D2.2 HELMET CONOPS

Due date of deliverable: 01/05/2020

Actual submission date: 23/04/2020

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

Reviewed (Y/N):

Document status		
Revision	**Date**	**Description**
01	23/04/2020	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**	Contributor / WP2 Leader
Filip Holík	UPA	Contributor / WP2 Deputy Leader
Alessandro Neri	RDL	Contributor
Maurizio Salvitti	RDL	Contributor
Panagiotis Xefteris	RDL	Contributor
Cesare Dionisio	RDL	Contributor
Pietro Salvatori	RDL	Contributor
Roberto Capua	SGI	Contributor
Luca Gattuso	SGI	Contributor
Manuele Innocente	SGI	Contributor
Omar Garcia Crespillo	DLR	Contributor
Ondrej Kutik	RBA	Contributor
Michael Loupis	ITC	Contributor

DISTRIBUTION LIST

Name	Company	Roles/Title
Alessandro NERI	RDL	Project Coordinator
Daniel LOPOUR	GSA	GSA Programme Officer
Eutimio Tiliacos	GSA	Project Reviewer
Jose Eugenio Naranjo	GSA	Project Reviewer
Maurizio Salvitti	RDL	Project Manager
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_D2.2	01	WP2 Leader	A.Filip (UPA)	-	23/04/2020
		Coordinator	A.Neri (RDL)	A.Neri RDL)	23/04/2020

EXECUTIVE SUMMARY

This document is the deliverable **D2.2 HELMET CONOPS** which describes Concept of Operations (CONOPS) 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 solution 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 HELMET CONOPS is used as a starting point for specification and justification of high-level user requirements for RAIL, AUTO and UAV user groups. The purpose of the HELMET CONOPS is to describe the operational needs, views, visions and expectations of the user's groups without provision of technical details on HELMET. The CONPOS is written in user language and generally represents a set of user requirements. It means that the high-level user requirements specified in the deliverable D2.1 (User Requirements Specification) have been extracted from this deliverable.

The HELMET CONOPS also defines high-level performance requirements, objectives and other HELMET rationales. It is a high-level (user) requirements document whose intention is to provide mechanisms for HELMET users to describe their expectations from HELMET solutions. The HELMET CONOPS deliverable includes:

- Identification of different operational modes/ scenarios for RAIL, AUTO and UAVs applications;
- Identification of various operational environments and constrains;
- Derivation of High-level User Requirements for HELMET solutions;
- Summary of High-level User Requirements for HELMET;
- Description of High-level safety concepts;
- Derivation of High-level safety requirements;
- Overview of High-level User safety requirements;
- Regulatory requirements for certification and authorization process.

The HELMET CONOPS serves as a basis for specification of high-level functional and system requirements (to be done in D2.3) and related technical specifications. Further, user needs and performance measures identified in the CONOPS are the fundamental information for the HELMET Requirements Traceability Matrix and Validation Plan elaboration to be used to validate the HELMET concept at the end of its development phase. The overview of the regulatory requirements for certification and authorization process in the given application areas will be utilised for standardization activities of HELMET solutions to be performed within WP6.

TABLE OF CONTENTS

CONTRIBUTING PARTNER ... 2

DISTRIBUTION LIST ... 2

APPROVAL STATUS ... 2

EXECUTIVE SUMMARY ... 3

Table of Contents ... 4

List of Figures ... 7

List of TABLes ... 9

Definitions and abbreviations ... 11

1. INTRODUCTION ... 16

1.1 The aim of HELMET project from viewpoint of user defined Concept of Operations (CONOPS) ... 16

1.2 Purpose of CONOPS generally ... 17

1.3 Objectives of CONOPS in the HELMET context ... 18

2. HIGH-LEVEL USER REQUIREMENTS FOR HELMET SOLUTION ... 20

2.1 RAIL: The latest set of high-level GNSS user requirements ... 20

2.2 AUTO: High level user requirements for self-driving cars (SDCs) ... 22

2.2.1 Societal safety requirements for SDCs ... 22

2.2.2 Harmonization of risk and safety requirements for SDCs ... 24

2.2.3 High-level user requirement for SDCs ... 25

2.2.4 High-level road user performance requirements ... 26

2.3 UAV/RPAS-PIT SEGMENT: HIGH LEVEL USER REQUIREMENTS FOR AERIAL IMTM SERVICES ... 27

2.3.1 Societal Safety Requirements for UAV/RPAS Inserted in ECAC's Airspace ... 27

2.3.2 User High Level Risk and Safety Requirements for UAS/RPAS ... 31

2.3.3 High-Level User Requirements for UAS/RPAS-PIT and IMTM Services ... 38

2.4 High-level user cyber security requirements for HELMET ... 55

3. OPERATIONAL SCENARIOS RELEVANT TO HELMET, ASSUMPTIONS ... 57

3.1 RAIL: Operational Scenarios and user requirements for HELMET ... 57

3.1.1 Track identification function ... 57

3.1.2 Odometer calibration function ... 61

3.1.3 Cold Movement Detection ... 62

3.1.4 Speed accuracy for ERTMS ... 63

3.2 AUTO: Operational Scenarios and user requirements for HELMET ... 63

3.2.1 Automated driving on highway ... 65

3.2.2 Automated driving on local roads ... 65

3.2.3 Automated driving on narrow and curved roads 66
3.2.4 Speed accuracy 67
3.3 UAS/RPAS: Operational scenarios and user requirements for HELMET 67
3.3.1 General 67
3.3.2 Main IMTM UAS/RPAS Operational Scenarios Constraints 68
3.3.3 Potential Sensor Technologies and Process Capabilities Required for the IMTM UAS/RPAS for Railway and Road Operational Applications. 70
3.3.4 Overview of the Common Required UAS/RPAS Operational Scenarios Framework for Railway and Road IMTM Applications 71
3.3.5 IMTM UAS/RPAS Operational Environment Framework 75
3.3.6 Typical Flight Operative Modes Applicable to IMTM UAS/RPAS Operations 76
3.3.7 UAS/RPAS IMTM Railway and Road Operational Scenarios....80
4. SUMMARY OF HIGH-LEVEL USER REQUIREMENTS FOR HELMET 84
5. HIGH-LEVEL SAFETY CONCEPTS 88
5.1 RAIL: Railway safety 88
5.1.1 Worst case approach 88
5.1.2 Fail-safe technique 88
5.1.3 Railway safety pillars 89
5.1.4 Safety integrity concept 89
5.1.5 Railway technical safety principles 89
5.1.6 Common Safety Methods: EC regulation 402/2013 90
5.2 AUTO: Fail-safe VS. fail-operational and fault-tolerant principles 91
5.2.1 Basic differences between ISO 26262 and IEC 61508/ EN 5012x 91
5.2.2 Fail-operational and fail-tolerant techniques 92
5.3 UAV: HIGH LEVEL SAFETY CONCEPTS FOR UAS/UAS/RPAS-PIT STATION....95
5.3.1 General 95
5.3.2 The Concept of Safety in Aviation: Background and Impact on UAS/RPAS 95
5.3.3 The UAS/RPAS Safety Process Logic Overview 96
5.3.4 Failure Condition Classification 97
5.3.4 Overview of Hazards Identification and Assessment for UAS/RPAS Operations 98
5.3.4 Safety Objectives 115
5.3.5 Certification Targets 116
6. DERIVATION OF HIGH-LEVEL SAFETY REQUIREMENTS 118
6.1 RAIL: Generic process for derivation of safety requirements for railway safety-related systems 118
6.2 AUTO: Derivation of high-level safety requirements for self-driving cars....119
6.2.1 Derivation of high-level safety requirements in aviation 120

6.2.2 Travel safety measures: Time versus Distance 123
6.2.3 Risk acceptance principles and criteria on European railways 125
6.2.4 Risk harmonization of railway technical systems....................126
6.2.5 Design safety targets as harmonised risk acceptance criteria 127
6.2.6 Derivation of system safety requirements according to functional safety standards (IEC 61508, CENELEC and ISO 26262) 129
6.2.7 Quantitative or qualitative way for high level safety requirements derivation for SDCs? 131
6.2.8 Proposal for harmonization of automotive safety requirements based on railway experience 132
6.3 UAVS/RPAS: Derivation of high-level safety requirements 133
7. HIGH-LEVEL USER SAFETY REQUIREMENTS....................134
7.1 RAIL: High-level safety target for HELMET exploitation in ERTMS....................134
7.2 AUTO: High-level safety target derivation for self-driving cars 134
7.3 UAS/RPAS: High-level safety target derivation....................137
8. REGULATORY REQUIREMENTS FOR CERTIFICATION AND AUTHORIZATION....................137
8.1 RAIL: Description of Certification Process 137
8.2 AUTO: Certification process for self-driving cars 140
8.2.1 Need for certification of self-driving cars 140
8.2.2 Shorter vehicle lifecycle on road-side digital infrastructure....................141
8.2.3 Type-approval framework for cars in EU 141
8.3 UAS/RPAS: requlatory Framework and Requirements 143
9. CONCLUSIONS....................149
10. REFERENCES....................150

LIST OF FIGURES

Figure 1. Multimodal AIMN Concept in HELMET Solution for Rail, Automotive and UAS/RPAS ... 16
Figure 2. CONOPS in the system lifecycle (IEC 61508, EN 50126) ... 17
Figure 3. Phases of HELMET WP2 solution ... 18
Figure 4. Classification of requirements for HELMET ... 19
Figure 5. Road traffic fatality rates (TFRs) per 100 000 population and year according to regions [3] ... 23
Figure 6. Common Mass-Produced Multi-copter UA/RPA ... 30
Figure 7. Schematic Representation of the SORA Concept (Source: EUROCONTROL) ... 32
Figure 8. Graphical Representation of SORA Semantic Model ... 34
Figure 9. Typical UAS/RPAS Data Links Classification and Functional Description Schematic ... 42
Figure 10. Safety risk assessment based on UAS/RPAS C3/UTM functions ... 43
Figure 11. Examples of UAV Mapping Steep Slopes and Contours ... 44
Figure 12. Examples of some Payload Types Required for IMTM UAS/RPAS Operations in Rail/Automotive ... 45
Figure 13. UAS/RPAS Main Functions ... 46
Figure 14. Major Causes of EGNSS Degradation ... 47
Figure 15. RPAS Operational Integrity ... 47
Figure 16. Integrity Computation Process on Board ... 48
Figure 17. Schematic View of the Overall Future Communication Scenario for UAS/RPAS ... 49
Figure 18. SESAR Evolution Steps ... 50
Figure 19. PIT Station Functions ... 53
Figure 20. PIT stations Architecture Schematic for Railways Applications ... 54
Figure 21. Scope of cyber security from the functional safety point of view applied in HELMET ... 56
Figure 22. Definition of Protection Level and Alert Limit for train position determination. Position of GNSS antenna is: (a) known, (b) unknown ... 57
Figure 23. Track identification function ... 58
Figure 24. Example of THR allocation for GNSS-based train position determination function in RHINOS project [25] ... 60
Figure 25. Definition of Alert Limit and Protection Level for automated car driving ... 63
Figure 26. Example of payload sensor technology ... 70
Figure 27. Required UAS/RPAS Operational Framework for Railway and Road IMTM Applications Block Diagram ... 71
Figure 28. Flight Planning Process Steps ... 72
Figure 29. Possible Transitions among Different Flight Modes ... 77
Figure 30. Overall IMTM UAS/RPAS-PIT Operational Scenario Application for HELMET ... 77
Figure 31. Example of IMTM UAS/RPAS Rail Operational Scenario with the Operational Area Constrained by Virtual Fences ... 78
Figure 32. UAS/RPAS Operation PIT to PIT Schematic ... 78
Figure 33. Obstacle detection by UAV ... 80
Figure 34. Example of UAS/RPAS Railway IMTM Application ... 80
Figure 35. Fail-safe techniques according to CENELEC: (a) composite fail-safety, and (b) reactive fail-safety. ... 90
Figure 36. Relation between safety and availability – parameters are reliability and maintainability ... 92
Figure 37. Example of fail-operational system for safe and dependable speed measurement ... 93

Figure 38. Eight Elements of the Aviation System Safety Process 96
Figure 39. Multidimensional Problem Space for Assessing Risk and Ensuring the Safety of UAS and UTM Operations.. 99
Figure 40. Example of risk analysis process for safety requirements derivation [19] 118
Figure 41. Target Level of Safety for GNSS in Aviation.. 120
Figure 42. Aviation Target Level of Safety allocation to integrity and continuity risks 121
Figure 43. Duration of operation for Integrity Risk specification.. 123
Figure 44. Transition from Target Individual Risk to THRs of safety-related functions to be implemented by technical system 124
Figure 45. Common Safety Method for risk evaluation and Assessment (CSM-RA).................... 126
Figure 46. Explicit risk estimation and evaluation within CSM 127
Figure 47. Harmonised approach for risk evaluation and determination of high safety integrity requirements for railway technical systems 129
Figure 48. Determination of safety requirements for automotive systems................................... 130
Figure 49. Proposed use of railway quantitative CSM-DT as a complementary method to the qualitative ASIL determination procedure in order to support harmonization of safety requirements for self-driving cars... 132
Figure 50. Derivation of harmonised design target for self-driving cars 135
Figure 51. European train control system with virtual balises detected by GNSS 137
Figure 52. Example of using the ERTMS for connected car 138
Figure 53. Relation between CSM-RA and CENELEC life cycle. 139
Figure 54. Chronology of regulations towards type-approval process of vehicles with ACSF in Europe 142

LIST OF TABLES

Table 1. Rail GNSS User Requirements [1]. 21
Table 2. Fatality risk of various forms of travel [11] 25
Table 3. Performance parameters of car position determination GNSS based [14] 26
Table 4. Overview of the EASA of some EU Member States' Regulations on UAV/RPAS up to 25kg TOW 28
Table 5. MTOM/Energy Threshold Requirements for UAS "Open" Category Sub-classes (Source EASA A-NPA 2015-10) 29
Table 6. Derived Safety Objectives to Maintain Safe Flight and Landing...................................... 31
Table 7. Airspace Encounter Categories and Air-Risk Classes (Source: EUROCONTROL) 33
Table 8. Main areas of user requirements for UAVs.. 39
Table 9. IMTM UAS/RPAS Physical, Functional and Operational Performance Requirements 41
Table 10. IMTM UAS/RPAS Physical, Functional and Operational Performance Comparison 41
Table 11. Performance Comparison performance objectives associated with operational communication.. 44
Table 12. High-Level User UAS/RPAS CNPC Forward and Return Link Performance Requirements (EUROCAE).. 45
Table 13. Spectrum Requirements Summary-Methodology 2 (Source ITU -R M.2171)................ 46
Table 14. GNSS accuracy of different techniques 51
Table 15. Summary of High-Level User GNSS Requirements for UAS/RPAS Operations 55
Table 16. Track spacing values for different tracks 59
Table 17. Requirements for GNSS from viewpoint of UAS/RPAS inspection operations 81
Table 18. Requirements for GNSS from viewpoint of UAS/RPAS monitoring operations 82
Table 19. Requirements for GNSS from viewpoint of UAS/RPAS traffic management operations. 84
Table 20. Summary of high-level user requirements for HELMET.. 84
Table 21. Summary of high-level user requirements for HELMET (speed accuracy)..................... 86
Table 22. Summary of High-Level UAS/RPAS Requirements for HELMET.................................. 87
Table 23. Characteristic features of safety techniques applicable to automated car driving 94
Table 24. UAS/RPAS Current Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 101
Table 25. UAS/RPAS Future Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 102
Table 26. UAS/RPAS Future Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 103
Table 27. UAS/RPAS Future Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 104
Table 28. UAS/RPAS Future Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 105
Table 29. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 106
Table 30. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 107
Table 31. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 108
Table 32. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 109

Table 33. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 110
Table 34. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 111
Table 35. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 112
Table 36. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 113
Table 37. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum) 114
Table 38. Manned Aircraft Accident Rates 115
Table 39. Derived Quantitative Systems Availability and Integrity Required to Maintain Safe Flight and Landing (excluding loss of safe separation) [JARUS AMC RPAS.1309. Issue 2, November 2015]........ 116
Table 40. Relationship among Aircraft Classes, Probabilities, Severity of Failure Conditions and Software and Complex hardware DALs, required to maintain safe flight and landing to that of equivalent manned aircraft (excluding loss of safe separation) [JARUS AMC RPAS.1309. Issue 2, November 2015] 117
Table 41. Harmonised CSM Design Targets for railway technical systems 128
Table 42 (a-d). Overview of some EU Member States’ Regulations on UAV/UAS/RPAS up to 25kg TOW 146

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
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
CAA	Civil Aviation Authority
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
CNPC	Control and Non-Payload Communications
CONOPS	Concept of Operations
CoP	Codes of Practice
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
DAA	Detection And Avoidance
DEM	Digital Elevation Model
DMI	Driver Machine Interface

DOP	Dilution of Precision
E/E/PE	Electrical/Electronic/Programmable Electronic
EASA	European Aviation Safety Agency
EC	European Commission
ECAC	European Civil Aviation Conference
EGNOS	European Geostationary Navigation Overlay Service, i.e. European SBAS
EGNSS	European GNSS
EMI	Electro-magnetic interference
ERA	The European Union Agency for Railways
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
FCU	Flight Control Unit
FDIR	Fault Detection, Isolation and Recovery
FTA	Fault tree Analysis
GA	General Aviation
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
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
GSM-R	Global System for Mobile Communications – Railway
HAP / HAPS	High-Altitude Platform(s)
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

LAAS	Local Area Augmentation System
LDS	Location Determination System
ICAO	International Civil Aviation Organization
I/F	Interface
IFR	Instrument Flight Rules
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
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
LOS	Line of Sight
LV-AL THR	Low Vertical Alert Limit THR
MEM	Minimum Endogenous Mortality
MOBU	Multi-sensor On-Board Unit platform
MTGW	Maximum Take-off Gross Weight
MTOM	Maximum Take-off Mass
NAVAIDS	Navigational Aids
NLOS	Non-line-of-sight reception
NP	No Power
NPA	Non-Precision Approach
OBU	On-Board Unit
OPS	Operational
OSO	Operational Safety Objectives
PE	Position Error
PF	Probability of Failure (average) per 1 hour
PL	Protection Level
PoC	Proof-of-Concept
PoF	Probability of Fatality
PPP	Precise Point Positioning
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
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
RTCA	Radio Technical Commission for Aeronautics
RTH	Return-to-Home
RTK	Real Time Kinematics
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
SDR	Software-Defined Radio
SESAR	Single European Sky ATM Research
SORA	Specific Operational Risk Assessment
STK	Satellite Tool Kit
SW	Software
SIL	Safety Integrity Level
SDC	Self-Driving Car
SOM	Start of Mission
TFR	Traffic Fatality Rate
THR	Tolerable Hazard Rate
TIR	Target Individual Risk
TLC	Telecommunications
TMPR	Tactical Mitigation Performance Requirements
TOW	Take off Weight
TS	Track Spacing
TSI	Technical Specifications for Interoperability
TSO	Technical Standard Order
TTA	Time-To-Alert
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
UIC	Union Internationale des Chemins de fer (International Union of Railways)
UCP	User Consultation Platform
VB	Virtual Balise
VBN	Visual Based Navigation
VBR	Virtual Balise Reader
VBTM	Virtual Balise Transmission Module
VCM (VMC)	Visual Meteorological Conditions
VLOS	Visual Line Of Sight
UTM	Unmanned Aircraft System Traffic Management; UAV Traffic Management
VFR	Visual Flight Rules
VHF	Very High Frequency
VHL	Very High Level flights
VLL	Very Low Level
VTOL	Vertical Take-Off and Landing

1. INTRODUCTION

1.1 The aim of HELMET project from viewpoint of user defined Concept of Operations (CONOPS)

The HELMET project aims to define a multi-modal Augmentation and Integrity Monitoring Network (AIMN) suitable for Rail, Automotive and Unmanned Aerial Vehicles (UAVs) applications by exploiting the current-stage SBAS infrastructures (in particular EGNOS) complemented with local networks, as well as the new features brought by Galileo, and state of the art carrier phase technologies. UAVs and in particular UAS/RPAS-PIT (Unmanned Aerial System/ Remotely Piloted Aerial System-PIT Station(s)) Segment is dedicated to Inspection, Monitoring and Traffic Management (IMTM) services for both rail and automotive field operations / assets. The high-level multi-modal AIMN concept is depicted in Fig. 1.

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 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.

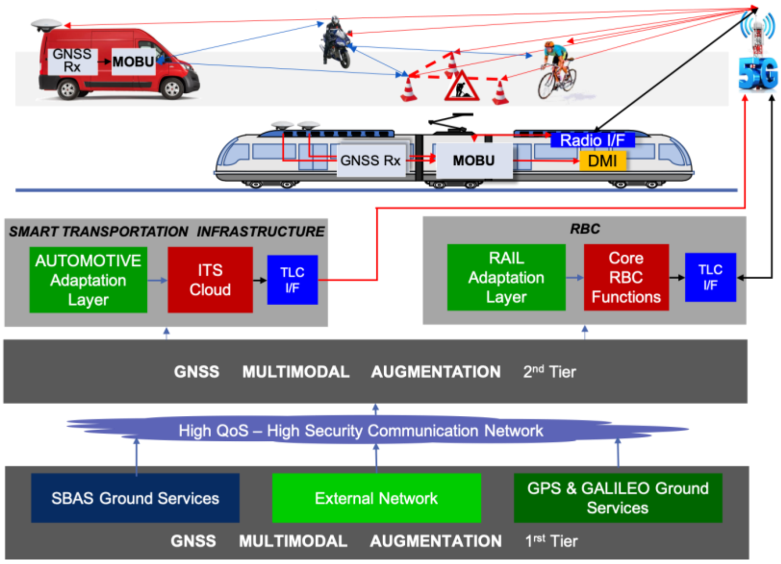

GNSS Rx
MOBU
5G
GNSS Rx
MOBU
Radio I/F
DMI
SMART TRANSPORTATION INFRASTRUCTURE
AUTOMOTIVE Adaptation Layer
ITS Cloud
TLC I/F
RBC
RAIL Adaptation Layer
Core RBC Functions
TLC I/F
GNSS MULTIMODAL AUGMENTATION 2nd Tier
High QoS – High Security Communication Network
SBAS Ground Services
External Network
GPS & GALILEO Ground Services
GNSS MULTIMODAL AUGMENTATION 1rst Tier

Figure 1. Multimodal AIMN Concept in HELMET Solution for Rail, Automotive and UAS/RPAS

The first phase of HELMET (WP2) is devoted to defining the user requirements for road, rail and UAS-PIT segments (supporting also in terms of IMTM the first two segments) applications and system requirements (including multimodal AIMN and Multi-sensor On-Board Unit platform, i.e. MOBU). This activity will firstly identify the user requirements and the operational use cases in cooperation with the rail, road and UAS/RPAS-PIT Stations stakeholders. After that, the system requirements (functional, performance, security and RAMS (Reliability, Availability, Maintainability, and Safety)) and their harmonisation will be defined, and these will be the drivers for the architecture design (WP3), including both AIMN and MOBU platform (in particular focusing on data integration and multi-sensor Fault Detection and Exclusion algorithms).

