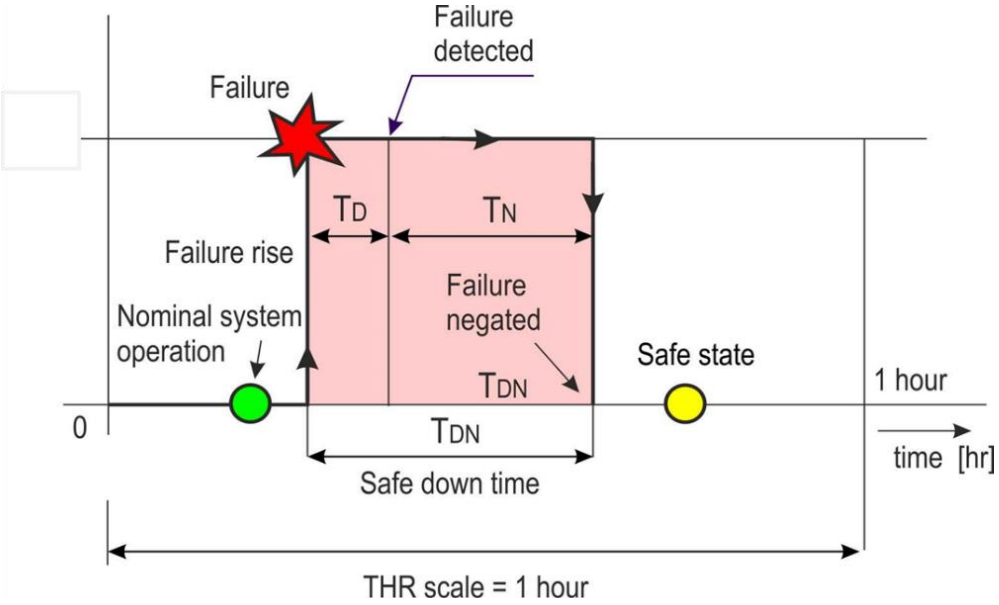


Figure 37. Presence of critical failure in fail-safe system

The presence of a critical failure in the fail-safe system is allowed for a time interval of (T_D +T_N), if the (T_D +T_N) complies with eqn. (2) for the required FFR (or THR) – see Figure 37.

Track/ lane discrimination

Track/ lane discrimination required for ERTMS Start of Mission (SOM) with UNKNOWN status (train position is not a priory known) is a decision problem. In this case it is not possible from the system design point of view to define a FAIL-SAFE STATE which could help to reduce (via fast diagnosis) safety requirements for subsystems (GNSS and independent diagnosis) and simultaneously meet required THR (FFR). We cannot say that determined position of train one track is safer than on the other one. Fast diagnosis used in the above Position Estimation Problem is not applicable for track discrimination. It would be wrong to say that fast diagnosis reduces the system FFR in this case. If we would (incorrectly) accept this possibility, then THR required for track discrimination (3.3e-10/ h) could be theoretically met by low quality functions A and B (let's say FR_A = FR_B=1e-2/ h) if SDT would be very short, i.e. 3.3e-6 hour = 0.01188 s - and it is a nonsense.

Functional Failure Rate of a track discrimination function during time interval of 1 hour can be calculated as follows

$$FFR = FR_A \times FR_B \times 1\,hour \qquad (3)$$

It is evident that realization of the Track discrimination function using composite safety requires higher demands on subsystems (A, B) from viewpoint of system integrity. For example, the THR requirement of 3.3e-10/ h for track discrimination function can be met by GNSS position determination as a Function A with FR_A of 1e-6/ h and independent diagnosis of GNSS as a Function B with FR_B of 1e-4/ h. In this case $FFR_{Track\ discrimination}$ equals to 1e-10/ h.

In case of Position estimation along track the THR requirement of 3.3e-10/ h can be met e.g. by GNSS as a Function A with FR_A of 1e-4/ h and independent diagnosis of GNSS as a Function B with FR_B of 5e-3/ h and SDT of 1 s. In this case $FFR_{Position\ estimation}$ equals to 2.7778e-10/ h.

Duration of track discrimination function is limited by operational reasons – i.e. by the average duration of Start of Mission in Staff Responsible, which is 3% of mission duration (1 hour) according to the SUBSET-088, i.e. 108 seconds. However, this operational parameter has no impact on safety integrity of the proposed system architecture. Therefore, values of 10s < TTA < 30 s proposed by the HELMET User Requirement UR_001 [1] is appropriate.

Further, ETCS onboard subsystem shall take no more than 60 s to go from No Power (NP) to being ready to accept data entry in Standby (SB).

Conclusion: It is evident that safety integrity requirements related to GNSS position determination function and independent diagnosis for a track discrimination function are about two orders higher than for a position determination along track. This fact should be considered during the HELMET system architecture design.

4.1.5 Experience with THR allocation from ERSAT GGC project

It was assumed in ERSAT GGC project [14] that train position determination along track used for detection of Virtual Balises would be based on a GNSS-based solution, and the track discrimination function would be performed using existing track-side infrastructure such as track circuits, axle counters and also physical balises. Track discrimination using the track-side infrastructure is out of HELMET scope. Therefore, a fault tree analysis (FTA) related to the VB detection based on GNSS developed in ERSAT GGC is further only recapitulated.

A fault tree related to the detection of Virtual Balises using an along track GNSS-based train position determination solution (hazardous event H7) developed within NGTC and ERSAT GGC activities is depicted in Figure 38 [14].

The THR related to hazardous event H7 (THR_{H7} of 3.3e-10/ h) is split between THR of Virtual Balise Reader VBR (THR_{VBR}) and THR related to Data Base Error (THR_{DB}). The THR_{DB} is considered as negligible. Therefore, the THR_{H7} of 3.3e-10/ h is allocated to THR_{VBR}, i.e. THR_{VBR}= 3.3e-10/ h. Hazardous event VBR represents Erroneous localization of Virtual Balise Group (VBG) with reception of valid balise information due to error within on-board Virtual Balise Reader (VBR) function - VBG position not correctly bounded.

The Virtual Balise Reader is based on GNSS. It is assumed that the GNSS Positioning integrity risk (Misleading Information) with $THR_{GNSS\text{-}MI}$ of 7.5e-6/ h can be theoretically achieved with

Augmentation and FDE. In order to meet the THR_{VBR}= 3.3e-10/ h, the use of an independent diagnosis (check) INDEP-CHK was proposed with $THR_{INDEP\text{-}CHK}$ of about 4e-5/ h to mitigate the cause of hazard GNSS-MI. Further THR allocation within the INDEP-CHK is under responsibility of the manufacturer.

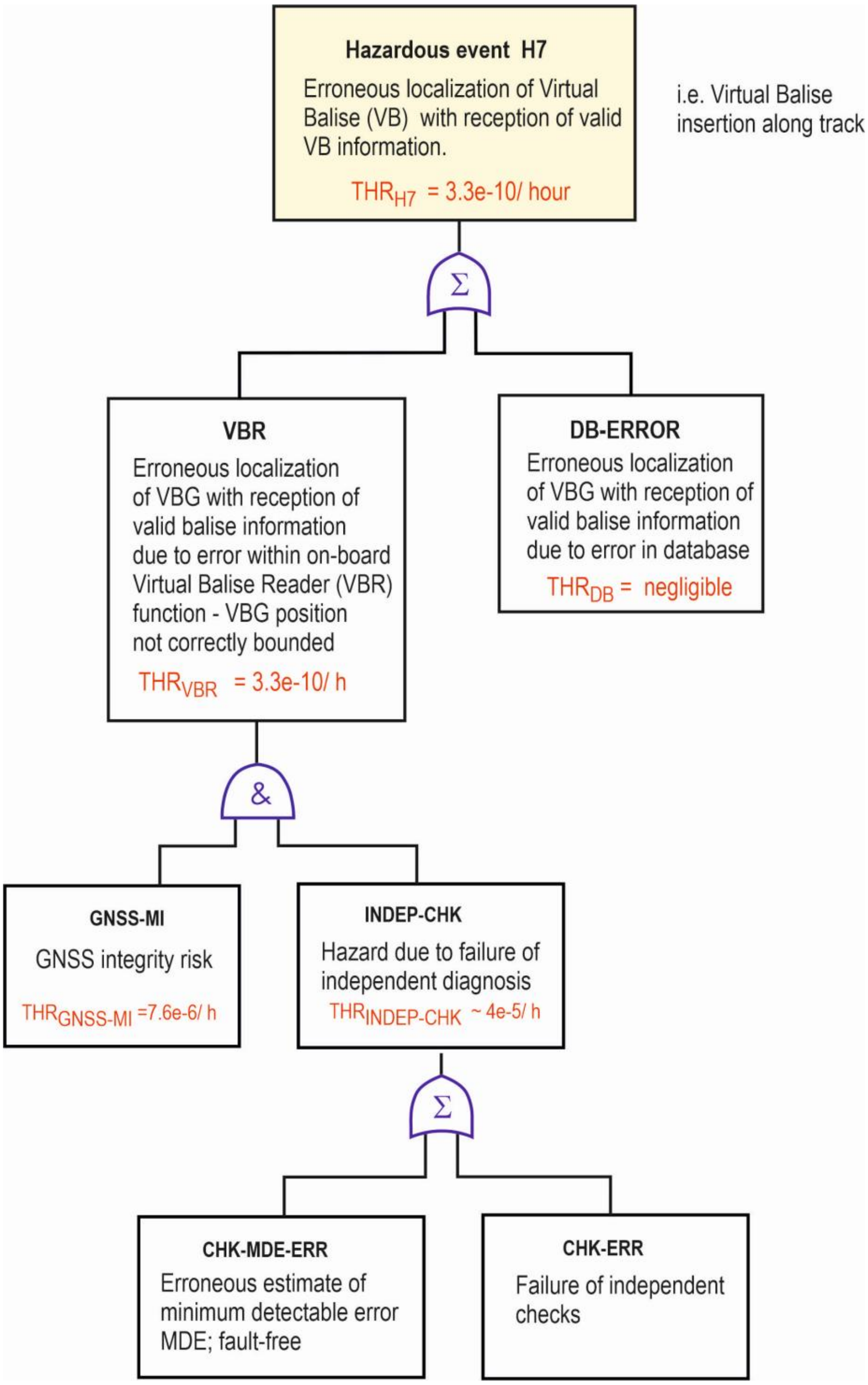

Hazardous event H7
Erroneous localization of Virtual Balise (VB) with reception of valid VB information.
THRH7 = 3.3e-10/ hour
i.e. Virtual Balise insertion along track
Σ
VBR
Erroneous localization of VBG with reception of valid balise information due to error within on-board Virtual Balise Reader (VBR) function - VBG position not correctly bounded
THRVBR = 3.3e-10/ h
DB-ERROR
Erroneous localization of VBG with reception of valid balise information due to error in database
THRDB = negligible
&
GNSS-MI
GNSS integrity risk
THRGNSS-MI =7.6e-6/ h
INDEP-CHK
Hazard due to failure of independent diagnosis
THRINDEP-CHK ~ 4e-5/ h
Σ
CHK-MDE-ERR
Erroneous estimate of minimum detectable error MDE; fault-free
CHK-ERR
Failure of independent checks

Figure 38. Allocation of THR related to Virtual Balise insertion along track to GNSS and diagnostic failures [14]

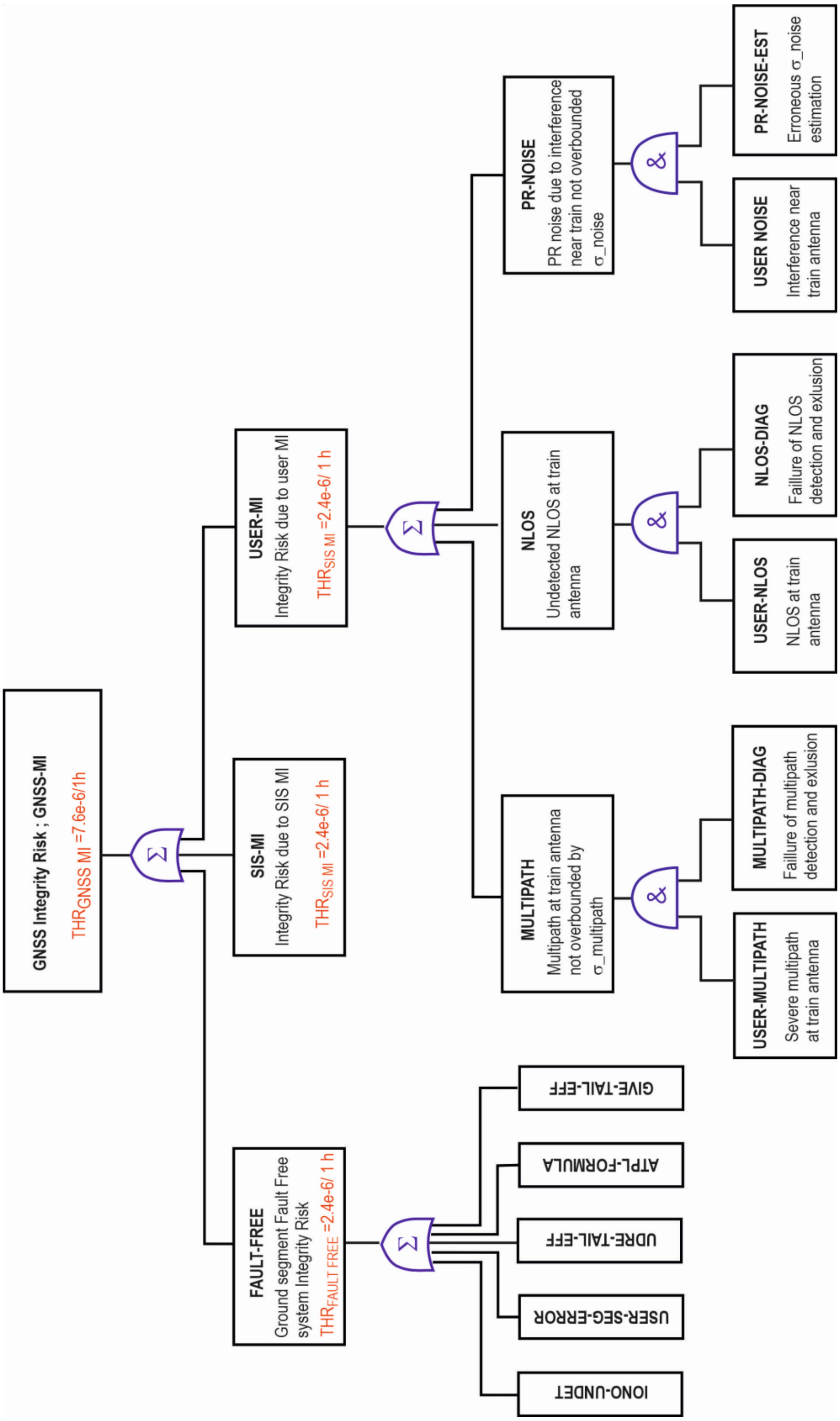

GNSS Integrity Risk ; GNSS-MI
$THR_{GNSS\ MI}$ =7.6e-6/1h
Σ
USER-MI
Integrity Risk due to user MI
$THR_{SIS\ MI}$ =2.4e-6/ 1 h
SIS-MI
Integrity Risk due to SIS MI
$THR_{SIS\ MI}$ =2.4e-6/ 1 h
FAULT-FREE
Ground segment Fault Free system Integrity Risk
$THR_{FAULT\ FREE}$ =2.4e-6/ 1 h
Σ
Σ
PR-NOISE
PR noise due to interference near train not overbounded σ_noise
&
USER NOISE
Interference near train antenna
PR-NOISE-EST
Erroneous σ_noise estimation
NLOS
Undetected NLOS at train antenna
&
USER-NLOS
NLOS at train antenna
NLOS-DIAG
Faillure of NLOS detection and exlusion
MULTIPATH
Multipath at train antenna not overbounded by σ_multipath
&
USER-MULTIPATH
Severe multipath at train antenna
MULTIPATH-DIAG
Faillure of multipath detection and exlusion
GIVE-TAIL-EFF
ATPL-FORMULA
UDRE-TAIL-EFF
USER-SEG-ERROR
IONO-UNDET

Figure 39. Allocation of THR related to GNSS Integrity Risk to GNSS hazard causes [14]

Allocation of THR related to GNSS Misleading Information GNSS-MI to GNSS hazard causes according to NGTC and ERSAT GGC results is outlined in Figure 39 [14] . GNSS-MI represents GNSS integrity risk defined as (ATPE >ATPL) and (TTA> X seconds)], where ATPE is Along Track Position Error, ATPL is Along Track Protection Level and TTA is Time to Alert.

The FAULT-FREE event includes the fallowing causes of hazards: 1) IONO-UNDET, i.e. Undetectable ionospheric perturbation (out of worst iono model conditions), 2) USR-SEG-ERR, i.e., Out-of-bounds user segment errors(extreme multipath, noise, tropospheric errors), 3) UDRE-TAIL-EFF, i.e. UDRE tails effects, 4) ATPL-FORMULA, i.e. ATPL formula leads to wrong translation of PR bounds to position bounds, and 5) GIVE-TAIL-EFF, i.e. GIVE tails effects.

The cause of hazard GNSS-MI is equally split among: 1) FAULT-FREE event, i.e. Ground segment Fault Free system integrity risk (without any failure in the system), 2) SIS-MI, i.e. Integrity risk due to SIS MI, and 3) USER-MI, i.e. Integrity risk due to user MI (local effect on signal) with $THR_{FAULT-FREE}$=THR_{SIS-MI} = $THR_{USER-MI}$ = 2.4e-6/ h. The USER MI event is further split among effects caused by MULTIPATH (Severe Multipath at train antenna), NLOS (Undetected NLOS at train antenna) and PR-NOISE (PR noise due to interference near train not bounded σ_noise).

4.1.6 ERTMS/ETCS reliability and availability requirements for HELMET

ERTMS Mission Reliability Targets are composed of qualitative and quantitative requirements. Quantitative requirements are expressed in terms of MTBF and are differentiated in reason of criticality (Immobilising, Service or Minor) of failures under consideration [43] - [45].

Immobilising failures
In the ERTMS context, Immobilising Failures may be identified as all the ERTMS failures, which cause two or more trains to be switched in on sight mode.

- The mean Time Between Immobilising hardware failures $MTBF-I_{ONB}$, defined for onboard equipment, shall be not less than $2.7x10^6$ hours.
- The Mean Time Between Immobilising hardware Failures $MTBF-I_{TRK}$, defined for Trackside Centralised equipment, shall be not less than 3.5 $x10^8$ hours.
- The Mean Time Between Immobilising hardware Failures $MTBF-I_{LNS}$, defined for Lineside Distributed equipment, shall be not less than $1.2x10^5$ hours.

Service failures
In the ERTMS context, Service Failures may be identified as all the ERTMS failures, which 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.

- The Mean Time Between Service hardware failures $MTBF-S_{ONB}$, defined for onboard equipment, shall be not less than $3x10^5$ hours.
- The Mean Time Between Service hardware Failures $MTBF-S_{TRK}$, defined for Trackside Centralised equipment, shall be not less than $4.0x10^7$ hours.

- The Mean Time Between Service hardware Failures MTBF-S_{LNS}, defined for Lineside Distributed equipment, shall be not less than 1.4x10^4 hours.

Minor hardware failures

- The mean Time Between Minor hardware failures MTBF_M_{ONB}, defined for onboard equipment, shall be not less than 8x10^3 hours.
- The Mean Time Between Minor hardware Failures MTBF-M_{TRK}, defined for Trackside Centralised equipment, shall be not less than 1.0x10^5 hours.
- The Mean Time Between Minor hardware Failures MTBF-M_{LNS}, defined for Lineside Distributed equipment, shall be not less than 3.6x10^2 hours.

Unavailability

- ETCS onboard equipment maximum unavailability: 1x10^{-6}
- Individual balise unavailability: < 2x10^{-5}

Conclusion

ERTMS Virtual Balise detection based on GNSS is performed by ETCS on-board subsystem. Therefore the following dependability requirements for the HELMET solution are specified in Section 5.1:

- The Mean Time Between Service hardware failures (MTBF) defined for onboard HELMET equipment shall be not less than 3x10^5 hours.
- HELMET onboard equipment maximum unavailability: 1x10^{-6} .

4.2 AUTO: SAFETY ANALYSIS FOR SELF-DRIVING CARS

4.2.1 Derivation of High-level safety system requirement for SDCs

A procedure for derivation of high-level safety target for self-driving cars is outlined in Figure 40. It is based on information presented in [15], [16]. The application of the harmonised risk acceptance approach based on CSM Design Targets is aiming at the derivation of really widely acceptable safety target for self-driving cars.

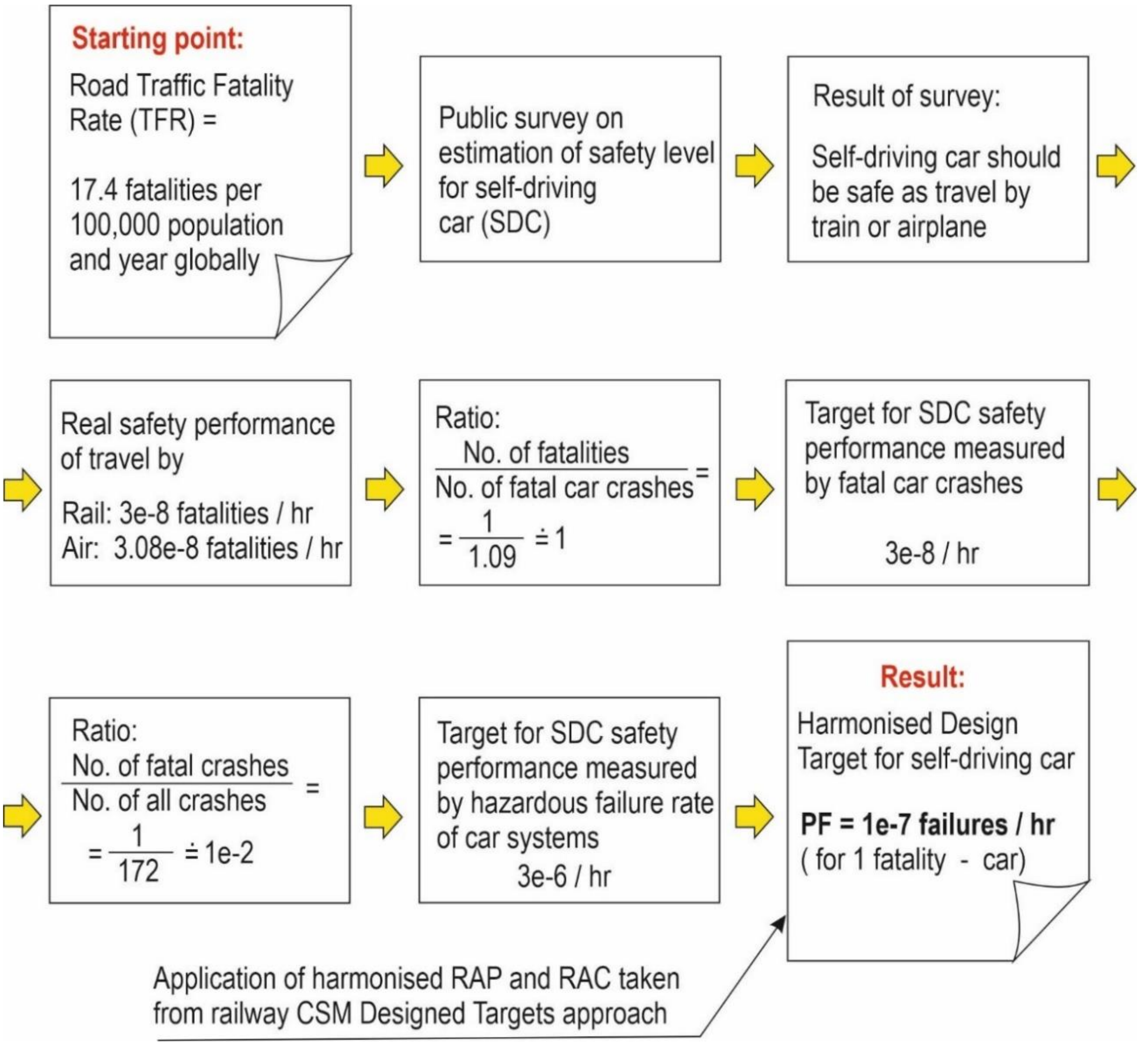

Starting point:
Road Traffic Fatality Rate (TFR) =
17.4 fatalities per 100,000 population and year globally
Public survey on estimation of safety level for self-driving car (SDC)
Result of survey:
Self-driving car should be safe as travel by train or airplane
Real safety performance of travel by
Rail: 3e-8 fatalities / hr
Air: 3.08e-8 fatalities / hr
Ratio:
No. of fatalities / No. of fatal car crashes =
= 1 / 1.09 ≐ 1
Target for SDC safety performance measured by fatal car crashes
3e-8 / hr
Ratio:
No. of fatal crashes / No. of all crashes =
= 1 / 172 ≐ 1e-2
Target for SDC safety performance measured by hazardous failure rate of car systems
3e-6 / hr
Result:
Harmonised Design Target for self-driving car
PF = 1e-7 failures / hr
(for 1 fatality - car)
Application of harmonised RAP and RAC taken from railway CSM Designed Targets approach

Figure 40. Derivation of harmonised design target for self-driving vehicles

Starting point of the procedure is road world Traffic Fatality Rate (TFR) as a measure of road safety - see Figure 40. It should be noted that this safety risk measure is not expressed per travelled km or mile but per population and year. Then conclusions of public survey on estimation of required safety level for self-driving car are recapitulated [15]. The survey indicates that safety level of SDCs should be approximately on the same level as safety of travel by airplanes or trains, i.e. approximately 3e-8/ hr – see [17]. In this HELMET report safety performance of rail or air is expressed per 1 hour rather than per distance travelled (km, miles). It is because human safety is usually evaluated (by means of RAP/RAC like MEM or ALARP) per time. Maintenance in aviation is e.g. also measured in hours and not per kms / miles. Speed of travel can introduce ambiguity into safety measurement. For example, if an aviation safety risk performance of 2e-10 fatalities/ mile is chosen as TLS for SDC [4], then also average speed of airplane should be also considered, otherwise the initial value of TLS would be overestimated.

Note: The aviation risk of 2e-10 fatalities/ mile chosen in [18] as TLS corresponds to 2e-10 fatalities/ 9.6 seconds if an average airplane speed of 600 km/ hr (375 miles/ hr) is considered. However, this risk is accumulated on the vehicle in time. The corresponding risk per 1 hour would be 7.5e-8/ hr. An average speed of car is less than one tenth of airplane speed, so TSL taken for SDC in [9] is about 10 x overestimated.

Real safety performance of travel by airplane or train (3e-8 fatalities/ 1 hour) can be considered as a tolerable risk, but not as acceptable risk. Tolerable means that society can live with it but cannot be regarded as negligible or as something what could be ignored. It should be further reduced if it is possible (ALARP). Acceptable risk means that everyone who might be impacted is prepared to accept it assuming no further changes in the risk control mechanisms are required. It means that a Risk Acceptance Principle/ Criteria should be introduced in the requirements derivation procedure.
In railway safety-related systems (socially acceptable) Risk Acceptance Principles/ Criteria (RAP/RAC) are usually introduced at the beginning of requirements derivation process – see e.g. TIR (Target Individual Risk) in equation (2). TIR can be specified e.g. by means of MEM or ALARP with acceptable probability of fatality occurrence of 1e-9/ hour. It is evident that real safety performance of travel by air or rail is lower (i.e. risk of 3e-8/ hr or 7.5e-8/ hr) than widely acceptable safety (i.e. risk of 1e-9/ hr or less).

Since this requirements derivation process starts from the real safety performance of travel by air/ train, which results from the results of the public survey described in Section 2.1, then RAP/RAC cannot be applied at the beginning of the requirement derivation process. In this report railway CSM-DT were proposed as (socially acceptable) RAP/RAC. CSM-DT specifies system Design (safety) Targets for a technical system in terms of failure occurrence rate per 1 hour – not in fatalities per hour. Due to this reason CSM-DT are applied at the end of the process – see Figure 40.

Application of CSM-DT as RAP/RAC for derivation safety requirements for SDC is the main differentiator with respect to the safety requirements derivation described in [9]. It can be also considered as a way how to get widely acceptable / harmonised safety requirements.

Based on car accident statistics one can assume that approximately 1 fatal accident cause 1 fatality [9]. It means that probability of occurrence of fatal accident could be 3e-8/ hr. Thus safety risk measured by fatalities / hr was converted to probability of occurrence of fatal car accident per 1 hr.

In aviation not every hazardous failure leads to an accident. This fact is described by fatal accident / incident ration in aviation TLS derivation, which is 1:10 (see Figure 40). In case of a car, any critical failure does not cause a fatal accident. It is stated in [9] that an automotive fatal accident to accident ratio based on statistical evaluation is 1:172. This ratio is conservatively chosen as 1:100 in [9]. The same figure is also used in Figure 40.

It is not generally straightforward to estimate such risk reduction ratio (for driver/ virtual driver) for SDCs. In railway safety-related systems this ratio can be estimated using e.g. risk matrix $\Sigma C_{jk}*F_{ik}$ as it is explained in HELMET D2.2 [2], equation (2) . This analysis must be performed for all potential hazards and operational scenarios. Related exposure frequencies and times should be also specified for all operational situations. The same should be done for SDCs but it is impossible to do all this work now. It could be quite risky to accept the assumption that only 1 critical system failure of 100 critical ones causes a fatal accident (in average). Especially in some very dangerous driving situations. However, if an additional RAP/RAC is used (i.e. CSM-DT in our case), which can a posteriori correct the previous risk estimate, then the fatal accident / accident ratio of 1:100 could be accepted. It can be discussed later.

Thus, the occurrence of fatal car accident per 1 hour (with about 1 fatality in average) was converted to the critical failure occurrence per 1 hour, which is 3e-6 critical failures / 1 hr/ car. Now it should be said whether this figure is also acceptable according to a long-term experience with building safety-related systems.

Since there is not a lot of experience with safety systems for automated driving, railway CSM Design Targets approach is used as Risk Acceptance Principle (RAP) and Risk Acceptance Criteria (RAC). It is assumed that single fatality in average is caused during one fatal accident and a low number of people (in average) is affected by accident. It corresponds to Class (b) system design target (see Table 41 in HELMET D2.2 [2]), which correspond to Probability of Failure of 1e-7/ 1 hour. It is the harmonised Design Target for the whole SDC safety system. Failure consequences are classified as Critical in this case.

4.2.2 Derivation of High-level safety system requirement for Car Localization Function

Allocation of the Harmonized Design Target for SDC (Probability of failure PF_{SYS} of 1e-7/ h) to main SDC safety subsystems is depicted in Figure 41. The Probability of Failure (PF_{SYS}) allocation has been performed according to the Logical model for SDCs (i.e. autonomous driving pipeline) outlined in Section 3.2 of D2.3.

The PF_{SYS} of 1e-7/ h is equally allocated to probabilities of Motion control failure (PF_{CON} of 5e-8/ h) and Failure of other car safety functions (PF_{OTH} of 0.5e-8/ h).

The PF_{CON} of 5e-8/ h is further allocated to a Failure probability of Car motion sensing PF_{SEN} of 1e-8/ h, a Failure probability of Message corruption PF_{COM} < 1e-9/ h and Failure probability of planning PF_{PLA} of 4e-8/ h. The PF_{PLA} of 4e-8/ h is allocated to Failure probabilities related to Car localization PF_{LOC} of 3e-8/ h, Message corruption PF_{COM} < 1e-9/ h (related to car localization) and Environment mapping PF_{ENV} of 1e-8/ h.

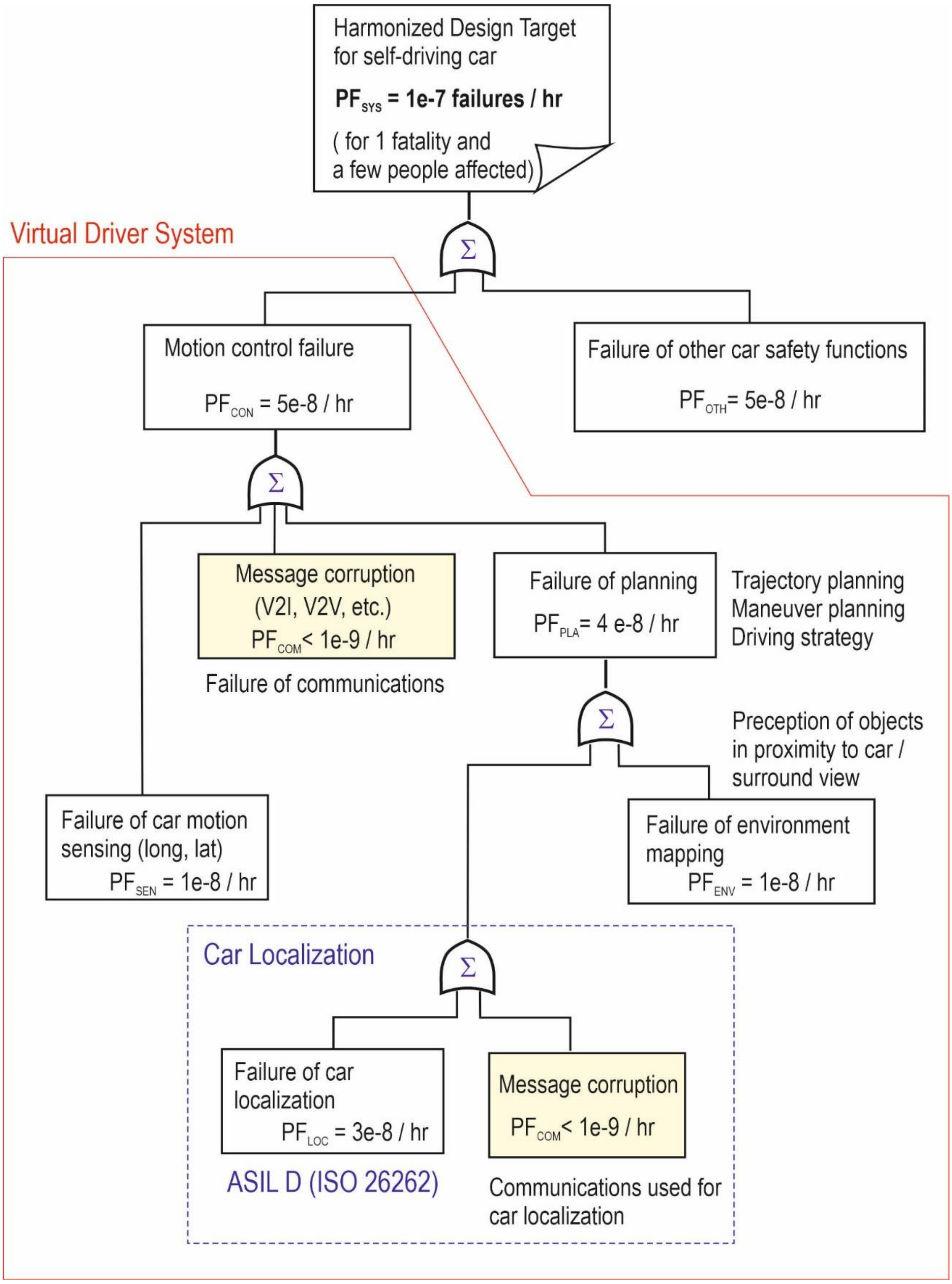

Harmonized Design Target for self-driving car
PF_{SYS} = 1e-7 failures / hr
(for 1 fatality and a few people affected)
Virtual Driver System
Σ
Motion control failure
PF_{CON} = 5e-8 / hr
Failure of other car safety functions
PF_{OTH}= 5e-8 / hr
Σ
Message corruption (V2I, V2V, etc.)
PF_{COM}< 1e-9 / hr
Failure of communications
Failure of planning
PF_{PLA}= 4 e-8 / hr
Trajectory planning
Maneuver planning
Driving strategy
Σ
Preception of objects in proximity to car / surround view
Failure of car motion sensing (long, lat)
PF_{SEN} = 1e-8 / hr
Failure of environment mapping
PF_{ENV} = 1e-8 / hr
Car Localization
Σ
Failure of car localization
PF_{LOC} = 3e-8 / hr
ASIL D (ISO 26262)
Message corruption
PF_{COM}< 1e-9 / hr
Communications used for car localization

Figure 41. Allocation of the Harmonized Design Target for SDC (probability of failure PF_{SYS}) to main SDC safety subsystems

A harmonised High-level fault tree resulting from NGTC / RHINOS and ERSAT GGC solutions which could meet safety integrity / robustness requirements for both RAIL and AUTO applications is depicted in Figure 42. It is obvious from the fault tree in Figure 41 that railway safety integrity requirements regarding position determination are almost two orders stricter than for the same requirement for SDCs. On the other hand SDCs have more demanding requirements for Alert Limit in lateral direction (RAIL AL < 1.78 m across track vs. AUTO AL < 20 cm - 75 cm across lane, depending on an operational scenario) as it is result from User Requirements UR_001 and UR_004-006 specified in HELMET D2.1 [1].