This deliverable (D2.2) deals with the user defined Concept of Operations (CONOPS) which is utilised within HELMET as an efficient instrument for 1) User Requirements Specification, and 2) System Requirements Specification. Since HELMET aims at development of the Augmentation and Integrity Monitoring Network (AIMN) for multi-modal applications (RAIL, AUTO, UAVs), then the structure and contents of the CONOPS document was also conformed to the objective. The intention of D2.2 elaboration was to find commonalities between AUTO, RAIL and UAVs applications, which could further facilitate harmonization of system requirements in D2.3 and thus to enable a single AIMN architecture definition for all the multi-modal applications. Therefore, each of main CONOPS Sections (2-9) includes Sub-sections devoted to AUTO, RAIL and UAVs.

User Requirements Specification for HELMET solution is an integral part of the D2.2 CONOPS deliverable. It is included in Sections 2-4 (of D2.2). Sections 5-7 (of D2.2) describe, how high-level safety requirements for the individual HELMET applications (RAIL, AUTO and UAVs/ UAS/RPAS) were derived. This knowledge will be further utilised within the D2.3 deliverable elaboration.

1.2 PURPOSE OF CONOPS GENERALLY

A CONOPS is a user-oriented document that describes systems characteristics for a proposed system from a user's perspective. The CONOPS also describes the user organization, mission, and objectives from an integrated systems point of view and is used to communicate overall quantitative and qualitative system characteristics to stakeholders. A position of CONOPS in system lifecycle is depicted in Fig. 2.

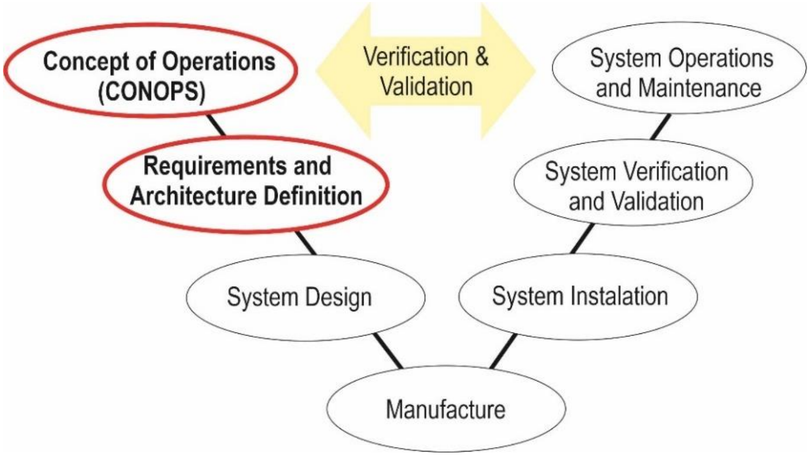

Concept of Operations (CONOPS)
Verification & Validation
System Operations and Maintenance
Requirements and Architecture Definition
System Verification and Validation
System Design
System Instalation
Manufacture

Figure 2. CONOPS in the system lifecycle (IEC 61508, EN 50126)

CONOPS describes the proposed system in terms of the user needs that it will fulfil, its relationship to existing systems or procedures, and the ways it will be used. CONOPS can be tailored for many purposes, for example, to obtain consensus among the acquirer, developers, supporters, and user agencies on the operational concept of a proposed system. Additionally, a CONOPS may focus on communicating the user's needs to the developer or the developer's ideas to the user and other interested parties.

1.3 OBJECTIVES OF CONOPS IN THE HELMET CONTEXT

In the HELMET project this CONOPS document is produced early in the requirements definition phase to describe what the HELMET solution (i.e. **H**igh integrity **E**GNSS **L**ayer for **M**ultimodal **E**co-friendly **T**ransportation) will do without saying HOW it will to do and WHY.

The purpose of the HELMET CONOPS is to describe the operational needs, views, visions and expectations of the user ‘s groups without provision of technical details on HELMET. The CONPOS is written in user language and generally represents a set of user requirements.

The HELMET CONOPS also defines high-level performance requirements, objectives and other HELMET rationales. It is a high-level (user) requirements document whose intention is to provide mechanisms for HELMET users to describe their expectations from HELMET solutions. The HELMET CONOPS document summarises:

- Identification of different operational modes/ scenarios for RAIL, AUTO and UAVs applications;
- Identification of various operational environments and constrains;
- Derivation of High-level User Requirements for HELMET solutions;
- Summary of specified High-level User Requirements for HELMET;
- Description of High-level safety concepts;
- Derivation of High-level safety requirements;
- Overview of High-level User safety requirements;
- Regulatory requirements for certification and authorization process.

The HELMET CONOPS document serves as a basis for specification of high-level functional, system requirements and related technical specifications. Further, user needs and performance measures that are identified in the CONOPS are the fundamental information for the HELMET Validation Plan that is used to validate the HELMET concept at the end of its development.

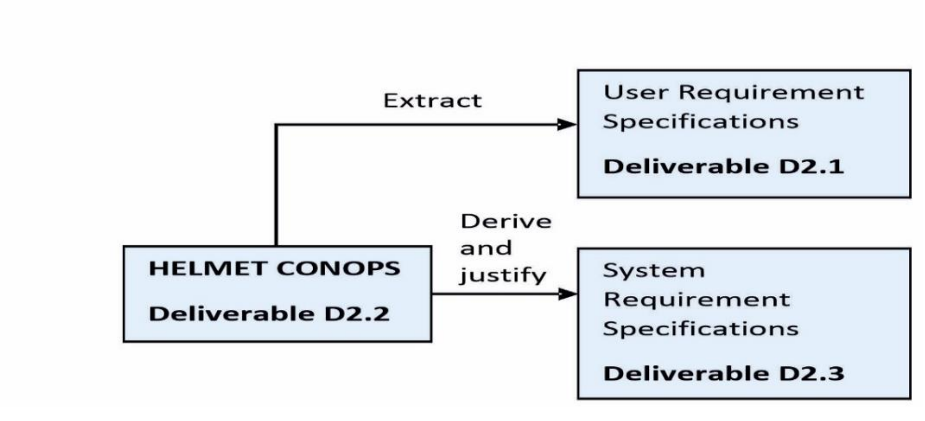


Figure 3. Phases of HELMET WP2 solution

The applied procedure for HELMET WP2 solution is outlined in Fig. 3. HELMET CONOPS (D2.2) specifies and justifies high-level user requirements for RAIL, AUTO and UAVs/UAS/RPAS user groups. The user requirements (for lucidity) have been already extracted from D2.2 in a separate deliverable D.2.1. Finally, the CONOPS will be used for derivation of more detail system requirements to be described and justified in the deliverable D2.3.

Classification of requirements utilised within the HELMET CONOPS is shown in Fig. 4.

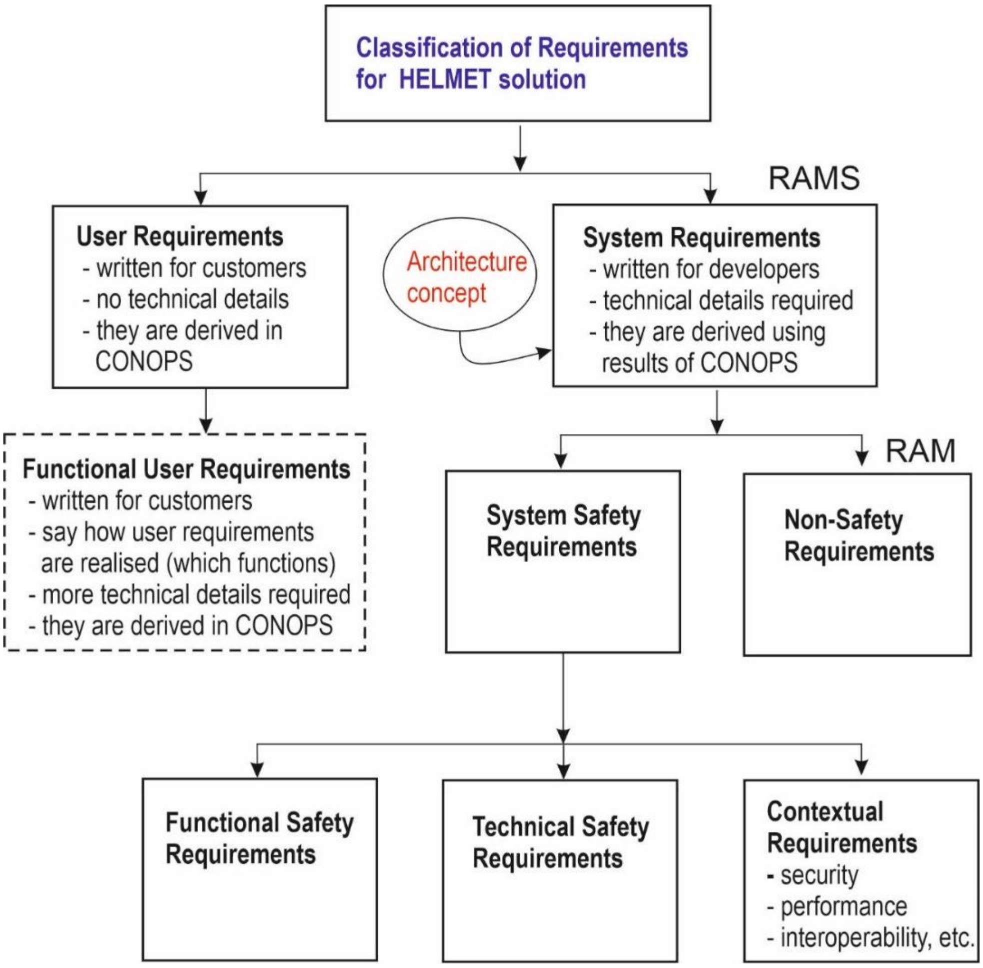

Classification of Requirements
for HELMET solution
RAMS
User Requirements
- written for customers
- no technical details
- they are derived in CONOPS
Architecture concept
System Requirements
- written for developers
- technical details required
- they are derived using results of CONOPS
Functional User 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.

Figure 4. Classification of requirements for HELMET

It is outlined in Fig. 4 that system requirements can be derived after the system architecture has been defined. System requirements specification process must be usually repeated several times depending on the progress in the architecture development. At first, high-level system requirements are defined and then these are subsequently refined in next system development phases.

2. HIGH-LEVEL USER REQUIREMENTS FOR HELMET SOLUTION

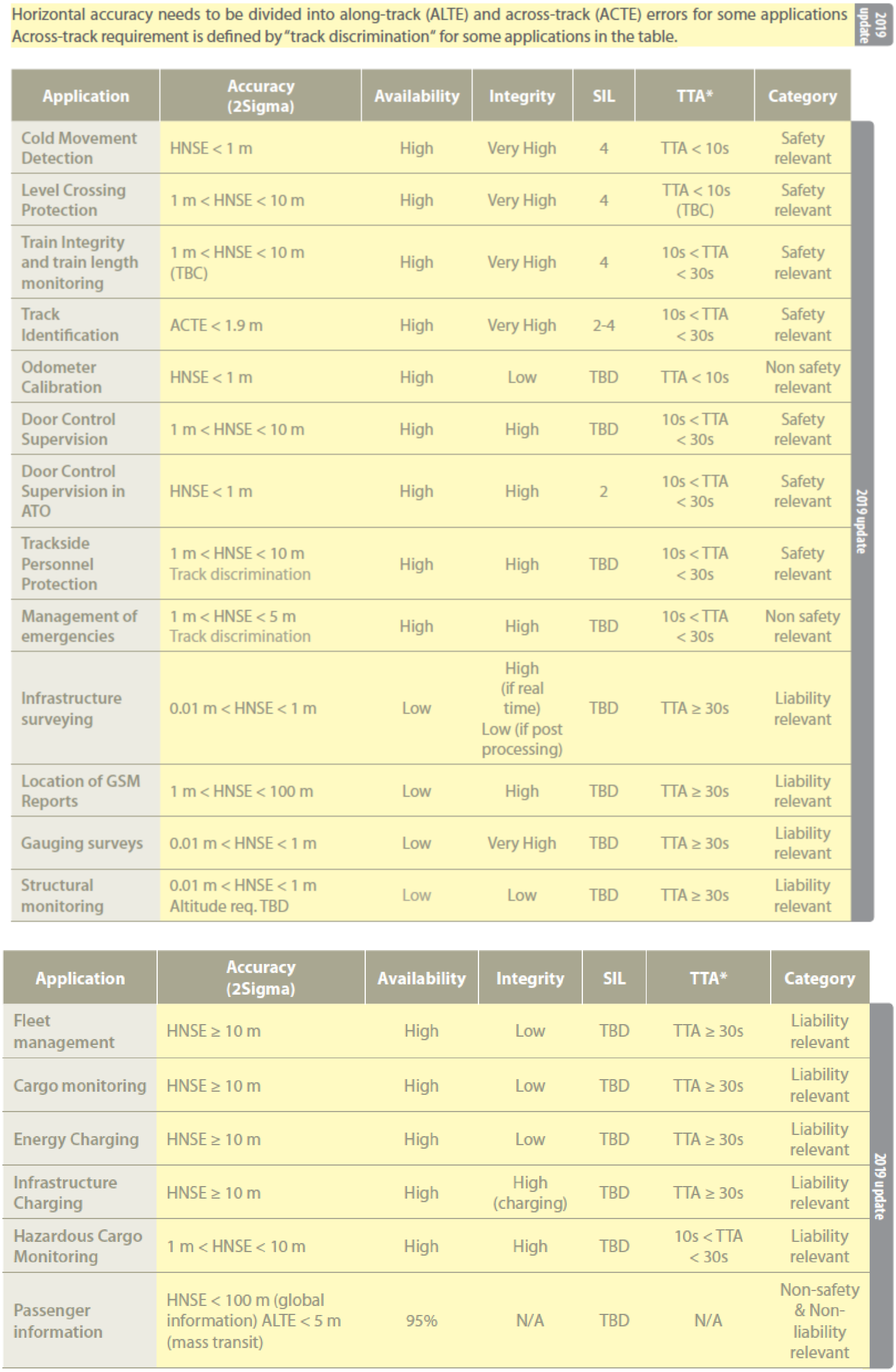
2.1 RAIL: THE LATEST SET OF HIGH-LEVEL GNSS USER REQUIREMENTS

European and North American railways have (in contrast to automotive industry) a long-term experience regarding user requirements specification for GNSS-based applications in railway sector. In Europe these activities started within the first international R&D projects in this field such as APOLO, RUNE, INTEGRAIL, ECORAIL, etc. It was in 1990's and early in the first decade of the 21st century.

In the period 1999-2000 the GNSS Rail Advisory Forum (in Brussels) specified the first set of widely acceptable user requirements for railway GNSS-based application in Europe. Such activities were continuing within the UIC Galileo Applications for Rail Working Group (2005-2011) and other research projects and activities such as GRAIL, SUGAST, ERSAT programme, etc. In the United States similar activities started approximately in the same period and were related to the Positive Train Control / Positive Train Separation programme.

The latest set of high-level GNSS rail user requirements is specified in Table 1 [1].

Table 1. Rail GNSS User Requirements [1].



Horizontal accuracy needs to be divided into along-track (ALTE) and across-track (ACTE) errors for some applications
Across-track requirement is defined by "track discrimination" for some applications in the table.

2019 update

Application	Accuracy (2Sigma)	Availability	Integrity	SIL	TTA*	Category
Cold Movement Detection	HNSE < 1 m	High	Very High	4	TTA < 10s	Safety relevant
Level Crossing Protection	1 m < HNSE < 10 m	High	Very High	4	TTA < 10s (TBC)	Safety relevant
Train Integrity and train length monitoring	1 m < HNSE < 10 m (TBC)	High	Very High	4	10s < TTA < 30s	Safety relevant
Track Identification	ACTE < 1.9 m	High	Very High	2-4	10s < TTA < 30s	Safety relevant
Odometer Calibration	HNSE < 1 m	High	Low	TBD	TTA < 10s	Non safety relevant
Door Control Supervision	1 m < HNSE < 10 m	High	High	TBD	10s < TTA < 30s	Safety relevant
Door Control Supervision in ATO	HNSE < 1 m	High	High	2	10s < TTA < 30s	Safety relevant
Trackside Personnel Protection	1 m < HNSE < 10 m Track discrimination	High	High	TBD	10s < TTA < 30s	Safety relevant
Management of emergencies	1 m < HNSE < 5 m Track discrimination	High	High	TBD	10s < TTA < 30s	Non safety relevant
Infrastructure surveying	0.01 m < HNSE < 1 m	Low	High (if real time) Low (if post processing)	TBD	TTA ≥ 30s	Liability relevant
Location of GSM Reports	1 m < HNSE < 100 m	Low	High	TBD	TTA ≥ 30s	Liability relevant
Gauging surveys	0.01 m < HNSE < 1 m	Low	Very High	TBD	TTA ≥ 30s	Liability relevant
Structural monitoring	0.01 m < HNSE < 1 m Altitude req. TBD	Low	Low	TBD	TTA ≥ 30s	Liability relevant
Fleet management	HNSE ≥ 10 m	High	Low	TBD	TTA ≥ 30s	Liability relevant
Cargo monitoring	HNSE ≥ 10 m	High	Low	TBD	TTA ≥ 30s	Liability relevant
Energy Charging	HNSE ≥ 10 m	High	Low	TBD	TTA ≥ 30s	Liability relevant
Infrastructure Charging	HNSE ≥ 10 m	High	High (charging)	TBD	TTA ≥ 30s	Liability relevant
Hazardous Cargo Monitoring	1 m < HNSE < 10 m	High	High	TBD	10s < TTA < 30s	Liability relevant
Passenger information	HNSE < 100 m (global information) ALTE < 5 m (mass transit)	95%	N/A	TBD	N/A	Non-safety & Non-liability relevant

2019 update

2019 update

These user requirements were specified after numerous discussions of rail community within User Consultation Platform (UCP) organised by the European GNSS Agency in the period 2017-2018. The requirements were updated in 2019.

The most demanding requirements in Table 1 regarding accuracy and safety integrity have been selected as a starting point for definition of the most relevant operational scenarios and further refinement of the GNSS UCP requirements for rail.

These most relevant high-accuracy and high-integrity railway operational scenarios for HELMET are following:

- Track identification,
- Odometer calibration, and
- Cold movement detection

These rail operational scenarios are described in more details in sections below in this document and the relevant user requirements are refined and justified. In addition, a guarantee of accuracy of speed measurement is also required.

Note: The rail sector has 1) a long-term experience with specification of user safety requirements for railway safety applications and definition of risk acceptance principles/ criteria by society (contained e.g. in CENELEC standards, EU safety regulations, ERTMS Technical Specifications for Interoperability, etc.) and 2) also very good knowledge regarding specification of detailed system safety requirements for railway safety-related systems. For example it is known the ERTMS/ETCS shall be compliant with THR of 2e-9/hour/ train (SIL 4). It is the reason why it is not necessary in this document to hark back to rail high-level user safety requirements on which bases rail system safety requirements (e.g. for ERTMS/ETCS) have been specified.

However, different situation is in the field of automated car driving where such widely acceptable user safety requirements are still missing. It is the reason why specification of high-level user safety requirements must naturally start from safety requirements for self-driving cars (SDCs) demanded by society. It is described in next section. Synergies with rail regarding risk harmonisation and specification of high-level user safety requirements for SDCs are utilised.

2.2 AUTO: HIGH LEVEL USER REQUIREMENTS FOR SELF-DRIVING CARS (SDCs)

2.2.1 Societal safety requirements for SDCs

At present many cars have already implemented some kinds of driver assistance functions and the race between automotive companies globally is heading towards fully self-driving cars (SDCs). Safety becomes out of doubt a fundamental issue in this development.

A risk acceptance criterion, which is a measure of the widely acceptable safety, represents a critical attribute reflecting a consumer trust in SDCs. It enables to estimate whether and when the driverless vehicles will be mass-produced and put into operations. How much safe should driverless vehicles be to be accepted by society? Respondents of one latest survey [2] expect that self-driving vehicles should be four to five times safer than human driven vehicles. It also implies that the responders expect the global road traffic fatality risk (TFR) should be reduced by about 2 orders (see Fig. 5) [2]. The current world TFR is estimated as 17.4 fatalities per 100,000 population and year (~ 10,000 hours). It implies that the responders also assume that the acceptable risk associated with a driverless car should approximately correspond to the safety level currently guaranteed on railway or in civil aviation [2].

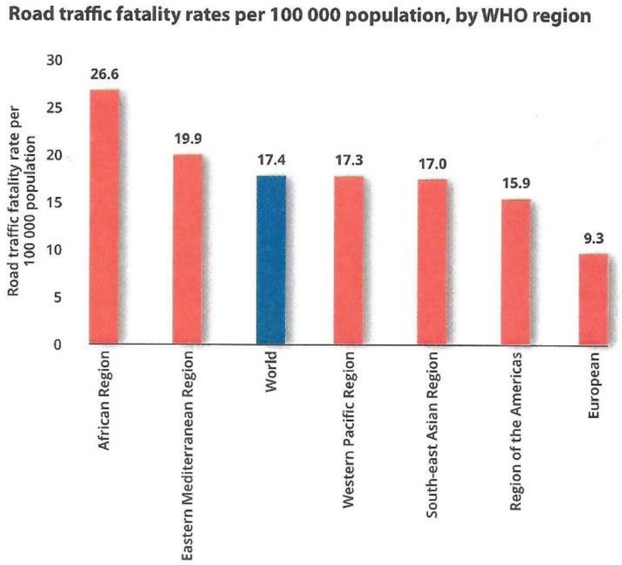


Figure 5. Road traffic fatality rates (TFRs) per 100 000 population and year according to regions [3]

Note: TFR as measure of safety risk is not defined per car occupant but generally per population and year in a given region.