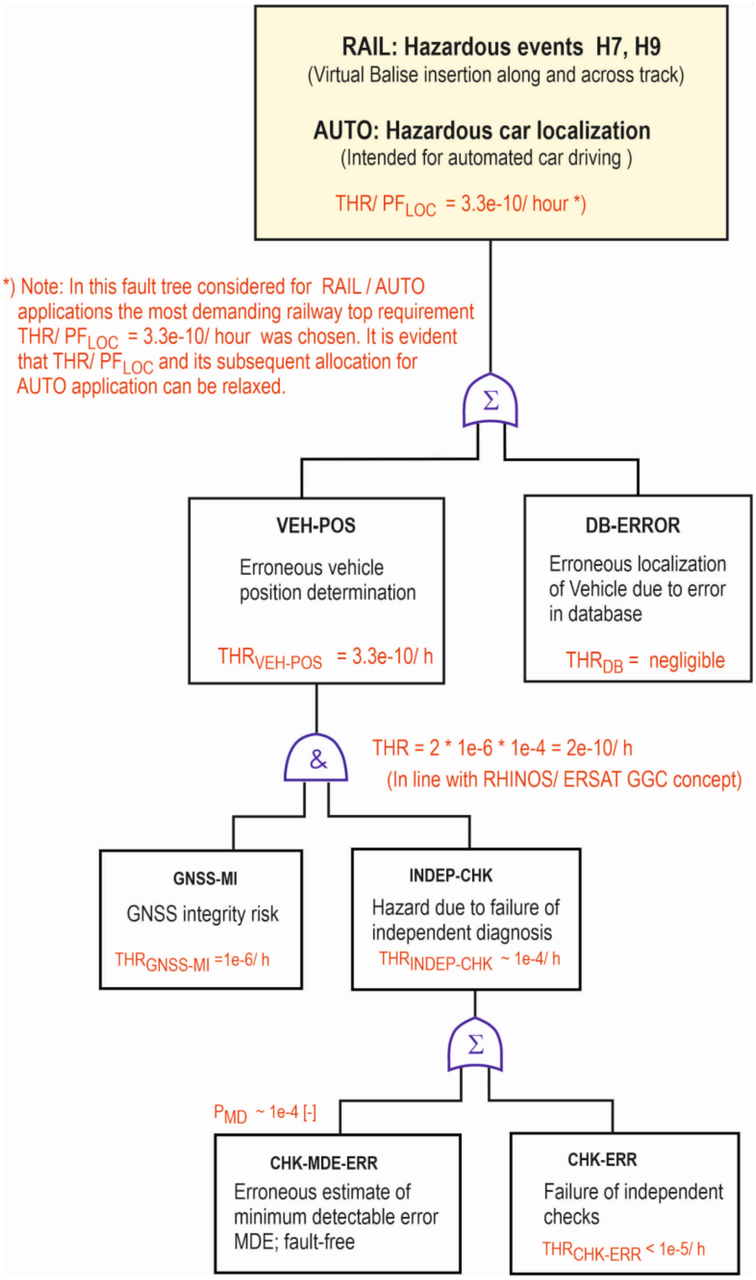

RAIL: Hazardous events H7, H9
(Virtual Balise insertion along and across track)
AUTO: Hazardous car localization
(Intended for automated car driving)
THR/ PF_LOC = 3.3e-10/ hour *)
*) Note: In this fault tree considered for RAIL / AUTO applications the most demanding railway top requirement THR/ PF_LOC = 3.3e-10/ hour was chosen. It is evident that THR/ PF_LOC and its subsequent allocation for AUTO application can be relaxed.
Σ
VEH-POS
Erroneous vehicle position determination
THR_VEH-POS = 3.3e-10/ h
DB-ERROR
Erroneous localization of Vehicle due to error in database
THR_DB = negligible
&
THR = 2 * 1e-6 * 1e-4 = 2e-10/ h
(In line with RHINOS/ ERSAT GGC concept)
GNSS-MI
GNSS integrity risk
THR_GNSS-MI =1e-6/ h
INDEP-CHK
Hazard due to failure of independent diagnosis
THR_INDEP-CHK ~ 1e-4/ h
Σ
P_MD ~ 1e-4 [-]
CHK-MDE-ERR
Erroneous estimate of minimum detectable error MDE; fault-free
CHK-ERR
Failure of independent checks
THR_CHK-ERR < 1e-5/ h

Figure 42. Harmonised fault tree for safe Train/ Car position determination based on NGTC, RHINOS and ERSAT GGC solutions

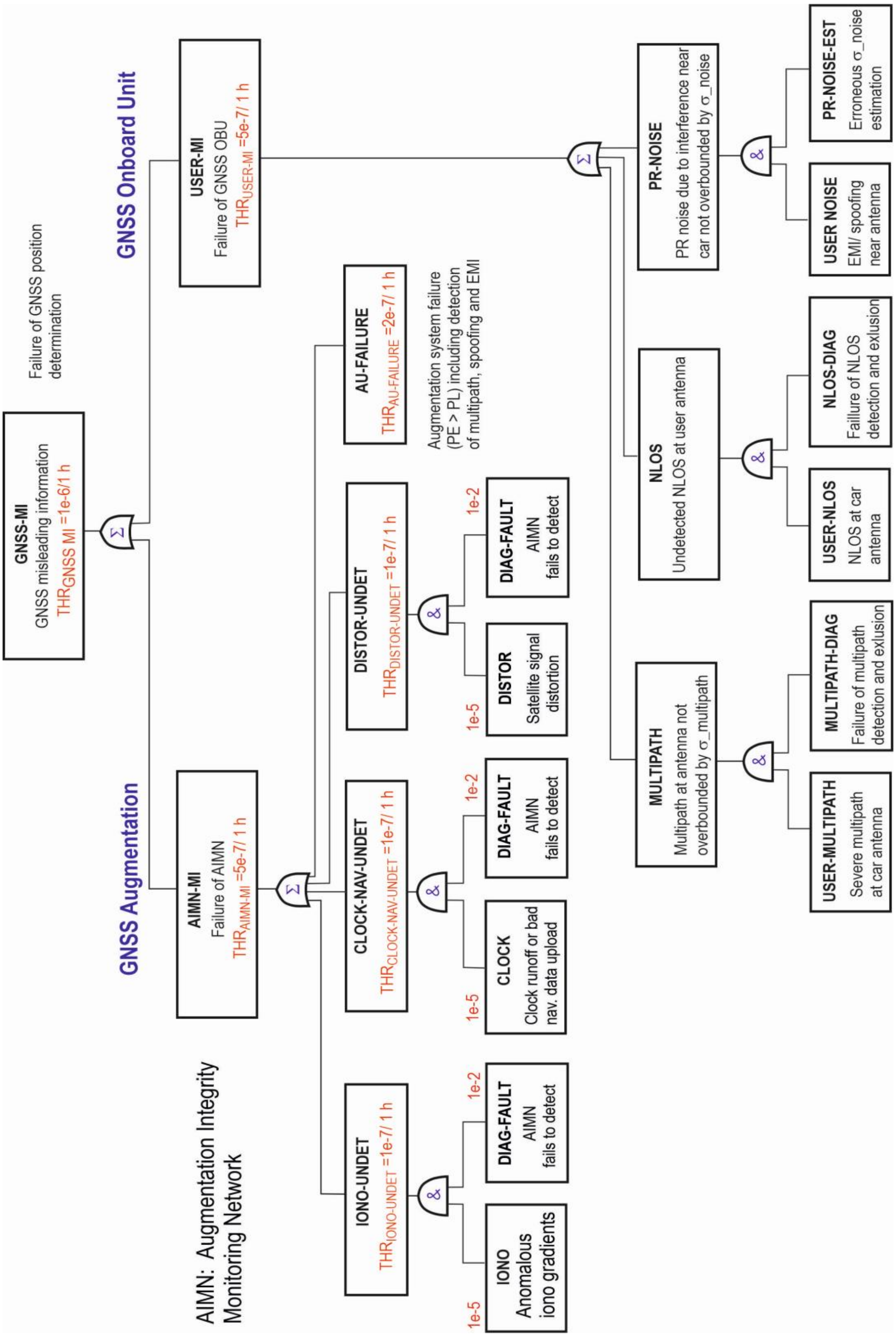

GNSS-MI
GNSS misleading information
THR$_{GNSS\ MI}$ =1e-6/1 h
Failure of GNSS position determination
GNSS Onboard Unit
USER-MI
Failure of GNSS OBU
THR$_{USER-MI}$ =5e-7/ 1 h
GNSS Augmentation
AIMN-MI
Failure of AIMN
THR$_{AIMN-MI}$ =5e-7/ 1 h
AIMN: Augmentation Integrity Monitoring Network
AU-FAILURE
THR$_{AU-FAILURE}$ =2e-7/ 1 h
Augmentation system failure (PE > PL) including detection of multipath, spoofing and EMI
DISTOR-UNDET
THR$_{DISTOR-UNDET}$ =1e-7/ 1 h
DISTOR
Satellite signal distortion
1e-5
DIAG-FAULT
AIMN fails to detect
1e-2
CLOCK-NAV-UNDET
THR$_{CLOCK-NAV-UNDET}$ =1e-7/ 1 h
CLOCK
Clock runoff or bad nav. data upload
1e-5
DIAG-FAULT
AIMN fails to detect
1e-2
IONO-UNDET
THR$_{IONO-UNDET}$ =1e-7/ 1 h
IONO
Anomalous iono gradients
1e-5
DIAG-FAULT
AIMN fails to detect
1e-2
PR-NOISE
PR noise due to interference near car not overbounded by σ_noise
USER NOISE
EMI/ spoofing near antenna
PR-NOISE-EST
Erroneous σ_noise estimation
NLOS
Undetected NLOS at user antenna
USER-NLOS
NLOS at car antenna
NLOS-DIAG
Faillure of NLOS detection and exlusion
MULTIPATH
Multipath at antenna not overbounded by σ_multipath
USER-MULTIPATH
Severe multipath at car antenna
MULTIPATH-DIAG
Failure of multipath detection and exlusion
Σ
&

Figure 43. Harmonised fault tree related to GNSS-MI hazard causes for safe Train/ Car position determination based on NGTC, RHINOS and ERSAT GGC solutions

A harmonised fault tree related to allocation of GNSS Misleading Information (GNSS-MI) to other GNSS hazard causes with respect to safe Train/ Car position determination based on NGTC, RHINOS and ERSAT GGC solutions is depicted in Figure 43.

It should be noted that requirements for GNSS-based RAIL and AUTO safety applications are generally very different from the operational / functional point of view and it also has a direct impact on safety architectures concepts (RAIL: Fail-safe vs. AUTO: Fail-operational), differences in RAMS specifications for RAIL, AUTO, etc. There is e.g. an essential difference between 1) Position estimation problem (along track/ route) and 2) Decision problem (lane/ track discrimination), because the Decision problem imposes much demanding safety requirements on the system than the position estimation task.

Therefore, the mentioned word ‘harmonized‘ means (taking account all the above mentioned differences in the RAIL, AUTO and UAVs applications) that there are some common high-level goals, strategies, applicable safety techniques and requirements in AUTO, UAVs and RAIL application areas, which should be considered during initial phases of HELMET safety architectures of design. Further development work will show how the individual solutions for the given applications (RAIL, AUTO, UAVs) will finally differ from each other. Nevertheless, the main goal for HELMET remains the same - GNSS position determination with (very) high accuracy and integrity.

4.3 UAV: SAFETY ANALYSIS OF UAS/RPAS-PIT STATION SEGMENT

4.3.1 UAS/RPAS-PIT station safety analysis approach

The overall High Level Safety Concepts for the Project are in accordance with the section 5.3 of the D2.2 document „HELMET CONOPS“ while in the subsections 2.3.2.1 and 2.3.2.2 of the same document were provided the Risk for Safety Assessment Methodology and the Airspace Specific Operational Risk Assessment (SORA) Procedure Overviews which they will be used for further and complete Safety Analysis during the Preliminary Design effort of the HELMET Project and specifically for the IMTM Applications employed UAS/RPAS types and configurations. The present section in this document will only provide a quick refresher on the Safety Assessment Standard Approach and a series of examples of Fault Tree Analysis specifically dealing with the most important operational safety issues of UAV/RPA Operations. These Fault Tree Analysis examples are taken by a Performed Research Regulatory Work as indicated in the Reference.

As Mentioned in the D2.2 HELMET CONOPS Document, the UAS/RPAS-PIT Station Safety Analysis Approach is based on risk analysis, assessment and mitigation process using the JARUS LORA Methodology which is in line with the illustrations in

Figure 44 and Figure 45. The risk assessment process considers hazards, their outcomes, and the operational environment (e.g., population density, airspace density of operations), and determines the associated level of risk based on the trajectory at impact (e.g., to people on the ground or to manned aircraft) and the effectiveness of any mitigation strategies that have been implemented. The level of risk can be compared to a target level of safety with and without the use of mitigations. The assessment of risk can lead to safety recommendations for reducing risk and improving safety. These basic steps are illustrated in

Figure 44:

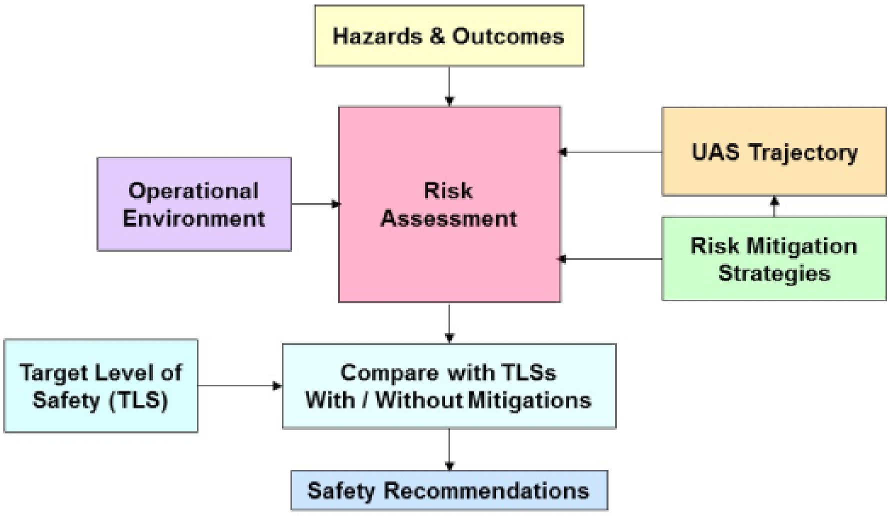

Hazards & Outcomes
Operational Environment
Risk Assessment
UAS Trajectory
Risk Mitigation Strategies
Target Level of Safety (TLS)
Compare with TLSs With / Without Mitigations
Safety Recommendations

Figure 44. High Level Risk Assessment Approach [41]

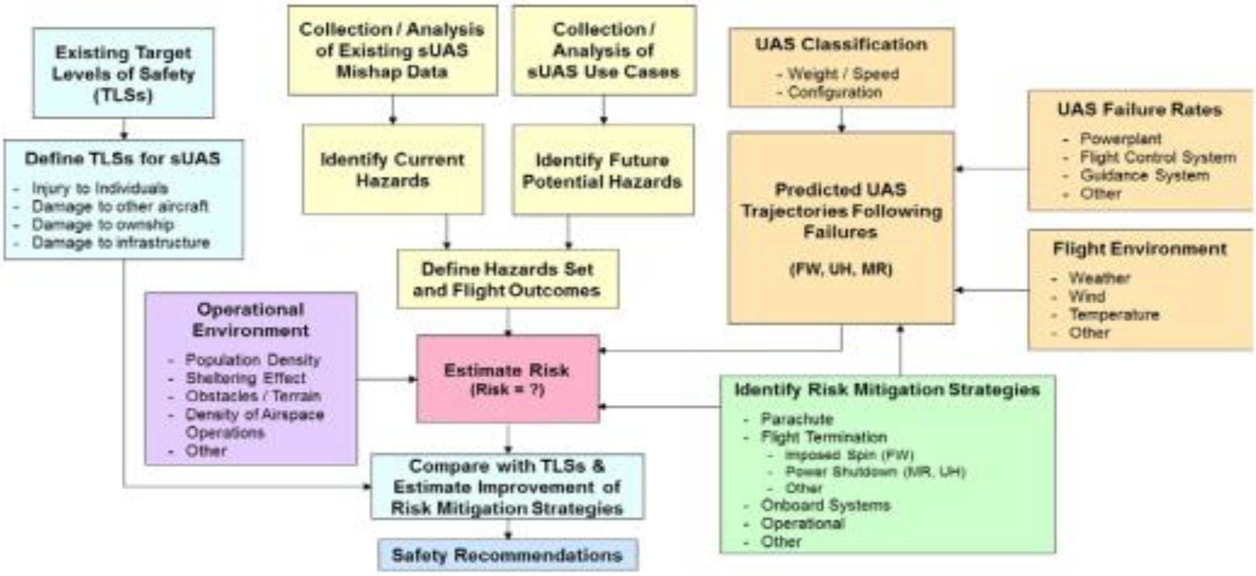


Figure 45. Detailed Risk Assessment Approach [41]

A typical starting point for any safety risk identification process is a review of existing accident and incident data. Such a review can provide general insights into the key hazards and their likely consequential outcomes and, depending on the scope and quality of the investigative reports available, the factors contributing to their occurrence. This is challenging for small UAS/RPAS operations, however, due to insufficient mishap (accident and incident) reporting for small UAS/RPAS and the proliferation of new small UAS/RPAS use cases that have not yet been implemented. Seldom does a review of accident and incident data provide a “comprehensive” identification of the potential hazards and their outcomes. This is particularly the case for UAS/RPAS, where limited data are available and the primary hazards are inherently rare events. Further, the ability to identify the complexity of factors contributing towards the occurrence of an accident or incident is often restricted by the method and quality of the records available. Nevertheless, it is possible to use the information available in several reports of small UAS/RPAS mishaps, accidents, and incidents in a hazard identification and risk analysis process.

4.3.1.1 The Key Risk Areas

The first stage in the analysis of the Safety involves the identification of the Key Safety Risk Areas (Outcomes) that derive from the Occurrence Categories. From the analysis of the Occurrence Categories in the example in Figure 46, the most common outcomes can be identified into the Key Risk Areas. Some of the actual Occurrence Categories are not outcomes, so these have been removed from the final Key Risk Areas, which are provided after the graph. Some of the Key Risk Areas are interlinked and may give rise to another outcome.

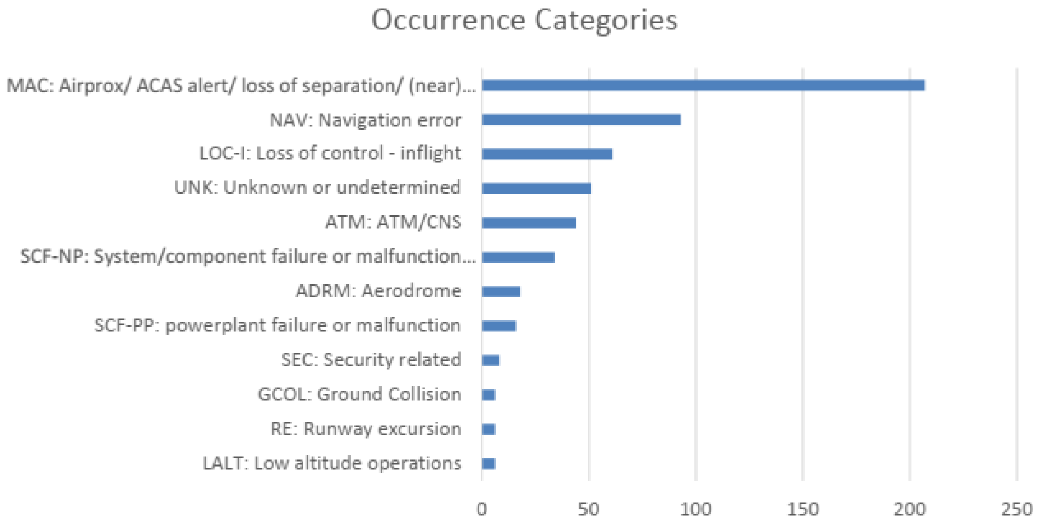


Figure 46. Occurrence Categories 2010-16 (EASA)

a) **Airborne Conflict**. Airborne conflict in the context of UAS/RPAS covers specifically the risk of
airborne collision between a UA/RPA and an aircraft in the air. Accounting for MAC/ Air prox and Navigation occurrences as well as a link to UTM/ATM.

b) **Aircraft Upset**. From the occurrence category analysis the 2nd Key Risk identified was Aircraft Upset, which covers the full range of Loss of Control situations. While UA/RPA upsets (Loss of Control) are different to those involved other aircraft because there is no risk to persons on board the aircraft, there is a potential for injuries to people on the ground depending on the planning of the flight and the reversion modes of the drone following a technical failure. Loss of control is particularly relevant for UAS/RPAS as they are likely to operate in closer proximity to the ground than other types of aviation.

c) **System Failures**. Both System/Component Failure Powerplant and Non-Powerplant feature in the outcome types and therefore would be included in the Key Risk Areas. For the purpose of the Safety Analysis this would be split into two areas. Firstly Engine Failure, which covers failure of the UAS/RPAS propulsion system and secondly Other System Failures which includes both electrical and control systems as well as software and data link failures.

d) **Third Party Conflict**. The final Key Risk Area covers the risk of UAS/RPAS conflicts (collisions) with people or property (i.e. not involving aircraft) where they may cause injuries or damage. There were no occurrences involving such damage or injuries but scenario based risk assessment has identified as a potential outcome that should be included as a key risk area for UAS/RPAS operations. It is known that accidents involving UAS/RPAS colliding with people on ground do occur. However, none have been formally reported within the EASA MS. As the UAS/RPAS industry is relatively new it could be possible that injuries due to UA/RPA are simply not reported on aviation level, but only in hospitals where the injuries are treated or at local law enforcement level.

4.3.1.2 Identification of Safety Issues

The second part of the Safety Analysis for the development of the Safety Risk process involves the identification of the Safety Issues that are associated with the different Key Risk Areas (Outcomes). Normally, this would involve a mainly quantitative analysis however due to the lack of detail in some of the UAS/RPAS data, the analysis of Event Types can only provide some indications on possible Safety Issues.

The identification of Safety Issues could be done in 2 stages. The first stage involves the initial analysis, which combined the analysis of the Event Types. The results of the first stage is captured in the Safety Risk process. The subsequent analysis is the identification of the Safety Issues in more detail. Figure 47 below shows the initial Event Types analysis in which precursors to Airborne Conflict accidents unsurprisingly feature highly. These include Airspace infringements and Loss of Separation, as well as near collisions. The vast majority of the Safety Issues subsequently identified, and the analysis that follows, covers this outcome category.

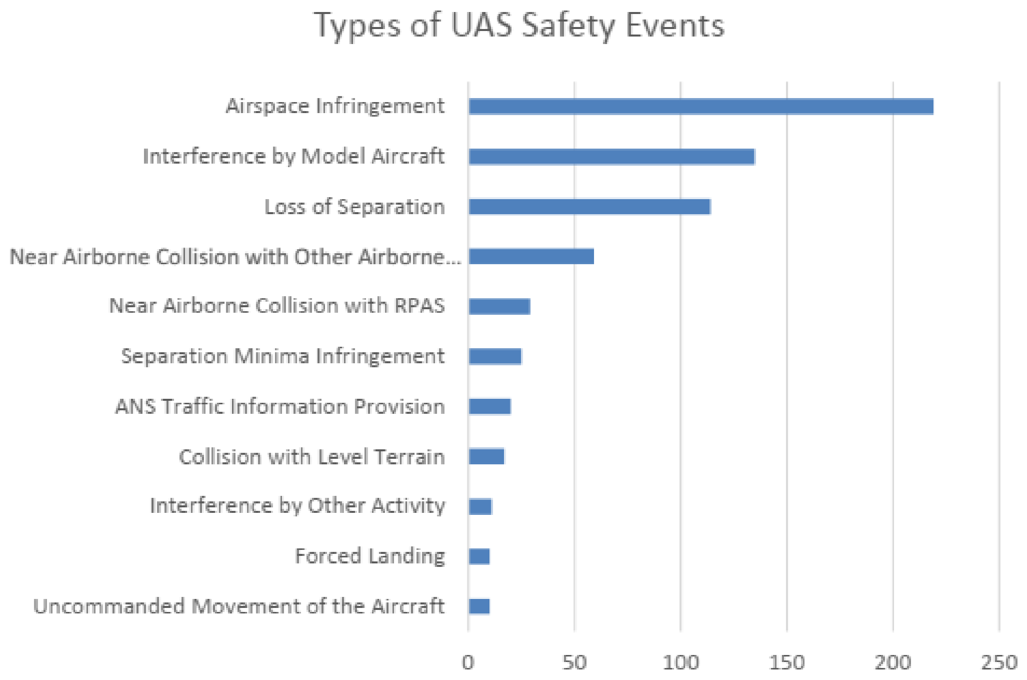


Figure 47. UAS/RPAS Occurrences of Safety Events In Accordance With EASA

In terms of the Safety Issues in the initial Safety Risk process, which have been identified by EASA, are summarised below:

1) **Detection, Recognition and Recovery of Deviation from Normal Operations**. The first Safety Issue, that was found most frequently in terms of accidents is related to the Key Risk Area of Aircraft Upset. It specifically relates to the operators' ability to recognise and recover from abnormal aircraft attitudes.

2) **UAS/RPAS Handling and Flight Path Management**. This Safety Issue is related to both Airborne Conflict and Aircraft Upset, as well as Third Party Conflict. It relates to both the normal handling of an UAS/RPAS and the planning and management of the flight path. There is also a relationship to the planning and preparation of UAS/RPAS operations.

3) **UAS/RPAS Infringement of Controlled Airspace/ UAS Proximity to Other Aircraft in Uncontrolled Airspace**. The next Safety Issue involves the risk of an UAS/RPAS either infringing controlled airspace or presenting a collision risk to other aircraft (manned and unmanned) in uncontrolled airspace. Work to investigating the potential benefits of Geo-Fencing to prevent UAS/RPAS flying into controlled airspace is already taking place. This Safety Issue is also linked to the Human Factors (HF) Safety Issues on UAS/RPAS Operator Knowledge of the Aviation System.

4) **Technical Safety Issues**. Three technical Safety Issues have been identified from the analysis of occurrences and cover the failures of the guidance and control system, propulsion system and power sources.

5) **Pre-Flight Planning and Preparation**. The first HF Safety Issue for UAS/RPAS involves the need for good pre-flight planning and preparation so that an UAS/RPAS operator conducts any flight in a safe manner. As UAS/RPAS operations involve many people that are unfamiliar with the aviation system, safety promotion will be important to make operators aware of good practices that they can easily follow.

6) **UAS Operator Knowledge of the Aviation System**. The second HF priority area is to ensure that anyone operating UAS/RPAS who is new to aviation can easily learn about the aviation regulatory framework as it applies to UAS/RPAS operations.

7) **Maintenance/ Manufacturing**. The final Safety Issue is related to the maintenance and manufacturing of UAS/RPAS and further analysis work is required to consider this issue in more detail.

4.3.2 Qualitative Safety Risk Assessment

4.3.2.1 Overview of Severity Categories

Manned aircraft system failures are defined in terms of their effect on both the aircraft and on persons. *Catastrophic* hazardous effects involve multiple fatalities, loss of the aircraft, or incapacitation of the flight crew. A *hazardous* event (sometimes referred to as a *severe major* hazard) is one that involves a serious or fatal injury to an aircraft occupant, a large reduction in the functional capabilities of the aircraft, a large reduction in safety margins, or physical distress or excessive workload that impairs the ability of the crew to perform tasks. A *major* hazard involves physical distress for passengers, significant reduction in safety margins, or significant increase in crew workload. A *minor* hazard involves physical discomfort for passengers, slight reduction in safety margins, or slight increase in crew workload. We have adapted these definitions for unmanned aircraft, omitting any reference to aircraft occupants. Also, we do not consider damage to the UAS itself. For unmanned aircraft, the severity categories used in our qualitative safety risk assessment are shown in the following Table 5.

Table 5. UAS/RPAS Hazard Severity Categories

Severity Category	**Injuries**	**Safety Margins**	**Crew Workload**
(1) Catastrophic	Multiple Fatalities		
(2) Hazardous	Single Fatality and/or Multiple Serious Injuries	Large Decrease	Compromises Safety
(3) Major	Non-Serious Injuries	Significant Decrease	Significant Increase
(4) Minor	None	Slight Decrease	Slight Increase
(5) No Safety Effect	None	No Effect	No Effect

4.3.2.2 Overview of Likelihood Classes

Likelihood is defined as the estimated probability or frequency of a hazard’s effect or outcome. Quantitative allowable probabilities for manned airplane hazards are taken from the various Civil Aviation Authority System Safety Regulations and Circulars. It should be noted that these are not exact values; the requirements for the allowable probabilities indicate an order of the listed value. The allowable probabilities for small airplanes differ from other aircraft by several orders of magnitude. At this juncture, it is not clear if small UAS/RPAS using rotors will be held to a higher standard than fixed wing UAS/RPAS. For the HELMET project, the intention is to use the small airplane standards. In designing systems for collision avoidance, small airplanes are not allowed any relaxation of the catastrophic probability. The quantitative and qualitative likelihood classifications used in the Safety Risk based Analysis are shown in the Table 6 below.

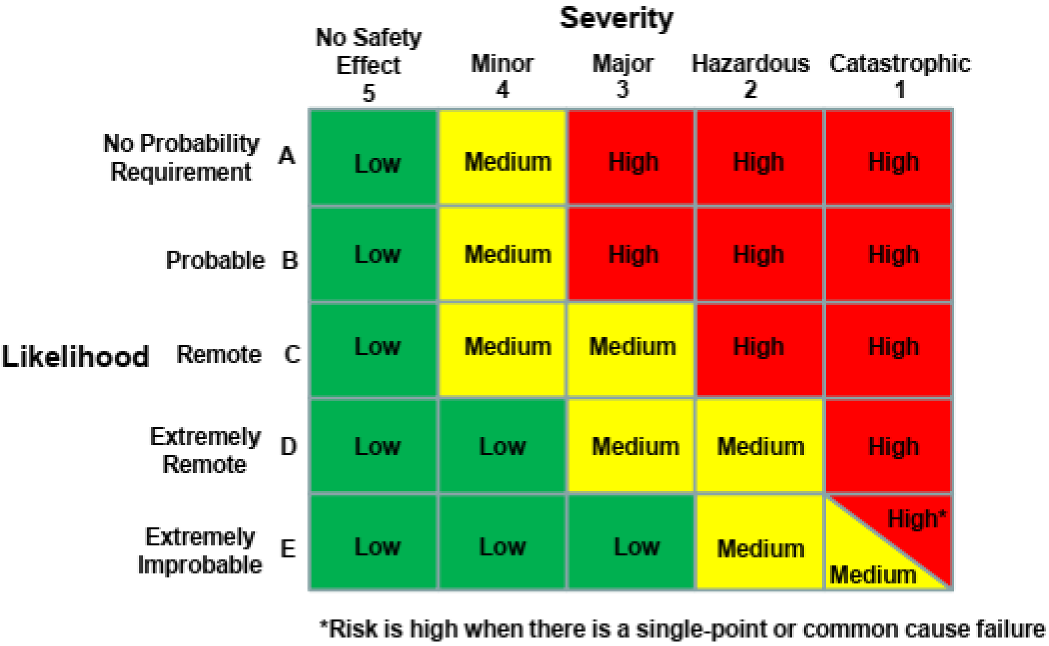
Table 6. Likelihood Classes Used in the Risk Analysis

Likelihood Class	**Allowable Probability**			
	Quantitative			**Qualitative**
	Small Airplane	**Small Rotary Wing Aircraft**	**Any Midair Collision**	

(A) No Probability Requirement	No Probability	No Probability	No Probability	No requirement on frequency of occurrence
(B) Probable	$< 10^{-3}$	$< 10^{-3}$	-----	Will occur several times in the life of an aircraft
(C) Remote	$< 10^{-4}$	$< 10^{-5}$	-----	Likely to occur once in the life of an aircraft
(D) Extremely Remote	$< 10^{-5}$	$< 10^{-7}$	-----	Unlikely, but possible to occur in the life of an aircraft
(E) Extremely Improbable	$< 10^{-6}$	$< 10^{-9}$	$< 10^{-9}$	It can be assumed that occurrence will not happen

4.3.2.3 Overview of Risk Matrix

The risk matrix shown in Figure 48 below is used to assign a risk level for each identified hazard based on the hazard effect’s severity and likelihood. High risk is unacceptable, and any proposed operational changes in the non-segregated airspace cannot be implemented unless the hazard’s associated risk is mitigated to medium or low.



		Severity				
		No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Likelihood	No Probability Requirement A	Low	Medium	High	High	High
	Probable B	Low	Medium	High	High	High
	Remote C	Low	Medium	Medium	High	High
	Extremely Remote D	Low	Low	Medium	Medium	High
	Extremely Improbable E	Low	Low	Low	Medium	High* Medium

*Risk is high when there is a single-point or common cause failure

Figure 48. Risk Matrix Used for the Risk Based Safety Analysis (EASA/JARUS)

4.3.3 Examples of Safety Probabilistic Assessment - Fault Tree Presentation

Figure 49 below presents the Fault Tree for total loss of UAS/RPAS control during landing operations with a subsequent uncontrolled crash. In this scenario the UAV is a multirotor, electrically powered aircraft. The Electrical power feeds all UAV systems such as the propulsion, Flight Controls and related links.

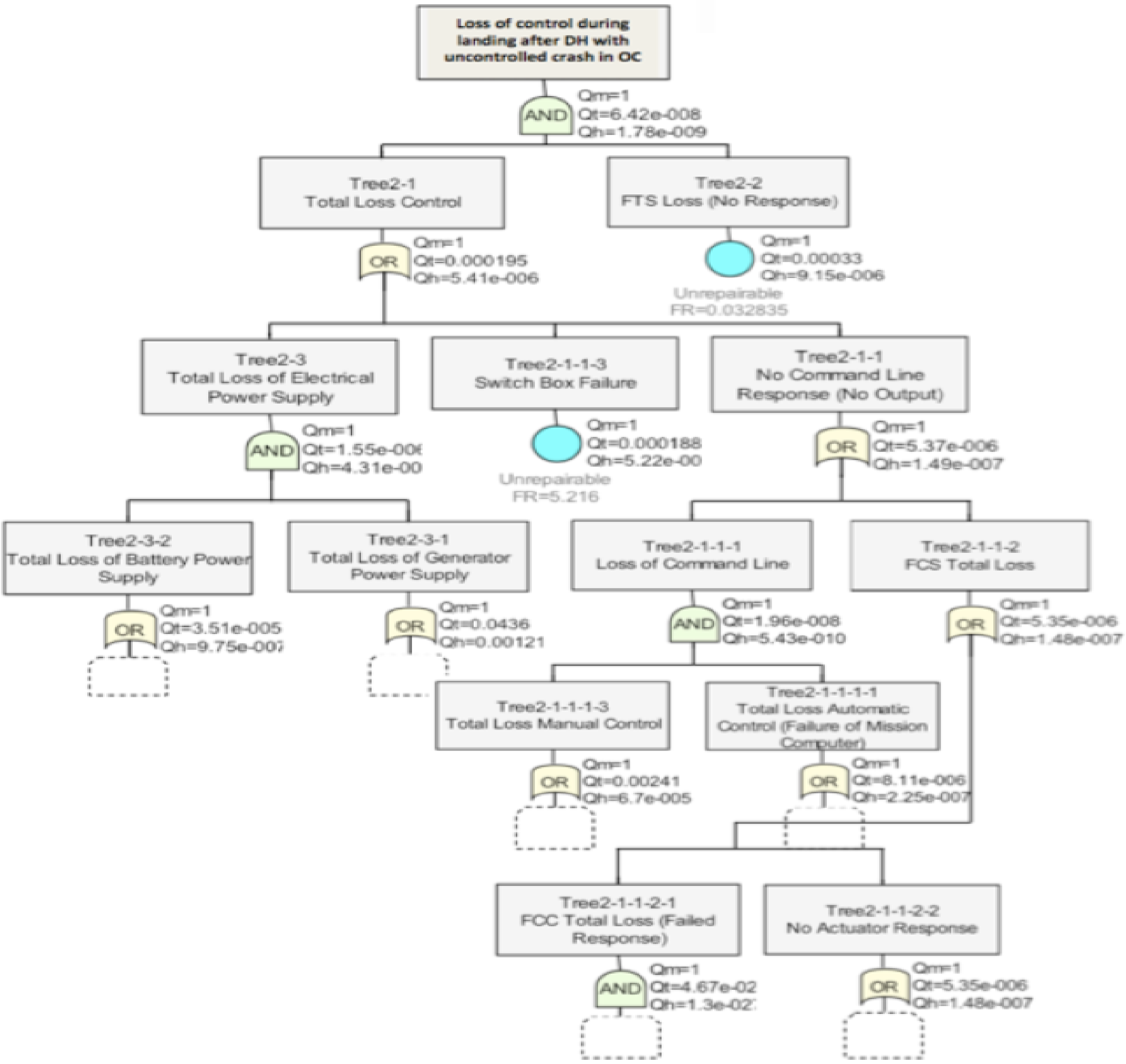


Figure 49. Fault Tree Presenting the Total Loss of a UAV and uncontrolled Crash Case

The second example in Figure 50 refers to the Total Failure of the Detect and Avoid (DAA) Function on board of the UAV during a programmed flight in BVLOS or BRLOS mode demonstrate the failure in ownship locatability function. As depicted in Figure 50, the failure in DAA capability onboard can be the result of five alternative events. Three of them are intermediate events: DAA 1A-failure in traffic detection function by cooperative sensors, DAA 2-failure on non-cooperative sensors and DAA 3-evaluation function failure. DAA 1A and DAA 2 are transferred to separate trees and illustrated in Figure 51 and Figure 52.The evaluation function failure traces the data processing function failure which indicates the failure in multi-sensor data fusion and the track evaluation failure indicates the failure probability of intruder track. The execute function failure is the failure probability to execute appropriate maneuvers as commanded. DAA 5 is the failure of the data link that is used to transfer data and receive command from the ground control station. Figure 51 outline the intermediate events DAA 1A. This sub-tree specifies the failure probability of traffic detection function by cooperative surveillance.

In this example, a voting OR gate is utilized to calculate the failure probability of DAA 1. VOTING OR indicates that the event will occur of k out of n events occur. In the fault tree presented in Figure 51 the DAA occurs if two out of three surveillance sensors failed to detect a traffic. VOTING OR gate is considered to account the current equipage scenario for unmanned as well as manned aircraft system. Using a universal AND gate would give a lower failure rate whereas using a universal OR gate would provide a higher failure rate than in an actual encounter scenario. For example, if onboard active surveillance system and TCAS system fails and the intruder which can be manned or unmanned, is not equipped with ADS-B, in spite of having a working ADS-B In ownship will fail to detect the intruder. Also, it is considered that without any catastrophic power failure onboard or without any external attack three systems will not be down at the same time. Thus, VOTING OR encompasses all the scenarios. Figure 52 presents the intermediate event DAA 2-failure in non-cooperative sensor which is the result of two alternatives sensors failure: one is air-to-air radar failure, and another is vision-based sensor failure. While tracing the events for vision-based sensor, a component wise failure probability is adopted as the component is assumed to be acquired off the shelf with a specified MTBF.

As stated earlier, a separate fault tree is constructed to determine the failure in ownship locatability function due to failure of cooperative surveillance system. Figure 53 to Figure 56 illustrate the faults trees of main event and intermediate events.
As detailed in Figure 53, the failure in cooperative surveillance function occurs if either Mode S or ADS-B out failed. This is a conservative choice that assumes mixed equipage requirements. The ownship ADS-B out system depends on the onboard satellite navigation and pressure altimeter. Figure 54 and Figure 55 present the transferred trees from the ADS-B out; Figure 55 outlines the failure in ADS-B due to onboard satellite navigation loss and Figure 56 outlines the failure due to corrupted data from navigation sources.

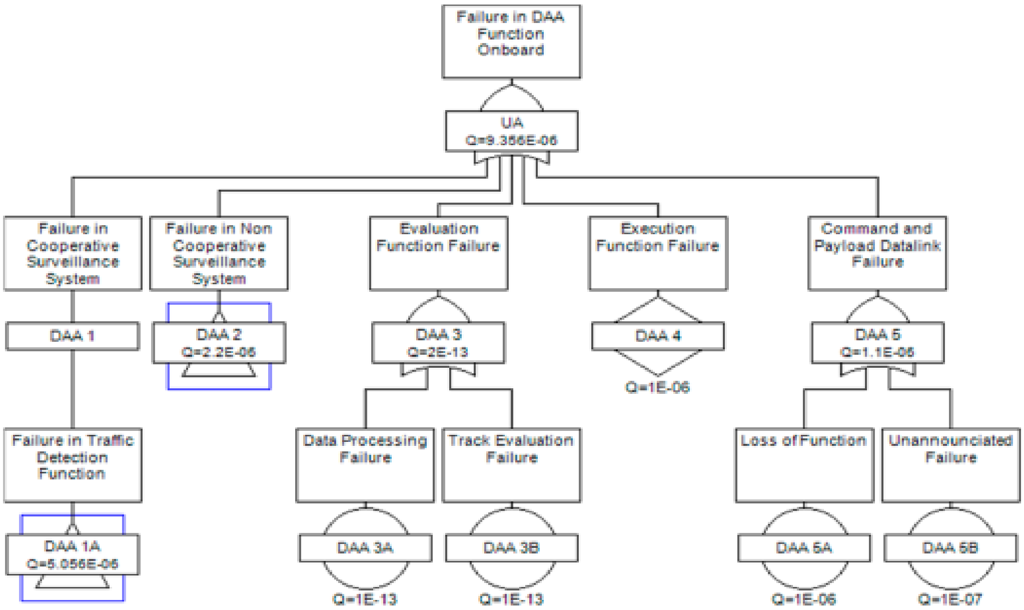

Failure in DAA Function Onboard
UA
Q=9.356E-06
Failure in Cooperative Surveillance System
Failure in Non Cooperative Surveillance System
Evaluation Function Failure
Execution Function Failure
Command and Payload Datalink Failure
DAA 1
DAA 2
Q=2.2E-06
DAA 3
Q=2E-13
DAA 4
Q=1E-06
DAA 5
Q=1.1E-06
Failure in Traffic Detection Function
Data Processing Failure
Track Evaluation Failure
Loss of Function
Unannounciated Failure
DAA 1A
Q=5.056E-06
DAA 3A
Q=1E-13
DAA 3B
Q=1E-13
DAA 5A
Q=1E-06
DAA 5B
Q=1E-07

Figure 50. Fault Tree for UAV Failure in DAA Capability [42]

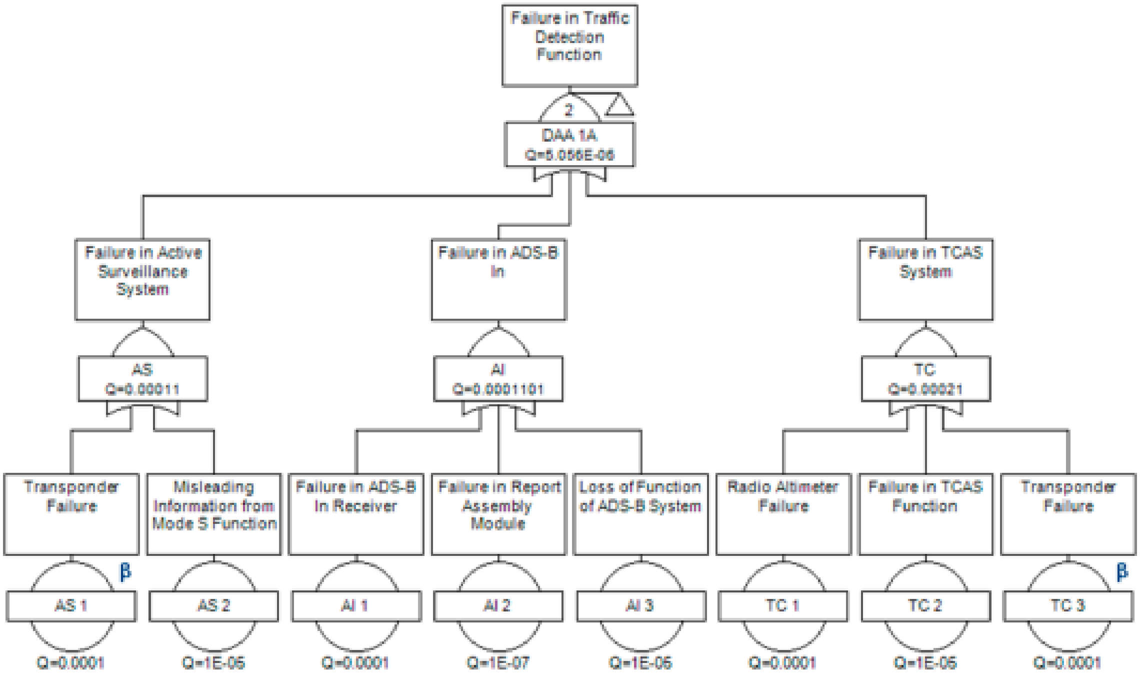


Figure 51. Fault Sub-Tree for Cooperative Traffic Monitoring/Surveillance (Traffic Management) [42]

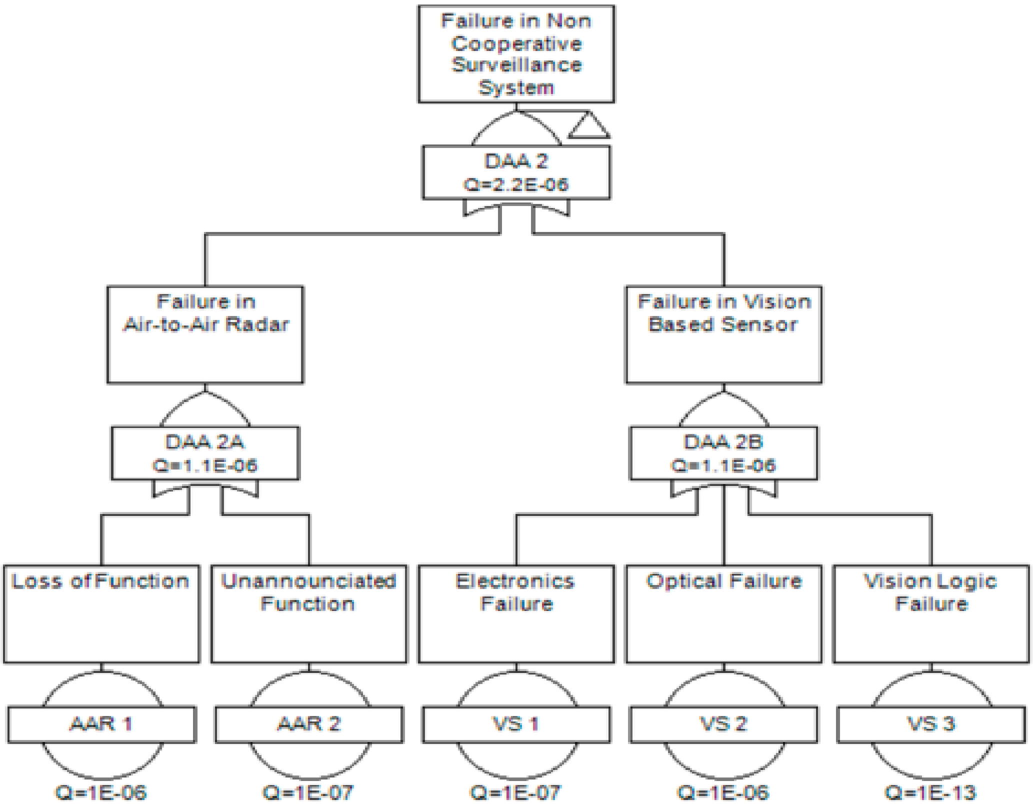


Figure 52. Fault Sub-Tree for Non-Cooperative Monitoring/Surveillance (Traffic Management) [42]

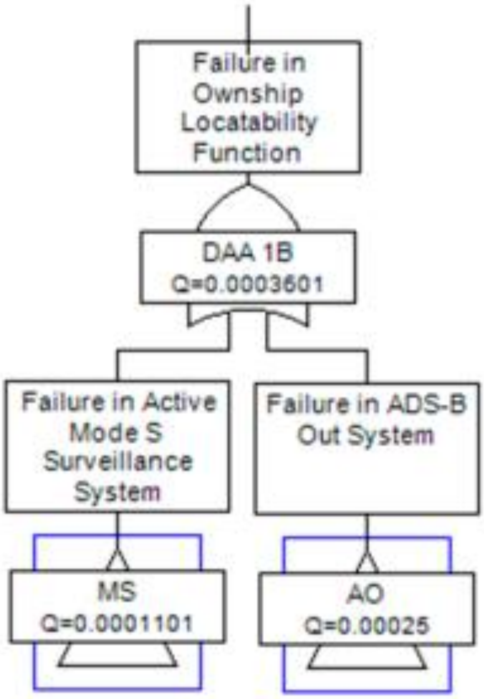

Failure in Ownship Locatability Function
DAA 1B
Q=0.0003601
Failure in Active Mode S Surveillance System
Failure in ADS-B Out System
MS
Q=0.0001101
AO
Q=0.00025

Figure 53. Fault Sub-Tree for Cooperative Surveillance (Ownship Locability) [42]

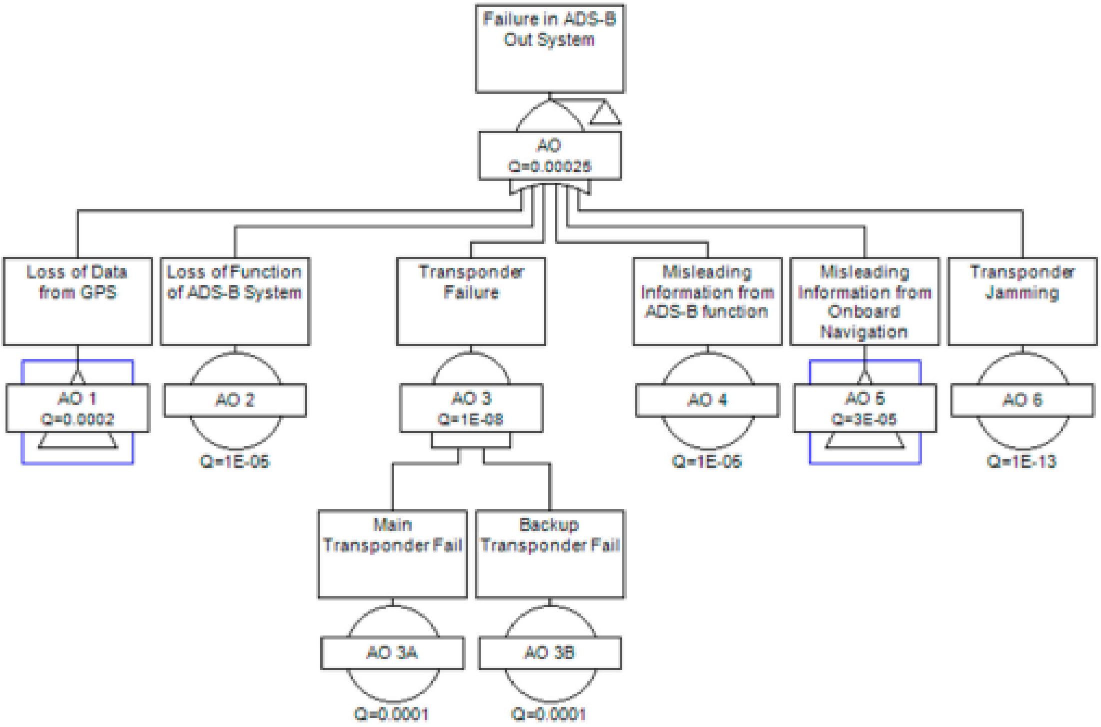


Figure 54. Fault Sub-Tree for ADS-B Out System [42]

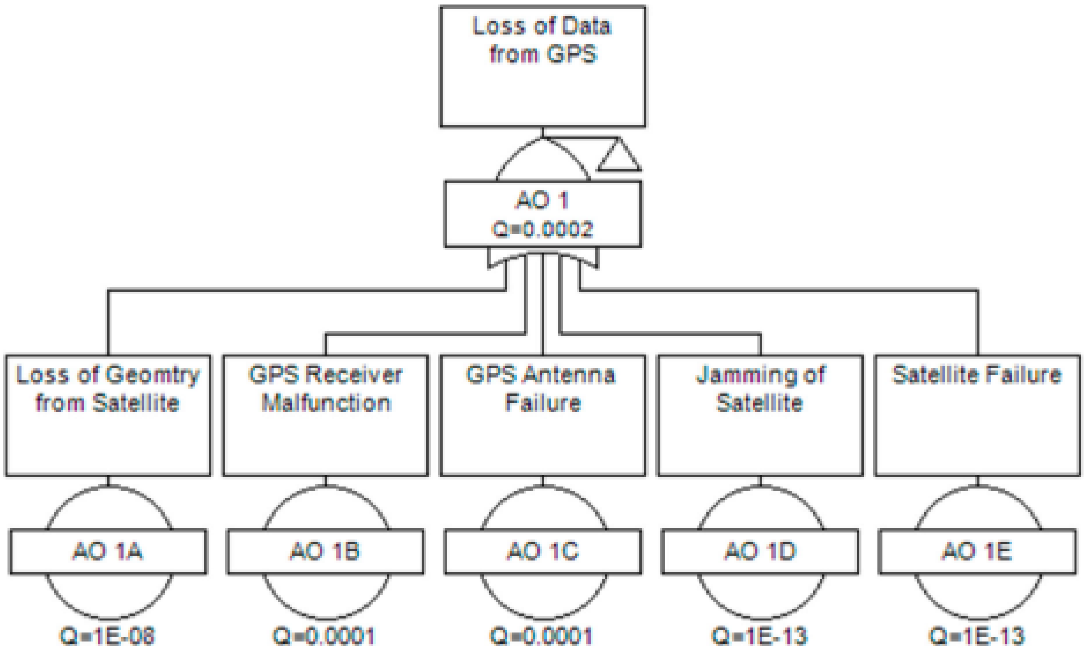


Figure 55. Fault Sub-Tree for the Loss of GPS Data [42]

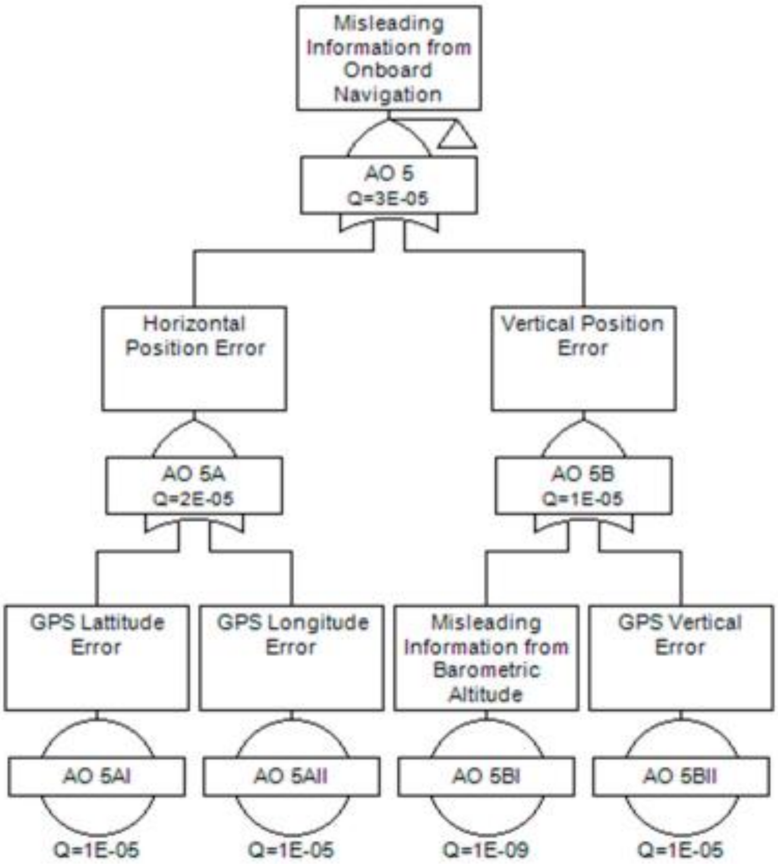


Figure 56. Fault Sub-Tree for Misleading Navigation Information [42]

The reliability data for the basic events used in the fault tree are extracted from the literature, aviation standard documents and Original Equipment Manufacturer (OEM) and presented in Table 7 below:

Table 7. Failure Probability Associated to the Basic Events

Basic Events	Description	Failure Probability (q)
DAA 3A	Data Processing Failure	1 × 10−13
DAA 3B	Track Evaluation Failure	1 × 10−13
DAA 4	Execution Function Failure	1 × 10-6
DAA 5A	Command Datalink Failure (Loss of Function)	1 × 10-6
DAA 5B	Command Datalink Failure (Unreported Failure)	1 × 10-7
AS 1/TC-3/AO 3A /AO 3B/MS-3	Transponder Failure (Main/Backup)	1 × 10-4
AS 2/MS-2	Misleading Information from Mode S Function	1 × 10−5
AI 1	Failure in ADS-B In Receiver	1 × 10−4
AI 2	Failure in Report Assembly Module	1 × 10−7
AI 3/AO 2	Loss of Function of ADS-B System	1 × 10−5
TC 1	Failure in Radio Altimeter	1 × 10−4
TC 2	Failure in Traffic Collision Avoidance System (TCAS) Function	1 × 10−5
VS 1	Electronics Failure	1 × 10−7
VS 2	Optical Failure	1 × 10−6
VS 3	Vision Logic Failure (Data processing failure)	1 × 10−13
AO 4	Misleading Information from ADS-B Function	1 × 10−5
AO 6	Transponder Jamming	1 × 10−13
AO 1A	Loss of Geometry from Satellite	1 × 10−8
AO 1B	GPS Receiver Malfunction	1 × 10−4
AO 1C	GPS Antenna Failure	1 × 10−4
AO 1D	Jamming of Satellite	1 × 10−13
AO 1E	Satellite Failure	1 × 10−13
AO 5AI/AO 5AII	Horizontal Position Error (Latitude/Longitude)	1 × 10−5
AO 5BI	Misleading Information from Barometric Altimeter	1 × 10−9
AO 5BII	GPS Vertical Error	1 × 10−5
MS 1	Failure in Barometric Altimeter	1.1 × 10−7

For the safety assessment, a general model is used, which considers the failure probability as constant across the lifespan of the component. Denoting basic failure probability as Qi with i = 1 . . . n and the top event failure as Q, assuming all basic events are independent, the model can be expressed as:

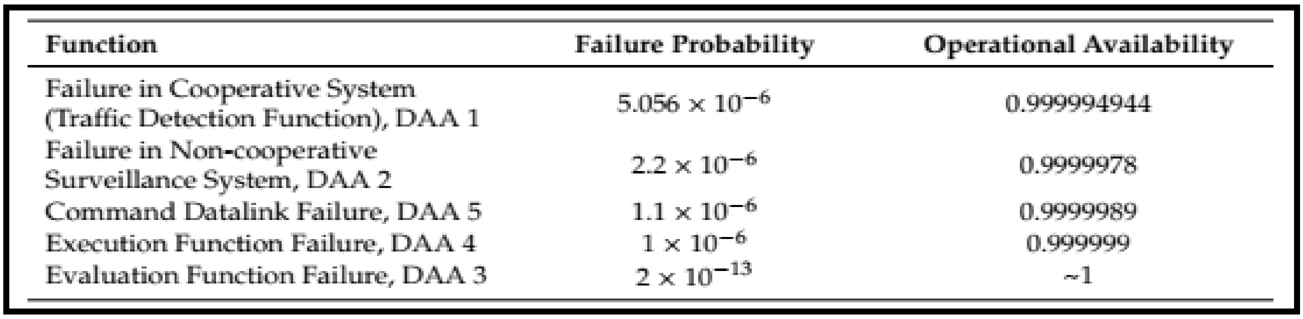
$$Q(t) = f\ (Q1(t), Q2(t), \ldots Qn(t))$$

This implies that if the state of each component in the fault tree is known at time t, then the state of the top event can also be determined regardless of what has happened up to time t. The top event probability is calculated by logically tracing the failure of basic events. *Q*(*t*), the probability of the hazard/top event occurrence is also known as the risk measure or unavailability. Thus, the availability of the system can be obtained as:

$$\text{Operational Availability} = 1 - Q(t)$$

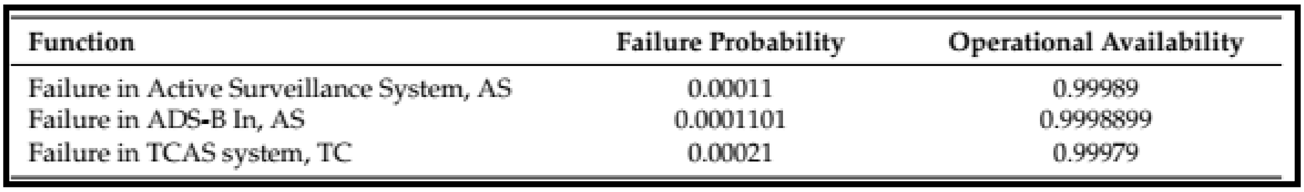
The failure in the DAA capability onboard deduced in Figure 50 is 9.356 × 10-6, which implies operational availability of higher than 99.99%. For the fault tree presented in Figure 50 two most important intermediate events are failure in cooperative and non-cooperative surveillance sensor failure. The following Table 8 and Table 9 summarize the results of intermediate events fault trees.

Table 8. Result Summary for DAA Capability Fault Tree Analysis (FTA) as per Fig. 50 [42]



Function	Failure Probability	Operational Availability
Failure in Cooperative System (Traffic Detection Function), DAA 1	5.056×10^{-6}	0.999994944
Failure in Non-cooperative Surveillance System, DAA 2	2.2×10^{-6}	0.9999978
Command Datalink Failure, DAA 5	1.1×10^{-6}	0.9999989
Execution Function Failure, DAA 4	1×10^{-6}	0.999999
Evaluation Function Failure, DAA 3	2×10^{-13}	~1

Table 9. Result Summary for the Cooperative Surveillance (traffic detection function) FTA as per Fig. 51 [42]



Function	Failure Probability	Operational Availability
Failure in Active Surveillance System, AS	0.00011	0.99989
Failure in ADS-B In, AS	0.0001101	0.9998899
Failure in TCAS system, TC	0.00021	0.99979

4.3.4 UAV Safety conclusion

The overall safety system requirement for the positioning and navigation for UAV application is fixed at 10-7. The following system detailed design will decompose this figure within the different component in space, ground augmentation and OBU. This will be done also exploiting the requirement and needs of the other two applications Road and Rail and the product that the HELMET core centre will delivery.

4.4 FAULT TREE ANALYSIS FOR THE MULTI-MODAL AUGMENTATION SYSTEM

The Augmentation System has to meet different performances required by Rail, Automotive and UAVs.
In order to meet the different requirements from Rail, Automotive and UAV sector, several Augmentation techniques have to be foreseen, having different safety requirements.
Main Augmentation techniques to be considered are:

- DGNSS
- RTK and NRTK
- PPP and PPP-RTK

Within ERSAT-EAV and RHINOS, the 2-Tiers approach has been developed, able to meet SIL-4 requirements for Rail applications (see [18]). Such an approach is based on the analysis of single difference among satellites and double difference residuals between Local Augmentation Reference Stations, SBAS EDAS RIMS raw data for detecting satellites/constellations and Reference Stations Faults.

The 2-Tiers approach is summarised in Figure 57.

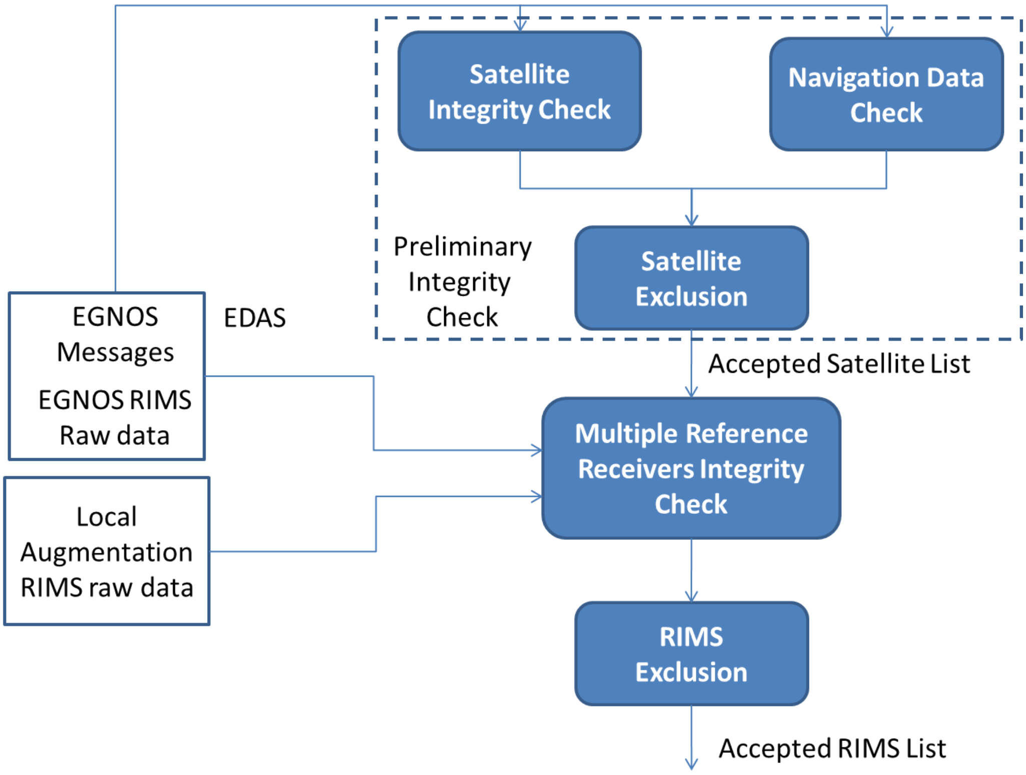


Figure 57- 2-Tiers Algorithm approach

Single differences of pseudorange residuals among satellites and of double difference residuals among reference stations and satellite are iteratively compared to a threshold calculated through the inverse of the generalised cumulative distribution for detecting and excluding Faulty satellites and Reference Stations, respectively.

Such an approach is applicable to DGNSS and RTK and allows using commercial receivers and networks for integrity monitoring purposes.

For NRTK, based on clusters of 4-5 Reference Stations, multiple Reference Stations faults and their combination have to be taken into account.

For PPP, the Integrity of the whole on field solution is significantly dependent on local effects (e.g. multipath and shadowing). Furthermore, due to the nature of PPP approach, very precise estimation of Precise Ephemeris, Clocks are needed, as well as Ocean Loading and Earth tides effects. For PPP-RTK, the estimation of satellite biases and the incorrect Ambiguity fixing on the receiver side play a relevant role.

PPP-RTK Integrity Monitoring algorithms are at a beginning phase and are still not mature for a commercial development (e.g. [19], [39]).

Therefore, in the following, RTK/NRTK FTA will be analysed in detail. Relevant results can be rescaled through the application of 2-Tiers Probability of Missed Detection ranges.

Galileo HAS can also be considered equivalent to the PPP case and it will be reviewed during the next phase, when the relevant ICD will available.

The list of possible Error Sources for the Augmentation Control Centre and OBU is reported in Table 10 [18].

Table 10. Augmentation Control Centre Error Sources and impact on OBU processing

Error Class	Error Source	Effect	Affected Function	Augmentation mitigation	Safety and Integrity
Satellite	Clock Drift	Acceleration in the PR	Augmentation Control Centre, OBU Processing	Mostly removed in differential positioning techniques; estimated in PPP	Detected by the Local Augmentation Control Centre
Satellite	Clock Offset	Offset in the PR	Augmentation Control Centre, OBU Processing	Mostly removed in differential positioning techniques; estimated in PPP	Detected by the PPP Augmentation Control Centre
Satellite	Instrumental biases estimation	biases the ambiguity	OBU Processing	Mostly removed in differential positioning techniques; estimated in PPP	Detected and estimated by the PPP Augmentation Control Centre
Satellite	Broadcast Ephemeris by the navigation satellite	Incorrect calculation of geometric range	Augmentation Control Centre, OBU Processing	Mostly removed in differential positioning techniques (distance decorrelation); estimated in PPP	Detected and estimated by the PPP Augmentation Control Centre
Satellite	Precise Ephemeris corrections	Incorrect calculation of precise ephemeris corrections (only for PPP)	OBU Processing	Removed in differential positioning	N/A
Satellite	Satellite Transmitter	Reduced signal power, C/N degradation	Augmentation Control Centre, OBU Processing	Reduction of PR noise through Carrier Smoothing for code measurements	N/A
Satellite	Satellite Code-Carrier divergence	Code advance, carrier delay	Augmentation Control Centre, OBU Processing		Detected and estimated by the PPP Augmentation Control Centre and LA Augmentation control Centre

Satellite	Satellite Signal Deformation	Correlation peak offset	Augmentation Control Centre, OBU Processing		Detected and estimated by the PPP Augmentation Control Centre and LA Augmentation control Centre
SIS Propagation	Troposphere (hydrostatic component)	Signal delay	Augmentation Control Centre, OBU Processing	Almost totally removed in differential positioning through modelling	To be bounded by statistical modelling
SIS Propagation	Troposphere (wet component)	Signal delay	Augmentation Control Centre, OBU Processing	No A priori models; estimated by OBU and Local Service Providers in PPP-RTK	Neglected in differential positioning
SIS Propagation	Ionosphere (first order effects)	Code-Carrier divergence, code delay, carrier advance	Augmentation Control Centre, OBU Processing	Almost removed through differential corrections (Distance correlated); precise estimation n PPP-RTK from Local Service Providers;	Local divergence monitoring and FDE on gradient by the Augmentation Control Centre
SIS Propagation	Ionosphere (higher order effects)	Neglected in Differential Positioning, slow convergence in PPP	Augmentation Control Centre, OBU Processing	Neglected in Differential positioning; to be estimated for PPP	N/A
SIS Propagation	unintentional Interferences near Reference Stations	Increased noise, C/N degradation	Augmentation Control Centre, OBU Processing	Smoothed by multiple Reference Station processing in NRTK	FDE by the Local Augmentation Control Centre
SIS Propagation	Intentional Interferences near Reference Stations (spoofing)	False SIS Carrier tracking, wrong positioning	Augmentation Control Centre, OBU Processing	C/N monitoring or advanced systems based on multiple antennas array	Anti-spoofing systems detection at Local Augmentation control Centre
SIS Propagation	Intentional Interferences near Rover (Spoofing)	False SIS Carrier tracking, wrong positioning	Augmentation Control Centre, OBU Processing	Local Augmentation or external monitoring means	Anti-spoofing systems detection at Local Augmentation control Centre
Augmentation Control Centre	Processing Failure	Multiple effects	OBU Processing	No error	Augmentation Control Centre detects

Augmentation Control Centre	Receiver Hardware	Multiple effects	OBU Processing	Recovery by Augmentation design or though human intervention	Augmentation Control Centre detects and Bound through B-value (GBAS) or exclusion
Augmentation Control Centre	Reference Station position error	Incorrect measurement for biases and measurements errors estimation	Augmentation Control Centre	Augmentation Control Centre Monitoring	Augmentation Control Centre Detection and exclusion
Site Displacement	Solid Earth tide	Multiple effects	OBU Processing	Augmentation Control Centre Monitoring	N/A
Site Displacement	Ocean Loading	Multiple effects	OBU Processing	Augmentation Control Centre Monitoring	N/A
Site Displacement	Pole Tide	Multiple effects	OBU Processing	Augmentation Control Centre Monitoring	N/A
Site Displacement	Atmospheric Loading	Multiple effects	OBU Processing	Augmentation Control Centre Monitoring	N/A
OBU Receiver	Receiver Hardware	Bias into measurements	OBU Processing	Augmentation Control Centre Monitoring	N/A
OBU Receiver	Phase Center offset and Phase Center Variations errors	Bias into measurements	OBU Processing	Augmentation Control Centre Monitoring	N/A
OBU Receiver	Incorrect Ambiguity fixing	Bias into measurements and noise in positioning	OBU Processing	OBU Correct Fixing Advanced Validation techniques	N/A
OBU Receiver	Cycle Slips	Impact on ambiguity Fixing	OBU processing	Cycle slips detection algorithms	Overbounding by Design

The detailed Fault-Tree for the Multimodal RTK GNSS Augmentation System is reported in the following Figure 58:

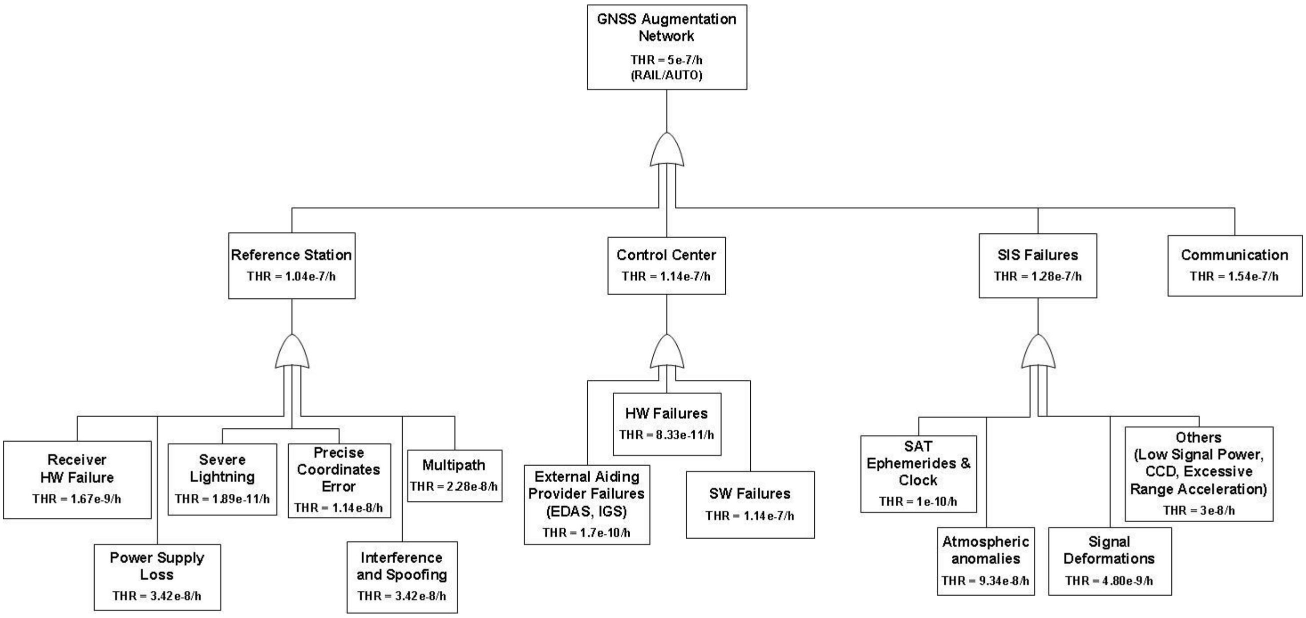


Figure 58 - Augmentation System Fault Analysis (RTK case)

From previous analysis and user requirements, the THR target for a GNSS positioning system, consisting of an On Board Unit GNSS receiver plus a Multimodal RTK GNSS Augmentation System (AIMN), is in the order of 1e-6/h for RAIL and 1e-5/h for AUTO.

The Fault-Tree for the Multimodal Augmentation has been derived, starting from the first level Safety Requirements reported in Figure 43 and the integration with the 2-Tiers method, in terms of probability of missed detection for Reference Stations and SIS. THR values are derived from GNSS Network operations statistics and literature values about anomalies.

The THR of the Multimodal RTK GNSS Augmentation System, apportioned taking into account the Augmentation Networks operations, depends on the THRs of the following failure sources:

- Reference Station Failure (1.04e-7/h)
- Control Center Failure (1.14e-7/h)
- Communication Failure (1.54e-7/h)
- Signal In Space Failure (1.28e-7/h)

The nominal value for the probability of missed detection used in the following derivation is 1e-4, taken from classical values in literature (e.g. [18]). Not modelled behaviours such as ionospheric scintillation, spoofing and interference are overbounded by design.

For the Reference Station we have:

- Loss of Power Supply
  Failures in Power Supply are due to a long term power loss (e.g. three days), when the Uninterruptible Power Supplies connected to the RS exhausts their batteries supplying capacity. Furthermore, power supply faults are due to transients interruptions, undervoltage or overvoltage, waveform distortion, frequency variations. Such behaviours can be absorbed by UPS systems only for a limited period of time. After that anomalous undetected behaviours can appear.
  The relevant not detected Probability of Fault per hour can be expressed as in the following:

Assuming the classical missed detection probability of 1e-4 and a fault probability of 3.42e-4/h (three fault per year):
THR = Pmd * Pfault = 3.42e-8/h.

- Reference Station Precise Coordinates Error
  Failures in the Reference Station position is due to an erroneous antenna position determination or Reference Framework determination, leading to not detected biases in the solution.
  Assuming a missed detection probability of 1e-4 and an assumed fault probability of 1.14e-4/h (one fault per year):
  THR = Pmd * Pfault = 1.14e-8/h.

- Severe Lightning
  Lightning can burn the gas capsule protecting the receiver. This can lead to anomalous behaviour of the Reference Stations in a limited amount of time
  Assuming 4 CG flashes/km^2/yr/average and a direct strike to building when lightning hits within 10 m [20], with a Reference Station area of 0.5m^2, the fault probability is set to 1.89E-7/h.
  Assuming a missed detection probability of 1e-4 , the relevant THR = Pmd * Pfault = 1.89e-11/h.

- Reference Stations Hardware Failure
  Receiver Hardware Faults concerns Hardware failures needing substitutions, firmware upgrades problems, partial channels unavailability, etc..
  Assuming a missed detection probability of 1e-4, and a MTBF in the order of 60000-100000 h of modern geodetic COTS receiver, the probability of fault can be estimated to 1.67e-5/h.
  THR = Pmd * Pfault = 1.67e-9/h.

- Multipath
  State of the Art geodetic receivers used in the current system are characterised by advanced multipath rejection techniques. With a suitable location selection at installation time, the multipath error is in average in the order of few decimetres. Furthermore, due to the repeatability, an on-site calibration of the error can significantly remove a great part of such error.
  Assuming a missed detection probability of 1e-4 and a fault probability of 2.28e-4/h (two fault per year):
  THR = Pmd * Pfault = 2.28e-8/h.

- Interference and Spoofing
  Assuming the classical missed detection probability of 1e-4 and a fault probability of 3.42e-4/h (three fault per year):
  THR = Pmd * Pfault = 3.42e-8/h

For the Control Center we have:

1. Hardware Failure

   A Control Center hardware failure does not occur when a single component is broken, thanks to redundancy and new technologies such as cloud and virtualizations. Therefore a Control Center can be very reliable, however it can be assumed a conservative MTBF of about 120000 h from technical specifications of major vendors, that leads to a fault probability of about 8.3e-8/h

Assuming a missed detection probability of 1e-3, THR = Pmd * Pfault = 8.3e-11/h.

2. Software Failure

   Relevant Software Faults to be considered in a Control Center are: Operative System interruption, data storage and application software faults. They can be mitigated through hot backup systems, data servers maintenance procedure and external monitoring. It can be assumed a relevant probability of missed detection of 1e-3 and a fault probability from literature data (referring to one fault per year), of 1.14e-4/h. The relevant THR can reach 1.14e-7/h.

3. External Aiding Provider Failures (EDAS, IGS)
   With a 1.5% of bad or empty data from IGS service in two years (e.g. [21]) and a similar fault rate for EDAS service, it can be assumed a fault probability of 1.7e-6/h. Assuming a missed detection probability of 1e-4, THR = Pmd * Pfault = 1.7e-10/h.

For the Signal In Space Failure we have:

1. Satellite Ephemeris and Clock Failure

   Concerning ephemeris errors, it is expected that through the access to Real-Time Precise Orbit products (e.g. IGS-RTS), relevant parameter can decrease by a 10 factor the impact of such component.
   In the GPS constellation, the observed service failure probability (from 5 events over 8 years and an average of 31 active satellites) is about 2.3e-6 per satellite per hour. In addition, due to the fact that the average service failure duration is much shorter than the maximum alerting time of 6 hours, the probability of any given satellite being in a service failure state is about 8e-7 [22].

   In the GALILEO constellation the nominal probability of hazardously misleading information is 1.7e-7 in 150 seconds, per hour it is achieved 4e-6/h [23]. Therefore, for both constellations, it can be assumed a fault probability of 1e-6/h and a missed detection probability of 1e-4, THR = Pmd * Pfault = 1e-10/h.

2. Atmospheric Anomalies

   Scintillation or local ionospheric anomalies can lead to undetected faults in Reference Stations behaviours.
   Considering the data from 2000 and 2004 which includes a solar maximum period [24], and selecting geomagnetic storms with extreme, severe, strong classification, we can assume a fault probability of 9.34e-5/h. Considering a missed detection probability of 1e-3, THR = Pmd * Pfault = 9.34e-8/h.

3. Signal Deformation

The prior probability of 2e-6 per 150-second, that a signal deformation fault occurs, is derived from an empirical analysis of these failures for the time that GPS has been active [25]. Therefore, we can consider a fault probability of 4.8e-5/h, and a missed detection probability of 1e-4 [26], a THR of 4.8-9/h is achieved.

4. Others: we include here not modelled behaviours to be overbounded by design (Low Signal Power, Excessive Range Acceleration) fault probability 3e-5/h and a missed detection probability 1e-3, THR = Pmd * Pfault = 3e-8/h.

For the Communication Failure: No Connection, Data Loss, Delay. An Integrity Monitor detects the link QoS (e.g. latency). If the latency is greater than a fixed threshold (e.g. 10 s), the Reference Station can be declared in fault.

Through advanced ICT QoS Monitoring, a missed detection probability of at least 1e-4 is obtained. A THR of 1.54e-7/h can be achieved for Communication Faults, with a fault probability of 1.54e-3/h.