But safety is not for free. Designing the required high safety levels into a technical system usually requires a lot of effort and great amount of financial resources. It is even more complicated in case of SDCs where one can anticipate millions and millions of different operational situations which cannot be sufficiently tested during a reasonable period of time to provide convincing evidence that the required safety of a self-driving car has been met. Therefore, it is necessary to look into other land transport sectors for which also high safety integrity systems were developed and where have been safely operated, and search for the experience right there.

Railway traditionally belongs to a regulated and very safe transport sector [3]. From the very beginning railway safety is based on conservative principles and worst-case approach. The worst-case approach considers many scenarios and assumptions that are unlikely to occur simultaneously. Excepting safety, a great attention is also paid to efficiency of railway operations. Railway technical systems shall be safe enough but shall be not safer than actually required, otherwise they would be more expensive and no one would use them.

The European Railway Traffic Management System (ERTMS) is a standardised commanded and control system conceived to intervene in case of driver's errors by supervising the maximum allowed speed and stopping position of the train. ERTMS is in operation by more than 20 years and it ensures the highest safety level ever achieved in the transport sector – it is compliant with a Tolerable Hazard Rate (THR) of 10^{-9}/h/train. ERTMS is also already considered a world-wide signalling standard, because after Europe it has become successful in Asia – mainly in China, Turkey, Taiwan and South Korea. Furthermore, the technical interoperability was a key driver for ERTMS [4] to allow trains to use equipment of different manufactures operated in railway command systems provided by other suppliers. Harmonised safety requirements for baseline ERTMS with track balises have been specified in CCS TSI (Control Command Signalling Technical Specifications for Interoperability) and related subsets. Safety requirements for ERTMS virtual balise detected by GNSS have been specified in the same way. It means that in case of ERTMS it was not necessary to start with derivation od safety requirements for GNSS and related Virtual Balise Reader (VBR) from the socially acceptable risk. It is because of a long-term experience of railways with operations of safety-related systems. The previous expertise concerning specification of system safety requirements for ERTMS significantly contributed to the simplified derivation of safety requirements for the virtual balise including GNSS. Harmonised safety requirement for GNSS position determination have been specified for ERTMS in Europe.

However, such approach cannot be repeated in case of determination of safety requirements for self-driving cars due to lack of sufficient experience with safety management process in this field. Here, it is necessary to start with requirements determination from scratch. After that the railway experience regarding risk harmonization could be utilized.

2.2.2 Harmonization of risk and safety requirements for SDCs

Safety risk of future automated car driving systems consisting of a vehicle on-board unit with automated steering functions and cooperating with a way-side infrastructure has to be appropriately measured, controlled and evaluated. While the society more or less accepts mortality figures caused by existing cars with no or limited grade of automated steering, there is likely to be almost zero tolerance for any fatal accidents due to a potential technical failure of Automatically Commanded Steering Functions (ACSF). If the above mentioned global road TFR value should be reduced by 2 orders on the basis of the survey results and expressed per 1 hour, then it corresponds to $TFR_{reduced} = 0.17x10^{-9}$/ h. One of risk acceptance criteria that is called MEM (Minimum Endogenous Mortality) and which has been used for railway safety evaluation, assumes that no single technical system should contribute more than $1x10^{-5}$ fatality/ year, i.e. $1x10^{-9}$/ h [5]. In some cases a magnitude of Target Individual Risk (TIR) of fatality, which can be used for railway Tolerable Hazard Rate (THR) determination, is conservatively set less than $1x10^{-9}$/ h - e.g. $1x10^{-10}$/ h [6], [7]. It is also sometimes justified by the assumption that 10% of the total risk ($1x10^{-9}$/ h) is allocated to railway signalling, or an additional safety factor of 10 is added to TIR [7]. It independently confirms the fact presented in previous section that the socially acceptable safety level of future driverless cars estimated in [2] should be approximately at the same (high) level as it common on railway.

There are currently not available widely acceptable Risk Acceptance Criteria (RAC), which could be used for safety evaluation and assessment of cars with automated driving on the transportation system level. There is not even any consensus among automated car makers regarding target safety system requirements (design targets), which could be used e.g. for comparison of automated driving systems from viewpoint of safety or for regulation purposes by public authorities. This situation is completely different in the field of railway systems where safety requirements for these systems are well specified, justified and harmonised.

The European railways already use the concept of Common Safety Targets (CST) [8], which means in fact the minimum safety levels that are to be reached by the railway system as a whole. CSTs are hence more generic and they do not relate to the technical system only. Excepting this, it is also recommended to railways to use so called Common Safety Method Design Targets (CSM-DT) [9]-[10] that are in fact harmonised quantitative safety requirements for railway safety systems if a so called explicit risk estimation should be performed – i.e. when a long-term experience with safety system is missing. CSM-DT well correspond to the current European safety levels and approaches to the qualitative risk assessment on railways. These railway safety levels are similar to the corresponding safety levels in aviation. It seems that the introduction of a similar safety measures for automated driving would not only to help to simplify specification of reasonable (and widely acceptable) safety requirements for SDCs, but also their certification and approval process of SDCs.

2.2.3 High-level user requirement for SDCs

Table 2 contains a set of safety measures used for comparison of different means of travel used for derivation for safety requirements for SDCs [11]. It is based on UK data in the period 1990-2000.   It is possible to find more recent risk statistics for different modes of travel evidencing transport safety improvement during last 2 decades, especially in more developed countries. Nevertheless it is also clear from recent German statistical accident data [12] that fatality risk in automobile is 75 times higher than in train (car: 2.26 fatality/ 1e9 person-km vs. train: 0.03 fatality /1e9 person-km) and injury risk in car is 127 times higher than fatality risk in train (car: 248.33 injuries/ 1e9 person-km vs. train: 1.96 injuries/ 1e9 person-km). There are also differences in railway safety according depending on regions. For example railway fatality risk for the EU-27 (2007-2012) was half of the railway fatality risk in USA [13]. In this report it is intended to start with derivation of safety requirements for SDCs from “average” values of safety measures, similarly as the world “average” road Traffic Fatality Rate is used as a measure of road safety.

As mentioned in Section 2.2.1, the conclusion of the public survey [2] is that responders would like to have SDCs as safe as trains or airplanes. Therefore, the safety performance of travel by rail or airplane (3e-8/ hr) is taken as a starting point for derivation of safety requirements for self-driving cars. The corresponding average speed of airplane and train converting fatality risk per km to safety risk per 1 hour is 600 km/ hr and 50 km/hr, respectively – see Table 2. An average speed of car is 42 km/ hr according to Table 2.

Table 2. Fatality risk of various forms of travel [11]

Fatalities per billion:	**Journeys**	**Hours**	**Kilometres**
Air	117	30.8	.05
Bicycle	170	550	44.6
Bus	4.3	11.1	.4
Car	40	130	3.1
Foot	40	220	54.2
Motorcycle	1,640	4,840	108.9
Rail	20	30	.6
Van	20	60	1.2
Water	90	50	2.6

Automotive GNSS applications are classified according to conclusions of GNSS‘ User Consultation Platform [14] into following groups:

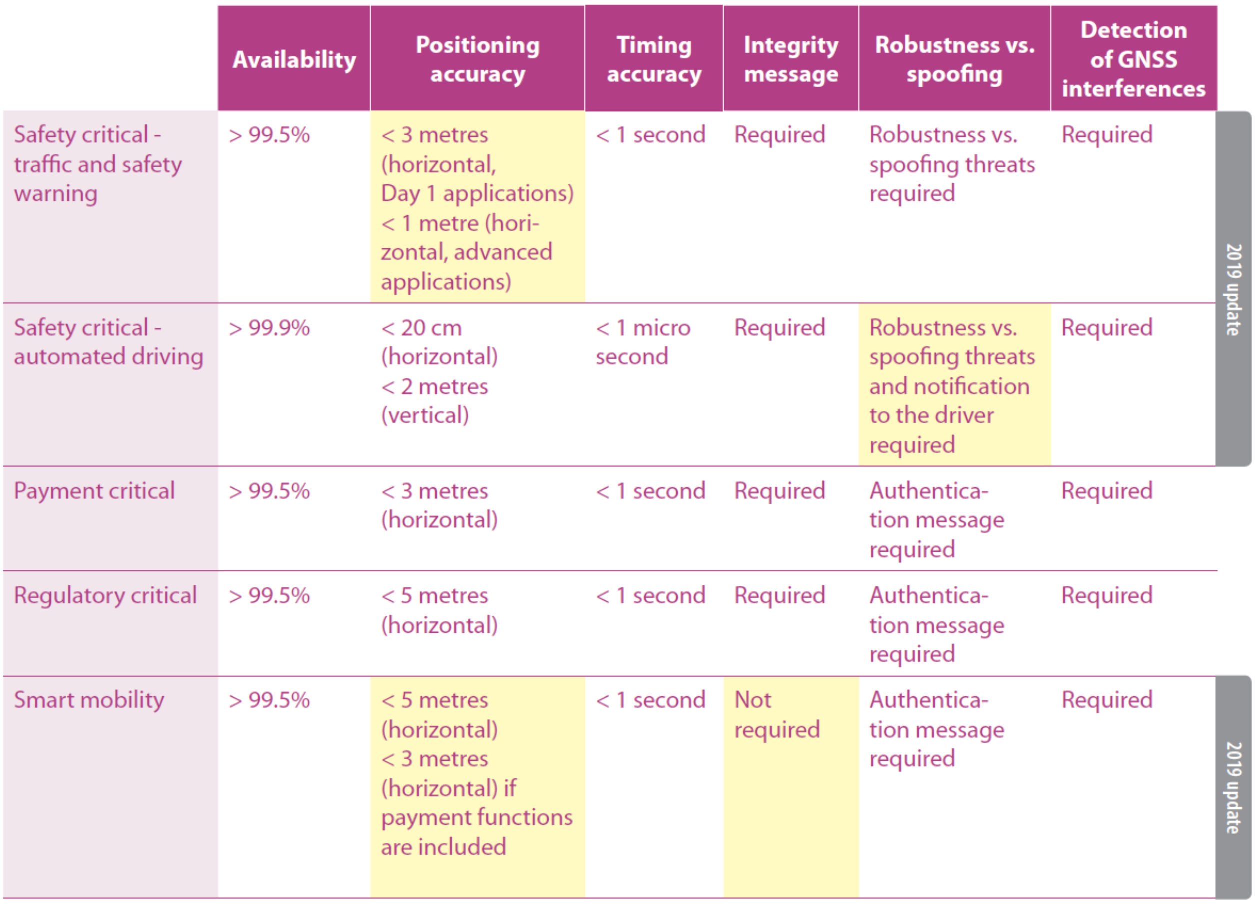
- Safety critical applications;
- Payment critical applications;
- Regulatory critical applications, and
- Smart mobility.

2.2.4 High-level road user performance requirements

The latest set of high-level road user performance parameters for GNSS-based positioning is shown Table 3 [14].

These user requirements were specified after numerous discussions of rail community within User Consultation Platform organised by the European GNSS Agency in the period 2017-2018. The requirements were updated in 2019.

Table 3. Performance parameters of car position determination GNSS based [14]



	Availability	Positioning accuracy	Timing accuracy	Integrity message	Robustness vs. spoofing	Detection of GNSS interferences	
Safety critical - traffic and safety warning	> 99.5%	< 3 metres (horizontal, Day 1 applications) < 1 metre (horizontal, advanced applications)	< 1 second	Required	Robustness vs. spoofing threats required	Required	2019 update
Safety critical - automated driving	> 99.9%	< 20 cm (horizontal) < 2 metres (vertical)	< 1 micro second	Required	Robustness vs. spoofing threats and notification to the driver required	Required	
Payment critical	> 99.5%	< 3 metres (horizontal)	< 1 second	Required	Authentication message required	Required	
Regulatory critical	> 99.5%	< 5 metres (horizontal)	< 1 second	Required	Authentication message required	Required	
Smart mobility	> 99.5%	< 5 metres (horizontal) < 3 metres (horizontal) if payment functions are included	< 1 second	Not required	Authentication message required	Required	2019 update

The most demanding requirements in Table 3 regarding accuracy and safety integrity have been selected as a starting point for definition of the most relevant operational scenarios and further refinement of the GNSS UCP requirements for automotive applications.

These most relevant high-accuracy and high-integrity railway operational scenarios for HELMET are following:

- Safety critical – automated driving, and
- Safety critical – traffic and safety warning.

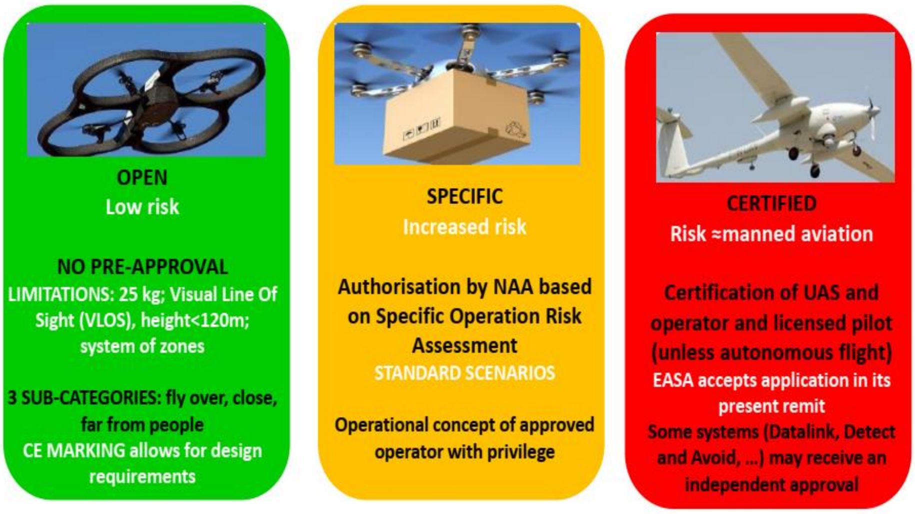
It is evident from Table 3 that the highest positioning accuracy < 20 cm horizontally, and < 2 m vertically is required by users for automated car driving applications, while horizonal accuracy < 3 m (or < 1 m horizontally for advanced applications) is required for traffic and safety warning. In addition, a guarantee of accuracy of speed measurement is also required. Since requirements for automated driving are most demanding from the road user point of view, this application is further described in more details below and the relevant user requirements are refined and justified.

2.3 UAV/RPAS-PIT SEGMENT: HIGH LEVEL USER REQUIREMENTS FOR AERIAL IMTM SERVICES

2.3.1 Societal Safety Requirements for UAV/RPAS Inserted in ECAC's Airspace

EU citizens are impacted by risks related to UAS/RPAS operations, either as clients of UAS/RPAS services or UAS/RPAS users for private purposes. UAS/RPAS could support innovative services with a high business potential; however, they pose a safety, security, and privacy risk. On request by the European Commission, Member States and other stakeholders, EASA has developed proposals for an operation centric,proportionate, risk- and performance-based regulatory framework for all unmanned aircraft (UA) establishing three categories with different safety requirements, proportionate to the risk, namely:

1) <u>"Open" (low risk)</u> is an UAV operation category that, considering the risks involved, does not require a prior authorization by the competent authority before the operation takes place;
2) <u>'Specific' (medium risk)</u> is an UAV operation category that, considering the risks involved, requires an authorization by the competent authority before the operation takes place and takes into account the mitigation measures identified in an operational risk assessment, except for certain standard scenarios where a declaration by the operator is sufficient;
3) <u>'Certified' (high risk)</u> is an UAV operation category that, considering the risks involved, requires the certification of the UAS, a licensed remote pilot and an operator approved by the competent authority, in order to ensure an appropriate level of safety.



OPEN
Low risk
NO PRE-APPROVAL
LIMITATIONS: 25 kg; Visual Line Of Sight (VLOS), height<120m; system of zones
3 SUB-CATEGORIES: fly over, close, far from people
CE MARKING allows for design requirements

SPECIFIC
Increased risk
Authorisation by NAA based on Specific Operation Risk Assessment
STANDARD SCENARIOS
Operational concept of approved operator with privilege

CERTIFIED
Risk ≈manned aviation
Certification of UAS and operator and licensed pilot (unless autonomous flight)
EASA accepts application in its present remit
Some systems (Datalink, Detect and Avoid, …) may receive an independent approval

The Table 4 below summarizes the current EASA's Concept of operations for UAV/RPAS. The Current Regulatory Frame Requirements of EASA (EU State Members Civil Aviation Regulatory Institutions) and Operational Limitations for small UAV/RPAS to up 25kg TOW.

Table 4. Overview of the EASA of some EU Member States' Regulations on UAV/RPAS up to 25kg TOW (Reference EASA A-NPA 2015-10).

AT	Below 5 kg maximum take-off weight (MTOM) Between 5–25 kg	Visual Line of Sight (VLOS) only	Undeveloped, Unpopulated, Populated, Densely populated
DK	Below 7 kg MTOM Between 7–25 k	VLOS only < 100 m above ground level (AGL)	150 m from road and buildings; never over densely built areas

FR	Below 2 kg MTOM Between 2–25 kg	S1 = VLOS < 100 m distance from remote pilot
		S2 = VLOS, within 1 000 m distance from remote pilot; maximum altitude < 50 m AGL
		S3 = VLOS, within 100 m distance from remote pilot
		S4 = observations — 150 m AGL
			S1 = unpopulated area
			S2 = unpopulated area
			S3 = populated area
			S4 = unpopulated area

DE	Below 5 kg MTOM: Federal State Above 5 kg: federal competence	VLOS only, < 100 m AGL	
ES	2 main categories: below/above 25 kg	< 2 kg: beyond visual line of sight (BVLOS) & AGL < 120 m < 25 kg VLOS 500 m and AGL < 120 m > 25 kg: subject to the limits imposed by the Civil Aviation Authority (CAA)	**< 2 kg:** only away from inhabited places **< 25 kg:** only away from inhabited places **> 25 kg:** specific conditions
IT	2 main categories: below/above 25 kg CAA may provide simplified procedures for UAV < 2 kg	'V70': 70 m (230 ft) max AGL and 200 m radius 'V150': 150 m (500 ft) AGL and 500 m radius	At least 150 m from congested areas and at least 50 m from persons and property

SE	Below 1.5 kg MTOM or <150 joule
	Between 1.5 and 7 kg or < 1 000 joule
	Between 7–150 kg
		S1 = VLOS, below 1.5 kg
		S2 = VLOS, 1.5 and 7 kg
		S3 = VLOS, > 7 kg
		S4 = beyond line of sight (BLOS) Always < 120 m AGL
			Distance drone/persons and property: > 50 m

UK16	Below 20 kg MTOM excl. fuel/incl. battery Between 20–150 kg	Max speed: 70 kt; 400 ft AGL < 500 m distance from remote pilot	> 150 m from buildings > 100 m from people

Maximum Take-off Mass (MTOM)/energy threshold requirements are one of the criteria for the sub-categorization of UAS/RPAS in the Open Category and impact the Societal Safety and thus the acceptance of these systems while Categories "Specific" and "Certified" require specific approvals and/or certification by the Civil Aviation Authorities. These criteria are used together with others in order to define sub-categories of operations and UAS classes. The rationale behind the masses and energy thresholds defined with regard to the risk posed by blunt-trauma injury (non-penetrating injury) inflicted on people by a UAS. Penetrating injuries should be prevented by a UAS/RPAS design that does not expose uninvolved persons to the risk of injury inflicted by acuminated parts or cutting edges, for example, blade protection. But this aspect is not addressed in more detail in this document.

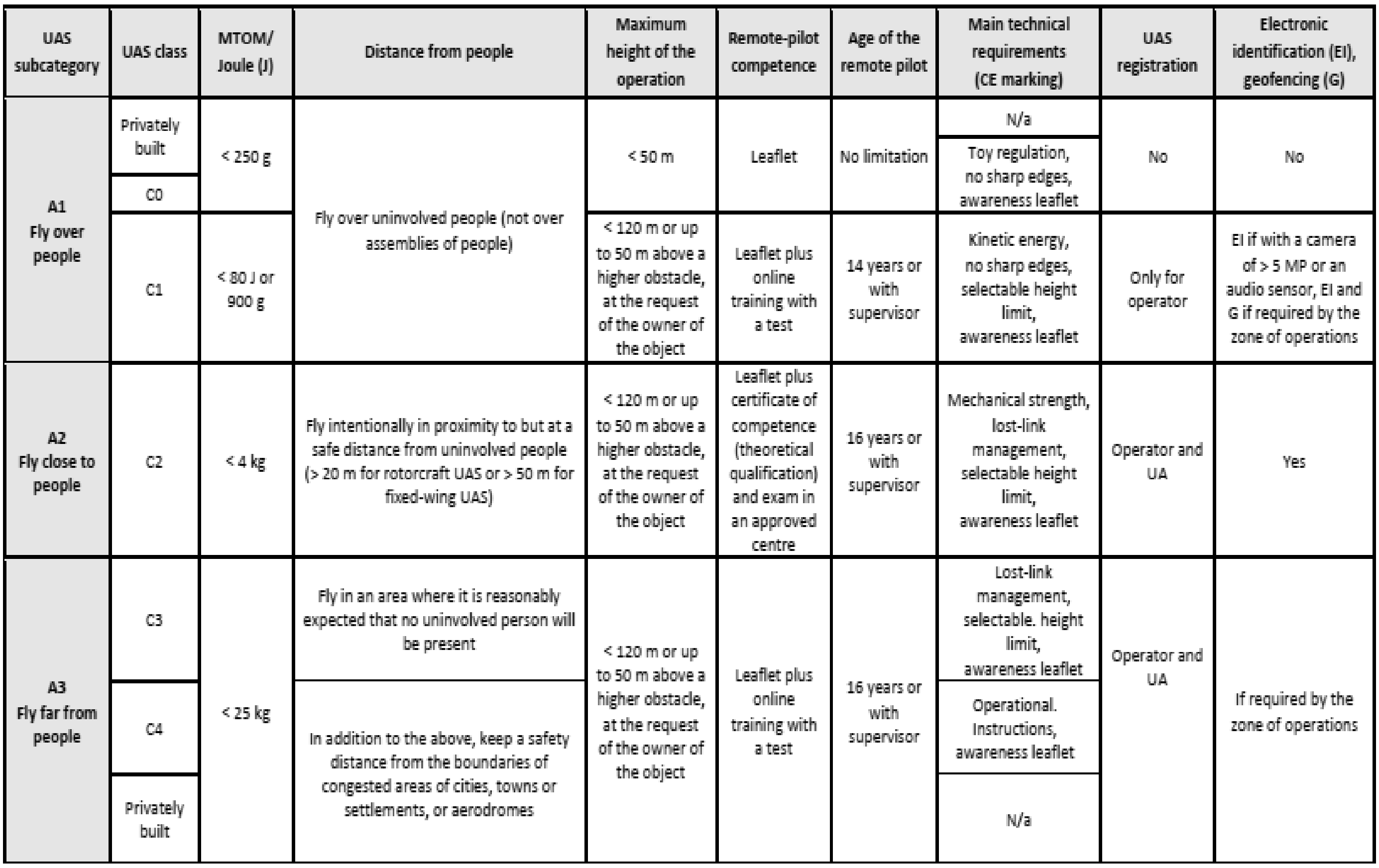
Referring to the Table 5 below, Subcategory A1, Class C0 can be operated by minors, without any training required. Occasionally, UAS/RPAS might fly over assemblies of people. In view of the above, a UAS of this Subcategory and Class must be intrinsically unable to harm people in case it collides with people due to remote pilot error or UA failure. The 250-g MTOM threshold is proposed as a conservative mass to prevent significant blunt trauma. This threshold is justified by the following:

a) It has been adopted for the smallest proposed category by the FAA Micro ARC of the March 2016, aimed at making a recommendation for a future FAA rule for UA/RPA allowed to fly over people.
b) It is the MTOM threshold identified by the FAA registration task force: UA with an MTOM of less than 250 g are not registered. To identify this MTOM, the risk equation was applied.

c) Considering RCC studies-based estimates, it has been shown that a kinetic energy of 44 J impacting a human body, averaged on the body of a person standing, would result in a probability of fatality (PoF) of 1%. From a linearization of the relationship between MTOM and terminal kinetic energy, valid for small rotorcraft, this equates to about 250 g. There is some evidence that RCC studies are overly conservative if applied to UAS collisions with people, however, given the scope of this Subcategory and Class, it is preferred to retain a very conservative value.