The Fault Tree Analysis for the PPP Augmentation is provided in Figure 59. Relevant values are derived from existing papers and assumptions about the apportionment (e.g. [27]).

The PPP and PPP-RTK Fault analysis can be rescaled (leading to lower Probability of Missed Detection assumptions) if advanced Integrity Monitoring algorithms, taking into account OBU Ambiguity Resolution validation techniques and under development Integrity Monitoring systems are considered.

The Fault Tree is in this case subject to three main possible fault branches:

- PPP Control Centre Augmentation Fault: it contains the not detected faults from the PPP augmentation Control Centre; they include modelling errors for standard PPP only (precise ephemeris and clocks errors and satellite biases, taken from literature, e.g.); such value can be gathered from external providers (in this case same values of IGS can be applied); for PPP-RTK performances, precise Local Ionospheric and tropospheric error mismodelling is foreseen as a relevant source of misleading information, while external data (e.g. PCV and Ocean Loading parameters) have been considered as a minor source of error); PPP Control Centre can anyway take as PPP augmentation sources existing international organisations solutions (e.g. IGS)
- Communication links: it is the link between the Augmentation System and the OBU for the transmission of augmentation messages; the future Galileo HAS message broadcasting fault is here included
- OBU Errors: this is the most relevant fault source, due to current technological limitations and level of maturity of PPP in terms of convergence time and PPP-RTK ambiguity resolution validation. It is added as reference for showing the impact of user side on the overall PPP-RTK Fault analysis.

From the analysis, it is evident how the Control Centre Augmentation faults have to be reduced as much as possible for allowing achieving the needed THR. Of particular relevance is the Precise Ephemeris and Clock fault, satellite biases as well as the precise STEC determination. Within this framework, the allocation present in literature of 7.66 E-8 has to be mitigated in order to implement a PPP-RTK system for the future. The redundancy message provided by Galileo HAS (especially if available through NTRIP by GSC), as an independent source, can help achieving the Safety Target.

Therefore, PPP analysis here carried out, but Augmentation solutions will be based on RTK and NRTK only.

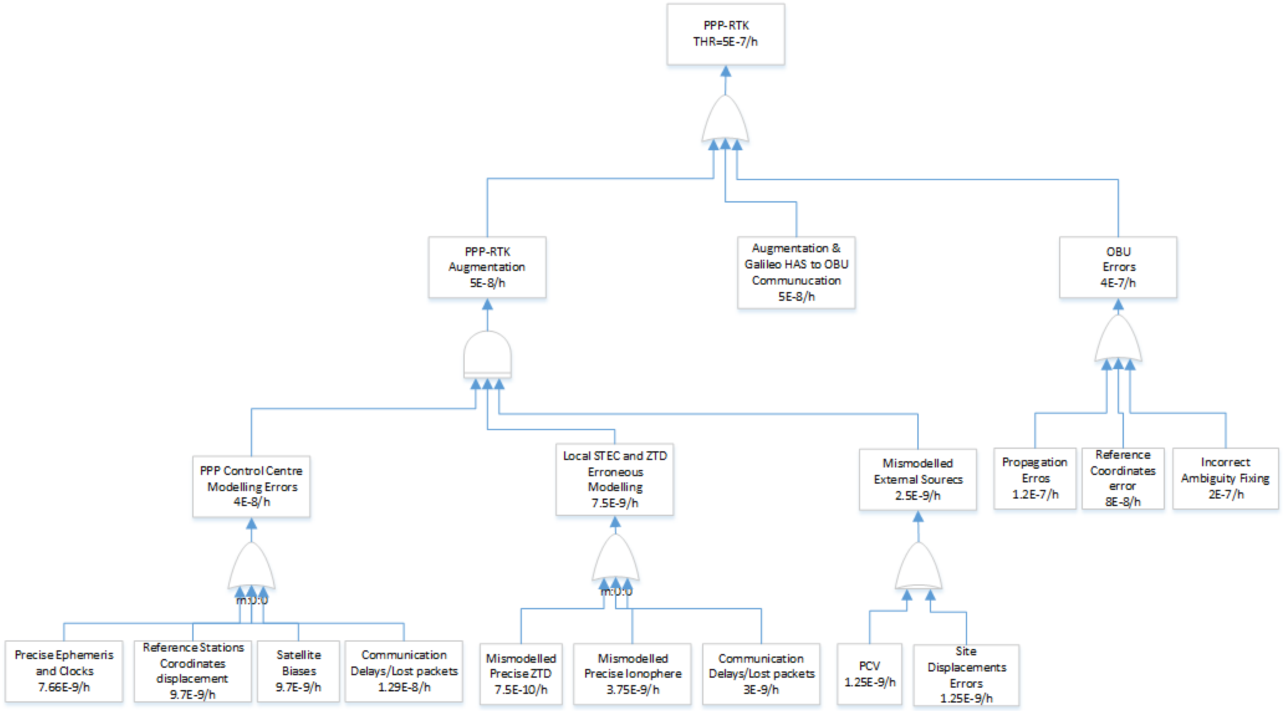


Figure 59. PPP/PPP-RTK Fault Tree

5. SPECIFICATION OF SYSTEM REQUIREMENTS

The system requirements for Reference Architecture are identified by a code, according to the following identification:

SR-SSR-TTT-N.a

where:

- **SR** is a fixed string standing for "System Requirement";
- **SSR** is a fixed string standing for "Sub-System Requirement"; (see *Table 11*)
- **TTT** is a three letters specification type code (see *Table 12*), compliant with ECSS Standards classification;
- **N** is the sequential number of the requirement, with respect to **TTT**;
- **a** is a progressive letter used in case of more than one specification belonging to the same N-level.

Table 11. Sub-System Requirements Codes

Code	Type	Description
AUG	Augmentation	Generalised Augmentation System
COM	Communication	Communication data transmission and receiver information gathering
OBU	On-Board Unit	Sensors and processing functions within the OBU
EXT	External Systems	Single applications functions implemented in application specific systems

Table 12. List of Requirements type codes

Requirement Class	Code
Functional Requirements	FUN
Performance Requirements	PER
Interface Requirements	INF
Operational Requirements	OPE
Resource Requirements	RES
Verification Requirements	VER
Acceptance Testing Requirements	ACC
Documentation Requirements	DOC
Security Requirements	SEC
Portability Requirements	POR
Quality Requirements	QUA
Reliability Requirements	REL
Maintainability Requirements	MAI
Safety Requirements	SAF

5.1 RAIL: ERTMS SYSTEM REQUIREMENTS

This section contains specification of Railway System Requirements for HELMET derived from the User Requirements Specification contained in the HELMET deliverable D2.1 and also using detailed analysis performed in Section 4.1 of this document.

The System Requirements for RAIL are specified in the format **SR-SSR-TTT-N.a**, with the codes SSR and TTT explained in Table 11 and Table 12 at the beginning of Section 5.

Note: Sequence numbers in the range of 001-100 were allocated to RAIL system requirements in HELMET.

ID	Name	Description
SR-OBU-SAF-001.a	Tolerable Hazard Rate of Virtual Balise subsystem hazard (VBTX)	This requirement defines Tolerable Hazard Rate of Virtual Balise subsystem hazard (VBTX), which is THR_{VBTX}= 6.7e-10/ h
Rationale		
The THR_{VBTX} requirement related to the Virtual Balise subsystem hazard is derived in the same way as the THR_{BTX} requirement (Balise/ Loop hazard) for a physical balise – see Figure 34 . The derivation is based on the ETCS Core Hazard allocation to the physical ETCS balise hazardous events. See for more details ERTMS/ETCS subset-088 (Part 3) and in the HELMET deliverable D2.3, Sections 4.1.1.		
References		
[13]; [14], HELMET D2.3, Sections 4.1.1.		

D	Name	Description
SR-OBU-SAF-002.a	Tolerable Hazard Rate of Virtual Balise insertion (TRANS-VBALISE-3)	This requirement defines Tolerable Hazard Rate of Virtual Balise insertion, i.e. $THR_{VB\_Insertion}$ = 6.6e-10/ h.
Rationale		
The $THR_{VB\_Insertion}$ = 6.6e-10/ h is derived from the THR_{VBTX}= 6.7e-10/ h – see Figure 34. The derivation of the $THR_{VB\_Insertion}$ is based on the same approach that it is used for the THR_{BTX}= 6.7e-10/ h allocation to physical balise hazardous events, i.e. TRANS-BALISE-1 (Message corruption), TRANS-BALISE-2 (Balise deletion), and TRANS-BALISE-3 (Balise insertion/ cross talk) – see Figure 34 and Figure 33. Since the Virtual Balise insertion TRANS-VBALISE-3 (i.e. cross-talk due to the incorrect GNSS-based train position determination) is much dangerous than the Virtual Balise deletion (TRANS-VBALISE-2), then the risk due to TRANS-VBALISE-2 is also allocated to TRANS-VBALISE-3. Note: The TRANS-BALISE-1 with $THR_{VB\ Corruption}$ < 1e-11/h is included in THR_{VBTX}= 6.7e-10/ h and represents the safety requirement for communications associated with the GNSS based position determination function. See for more details HELMET deliverable D2.3, Sections 4.1.1, 4.1.2 and 4.1.3.		
Notes		
References		
[14]; HELMET D2.3, Sections 4.1.1, 4.1.2 and 4.1.3.		

ID	Name	Description
SR-OBU-SAF-003.a	Tolerable Hazard Rate of Virtual Balise insertion across track	This requirement defines Tolerable Hazard Rate of Virtual Balise insertion across track, i.e. THR$_{H9}$ = 3.3e-10/ h
Rationale		
The THR$_{VB\_Insertion}$ of 6.6e-10/ h is equally split between THR of two following events: 1) Virtual Balise insertion along track, i.e. erroneous localization of Virtual Balise with reception of valid VB with THR$_{H7}$ = 3.3e-10/ h, and 2) Virtual Balise insertion across track, i.e. erroneous reporting of VB in a different track information with THR$_{H9}$ = 3.3e-10/ h - see Figure 34		
Notes		
References		
[14]; HELMET D2.3, Sections 4.1.2.		

ID	Name	Description
SR-OBU-SAF-004.a	Tolerable Hazard Rate of Virtual Balise insertion along track	This requirement defines Tolerable Hazard Rate of Virtual Balise insertion along track, i.e. THR$_{H7}$ = 3.3e-10/ h
Rationale		
The THR$_{VB\_Insertion}$ of 6.6e-10/ h is equally split between THR of two following events: 1) Virtual Balise insertion along track, i.e. erroneous localization of Virtual Balise with reception of valid VB with THR$_{H7}$ = 3.3e-10/ h, and 2) Virtual Balise insertion across track, i.e. Erroneous reporting of VB in a different track information with THR$_{H9}$ = 3.3e-10/ h - see Figure 34		
Notes		
References		
[14]; HELMET D2.3, Sections 4.1.2.		

ID	Name	Description
SR-OBU-SAF-005.a	Alert Limit (AL) across track related to Track identification	This requirement defines Alert Limit (AL) across track related to Track identification, i.e. AL$_{TI}$ = 1.785 m
Rationale		
The track identification function is available when Protection Level calculated by OBU (integrating GNSS receiver) using augmentation data doesn't exceed Alert Limit, which should be less than half of the track spacing TS value – see Fig. 20, HELMET D2.1 [1]. Typical values of track spacing TS for different types of track in different areas are listed in Table 16 - HELMET D2.1. It is evident from Table 16 that the minimum value of TS is allowed for multi-track lines between stations, which is 3570 mm. It means that the maximum value of Alert Limit for track identification function for HELMET solution should be less than 3570 mm/ 2, i.e. 1.785 m.		
Notes		
References		
HELMET D2.1 [1].		

ID	Name	Description
SR-OBU-PER-006.a	Accuracy of train position determination across track (2*sigma) for Track identification	This requirement defines Accuracy of train position determination across track (2*sigma) for Track identification, i.e. ≈ 0.7 m.
Rationale		
The required accuracy of HELMET position determination function depends on the HEMET system solution, on the safety architecture, applied safety principles, etc. Based on the experience gained within the RHINOS project with the composite fail-safety solution (see Fig. 21), where THR of 1e-6/ hr was allocated to GNSS, then K – multiplier factor for AL to estimate sigma (AL = K* sigma) can be determined for Gaussian error distribution using Matlab as follows: abs(norminv(1e-6/2 ,0,1)) = 4.8916 ~ 5 . If AL of 1.785 m (3570 mm/2) is considered, then 1 sigma should be 0.357 m and 2*sigma ~ 0.714 m. It is a preliminary estimated value and will be clarified during HELMET solution.		
Notes		
References		
HELMET D2.1 [1], Section 3.		

ID	Name	Description
SR-OBU-FUN-007.a	Time to Alert (TTA) related to Track identification	This requirement defines Time to Alert (TTA) related to Track identification, i.e 10s < TTA < 30 s
Rationale		
Parallel track discrimination function is not a position estimation problem, but a decision problem. It means that TTA has mainly impact on the operational availability and not on the functional system safety. An average duration of the ERTMS Start of Mission in Staff Responsible is 3% of mission (SUBSET-088). Since an average duration of mission (train journey) is 1 hour, then duration of Start of Mission is 108 s. Further, ETCS onboard subsystem shall take no more than 60 s to go from No Power (NP) to being ready to accept data entry in Standby (SB). Therefore, values of 10s < TTA < 30 s proposed by the HELMET User Requirement UR_001 is appropriate. The difference between the Position estimation problem and Decision problem and its impact on the system requirements specification is described in the HELMET deliverable D2.3, Section 4.1.4.		
Notes		
References		
HELMET D2.1 [1], Section 3., HELMET D2.3, Section 4.1.4		

ID	Name	Description
SR-OBU-SAF-008.a	Tolerable Hazard Rate of Message corruption related to Virtual Balise detection	This requirement defines Tolerable Hazard Rate of Message corruption related to Virtual Balise detection, i.e. $THR_{VB\ Corruption}$ < 1e-11/h
Rationale		
The $THR_{VB\ Corruption}$ < 1e-11/h directly results from the ETCS Core hazard allocation to Balise subsystem hazard – see Figure 33, Figure 34		
Notes		
References		
[13]; HELMET D2.3, Sections 4.1.1 and 4.1.2.		

ID	Name	Description
SR-OBU-COM-009.a	Communication delay related to Virtual Balise detection	This requirement defines Communication delay related to Virtual Balise detection, i.e. T_{Delay} = 5 s max
Rationale		
Age of GNSS differential corrections up to 5 seconds doesn't cause degradation of the position determination accuracy.		
Notes		
References		

ID	Name	Description
SR-OBU-FUN-010.a	Accuracy of train position determination along track (2*sigma) related to Odometry calibration	This requirement defines Accuracy of train position determination along track (2*sigma) related to Odometry calibration, i.e. 0.7 m
Rationale		
Location accuracy for vital purposes: The location accuracy (of on-board ERTMS Balise Transmission Module – BTM) shall be within ± 1 for each balise, when a balise has been passed [28]. More detailed specification of the location accuracy (e.g. using sigma) is missing in [28]. Accuracy expressed using 2*sigma (95% confidence) or 3*sigma (99.7% confidence) is usually sufficient for many of technical applications. Let's conservatively assume an accuracy of 3*sigma for the odometry calibration function. Then the 1 sigma is 1 m /3 = 0.333 m . Conclusion: Accuracy (2*sigma) of 0.666 m =0.7 m. This value will be clarified within next phases of HELMET solution.		
Notes		
References		
[28] ERTMS/ETCS – Class 1, SUBSET-036: FFFIS for Eurobalise; [2] HELMET D2.2 Section 3.		

ID	Name	Description
SR-OBU-SAF-011.a	Alert Limit (AL) along track related to Odometry calibration	This requirement defines Alert Limit (AL) along track related to Odometry calibration, i.e. $AL_{OC} = 1.7$ m
Rationale		
To estimate a magnitude of Alert Limit for the odometry calibration function (vital function), let's assume that AL approximately equals to 5*sigma – see Track identification section. Then AL ~ 5 * sigma = 5 * 0.333 = 1.665 m.		
Notes		
References		
[1] HELMET D2.1, Section 3.1.2		

ID	Name	Description
SR-OBU-SAF-012.a	Time to Alert (TTA) related to Odometry calibration	This requirement defines Time to Alert (TTA) related to Odometry calibration, i.e. TTA < 1 second
Rationale		
Odometry calibration requires a train position determination function. TTA (time to alert / time to fault detection and negation) has usually impact on the final system integrity. A TTA value depends on the safety-related system architecture and the required Safety Integrity Level. A typical TTA value < 1 second is required for safety systems compliant with SIL 4. This value will be clarified during next phases of HELMET.		
Notes		
References		
[1] HELMET D2.1, Section 3.1.2		

ID	Name	Description
SR-OBU-SAF-013.a	Alert Limit (AL) along track related to Cold movement detection	This requirement defines Alert Limit (AL) along track related to Cold movement detection, i.e. $AL_{CMD} = 5$ m.
Rationale		
The ETCS Cold Movement Detection function shall invalidate the stored ETCS position information for any movement in excess of 5 m (Normative). Integration with train operations: Moving a rail vehicle up to 5 m is considered to be the maximum acceptable distance allowance for revalidating train position upon leaving NP (No Power). The Cold Movement Detection function shall only indicate any movement excessing 5 m [29]. This value is taken as a user defined Alert Limit for odometer calibration function.		
Notes		
References		
[29]; [1] HELMET D2.1, Section 3.1.3.		

ID	Name	Description
SR-OBU-FUN-014.a	Accuracy of train position determination across track (2*sigma) related to Cold movement detection	This requirement defines Accuracy of train position determination across track (2*sigma) related to Cold movement detection, i.e. 2 m
Rationale		
The required accuracy of HELMET position determination function intended for the Cold Movement Detection function depends on the HEMET system solution, on the safety architecture, applied fail-safe principles, etc. Based on the experience gained within RHINOS project (AL ~ 5 * sigma) and considering a composite fail-safety solution together with AL of 5 m, then 1 sigma should be 1 m. Accuracy (2*sigma) of train position determination has to be less than 2 m.		
Notes		
References		
[1] HELMET D2.1, Section 3.1.2		

ID	Name	Description
SR-OBU-SAF-015.a	Time to Alert (TTA) related to Cold movement detection	This requirement defines Time to Alert (TTA) related to Cold movement detection, i.e. TTA < 10 s
Rationale		
This requirement was estimated within the GNSS User Consultation Platform. It will be clarified in next phase of HELMET solution.		
Notes		
References		
Report on Rail User Needs and Requirements: Outcome of the European GNSS' User Consultation Platform. GSA-MKD-RL-UREQ-250286, Issue/Revision: 2.0, Date: 01/07/2019, 80 pages; HELMET deliverable D2.1, Section 4.		

ID	Name	Description
SR-OBU-SAF-016.a	Safety Integrity level of train position determination function	This requirement defines Safety Integrity level (SIL) of train position determination function in OBU - it should be compliant with SIL 4.
Rationale		
THR allocated to the Virtual Balise subsystem hazard (THR_{VBTX}) is 0.67e-9/ 1 h – see Figure 34 in this document. It corresponds to SIL 4. It is also assumed that Odometer calibration and Cold movement detection functions shall be compliant with SIL 4.		
Notes		
References		
[1] HELMET D2.1, Sections 3 and 4.		

ID	Name	Description
SR-OBU-PER-017.a	Dependability of position determination function	- The Mean Time Between Service hardware failures MTBF of HELMET onboard equipment shall be not less than 3x10^{5} hours; - HELMET OBU maximum unavailability: 1x10^{-6}
Rationale		
It results from the analysis performed in Section 4.1.6		
Notes		
	Availability has indirect impact on railway safety.	
References		
[30], [43] - [45]		

ID	Name	Description
SR-OBU-SEC-018.a	Security of position determination function	This requirement defines security of position determination function – it shall be HIGH
Rationale		
Security of position determination function shall be HIGH in order to preserve related RAMS and confidentiality. It will be specified in detail within next project phases.		
Notes		
References		
[30]		

ID	Name	Description
SR-OBU-SAF-019.a	Speed accuracy for ERTMS	This requirement defines Speed accuracy for ERTMS applications as follows: ± 2 km/h for speed lower than 30 km/h, then increasing linearly up to ± 12 km/h at 500 km/h.
Rationale		
Defined in ERTMS/ETCS Subset 041.		
Notes		
References		
ERTMS/ETCS Subset 041.		

5.2 AUTO: AUTOMATED DRIVING SYSTEM REQUIREMENTS

In this section, we derive the automotive system requirements for horizontal position, system reaction time, data rate, availability and continuity. A summary of all automotive system requirements can be found in

Table 15.

5.2.1 Horizontal Position Requirements

The main operational requirements relate to the total system error of automated cars under certain scenarios. Here we try to further narrow down the requirements on the localization system. We split the complete localization of the automated car into two problems: a) the identification of the lane the car is driving and b) the positioning of the car within this lane. The latter can be further separated into lateral and longitudinal localization of the vehicle. In general, these three localization problems might present different particularities and challenges that can be potentially solved by different subsystems within the localization system.

Lane-level Localization/ Identification

The first step for a complete lateral localization of a vehicle in a road with multiple parallel lanes consist in the correct determine of the lane the vehicle is. Although in a continuous navigation of the vehicle, the vehicle is expected to maintain its positioning within the lane and not abandon it unwillingly, the function that identifies the correct lane is important for the following situations:

- The start of the navigation system (similarly to the start of mission in railway).
- The warm restart of the system after a loss of availability or loss of continuity event.
- The determination of the status of overtakes: Non-initiated, transition, in parallel lane, completed.
- As information that the vehicle hasn’t invaded the other lane, particularly important in two direction roads.
- To support localization in roads with bad or non-existent lane markings.

In order to derive requirements for the lane-level localization, we start by assuming that the vehicle is within the limits of one lane (e.g., guaranteed by the in-lane positioning that will be described in the next section). Moreover, we want to satisfy that the vehicle is localized in the lane it actually is, or similarly we want to guarantee that the probability of localizing the vehicle in the wrong lane is smaller than the risk we can assume for that (IR):

$$P\left(\hat{L} \in A \middle| L \in B\right) \leq IR,$$

where $\hat{L}$ is the estimated location of the vehicle, L is the real location of the vehicle and $A,\ B$ are just general sets of possible positions within lane $a,\ b$, respectively.

The most limiting case is when the vehicle is close to the lane marks/boundaries as shown in Figure 60.

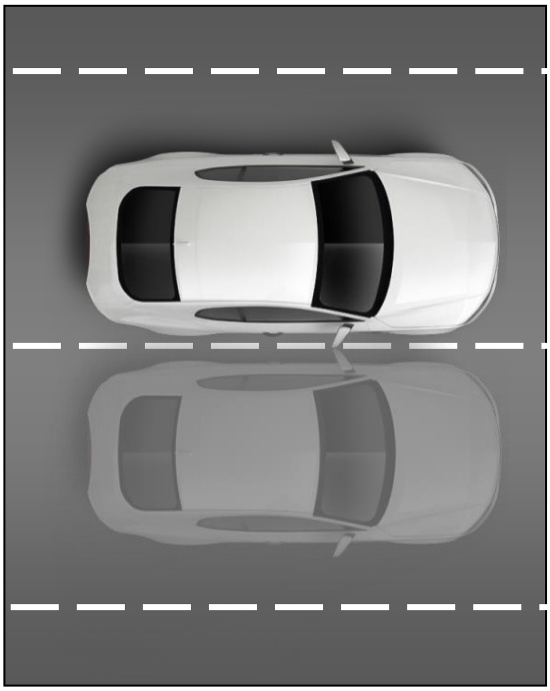


Figure 60. Limiting lane-level localization

The distance between the two lanes possible locations is therefore the car width plus the lane marker's width. In order to perform correct lane identification, we can only allow certain maximum position error produced laterally by the localization system. This maximum acceptable error is equivalent to the lateral alert limit:

$$\varepsilon_{lat,max} = AL_{lane} = (W_{veh} + W_{marking})/2$$

Lane markings are reported to have a width between 10 and 15 cms. Therefore, 10 cm is the most restrictive value. Car widths are reported in [9] between 1.72 m and 2.43m. Being the smallest value the most restrictive one for one study. This leads to a lateral alert limit for lane identification of $AL_{lane} = \frac{1.82}{2}\mathrm{m} = 91\mathrm{cm}.$

The error associated with lane localization is the sum between the error in the positioning system and the error in the map. We expressed it here by their related variances:

$$\sigma_{lane}^2 = \sqrt{\sigma_{pos,lane}^2 + \sigma_{map,lane}^2}$$

Let us assume that in a nominal case, the error in the map is some order of magnitude smaller than the positioning error. This could be justified if the map has been built by a geo-referencing process or finally improved by the accumulation of extensive data over the roads over time.
In this situation, in a nominal case, we lead to:

$$k_1\sigma_{pos,lane} \leq (W_{veh} + \ W_{marking})/2$$

The allocated risk for the complete car localization system is 3e-8 /hr. The one dimensional k_1 is therefore for this situation 5.5415, which leads us to:

$$\sigma_{pos,lane} = 16.4\ cm$$

And gives us a lane position accuracy requirement ($2\sigma_{pos,lat}$) of less than 33 cm.

In-lane localization/positioning – see Figure 61
Following a similar approach as it is done in aviation; we can consider initially the following different errors that contribute to the total in-lane system error:

1. The **navigation system error (NSE)** (i.e., the ability of the vehicle to know its own position in the desired frame of reference and determine where it should go).
2. The **driving technical and control error (DTE)** (i.e., the capacity of the vehicle to maintain the desired trajectory).
3. The **path definition error (PDE) .** The error made when designing or updating the path the vehicle should follow.

Assuming that NSE, DTE and PDE are stochastically independent, the standard deviation of the TSE can be expressed as:

$$\sigma_{TSE}^2 = \sigma_{NSE}^2 + \sigma_{DTE}^2 + \sigma_{PDE}^2$$

The TSE can also be split in longitudinal and lateral in-lane error components:

$$\sigma_{TSE}^2 = \sigma_{TSE,lat}^2 + \sigma_{TSE,long}^2$$

Regarding the ***lateral component***, the vehicle ideally must try to stay cantered as a nominal lateral position inside the lane with a “total system error” that is less than half the width of the lane minus half their respective car width. This can be expressed in the following way:

$$\underbrace{k\sigma_{TSE,lat}}_{\text{lateral TSE}} \le \frac{W_{lane}}{2} - \frac{W_{veh}}{2}$$

Where W_{lane} and W_{veh} are the width of the road lane and vehicle respectively, $\sigma_{TSE,lat}$ is the standard deviation of the TSE in lateral dimension and the multiplier *k* is obtained related to the allocated risk for the operation. In this case it is considered 3e-8 / hour/ car.

Note: The example above can be generalized for other operations by considering that the cars need to follow a certain path that is either predefined or updated online as a result of a decision process (i.e., path planning). This path planning process might be also imperfect, it might also depend on some external input about the traffic situation, the position of other vehicles and so on, but in any case it has to be determined how it contributes to the total system error. In order to keep things simpler, we neglect the PDE for the moment and it will be revisited in WP3.

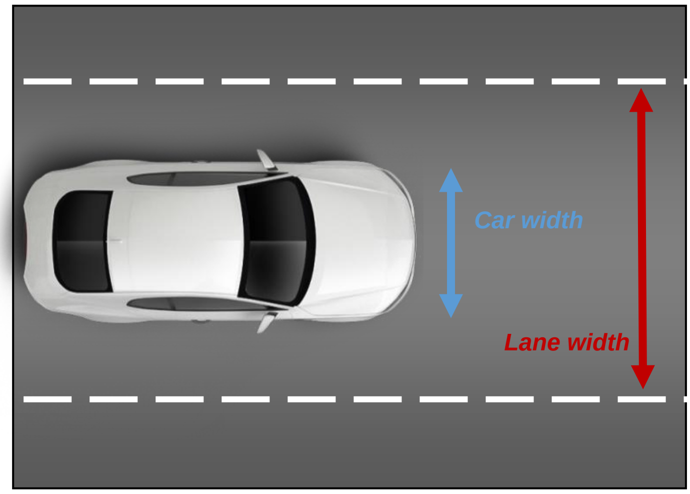


Figure 61. In-lane vehicle localization/positioning

Obtaining values for the DTE is challenging, they highly depend on the vehicle itself, the conditions of the road and the dynamics of the vehicle apart from the specific controller that is implemented. In [31], for the lane keeping scenario, the authors report simulations for a very slippery road a worst case lateral error of 28 cm. Since it is difficult also to know the exact distribution of DTE, we will consider that there is a certain worst case value for the current scenario that we can use. The lateral NSE can be therefore expressed now as:

$$NSE_{lat} \leq \frac{W_{lane}}{2} - \frac{W_{veh}}{2} - DTE_{max}$$

This expression gives us a straight forward relationship for computing the in-lane Alert limit:

$$AL_{lat} = \frac{W_{lane}}{2} - \frac{W_{veh}}{2} - DTE_{max}$$

as a function of the road lane width, the vehicle width and the maximum driving technical and control error expected.

Integrity allocation to NSE is 3e-8/hr, which we can initially split in half for the longitudinal and lateral. With this information, in the nominal navigation case, the previous equation can be used to obtain the standard deviation of the navigation error that would impose the accuracy requirement:

$$k_1\sigma_{acc,lat} \leq \frac{W_{lane}}{2} - \frac{W_{veh}}{2} - DTE_{max}$$

Where k_1 is the Gaussian multiplier based on the allocated risk to the NSE, which is 1.5e-8, and therefore $k_1 = 5.66$. Navigation accuracy is obtained as

$$Accuracy_{lat} = k_2\sigma_{acc,lat}$$

With k_2=2 (95% of the distribution).

Note that the navigation errors, even in the nominal situation may not have a Gaussian distribution. This is however a reference tool that it is commonly used to assess the operational requirements.

Notice that this accuracy value is valid for a positioning system that computes directly the lateral position of the vehicle with respect to the lane positions. If the position within the lane is computed by means of a global positioning system, the error in the information of the road map (i.e. lane positions) must be also taken into account, which would make the accuracy requirement more stringent.

In the following, let us study the sensitivity of the accuracy requirement for different values of lane width, vehicle width and lateral DTE (see Figure 62 – Figure 67):

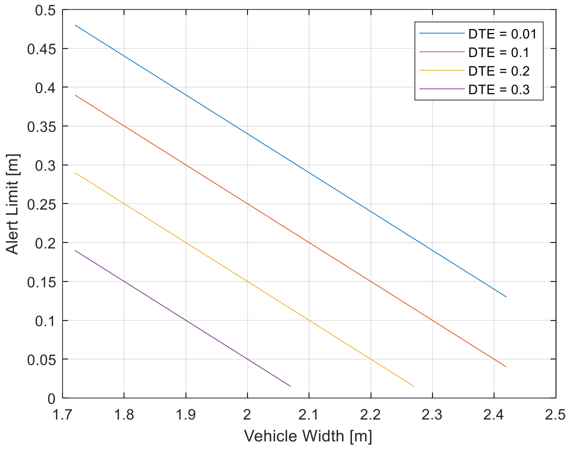


Figure 62. Lateral Alert Limit Sensitivity with respect to vehicle width (Lane width used 2.7 m)

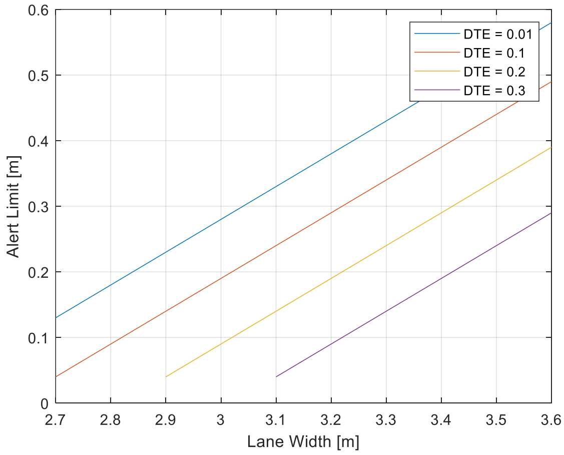


Figure 63. Lateral Alert Limit Sensitivity with respect to lane width (vehicle width used 1.72 m)

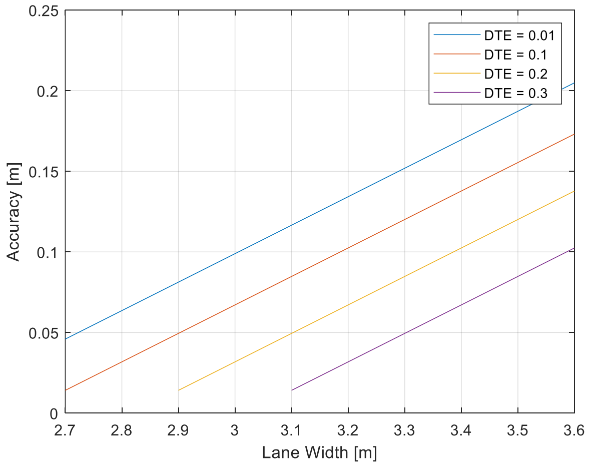


Figure 64. Lateral accuracy sensitivity with respect to lane width (IR=1.5e-8)

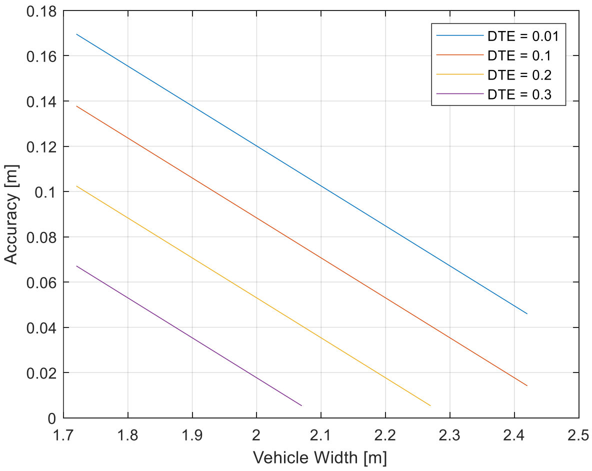


Figure 65. Lateral accuracy sensitivity with respect to vehicle width (IR=1.5e-8)

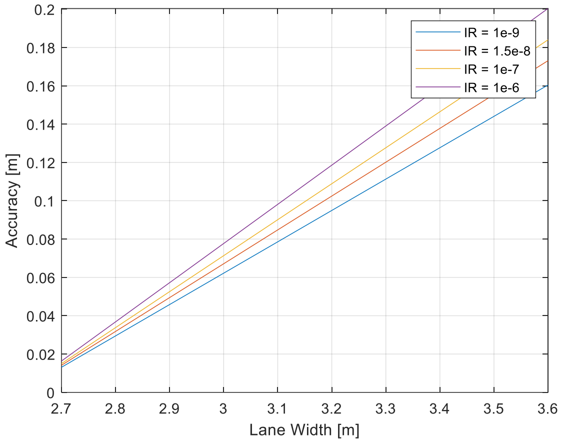


Figure 66. Lateral accuracy sensitivity with respect to lane width (DTE = 0.1 m)

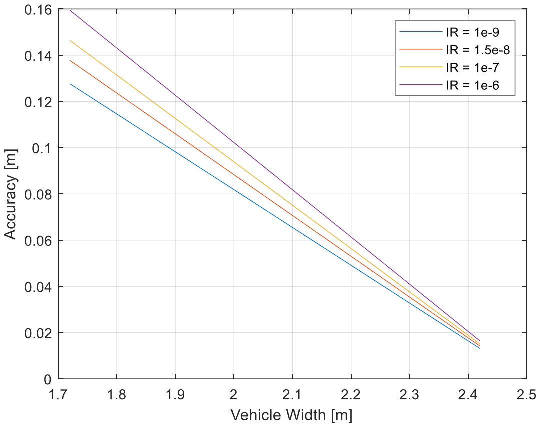


Figure 67. Lateral accuracy sensitivity with respect to vehicle width (DTE = 0.1 m)

For the most restrictive cases, we can see that the accuracy requirement must be in the order of few centimeters.

To define the ***longitudinal component** requirement*, we need to take the road/lane geometries into account. Evidently, the longitudinal requirement for straight lanes segments without any intersections/merge points might be less stringent that during curves or at crossings. In the following we want to look in more detail on the requirement for curves and crossings.

Taken into account the constraint that the lateral and longitudinal requirements must stay within the lane geometry for all time, this might lead to an independent lateral and longitudinal requirement on straight or quasi straight road segments. However, any curve may introduce a coupling of lateral and longitudinal requirements [9]. We can exploit the resulting coupling of lateral and longitudinal requirement to determine the latter for given particular vehicle dimensions and lateral requirements as stated above. This is illustrated in Figure 68.

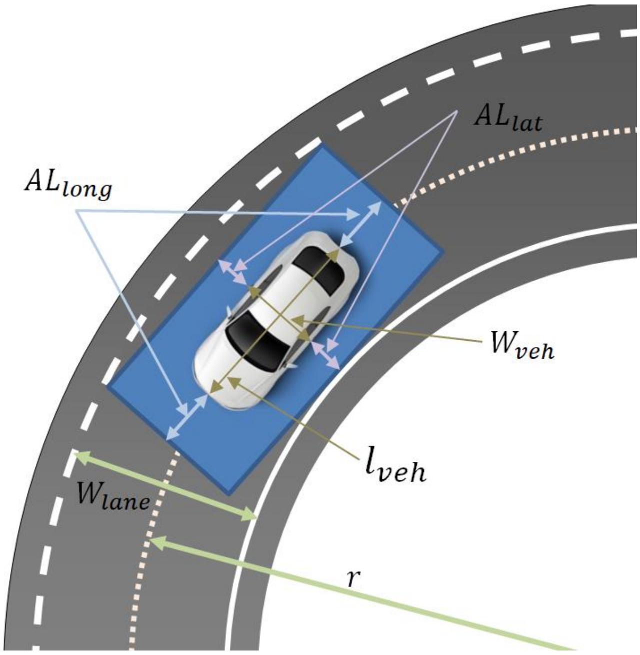


Figure 68. Illustration of maximum allowed error bounding box depending road geometry under the condition that the alert limits are ensured to stay within the lane [9]

As shown in [9], the coupling between the two requirements can be expressed as

$$\left(\frac{2AL_{long}+l_{veh}}{2}\right)^2+\left(r-\frac{W_{lane}}{2}+2AL_{lat}+W_{veh}\right)^2=\left(r+\frac{W_{lane}}{2}\right)^2$$

Where r is the curve radius and l_{veh} is the length of the vehicle. Reformulating this equation, we get for the longitudinal requirement:

$$AL_{long,curve}=\sqrt{\left(r+\frac{W_{lane}}{2}\right)^2-\left(r-\frac{W_{lane}}{2}+2AL_{lat}+W_{veh}\right)^2}-\frac{1}{2}l_{veh}$$

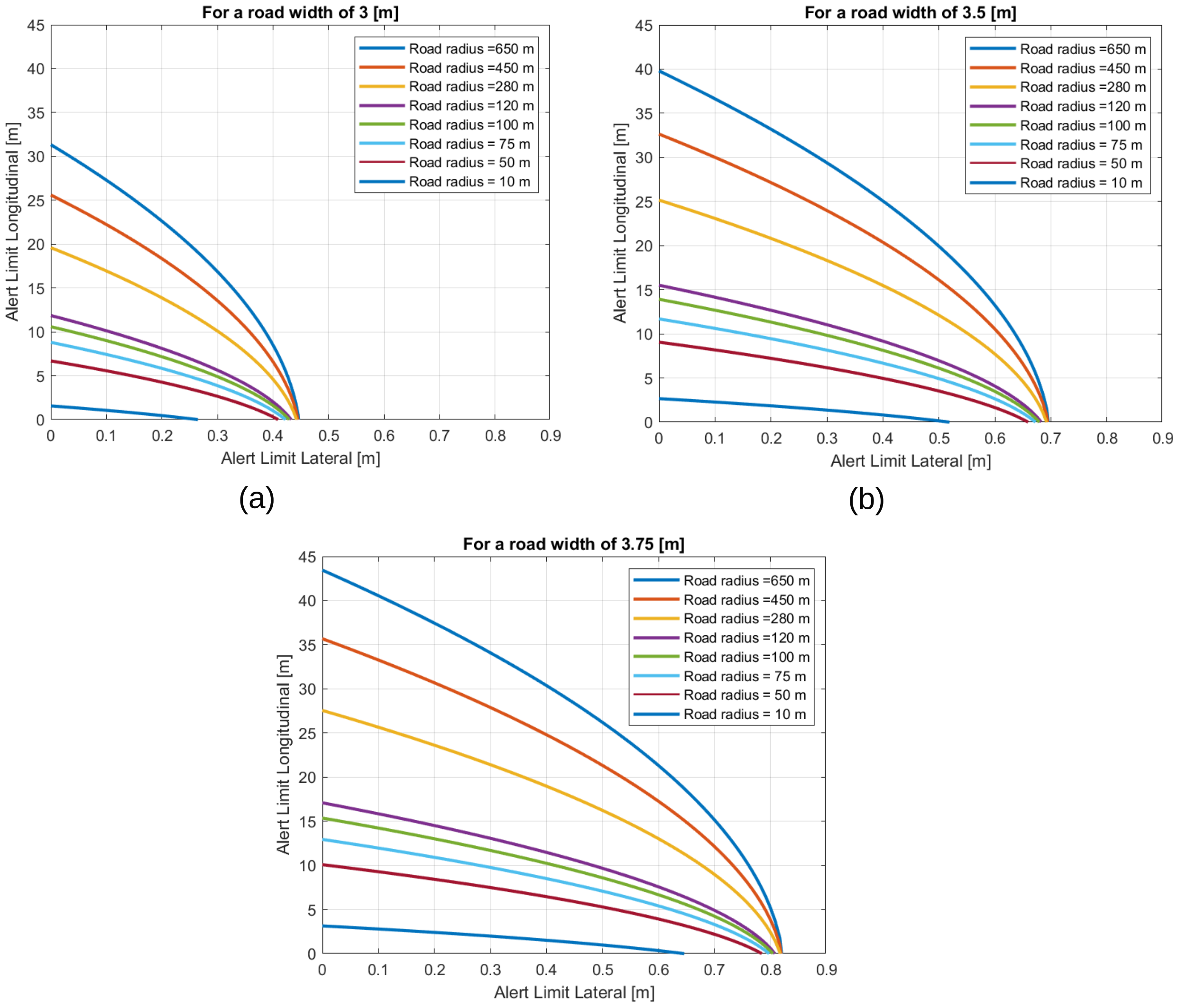
The curve radius of the road depends on the road type and might differ from country to country. Normally the minimum allowed radii for highways are in relation to the designed speed requirement of the road. Typical values for European highways are shown in the Table 13 below:

Table 13. Design speed vs. allowed minimum radii on European highways

Design Speed [km/h]	60	80	100	120	140
minimum radii at 7% crossfall [m]	120	240	450	650	1000

However the curve radii can go down to 10m for narrow roundabouts. To illustrate the impact of road geometry (curve radii and lane widths) more in detail, we have conducted a small sensitivity analyses. We used a standard vehicle length of 5.8m and width of 2.1m. The results can be seen in the

Figure 69 below.



(a)

(b)

(c)

Figure 69. Sensitivity analyses of the longitudinal and lateral alert limit coupling based on lane geometry and vehicle dimensions: the curve radii indicated by the different colours and are given in meters, the standard vehicle length is set to 5.8m and the width to 2.1m

As we can see the more stringent the requirements for the lateral alert limits are the more lose the longitudinal requirement can be.

Before crossings or traffic lights, the vehicle needs to stop at the stop/yield line before entering the next road segment. In Germany, this line is at least one meter before any crossing or traffic light. Hence, the maximum allowed longitudinal error in this situation is also one meter.

$$AL_{long,stop} = 1m$$

Taken all this into account, we can determine a longitudinal requirement for each road segment. The overall longitudinal alert limit is given as the minimum of all alert limits encounter during a particular road/path:

$$AL_{long} = \min\left(AL_{long,i}\right)$$

Depending on the road type/situation, vehicle dimension and previously determined lateral alert limit, we are now able to obtain the corresponding longitudinal alert limit. Similar to the lateral accuracy requirement, we can derive the longitudinal accuracy requirement for the nominal case such as:

$$k_1\sigma_{acc,long} \leq AL_{long} - DTE_{max,long}$$

Where k_1 is the Gaussian multiplier based on the allocated risk to the longitudinal Navigation System Error (NSE), which is here assumed to be the same as for the lateral NSE (1.5e-8), and therefore $k_1 = 5.66$.

Navigation accuracy is obtained as

$$Accuracy_{long} = k_2\sigma_{acc,long}$$

With k_2=2 (95% of the distribution).

5.2.2 Speed Requirement

As it has been stated already in D2.1 and D2.2, the speed accuracy requirement is defined by the EU/ UN ECE Regulation 39 (1958), retrieved 30 Jan 2015. It has direct impact on safety. It is formulated as follows:

- The indicated speed must never be less than the actual speed, i.e. it should not be possible to inadvertently speed because of an incorrect speedometer reading.
- The indicated speed must not be more than 110 percent of the true speed plus 4 km/h at specified test speeds. For example, at 80 km/h, the indicated speed must be no more than 92 km/h.

We denote the speed estimation error as $e_v = \hat{v} - v_{true}$, where is the estimated speed. Given the EU UN Regulation No. 39 - Rev.2 [32], we can state the following error requirements:

$$0 \leq e_v \leq \begin{array}{ll} 0.1v_{true} + 6\text{km/h} & \text{vehicles Cat. M und N} \\ 0.1v_{true} + 8\text{km/h} & \text{vehicles Cat. L}_3\text{, L}_4 \text{ and L}_5 \\ 0.1v_{true} + 4\text{km/h} & \text{vehicles Cat. L}_1 \text{ und L}_2 \end{array}$$

where the categories are summarized in the Table 14 below:

Table 14: Vehicle categories defined for EU

Category	Vehicle type
Category L	Mopeds, Motorcycles, Motor Tricycles and Quadricycles
Category M	Motor vehicles having at least four wheels and for the carriage of passengers
Category N	Power-driven vehicles having at least four wheels and for the carriage of goods

5.2.3 System Reaction Time Requirements

The system reaction time requirement for automated cars is defined by the maximum range distance of the relative distance sensor. In order to avoid collision a ‘safe distance’ between two vehicles needs to be ensured and this distance needs to be also covered by the relative distance sensor in the automated car. The Vienna Convention on Road Traffic defines a ‘safe distance’ as the distance such that a collision between vehicles can be avoided if the vehicle in front performs an emergency brake [33]. This distance is scenario dependent and it affected by Speed/ velocity of the automated car

- Car properties such as
- Quality of tires and their friction on the road
- Conditions of brakes
- Environment such as
- Inclination/slop of the road
- Weather conditions
- Reaction/detection time of the system to determine that emergency braking needs to be performed. This depends on the systems/control loop.

The safe distance can be represented by the sum of reaction distance and braking distance:

$$d_{\text{safe}} = d_{\text{react}} + d_{\text{brake}}$$

he *reaction distance* is the distance travelled before an emergency brake is enabled. This can be triggered by the driver or the automated system and can be determined assuming that the vehicle travels at a constant speed for a short time period by

$$d_{\text{react}} = v * t_{\text{reaction}}$$

where the velocity is denoted by v and the reaction or decision time is denoted by t_{reaction}. If a human driver is triggering this event, typical reaction times varies from 0.75s as far as 2.5s to represent reaction times from very elderly, debilitated, intoxicated, or distracted drivers.

The *braking distance* is the distance the car travels from the point when braking procedure is injected until the car stands still. It depends on the velocity and maximum deceleration the car is capable to achieve based on the given environment and car properties:

$$d_{\text{brake}} = \frac{v^2}{2a_{\max}} = \frac{v^2}{2\mu g},$$

where μ stands for the coefficient of friction between the road surface and the tires and g for the gravity of Earth, respectively. Please note that only for a level surface the deceleration is equivalent to the product of coefficient of friction and the gravity of Earth. The coefficient of friction may vary between 0.25 or lower on wet or frozen asphalt, and 0.9 or higher if anti-skid brakes and season specific performance tires may be used to compensate for driver error and conditions. A typical value to be used is $\mu = 0.7$. For a comparison, the safe distances between two vehicles depending on the velocity and different friction coefficients are depicted in Figure 70 for a reaction time of 1.5s.

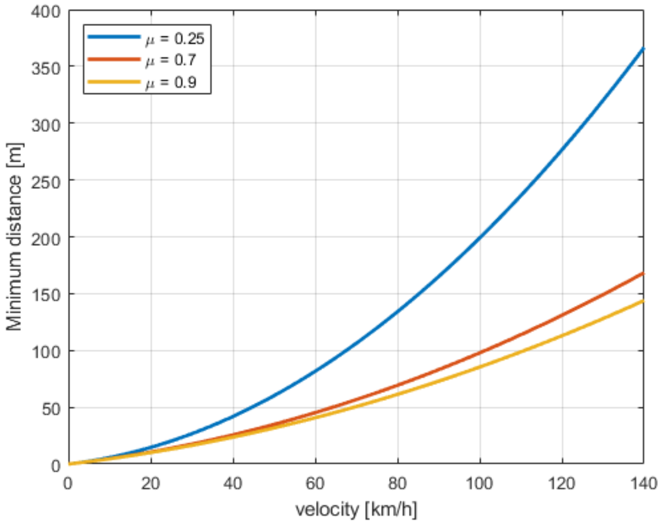


Figure 70. Safe distances between two vehicles depending on the last vehicle's velocity for a reaction time of 1.5s and three different friction coefficients

The most common commercial LIDAR sensors can fulfil detection range of 100 meters with accuracy no worse than 10 [cm], according to the investigation [34]. Based on this value, we can derive the maximum system reaction time of the control loop of the automated car and which ensures that the safe distance is still hold:

$$d_{max} \geq d_{\text{safe}}$$

$$d_{max} \geq v * t_{\text{reaction}} + \frac{v^2}{2\mu g}$$

The minimum reaction time is determined by the maximum allowed speed on the road segment:

$$AL_{time} = \frac{d_{max}}{v_{max}} - \frac{v_{max}}{2\mu g}$$

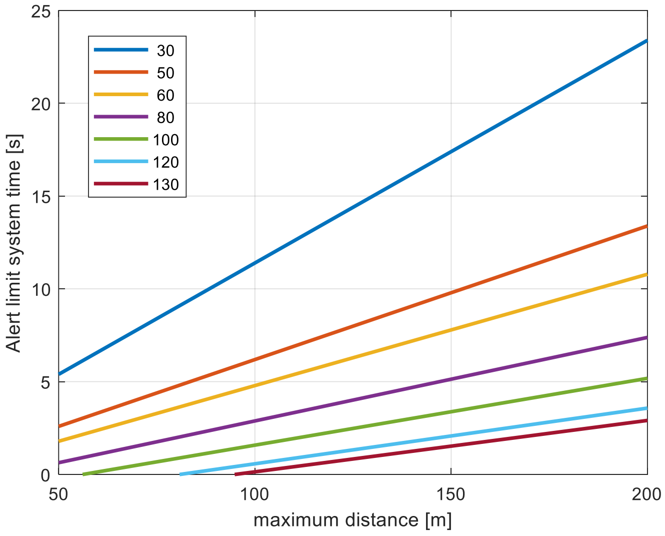


Figure 71. Alert limit of system reaction time depending on maximum allowed velocity and maximum range distance

5.2.4 Data Rate Requirements on Self-Driving Cars

The sampling frequency of the sensor measurements has impacts on the safety aspect of automated driving systems. As shown in Figure 72, the sensor has a constant sampling rate f_{sample}. A hazardous event may happen between two consecutive sensor measurements. The risk can only be detected after the next upcoming measurement is taken. Denote the processing time to detect the hazardous event as t_{proc}, which depends on the processing hardware as well as the monitoring methods. The reaction time is the summation of the processing time and the duration from the hazardous event happens till the following sensor measurement is taken. Then the proper action, e.g., emergency brake can be executed.

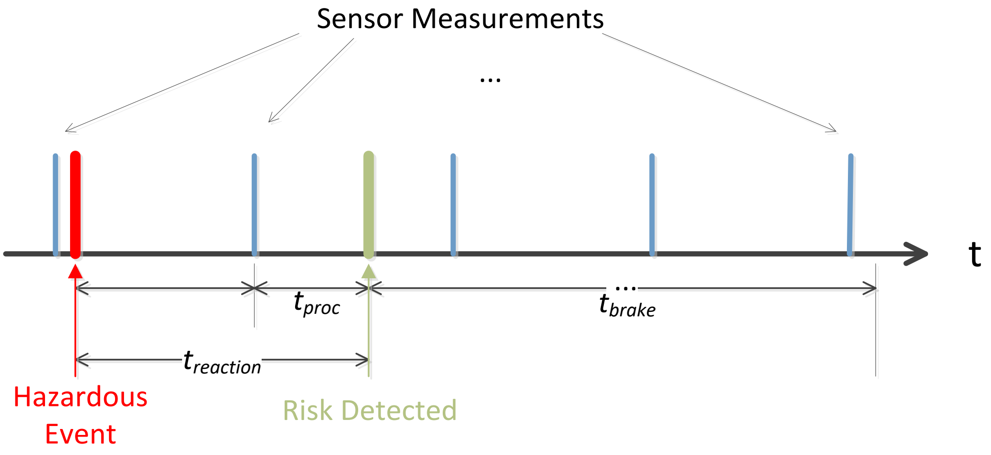


Figure 72. Data rate requirement

In the worst-case scenario, the hazardous event may happen immediately after a nominal measurement. The sampling frequency of the sensor should ensure that the sampling time satisfies $t_{sample} + t_{proc} \leq t_{rea,max}$, where $t_{rea,max}$ is the maximum allowed reaction time. As a result, the main sensors that detect the hazardous events must have a sampling frequency no smaller than

$$f_{sample} \geq \left(t_{rea,max} - t_{proc}\right)^{-1}.$$

The time to alert of the localization system should be shorter than the maximum allowed reaction time. As a result, we can bound the sampling time using the TTA., we can state $t_{sample} + t_{proc} \leq TTA$ [s].

5.2.5 Continuity and Availability

Based on the GSA Report on “Road User Needs and Requirements” [35], we can recall the following numbers for availability and continuity:

- The availability defined as the percentage of time the position, navigation or timing solution can be computed by the user, is supposed to be better than 99,5%.
- Continuity is the ability to provide the required performance during an operation without interruption once the operation has started. The continuity requirement for automated car driving is set to high.

The above derived requirements related to car position determination are summarized in Table 15.

Table 15. Summary of derived requirements for car position determination

Operational scenario Requirement	Automated driving on highway; velocity 80-130 km/hr	Automated driving on local roads; velocity 60-90 km/ hr	Automated driving on narrow and curved roads; velocity 20-60 km/ hr
Safety Integrity	Very high (ASIL D)		
Considered lane width (W_{lane})	3.5-3.75 m	3.5 m	3 m
Lane Alert Limit[1]	91cm	91cm	91cm
Lane Accuracy[2]	33cm	33cm	33cm
Lateral Alert Limit[3]	50-60cm	50cm	25cm
Lateral Accuracy[4]	17.67-21.2cm	17.67cm	8.83cm
Minimum Road Radius	240m	120m	10m
Longitudinal Alert Limit based on curve[5]	11m - 11.84m	6.96m	10.67cm
Longitudinal Alert Limit based on crossing	1m		
Longitudinal Accuracy[6]	35.34cm	35.34cm	3.89cm
Speed	• indicated speed must never be less than the actual speed • indicated speed must not be more than 110 percent of the true speed plus 4 km/h at specified test speeds		
System Reaction Time[7]	0.14s	2.18s	4.79s
Data Rate Requirement	≤1s	≤1s	≤1s
TTA Requirement [35]	1s	1s	1s
Continuity	high		
Availability	better than 99.5%; it will be clarified during WP3		
Security	very high		
Notes	Integrity of vertical position required to confirm road level on multilevel crossing		
Requirement Code	UR_004	UR_005	UR_006

[1] For minimum vehicle width of 1.72m and lane mark width of 10cm

[2] Accuracy is defined a 2 sigma and IR of 3e-8/hr

[3] For a minimum vehicle width of 1.72m and maximum lateral DTE of 0.2m

[4] Accuracy is defined a 2 sigma and integrity risk a 1.5e8/hr

[5] For a minimum vehicle width of 1.72 and length 5.8m

[6] Based an the total longitudinal Alert Limit and with accuracy is defined a 2 sigma and integrity risk a 1.5e8/hr

[7] For a maximum distance measurement of 100m, friction coefficient of 0.7

5.2.6 Automotive System Requirements

This section contains specification of the Automotive System Requirements for HELMET solution derived from User Requirements Specification contained in the HELMET D2.1 deliverable and also using detailed analysis performed in Section 5.2. of this document.

The AUTO System Requirements are specified in the format **SR-SSR-TTT-N.a** with the codes SSR and TTT explained in Table 11 and Table 12 at the beginning of Section 5.

Note: Sequence numbers in the range of 101-200 were allocated to AUTO system requirements.

ID	**Name**	**Description**
SR-OBU-SAF-101.a	Automotive Safety Integrity Level (ASIL) for car position determination.	This requirement defines ASIL D (ISO 26262) for car position determination.
Rationale		
ASIL D for car position determination/ localization results from the safety analyses performed in HELMET D2.3, Section 4, where allocated Probability of Failure to car localization function (PF_{LOC} of 3e-8/ h) corresponds to ASIL D according to ISO 26262.		
Notes		
References		
HELMET User requirements UR_004, UR_005, UR_006; Section 4 in HELMET D2.3.		

ID	**Name**	**Description**
SR-OBU-SAF-102.a	Alert Limit (lateral) for automated driving on highway.	This requirement defines Alert Limit (lateral) < 75 cm for automated driving on highway.
Rationale		
This requirement results from the analysis of the operational scenarios performed in the HELMET D2.1 [1] Section 3.2. It is defined within the HELMET User Requirement UR_004.		
Notes		
References		
HELMET deliverable D2.1, Section 3.2 and Section 4.		

ID	**Name**	**Description**
SR-OBU-PER-103.a	Accuracy (2*sigma) of position determination related to automated driving on highway.	This requirement defines Accuracy (2*sigma) of position determination of 34 cm (lateral) related to automated driving on highway.
Rationale		
This requirement results from the analysis of the operational scenarios performed in the HELMET D2.1 [1], Section 3.2. It is defined within the HELMET User Requirement UR_004.		
Notes		
References		
HELMET D2.1 [1], Section 3.2 and Section 4.		

ID	**Name**	**Description**
SR-OBU-SAF-104.a	Alert Limit (lateral) for automated driving on local roads.	This requirement defines Alert Limit (lateral) < 45 cm for automated driving on local roads.
Rationale		
This requirement results from the analysis of the operational scenarios performed in the HELMET deliverable D2.1, Section 3.2. It is defined within the HELMET User Requirement UR_005.		
Notes		
References		
HELMET deliverable D2.1 [1], Section 3.2 and Section 4.		

ID	**Name**	**Description**
SR-OBU-PER-105.a	Accuracy (2*sigma) of position determination related to driving on local roads.	This requirement defines Accuracy (2*sigma) of position determination of 20 cm (lateral) related to driving on local roads.
Rationale		
This requirement results from the analysis of the operational scenarios performed in the HELMET deliverable D2.1 [1], Section 3.2. It is defined within the HELMET User Requirement UR_005.		
Notes		
References		
HELMET D2.1 [1], Section 3.2 and Section 4.		

ID	Name	Description
SR-OBU-SAF-106.a	Alert Limit (lateral) for automated driving on narrow and curved roads.	This requirement defines Alert Limit (lateral) < 45 cm for automated driving on narrow and curved roads.
Rationale		
This requirement results from the analysis of the operational scenarios performed in the HELMET deliverable D2.1, Section 3.2. It is defined within the HELMET User Requirement UR_006.		
Notes		
References		
HELMET D2.1 [1], Section 3.2 and Section 4.		

ID	Name	Description
SR-OBU-PER-107.a	Accuracy (2*sigma) of position determination related to driving on narrow and curved roads.	This requirement defines Accuracy (2*sigma) of position determination of 9 cm (lateral) related to driving on narrow and curved roads.
Rationale		
This requirement results from the analysis of the operational scenarios performed in the HELMET deliverable D2.1, Section 3.2. It is defined within the HELMET User Requirement UR_006.		
Notes		
References		
HELMET D2.1 [1], Section 3.2 and Section 4.		

ID	Name	Description
SR-OBU-SAF-108.a	Time-to-Alert.	This requirement defines Time-to-Alert (TTA) < 1 second for all automated car driving scenarios.
Rationale		
This requirement is an outcome of the GNSS User Consultation Platform / Report on Road User Needs and Requirements, 01/07/2019. At this moment the TTA value is just estimation. Nevertheless, the same value is also required for SDT (Safe Down Time) that represent an important parameter of railway safety related systems. The TTA value will be clarified within the HELMET architecture design.		
Notes		
References		
HELMET D2.1 [1], Section 4, User Requirements UR_004, UR_005, UR_006.		

ID	Name	Description
SR-OBU-FUN-109.a	Timing Accuracy.	This requirement defines Timing Accuracy < 1 μs.
Rationale		
This requirement is an outcome of the GNSS User Consultation Platform / Report on Road User Needs and Requirements, 01/07/2019. At this moment the Timing Accuracy value is just estimation. It is assumed this value is required for time synchronization of on-board equipment. The Timing Accuracy value will be clarified within the HELMET architecture design.		
Notes		
References		
HELMET deliverable D2.1 [1], Section 4, User Requirements UR_004, UR_005, UR_006.		

ID	Name	Description
SR-OBU-SAF-110.a	Availability of car localization.	This requirement defines Availability of car position determination/ localization as a High.
Rationale		
This requirement is an outcome of the GNSS User Consultation Platform / Report on Road User Needs and Requirements, 01/07/2019. At this moment the Availability is specified qualitatively. In case of automated car driving Availability can have direct impact on safety of the Virtual driver System. The requirement on Availability will be clarified later during the HELMET architecture design.		
Notes		
References		
HELMET deliverable D2.1 [1], Section 4, User Requirements UR_004, UR_005, UR_006.		

ID	Name	Description
SR-OBU-SEC-111.a	Security of car localization.	This requirement defines Security of car localization as Very high.
Rationale		
This requirement is an outcome of the GNSS User Consultation Platform / Report on Road User Needs and Requirements, 01/07/2019. At this moment Security of car localization is specified qualitatively. It is evident that Security has a direct impact on safety of cad position determination and automated driving. Note: The IT security must be treated similarly as safety guards protecting against systematic hazard causes and faults. Probabilistic evaluation of IT security threats is considered infeasible. The safety aspects of electronic HW and systems are covered by EN 50129 and security issues are taken into account by EN 50129 as far as they affect safety issues. This approach combined with IEC 62443 recommendation will be applied in HELMET solutions – preservation of RAMS attributes of HELMET solutions against potential security threats. Security provisions will be discussed during the HELMET architecture design.		
Notes		
References		
HELMET deliverable D2.1 [1], Section 4, User Requirements UR_004, UR_005, UR_006.		

ID	Name	Description
SR-OBU-SAF-112.a	Speed accuracy	This requirement defines Speed accuracy as follows: • The indicated speed must never be less than the actual speed, i.e. it should not be possible to inadvertently speed because of an incorrect speedometer reading. • The indicated speed must not be more than 110 percent of the true speed plus 4 km/h at specified test speeds. For example, at 80 km/h, the indicated speed must be no more than 92 km/h.
Rationale		
This requirement is defined by the EU/ UN ECE Regulation 39 (1958), retrieved 30 Jan 2015. It has direct impact on safety. The requirement will be clarified during the HELMET architecture design.		
Notes		
References		
HELMET deliverable D2.1 [1], Section 4, User Requirement UR_008.		

ID	Name	Description
SR-OBU-SAF-113.a	Harmonized Design Target for SDC safety systems	This requirement defines Harmonized Design Target for SDC safety systems as a Probability of Failure PF_{SYS} of 1e-7/ h.
Rationale		
The whole procedure regarding derivation of high-level safety target for self-driving cars is described in the HELMET deliverable D2.3, Section 4.2.1. Derivation of the safety target is based on harmonized risk acceptance approaches used in railway and aviation sectors.		
Notes		
References		
HELMET D2.3, Section 4.		

ID	Name	Description
SR-OBU-SAF-114.a	Probability of Failure of car localization	This requirement defines Probability of Failure of car localization as PF_{LOC} of 3e-8/ h
Rationale		
The PF_{SYS} of 1e-7/ h allocation to PF_{LOC} of 3e-8/ h is described in HELMET deliverable D2.3, Section 4.		
Notes		
References		
HELMET D2.3, Section 4.		

ID	Name	Description
SR-COM-SAF-115.a	Probability of Failure of Communications used for car localization from the Control Centre to the OBU	This requirement defines Probability of Failure of Communications used for car localization $PF_{COM} < 1e-9/ h$.
Rationale		
In case of GNSS augmentation used for aviation Terminal and CAT I operations it is assumed that the Integrity risk related to VHF Date broadcast < 1e-9/ h. In case of ERTMS THR related to message corruption is about 1e-11/ h. It means that the value $PF_{COM} < 1e-9/ h$ is realistic.		
Notes		
References		
HELMET D2.3, Section 4.		

ID	Name	Description
SR-OBU-SAF-116.a	Alert Limit (lane) for automated driving	This requirement defines the maximum allowed error associated with the lane identification
Rationale		
For minimum vehicle width of 1.72m and lane mark width of 10cm, this values might be 91cm		
Notes		
References		
HELMET D2.3 Section 5.2		

ID	Name	Description
SR-OBU-PER-108.a	Accuracy (2*sigma) of lane identification	This requirement defines the two sigma accuracy associated with the lane identification
Rationale		
For an integrity risk of 3e-8/hr associated with this error, the accuracy might be 33cm		
Notes		
References		
HELMET D2.3 Section 5.2		

ID	Name	Description
SR-OBU-SAF-117.a	Alert Limit (longitudinal) for automated driving on highway	This requirement defines the maximum allowed error for automated driving on highway
Rationale		
For a minimum vehicle width of 1.72 and length 5.8m, minimum radii of 280m and lane width of 3.75 and 3.5m, respectively. The longitudinal AL associated to curves could be 11m - 11.84m and for approaching crossings 1m. The total longitudinal AL is 1 m.		
Notes		
References		
HELMET D2.3 Section 5.2		

ID	Name	Description
SR-OBU-PER-108.a	Accuracy (2*sigma, longitudinal) of position determination related to driving on highway	This requirement defines the longitudinal Accuracy in terms of two sigma value of position determination related to driving on highway
Rationale		
The two sigma accuracy, related to the SR-OBU-SAF-117.a for an Integrity Risk of 1.5e8/hr, is 35.34 cm.		
Notes		
References		
HELMET D2.3 Section 5.2		

ID	Name	Description
SR-OBU-PER-109.a	System Reaction Time related to driving on highway	This requirement defines the maximum system reaction time related to driving on highway
Rationale		
For a maximum distance measurement of 100m, friction coefficient of 0.7, the maximum allowed system reaction time is 0.14s		
Notes		
References		
HELMET D2.3 Section 5.2		

ID	Name	Description
SR-OBU-SAF-118.a	Alert Limit (longitudinal) for automated driving on local roads	This requirement defines the maximum allowed error for automated driving on local roads
Rationale		
For a minimum vehicle width of 1.72 and length 5.8m, minimum radii of 120m and lane width of 3.5m, respectively. The longitudinal AL associated to curves could be 6.96m and for approaching crossings 1m. The total longitudinal AL is 1 m.		
Notes		
References		
HELMET D2.3 Section 5.2		

ID	Name	Description
SR-OBU-PER-110.a	Accuracy (2*sigma, longitudinal) of position determination related to driving on local roads	This requirement defines the longitudinal Accuracy in terms of two sigma value of position determination related to driving on local roads
Rationale		
The two sigma accuracy, related to the SR-OBU-SAF-118.a for an Integrity Risk of 1.5e8/hr, is 35.34 cm.		
Notes		
References		
HELMET D2.3 Section 5.2		

ID	Name	Description
SR-OBU-PER-111.a	System Reaction Time related to driving on local roads	This requirement defines the maximum system reaction time related to driving on local roads
Rationale		
For a maximum distance measurement of 100m, friction coefficient of 0.7, the maximum allowed system reaction time is 2.18s		
Notes		
References		
HELMET D2.3 Section 5.2		

ID	Name	Description
SR-OBU-SAF-119.a	Alert Limit (longitudinal) for automated driving on narrow and curved roads	This requirement defines the maximum allowed error for automated driving on narrow and curved roads
Rationale		
For a minimum vehicle width of 1.72 and length 5.8m, minimum radii of 10m and lane width of 3m, respectively. The longitudinal AL associated to curves could be 10.67cm and for approaching crossings 1m. The total longitudinal AL is 11 cm.		
Notes		
References		
HELMET D2.3 Section 5.2		

ID	Name	Description
SR-OBU-PER-112.a	Accuracy (2*sigma, longitudinal) of position determination related to driving on narrow and curved roads	This requirement defines the longitudinal Accuracy in terms of two sigma value of position determination related to driving on narrow and curved roads
Rationale		
The two sigma accuracy, related to the SR-OBU-SAF-119.a for an Integrity Risk of 1.5e8/hr, is 3.77 cm.		
Notes		
References		
HELMET D2.3 Section 5.2		

ID	Name	Description
SR-OBU-PER-113.a	System Reaction Time related to driving on narrow and curved roads	This requirement defines the maximum system reaction time related to driving on narrow and curved roads
Rationale		
For a maximum distance measurement of 100m, friction coefficient of 0.7, the maximum allowed system reaction time is 4.79s		
Notes		
References		
HELMET D2.3 Section 5.2		

ID	Name	Description
SR-COM-SAF-120.a	Continuity of car localization	This requirement defines the ability to provide the required performance during an operation without interruption once the operation has started.
Rationale		
This requirement is an outcome of the GNSS User Consultation Platform / Report on Road User Needs and Requirements, 01/07/2019. The continuity requirement for automated car driving is set to high.		
Notes		
References		
HELMET D2.3 Section 5.2		

5.3 UAV: UAS/ RPAS-PIT STATION SEGMENT SYSTEM REQUIREMENTS

The following Tables summarize the UAS/RPAS-PIT STATION Segment Requirements which comprise the Operational, Functional, Performance, Interface, Security, Safety, and Verification Requirements necessary to explore the UAS/RPAS-PIT STATION Segment Preliminary Design and its related detailed Specification. The present requirements are based on the HEMET D2.1 and D2.2 Documentation.

The UAS system requirements are specified in the format **UAS-SR-SSR-TTT-N.a** with the codes SSR and TTT explained in Table 11 and Table 12 at the beginning of Section 5.

UAS/RPAS-PIT STATION INTEGRATED SYSTEM-Operational Requirements (OPE)

Req. ID	Requirement Description	Remarks/Explanatory Notes
UAS-SYS-OPE-REQ-01	The UAS/RPAS-PIT shall support all and/or selected Rail and Automotive Assets by providing, Monitoring and Traffic Management (IMTM) operational services in scenarios related to Open Sky, Restricted Regional/Sub-Urban, and Urban Local Operational Environments. All Operational Modes shall be in accordance with D2.2 HELMET CONOPS Document, section 3.3. As such the UAS/RPAS-PIT Station Highly Integrated System Network Segment within the HELMET infrastructure shall be composed of the following main four (4) Physical Operational Elements, namely: 1) The Operating UAS/RPAS Element shall encompass the Unmanned Aircraft (UA)/Remotely Piloted Aircraft (RPA) in a specific Configuration and Remote Pilot Stations (RPS) operating in LOS and/or BLOS mode by means of a Control and Non-Payload Communications (CNPC) Link (UP and DOWN Data and Voice Link) and Navigation Aid Components utilizing for this purpose a Terrestrial and/or Satellite based Network for Command, Control, Communications, Sense and Avoid (or Detect and Avoid) services covering all appropriate UTM airspace classes for railway and automotive related assets , in all integration cases and flight phases. This element shall include the operational services and capabilities provided by each PIT Station system but from this is excluded the UAS/RPAS Logistic Support element. 2) The UAS/RPAS dedicated PIT Integrated Logistic Support (ILS) Element: which shall guarantee UAS/RPAS supportability, operational availability and safety throughout its Operational Life-Cycle. 3) The HELMET Augmentation Network Element dedicated to UAS/RPAS Ground and Aerial Operations this shall encompass the physical connectivity of the UAS/RPAS Navigation subsystem with the GNSS Galileo and potential Augmentation Services by the HELMET multi-modal Augmentation and Integrity Monitoring Network. 4) Communication Network infrastructure: intended all the links that connect the various components of the systems: - UAV/PIT station - PIT station/GCS (Ground Control System) - Helmet core centre/PIT station/Operator Centre - Operator Centre/UTM Centre	

UAS-SYS-OPE-REQ-02	The Operational Characteristics of the UAS/RPAS shall be those of ≤25kg Max.Take-off Mass (MTOM) under the EASA Categories Specific and Certified and under the Operational Scenarios in accordance with the D2.2 CONOPS Document, subsection 3.3.7.1	The Physical and Functional Characteristics of the UAs to be used in the HELMET Project are shown in Table 9 of Doc. D2.2 CONOPS and specifically the Multi-Rotor, Single Rotor and Hybrid Types since they are compatible with the PIT-Station Configuration and Capabilities.
UAS-SYS-OPE-REQ-03	A series of PIT station deployed all along the service areas shall provide support to all Aerial Operation and mission Profile of the UAV/RPAS	
UAS-SYS-OPE-REQ-04	The integration of UAS/RPAS shall not imply a significant impact on the current users of the airspace.	
UAS-SYS-OPE-REQ-05	The UAS/RPAS-PIT shall cover all Very Low Level (VLL) airspace UTM classes and all integration cases in accordance with the EASA Regulations of Very low level (VLL) operations (alias non-standard VFR or IFR operations) below the typical IFR and VFR altitudes for manned aviation and shall not exceed 400 ft. Above Ground Level (AGL).	
UAS-SYS-OPE-REQ-06	The UAS/RPAS-PIT operations shall comply with existing and future Civil Aviation Regulations and Procedures including those dedicated to UTM	
UAS-SYS-OPE-REQ-07	The UAS/RPAS-PIT integration shall not compromise existing aviation safety levels, nor increase risk: the way UAS/RPAS operations are conducted shall be equivalent to manned aircraft, as much as possible;	
UAS-SYS-OPE-REQ-08	The UAS/RPAS shall comply with the SESAR trajectory management process	
UAS-SYS-OPE-REQ-09	The UAS/RPAS shall be able to comply with ATM/UTM air traffic control rules/procedures	
UAS-SYS-OPE-REQ-010	The UAS/RPAS shall comply with the capability requirements applicable to the UTM airspace within which they shall to operate.	
UAS-SYS-OPE-REQ-011	During operations if the UA/RPA loses communications or loses its GNSS NAV signal or both (CNPC Link Failure), then it shall be capable to return to a predetermined location within the planned operating area and land on the closest PIT-Station.	

UAS-SYS-OPE-REQ-012	The UAS/RPAS shall be capable to operate in the following operational modes in accordance with EASA Rules, as follows: a) Visual line of Sight (VLOS) in a range not greater than 500 meters from the remote pilot, in which the remote pilot maintains direct unaided visual contact with the UA/RPA; b) Extended Visual Line of Sight (EVLOS) where, beyond 500 meters, the pilot is supported by one or more observers or other means, in which the crew maintains direct unaided visual contact with the UA/RPA; The PIT-Station shall be capable of supporting an EVLOS operation(s) including the planned trajectory. c) Beyond VLOS (BVLOS) and Beyond Radio Line of Sight (BRLOS) where the operations are also below 400 ft. The BRLOS mode shall require additional technological support such as an appropriate Satellite CNPC Link and Band(s). The system in both BVLOS and BRLOS shall also require some means of Detect and Avoid (DAA) or Sense and Avoid (SAA).	1)The key capability of 'detect and avoid' (DAA) is required in relation to cooperative and non-cooperative nearby traffic (otherwise specific procedures and restrictions shall apply). 2) For the forth seen employment of small UAS/RPAS for the IMTM operations within the HELMET environment, the modes VLOS, E-VLOS and BVLOS/BRLOS shall require (apart the DAA) some type of safety technologies and the possibility for Redundant CNPC Link (which includes NAVAIDS).
UAS-SYS-OPE-REQ-013	The Communications satellite component within the architecture shall cover all flight phases at least in BRLOS operations utilizing the PIT-Station as a Relay between the satellite and UA/RPA systems or between UA/RPA and Ground Control Station(s) .Such satellite system architecture shall cover all ECAC Member States and it shall support the Command and Control, ATC relay, Sense and avoid communication flows.	
UAS-SYS-OPE-REQ-015	For BRLOS Operations the Communications Satellite Spectrum Requirements shall be in line with Methodology 2, ITU -R M.2171	
UAS-SYS-OPE-REQ-017	The UAS/RPAS-PIT Station shall automatically handle satellite to terrestrial and terrestrial to satellite link handovers in the forward and return links.	Via PIT station
UAS-SYS-OPE-REQ-018	The UAS/RPAS system shall be adaptive to changes in the conditions of the command and control link. The system shall be able to implement ACM and spectrum management techniques.	
UAS-SYS-OPE-REQ-019	The PIT Station in terms of Satellite Communication and GNSS services within the HELMET System shall be capable of serving a heterogeneous population of UAS/RPAS with different constraints on power, high power amplifier, terminal and antenna accommodation.	
UAS-SYS-OPE-REQ-020	The PIT Station shall be capable of changing the required service on the flight as requested by the users according to their operational needs.	
UAS-SYS-OPE-REQ-021	The UAS/RPAS-PIT Station Segment shall be capable of supporting multiple users (Rail and Automotive) simultaneously making an efficient use of the available resources.	