Referring to Table 5 again to Subcategory A1, Class C1 then in this case, a minimum age and a minimum level of knowledge would be required for operating the UA/RPA, and flying over crowds, even occasionally, would be prohibited; it would be allowed to fly the UA/RPA only over isolated people and at a safe distance. A kinetic-energy value was calculated based on experiments that better resemble the possible UAS/RPAS impact on a person. The impact scenario considered is that of a multi-rotor UA/RPA falling from the maximum allowed altitude and reaching a person's head at a 45 ° angle with respect to the vertical. Among available data from literature, it is proposed to consider the Gurdjian experiments with real embalmed human heads being dropped from a certain height on a solid, not moving plate. 17 specimens were impacted on the anterior parietal zone, 10 on the posterior parietal zone. The frontal zone is not considered as people would normally spot a UAS approaching, with their frontal zone facing the UAS, and would either shift or cover themselves with their hands. Temporal data are not available.

Table 5. MTOM/Energy Threshold Requirements for UAS "Open" Category Sub-classes (Source EASA A-NPA 2015-10)



UAS subcategory	UAS class	MTOM/ Joule (J)	Distance from people	Maximum height of the operation	Remote-pilot competence	Age of the remote pilot	Main technical requirements (CE marking)	UAS registration	Electronic identification (EI), geofencing (G)
A1 Fly over people	Privately built	< 250 g	Fly over uninvolved people (not over assemblies of people)	< 50 m	Leaflet	No limitation	N/a	No	No
	C0						Toy regulation, no sharp edges, awareness leaflet		
	C1	< 80 J or 900 g		< 120 m or up to 50 m above a higher obstacle, at the request of the owner of the object	Leaflet plus online training with a test	14 years or with supervisor	Kinetic energy, no sharp edges, selectable height limit, awareness leaflet	Only for operator	EI if with a camera of > 5 MP or an audio sensor, EI and G if required by the zone of operations
A2 Fly close to people	C2	< 4 kg	Fly intentionally in proximity to but at a safe distance from uninvolved people (> 20 m for rotorcraft UAS or > 50 m for fixed-wing UAS)	< 120 m or up to 50 m above a higher obstacle, at the request of the owner of the object	Leaflet plus certificate of competence (theoretical qualification) and exam in an approved centre	16 years or with supervisor	Mechanical strength, lost-link management, selectable height limit, awareness leaflet	Operator and UA	Yes
A3 Fly far from people	C3	< 25 kg	Fly in an area where it is reasonably expected that no uninvolved person will be present	< 120 m or up to 50 m above a higher obstacle, at the request of the owner of the object	Leaflet plus online training with a test	16 years or with supervisor	Lost-link management, selectable. height limit, awareness leaflet	Operator and UA	If required by the zone of operations
	C4		In addition to the above, keep a safety distance from the boundaries of congested areas of cities, towns or settlements, or aerodromes				Operational. Instructions, awareness leaflet		
	Privately built						N/a		

From the reported terminal speeds, when the initial fracture was recorded, as well as from the weight of the specimens, it is possible to derive the kinetic energy at impact and take the overall average. The result is about 80J. A Monash University paper refers to computer simulation of head impacts on a flat rigid structure, yielding energy values between 80 and 95J, to start seeing skull fractures. This information seems to conservatively confirm the 80J identified through the Gurdjian experiments. Other fracture experiments are also available in literature, where pressure was applied to various parts of the skull.

In some cases, recorded data include peak forces and accelerations, but the skulls seem to have been compressed on relatively smaller areas. It is believed that between the two kinds of experiments, those involving collision with a flat surface have a better resemblance with the blunt trauma resulting from a possible UAS/RPAS impact. In the Gurdjian experiments, the energy is fully transferred to the head as there is no deformation or movement of the surface impacted. In conclusion, the value of 80J is retained as the threshold kinetic energy that the head of the average person would be able to absorb without the skull being fractured. It is difficult to associate a PoF with this threshold, but there are reasons to consider the above estimate as conservative:

a) the experiments with the skull specimens included several impacts before fracture; as a consequence, it may be assumed that the skulls could have been weakened before reaching the rupture threshold;
b) a living person's head should be more resistant than the embalmed heads used in the experiments; and
c) the rupture of the skull does not necessarily lead to a fatality (although it would certainly be a major trauma).

This substantiates the 80J threshold value of absorbed kinetic energy as an acceptable one for Class C1. In a collision with a UA/RPA, only a fraction of the UA/RPA kinetic energy would be transferred to the head. As described further, the kinetic energy absorbed in average by a human head hit by a UA in free fall is estimated to be 46.5 % of the terminal kinetic energy of the UA/RPA, expressed as half of the aircraft MTOM multiplied by the square of its terminal velocity (reaching ground). This fractional value may have been conservatively calculated, and, given the uncertainties of collision dynamics, other assumptions may be possible. A terminal kinetic energy under 80/0.465 = 172J for the UA/RPA would be therefore allowed. Using a linear approximate relationship between terminal kinetic energy and MTOM (about 48J for every 250 g of MTOM of relatively small multi-copter currently available on the market), the 172J threshold equates to an MTOM of approximately 900 g. In conclusion, an MTOM of 900 g can be considered as a good threshold to allow a Class C1 UA/RPA to be flown over isolated people. UAS/RPAS with a greater MTOM could also qualify if the manufacturer demonstrates that the kinetic energy transmitted to the head would be less than 80J.

<u>Note:</u> *on 28 April 2017, the final report of the FAA UAS Center of Excellence Task A4 'UAS Ground Collision Severity Evaluation' was published. This very detailed and rich in information report will be analysed by EASA during the public-consultation period of this NPA, to assess potential implications for the thresholds established above. Considerations on the kinetic energy transferred to a human head during a collision with a vertically falling multi-copter. The most common mass-produced multi-copter UA on the market, with an MTOM between 250 g and 2 kg, is the Phantom DJI. Its dimensions are approximately the ones provided in the following picture:*

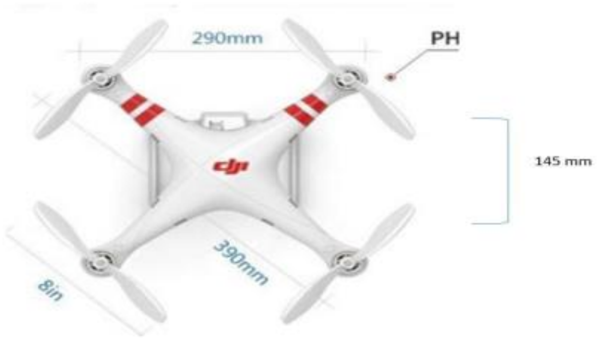


Figure 6. Common Mass-Produced Multi-copter UA/RPA

Herein are provided some considerations on the kinetic energy transferred to a human head during a collision with a vertically falling multi-copter. The most common mass-produced multi-copter UA/RPA, with an MTOM between 250 g and 2 kg, is the Phantom DJI. Its dimensions are approximately the ones provided in Figure 6 above.

In general, it is assumed that if the UA/RPA hits a person's head with one of its arms, the UA would rotate away and a relatively small fraction (F1) of the impacting kinetic energy would be transferred during the impact. The fraction would be much higher (F2) if the collision would occur at the centre of or within the square area of the 145mm side in the example above. The following is an evaluation of those values (F1 and F2): For value F1 and based on information presented during EASA expert meetings on the subject of small UA/RPA and energy balances that could be considered during a collision, as well as on engineering judgment, it is considered that by hitting exactly in the centre, the UA/PRA would partially bend or be destroyed, absorbing in the process about 7 % of the impacting kinetic energy: Kinetic energy transferred = 0.93 x impacting kinetic energy As for value F2, if the UA/RPA would hit the head with its terminal part of the arm (tip), the transferred kinetic energy would tend to zero as the UA/RPA would most likely rotate away. In order to simplify those two scenarios, a linear behaviour of the kinetic energy transferred to the person's head between the following two extremes is assumed:

a) impact at the centre: 0.93 x impacting kinetic energy; and
b) impact at the tip: 0.

The average would therefore be (0.93 x impacting kinetic energy + 0)/2 = 0.465 x impacting kinetic energy. The impacting kinetic energy of a UAS/RPAS in free fall can be conservatively considered to be its terminal kinetic energy. In conclusion, according to the above estimates, it is considered that the kinetic energy of a UA/RPA in free fall transmitted to a person's head would be in average 46.5 % of the UA terminal kinetic energy.

2.3.2 User High Level Risk and Safety Requirements for UAS/RPAS

2.3.2.1 Risk for Safety Assessment Methodology Overview

A detailed Risk Assessment for Safety shall take into account the UAS/RPAS operational complexity factors, including the size of the aircraft, location, altitudes, airspace classification and complexity of the operation, day/night operations and mitigations that may be imposed. In general the Risk for Safety requirements are related to the following items:

a) UA size and physical characteristics (mass and materials) could influence the likelihood that the aircraft may injure people, damage property or damage another aircraft
b) Proximity to aerodromes or restricted/segregated airspace could increase the likelihood of a collision with other airspace users
c) Operations in populated or congested areas could increase the likelihood of injury to persons and loss of control due to frequency interference, loss of GNSS signal or other factors
d) Operating altitudes and/or airspace classification could influence the likelihood of a collision with other airspace users
e) Complex pilot tasks or complex operating environments could also increase the likelihood of an incident or accident

Table 6 provides the safety objectives to maintain safe flight and landing of various UA/RPA categories

Table 6. Derived Safety Objectives to Maintain Safe Flight and Landing

Example Aircraft Type	RPAS Complexity Level	Accident Rate (pfh)	10% Due to Systems	No. of Potential Catastrophic failure conditions	Probability of a Catastrophic Failure Condition (pfh)
Manned CS-23 class I	N/A	1x10-4	1x10-5	10 (10-1)	1x10-6
RPAS CS-23 class I	CL I	1x10-4	1x10-5	10 (10-1)	1x10-6
CL II	1x10-4	1x10-5	100 (10-2)	1x10-7	
CS-LURS	CL I	1x10-4	1x10-5	10 (10-1)	1x10-6
CL II	*1x10-4*	*1x10-5*	*100 (10-2)*	*1x10*	

2.3.2.2 Airspace Specific Operational Risk Assessment (SORA)

The Joint Authorities on Rulemaking for Unmanned Systems (JARUS) has developed guidelines on performing a Specific Operational Risk Assessment (SORA) [JARUS, 2017]. EASA has adopted the final version of the SORA, which is available since early 2019, as an Acceptable Means of Compliance for the risk assessment required from operators in the Specific category. UAS can pose a serious safety and security threat. There is a real need to ensure that they only fly in areas of airspace and in certain conditions in a way that will ensure the safety, security, privacy of people, property and state apparatus to the greatest extent possible. The environmental impact should also be minimised. SORA provides a method for minimising this: especially those aspects that concern the safety of people or of property through assessments of ground risks and air risks. SORA looks at these risks from the operator's perspective. It proposes a means of evaluating risks and mitigations to enable an authority to authorise a given operation. It analyses whether the operator has ensured all that is required to conduct a safe flight, i.e. it deals with the pilot, the aircraft, the airspace, and people and infrastructure on the ground.

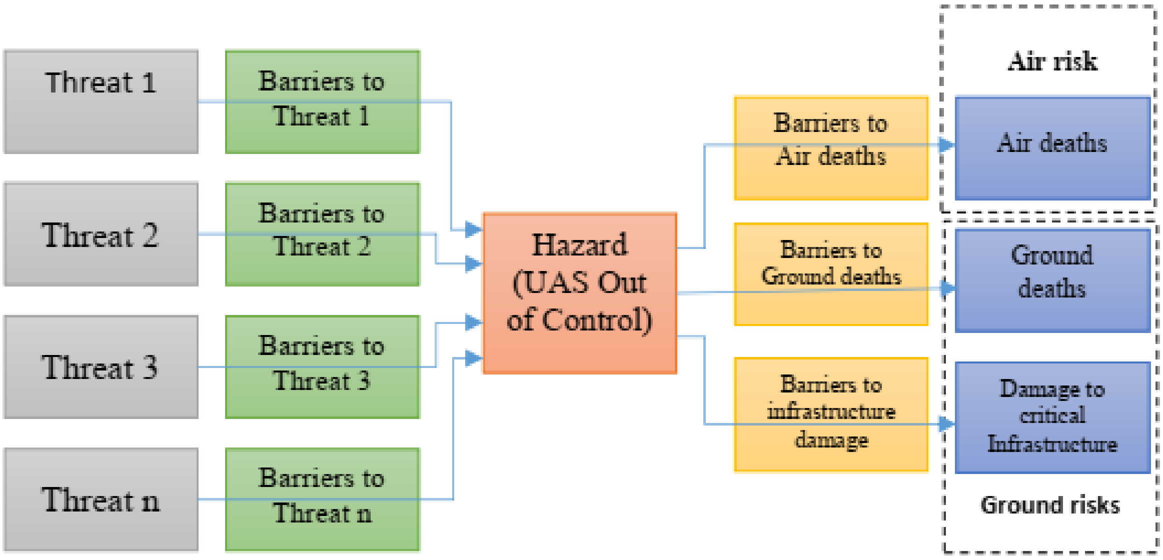
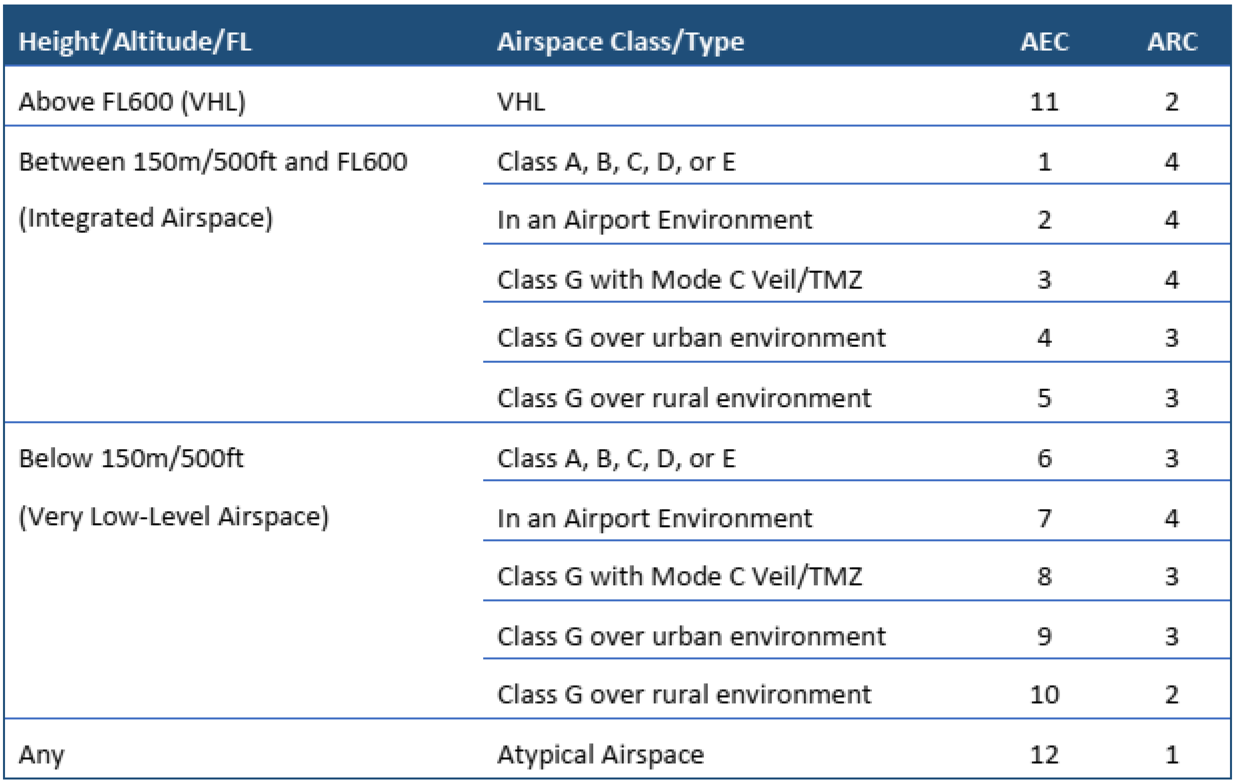


Figure 7. Schematic Representation of the SORA Concept (Source: EUROCONTROL)

The SORA concept is based around the idea of the "hazard" that a UAS operation could become "out of control", which the guidelines consider in its widest sense of its being conducted outside of its approved conditions. It looks at the "threats" that could cause this loss of control and the impacts (or "harms" as it calls them) that it could have. The risks of these "harms" occurring are divided into ground risk and air risk. SORA enables the operator to specify the barriers and mitigations to these threats and impacts that have been put in place to minimise these risks. This is shown in Figure 7. For the ground risk, ground risk classes are assigned and barriers that can mitigate the death and destruction on the ground are identified. The final lethality of the ground risk can then be determined. If the operation in question is BVLOS over a populated area with a UA of 3m or more, or VLOS over a populated area with a UA of 8m or more, the ground risk is so great that the SORA is not an appropriate tool for ensuring safety. Similarly, the perceived level of air risk – the risk of a mid-air collision - is incorporated though an Airspace Encounter Category (AEC) for a given region of airspace. The SORA method assigns an Air Risk Class (ARC) ranging from 1 (low risk) to 4 (high risk) to these AECs – see Table 7– based on three factors: the rate of proximity, dependent on the number of aircraft assumed to be in the airspace; the geometry of the aircraft, use of specific routes etc., in the airspace; dynamics, or how fast aircraft travel in the airspace. Measures can be proposed to reduce these impacts.

Table 7. Airspace Encounter Categories and Air-Risk Classes (Source: EUROCONTROL)



Height/Altitude/FL	Airspace Class/Type	AEC	ARC
Above FL600 (VHL)	VHL	11	2
Between 150m/500ft and FL600 (Integrated Airspace)	Class A, B, C, D, or E	1	4
	In an Airport Environment	2	4
	Class G with Mode C Veil/TMZ	3	4
	Class G over urban environment	4	3
	Class G over rural environment	5	3
Below 150m/500ft (Very Low-Level Airspace)	Class A, B, C, D, or E	6	3
	In an Airport Environment	7	4
	Class G with Mode C Veil/TMZ	8	3
	Class G over urban environment	9	3
	Class G over rural environment	10	2
Any	Atypical Airspace	12	1

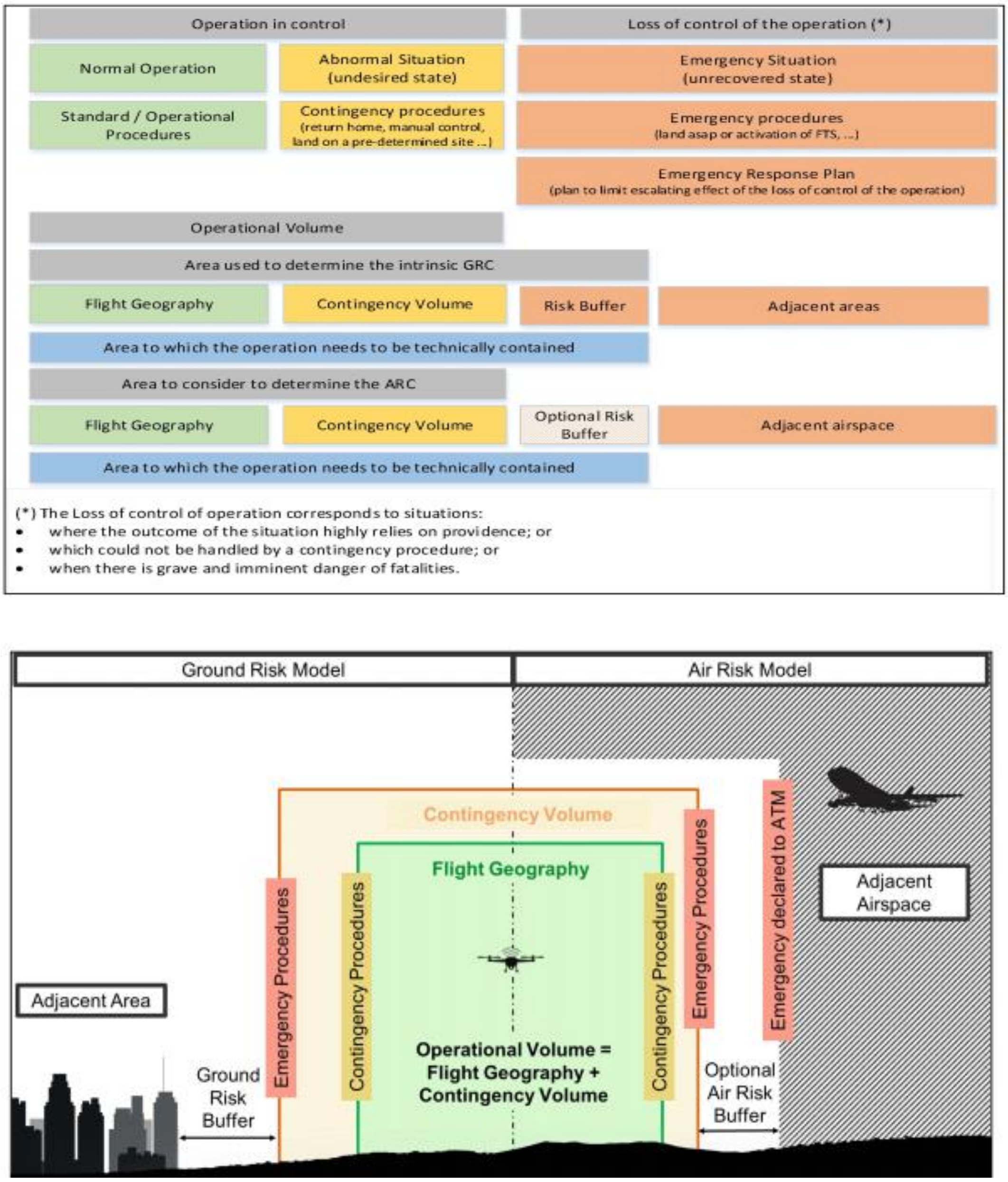
Once the ground and air risks and their mitigations have been determined, the mitigation of, or barriers to, the various threats that could cause the loss of control can be analysed. Finally, the safety of the operation can be confirmed. It is clear that an airspace assessment is necessary for evaluation both air and ground risks – which regions are above large populations, which are in proximity of vital infrastructure etc. Such an assessment will also provide the operator with additional barriers to the impacts that they need for the flight to be authorised by enabling a flight to be planned to avoid areas of high impact where possible. These airspace assessments can also be a major factor in reducing the threats of an out-of-control flight by an operator to keep the UA clear of areas of electromagnetic interference etc.