UAS-SYS-OPE-REQ-022	The UAV/RPAS characteristics shall reduce to maximum the likelihood that during operations in the prospected mission scenarios will allow the injury of people, damages to property or damages to another aircraft and/or vehicles.	For example the use of a ballistic parachute maybe one of the solutions for not damaging property or injuring people during impact. On the other hand the use of some type of DAA or vicinity alert sensors may satisfy the requirement of impacting other aerial or terrestrial moving systems.
UAS-SYS-OPE-REQ-023	When the UAV/RPAS system operates at the proximity to aerodromes or restricted/segregated airspace shall not increase the likelihood of a collision with other airspace or ground users and their assets.	
UAS-SYS-OPE-REQ-024	Operations in or over populated or congested areas shall not increase the likelihood of injury to persons and loss of control due to frequency interference, loss of GNSS signal or other factors.	
UAS-SYS-OPE-REQ-025	Operating altitudes and/or airspace classification shall not influence the likelihood of a collision with other airspace users.	
UAS-SYS-OPE-REQ-026	Complex pilot and PIT Station tasks or complex operating environments shall not increase the likelihood of an incident or accident.	
UAS-SYS-OPE-REQ-027	The UAS/RPAS-PIT Station System shall be capable of conforming to all air traffic rules and communication protocols with the UTM System when the operation is in the UTM jurisdiction.	
UAS-SYS-OPE-REQ-028	The UAS/RPAS-PIT Station shall be dedicated to the following Inspection, Monitoring and Traffic Management (IMTM) (Ref. to OPE-REQ-01) operational tasks and specific applications for: a) Structural monitoring, especially for critical assets like bridges and tunnels, and for fault detection (i.e. diagnostics/prognostics). b) Environmental security monitoring such as assessments of fire, explosions, earthquakes, floods and landslides along the railway, road and highway tracks/lanes informing the User on the real time status. c) Physical security monitoring of high value rail and automotive infrastructural assets. Detection of intrusions, objects stolen or moved, graffiti, etc. d) Safety monitoring, e.g., to early detect failures on all elements/devices or obstacles on the rail and/or road tracks. e) Situation assessment and emergency/crisis management. To monitor accident scenarios and coordinate the intervention of first responders. f) Supporting the Design, Development, and Construction of new Railway/Road/Highways by providing Mapping and Survey Data.	

	g) Support Performance Diagnostics and Operational Tests of other Integrated Systems and Services (e.g. Satellite Based Augmentation System (SBAS) Services for improving the accuracy, integrity and availability of basic GNSS signals). h) Monitor the rail and automotive routine operations and provide accurate traffic (including emergencies) management to both users. i) Provide safety and security information while monitoring rail and automotive operations. j) Support Law Enforcement and Patrol Units Operations for both railway and automotive segments. k) Provide real time and/or near real time operational support under emergency traffic conditions for both rail and automotive users. l) Provide Wi-Fi connectivity (especially during emergency operations) as required.	
UAS-SYS-OPE-REQ-029	The dedicated use of the UAS/RPAS-PIT Station Highly Integrated System Network within the HELMET infrastructure shall provide to the Users with the following overall benefits: 1) Overall Reduction of risk to staff and people and increase of infrastructural assets safety 2) Reduced planning cycles (Scheduled and Non-Scheduled) 3) Enhancement of the work process efficiency in IMTM services 4) Enhancement of flexibility, affordability of verification tooling 5) Higher quality data available in larger quantities at lower costs	
UAS-SYS-OPE-REQ-030	For the specific Inspection, Monitoring and Traffic Management (IMTM) operations, the employed UAS/RPAS shall be compliant to all relative Rules of the Air Requirements as being imposed by EASA Regulations by UAS/RPAS Category.	For the IMTM UAS/RPAS HELMET Project it will be assumed the use of EASA UAS/RPAS Specific and Certified Categories.
UAS-SYS-OPE-REQ-031	The IMTM UAS/RPAS for railway and road applications shall be expected to operate within a range of operational constraints as per D2.2 subsection 3.3.2, which shall be used in the detailed architectural design of the segment. Such constraints shall be in the following issues: 1) Geofencing 2) Weather 3) Hours of Operation 4) Remote Operation Range 5) Endurance 6) UA/RPA Weight and Size 7) Operational Altitude	

	8) Security 9) Noise 10) Privacy 11) Human proximity 12) Human Factors 13) Physical and Operational Safety	
UAS-SYS-OPE-REQ-032	The entire operational UAS/RPAS-PIT Station Scenarios shall involve the following Framework Components for all Railway and Road IMTM Applications, as per D2.2 subsection 3.3.4: 1) Operational Framework Definition, 2) Flight Planning, 3) Flight Implementation, 4) Data Acquisition, 5) Data Processing and Analysis, 6) Data Interpretation and 7) Optimized Traffic Application.	
UAS-SYS-OPE-REQ-033	The following typical Flight Operative Modes shall be Applicable to IMTM UAS/RPAS Operations in accordance with D2.2 subsection 3.3.6: a) Manual Mode b) Assisted Mode c) IOC (Intelligent Orientation Control) d) Auto (Waypoint Navigation) e) Fail Safe Mode	1) The SW integration level of the UA/RPA and the pilot's workload is intended on a qualitative scale of five values: None, Low, Medium, High, Very High. 2) The failsafe operating mode, when is automatically driven through the on-board software, forces the aircraft to implement autonomously one of the following procedures: a) Return-to-Home: Failsafe RTH is activated automatically if the remote C2 signal is lost for more than 3 seconds provided that the Home Point has been successfully recorded and the compass is working normally. The pilot can interrupt (override) the Return-To-Home procedure and regain full control of the aircraft if the remote controller signal is recovered. b) Auto-Landing: Failsafe auto landing is activated automatically if the remote controller

		signal (including video relay signal) is lost for more than 3 seconds and there’s no sufficient GNSS signal for RTH procedure.
UAS-SYS-OPE-REQ-034	In defining the details of the Detailed Physical and Functional UAS/RPAS-PIT Station Segment Architecture shall be considered but not limited to the Operational Scenarios found in D2.2 subsection 3.3.7	
UAS-SYS-OPE-REQ-035	All UA/RPA should always be entirely confined within the pre-defined area of IMTM operations . This shall be achieved either through the PIT STATION/GCS technology or operational limitations such as flying in an enclosed area such the UTM geo-fenced flight operations regulated areas.	
UAS-SYS-OPE-REQ-036	UAS/RPAS-PIT STATION network Maintenance operations shall include the accomplishment of scheduled and unscheduled servicing and inspection tasks to ensure continuing UAS/RPAS airworthiness and Operational Availability of the PIT STATION network. The Operator should have a system of assessment e.g. through reliability programme, to support the continuing airworthiness of UAS/RPAS and the operational availability of the PIT STATION network and to provide a continuous analysis of the effectiveness of the maintenance programme in use.	
UAS-SYS-OPE-REQ-037	The UAS/RPAS Operator should plan all routes (for normal IMTM and Emergency Operations) to a level consistent with aviation safe operations. Considerations should be made based on the accuracy of the UA/RPA flight control and navigation system or the accuracy of the UAS/RPAS’ DAA system, whichever is less precise.	
UAS-SYS-OPE-REQ-038	All landing areas (PIT STATION Network and/or alternative areas), including emergency landing areas (PIT or other designated areas), should allow the recovery of the UA/RPA in an expeditious manner with adequate considerations made to safety and security requirements.	The Operator will have the responsibility to identify landing areas for emergency recovery. If applicable, the emergency landing areas may be located within the trajectory limits of the UAS/RPAS and at a safe distance from areas with human traffic.
UAS-SYS-OPE-REQ-039	The Operator shall ensure that all geographical (air navigation maps within the UTM Authority) data necessary for navigation, including for the purpose of situational awareness and detect and avoid, are updated for all IMTM operations. All map data should be accurate to a level sufficient for the safe operations of the system (to include ground fixtures and temporary erected structures if necessary, beyond the PIT STATION network capabilities).	

UAS-SYS-OPE-REQ-040	All software and firmware deployed on the UAS/RPAS-PIT STATION network should be functional in all phases of flight and IMTM operational envelops. Verifications can be made through analysis or testing with special attention given to functionalities which are operationally critical or in which their failure will lead to hazardous or catastrophic failure conditions.	

UAS/RPAS SUB-SEGMENT-Functional Requirements (FUN)		
Req. ID	**Requirement Description**	**Remarks/Explanatory Notes**
UAS-SYS-FUN-REQ-01	The UAS/RPAS shall provide functional capabilities to support and/or enable operations primarily for rail and road IMTM applications.	
UAV-SYS-FUN-REQ-02	There shall be at least four(4) UAS/RPAS main functions available for operations for rail and road IMTM applications, namely: 1) Avoid Hazards 2) Communicate 3) Navigate 4) Control	
UAV-SYS-FUN-REQ-03	The Avoid Hazards Function shall principally refer but not limited to the following sub-functions: 1) Provide Ability to Detect and Avoid (DAA) Traffic 2) Provide Clearance from Structures, Obstacles, and Terrain 3) Provide Clearance from Atmospheric or Meteorological Hazards 4) Provide Clearance from Unauthorized Airspace 5) Provide Clearance from Below-Minimum Visibility Conditions	DAA function is currently conceived passing through the operator centre in contact with UTM
UAS-SYS-FUN-REQ-04	The Communicate Function shall principally refer but not limited to voice and data exchanges among the UAS/RPAS operator, UTM and proximate traffic to communicate intent, instructions, and responses. It shall also include any exchange of information among UAS/RPAS operational personnel. The Communicate Function shall mainly include the following sub-functions: 1) UAS/RPAS External Communications	

	1.1) Provision for External Communications between UAS/RPAS Operator(s) and UTM; 1.2) Provision for External Voice Communications between UAS/RPAS Operator and Operators of Proximate Traffic; 1.3) Provision for External Non-Voice Communications (i.e. Messaging) from UA/RPA to UTM. 1.4) Provision for External Non-Voice Communications between UA/RPA and Proximate traffic. 1.5) Provision for External Communications with HELMET OPS Centre and/or Ancillary Services. 2) UAS/RPAS Internal Communications which shall provide the function of communications among the various interfacing UAS/RPAS crews and related personnel within the HELMET Network.	
UAS-SYS-FUN-REQ-05	The Navigate Function shall refer to the ability in obtaining and maintaining knowledge of the ownship current positional and geographic orientation information and of its destination(s) using reference cues (electronic or visual). It shall include the determination of path(s) to fly from its current position to its subsequent position or to its destination(s). The Navigate Function shall mainly include the following sub-functions: 1) Provision for UA/RPA Altitude Information 2) Provision for UA/RPA Heading and Course information 3) Provision for UA/RPA Ground Position Information 4) Provision for UA/RPA Temporal Data 5) Provision for UA/RPA Trajectory Definition	
UAS-SYS-FUN-REQ-06	The Control Function shall refer to the capability/means of directing, regulating or restraining the aircraft's movement. The Non-flight functions shall refer to items such as transponder codes, radio frequencies, deploying the landing gear (if applicable) and making queries or initiating tests on UAS/RPAS sub-systems. The Control Function shall mainly include the following sub-functions: 1) Provision for Command of UA/RPA Flight Controls 2) Provision for Feedback from UA/RPA Flight Controls 3) Provision for Command of UA/RPA non-Flight Controls 4) Provision for Feedback from UA/RPA non-Flight Controls	
UAS-SYS-FUN-REQ-07	The UAS/RPAS shall have the functional capability of Detect and Avoid (DAA) means which shall enable the UA/RPA to avoid other UAs in the airspace and Manned Aircraft.	TBD Initially only ADS-B tx on board
UAS-SYS-FUN-REQ-08	The UAS/RPAS DAA function shall operate in all airborne phases of flight.	
UAS-SYS-FUN-REQ-09	The Provide Ability to DAA Traffic function shall operate also during surface movement.	TBD In collaboration with UTM

UAS-SYS-FUN-REQ-10	The UAS/RPAS DAA system shall perform Self-Separation.	TBD
UAS-SYS-FUN-REQ -11	The UAS/RPAS DAA system shall perform Collision Avoidance.	TBD Future DAA standards may specify a means to implement DAA using Self-Separation alone an implementation would need to satisfy the required safety level, and may involve additional requirements.
UAS-SYS-FUN-REQ -12	The Collision Avoidance shall provide clearance from structures, obstacles and terrain function and it shall operate in all airborne phases of flight (including turns) and surface movement.	TBD
UAS-SYS-FUN-REQ -13	The provide clearance from structure, obstacles and terrain function can use database(s) for terrain, obstacle, and near airport or UTM information. The accuracy and resolution of the information shall be suitable for the system to perform its intended fuction.	TBD
UAS-SYS-FUN-REQ -14	The Collision Avoidance function shall be capable of accepting updated terrain, obstacle, and airport proximity.	TBD
UAS-SYS-FUN-REQ -15	The Collision Avoidance function shall be capable of accepting and processing UA/RPA performance related data or UA/RPA dynamic data and providing the capability to timely update its alerts.	TBD
UAS-SYS-FUN-REQ -16	The Collision Avoidance function shall support an internal priority alerting system (scheme) to ensure that more critical alerts override the presentation of any alert of lesser priority.	TBD
UAS-SYS-FUN-REQ -17	The Collision Avoidance function shall permit to take effective action to prevent a collision with the obstacle hazard(s).	TBD
UAS-SYS-FUN-REQ -18	The Collision Avoidance function shall provide the UAS/RPAS GC or PIT with sufficient alerting to permit the GC or PIT (if necessary) to take effective action to prevent a collision with an obstacle.	TBD
UAS-SYS-FUN-REQ -19	The Collision Avoidance function shall look ahead of the UA/RPA along and below its lateral and vertical flight path and shall provide suitable alerts if a potential collision threat with obstacle(s) exists.	TBD
UAS-SYS-FUN-REQ -20	The Collision Avoidance function shall permit the UA/RPA to take effective action to prevent a collision with terrain.	TBD
UAS-SYS-FUN-REQ -21	The Collision Avoidance function shall provide the CGS (and PIT if needed) with sufficient alerting to permit the CGS to take effective action to prevent a controlled flight into terrain.	TBD
UAS-SYS_-FUN-REQ-22	The Collision Avoidance function shall look ahead of the UA/RPA along and below its lateral and vertical flight path and provides suitable alerts if a potential collision threat with the terrain exists.	TBD

UAS-SYS-FUN-REQ -23	The UAS/RPAS must be able to avoid meteorological conditions that are hazardous to its specific airframe.	TBD
UAS-SYS-FUN-REQ -24	The Collision Avoidance function shall permit the UA/RPA to take effective action to prevent a controlled flight into these adverse conditions.	TBD
UAS-SYS-FUN-REQ -25	The Collision Avoidance function shall provide information on meteorological hazards to be presented to CGS (and PIT if needed).	TBD
UAV-SR-FUN-REQ -26	The Collision Avoidance function shall look ahead of the UA/RPA along and below its lateral and vertical flight path and provides suitable alerts, if a potential threat exists.	TBD
UAS-SYS -FUN-REQ -27	The Collision Avoidance function shall be capable of accepting and processing UA/RPA performance related data or UA/RPA dynamic data and providing the capability to timely update its alerts.	TBD
UAS-SYS FUN-REQ -28	The Collision Avoidance function shall support an internal priority alerting system to ensure that more critical alerts override the presentation of any alert of lesser priority.	TBD
UAS-SYS -FUN-REQ -29	The UAS/RPAS shall be capable of remaining outside any portion of UTM airspace where the flight is not permitted.	Ie inside geofencing
UAS-SYS -FUN-REQ -30	The UAS/RPAS shall be capable of remaining within the minimum visibility requirements as specified in the EASA Regulations for VFR and IFR flights.	
UAS-SYS -FUN-REQ -31	The system shall provide for Voice Communications between the UAS/RPAS crew and UTM.The CGS shall have the capability to send and receive Verbal Communications to and from the UTM Controller.	
UAS-SYS -COM-REQ -32	The CGS shall have the capability to send and receive a verbal communication to the UAS/RPAS in the vicinity.	
UAS-SYS -COM-REQ -33	The UAS/RPAS shall provide External Non-Verbal Communications from UAV/RPAS to UTM and thus shall have the capability of transmitting and receiving non-voice messages to and from the UTM.	
UAS-SYS -COM-REQ -34	The UA/RPA shall be capable to transmit and receive to and from another UAV/RPAS in the vicinity.	
UAS-SYS -COM-REQ -35	The CGS shall be capable to transmit and/or receive information to and from the HELMET network, PIT Station and ancillary services.	
UAS-SYS -COM-REQ -36	The UAS/RPAS shall provide Internal Communications among its crew and HELMET personnel	
UAS-SYS -FUN-REQ -37	IMTM UAS/RPAS avionics suit shall be equipped to support navigation and positioning integrity by suitable equipment supported by SBAS and GBAS in the different phase of flight.	

UAS-SYS -FUN-REQ -38	On board avionics shall adopt a VBN (visual based navigation) for geo-localization enhancement, position recovery and landing support,	used for navigation check-point and attitude calibration.
UAS-SYS-FUN-REQ -39	The IMTM UAS/RPAS payload technologies and related configurations shall be off-the-self and may include items such as depending on the application typology and related overall performance: a) High Definition (HD) Camera and/or Multispectral Sensors b) Infrared Thermography sensor c) Light Detection and Ranging (LiDAR) d) Robotic Arm Extender Holding Ultrasonic Equipment	
UAS-SYS -FUN-REQ -40	The CGS and PIT-Station shall be capable to receive the estimated UAV/RPAS position.	
UAS-SYS -FUN-REQ -41	The UAS/RPAS shall support UTM surveillance, when the UAV/RPAS is operated in such airspace.	
UAS-SYS -FUN-REQ -42	The UAS/RPAS shall calculate/derive aircraft performance airspeeds to be used all phases of flight.	
UAS-SYS -FUN-REQ -43	The UAS/RPAS Estimate Position Function shall use current altimeter (barometric) setting.	
UAS-SYS -FUN-REQ -44	In a UTM airspace under both IFR and VFR Flight Operations, the UAS/RPAS Define Path Function shall support the use of navigation charts and flight plan as applicable.	
UAS-SYS -FUN-REQ -45	For NAV operations, the UAS/RPAS Define Path Function shall be able to retrieve the procedure by system from the navigation database, not just as a manually entered series of waypoints.	
UAS-SYS -FUN-REQ -46	The UAS/RPAS Define Path Functions shall provide required intent information in all airborne phases of flight and PIT Station operations.	
UAS-SYS -FUN-REQ -47	The UAS/RPAS Define Path Function shall determine the UA path in the case of deviation(s) requested by the UTM.	
UAS-SYS -FUN-REQ -48	The UAS/RPAS Steer Along Path Function shall provide guidance cues to the GCS or the Flight Control Function to steer the UA/RPA on the route of flight provided by the Define Path Function.	Covers operational requirements on 3D positional information for airborne phases of flight.
UAS-SYS -FUN-REQ -49	The UAS/RPAS Steer Along Path Function shall provide guidance cues to the GCS or the flight control function to maintain the appropriate airspeed, flight plan or upon UTM request.	
UAS-SYS -FUN-REQ -50	The UAS/RPAS Steer Along Path Function shall support landing.	
UAS-SYS -FUN-REQ -51	The Required Navigation Performance (RNP) Navigation, the UAS/RPAS Steer Along Path Function shall be able to monitor the achieved navigation performance and to identify to the GCS whether the operational requirement is, or is not, being met during an operation.	

UAS-SYS -FUN-REQ -52	The navigate function shall provide the capability to load the flight data relevant for the flight.	Flight data includes flight plan information, contingency plans, automated landing plan etc. This requirement makes the assumption of a single access point to load the information; architectures with multiple loading points may need to be accommodated.
UAS-SYS -FUN-REQ -53	The navigate function shall provide the capability to verify the loaded flight data.	“Verify” addresses validity, accuracy, and completeness of the flight data relevant for the flight.
UAS-SYS -FUN-REQ -54	The navigate function shall provide the capability to distribute the loaded and verified flight data to the other UAS/RPAS functions as required.	
UAS-SYS -FUN-REQ 55	The Navigation data shall check compatibility of the navigation data with EUROCONTROL and/or UTM Air Navigation Database Waypoints.	
UAS-SYS -FUN-REQ -56	The navigation function shall validate navigation database parameters supporting the requirements associated with the other navigation or UAS/RPAS functions, equipment(s) on-board the UA/RPA and the operation(s).	This high-level requirement is to cover the requirements associated with the content of database for flight planning, trajectory computation, GNSS, multi-sensor Nav equipment, avoidance manoeuvring algorithms, and cover all phases of flight and navigation modes.
UAS-SYS FUN-REQ -57	The navigate function shall validate that the database used for navigation fixes and instrument procedures is maintained current for all operations (VFR/IFR)	
UAS-SYS -FUN-REQ -58	The navigate function shall provide the capability to set and/or reset navigation sensor(s) by either the UAV/RPAS GCS and/or the PIT-Station.	
UAS-SYS -FUN-REQ -59	The UAV/RPAS GCS but also the PIT-Stations shall receive information from the Navaids.	
UAS-SYS -FUN-REQ -60	The Control Function shall provide means to directing, regulating, or restraining the UA/RPA movement on the surface and in flight.	
UAS-SYS -FUN-REQ -61	The GCS or local PIT-Station shall send flight control information to the UAV/RPAS and the UAV/RPAS shall receive flight control information from the GCS and/or local PIT-Station	
UAS-SYS -FUN-REQ -62	The Command Function shall ensure that controls intended for use during flight cannot be operated in any position, combination or sequence, which would result in a condition detrimental to the reliability of the systems or equipment hosting the function, or operation of the aircraft.	The UA/RPA pilot is remote from the UA, and thus does not benefit from direct feedback from the UA/RPA behaviour. The latency in the loop is

		more critical than for manned aircraft in terms of stability of the closed loop. The requirement covers cases similar to manned aircraft such as “hardcover controls”.
UAS-SYS -FUN-REQ -63	The control function shall protect against inadvertent adjustment or engagement by the UA/RPA pilot(s) during UA/RPA flight operations.	
UAS-SYS -FUN-REQ -64	The control function shall use dedicated control in the GCS to engage any flight control mode of the UA/RPA.	
UAS-SYS -FUN-REQ -65	The control function shall prevent inadvertent engagement of any flight control mode of the UA/RPA.	
UAS-SYS -FUN-REQ -66	The control function shall not result in unacceptable jamming or loading of the UA/RPA primary flight controls.	
UAS-SYS -FUN-REQ -67	The UA/RPA shall send flight control information to the GCS which shall received it without containing contradictory information.	
UAS-SYS -FUN-REQ -68	Control modes of the UA/RPA, whether engaged, armed, in transition and/or in reversion shall be indicated visually in the GCS.	
UAS-SYS -FUN-REQ -69	The control function shall ensure the UA/RPA pilot(s) is made aware of the status of UA/RPA controls.	
UAS-SYS -FUN-REQ -70	The control function shall provide timely attention-getting cues through at least two different senses by a combination of aural, visual, or tactile indications in case of disengagement of an automatic flight control mode of the UA/RPA.	
UAS-SYS -FUN-REQ -71	The GCS shall prevent engagement of a UA/RPA control mode prior to its reaching a fully operable condition.	
UAS-SYS -FUN-REQ -72	The GCS shall provide the UA/RPA pilot(s) with situational awareness in the case of a control mode change.	
UAS-SYS -FUN-REQ -73	The UAS/RPAS shall monitor and confirm the execution of UAV/RPA flight controls.	To assure UA/RPA pilot situational awareness, means must be provided to monitor and confirm the execution of the flight control commands. The remote location of the UA/RPA pilot adds a latency between the command input and the feedback from aircraft behaviour, compared to manned aircraft. The UAV/RPAS pilot does not

		“feel” the aircraft dynamic response to his/her commands, the monitoring and confirmation aims at mitigating it.
UAS-SYS -FUN-REQ -74	The GCS shall send non-flight control information to the UAV/RPAS and the UAV/RPAS shall receive non-flight control information from the GCS	
UAS-SYS -FUN-REQ -75	Where operationally applicable, the PIT-Station(s) shall send non-flight control information to the UAV/RPAS. The UAV/RPAS shall receive non-flight control information from the PIT-Station(s) when operationally required.	
UAS-SYS -FUN-REQ -76	The UAV/RPAS non-flight controls shall provide feedback and send non-flight control information to the GCS.	
UAS-SYS -FUN-REQ -77	The GCS shall receive non-flight control information from the UAV/RPAS. The UAV/RPAS shall send non-flight control information to the PIT-Station.	All systems checks require data exchange between the system and the PIT performing the check. Post-flight data collection is performed by the related PIT-Station.
UAS-SYS -FUN-REQ -78	The related PIT-Station shall receive non-flight control information from the UA/RPA	
UAS-SYS -FUN-REQ -79	The UAS/RPAS sub-systems shall report their operational status to the UA/RPA pilot.	This requirement does not imply a centralized monitoring system, the requirement can be allocated to each system independently.
UAS-SYS -FUN-REQ -80	All data and voice messages sent between the GCS or PIT and the UA/RPA shall be recorded.	
UAS-SYS -FUN-REQ -81	The Flight Planning Function shall be able to integrate datalink performance data or other data to support the computation of datalink performance relative to meteorological conditions, terrestrial features and UAS/RPAS capabilities.	
UAS-SYS -FUN-REQ -82	The Flight Planning Function shall provide the capability to verify that the contingency plan for lost control datalink complies with the EASA regulations.	

OBU SUB-SEGMENT-Functional Requirements (FUN)

Req. ID	Requirement Description	Remarks/Explanatory Notes
UAS-OBU-FUN-REQ-100	OBU avionics shall support any operative mode and mission classes envisaged for Helmet applications	

UAS -OBU -FUN-REQ-101	OBU avionics suit shall be equipped but not limited to: 1) EGNSS multifrequency receiver 2) IMU (accelerometer, gyro) 3) Magnetic compass, barometer 4) SW for position and navigation integration based on Kalman filter 5) Autopilot 6) Augmentation/UTM control communication link (can be included in the CNPC link) 7) Remote CNPC link 8) VBN (visual based navigation) on the basis of PIT station reference and sleeper coding, used for navigation check-point and attitude calibration. 10) ADS-B transmitter (optional)	
UAS-OBU- FUN-REQ-102	OBU shall adopt an FDIR SW program	
UAS-OBU-FUN-REQ-103	OBU shall be capable to continuous to operate in graceful degradation mode	
UAS-OBU-FUN-REQ-104	OBU shall support navigation accuracy requirement foreseen for the mission in any flight phase	
UAS-OBU-FUN-REQ-105	OBU shall process data from all the source (space and ground) in order to achieve the current best accuracy and navigation performance	
UAS-OBU-FUN-REQ-106	OBU shall be capable to take recovery actions according to a programmed plan	
UAS-OBU-NAV-REQ-107	OBU shall be able to produce navigation data for flying automatically inside the schedule flight plan following a waypoint	
UAS-OBU-AUG-REQ-108	OBU can store ground geolocalized images and process them in order to get position data	
UAS-OBU-AUG-REQ-109	OBU shall provide navigation data integrity by combining SBAS,GBAS (via PIT station) and internal processing	
UAS-OBU-AUG-REQ-110	OBU shall embed a ARAIM function	
UAS-OBU-AUG-REQ-111	OBU shall embed a ABIA integrity function with integrity warnings & alarm	
UAS-OBU-FUN-REQ-112	OBU shall augment position accuracy via PPP-RTK concept	
UAS-OBU-FUN-REQ-113	OBU shall comply all the safety requirement foreseen for the application	
UAS-OBU-FUN-REQ-114	OBU shall support automatic or assisted landing based on VBN	

PIT STATION SUB-SEGMENT-Functional Requirements (FUN)

Req. ID	Requirement Description	Remarks/Explanatory Notes
UAS-PIT-FUN-REQ-83	PIT station can be deployed in any remote and anthropic areas	

UAS-PIT-FUN-REQ-84	Relay Communication with UAV via an omnidirectional and a directional antenna one	
UAS -PIT- AUG-REQ-85	Acquire EGNSS signal for Galileo e GPS constellation in two (three) BW's multipath free	
UAS-PIT-FUN-REQ-86	Acquire ADS-B data (option)	
UAS-PIT-FUN-REQ-87	Auto diagnosis and fault detection with signalling of status to GCS	
UAS-PIT-FUN-REQ-88	Wide FOV optical vision system for surrounding and landing areas monitoring	
UAS-PIT-FUN-REQ-89	Communication of all the acquired data to the GCS via terrestrial network or satellite (EGNSS, ADS-B, Optical images, measurement data, etc)	
UAS-PIT FUN-REQ-90	PIT station can monitor the surrounding environmental EM environment providing status	
UAS-PIT-FUN-REQ-91	PIT station can monitor around meteo data and visibility level (by WFOV optical system)	
UAS-PIT-FUN-REQ-92	The system shall allow the PIT Station to communicate (rx) simultaneously through the terrestrial, satellite and/or near future intermediate aerial links such as HAPS (High Atmosphere Systems) or LEO systems. In addition, the system shall be able to receive simultaneously from terrestrial and satellite links and tx only in one direction.	
UAS-PIT-FUN-REQ-93	The UAS/RPAS-PIT Station shall automatically handle satellite to terrestrial and terrestrial to satellite link handovers in the forward and return links.	
UAS-PIT-FUN-REQ-94	The PIT Station in terms of Satellite Communication and GNSS services within the HELMET System shall be capable of serving a heterogeneous population of UAS/RPAS with different constraints on power, frequencies, Bandwidth and antenna accommodation.	
UAS-PIT-FUN-REQ-95	The PIT station shall support all the activities needed for take-off preparation, UAV maintenance and landing	

UAS/RPAS SUB-SEGMENT-Performance Requirements (PER)		
Req. ID	**Requirement Description**	**Remarks/Explanatory Notes**

<table>
<tr><td>UAS-EXT-PER-REQ-01</td><td>The minimum range of Multi-Rotor UA/RPA General Physical and Performance Requirements for Rail and Road Inspection, Monitoring and Traffic Management Operations are summarized as follows:
<table>
<tr><th>SMALL UAV TYPE</th><th>MTGW Range (Kg)</th><th>Speed Range (Km/h)</th><th>Max. Banking & Max.Ver</th><th>Normal OPS Altitude Range (m)</th><th>Max. Flight Endurance (min)</th><th>Operating Temp</th><th>Mission Radius Range (Km)</th></tr>
<tr><td>Multi-Rotor
 </td><td>≤ 1 TO ≤ 25</td><td>30-80</td><td>6 °/s
±3 m/s to ±10 m/s</td><td>≤ 3 to ≤ 400</td><td>45-90</td><td>-20 to 55 °C
(Electrical Powe
-40 to 55 °C
(Non-Electric)</td><td>1.6 TO ≤ 100</td></tr>
</table></td></tr>
<tr><td>UAS-EXT.PER-REQ-02</td><td>The minimum range of Single-Rotor UA/RPA General Physical and Performance Requirements for Rail and Road Inspection, Monitoring and Traffic Management Operations are summarized as follows:
<table>
<tr><th>SMALL UAV TYPE</th><th>MTGW Range (Kg</th><th>Speed Range (Km/h</th><th>Max. Banking & Max.Ver</th><th>Normal OPS Altitude Range (m)</th><th>Max. Flight Endurance (min)</th><th>Operating Temp (C</th><th>Mission Radius Range (Km)</th></tr>
<tr><td>Single-Rotor
 </td><td>1 TO ≤ 25</td><td>20-60</td><td>6 °/s
±3 m/s to ±10 m/s</td><td>≤ 3 to ≤ 400</td><td>30 - 60</td><td>-20 to 55 °C
(Electrical Power)
-40 to 55 °C
(Non-Electric)</td><td>1.6 TO ≤ 100</td></tr>
</table></td></tr>
<tr><td>UAS-EXT-PER-REQ-03</td><td><table>
<tr><th>SMALL UAV TYPE</th><th>MTGW Range (Kg)</th><th>Speed Range (Km/</th><th>Max. Banking & Max.Ver</th><th>Normal OPS Altitude Range (m)</th><th>Max. Flight Endurance (min)</th><th>Operating Temp (C°)</th><th>Mission Radius Range (Km)</th></tr>
<tr><td>Fixed-Wing

Hybrid</td><td>≤ 3 TO ≤ 25</td><td>30-100</td><td>4 - 6 °/s
±3 m/s to ±10 m/s</td><td>≤ 10 to ≤ 400</td><td>45 -120</td><td>-20 to 55 °C
(Electrical Power)
-40 to 55 °C
(Non-Electric)</td><td>50 TO ≤ 200</td></tr>
</table>
The minimum range of Fixed-Wing Hybrid UA/RPA General Physical and Performance Requirements for Rail and Road Inspection, Monitoring and Traffic Management Operations are summarized as follows</td></tr>
<tr><td>UAS-COM-PER-REQ-04</td><td>The UAS/RPAS CNPC Link Availability (Probability/Flight Hour) shall be for the:
a) Forward Link : 0.999997and b) Return Link: 0.999997 With RCP 10 Separation: 5nm, Transaction Time: 10sec</td><td>:</td></tr>
</table>

UAS-COM-PER-REQ-05	The UAS/RPAS CNPC Link Continuity(Probability/Flight Hour) shall be for the: a) Forward Link : 0.99985, and b) Return Link: 0.99985 With RCP 10 Separation: 5nm, Transaction Time: 10sec	
UAS-COM-PER-REQ-06	The UAS/RPAS CNPC Link Integrity(BER/PER) (Acceptable Rate/Flight Hour) shall be for the Forward Link: 1.43 x10^{-6} and for the Return Link: 1.43 x10^{-6} with RCP 10 Separation: 5nm, Transaction Time: 10sec.	
UAS-COM-PER-REQ-07	The UAS/RPAS CNPC Link Latency (Maximum Permitted) for Real-time safety critical information shall be for the Forward Link: 130ms and for the Return Link: 130ms.	
UAS-COM-PER-REQ-08	The UAS/RPAS CNPC Link Latency (Maximum Permitted) for Near Real-time safety critical information shall be for the Forward Link: 520ms and for the Return Link: 520ms.	
UAS-COM-PER-REQ-09	The UAS/RPAS CNPC Link Latency (Maximum Permitted) for Low Priority safety critical information shall be for the Forward Link: 5.2s and for the Return Link: 5.2s.	
UAS-COM-PER-REQ-10	The UAS/RPAS CNPC Link Latency (Maximum Permitted) for Non-safety critical information shall be for the Forward Link: 20.8s and for the Return Link: 20.8s.	
UAS-COM-PER-REQ-11	The UAS/RPAS CNPC Link Jitter shall be for the Forward Link: 50μ and for the Return Link: 50μ Packet to packet.	
UAS-COM-PER-REQ-12	The UAS/RPAS Performance Requirement associated with operational communication in an Unexpected interruption of a transaction shall be 10^{-4} per aircraft per flight hour	
UAS-COM-PER-REQ-13	The UAS/RPAS Performance Requirement associated with operational communication in a Loss of communication transaction shall be 10^{-5} per aircraft per flight hour.	
UAS-COM-PER-REQ-14	The UAS/RPAS Performance Requirement associated with operational communication in a Loss of service shall be 10^{-6} per aircraft per flight hour.	
UAS-COM-PER-REQ-15	The UAS/RPAS Performance Requirement associated with operational communication in an Undetected corrupted transaction shall be 10^{-5} per aircraft per flight hour.	
UAS-COM-PER-REQ-16	UAS/RPAS IMTM railway and road operations environmental noise emission requirements and limits shall be compliant EU and EASA Protection of the Environment Operational Restrictions and Regulations. However, Noise Requirements shall not exceed the 80 dB re 20 μPa and 81 dB re 20 μPa (rms), with fundamental frequencies centered at 60 Hz and 150 Hz for all considered models.	

<table>
<tr>
<td>UAS-COM-PER-REQ-17</td>
<td>The UAS/RPAS CNPC Spectrum Requirements shall be in accordance with Methodology 2 of ITU -R M.2171 as follows:
<table>
<tr><td>Functional Category</td><td colspan="2">Aggregate Bandwidth Requirement (MHz)</td></tr>
<tr><td></td><td><b>LOS Terrestrial System</b></td><td><b>BLOS Spot-Beam Satellit</b></td></tr>
<tr><td>Command and Control</td><td>1.61</td><td>9.01</td></tr>
<tr><td>ATC Relay</td><td>2.72</td><td>6.50</td></tr>
<tr><td>Sense and Avoid or DAA</td><td>23.51</td><td>21.81</td></tr>
<tr><td>Total</td><td><b>27.84</b></td><td><b>37.32</b></td></tr>
</table>
</td>
<td>In accordance with the with Methodology 2 of ITU -R M.2171 the Terrestrial Spectrum requirements are divided as follows:
1) GCS/RPS to UA/RPA = 2.0 MHz
2) UA/RPA to GCS/RPS = 25.9 MHz.
The spot-beam satellite spectrum requirements are divided as follows:
1) UA/RPA to SAT = 15.32 MHz
2) GCS/RPS to SAT = 3.29 MHz
3) SAT to UA/RPA = 3.29 MHz
4) SAT to GCS/RPS = 15.32 MHz.</td>
</tr>
<tr>
<td>UAS-AUG-PER-REQ-18</td>
<td colspan="2">The UAS/RPAS Typical Flight Operation (No Specific Mission)/Flight Phase High Level Requirements for HELMET are summarized as follows:
<table>
<tr><td>UAV Typical Flight Operation (No Specific Mission)/Flight Phase</td><td>Accuracy
<b>Horizontal 95%</b></td><td>Accuracy
<b>Vertical 95%</b></td><td>Integrity</td><td>Time-to-Alert</td><td>Continuity</td><td>Availability</td></tr>
<tr><td>En-route</td><td>3.7 km (2.0 NM)</td><td>N/A</td><td>1 – 1×10–7/h</td><td>5 min</td><td>1–1×10–4/h to 1–1×10–8/h</td><td>0.99 to 0.99999</td></tr>
<tr><td>Arrival (Landing)</td><td>0.74 km (0.4 NM)</td><td>N/A</td><td>1 – 1×10–7/h</td><td>15 s</td><td>1–1×10–4/h to 1–1×10–8/h</td><td>0.99 to 0.</td></tr>
<tr><td>Approach, Departure (Take-off)</td><td>220 m (720 ft)</td><td>N/A</td><td>1 – 1×10–7/h</td><td>10 s</td><td>1–1×10–4/h to 1–1×10–8/h</td><td>0.99 to 0.99999</td></tr>
<tr><td>Field Approach Operations</td><td>16.0 m (52 ft)</td><td>20 m (66 ft)</td><td>1 – 2× 10–7
in any approach</td><td>10 s</td><td>1 – 8× 10–6 per 15 s</td><td>0.99 to 0.99999</td></tr>
<tr><td>Precision Approach (PIT Station Approach)</td><td>16.0 m - 4m</td><td>6.0 m to 4.0 m
(20 ft to 13 ft)</td><td>1 – 2× 10–7
in any approach</td><td>6 s</td><td>1 – 8× 10–6 per 15 s</td><td>0.99 to 0.99999</td></tr>
</table>
</td>
</tr>
<tr>
<td>UAS-AUG-PER-REQ-19</td>
<td colspan="2">The UAS/RPAS Specific Flight Operations for Rail and Automotive Inspection, Monitoring and Traffic Management Application Operations High Level Requirements for HELMET are summarized as follows:
<table>
<tr><td><b>SPECIFIC FLIGHT OPERATIONS (RAIL/AUTOMOTIVE)</b></td><td><b>ACCURACY HORIZONTAL</b></td><td><b>ACCURACY VERTICAL</b></td><td><b>INTEGRITY</b></td><td><b>TIME-TO-ALERT</b></td><td><b>CONTINUITY</b></td><td><b>AVAILABILITY</b></td></tr>
<tr><td><b>MONITORING MISSION (RAIL/AUTOMOTIVE)</b></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td>
</tr>
</table>

	Position/Navigation (Urban/Non-Urban)	1 m /10m	1 m /10m	1 – 2× 10–7	1s (HOT)-6s (COLD)	1–1×10–4/h to 1–1×10–8/h	0.95-0.99
	GEO-Awareness	1m	1m	1 – 2× 10–7	1s (HOT)-6s(COLD)	1–1×10–4/h to 1–1×10–8/h	0.95-0.99
	INSPECTION MISSION (RAIL/AUTOMOTIVE)						
	Position/Navigation (Urban/Non-Urban)	1 m /10m	1 m /10m	1 – 2× 10–7	1s (HOT)-6s(COLD)	1–1×10–4/h to 1–1×10–8/h	0.95-0.99
	GEO-Awareness	1m	1m	1 – 2× 10–7	1s (HOT)-6s(COLD)	1–1×10–4/h to 1–1×10–8/h	0.95-0.99
	TRAFFIC MANAGEMENT MISSION (RAIL/AUTOMOTIVE)						
	Position/Navigation (Urban/Non-Urban)	10m / 30m	10m / 30m	1 – 2× 10–7	1s(HOT)-10s(COLD)	1–1×10–4/h to 1–1×10–8/h	0.95 to 0.99
	GEO-Awareness	1m	1m	1 – 2× 10–7	1s (HOT)-6s(COLD)	1–1×10–4/h to 1–1×10–8/h	0.95 to 0.99

COM SUB-SEGMENT-Performance Requirements (PER)		
Req. ID	**Requirement Description**	**Remarks/Explanatory Notes**
UAS_COM-PER-REQ-20	Communication DR with GCS: 100 Mbits/s Latency <100ms for high priority communications	
UAS-COM-PER-REQ-21	Communication DR with UAV TT&C (includes also GNSS augmentation) FWD: 10 Kbits Return: 300 Kbits Integrity requirement: 10-5	
UAS-COM-PER-REQ-22	Communication DR with UAV mission data Return: 1 Mbits	

UAS/RPAS-PIT STATION SEGMENT-EXT Interface Requirements		
Req. ID	**Requirement Description**	**Remarks/Explanatory Notes**
UAS-EXT-AUG-REQ-01	HCC shall provide PPP-RTK and DGNSS data	
UAS-EXT-AUG-REQ-02	HCC shall provide EGNSS satellite mask data for OBU processing	
UAS-EXT-AUG-REQ-03	HCC shall provide multi-constellation integrity status	
UAS-EXT-AUG-REQ-04	HCC shall provide accuracy available forecast (considering DOP, satellite health and errors, ect)	
UAS-EXT-AUG-REQ-05	HCC shall provide PIT station system areas integrity status including EM	

UAS/RPAS-PIT STATION SEGMENT Security Requirements (SEC) [Includes Jamming and Spoofing Requirements]		
Req. ID	**Requirement Description**	**Remarks/Explanatory Notes**
UAS-SYS-SEC-REQ-01	The system shall provide data confidentiality, authentication and integrity.	The system shall foresee encryption and authentication mechanisms. Data integrity by error control mechanism and ARQ.
UAV-SYS-SEC-REQ-02	The system shall provide electronic counter measures (e.g. anti-jamming, anti-spoofing) at communication system level	Anti-spoofing by authentication, Anti-jamming by spectrum analysis and frequency hopping
UAV-SYS -SEC-REQ-03	Detection means shall be provided to enable the measurement and monitor the basic signal-in-space (SiS) characteristics.	By comparing the characteristics of the SiS in the past with the actual ones it is possible to detect jamming. Via Helmet core center or in local
UAV-SYS-SEC-REQ-04	Detection means shall be able to store information about the usual amount of signal power in the bandwidth of interest.	Consider the usual amount of signal power permits to register sudden and anomalous increase that indicates an attack is in place.
UAV-SYS -SEC-REQ-05	Detection means shall be able to check if the Satellite ID (SID) extracted from the navigation message is a valid SID.	Important to detect if the message is built from an offender or is authentic. Only for
UAV-SYS-SEC-REQ-06	If a valid SID is extracted by the navigation message, detection means shall be able to establish if the satellite is in the field of view of UAS/RPAS and drop the unfeasible messages.	Important to detect if the message is built from an offender or is authentic.

UAV-SYS-SEC-REQ-7	Detection means shall be able to compare ionospheric correction extracted from I/NAV-F/NAV message and the correction provided by the models.	Ionospheric corrections more “compatible” with GPS model respect to Galileo 3D model could be sign of possible “spoofing attack”.
UAV-SYS-SEC-REQ-8	Detection means shall be able to compare the Issue Of Data received in the message with ephemeris, satellite clock correction parameter and SISA in order to detect potential spoofing.	Differences in these parameters can be a possible sign of “spoofing attack”.
UAV-SR-SEC-REQ-9	Detection means shall be able to compare the Issue Of Data received in the message with the almanacs.	Differences in these parameters can be a possible sign of “spoofing attack”.
UAS-SYS-SEC-REQ-10	Detection means shall be able to store ephemeris information and maintain them for at least 4h.	Ephemeris information will not change for about 4h. This information can be used to spot a possible “spoofing attack”.
UAS-SYS-SEC-REQ-11	Use of correlation of the envelope detector output shall be used in order to spot a possible spoofing attack.	Differences in this parameter can be a possible sign of “spoofing attack”.
UAS-SYS-SEC-REQ-12	Detection means shall be able to collect historical records of SISA in order to generate Cumulative Density Functions	The correctness of SISA in the message to be used as possible sign of spoofing attack.
UAS-SYS-SEC-REQ-13	Detection means shall be able to compute SISE and check its coherence with the SISA received.	The correctness of SISA in the message to be used as possible sign of spoofing attack.
UAS-SYS -SEC-REQ-17	S/GALILEO almanac should be provided to the detection tool in order to compute the similarity of the almanacs received with the GPS/GALILEO’s ones.	Offender could generate spoofed message from GPS signal.
UAS-SYS -SEC-REQ-18	The detection means shall be able to store successive clock bias in order to verify that smooth variation of the clock bias.	When the receiver moves with respect to the spoofer antenna, the clock bias will change rapidly.
UAS-SYS -SEC-REQ-19	The detection means shall be able to send/receive navigation data received by GNSS to the UAS/RPAS-PIT STATION (if needed).	Cooperation within UAS/RPAS in order to detect spoofing attack.
UAS-SYS -SEC-REQ-20	During communication with the UAS/RPAS-PIT, detection tool shall be able to recognize replay attack and discard the relevant packets.	Important to detect if the message is built from an offender or is authentic.
UAS-SYS SEC-REQ-21	The detection means shall be able to access to stand-alone inertial equipment in order to extract information about PVT	These parameters can be used to detect spoofing by comparing with GNSS ones.
UAS-SYS -SEC-REQ-22	The UAS/RPAS-PIT shall be able to access and elaborate EDAS data. Cooperation within UAS/RPAS-PIT in order to detect spoofing attack.	Via HCC
UAS-SYS -SEC-REQ-23	The Remote Piloted Controller shall estimate by its own, the UAS/RPA’s PVT by means of an autonomous system.	

<table>
<tr><td>UAS-SYS SEC-REQ-24</td><td>The Remote Pilot shall compare its PVT estimation with the ones received from UAS/RPAS.</td><td></td></tr>
<tr><td>UAS-SYS-COM-SEC-REQ-25</td><td>The CNPC link shall put in place authentication at the beginning of the communication between the two parts.</td><td></td></tr>
<tr><td>UAS-SYS-SEC-REQ-27</td><td>The field strength of ECE = 10 Vm^{-1} shall represent the EMC immunity required by EU regulations for all electronic equipment used in industrial environments. The following Table provides some experimental data that might be used during preliminary design.
<table>
<tr><th>Frequency</th><th>Test parameter*</th><th>Observed effects</th><th>Performance class required/ reached</th><th>Evaluation</th></tr>
<tr><td>80 MHz–1 GHz</td><td>10 V m^{-1}, AM</td><td>none</td><td>a/a</td><td>pass</td></tr>
<tr><td>1.4–2 GHz</td><td>3 V m^{-1}, AM</td><td>2.4 GHz remote control link disturbed</td><td>b/b</td><td>pass</td></tr>
<tr><td>2–2.7 GHz</td><td>10 V m^{-1}, AM</td><td>between 1887–2002 MHz
2.4 GHz remote control link disturbed</td><td>b/b</td><td>pass</td></tr>
<tr><td>400 MHz</td><td>30 V m^{-1}, GSM</td><td>between 2040–2616 MHz none</td><td>a/a</td><td>pass</td></tr>
<tr><td>2400 MHz</td><td>30 V m^{-1}, GSM</td><td>none</td><td>a/a</td><td>pass</td></tr>
<tr><td>5200 MHz,</td><td>30 V m^{-1}, GSM</td><td>none</td><td>a/a</td><td>pass</td></tr>
<tr><td>5800 Mhz
810 MHz,</td><td>30 V m^{-1}, GSM</td><td>none</td><td>a/a</td><td>pass</td></tr>
<tr><td>1840 MHz,</td><td></td><td></td><td></td><td></td></tr>
<tr><td>2660 MHz
3020 MHz,</td><td>30 V m^{-1}, Pulse</td><td>none</td><td>a/a</td><td>pass</td></tr>
<tr><td>9375 MHz</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="5">∗ AM = Amplitude modulation 80 %, 1 kHz; GSM = Pulse modulation 570 µs/4.6 ms; Pulse = Pulse modulation 1µs/1 ms.</td></tr>
</table></td><td>The EU Regulations are, valid for LTE800 and GSM900 mobile networks. For services using frequencies in the range 1.4 up to 2 GHz, like GSM1800 and LTE1900, the tested severity level is just ECE = 3 Vm^{-1} Above 2 GHz where services like UMTS and LTE2600 are located the tested level is lowered to ECE = 1 Vm^{-1}. The EMC immunity performance of typical commercial UAS/RPAS beyond these test levels is most probably unknown for lack of any additional conformity requirements taking the extended spatial mobility into account. Under the field strength of ECE = 10 Vm^{-1} the immunity distance for an operating UA/RPA is about 18m.</td></tr>
<tr><td>UAS-SYS-SEC-REQ-28</td><td>UAS/RPAS IMTM railway and road operations may be constrained by privacy requirements, such as in private residential areas, but even in public places where there are requirements in the law that limit or prohibit the unauthorised video or imaging of private persons without their express authorisation. Mission plans shall need to account for these privacy constraints as per EU and local State Member Regulations.</td><td></td></tr>
</table>

UAS/RPAS-PIT STATION SEGMENT- Safety Requirements (SAF)		
Req. ID	**Requirement Description**	**Remarks/Explanatory Notes**
UAS-SYS-SAF-REQ-01	Safety requirements for the IMTM UAS/RPAS railway and road operations and use cases shall need to consider a range of physical and operational safety controls, including but not limited to the following: 1) certified safety-critical flight control systems and avionics 2) crashworthy body design with crumple zones and impact protection 3) redundant power, propulsion and flight control subsystems 4) Remote Pilot (RP) warning systems and indicators	
UAS-SYS-SAF-REQ-02	All flight critical components (Airborne and Ground board) in the UAS/RPAS-PIT STATION or sub-systems of the UAS/RPAS affecting safety of operations, shall be designed and installed such that: (i) It should perform as intended under the UAS/RPAS IMTM operating and environmental conditions for which it is designed for. (ii) All other equipment/components, should they become unserviceable, should not reduce the level of safety and should not adversely affect the proper functioning of all flight critical components.	
UAS-SYS-SAF-REQ-03	The UAS/RPAS-PIT STATION shall be designed to minimise system degradation and/or failures that, at minimum, address the following: (i) Total loss of the UA/RPA power to the avionics and propulsion system (ii) Total loss of power to the Ground Control System (GCS) and PIT-STATION (iii) Loss of the ability for UA/RPA to navigate within allowable system accuracy (iv) Loss of the ability to make autonomous decisions (v) Catastrophic or hazardous failure conditions. The Operator should have to identify all possible hazards and demonstrate an acceptable level of safety to EASA, through one or more of the following methods: (i) System redundancies (ii) Reliability testing (iii) Operational procedures.	
UAS-SYS-SAF-REQ-04	The UAS/RPAS specific category shall be subjected to EASA LORA procedure and related Regulations while the certified category shall be subject to EASA Regulations which are conformable to manned aviation.	
UAS-SYS-SAF-REQ-05	The UAS/RPAS-PIT STATION operators (pilot and payload operator) should be made aware of minor UA/RPA-PIT STATION system failures or unsafe conditions that will result in one or more of the following: (i) Degradation to the UA/RPA flight and PIT performances; (ii) Eventual failure of any of the UA/RPA airborne and PIT ground critical flight systems; (iii) Eventual loss of capability to maintain situational awareness of airspace traffic, terrain, obstacles and/or weather; or (iv) Eventual loss of power The UA/RPA operators must implement the relevant corrective actions as stipulated in the UAS/RPAS Flight Manual and PIT STATION Operations Manual .	
	The UAS/RPAS operators should be made aware of critical system failures or unsafe conditions that will result in one or more of the following: (i) Severe degradation to the UA/RPA flight performance such that the UA/RPA is unable to maintain its flight path or current location; (ii)	

UAS-SYS-SAF-REQ-06	Failure of any of the UA/RPA on-board critical flight systems; (iii) Loss of capability to maintain situational awareness of airspace traffic, terrain, obstacles and/or weather; The UA/RPA Operators should be able to perform emergency recovery and/or landing using the recovery facilities of the nearest to the flight path PIT STATION or alternative for such emergencies geo-fenced locations in the event of such critical system failures as soon as practicable.	
UAS-SYS-SAF-REQ-07	In the event of multiple failures, failure handling (either manually by the UA/RPA operator or automatically by the UAS/RPAS under the support of the PIT STATION capabilities for such occurrences) should prioritise and handle all failures in order of severity.	
UAS-SYS-SAF-REQ-08	There should be adequate means to maintain situational awareness of the UA/RPA and its surroundings (both in the air and on the ground). Examples will include monitoring of flight routes and flight corridors and/or having systems on board to avoid collision with obstacles (DAA).	
UAV-SYS-SAF-REQ-09	In accordance with EASA limits, the IMTM UAS/RPAS flight operations shall not be less than 30 m from humans (other than the UAS/RPAS pilot, mission owner and other authorised staff).	

5.4 MULTIMODAL SYSTEM REQUIREMENTS FOR GNSS AUGMENTATION

This section includes system requirements for the HELMET Multi-modal Augmentation System.

ID	Name	Description
SR-AUG-OPE-001	Augmentation System Fault Detection and Exclusion THR	The Augmentation System Fault Detection and Exclusion for RTK and NRTK has to be based on the 2-Tiers Method
Rationale		
The 2-Tiers approach has been presented and tested in the Rail sector within the GSA project ERSAT-EAV and RHINOS		
Notes		
References		
[20]		

ID	Name	Description
SR-AUG-PER-002	Augmentation System THR	The Augmentation System has to guarantee a THR of 5e-7/h for RTK and NRTK
Rationale		
GNSS THR has to be divided by Augmentation THR and OBU THR, taking into account that OBU local effects (e.g. multipath, shadowing and ambiguity fixing) counts for 90% of the Faults		
Notes		
References		

ID	Name	Description
SR-AUG-FUN-003	Augmentation messages contents	The Augmentation System performs SIS and Reference Stations Fault Detection and Exclusion for RTK and NRTK. Constellation, satellites and Reference Stations Faults are detected and excluded. A constellation, satellite and Reference Station Healthy mask is transmitted to the OBU for the needed relevant exclusion
Rationale		
The Augmentation control Centre performs a SIS and Reference Stations Fault Detection and Exclusion based on the 2-Tiers approach. Relevant masks are also transmitted to the OBU for relevant exclusion. Communication Faults and OBU Faults are not in charge of the Augmentation Control centre		

Notes		
References		
SR-AUG-INF-004 **SR-AUG-INF-005**		

ID	**Name**	**Description**
SR-AUG-INF-004	Standardised Augmentation System Protocol and Format for accuracy augmentation messages	The Augmentation system has to transmit Augmentation messages through RTCM NTRIP protocol and RTCM SC-104 standard (latest issue) for not integrity messages
Rationale		
RTCM NTRIP and relevant Data formats are the most widely augmentation standard currently implemented by Service Providers and manufacturers		
Notes		
References		
[27],[36]		

ID	**Name**	**Description**
SR-AUG-INF-005	Not Standardised Augmentation System Protocol and Format for accuracy augmentation messages	The Augmentation system has to transmit and log the Augmentation messages for integrity through RTCM NTRIP protocol and RTCM SC-104 and RTCM SC-134 data fields and messages to be defined using existing data types
Rationale		
New messages for transmitting Integrity Support messages, will be provided through a subsystem of relevant Integrity. Support messages proposed within the ERSAT-EAV Project and within the RTCM SC-134 Committee are here used and possibly updated		
Notes		
1.	RTCM Message updates will be presented to the RTCM SC-134 and relevant for official approval, after HELMET project Coordinator and GSA authorisation. This task is facilitated, being R. Capua (Sogei) the Chairman of SC-134, that still asked for the official support letter from RTCM for the project	
References		
[27],[36] ERSAT-EAV 2-Tiers Messages proposals RTCM SC-134 draft proposal		

ID	**Name**	**Description**
SR-AUG-FUN-006	Augmentation to Service Level allocation	The Augmentation system to service level allocation is reported in *Table 16*
Rationale		

Table 16 Level to Augmentation Systems allocation

Service Level	Augmentation System
SL1	DGNSS+2-Tiers, EGNOS, SBAS Galileo HAS
SL2	RTK/NRTK Float, DGNSS+2-Tiers, Galileo HAS, INS
SL3	Multi-constellation and dual or triple frequency OBU, RTK/NRTK Fixed or Float solution + INS+ odometer
SL4	Multi-constellation and dual or triple frequency OBU, RTK/NRTK Fixed or Float solution + INS + odometer

Notes	
1.	The allocation is based on the performance analysis review and experimental data
References	
[27],[36]	

ID	Name	Description
SR-AUG-OPE-008	RTK Augmentation maximum service coverage	The Service Coverage for RTK Fixed solution is 30 km
Rationale		
Following recent		
Notes		
1.	Current RTK technology allows achieving ambiguity fixing till 50 km of distance from the nearest Reference Station. Here the nominal distance of 30 km is assumed as reference in order to be conservative	
References		
[27],[36]		

ID	Name	Description
SR-AUG-OPE-009	NRTK Augmentation Reference Stations distribution	At least 4 Reference Station, distributed in a polygon with maximum edges length of 70 Km and including the demonstration area, have to be provided for implementing the NRTK service
Rationale		
Following recent NRTK development, nominal maximum interdistance is assumed to be 70 km.		
Notes		
1.	RTCM Message updates have to be presented to the RTCM SC-134 and relevant and approval and validation process started	
2.	For the HELMET Pilot Projects, in order to avoid development costs increase, NRTK implementation will be subject the availability of at least 4 Reference Stations surrounding the Pilot selected site	
References		
[27],[36]		

ID	Name	Description
SR-AUG-OPE-010	2-Tiers connection to EDAS	The Augmentation control Centre has to be connected to the EDAS system for gathering RIMS raw data through RTCM SC-104 data format and NTRIP protocol for implementing the 2-Tiers Algorithm
Rationale		
Notes		
References		
[27],[36]		

ID	Name	Description
SR-AUG-OPE-011	Augmentation Centre Service Mountpoints	The Augmentation Control Centre provide messages for each Service Levels through distinct RTCM NTRIPCaster mountpoints
Rationale		
Services separation is performed through RTCM mountpoints diversity		
Notes		
References		
[27],[36] **SR-FUN-AUG-00X**		

ID	**Name**	**Description**
SR-AUG-OPE-012	Augmentation correction messages update rate	The Augmentation Control Centre provides correction messages to an update rate of 1Hz or 10 Hz
Rationale		
The rate of the correction messages sent by the Augmentation Control Centre to the OBUs is set to 1 Hz or 10 Hz, in order to fulfil HELMET service level requirements.		
Notes		
References		
SR-AUG-FUN-006		

ID	**Name**	**Description**
SR-AUG-OPE-013	2-Tiers Probability of missed detection	The 2-Tiers Probability of missed detection for the Augmentation System and the SIS is set to1e-4 or 1e-3
Rationale		
The Augmentation Control Centre implements the 2-Tiers integrity algorithms, whose Probability of missed detection is set in the range [1e-4, 1e-3].		
Notes		
References		
SR-AUG-OPE-001		

5.5 PRELIMINARY SELECTION OF SENSORS

In the context of HELMET project, the on-board system architecture and sensor fusion algorithms will be validated with real data collected in different scenarios for the different target applications (Automotive, railway, UAV).
In the following, we provide with some general requirements on the sensor specifications, synchronization, logging computer and interfacing that will be used during the project.

The specific sensors that will be needed to satisfy the user and OBU system requirements will be defined more in detail in D3.1. Nevertheless, within the context of HELMET, we foresee the recording of measurements from the following sensors:

Necessary sensors:

- GNSS Antenna and Receiver
- Inertial Measurement Unit (IMU)
- Camera
- Odometer (for automotive and railway) in case no other means of measuring odometry is provided (e.g. visual odometry using camera)

Optional sensors:

- Lidar
- Radar
- Additional GNSS Antenna and Receiver / Dual antenna receiver (GNSS heading)

In the following we detail the main requirements associated with each sensor if they are used as part of the MOBU (Multi-sensor On-Board Unit platform) recording unit:

5.5.1 GNSS Antenna and Receiver Requirements

GNSS antenna requirements:

- The antenna must support multifrequency with at least support for E1/L1 and E5\L5 and multiconstellation (GPS and Galileo at least)
- The antenna should support also E6 frequency when possible.
- The antenna must be active; cost-effective and must NOT contain advanced multipath rejection capabilities (e.g., choke ring type). Pre-filtering is acceptable.
- The antenna must be installed directly to a ground metal plane (e.g., to the roof) without edges closer to 1 wavelength of the most restrictive frequency (i.e., E5 with minimum 25.48 cm distance). Note: This is mainly relevant for automotive and railway. For small UAV this requirement cannot be typically achieved and the additional effects due to antenna installation must be handled at the signal processing or algorithm level.

GNSS receiver requirement:

- The GNSS receiver must support multifrequency-multiconstellation signal processing and raw code and carrier measurement generation.

- The GNSS receiver must not include advance multipath rejection capability or unknown smoothing processing to the pseudoranges (or this option must be completely deactivatable or revertible).
  - The GNSS receiver must be able to output Automatic Gain Control (AGC) values and Power Spectrum Density (PSD) information for the different bands. Instead of direct PSD values, the output of I-Q samples can be considered also an option.
  - The GNSS receiver should allow for the configuration of the tracking loops parameters or should be able to provide information about their specific values.
  - The GNSS receiver must allow to synchronize to an external clock source (e.g. 10MHz or PPS signal)
  - The GNSS receiver must allow to output of a PPS signal.
  - The GNSS receiver must be able to generate measurements at a rate up to 10 Hz.
  - The GNSS receiver must provide tracking channel status consisting at least of C/N0, and tracking loop state
  - Additional Receiver / Dual antenna receiver used should provide directly the GNSS heading information or relative rover position (e.g. ENU frame)

5.5.2 Inertial Measurement Unit Requirements

- The IMU must consist contain at least:
  - 3D orthogonal axis accelerometer
  - 3D orthogonal gyroscopes
  - Temperature sensor
- Optionally for automotive and railway, the “IMU” also contains a 3D magnetometer and a barometer sensor
- For UAV application, a barometer and magnetometer-based compass sensor must be available either as part of the IMU unit or as a separate sensor.
- The IMU sensor should be cost-effective and therefore typically based on MEMS technology.
- Some minimum performances of the IMU sensors should be:
  - Accelerometer in-run bias stability < 160 [micro-g]
  - Accelerometers noise density < 120 [micro-g/sqrtHz]
  - Gyroscope in-run bias stability < 10 [deg/h]
  - Gyroscope noise density < 15 [deg/hr/sqrtHz]
- The IMU sensor must be able to provide specific force and angular rates measurements at a frequency of at least 200Hz.

- The IMU sensor must be able to accept a synchronization/trigger signal
- The IMU sensor should be able to output a trigger signal

The IMU should be able to accept mis-alignment and calibration parameters and apply them internally before the measurement output.

5.5.3 Camera Requirements

- The camera must have a global shutter.

A rolling shutter will result in unsynchronized measurements on different pixels.

- The camera must be able to have a frame rate of at least 30 frames/second.

30 frames/second corresponds to approximately 2m travelled distance between two consecutive frames when the vehicle is as fast as 200km/h, so that the change of scenes is not significant between frames. Also, it ensures a short brake distance in emergency situations.

- The camera image sensor should provide quantum efficiency no less than 65%.

The quantum efficiency of the imaging sensor has influences on the dynamic range, noise, and low light performance of the camera. It depends on the type of sensor and the sensor size. A large sensor size is more important than high resolution for navigation purposes.

- The camera should be compliant with the IP67 standard.

The camera should be waterproof to provide measurements in different weather conditions.

- The camera sensor must accept an external trigger signal.

On the contrary to a commercial camera, the camera sensor must be able to be digitally triggered by an external signal, so that the measurements can be synchronized and aligned with other sensors including GNSS and IMU.

- The camera should have a datalink that supports the bandwidth required by the rest of the minimum requirements..

The datalink must be able to transfer generated data without filling out the buffer. For 30 frames of 1 megapixel image per second, the average data rate (not peak) must be larger than 90 MBytes/sec (assuming 3 channels - RGB). USB3 (maximum bandwidth 640 MB/sec) or GigE (maximum bandwidth 125 MB/sec) can provide the capability, while USB2.0 cannot. GigE ports are physically more stable than USB3 ports, and support PTP (Precision Time Protocol) synchronization. For 2megapixel resolution a USB3 datalink must be used to handle the data rate.

- The camera should be a color camera with possibility to reconfigure it to a direct grayscale output mode.

Color information can help in perception, recognition, and detection. For motion tracking grayscale images will be applied.

- The lens should be a fixed focal length lens that can be stably attached to the camera.

For machine vision the fixed focal length has advantages in calibration. The attachment to the camera must be mechanically stable.

- The lens must have at least 75° field of view horizontally and 60° vertically.

75° FOV corresponds to a covered range of about 1.5 m at a distance of one meter in front of the camera, and 60° FOV corresponds to a covered range of about 1 m.

- The lens distortion of the optical system must be less than 2%.

The distortion of the lens significantly affects the uncertainty of the geometric measurements, e.g., feature points locations, in the image plane.

- The camera sensor must have a minimum resolution of 1 megapixels for the above minimum field of view (the resolution should scaled up with the lens field of view).

For the above FOV, a 3m*2m size object (e.g., a car) in 500 meters away will take up 16 pixels for a 1 megapixel camera, and 32 pixels for a 2 megapixel camera. Low resolution may result in low detection capability. Significantly high resolution may result in unnecessary high computational costs.

- The lens must support the resolution.

The optics of the lens must support the sensor resolution; otherwise the lens resolution will become the bottleneck of the overall resolution.

- Digital adjustment (instead of mechanical) capability of changing aperture/focal distance of the lens will be preferred.

This is a preferred feature. The aperture adjustment is helpful when the lighting condition varies significantly (e.g., when driving inside/outside a tunnel). On most commercial lenses this adjustment is available through mechanics, e.g., a tuning ring. However, for machine vision it should be digitally available. If there is a mechanical adjustment ring, it must be sufficiently stable against shaking so that it will not affect the system in manoeuvres.

5.5.4 Odometer Requirements

For automotive and railway, the odometer provides additional input that can be included in the fusion. Generally, the sensor is more valuable for railway where its accuracy is higher thanks to the more stable environment (rail flatness, wheel radius variations).

- The odometer must provide travelled distance

- The accumulated distance error must be less than ± (5m + 5%) over travelled distance

The odometer system internally compensates for vehicle rotations or provides means to do it by the user. This can be achieved by monitoring multiple vehicle wheels simultaneously and reflecting the different radius based on the steering wheel rotation. Relevant especially for automotive.

- The odometer must provide measurements at rate 10Hz at minimum

- The odometer should provide velocity

- The velocity estimate should meet the accuracy requirements from D2.1 summarized below

  Rail

  - ± 2 km/h for speed lower than 30 km/h, then increasing linearly up to ± 12km/h at 500 km/h.

  Automotive

  - The indicated speed must never be less than the actual speed, i.e. it should not be possible to inadvertently speed because of an incorrect speedometer reading.
  - The indicated speed must not be more than 110 percent of the true speed plus 4 km/h at specified test speeds. For example, at 80 km/h, the indicated speed must be no more than 92 km/h.

- The odometer should provide acceleration
- The acceleration g-range should be at least ±1g

Acceleration from 0 to 100km/h in 3seconds is equal to approximately 1g.

The acceleration estimate should meet the accuracy ±5%

5.5.5 LIDAR Requirements

One use case for Lidar is to validate the visual odometry, It enables to verify in the region of interest the visual odometry under harsh conditions (e.g. dark) and to test the decision criteria when the visual odometry claims operation / no operation.

- Minimum filed-of-view (FOV) must be at least 75° horizontal and 20° vertical

Horizontal FOV is identical to the camera, whereas vertical is reduced to enable usage of Lidar at reasonable cost.

- Lidar must provide at 100 klx sunlight detection range (detection probability >= 90% and false alarm rate <= 0.01%) at least 100m for 80% reflectivity and at least 30m for 10% reflectivity

Long range enables to detect more objects, although due to angular resolution constraints the granularity decreases at longer ranges. 100m is a good trade-off.

- Angular resolution must be less than 0.2° horizontal and less than 2.2° vertical.

Angular resolution of 0.2° translates to about 7cm at the distance 20m and 35cm at the distance 100m.

Angular resolution of 2.2° translates to about 0.8m at the distance 20m and 3.5m at the distance 100m.

- Range precision (1σ @ 20m) must be at least 3cm and angular precision (1σ) must be less than 0.1°

Centimeter level precision is required to provide better or similar accuracy as the visual odometry.

- Minimum update rate must be at least 10Hz assuming at least 50% FOV coverage

Fast update rate improves resolution at higher vehicle speed. 10Hz corresponds to approximately 1.4m travelled distance between two consecutive scans when the vehicle is as fast as 50km/h.

- The lidar must be possible to synchronize to the external clock source.

Simplifies synchronization and alignment with other sensors including GNSS, IMU and camera.

- The lidar should be compliant with the IP67 standard.

The lidar should be waterproof to provide measurements in different weather conditions.

5.5.6 Radar Requirements

The benefit of radar in this project is a prominent support in identification, tracking and filtration of dynamic objects.

- The distance range of radar must cover (0.2m – 100m) at least

Objective is to identify pedestrians and other vehicles.

- The FOV must be at least 15° horizontally and 10° vertically.

A longer range comes typically with a smaller FOV. This is a good trade-off.

- The radar must provide measurements at rate at least 15Hz.
- The distance accuracy should be no greater than ±0.5m.
- The radar must provide measurements at rate at least 15Hz.
- The radar must be able to identify dynamic objects moving faster than 0.5m/s (about 2km/h)

Pedestrians are the slowest member of the traffic. Typical pedestrian velocity is about 4km/h.

- The angle resolution must be no more that ±0.3°.
- The radar must be able to track objects at velocities of ±200km/h

This should allow to track even fast-moving objects e.g. vehicles on highway.

- The radar must be able to track at least 64 dynamic objects.
- The radar should support a CAN interface for communication.

CAN interface is the most common one for any reasonably affordable radar on the market.

- The radar should be possible to synchronize to the external clock source.

Simplifies synchronization and alignment with other sensors including GNSS, IMU and camera.

- The radar should be compliant with the IP67 standard.

The sensor should be waterproof to provide measurements in different weather conditions.

5.6 PRELIMINARY SPECIFICATION OF RECORD / PLAYBACK UNIT

Record and Playback unit enables to the project members to record raw sensor data and playback them later. The main benefits of Record and Playback unit are

- Enable algorithm development using real sensor data
- Bring repeatability to the test environment.

5.6.1 Timing and Synchronization Requirements

Regarding the time related requirements for the recording unit, we must make the distinction of two different but important aspects:

- **Timestamping**: It relates each specific sensor measurement with a certain time in a specific common time reference system. The availability of a timestamp for each measurement allows for the correct ordering in time of the recorded measurements.
- **Measurement alignment**: Since different sensors may produce measurements at different rates, the measurements of two sensors are considered aligned when for a given sensor 'a' with measurement frequency f_s^a, and a given sensor 'b' with f_s^b with $f_s^a \geq f_s^b$, whenever there is a measurement of sensor 'b' at a certain time t_k^b, there is also a measurement of sensor 'a' at time $t_k^b = t_{k+l}^a$ with $l \in \mathbb{Z}$.

The related timing requirements are:

- The timestamping of all sensor measurements must be performed with respect to the same common time frame with a minimum accuracy of 1µs.

  This is driven by the requirement in D2.2 which states that for automotive the timing accuracy must be < 1 µs.

- The alignment of measurements from accelerometer, gyroscope (and magnetometer when applicable) must be ensured.

  Note: this is typically guaranteed if the sensors belong to the same inertial unit.

- The alignment of measurements from multiple cameras or IMUs (if available) must be guaranteed. When possible, this requirement should be extended to multiple LIDAR or Radars.
- When possible or applicable, the alignment of all sensor measurements should be provided between them.
- For sensors that do not support time synchronization, the recording system must provide the time of measurement arrival

Note: this is typically problem of build-in odometers and radars. The timing inaccuracy should be considered by the positioning system.

5.6.2 Logging Requirements

We need to distinguish two different times for each measurement:

- **Time of measurement** is the time when the measurement has been created.
- **Time of availability** is the time when the measurement became available to the system. It is a bit later than the Time of measurement. The delay between Time of measurement and Time of availability is different for each sensor and can vary over time.

Logging requirements

- The recording unit must be able to record at least 60 min of sensor data

The largest contributors to required space are camera and lidar. Assuming 2x camera = 400MB/min (compressed) and lidar = 550MB/min, we get that the sensor system generates about 1GB/min.

- The recording unit must be able to record data at least from the following sensors:
  - GNSS receiver recording at least GNSS raw measurements (code, carrier, Doppler and CN0) + tracking status + navigation message for all in-view GPS (L1/L5) and Galileo satellites (E1, E5a+b) in the same format as the receiver
  - IMU raw data in the same format as the sensor
  - 2x Camera in a compressed format (H.264 or VP8)

- The recording unit should be able to record raw data from AIMN

Although AIMN receiver is not a sensor itself, it is and important functional block in the MOBU improving the integrity of the navigation solution. AIMN provides MOBU RTCM Augmentation messages that the GNSS receiver must apply in RTK mode. AIMN calculates constellations, satellites and Reference Receivers Integrity masks that the receiver can apply for enabling or disabling relevant faulty sources, which are transmitted using RTCM NTRIP Protocol and integrity masks RTCM messages defined within the RSAT project. For the proof-of-concept the AIMN data could be provided as part of post-processing activity.

- The recording unit must provide for each measurement two timestamps using the same master clock as all sensors
  - Time of measurement
  - Time of availability
- The recording unit shall be able to record data on mounted drive.

This hard drive can be taken to the lab to download the data.

- The recorded trace should contain metadata (configuration and date of record at least).

5.6.3 Playback Requirements

- Playback system must enable user to select recorded trace to be replayed
- Recorded data must be replayed in way that the consumer will not have to differentiate between live data and playback data

This simplifies the development and testing.

- Playback system must order the sensor data according to its time of availability to the system

- Playback system should HW accelerate video playback (support at least Nvidia and Intel accelerators)
- Playback system must support Seek functionality when the whole processing chain must remain synchronized
- Playback system must support control mechanism: Play, Stop, Pause
- Playback system should support Step functionality when the system plays user defined time frame (e.g. 200ms)
- Playback system should support Slow and Fast motion.

5.6.4 Visualization Requirements

Visualization of data simplifies the development and testing. The engine will visualize output of customizable workers (filters), where each worker represents one data stream (e.g. lidar data, position solution, …)

- The visualization engine must visualize outputs of customizable workers (filters)

Note: time synchronization of various workers is out of scope of visualisation.

- The visualization engine must enable user to turn on/off individual layers

Layer is an output of one or multiple combined workers (e.g. lidar scanpoints).

- The visualization engine must provide UI for the Playback control mechanisms
  - *Recorded trace selection*
  - *Play, Stop, Pause*
  - *Seek*
  - *Slow and Fast motion*
- The visualization engine must provide information about the relative time in the replayed trace
- The visualization engine should provide metadata of the replayed trace (date, trace length, sensor set and their versions, configurations…)

5.6.5 Physical and Environmental Requirements

This set of requirements describes the MOBU (Multi-sensor On-Board Unit platform) platform environmental and physical requirements relevant to the project, not necessarily to the final product. The platform consists of sensors and the recording unit.

- The platform should operate in the temperature range -20°C to 55°C
- The platform should operate under standard vehicle vibration conditions
- The platform should support 4x Ethernet, 3x UART, 1x CAN at least

This enables to add additional sensors. For example, to connect a high grade IMU as a source of ground true, or input of AIMN integrity data

- The platform should not exceed the lateral and longitudinal dimensions of the vehicle it is mounted on
- The platform should be portable by two persons at maximum.

5.6.6 MOBU Record Unit Architecture

The preliminary architecture of the MOBU (Multi-sensor On-Board Unit platform) record unit is shown in the Figure 73 below. The system consists of accurate time source, which is used to discipline all sensors using various synchronization protocols (PPS, PTP, 10MHz clock, external Trigger).

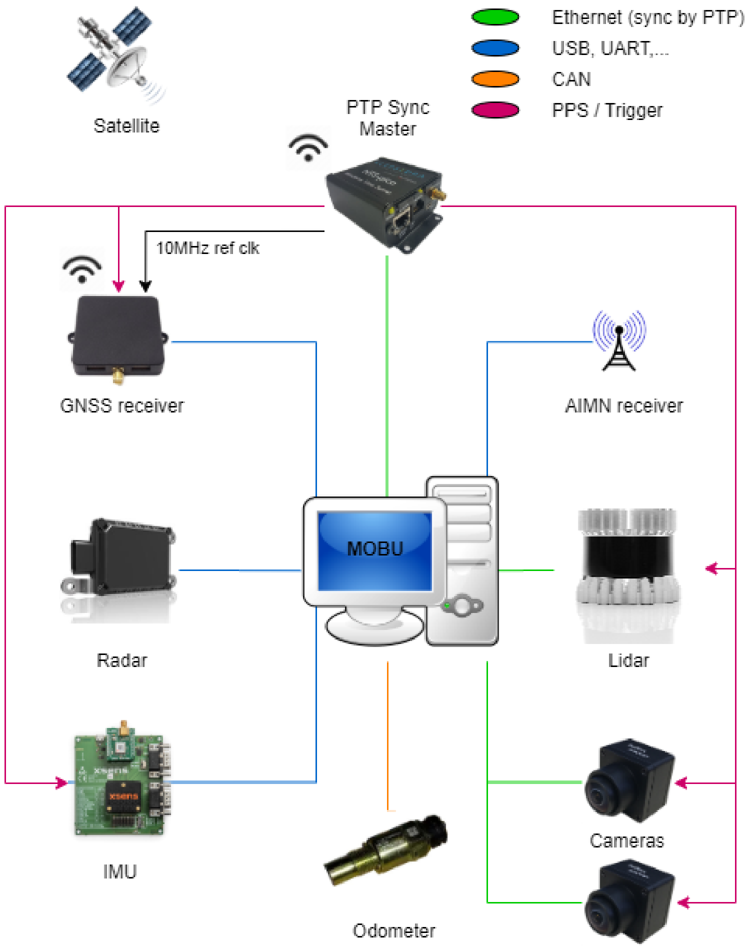


Figure 73. Sensor and Recording unit architecture

6. HIGH-LEVEL HELMET ARCHITECTURE WITH KEY SAFETY MEASURES ALLOCATION

The allocation of Safety Requirements to High-level Architectural components is reported in

Figure 74. The high-level architecture reported in Figure 31 has been considered as a reference.

Allocation considered as negligible or embedded in other components have been removed from RAIL / AUTO and UAV requirements have been divided and grouped by relevant components.

The impact of the same Faults (e.g. SIS) on different architectural components has been coherently assigned, taking into account different Probabilities of missed detection.