For the purposes of the HELMET Project, the standard methodology to derive UAS/RPAS Risk for Safety parameters to be used detailed assessment of Risks shall be in accordance with JARUS guidelines on SORA Package, Related Annexures and JARUS-STS-01, JAR-DEL-WG6 -D.04 Edition No. 1.1, 11 November 2019 and JARUS guidelines on SORA JARUS-STS-02, JAR-DEL-WG6 -D.04 Edition No.1, 25 September 2019.

The SORA methodology (see Fig. 8) is intended to cover UAS/RPAS operations for performed in the Specific category (category B) with the following main attributes:

a) unmanned aircraft with a maximum characteristic dimension (e.g. wingspan or rotor diameter/area) up to 3 m and a typical kinetic energy up to 34 kJ,
b) operated beyond visual line of sight (BVLOS) of the remote pilot, over sparsely populated areas,
c) In airspace reserved for the operation, either danger area or restricted area appropriate for unmanned aircraft operations.
d) under 150m (500 ft) above the overflown surface (or any other altitude reference defined by the state), (JARUS-STS-02) and
e) in uncontrolled airspace (JARUS-STS-02)

The above attributes are in line with the HELMET Project small UAS/RPAS (EASA Specific and Certified Categories) for BVLOS operations for IMTM services to Rail and Automotive in Extra-Urban environments.



Operation in control | Loss of control of the operation (*)

Normal Operation | Abnormal Situation (undesired state) | Emergency Situation (unrecovered state)

Standard / Operational Procedures | Contingency procedures (return home, manual control, land on a pre-determined site ...) | Emergency procedures (land asap or activation of FTS, ...)

Emergency Response Plan (plan to limit escalating effect of the loss of control of the operation)

Operational Volume

Area used to determine the intrinsic GRC

Flight Geography | Contingency Volume | Risk Buffer | Adjacent areas

Area to which the operation needs to be technically contained

Area to consider to determine the ARC

Flight Geography | Contingency Volume | Optional Risk Buffer | Adjacent airspace

Area to which the operation needs to be technically contained

(*) The Loss of control of operation corresponds to situations:

- where the outcome of the situation highly relies on providence; or
- which could not be handled by a contingency procedure; or
- when there is grave and imminent danger of fatalities.

Figure 8. Graphical Representation of SORA Semantic Model

2.3.2.2.1 Overview of the Required Specific Operations Risk Assessment (SORA)

There are several different types of environment to be taken into account when performing an airspace risk for safety assessment with SORA (Fig. 8):

1) <u>Ground Risk</u>
   a) <u>Population Risks:</u> Those are risks which in general are related to permanently and/or cyclic populated areas (cycle < 1 day), Dense areas (city centre streets, etc.), Sensitive areas (schools, hospitals, etc.), Occasional and/or seasonal events (concerts, stadiums, etc.)
   b) <u>Security Risks:</u> Those are risks which in general are related to areas with military installations and/or facilities (airbases, shooting ranges, etc.), government off limits facilities, law enforcement areas etc.

c) Industry Risks: Those are risks which in general are related to Permanent and/or non-permanent industrial sites, Chemical and Nuclear sites, Laboratories, wind farm arrays, power stations, power lines, Cranes, obstacles, buildings, etc.
d) Transport Risks: Those are risks which in general are related to Airports, aerodromes and identified take-off and landing sites, model-flying sites, Roads and highways, Harbours, Rail, etc.
e) Environment Risks: Those are risks which in general are related to Animal Reservations

2) Air Risk: This risk is in general are related to High probability of traffic (hospitals, etc.), Seasonal or permanent recreational activities (base jump, flying suits, kite surf, etc.), uncontrolled airports, para-gliding areas, gliders, known areas for GA, Localised events (hotels water jets, geysers, etc.), Airports, aerodromes, emergency landing areas, and identified take-off and landing sites, helipads, model-flying sites, etc.

3) Threat Related Risk: This risk is in general are related to EMI due to Electro-magnetic wave-emitting sites (radars, high-voltage lines, solar farms, etc.), GNSS-outage forecast areas, EMC issues, Cyber Security issues, intentional and/or unintentional interference, etc.

In mitigating the above risks UAS/RPAS shall operate in a specific UTM system and/or operating under specific Geo-fenced applications, as soon as they are becoming available, which are capable of preventing UAS/RPAS from approaching restricted areas, such as airports, or on the contrary, ensuring that they do not fly outside of a given authorised area. Such systems could be used to restrict access to certain areas of sensitive airspace (geo-restriction) or to create “UAS/RPAS-dromes” where, for example, novice open category users could operate without interfering with other airspace users (geo-caging). Deciding which of these will apply to a given airspace zone is one of the major tasks of airspace assessment. For the specific IMTM UAS/RPAS HELMET Operations geo-fencing and/or geo-restriction can be imposed only partially and/or where possible.

2.3.2.2.2 Overview of the Required Specific Operations Risk Assessment (SORA) Methodology Steps

The SORA methodology consists of ten systematic steps:

Step 1: CONOPs Description
The CONOPs contains all the relevant technical, operational, and system information needed to assess the risk associated with the intended operation. It includes such things as the flight path, airspace, air and ground density maps, Air Navigation Service Provider (ANSP) interface, and other information related to the intended use of the UAS.

Step 2 and Step 3: Determination of Ground Risk Class (GRC)

a) Step2: The Intrinsic Ground Risk Class (scaled from 1 to 10) is first determined, depending on the UAS weight and physical dimensions, (with indication of typical expected kinetic energy released upon ground) as well as the intended operation.

b) Step3: The Final Ground Risk Class (that may be higher or lower than the intrinsic Ground Risk Class) is determined considering design aspects which may have a significant effect on the lethality of the drone and three mitigation measures :
   1. Strategic mitigations based upon ground risk buffer and overflown population density.

2. Mitigations intended to reduce the effect of a ground impact.
3. An Emergency Response plan to address and limit the effect of an operation out of control.

Step 4 and 5: Determination of the Air Risk Class (ARC) Both the initial and the residual risk after mitigations are applied.

a) Step 4: The initial ARC is assessed based on the airspace requested in the CONOPS. The parameters that define the airspace class are: atypical (e.g. segregated) versus typical airspace altitude, controlled by air traffic versus uncontrolled, airport environment versus non-airport, and airspace over urban versus rural environments.

b) Step 5: The Residual ARC is the residual air risk after applying strategic mitigation measures. Two types of strategic mitigations measures exist in the SORA. Air risk mitigations are either operational restrictions (e.g. boundaries, time of operation) controlled by the UA operators or by structure of the airspace and the associated rules controlled by the relevant authorities. Strategic mitigations are applied before flight. Determination of ARC requires full coordination with and agreement by the ANSP for the given operation.

Step 6: Tactical Mitigation Performance Requirement (TMPR) and Robustness Levels Tactical mitigations are applied during the conduct of the operation, and are used to mitigate any residual risk of a mid-air collision that may remain after the strategic mitigations have been applied. Tactical Mitigation Performance Requirements (TMPR) address the functions of Detect, Decide, Command, Execute and Feedback Loop for each Air Risk Class. These mitigations range from simple, for example relying on UTM infrastructure, to more complex TSO (Technical Standard Order) DAA equipment that addresses the risk of non-cooperative air traffic (those without transponders) and cooperative air traffic.

Step 7: SAIL Determination A SAIL (scaled from I to VI) is then determined using the proposed CONOPs, and the consolidation of the final GRC and residual ARC.

Step 8: Identification of Operational Safety Objectives (OSO) For the assigned SAIL, the operator will be required to show compliance with each of the 24 OSOs, although some may be optional for lower SAILs. Each OSO shall be met with a required Level of robustness (High, Medium or Low), depending on the SAIL. OSOs cover the following areas:

a) UAS Technical Issue
b) Deterioration of external systems
c) Human Error
d) Adverse environmental conditions
e) Integrity and Assurance Level Criteria (Low, Medium, High) for each OSO and SAIL level

Step 9: Adjacent Area/Airspace Considerations Compliance with safety requirements associated with technical containment design features required to stay within the operational volume regardless of the SAIL. This addresses the risk posed by an operational loss of control that would possibly infringe on areas adjacent to the operational volume whether they be on the ground or in the air.

Step 10: Comprehensive Safety Portfolio A comprehensive Safety Portfolio is the SORA safety case submitted to the competent authority and the ANSP prior to final authorization. The Safety Portfolio contains the following information:

a) Mitigations used to modify the intrinsic GRC
b) Strategic mitigations for the Initial ARC
c) Tactical mitigations for the Residual ARC
d) Adjacent Area/Airspace Considerations
e) Operational Safety Objectives

If compliance with the required safety objectives is not achieved for the given SAIL, additional mitigation measures may be needed to further reduce the GRC or/and ARC or a change to the operational volume and CONOPs may be required.

In terms of Safety, EASA has identified the following main issues which are summarised below and form the required basis for UAS/RPAS Safety assessment for the IMTM in Rail and Automotive applications within the HELMET Concept of Services:

a) **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.
b) **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 RPAS and the planning and management of the flight path. There is also a relationship to the planning and preparation of UAS/RPAS operations.
c) **UAS Infringement of Controlled Airspace/ UAS/RPAS Proximity to Other Aircraft in Uncontrolled Airspace**. The next Safety Issues in UAS involves the risk of a UAS either infringing controlled airspace or presenting a collision risk to other aircraft in uncontrolled airspace. Work to investigating the potential benefits of Geo-Fencing to prevent UAS flying into controlled airspace is already taking place. This Safety Issue is also linked to the Human Factors (HF) Safety Issues on UAS Operator Knowledge of the Aviation System.
d) **Technical Safety Issues**. Three technical Safety Issues have been identified from the analysis of occurrences and covers the failures of the guidance and control system, propulsion system and power sources.
e) **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.
f) **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 is able to easily learn about the aviation regulatory framework as it applies to UAS/RPAS operations.
g) **Maintenance/ Manufacturing**. This Issue is related to the maintenance and manufacturing of UAS/RPAS and further analysis work is required to consider this issue in more detail as minimal information was available from the analysis.
h) **Visual Loss of UAS/RPAS**. This is a safety issue that is a causal factor linked to other Safety Issues and that shall undergo a formal Risk Assessment. It can include issues such as UAS/RPAS lighting or colour design. This Safety Issue includes the problem of keeping UAS/RPAS in Visual Line Of Sight (VLOS) by suggesting a reduction of the current limitation of their flight path of 150m height (minimum flight limit of manned aircrafts) and 250m radius around the operator to only a 50m height. In case of visual loss and in order to avoid collision whether with moving or non-moving objects, an option could include the need to install a Detection and Avoidance (DAA) system as mandatory equipment for certain categories of UAS.
i) **Frequency Jamming**. It has been highlighted that because small UAS/RPAS usually use 2.4GHz frequency to communicate with the ground station also used by wireless computer networks the probability of interference when an UAS/RPAS is being flown in a heavily dense housing area both in the case of commercial or aerial work operations could lead to jamming of frequencies. Another possible problematic aspect raised is in regards to the operation of several UAS/RPAS in the same area at the same time when the radio allocated spectrum for UAS/RPAS is not wide enough to allow a huge amount of different UAS/RPAS operated by different operators.

j) **UAS/RPAS Task Management**. Many UAS/RPAS operate in a First Person View use mode, where the operator sees the equivalent view from the aircraft as if they were in a cockpit using a video link often using goggles. When performing IMTM work for example the operator must both fly the UAS/RPAS and concentrate on the task they are performing, which could cause a loss of control of the UA/RPA during such critical phase of operation. This is a problem that could be addressed by considering the need for an extra observer for certain tasks.

k) **UAS/RPAS Hard Landings**. Hard landings can cause extensive damages to UAS/RPAS, as well as to both people and property in the surrounding area. Following such events, close inspection of the UAS is needed before future flights to ensure that it is still in a serviceable condition.

l) **Instructions for Use of UAS/RPAS equipment**. It has been identified by UAS/RPAS users that the User Manuals provided by UAS manufacturers are not up the standard they need to be. Hence, proper knowledge on the behaviour of individual systems and how they interact with other systems on board is not clearly laid out causing incidents of unexpected behaviour and in the worst cases loss of control.

2.3.3 High-Level User Requirements for UAS/RPAS-PIT and IMTM Services

The UAS/RPAS-PIT Station (UAS/RPAS main operational support platform) Highly Integrated System Network within the HELMET infrastructure shall be architecturally designed to satisfy Inspection Monitoring and Traffic Management (IMTM) tasks to support both Rail and Automotive operations and assets so as to enhance their Reliability, Maintainability, Availability and Safety, thus contributing to operational Risk Management. The overall IMTM required tasks shall include but not limited to the following:

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.

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:

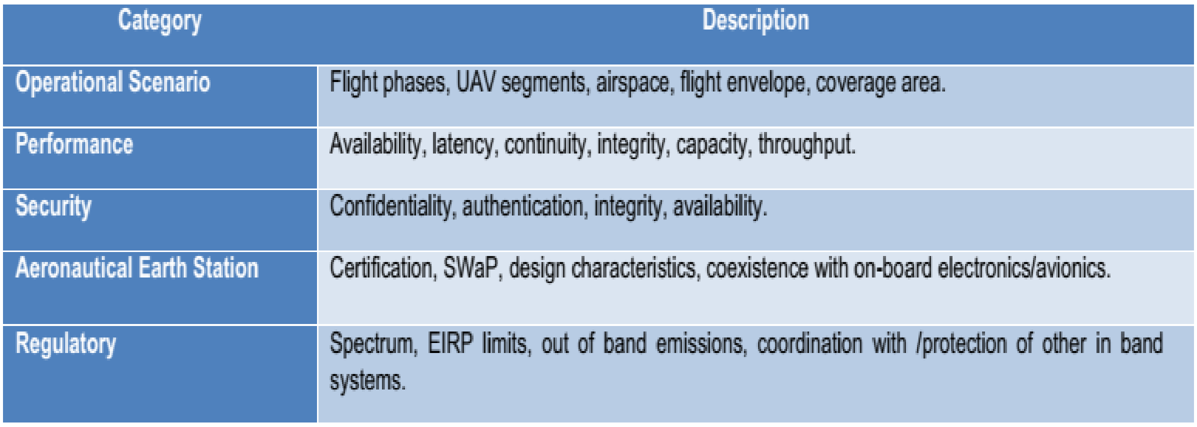
1) Overall Reduction of risk to staff and people and increase of infrastructural assets safety
2) Reduced planning cycles (Scheduled and Non-Scheduled)
3) Enhancement of the work process efficiency in IMTM services
4) Enhancement of flexibility, affordability of verification tooling
5) Higher quality data available in larger quantities at lower costs

As such the UAS/RPAS-PIT Station Highly Integrated System Network Segment within the HELMET infrastructure shall be composed of the following main three (3) Physical Operational Elements, namely:

1) The Operating UAS/RPAS Element 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.

The main areas of user requirements are summarized in Table 8:

Table 8. Main areas of user requirements for UAVs



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.

In accordance with the European UAS/RPAS Steering Group general directives and in operational terms, the overall approach towards integration is that UAS/RPAS shall have to fit into the ATM/UTM system and not that the ATM/UTM system needs to significantly adapt to enable the safe integration of UAS/RPAS. UAS/RPAS at all typologies/categories and classes of operations shall have to prove to be as safe as current manned operations, or safer. UAS/RPAS behaviour in operations will also have to be equivalent to manned aviation, in particular for the air traffic control (ATC) and/or UTM, as it will not be possible for the ATC/UTM to effectively handle many different types of RPAS with different contingency procedures. 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 Regulation 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.

2.3.3.1 High Level UAS/RPAS User Operational Requirements

In summary the High Level UAS/RPAS Operational Requirements shall have as follows:

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 UA/RPA loses communications or loses its GNSS NAV signal, it must return to a predetermined location within the planned operating area.

In terms of operational modes and overall limitations, the UAS/RPAS dedicated to the IMTM missions shall satisfy the following rules:

1) Very low level (VLL) operations (alias non-standard VFR or IFR operations) below the typical IFR and VFR altitudes for manned aviation: i.e. not to exceed 400 ft. above ground level; they shall comprise:

   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;
   c) Beyond VLOS (BVLOS) where the operations are also below 400 ft., but beyond visual line of sight requiring additional technological support.

2) UAS/RPAS operations in VFR or IFR, above 400 ft. and above minimum flight altitudes; they shall comprise:

   a) IFR (or VFR) operations in radio line-of-sight (RLOS) of the RPS in non-segregated airspace where manned aviation is present. The key capability of 'detect and avoid' (DAA) is required in relation to cooperative and non-cooperative nearby traffic (otherwise specific procedures and restrictions would apply);
   b) IFR (or VFR) operations beyond radio line-of-sight (BRLOS) operations, when the RPA can no longer be in direct radio contact with the RPS and therefore wider range communication (COM) services (including via satellite) are necessary. In this case COM would typically be offered by a COM service provider.

NOTE: The altitudes that are identified for the above mentioned operations are of a generic nature not taking into consideration National differences and exemptions.

The integration of IMTM UAV/RPAS for HELMET shall be appropriately equipped to operate in the following phases of flight:

1) Mission/Flight Planning Phase;
2) Take off & climb Phase;
3) En-route and Aerial Work Phase (includes loitering over the mission area executing planned or unplanned aerial work);
4) Arrival phase (Landing) and Post-Flight Phase;

For small UAS/RPAS, operations in RLOS, E-VLOS and BVLOS it will be necessary the system to have some type of Detect and Avoid capability, and among other safety required technologies the possibility for Redundant CNPC Link (which includes NAVAIDS).

2.3.3.2 Overall IMTM UAS/RPAS Physical, Functional and Operational Performance High Level User Requirements

The average overall Physical, Functional and Operational Performance requirements for each small IMTM-UA/RPA type configuration to be considered and traded-off for the HELMET project work are summarized in the Table 9 below:

Table 9. IMTM UAS/RPAS Physical, Functional and Operational Performance Requirements

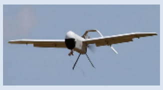
SMALL UAV TYPE	MTGW Range (Kg)	Speed Range (Km/h)	Max. Banking & Max. Vertical Rate	Normal OPS Altitude Range (m)	Max. Flight Endurance (min)	Operating Temp (C°)	Mission Radius Range (Km)
Multi-Rotor	≤ 1 TO ≤ 25	30-80	6 °/s ±3 m/s to ±10 m/s	≤ 3 to ≤ 400	45	-20 to 55 °C (Electrical Power) -40 to 55 °C (Non-Electric)	1.6 TO ≤ 100
Fixed-Wing 	1 TO ≤ 25	40-120	4 - 6 °/s Climb/Descent Rate 15m/s	≤ 20 to ≤ 400	45 -120	-20 to 55 °C (Electrical Power) -40 to 55 °C (Non-Electric)	50 TO ≤ 200
Single-Rotor	1 TO ≤ 25	20-60	6 °/s ±3 m/s to ±10 m/s	≤ 3 to ≤ 400	30 - 60	-20 to 55 °C (Electrical Power) -40 to 55 °C (Non-Electric)	1.6 TO ≤ 100
Fixed-Wing Hybrid	≤ 3 TO ≤ 25	30-100	4 - 6 °/s ±3 m/s to ±10 m/s	≤ 10 to ≤ 400	45 -120	-20 to 55 °C (Electrical Power) -40 to 55 °C (Non-Electric)	50 TO ≤ 200

Table 10 Provides a traded-off summary of the Physical, Functional and Operational Performance and Capabilities of the various UAS/RPAS Configurations as candidates for potential for use as IMTM in HELMET Project. Further and more detailed trade-off results shall be found in the IMTM UAS/RPAS-PIT Detailed Specifications of the HELMET Project.

Table 10. IMTM UAS/RPAS Physical, Functional and Operational Performance Comparison

TYPE	ADVANTAGES	DISADVANTAGES	TYPICAL USES
Multi-Rotor	• Accessibility • Ease of use • VTOL and hover flight • Good camera control • Can operate in a confined area • Low Cost	• Short flight times • Small payload capacity	Aerial Photography and Video Aerial Inspection, Urban Delivery Services
	• Long endurance • Large area coverage • Fast flight speed	• Launch and recovery needs a lot of space • No VTOL/hover • Harder to fly, more training needed • Expensive	Aerial Mapping, Pipeline, Road, Rail and Power line inspection
Single-Rotor	• VTOL and hover flight • Long endurance • Heavier payload capability	• More dangerous • Harder to fly, more training needed • Expensive	Aerial LIDAR laser scanning
	• VTOL and long-endurance flight	• Not perfect at either hovering or forward flight • Still in development	Urban/Extra-Urban Delivery Services

In terms of UAS/RPAS Data Link Required Categories and Performances the IMTM UAS/RPAS-PIT Figure 9 below provides a general schematic of the UAS/RPAS Data Links Classification. At the first level of UAS/RPAS Data Link decomposition there are two main logical elements of such link, namely:

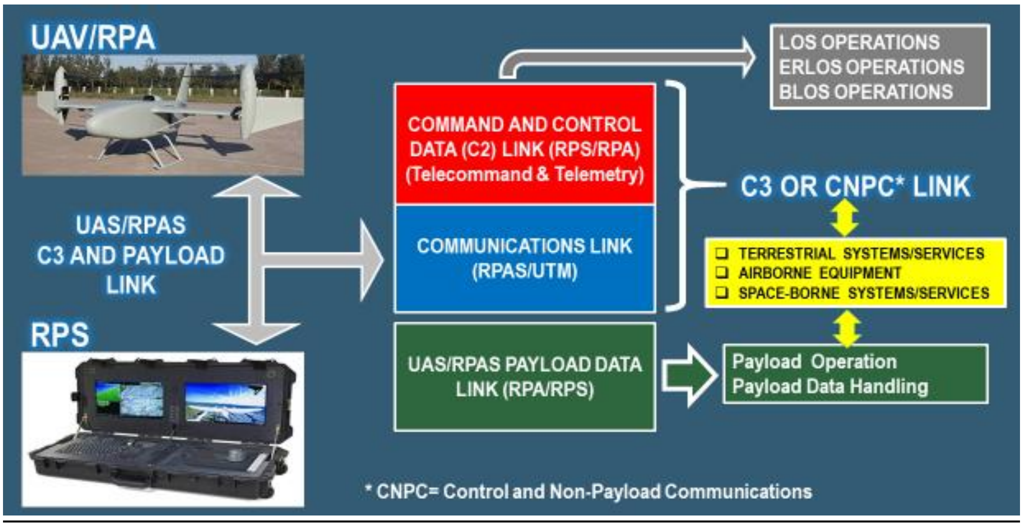

UAV/RPA
UAS/RPAS C3 AND PAYLOAD LINK
RPS
COMMAND AND CONTROL DATA (C2) LINK (RPS/RPA) (Telecommand & Telemetry)
COMMUNICATIONS LINK (RPAS/UTM)
UAS/RPAS PAYLOAD DATA LINK (RPA/RPS)
LOS OPERATIONS
ERLOS OPERATIONS
BLOS OPERATIONS
C3 OR CNPC* LINK
❑ TERRESTRIAL SYSTEMS/SERVICES
❑ AIRBORNE EQUIPMENT
❑ SPACE-BORNE SYSTEMS/SERVICES
Payload Operation
Payload Data Handling
* CNPC= Control and Non-Payload Communications

Figure 9. Typical UAS/RPAS Data Links Classification and Functional Description Schematic

a) Control and Non-Payload Communications (CNPC) Link: This link is the carrier of all logical data flows associated with the command and control of the UA/RPA flight and the health and usage monitoring of all UA/RPA systems, subsystems and components and the management of the CNPC link. Since the communications are part of controlling the RPA, they are also included within this system. This link is not dedicated to the mission payload(s) data and therefore doesn't carry any payload information. The CPNC Link compared to the payload links, carries signals that are expected to be relatively narrowband, with the possible exception of the situation awareness function enhancing video streams. The CNPC link shall require to reside in a protected spectrum and managed by the Civil Aviation Regulatory Authority (e.g. EASA); and

b) Payload Link: This link is the carrier of all logical data flows which associated with the mission payload package. It is generally expected to be broadband compared to the CNPC signals. Since this link doesn't contain safety-of-flight information, it doesn't require to be in aviation safety protected spectrum.

c) The CNPC link is decomposed into two (2) logical elements, namely:

   1) RP/UTM/ATC Communications Link: carrying:

   a) Voice or messaging communications between pilots and UTM/ other Airspace users

   b) Data communications (e.g. CPDLC)

   2) UAS/RPAS Control Link: this link carries safety-related information between the pilot in a GCS/RPS and the UA/RPA. The control link is further decomposed into two logical elements, namely:

   2.1) Tele-command Link: which carries from the RP to the UA/RPA:

      a) Information required to control the RPA flight trajectory

      b) Information required to control all RPA systems for safe flight

   2.2) Telemetry Link: This is a downlink that carries, from the UA/RPA to the RP, information required for the safe flight of the UA/RPA and as such shall include the following:

      a) RPA Location, attitude and speed

      b) RPA subsystems operating modes and status

      c) Data from onboard NAVAIDS (Navigational Aids) and GNSS

d) Target tracking data required by the Detect and Avoid (DAA) subsystem of the RPA
e) Data from an onboard the RPA Airborne Weather Radar (AWR) (if present on the RPA)
f) Video stream from the onboard situational-awareness-enhancing video camera (if present and if the CNPC link is being used for that purpose).

The Required Link Performance (RLP) as an indicator summarizes the class of performance of a Command and Control (C3) link for the UAS/RPAS. In defining the detailed RLP requirements they shall be considered four (4) performance indicators, namely:

1) Transaction Time: which is the minimum proportion of operational communication transactions to be completed within the specified RLP transaction time, given that the service was available at the start of the transaction.
2) Availability: The required probability that an operational communication transaction can be initiated when needed (C3 Link Available). Typical required Availability of RPAS C3Links in VLOS and BVLOS modes of operation is 0.998.
3) Continuity: the minimum proportion of operational communication transactions to be completed within the specified RLP transaction time, given that the service was available at the start of the transaction.
4) Integrity: the required probability that an operational communication transaction is completed with no undetected errors.

The JARUS methodology proposes to calculate target values for transaction time, availability, continuity and integrity by conducting a safety risk assessment based on UAS/RPAS C3/UTM functions and characteristics of the selected operational environment, as summarized by the diagram in Fig. 10:

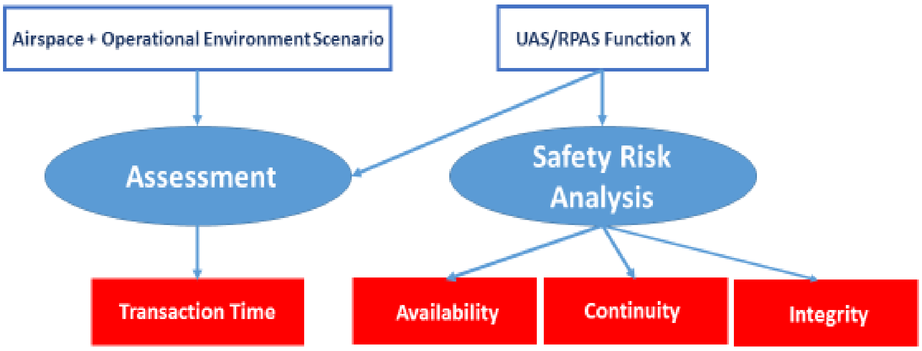


Figure 10. Safety risk assessment based on UAS/RPAS C3/UTM functions

Transaction Time target is to be estimated by taking into account the safety impact on the operational scenario context, for example the expected latency in ATC/UTM instruction compliance. In the case of ATC/UTM communications are relayed through the C3 data link, then the RLP must be less than the RCP requirement prescribed for the same airspace class. Target values for availability, continuity and integrity shall be calculated as a result of an operational hazard assessment, which will take into account different types of communication errors, depending on the parameter. Detected errors and communications exceeding the transaction time slot contribute to the continuity parameter; Detected inability to start a communication is accounted for in the availability parameter. Undetected errors and undetected loss of communication service contribute to the integrity parameter. As result of the hazard assessment, safety requirements shall be generated to mitigate potential emerging risks. Severity assessment and identification of the most stringent among safety objectives associated with the severity shall provide the final target parameters. The Latency calculation shall be performed on the worst case basis i.e. altitude abrupt change or banking etc. the total latency value will be the sum of all the contributions from the latency budget. The performance objectives associated with operational communication transaction for an altitude change request from the remote pilot are shown as an example in the Table 11 below. This table only considers performance objectives for major hazards.

Table 11. Performance Comparison performance objectives associated with operational communication

PARAMETER DESCRIPTION	VALUE
Unexpected interruption of a transaction	10^{-4} per aircraft per flight hour
Loss of communication transaction	10^{-5} per aircraft per flight hour
Loss of service	10^{-6} per aircraft per flight hour
Undetected corrupted transaction	10^{-5} per aircraft per flight hour

In terms of Payload requirements for IMTM UAS/RPAS Operations in Rail and Automotive applications there is a variety of Optical Sensors (Cameras) which are the most common sensor used on a UAV/RPAS. However, dynamic sensor technologies created for use with UAVs provide essential situational awareness and a level of detail often missed by the human eye and standard cameras. Light Detection and Ranging (LiDAR) sensors on UAVs, such as that shown in Figure 11 below, capture high quality imagery. A LiDAR sensor mounted on a UAV, along with sophisticated software, can produce accurate three-dimensional images very quickly. UAV payloads can integrate sensors of a different nature, such as temperature sensors or multispectral cameras to provide diverse functionalities, depending on energy consumption and maximum allowed weight. Self-powered chemical sensors can be mounted on the aerial platform to provide quick and safe analyses of chemical or air samples e.g. near a derailment.

Current standard UAS technology allows the registration and tracking of position with Global Positioning Systems (GPS), or Inertial Navigation Systems (INS), and orientation of the implemented sensors in a local or global coordinate system. UAS-based photogrammetry, or the practice of making measurements from imagery, now allows for the collection of information from platforms that are remotely controlled or operated in a semi-autonomous or autonomous manner, therefore, eliminating the need for a pilot sitting in the vehicle.

The collection of three-dimensional data by conventional surveying methods can be quite time consuming, expensive and even dangerous for the field operator, especially on steep slopes and cuts where there are potential rock falls, landslides or mudslides. Visual inspection of the terrain in such locations, just as geodetic data collection with classical methods, can result in incomplete and insufficiently detailed data, thus posing a risk to the railroad and/or road. The use of UAVs in such locations can greatly complement, enhance and even completely replace the classical methods of mapping, determining the volume, cross-sections, contours and other parameters that are necessary for the remediation measures as illustrated in Figure 11 below.

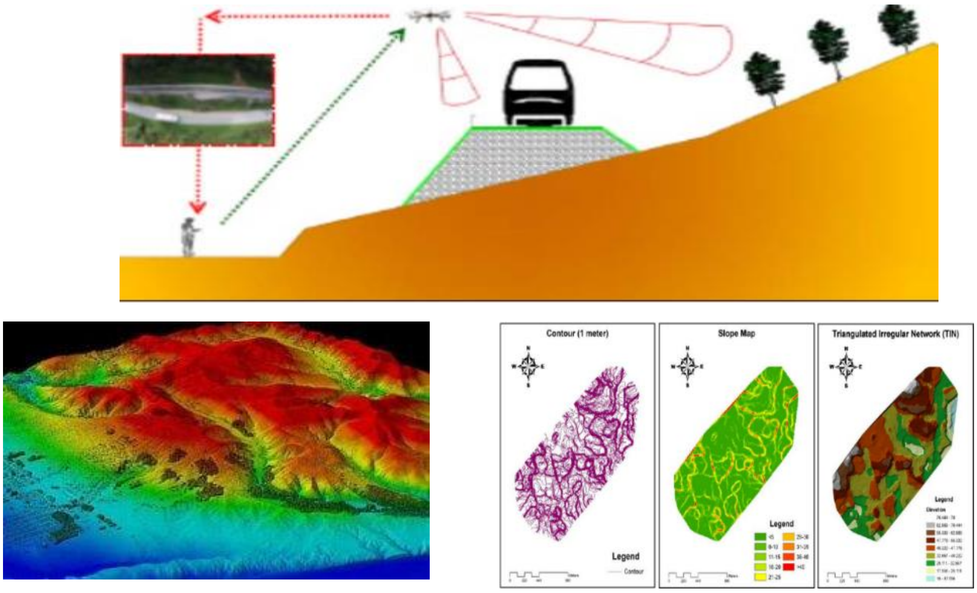


Figure 11. Examples of UAV Mapping Steep Slopes and Contours

The challenge will be to increase the level of automation to reduce the need for human interventions with the ongoing enhancement of UAS/RPAS endurance and payloads, even in critical situations. The number of scenarios in which railway/road/highway UAS/RPASs would be useful will be proportional to UAS/RPAS performance growth. The UAS/RPAS-PIT Detailed Specification shall provide Technical Physical, Functional and Operational (including performances) characteristics of traded-off and selected payloads which shall fully satisfy IMTM operations for rail and automotive applications (see Fig. 12).

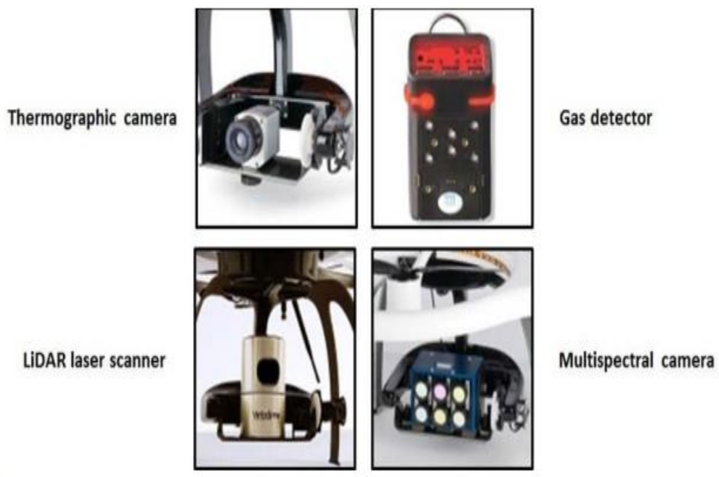


Figure 12. Examples of some Payload Types Required for IMTM UAS/RPAS Operations in Rail/Automotive

Table 12 summarizes the maximum UAS/RPAS forward and return CNPC link performance requirements for LOS and BLOS operations as established by a number of studies by RTCA, JARUS, ICAO and ITU:

Table 12. High-Level User UAS/RPAS CNPC Forward and Return Link Performance Requirements (EUROCAE)

Required Parameter	Forward Link Requirement	Return Link Requirement	Remarks
Availability (Probability/Flight Hour)	0.999997	0.999997	RCP 10 Separation: 5nm, Transaction Time: 10sec
	0.99985	0.99985	RCP 10 Separation: 5nm, Transaction Time: 10sec
Integrity (BER/PER) (Acceptable Rate/Flight Hour)	$1.43\ x10^{-6}$	$1.43\ x10^{-6}$	RCP 10 Separation: 5nm, Transaction Time: 10sec
	1) 130ms 2) 520ms 3) 5.2 s 4) 20.8s	1) 130ms 2) 520ms 3) 5.2 s 4) 20.8s	1) Real-time safety critical information (C2 manual, voice, DAA, Video) (only Ground link) 2) Near real-time safety critical information (C2 automatic, ATC-D data, ATC-V voice, Video) 3) Low priority safety information 4) Non-safety critical information
Jitter	50µ	50µ	Packet to packet

2.3.3.3 User Spectrum CNPC High Level Requirements for Small IMTM-UA/RPA to be Supported for HELMET Operations

The UAS/RPAS-PIT detailed specification shall provide the density number of evenly distributed and operating IMTM-UAS/RPAS in % per flight phase serving a pilot area of HELMET Operational coverage in LOS and/or BLOS Modes. This shall provide an estimation of the potential traffic levels of all types of small IMTM-UA/RPA employed for HELMET Applications so as to give the density levels in line with ITU-R M.2171 Methodology 2 obtaining the terrestrial (LOS) and satellite (BLOS) aggregate bandwidth requirements for CNPC. In terms of aggregate bandwidth requirements shall be identical to those of ITU-R M.2171 Methodology 2 since the system is similar to the one studied in the ITU Report (BLOS Spot–Beam and LOS Terrestrial System).However, for the purposes of this project in terms of required number of small IMTM-UA/RPA to be supported, Non-payload throughput requirements for single small UA/RPA (bit/s), spectrum requirements, aggregate bandwidth requirements for LOS and BLOS will be also in accordance with the ITU-R M.2171 Method 2 approach since small UAS/RPAS can be supported only by Spot Beam Systems. In accordance with the ITU-R M.2171 Methodology 2 for assessing the spectrum needs, the following Table 13 summarizes the bandwidth requirements calculated for each of the three major functional communications categories (Command and Control, ATC Relay and Sense and Avoid or DAA data) in each of the three alternative system implementations (LOS, BLOS satellite spot beam, and BLOS satellite regional-beam).

Table 13. Spectrum Requirements Summary-Methodology 2 (Source ITU -R M.2171)

Functional category	Aggregate Bandwidth Requirement (MHz)		
	LOS Terrestrial System	BLOS Satellite System	
		Spot-Beam	Regional-Beam[1]
Command and Control	1.61	9.01	6.54
ATC Relay	2.72	6.50	11.47
Sense and Avoid or DAA	23.51	21.81	38.29
Total	**27.84**	**37.32**	**56.31**
[1] *Regional-beam system does not support small UA/RPA.*			

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.

2.3.3.4 High-Level User EGNSS Performance Requirements for UAS/RPAS IMTM Operations

2.3.3.4.1 General

As it was mentioned in previous sections, the aerospace applications need very stringent integrity requirement in particular for mission and safety critical missions. These are even more for UAS/RPAS applications that are remotely piloted today in LOS and in future in BLOS 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 UAS/RPAS operations and support the future UTM (UAV Traffic management).In Figure 13 the overall picture are reported the main UAS/RPAS functions required for their safe operation.

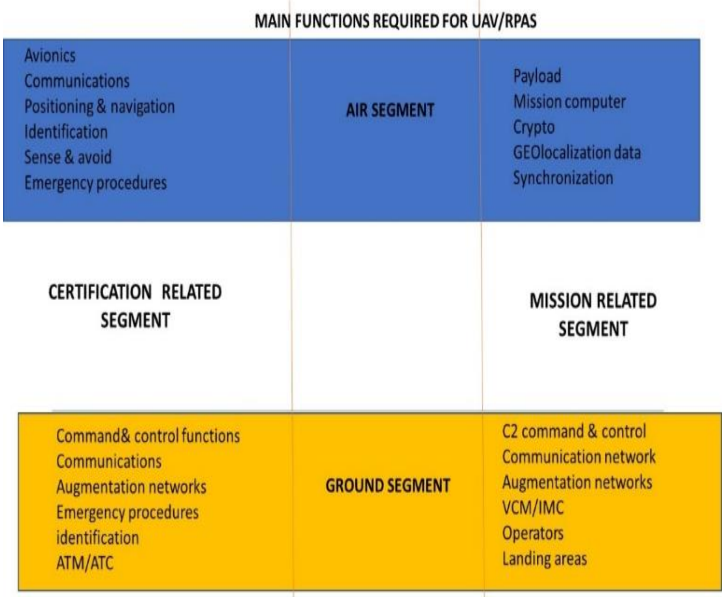


Figure 13. UAS/RPAS Main Functions

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 STK. 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 RPAS navigation and positioning requirement.

2.3.3.4.2 Overview of Major of EGNSS Degradation and RPAS Integrity

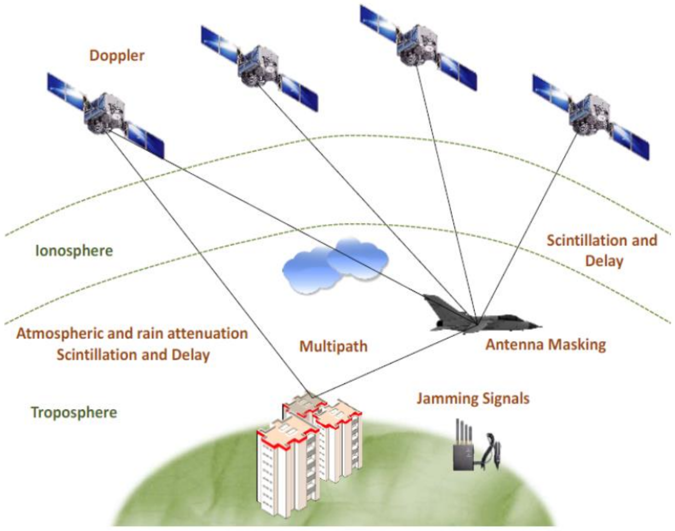


Figure 14. Major Causes of EGNSS Degradation

The Major causes EGNSS (see Fig. 14) of errors outages and severe performance degradations are:

a) Obscuration of satellite signals during manoeuvring (Antenna obscuration)
b) Bad satellite geometries (DOP)
c) Fading so low C/N0
d) Doppler shift
e) Multipath
f) Interference or jamming

Note that the same causes may affect also the communications by which should be possible augment integrity and accuracy.

The overall functional block diagram of RPAS operation integrity is outlined in Fig. 15.