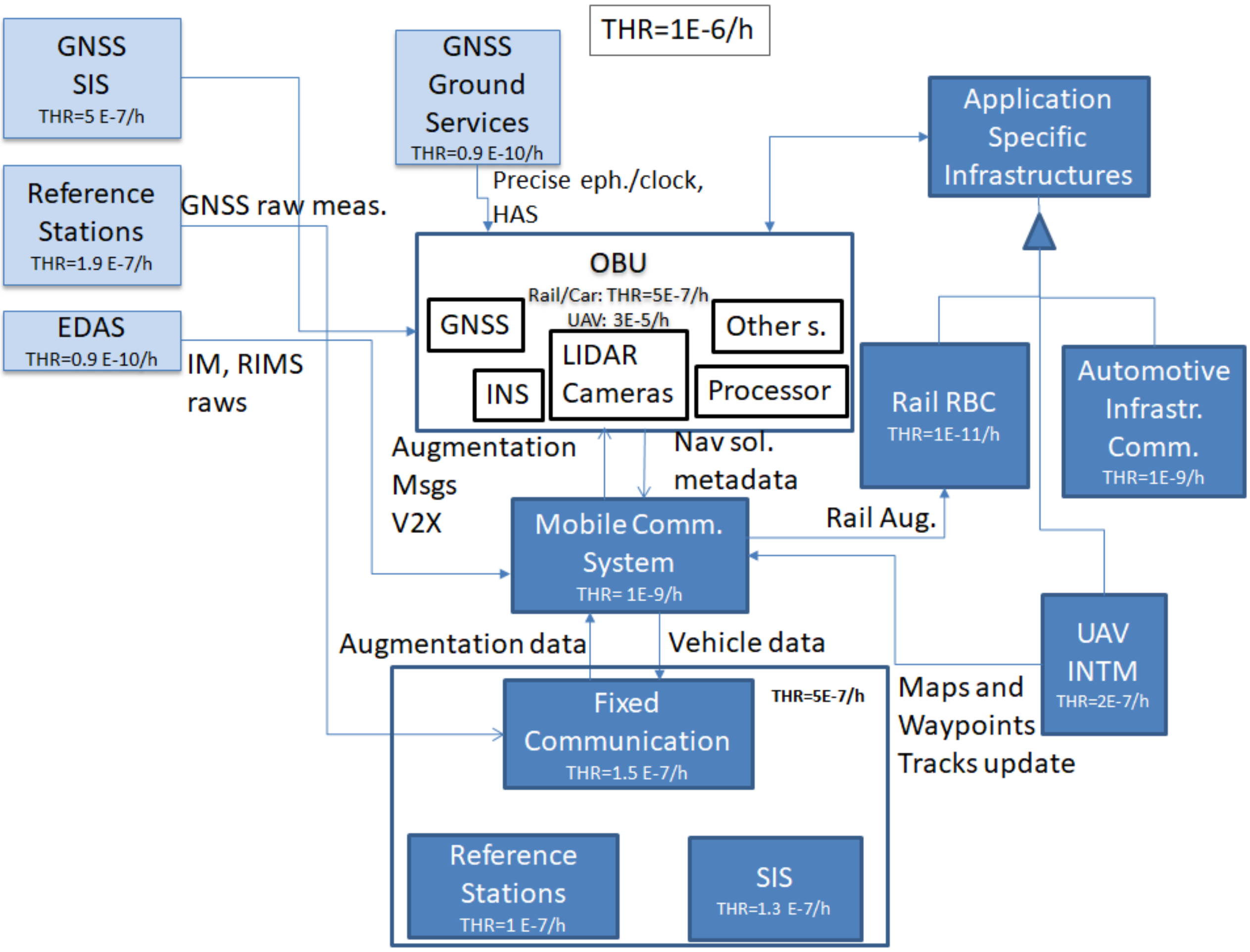


Figure 74. Allocation of key safety measures to Architectural Components

7. REQUIREMENTS TRACEABILITY MATRICES (RTMs) FOR MULTI-MODAL APPLICATIONS

This section includes Requirements Traceability Matrix (RTM) for RAIL, AUTO and UAV/ UAS applications. The RTM is a table which maps User Requirements and related System Requirements.

7.1 RTM FOR RAIL APPLICATIONS

This subsection includes Requirements Traceability Matrix (RTM) for RAIL applications.

REQUIREMENTS TRACEABILITY MATRIX - RAIL			
Project Name: HELMET			
User Requirements		System Requirements	
User Requirement ID#	**User Requirement / Use Case**	**System Requirement ID#**	**System Requirement / Use Case**
UR_001	Track identification	SR-OBU-SAF-001.a	Tolerable Hazard Rate of Virtual Balise subsystem hazard (VBTX)
		SR-OBU-SAF-002.a	Tolerable Hazard Rate of Virtual Balise insertion (TRANS-VBALISE-3)
		SR-OBU-SAF-003.a	Tolerable Hazard Rate of Virtual Balise insertion across track
		SR-OBU-SAF-004.a	Tolerable Hazard Rate of Virtual Balise insertion along track
		SR-OBU-SAF-005.a	Alert Limit (AL) across track related to Track identification
		SR-OBU-PER-006.a	Accuracy of train position determination across track (2*sigma) for Track identification
		SR-OBU-FUN-007.a	Time to Alert (TTA) related to Track identification
		SR-OBU-SAF-008.a	Tolerable Hazard Rate of Message corruption related to Virtual Balise detection
		SR-OBU-COM-009.a	Communication delay related to Virtual Balise detection
UR_002	Odometry calibration	SR-OBU-FUN-010.a	Accuracy of train position determination along track (2*sigma) related to Odometry calibration
		SR-OBU-SAF-011.a	Alert Limit (AL) along track related to Odometry calibration
		SR-OBU-SAF-012.a	Time to Alert (TTA) related to Odometry calibration
UR_003	Cold movement detection	SR-OBU-SAF-013.a	Alert Limit (AL) along track related to Cold movement detection
		SR-OBU-FUN-014.a	Accuracy of train position determination across track

			(2*sigma) related to Cold movement detection
		SR-OBU-SAF-015.a	Time to Alert (TTA) related to Cold movement detection
UR_001 UR_002 UR_003	Track identification Odometry calibration Cold movement detection	SR-OBU-SAF-016.a	Safety Integrity level of train position determination function
UR_001 UR_002 UR_003	Track identification Odometry calibration Cold movement detection	SR-OBU-PER-017.a	Dependability of position determination function
UR_001 UR_002 UR_003	Track identification Odometry calibration Cold movement detection	SR-OBU-SEC-018.a	Security of position determination
UR_007	Speed accuracy for ERTMS	SR-OBU-SAF-019.a	Speed accuracy for ERTMS

7.2 RTM FOR AUTO APPLICATIONS

This subsection includes Requirements Traceability Matrix (RTM) for AUTO applications.

REQUIREMENTS TRACEABILITY MATRIX - AUTO			
Project Name: HELMET			
User Requirements		**System Requirements**	
User Requirement ID#	**User Requirement / Use Case**	**System Requirement ID#**	**System Requirement / Use Case**
UR_004 UR_005 UR_006	Automated driving on highway, local roads and narrow and curved roads	SR-OBU-SAF-101.a	Automotive Safety Integrity Level (ASIL) for car position determination
UR_004 UR_005 UR_006	Automated driving on highway, local roads and narrow and curved roads	SR-OBU-SAF-116.a	Alert Limit (lane) for automated driving
UR_004 UR_005 UR_006	Automated driving on highway, local roads and narrow and curved roads	SR-OBU-PER-108.a	Accuracy (2*sigma) of lane identification
UR_004	Automated driving on highway; velocity 80-130 km/hr	SR-OBU-SAF-102.a	Alert Limit (lateral) for automated driving on highway
		SR-OBU-PER-103.a	Accuracy (2*sigma, lateral) of position determination related to driving on highway
		SR-OBU-SAF-117.a	Alert Limit (longitudinal) for automated driving on highway
		SR-OBU-PER-108.a	Accuracy (2*sigma, longitudinal) of position determination related to driving on highway
		SR-OBU-PER-109.a	System Reaction Time related to driving on highway
UR_005	Automated driving on local roads; velocity 60-90 km/ hr	SR-OBU-SAF-104.a	Alert Limit (lateral) for automated driving on local roads

		SR-OBU-PER-105.a	Accuracy (2*sigma) of position determination related to driving on local roads
		SR-OBU-SAF-118.a	Alert Limit (longitudinal) automated driving on local roads
		SR-OBU-PER-110.a	Accuracy (2*sigma, longitudinal) of position determination related to automated driving on local roads
		SR-OBU-PER-111.a	System Reaction Time related to driving on local roads
UR_006	Automated driving on narrow and curved roads; velocity 20-60 km/ hr	SR-OBU-SAF-106.a	Alert Limit (lateral) for automated driving on narrow and curved roads
		SR-OBU-PER-107.a	Accuracy (2*sigma) of position determination related to driving on narrow and curved roads
		SR-OBU-SAF-119.a	Alert Limit (longitudinal) automated driving on narrow and curved roads
		SR-OBU-PER-112.a	Accuracy (2*sigma, longitudinal) of position determination related to automated driving on narrow and curved roads
		SR-OBU-PER-113.a	System Reaction Time related to driving on narrow and curved roads
UR_004 UR_005 UR_006	Automated driving on highway, local roads and narrow and curved roads	SR-OBU-SAF-108.a	Time-to-Alert
UR_004 UR_005 UR_006	Automated driving on highway, local roads and narrow and curved roads	SR-OBU-FUN-109.a	Timing Accuracy (It can also affect safety)
UR_004 UR_005 UR_006	Automated driving on highway, local roads and narrow and curved roads	SR-OBU-SAF-110.a	Availability of car localization (It can have direct impact on safety)
UR_004 UR_005 UR_006	Automated driving on highway, local roads and narrow and curved roads	SR-OBU-SEC-111.a	Security of car localization
UR_008	Speed accuracy	SR-OBU-SAF-112.a	Speed accuracy (direct impact on safety)
UR_004 UR_005 UR_006	Automated driving on highway, local roads and narrow and curved roads	SR-OBU-SAF-113.a	Harmonized Design Target for SDC safety systems
UR_004 UR_005 UR_006	Automated driving on highway, local roads and narrow and curved roads	SR-OBU-SAF-114.a	Probability of Failure of car localization
UR_004 UR_005 UR_006	Automated driving on highway, local roads and narrow and curved roads	SR-COM-SAF-115.a	Probability of Failure of Communications used for car localization
UR_004 UR_005 UR_006	Automated driving on highway, local roads and narrow and curved roads	SR-COM-SAF-120.a	Continuity of car localization

7.3 RTM FOR UAVs APPLICATIONS

This subsection includes Requirements Traceability Matrix (RTM) for UAVs applications.

REQUIREMENTS TRACEABILITY MATRIX - UAV			
Project Name: HELMET			
UAV APPLICATION User Requirements		UAV APPLICATION System Requirements	
User Requirement ID#	**User Requirement / Use Case**	**System Requirement ID#**	**System Requirement / Use Case**
2.3.1 / 2.3.2	Societal Safety Requirements for UAV/RPAS Inserted in ECAC's Airspace. User High Level Risk and Safety Requirement for UAS/RPAS	UAS-SYS-SAF-REQ-01 UAS-SYS-SAF-REQ-02 UAS-SYS-SAF-REQ-03 UAS-SYS-SAF-REQ-04 UAS-SYS-SAF-REQ-05 UAS-SYS-SAF-REQ-06 UAS-SYS-SAF-REQ-07 UAS-SYS-SAF-REQ-08 UAS-SYS-SAF-REQ-09 UAS-SYS-OPE-REQ-022 UAS-SYS-OPE-REQ-023 UAS-SYS-OPE-REQ-024 UAS-SYS-OPE-REQ-025 UAS-SYS-OPE-REQ-026	Safety requirement for Rail and Road applications Safety requirements for the IMTM UAS/RPAS railway and road operations and use cases shall need to consider a range of physical and operational safety controls, The UAS/RPAS-PIT STATION shall be designed to minimise system degradation and/or failures The UAS/RPAS operators should be made aware of critical system failures or unsafe conditions There should be adequate means to maintain situational awareness of the UA/RPA and its surroundings (both in the air and on the ground). In accordance with EASA limits, the IMTM UAS/RPAS flight operations shall not be less than 30 m from humans. The UAV/RPAS characteristics shall reduce to maximum the likelihood that during operations in the prospected mission scenarios will allow the injury of people, damages to property or damages to another aircraft and/or vehicles

2.3.3	High-Level User Requirements for UAS/RPAS-PIT and IMTM Services	UAS-SYS-OPE-REQ-01	The UAS/RPAS-PIT shall support all and/or selected Rail and Automotive Assets by providing, Monitoring and Traffic Management (IMTM) operational services in scenarios related to Open Sky,
		UAS-SYS-OPE-REQ-028	Restricted Regional/Sub-Urban, and Urban Local Operational Environments The UAS/RPAS-PIT Station shall be dedicated to the following Inspection, Monitoring and Traffic Management (IMTM) (Ref. to OPE-REQ-01) operational tasks and specific applications for……
		UAS-SYS-OPE-REQ-029	The dedicated use of the UAS/RPAS-PIT Station Highly Integrated System Network within the HELMET infrastructure shall provide to the Users with benefits
		UAV-SYS-FUN-REQ-02	The UAS/RPAS shall provide functional capabilities to support and/or enable operations primarily for rail and road IMTM applications.
		UAV-SYS-FUN-REQ-02	There shall be at least four(4) UAS/RPAS main functions available for operations for rail and road IMTM applications, namely: 1) Avoid Hazards 2) Communicate 3) Navigate 4) Control

2.3.3.1	High Level UAS/RPAS User Operational Requirements	UAS-SYS-OPE-REQ-04 UAS-SYS-OPE-REQ-05 UAS-SYS-OPE-REQ-06 UAS-SYS-OPE-REQ-07 UAS-SYS-OPE-REQ-08 UAS-SYS-OPE-REQ-09 UAS-SYS-OPE-REQ-010 UAS-SYS-OPE-REQ-011	The integration of UAS/RPAS shall not imply a significant impact on the current users of the airspace. The UAS/RPAS-PIT shall cover all Very Low Level (VLL) airspace UTM classes The UAS/RPAS-PIT operations shall comply with existing and future Civil Aviation Regulations and Procedures including those dedicated to UTM. The UAS/RPAS shall be able to comply with ATM/UTM air traffic control rules/procedures During operations if the UA/RPA loses communications or loses its GNSS NAV signal or both (CNPC Link Failure), then it shall be capable to return to a predetermined location within the planned operating area and land on the closest PIT-Station
		UAS-SYS-OPE-REQ-023 UAS-SYS-OPE-REQ-027	When the UAV/RPAS system operates at the proximity to aerodromes or restricted/segregated airspace shall not increase the likelihood of a collision with other airspace or ground users and their assets.
		UAS-SYS-OPE-REQ-030	For the specific Inspection, Monitoring and Traffic Management (IMTM) operations, the employed UAS/RPAS shall be compliant to all relative Rules of the Air Requirements as being imposed by EASA Regulations
		UAS-SYS-OPE-REQ-031	The IMTM UAS/RPAS for railway and road applications shall be expected to operate within a range of operational constraints as per D2.2 subsection 3.3.2,

2.3.3.2	Overall IMTM UAS/RPAS Physical, Functional and Operational Performance High Level User Requirements	UAS-SYS-OPE-REQ-02 UAS-SYS-OPE-REQ-03 UAS-SYS-OPE-REQ-012 UAS-SYS-OPE-REQ-015 UAS-SYS-OPE-REQ-017 UAS-SYS-OPE-REQ-018 UAS-SYS-OPE-REQ-019 UAS-SYS-OPE-REQ-020 UAS-SYS-OPE-REQ-021 UAS-SYS-OPE-REQ-032 UAS-SYS-OPE-REQ-033 UAS-SYS-OPE-REQ-034 UAS-SYS-OPE-REQ-035 UAS-SYS-OPE-REQ-036 UAS-SYS-OPE-REQ-037 UAS-SYS-OPE-REQ-038 UAS-SYS-OPE-REQ-039	The Operational Characteristics of the UAS/RPAS shall be those of ≤25kg Max.Take-off Mass (MTOM) under the EASA Categories Specific and Certified A series of PIT station deployed all along the service areas shall provide support to all Aerial Operation and mission Profile of the UAV/RPAS The UAS/RPAS shall be capable to operate in the operational modes in accordance with EASA Rules, The UAS/RPAS system shall be adaptive to changes in the conditions of the command and control link. The UAS/RPAS-PIT Station Segment shall be capable of supporting multiple users (Rail and Automotive) simultaneously making an efficient use of the available resources. The entire operational UAS/RPAS-PIT Station Scenarios shall involve the following Framework Components for all Railway and Road IMTM Applications, as per D2.2 subsection 3.3.4 Flight Operative Modes shall be Applicable to IMTM UAS/RPAS Operations in accordance with D2.2 subsection 3.3.6: In defining the details of the Detailed Physical and Functional UAS/RPAS-PIT Station Segment Architecture shall be considered but not limited to the Operational Scenarios found in D2.2 subsection 3.3.7 Operator plan and operations

		UAS-SYS-OPE-REQ-040	SW/HW functionality
		UAV-SYS-FUN-REQ-03	Avoid Hazards Function
		UAS-SYS-FUN-REQ-04	Communicate Function
		UAS-SYS-FUN-REQ-05	Navigate Function
		UAS-SYS-FUN-REQ-06	Control Function
		UAS-SYS-FUN-REQ-07 UAS-SYS-FUN-REQ-08 UAS-SYS-FUN-REQ-09 UAS-SYS-FUN-REQ-10 UAS-SYS-FUN-REQ -11 UAS-SYS-FUN-REQ -12 UAS-SYS-FUN-REQ -13 UAS-SYS-FUN-REQ -14 UAS-SYS-FUN-REQ -15 UAS-SYS-FUN-REQ -16 UAS-SYS-FUN-REQ -17 UAS-SYS-FUN-REQ -18 UAS-SYS-FUN-REQ -19 UAS-SYS-FUN-REQ -20 UAS-SYS-FUN-REQ -21 UAS-SYS_-FUN-REQ-22 UAS-SYS-FUN-REQ -23 UAS-SYS-FUN-REQ -24 UAS-SYS-FUN-REQ -25 UAV-SR-FUN-REQ -26 UAS-SYS -FUN-REQ -27	Detection & Avoidance

		UAS-SYS FUN-REQ -28	
		UAS-SYS -FUN-REQ -29 UAS-SYS -FUN-REQ -30 UAS-SYS -FUN-REQ -31 UAS-SYS -COM-REQ -32 UAS-SYS -COM-REQ -33	UTM
		UAS-SYS -COM-REQ -34 UAS-SYS -COM-REQ -35 UAS-SYS -COM-REQ -36	Communication with vicinity and operators
		UAS-SYS -FUN-REQ -37	On board avionics for navigation with SBS/GBAS
		UAS-SYS -FUN-REQ -38	On board avionics for navigation with VBN
		UAS-SYS-FUN-REQ -39	COTS technologies requirement
		UAS-SYS -FUN-REQ -40	PIT station data relay vs operator
		UAS-SYS -FUN-REQ -41 UAS-SYS -FUN-REQ -42 UAS-SYS -FUN-REQ -43 UAS-SYS -FUN-REQ -44 UAS-SYS -FUN-REQ -45 UAS-SYS -FUN-REQ -46 UAS-SYS -FUN-REQ -48 UAS-SYS -FUN-REQ -49 UAS-SYS -FUN-REQ -50	UAS/RPAS navigation operation & UTM support

		UAS-SYS -FUN-REQ -51	The Required Navigation Performance (RNP) Navigation, the UAS/RPAS Steer Along Path Function shall be able to monitor the achieved navigation performance and to identify to the GCS whether the operational requirement is, or is not, being met during an operation
		UAS-SYS -FUN-REQ -52 UAS-SYS -FUN-REQ -53 UAS-SYS -FUN-REQ -54 UAS-SYS -FUN-REQ 55 UAS-SYS -FUN-REQ -56 UAS-SYS FUN-REQ -57 UAS-SYS -FUN-REQ -58	Navigate function vs loaded data, compatibility validation
		UAS-SYS -FUN-REQ -59 UAS-SYS -FUN-REQ -60 UAS-SYS -FUN-REQ -61 UAS-SYS -FUN-REQ -62 UAS-SYS -FUN-REQ -63 UAS-SYS -FUN-REQ -64 UAS-SYS -FUN-REQ -65 UAS-SYS -FUN-REQ -66 UAS-SYS -FUN-REQ -67 UAS-SYS -FUN-REQ -68 UAS-SYS -FUN-REQ -69 UAS-SYS -FUN-REQ -70 UAS-SYS -FUN-REQ -71 UAS-SYS -FUN-REQ -72 UAS-SYS -FUN-REQ -73 UAS-SYS -FUN-REQ -74 UAS-SYS -FUN-REQ -75 UAS-SYS -FUN-REQ -76 UAS-SYS -FUN-REQ -77 UAS-SYS -FUN-REQ -78	Control functions vs flight operations

		UAS-SYS -FUN-REQ -79 UAS-SYS -FUN-REQ -80	
		UAS-SYS -FUN-REQ -81 UAS-SYS -FUN-REQ -82	Flight Planning functions
		UAS-OBU-FUN-REQ-100	OBU avionics shall support any operative mode and mission classes envisaged for Helmet applications
		UAS -OBU -FUN-REQ-101	OBU equipment’s
		UAS-OBU- FUN-REQ-102 UAS-OBU-FUN-REQ-103 UAS-OBU-FUN-REQ-104 UAS-OBU-FUN-REQ-105 UAS-OBU-FUN-REQ-106 UAS-OBU-NAV-REQ-107 UAS-OBU-AUG-REQ-108 UAS-OBU-AUG-REQ-109 UAS-OBU-AUG-REQ-110 UAS-OBU-AUG-REQ-111 UAS-OBU-FUN-REQ-112 UAS-OBU-FUN-REQ-113	OBU Capabilities and functionalities
		UAS-PIT-FUN-REQ-83 UAS-PIT-FUN-REQ-84 UAS -PIT- AUG-REQ-85 UAS-PIT-FUN-REQ-86	PIT station function requirement

		UAS-PIT-FUN-REQ-87 UAS-PIT-FUN-REQ-88 UAS-PIT-FUN-REQ-89 UAS-PIT FUN-REQ-90 UAS-PIT-FUN-REQ-91 UAS-PIT-FUN-REQ-92 UAS-PIT-FUN-REQ-93 UAS-PIT-FUN-REQ-94 UAS-PIT-FUN-REQ-95	
		UAS-EXT-PER-REQ-01 UAS-EXT.PER-REQ-02 UAS-EXT-PER-REQ-03	UAV typologies for Rail and Road Helmet service

2.3.3.3	User Spectrum CNPC High Level Requirements for Small IMTM- UA/RPA to be Supported for HELMET Operations	UAS-COM-PER-REQ-04 UAS-COM-PER-REQ-05 UAS-COM-PER-REQ-06 UAS-COM-PER-REQ-07 UAS-COM-PER-REQ-08 UAS-COM-PER-REQ-09 UAS-COM-PER-REQ-10 UAS-COM-PER-REQ-11 UAS-COM-PER-REQ-12 UAS-COM-PER-REQ-13 UAS-COM-PER-REQ-14 UAS-COM-PER-REQ-15 UAS-COM-PER-REQ-16	Communication requirement Availability Latency Transaction Continuity BW
		UAS-COM-PER-REQ-17 UAS_COM-PER-REQ-20 UAS-COM-PER-REQ-21 UAS-COM-PER-REQ-22	Spectrum requirement form ITU Comm sub-segment performance requirement
2.3.3.4	High-Level User EGNSS Performance Requirements for UAS/RPAS IMTM Operations	OBU /PIT Station & HCC requirement UAS-PIT-FUN-REQ-XX UAS-OBU-FUN-REQ-XX	

2.3.3.5	Summary of High-Level User GNSS Requirements for UAS/RPAS-PIT Operations	UAS-AUG-PER-REQ-18 UAS-AUG-PER-REQ-19 UAS-EXT-AUG-REQ-XX UAS-OBU-FUN-REQ-XX	All User requirement are embedded in UAV system design HCC data OBU processing
En-route	**UR_009**		
	Accuracy H/V	OBU + PIS+ SBAS	OBU based on SBAS
	integrity	UAS-EXT-AUG-REQ-XX UAS-OBU-FUN-REQ-XX	SBAS+ARAIM+ABIA+PITS
	TTA	UAS-EXT-AUG-REQ-XX UAS-OBU-FUN-REQ-XX	OBU
Arrival (Landing)	**UR_010**		
	Accuracy H/V	UAS-PIT-FUN-REQ-95 UAS-OBU-FUN-REQ-114 UAS-OBU-FUN-REQ-112	Visual support landing in combination with HCC shall provide PPP-RTK and DGNSS data

	Integrity	UAS-EXT-AUG-REQ-XX UAS-PIT-FUN_RQ-XX UAS-OBU-FUN-REQ-XX	OBU VBN+ABIA+PITS
	TTA	UAS-EXT-AUG-REQ-XX UAS-OBU-FUN-REQ-XX	
Approach,	**UR_011**		
	Accuracy H/V	UAS-PIT-FUN-REQ-95 UAS-OBU-FUN-REQ-114 UAS-OBU-FUN-REQ-112	OBU + PIS+ SBAS
	Integrity	UAS-EXT-AUG-REQ-XX UAS-PIT-FUN_RQ-XX UAS-OBU-FUN-REQ-XX	
	TTA	UAS-EXT-AUG-REQ-XX UAS-OBU-FUN-REQ-XX	
Departure (Take-off)	**UR_012**		
	Accuracy	UAS-PIT-FUN-REQ-95 UAS-OBU-FUN-REQ-114 UAS-OBU-FUN-REQ-112	
	Integrity	UAS-EXT-AUG-REQ-XX UAS-PIT-FUN_RQ-XX UAS-OBU-FUN-REQ-XX	
	TTA	UAS-EXT-AUG-REQ-XX UAS-OBU-FUN-REQ-XX	
Field Approach Operations	**UR_013**		
	Accuracy H/V	UAS-PIT-FUN-REQ-95 UAS-OBU-FUN-REQ-114 UAS-OBU-FUN-REQ-112	

	Integrity	UAS-EXT-AUG-REQ-XX UAS-PIT-FUN_RQ-XX UAS-OBU-FUN-REQ-XX	
	TTA	UAS-EXT-AUG-REQ-XX UAS-OBU-FUN-REQ-XX	
Precision Approach (PIT Station Approach)	**UR_013**		
	Accuracy H/V	UAS-PIT-FUN-REQ-95 UAS-OBU-FUN-REQ-114 UAS-OBU-FUN-REQ-112	
	Integrity	UAS-EXT-AUG-REQ-XX UAS-PIT-FUN_RQ-XX UAS-OBU-FUN-REQ-XX	
	TTA	UAS-EXT-AUG-REQ-XX UAS-OBU-FUN-REQ-XX	

7.4 RTM FOR GNSS AUGMENTATION NETWORK

This subsection includes Requirements Traceability Matrix (RTM) for GNSS Augmentation Network intended for the HELMET multi-modal applications.

REQUIREMENTS TRACEABILITY MATRIX – MULTI-MODAL AUGMENTATION SYSTEM			
Project Name: HELMET			
User Requirements		System Requirements	
User Requirement ID#	**User Requirement / Use Case**	**System Requirement ID#**	**System Requirement / Use Case**
UR_001 UR_002 UR_004 UR_005 UR_006 UR_007 UR_008	Track Identification Odometry calibration Automated driving on highway, local roads and narrow and curved roads Speed accuracy for ERTMS Speed accuracy for Auto	SR-AUG-OPE-001	Augmentation System Fault Detection and Exclusion THR
UR_001 UR_002 UR_004 UR_005 UR_006 UR_007 UR_008	Track Identification Odometry calibration Automated driving on highway, local roads and narrow and curved roads Speed accuracy for ERTMS Speed accuracy for Auto	SR-AUG-PER-002	Augmentation System THR
UR_001 UR_002 UR_004 UR_005 UR_006 UR_007 UR_008	Track Identification Odometry calibration Automated driving on highway, local roads and narrow and curved roads Speed accuracy for ERTMS Speed accuracy for Auto	SR-AUG-FUN-003	Augmentation messages contents
UR_001 UR_002 UR_003 UR_004 UR_005 UR_006 UR_007 UR_008	Track Identification Odometry calibration Cold movement detection Automated driving on highway, local roads and narrow and curved roads Speed accuracy for ERTMS Speed accuracy for Auto	SR-AUG-INF-004	Standardised Augmentation System Protocol and Format for accuracy augmentation messages

UR_001 UR_002 UR_003 UR_004 UR_005 UR_006 UR_007 UR_008	Track Identification Odometry calibration Cold movement detection Automated driving on highway, local roads and narrow and curved roads Speed accuracy for ERTMS Speed accuracy for Auto	SR-AUG-INF-005	Not Standardised Augmentation System Protocol and Format for accuracy augmentation messages
UR_001 UR_002 UR_003 UR_004 UR_005 UR_006 UR_007 UR_008	Track Identification Odometry calibration Cold movement detection Automated driving on highway, local roads and narrow and curved roads Speed accuracy for ERTMS Speed accuracy for Auto	SR-AUG-FUN-006	Augmentation to Service Level allocation
UR_004 UR_005 UR_006 UR_008	Automated driving on highway, local roads and narrow and curved roads Speed accuracy for Auto	SR-AUG-OPE-008	RTK Augmentation maximum service coverage
UR_004 UR_005 UR_006 UR_008	Automated driving on highway, local roads and narrow and curved roads Speed accuracy for Auto	SR-AUG-OPE-009	NRTK Augmentation Reference Stations distribution
UR_001 UR_002 UR_003 UR_004 UR_005 UR_006 UR_007 UR_008	Track Identification Odometry calibration Cold movement detection Automated driving on highway, local roads and narrow and curved roads Speed accuracy for ERTMS Speed accuracy for Auto	SR-AUG-OPE-010	2-Tiers connection to EDAS
UR_001 UR_002 UR_003 UR_004 UR_005 UR_006 UR_007	Track Identification Odometry calibration Cold movement detection Automated driving on highway, local roads and narrow and curved roads Speed accuracy for ERTMS	SR-AUG-OPE-011	Augmentation Centre Service Mountpoints

UR_008	Speed accuracy for Auto		
UR_001 UR_002 UR_003 UR_004 UR_005 UR_006 UR_007 UR_008	Track Identification Odometry calibration Cold movement detection Automated driving on highway, local roads and narrow and curved roads Speed accuracy for ERTMS Speed accuracy for Auto	SR-AUG-OPE-012	Augmentation correction messages update rate
UR_001 UR_002 UR_003 UR_004 UR_005 UR_006 UR_007 UR_008	Track Identification Odometry calibration Cold movement detection Automated driving on highway, local roads and narrow and curved roads Speed accuracy for ERTMS Speed accuracy for Auto	SR-AUG-OPE-013	2-Tiers Probability of missed detection

8. CONCLUSIONS

The purpose of the deliverable **D2.3 System Requirement Specifications** (with traceability matrix) was to specify the Systems Requirements for the HELMET solution from viewpoint of high-accuracy and high-integrity EGNSS applications in rail (RAIL) and automotive (AUTO) sectors supported by Unmanned Aerial Vehicles / Systems (UAV).

The System Requirements Specification process employed within the HELMET WP2, Task 2.2 was consisting of the following activities:

- HELMET CONOPS development;
- High-level User Requirements specification (as a result of CONOPS);
- Identification of general constrains and limitations;
- Specification of Logical Concepts and Models for the User's groups;
- Safety analysis for the Logical Concepts for multi-modal applications;
- Development of Requirements Traceability Matrices (RTMs) for the maim HELMET User's groups (RAIL, AUTO, UAVs);
- Description and justification of individual Systems Requirements;
- Specification of Systems Requirements for High-Level HELMET architecture.

The Requirements Traceability Matrices (RTMs) for the individual user's groups (RAIL, AUTO, UAVs) including GNSS Augmentation are contained in Section 7. The RTMs were developed for mapping links and dependences between the high-level User Requirements (D2.1) and the System Requirements (D2.3) in order to facilitate, make transparent and justify the above System Requirements Specification process used in HELMET.

The System Requirements for RAIL, AUTO and UAVs applications including system requirements for GNSS augmentations summarised in Section 5 represent the main output from the HELMET Task 2.2. Section 6 outlines the High-level HELMET architecture with the key safety measures. The architecture will be further developed in detail within WP3 using the System Requirements specified in this deliverable.

9. REFERENCES

[1] HELMET_D2.1 User Requirements Specification_rev.01_24.03.2020.

[2] HELMET_D2.2 CONOPS (Concept of Operations) _rev.01_23.04.2020.

[3] Standalone and RTK GNSS on 30,000 km of North American Highways, Reid, Tyler G. R., Pervez, Nahid, Ibrahim, Umair, Houts, Sarah E., Pandey, Gaurav, Alla, Naveen K.R., Hsia, Andy, *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, Miami, Florida, September 2019.

[4] Precise and Robust RTK-GNSS Positioning in Urban Environments with Dual-Antenna Configuration, Peirong Fan, Wenyi Li, Xiaowei Cui, Mingquan Lu, *Sensors 2019, 19, 3586.*

[5] Tightly combined GPS/Galileo RTK for short and long baselines: Model and performance analysis, Mingkui Wu, Wanke Liu, Renpan Wu, Xiaohong Zhang, *Advances in Space Research Volume 63, Issue 7, Pages 2003-2020*, 1 April 2019.

[6] High accuracy positioning in urban environments using single frequency multi-GNSS RTK-MEMS-IMU integration, Tuan Li, Hongping Zhang, Zhouzheng Gao, Qijin Chen, Xiaoji Niu, *Remote Sens. 2018, 10, 205.*

[7] Performance of Tightly Coupled Integration of GPS,BDS,MEMS-INS Odometer for Real-Time High-Precision Vehicle Positioning in Urban Degraded and Denied Environment, Fei Liu, Houzeng Han, Xin Cheng, Binghao Li, *Journal of Sensors Volume 2020, Article ID 8670262*, 2020.

[8] A new Approach for Positioning Integrity Monitoring of Intelligent Transport Systems Using Integrated RTK-GNSS, IMU and Vehicle Odometer, El-Mowafy, A., Kubo, N., *IET Intelligent Transport Systems 12(8): 901 –908*, 2018.

[9] Reid, T. G. R., Houts, S. E., Cammarata, R., Mills, G., Agarval, S. Vora, A. and Pandey, G.: Localization Requirements for Autonomous Vehicles. 3 June 2019. https://arxiv.org/pdf/1906.01061.pdf

[10] ERSAT GGC_WP2 D2.1, “Enhanced Functional ERTMS Architecture Capable of using GNSS and Public Radio TLC Technologies”, Rev 3, 21/11/2019.

[11] UNISIG – “SUBSET-026 System Requirements Specification”, Ver. 3.6.0.

[12] Zender, J.: Functional Safety for Autonomous Driving. Int. Symp. On Electronic Imaging 2017; Autonomous Vehicles and Machines 2017. 29 Jan – 2 Feb 2017. NVIDIA. http://www.imaging.org/Site/PDFS/Conferences/ElectronicImaging/EI2017/Keynotes/EI2017_AVM_Keynote_Justyna_Zander.pdf

[13] UNISIG – “SUBSET-088 ETCS Application Levels 1 & 2 - Safety Analysis Part 3 - THR Apportionment”, Ver. 2.3.0.

[14] ERSAT GGC D3.2 GNSS Quantitative Study for ERSAT GGC Project, Rev. 3, 22/11/2019.

[15] Liu, P., Yang, R., Xu, Z.: ‘How Safe Is Safe Enough for Self-Driving Vehicles?’ Risk Analysis Vol. 0, No. 0, 2018, 11 pages.

[16] Global status report on road safety 2015. https://www.who.int/violence_injury_prevention/road_safety_status/2015/en/

[17] Aviation safety. https://en.wikipedia.org/wiki/Aviation_safety

[18] Minimum Aviation System Performance Standards for the Local Area Augmentation System (LAAS), RTCA DO-245 A, 2004.

[19] High Integrity Two-tiers Augmentation Systems for Train Control Systems, A. Neri, R. Capua, P. Salvatori, Pacific PNT 2015.

[20] National Lightning Safety Institute. http://www.lightningsafety.com/nlsi_pls/probability.html

[21] Liang Heng, Grace Xingxin Gao, Todd Walter, Per Enge, Digging into GPS Integrity, 2011.

[22] S. Pullen, 'Lessons Learned from the Development of GNSS Integrity Augmentations', https://mycoordinates.org/lessons-learned-from-the-development-of-gnss-integrity-augmentations/.

[23] H. Blomenhofer, W. Ehret, H. Su, E. Blomenhofer, 'Sensitivity Analysis of the Galileo Integrity Performance Dependent on the Ground Sensor Station Network'

[24] J. Lee, S.Jung, E. Bang, S. Pullen, P. Enge 'Long Term Monitoring of Ionospheric Anomalies to Support the Local Area Augmentation System', 2010.

[25] S. Pullen, J. Rife, P. Enge, 'Prior Probability Model Development to Support System Safety Verification in the Presence of Anomalies' 2006.

[26] R. E. Phelt, G. Wong, T. Walter, P. Enge, 'Signal Deformation Monitoring for Dual-Frequency WAAS' 2013.

[27] RTCM 10403.3, Differential GNSS (Global Navigation Satellite Systems) Services - Version 3 + Amendment 1.

[28] UNISIG – SUBSET-036 " FFFIS for Eurobalise " Ver. 2.4.1.

[29] ERTMS/ETCS Baseline 3 Onboard Subsystem Requirements: New Trains. Rail Industry Standard RIS-0798-CCS Issue: One, RSSB UK, September 2018.

[30] Report on Rail User Needs and Requirements: Outcome of the European GNSS' User Consultation Platform. GSA-MKD-RL-UREQ-250286, Issue/Revision: 2.0, Date: 01/07/2019, 80 pages.

[31] M. S. Netto, S.Chaib, S. Mammar, "Lateral adaptive control for vehicle lane keeping". Proceeding of the American Control Conference Boston, Massachusetts June 30 - July 2, 2004.

[32] UN Addendum 38 – Regulation No.39 Revision 2 from 2018 https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/r039r1e.pdf

[33] Vanholme, B., Gruyer, D., Lusetti, B., Glaser, S., Mammar, S.: Highly automated driving on highways based on legal safety. IEEE Transactions on Intelligent Transportation Systems14(1), 333–347 (2013).

[34] HEXAGON, LiDAR Comparison Chart, https://autonomoustuff.com/lidar-chart/

[35] Report on Road User Needs and Requirements: Outcome of the European GNSS' User Consultation Platform. Reference: GSA-MKD-RD-UREQ-250283 Issue/Revision: 2.0, Date: 01/07/2019, 50 pages. https://www.gsc-europa.eu/sites/default/files/sites/all/files/Report_on_User_Needs_and_Requirements_Road.pdf

[36] RTCM 10410.1 Standard for Networked Transport of RTCM via Internet Protocol (Ntrip) Version 2.0 with Amendment 1, June 28, 2011.

[37] Liu, W. Wu, Z. Wu, L. He e K. Tang: 'Spoofing Detection Algorithm Based on Pseudorange Differences', https://www.mdpi.com/journal/sensors, 2018.

[38] Integrity Monitoring for Carrier Phase Ambiguities, Feng, S.; Ochieng, W.; Samson, J.; Tossaint, M.; Hernandez-Pajares, M.; Juan, J.M.; Sanz, J.; Aragón-Àngel, À.; Ramos-Bosch, P., Navigation 2012.

[39] PPP Integrity for Advanced Applications, Including Field Trials with Galileo, Geodetic and Low-Cost Receivers and a Preliminary Safety Analysis, Navarro Madrid, P. F., Martínez Fernández, L., Alonso López, M., Laínez Samper, M. D., Romay Merino, ION GNSS 2016.

[40] UNISIG – SUBSET-041 ”Performance Requirements for Interoperability“, Ver. 3.1.0.

[41] AIAA “Preliminary Risk Assessment for Small Unmanned Aircraft Systems” June 2017

[42] Probabilistic Safety Assessment for UAS Separation Assurance and Collision Avoidance Systems“ February 2019 Asma Tabassum , Roberto Sabatini, and Alessandro Gardi.

[43] INTEGRAIL ERTMS Requirements Assessment. Technical Note. INTEG-BTSIG-TN-E-0110.

[44] ERTMS Users Group: ERTMS/ETCS RAMS Requirements Specification, Chapter 2 – RAM. Reference EEIG : 96S126, 1998.

[45] ERTMS/ETCS – Class 1: Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 3. Ref: SUBSET-091, ISSUE: 2.5.0, Date: 05-05-2009.

[46] “Performance test in GNSS outages”, I. Clarke, https://support.oxts.com/hc/en-us/articles/360001026269-Performance-test-in-GNSS-outages

--- END OF FILE ---