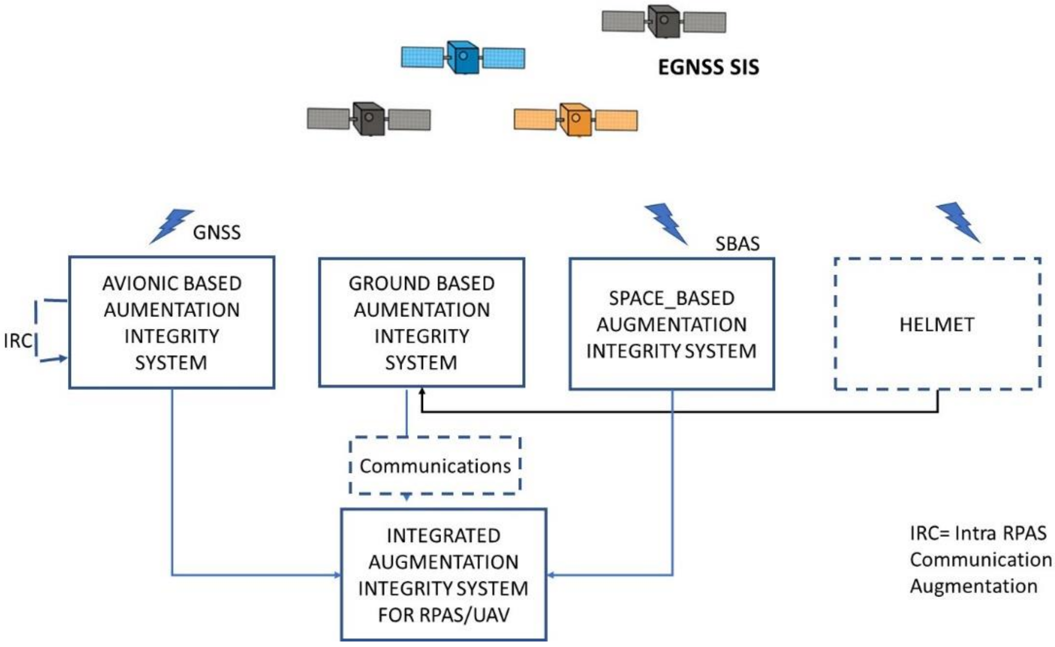

EGNSS SIS
GNSS
SBAS
IRC
AVIONIC BASED AUMENTATION INTEGRITY SYSTEM
GROUND BASED AUMENTATION INTEGRITY SYSTEM
SPACE_BASED AUGMENTATION INTEGRITY SYSTEM
HELMET
Communications
INTEGRATED AUGMENTATION INTEGRITY SYSTEM FOR RPAS/UAV
IRC= Intra RPAS Communication Augmentation

Figure 15. RPAS Operational Integrity

2.3.3.4.4 Overview of the Context of Improved Integrity User Requirements for UAS/RPAS

Figure 16 shows schematically the overall contest of improved integrity for RPAS/UAV and in general aeronautic.

a) On Board Augmentation This is provided by avionics and specific applications such ARAIM. Integrated avionics allow to estimate integrity from the diverse source and also provide internal FDIR capability. Decision can be taken on board or remote pilot depending on the on board autonomy.
b) Space Based Augmentation. This is provided by SBAS system, such as EGNOS in Europe. However, EGNOS presents same limits in terms of local integrity and accuracy that can be improved only by dedicated ground augmentation systems.
c) Ground Based Augmentation. This provides differential corrections and integrity. This is a key issue for UAS/RPAS operators in particular for landing and take-off in absence of other mechanism. Of interest are the situation where a landing area is used form more UAS/RPAS and then as for small airport it is necessary to adopt specific procedures with priority rights.

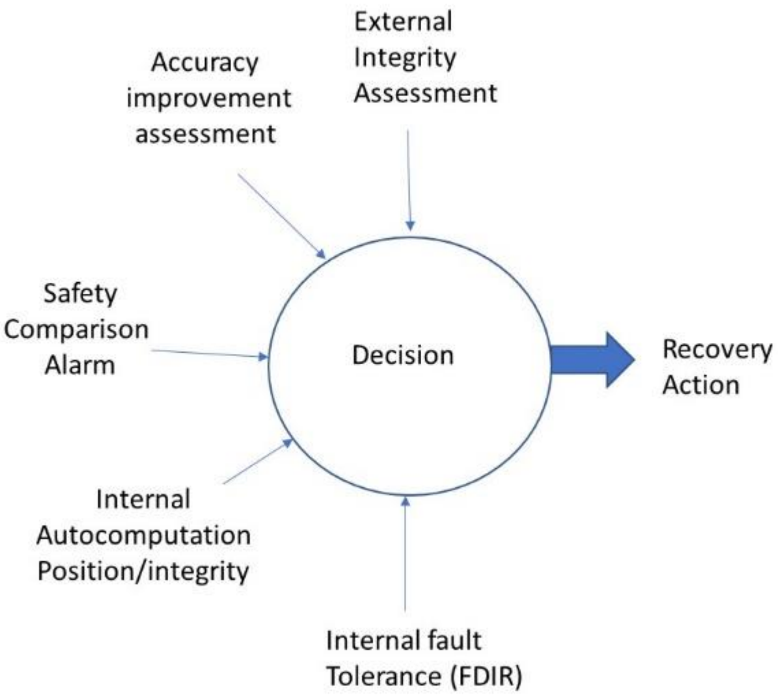

External Integrity Assessment
Accuracy improvement assessment
Safety Comparison Alarm
Decision
Recovery Action
Internal Autocomputation Position/integrity
Internal fault Tolerance (FDIR)

Figure 16. Integrity Computation Process on Board

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 where a recovery action can be adopted. Moreover from Figure 16 (RPAS Operational Integrity) it can be recognized the key importance of communications for bringing the augmentation ground data to/from the UAS/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).

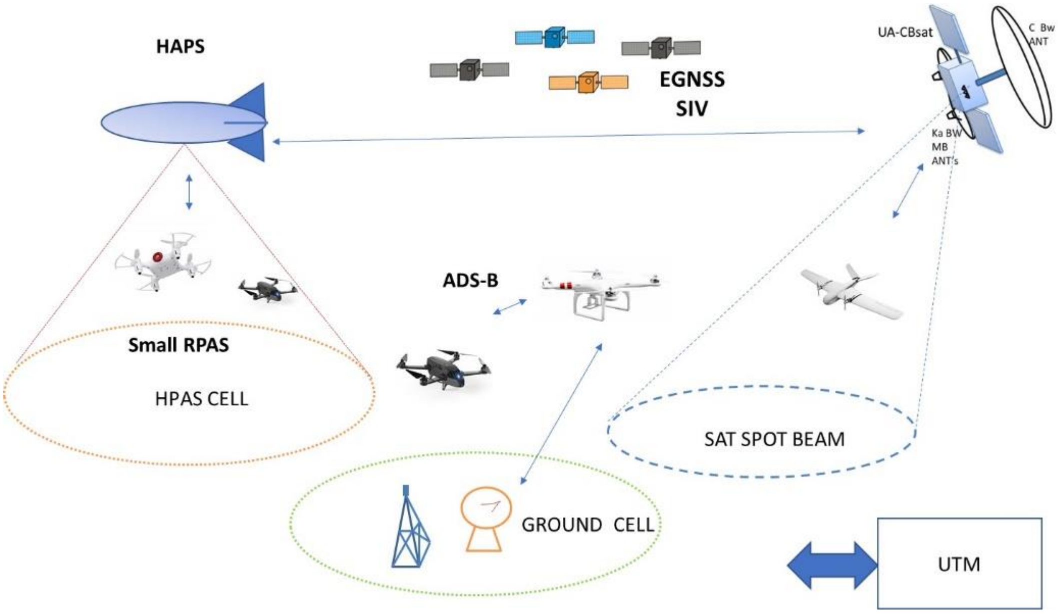


Figure 17. Schematic View of the Overall Future Communication Scenario for UAS/RPAS

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.

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.

From Figure 17 (Schematic View of the Overall Future Communication Scenario for UAS/RPAS) it is possible to distinguish four potential sources of communications:

a) 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.
b) HAPS Communications: HAPS are under developing and can provide not only communication pilot-RPAS but also additional navigation and positioning services.
c) 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.
d) 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 UAS/RPAS operation completely different form the other applications for the time being where there is 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 UA/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 ballistic parachute is launched).
The HELMET architecture should provide a contribution to merge those different sources of integrity for improving mission and safety critical operations and systems. In order to improve safety the following functions should be introduced:

a) Prediction (Caution Flags): Prediction is mainly based on Space augmentation but more in particular on ground augmentation system that only can provide status of integrate navigation and communication wealth of the particular area where it is placed. This allows a better plan of the RPAS mission and the overall UTM traffic management.
b) Avoidance Optimal Flights Path Guidance: The availability of good integrity data allows to optimize flight path and also to define potential dangerous situation anticipating correction manoeuvring or flight reprograms.
c) Reactions (Warnings Flags): When a warning is detected then the action should be performed. It is important to minimize the false warnings.
d) Corrections (Recovery Path Guidance): Correction are needed in case of emergency situations. In this case it is important to get awareness of situation around UAS/RPAS for optimizing escape or avoidance manoeuvres.

It is important to emphasize here the difference of actions in case of emergency with 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:

a) The UAS/RPAS autonomously (or assisted by local augmentation system or operator) land in a pre-defined area pre-planned before mission start
b) The UAS/RPAS remain in flight possibly loitering over a pre-planned area

For UAS/RPAS operations within the objectives of HELMET ie Railways and Highways operations the achievement of flight and safety requirement can be simplified by the adoption of specific ground aid infrastructure as already proposed in the proposal. This consist in the PIT station concept.

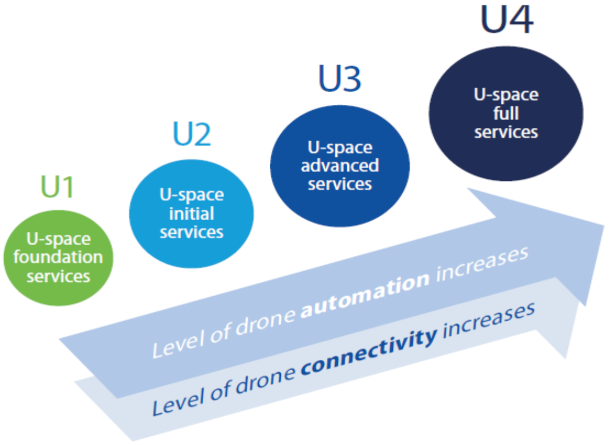

U1
U-space foundation services
U2
U-space initial services
U3
U-space advanced services
U4
U-space full services
Level of drone automation increases
Level of drone connectivity increases

Figure 18. SESAR Evolution Steps

Of course a new initiative should take into considerations the program under development in Europe such for instance SESAR (Refer to Fig. 18 “SESAR Evolution Steps”) that foreseen a full service environment for UAS/RPAS by 2035. With reference of EC GSA White paper it can be defined as follows:

a) Geo-Fencing: This is a virtual barrier definition for RPAS/UAV operations

b) Waypoint Navigation: This defines the trajectory to be followed by the UA/RPA
c) Geo-Tagging: The process of adding to the on board avionic navigation system other geographical information for camera or other sensors.

Other identified capabilities are:

a) Drone telemetry/tracking position reported to pilot
b) Detect & avoid by additional sensors or ADS-B or UTM data
c) Drone Identification: only identified aircraft will be authorized to fly in the future aerospace
d) Recovery actions:
   1) Return to home
   2) Altitude hold
   3) Loiter on an area

GNSS can contribute to the above service providing an accuracy function of the typology of signal processing and augmentation (see Table 14):

Table 14. GNSS accuracy of different techniques

Processing	Accuracy	Comment
Standalone GNSS	Better than 5 m	
SBAS	< 1 m 3D	Better integrity and reliability of positioning Accurate time signal
PPP	0,1-1 m horizontal accuracy	To be delivered by L band satellite or ground station. High convergence time
RTK	1-5 cm	Differential method short range. Need reference station
ABAS (Air Borne Augmentation System)		Avionic solution that process GNSS data with other on board sensors to check integrity. RAIM or ARAIM algorithms normally used. Additional integrity parameters are generated at ground level and encapsulated into ISM (integrity Support Messages)

In order to get high order of accuracy and integrity it essential to implement a multi-sensor avionics fusing data (magnetometer, barometer, IMU, etc). Another important requirement to satisfy 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 UA/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:

a) Open service message authentication
b) Commercial authentication services (based on E6)

Important is also the possibility to authenticate the UAS/RPAS position and timing for different purposes such assurance but also for police and law enforcement assessment.
In accordance with the above it is believed that a suitable augmentation infrastructure can be conceived to support the Helmet applications, that are:

a) Railway:
   In this case the RPAS application has several advantages:
   1) The area above the railways can be segregated and are easy to virtual fenced
   2) The rails itself may constitute a reference item to refer RPAS localization

3) The presence of staggered small stations allows good location for RPAS augmentation /recovery/ maintenance/operation
4) Stations may become area of emergency landing

b) Highway/Roads:
   1) Here segregation space is likely not achievable however the large paths are still a good reference for navigation.
   2) The lack of station should be compensated additional dedicated infrastructure.

In conclusion, the augmentation of GNSS shall benefit the entire aviation domain and thus the UAS/RPAS together with its peculiarities, in many respects by:

a) Increasing the access to the landing areas
b) Allowing direct en-route flight paths
c) Improving and innovating approach services
d) Reducing or simplifying on board equipment

While with the HELMET multi-modal Augmentation and Integrity Monitoring Network (AIMN) can be achieved the following:

a) Improve PVT integrity
b) Provide accuracy services
c) Improve safety and security of flights
d) Aid emergency operations
e) Improve mission plan and control
f) Allow BLOS operations

2.3.3.4.3 Overview of IMTM UAS/RPAS-PIT Architectural Requirements

In terms of IMTM UAS/RPAS-PIT Infrastructure Architectural needs, that intend to satisfy the expected services toward the HELMET rail and automotive segments while they meet the overall unmanned aviation operational safety requirements, are expected to:

a) improve small UAS/RPAS capabilities, resilience and integrity and permit their operations in both LOS and BLOS supported by space communications.
b) consist of a network of PIT stations that shall include UAS/RPAS landing area, a communication package and a GNSS integrity monitoring and improvement system.

In this PIT station the UA/RPA 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 EGNSS loss more effective and keep the on-board unit always calibrated so that the UAS/RPAS can reach the area where PIT stations provide autonomous landing service.

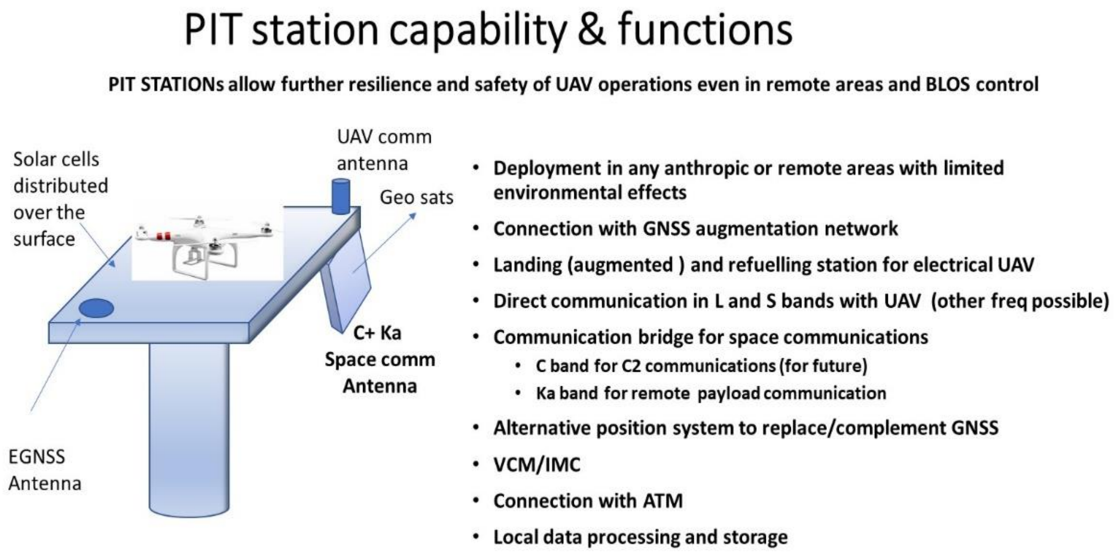
For instance it is possible to anticipate to the situation of a complete loss of GPS signal using the integrity information included in EGNOS messages or compute this information on ground and transmit it to the UAS/RPAS and pilot and take some countermeasures. EGNOS-capable receivers can use the integrity 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, they might be different situations:

a) GNSS data is 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.

b) Same situation as above with additional data form ground (differential, PPP or RTK) to get needed accuracy for the specific application.
c) 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.
d) 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
e) GNSS receiver is not able to calculate a position solution. As above.

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 functionality can try to reach the planned area of landing where operation are in loco assisted. The PIT station functions are (Fig. 19):

1) Deployment in any anthropic or remote areas with limited environmental effects
2) Landing (augmented and automated) site and refuelling station for electrical UA/RPAS
3) Direct communication in L and S bands with UA/RPAS (other frequencies are possible)
4) Communication bridge for space and ground C2/3 communications
5) C band for C2 communications (future)
6) Ka band for remote payload communication
7) GNSS local integrity station (including inference monitoring and position accuracy augmentation) with communication messages in contact with HELMET augmentation station
8) Local data processing and storage
9) Support for ATM
10) Provide geo-referenced site for optical navigation augmentation sensor.
11)



PIT station capability & functions

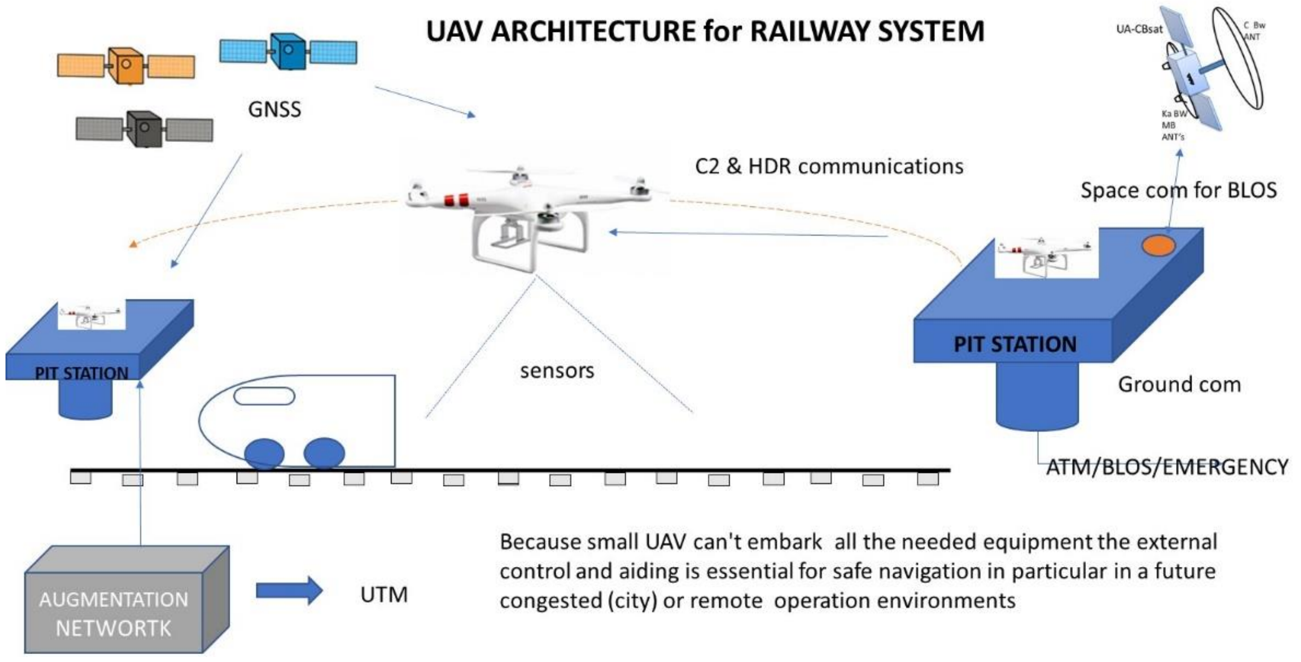
PIT STATIONs allow further resilience and safety of UAV operations even in remote areas and BLOS control

- **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 19. PIT Station Functions

The overall benefits of the PIT Station concept are as follows:

a) Improved UAV resilience by local fast refuelling
b) Improved range autonomy by multiple refuelling
c) BLOS operations even for small UAV
d) Higher data rate remote communications
e) Multiple UAV operations
f) Higher position accuracy and integrity for navigation


UAV ARCHITECTURE for RAILWAY SYSTEM

Because small UAV can't embark all the needed equipment the external control and aiding is essential for safe navigation in particular in a future congested (city) or remote operation environments

Figure 20. PIT stations Architecture Schematic for Railways Applications

Depending on the application the PIT station shall become the local augmentation station for UAS/RPAS operations in particular for supporting BLOS operations of small UAS/RPAS. Based on PIT station will be possible for a UAS/RPAS to operate for a long path same time refuelling or executing specific tasks such transport of emergency goods – see Fig. 20.

In addition, along the path the UAS/RPAS can collect telemetry data that can be damped in a PIT station and then transmitted to the control centre. This procedure may result more economic and effective than to transmit data on a ground collector unit or directly via satellite.

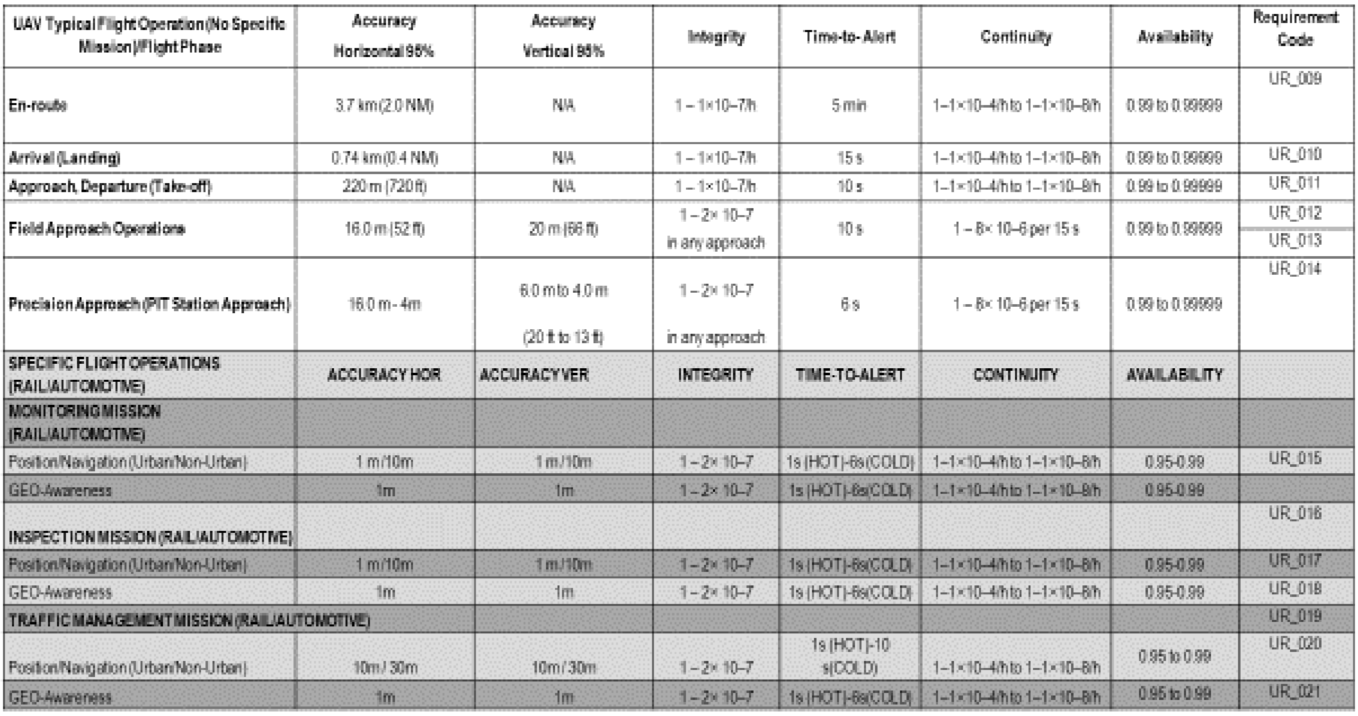
In case of rail than it is possible to complement navigation data simply painting the railways sleepers with a code indicating positioning (kilometres) . In case of Highway specific ground items can be geo-localized in order to be detected by the on board optical sensors.

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.

2.3.3.5 Summary of High-Level User GNSS Requirements for UAS/RPAS-PIT Operations

The following Table 15 summarizes the GNSS Performance Required by UAS/RPAS-PIT Operations. The top part of the Table contains the performance requirements of an UA/RPA in a Mission-less Mode Operating in a typical Flight Envelop and Trajectory while the bottom second part of the Table provides the specific UA/RPA mission in the rail and/or automotive environment and specifically during En-Route/Aerial Work Flight Phase.

Table 15. Summary of High-Level User GNSS Requirements for UAS/RPAS Operations



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)-10 s(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

2.4 HIGH-LEVEL USER CYBER SECURITY REQUIREMENTS FOR HELMET

The intention of the HELMET project is not only to provide high-accurate and high-integrity solution, but also secured solution as it is defined by the 1st Objective of HELMET.

Cyber security is a process preserving availability, integrity and confidentiality of information and RAMS (Reliability, Availability, Maintainability and Safety) of safety-related systems. The HELMET project is mainly focused on development of a secured high-precision and safety-integrity position determination solution intended for the multi-modal transportation (RAIL, AUTO, UAVs). Communication network is out of the HELMET scope. Therefore, IT-security protecting communications against security threats will not be solved in this project. Instead cyber security provisions will be considered from the functional safety point of view – to preserve RAMS of HELMET solutions, as it is depicted in Fig. 21.

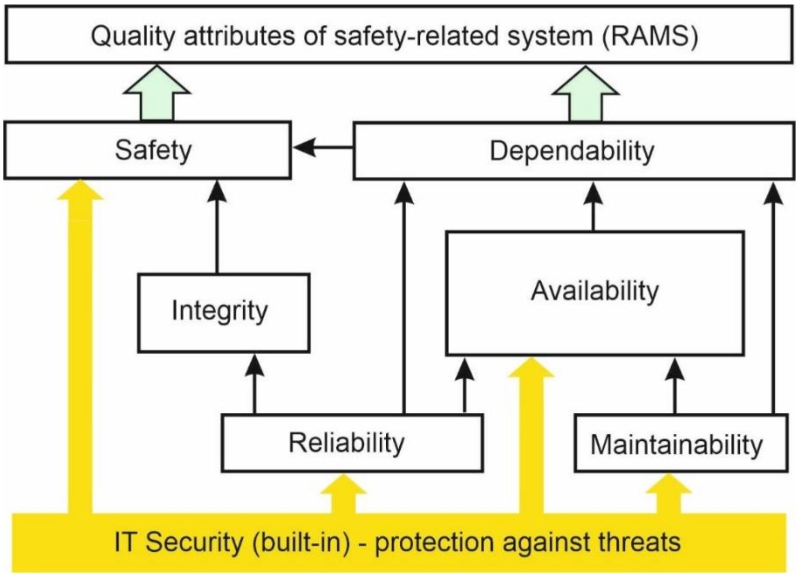

Quality attributes of safety-related system (RAMS)
Safety
Dependability
Integrity
Availability
Reliability
Maintainability
IT Security (built-in) - protection against threats

Figure 21. Scope of cyber security from the functional safety point of view applied in HELMET

Proposed cyber security solutions in HELMET:

The following five principles of cyber security control design will be applied in the HELMET functional safety concept [15]:

- ‘If it is not secure, it is not safe’: States of safety shall be derived from security considerations.
- Proportionate Response: Measures shall be appropriate to the risk being considered but not hinder rail operations.
- Goal-based Security: Establishing goals rather than initiatives ensures more pervasive security and organisation adoption. ¨
- Designed-in Security: Security should be at every level of design and development and never seen as a “bolt on”.
- Defence-in-Depth: For each threat there should be multiple independent overlapping controls.

Security considerations will be integral to the HELMET solution design and development.

While in railway automation harmonized functional safety standards (EN 5012x based on IEC 61508) were elaborated about 2 decades ago, up to now no harmonized international IT security requirements for railway automation exist. Nevertheless, EN 50129 (2018) deals with physical security (un-authorised access) and IT security and recommends several IEC/ISO standards (ISO 27000ff, ISO/IEC/TR 19791 and the IEC 62443 series), which give a detailed advise on how to deal with IT security threats. The IEC 62443 standard is not railway specific and focuses on industrial control systems including automated car driving. Railways plan to integrate IEC 62443 security requirements into the domain specific safety standard (EN 50129 and EN 50159). In automotive industry it is proposed to integrate security concerns in ISO 26262 for a combined safety and security standard.

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, as it is outlined in Fig. 21.

3. OPERATIONAL SCENARIOS RELEVANT TO HELMET, ASSUMPTIONS

3.1 RAIL: OPERATIONAL SCENARIOS AND USER REQUIREMENTS FOR HELMET

In this section the most demanding rail operational scenarios from viewpoint of high-accuracy and high-integrity determination for HELMET solutions are described and high-level user requirements specified.

3.1.1 Track identification function

The purpose of the track identification function is to determine position of train on which of tracks in station or on multi-track line between station is located. This function is important e.g. for ERTMS Start of Mission (SOM) in Staff Responsible mode, when the last position of train is not a priory known before the onboard unit initialization / system start-up.

Alert Limit (AL) - across track

Definition of GNSS train position determination error (PE), which is required for specification of the maximal allowed train position determination error (Alert Limit - AL) defined by a user is outlined on Fig. 22.

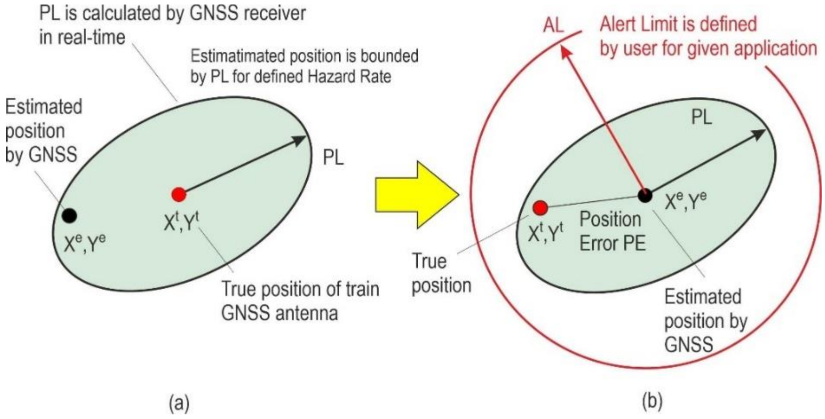


Figure 22. Definition of Protection Level and Alert Limit for train position determination. Position of GNSS antenna is: (a) known, (b) unknown

If true position of train antenna is known (X^t,Y^t), then the estimated position of GNSS antenna (X^e,Y^e) can differ from the true position (X^t,Y^t) – see Fig. 22(a). The difference between (X^t,Y^t) and (X^e,Y^e) represents a train position determination error PE. A guarantee of the PE with a certain level of probability (corresponding to the required certain level of safety defined by THR) is provided by the Protection Level (PL) calculated by GNSS receiver (part of OBU), which is usually expressed by multiples of standard deviations (sigma) related to position determination. The guarantee of PE is provided when PL correctly overbounds the (X^e,Y^e) .

If a train (GNSS antenna) position is unknown and the GNSS receiver correctly estimates its position, then the true antenna position (X^t,Y^t) must be also bounded by PL – see Fig. 22 (b). The maximum allowed value of PL is called Alert Limit (AL) and it is defined by user. AL is important parameter enabling to describe the track identification/ discrimination function – see Fig. 23.

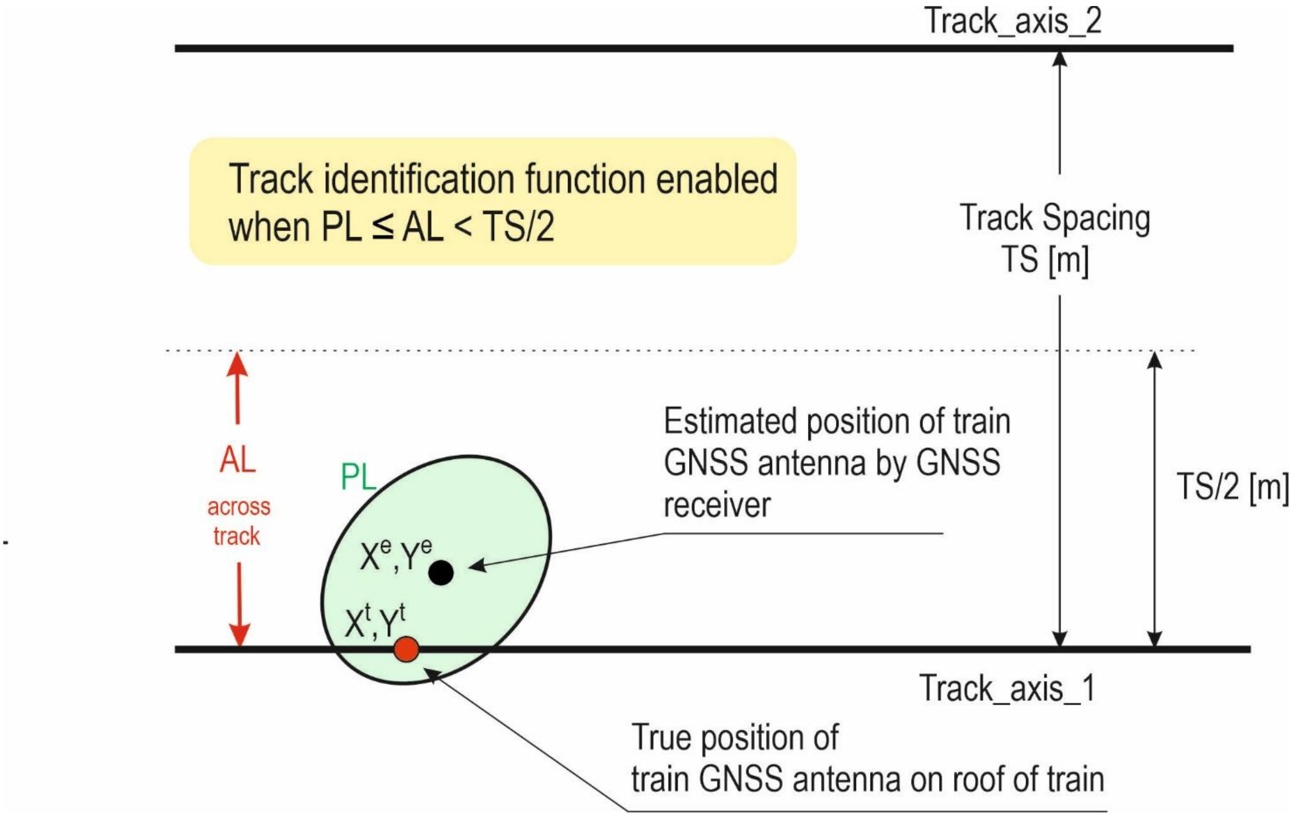

Track_axis_2
Track identification function enabled when PL ≤ AL < TS/2
Track Spacing TS [m]
AL
across track
PL
Estimated position of train GNSS antenna by GNSS receiver
TS/2 [m]
Xe,Ye
Xt,Yt
Track_axis_1
True position of train GNSS antenna on roof of train

Figure 23. Track identification function

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.

Typical values of track spacing TS for different types of track in different areas are listed in Table 16. 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.

Table 16. Track spacing values for different tracks

Area	Location	Track spacing (centre-to-centre) TS		Note
		Nominal [mm]	Minimum allowed [mm]	
Interstation section	Between tracks on double-track	4000	3570	v < 160 km/ hr
Station	Between running tracks	5000	4750	
	Between service tracks	5000	4750	
	Between tracks with platform between them with elevated access	10000	9500	
	Between tracks and platform between them without elevated access	6000	4750	
	Between transhipment siding/ tracks	3750	3750	
	Distance between track groups	6000	5000	

*Accuracy (2*sigma) - across track*

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. 24), 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 .

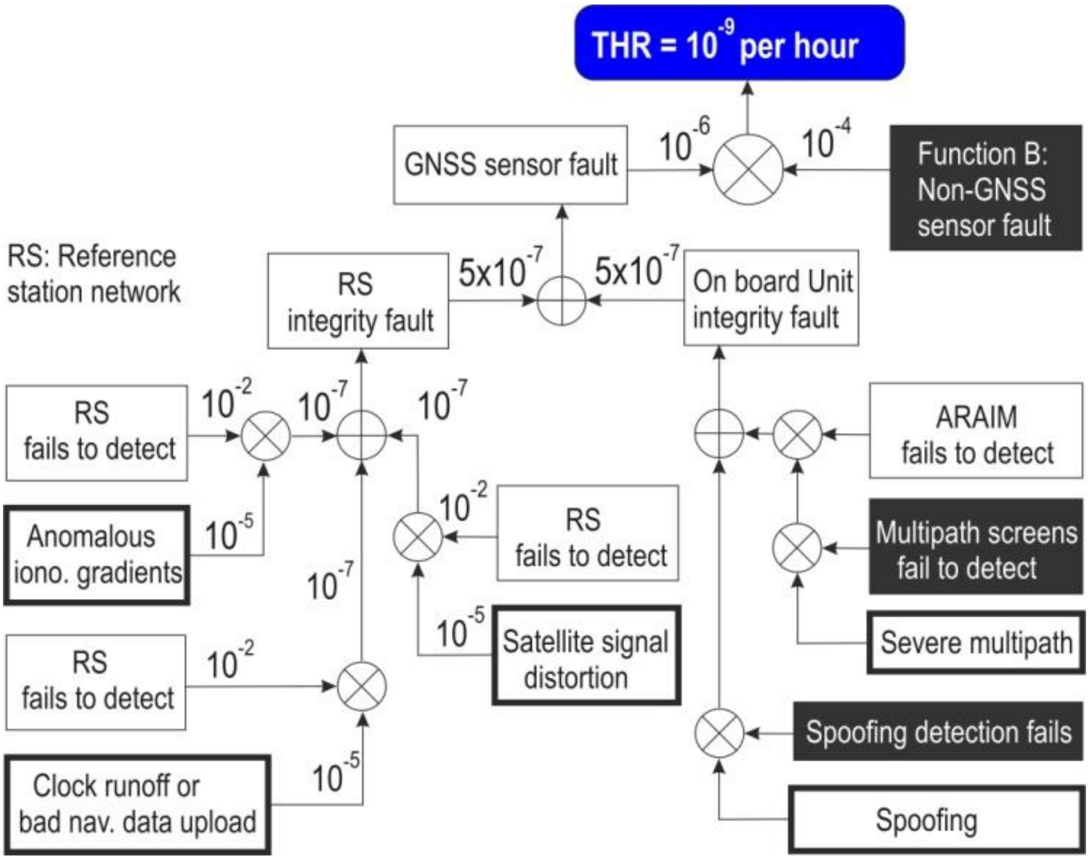


Figure 24. Example of THR allocation for GNSS-based train position determination function in RHINOS project [25]

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. This requirement for accuracy (2*sigma) is stricter than it is specified in Table 1 [1].

Conclusion: Accuracy (2*sigma) of train position determination shall be less than 1 m.

Availability

Availability of track identification function shall be HIGH [1]. This high-level user qualitative requirement will be specified in more details (quantitatively) in the deliverable D2.3.

Safety Integrity Level (SIL)

Safety integrity of track identification function shall be Very High and compliant with SIL 4. This requirement results from recent projects such as 3InSat, ERSAT EAV, RHINOS, ERSAT GGC.

Time-to-Alert (TTA)

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 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) [16].

Rationale:

- Availability: The time taken to initialise the ETCS onboard subsystem has operational implications, for example, it influences how long it takes to make a train ready to start a new journey when it reverses at a terminal station.
- Performance: Significantly increasing the time taken to make trains ready to start could impact on the ability to deliver the train timetable.

Therefore values of 10s < TTA < 30 s defined in [1] seems reasonable.
Conclusion: TTA shall be from 10 to 30 seconds.

Security

Security of the odometry calibration function should be HIGH in order to preserve related RAMS and confidentiality.

3.1.2 Odometer calibration function

ERTMS balises on a track are used to calibrate devices responsible for distance measurement, i.e. ERTMS odometry. The calibration of odometry is required due to a wheels wear. Solutions to improve ERTMS odometry performance shall provide efficient mechanism to reset/ calibrate/ periodically correct data to keep train position information within accuracy targets during the mission [18].

Rationale: maintenance activity for reset/calibrate *is costly and is sensitive action regarding introduction of errors, manual calibration should be avoided; reset/ calibrate/ periodically correct data mechanism have to be defined to fulfil accuracy targets.*

Solutions to improve ERTMS odometry performance shall be able to self-diagnose when accuracy targets are not fulfilled and the relevant mitigation/measure shall be identified, provided that safety is not affected. *Rationale: ERTMS needs odometry error determination to calculate the train confidence interval.*

It is assumed that the Odometry calibration function could be performed using a high accuracy and integrity GNSS solution.

*Accuracy (2*sigma) – along track*

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 [17]

More detailed specification of the location accuracy (e.g. using sigma) is missing in [17]. 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 < 1 m is required

Alert Limit – along track

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.

Time-to-Alert (TTA)

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 specification 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 .

Conclusion: TTA has to be less than 1 second.

Availability

Availability of the odometry calibration function shall be HIGH [1]. This high-level user qualitative requirement will be specified in more details (quantitatively) in the deliverable D2.3.

Safety Integrity Level (SIL)

Safety integrity the odometry calibration function shall be Very High and compliant with SIL 4 since ERTMS odometry is compliant with SIL 4.

Security

Security of the odometry calibration function should be HIGH in order to preserve related RAMS and confidentiality.

3.1.3 Cold Movement Detection

The ETCS onboard subsystem shall include (according to the ERTMS/ETCS Baseline 3 requirements) a Cold Movement Detection system. Cold Movement Detection serves to revalidate the train position upon leaving NP (No Power) , subject to the train not having moved. Maintenance of a valid position helps to reduce the dependency on operational procedures that result from degraded operation when starting with an invalid position.

The ETCS Cold Movement Detection function shall only be used to validate stored information if the information was known to be correct upon entry to NP.

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.

Alert Limit – along track

The Cold Movement Detection function shall only indicate any movement excessing 5 m [16]. This value is taken as user defined Alert Limit for odometer calibration function.

*Accuracy (2*sigma) – along track*

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

This requirement for accuracy (2*sigma) of 2 m is compliant with the accuracy interval of to the Rail [1].
Conclusion: Accuracy (2*sigma) of train position determination has to be less than 2 m.

Safety Integrity Level (SIL)

Safety integrity of the Cold Movement Detection function shall be Very High and compliant with SIL 4 since the Cold Movement Detector directly supports the ERTMS virtual balise detection function, which shall be also compliant with SIL 4.

Availability

Availability of the odometry calibration function shall be HIGH [1]. This high-level user qualitative requirement will be specified in more details (quantitatively) in the deliverable D2.3.

Security

Security of the cold movement detection function should be HIGH in order to preserve related RAMS and confidentiality.

3.1.4 Speed accuracy for ERTMS

It is required by ERTMS/ETCS Subset 041, that accuracy of speed known on-board shall be ± 2 km/h for speed lower than 30 km/h, then increasing linearly up to ± 12 km/h at 500 km/h.

Note: Only in target speed monitoring when the compensation of the speed measurement inaccuracy is not inhibited: the on-board equipment shall also evaluate a safe confidence interval in case of malfunctioning.

3.2 AUTO: OPERATIONAL SCENARIOS AND USER REQUIREMENTS FOR HELMET

In this section, the most demanding automotive operational scenarios from viewpoint of high-accuracy and high-integrity determination for HELMET solutions are described and related user requirements specified.

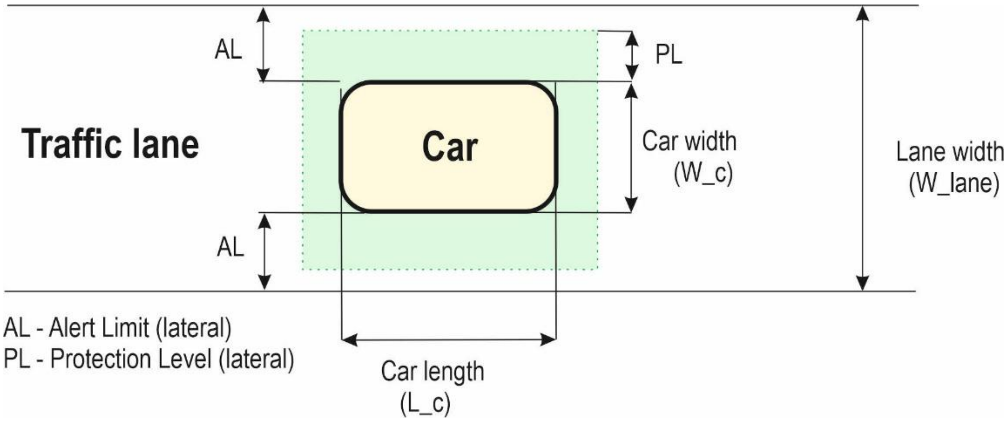


Figure 25. Definition of Alert Limit and Protection Level for automated car driving

Figure 25 outlines determination of lateral Alert Limit, which is used for derivation of HELMET accuracy for basic operational scenarios in sections below. The following dimensions of passenger car are used: Car with W_c = 2.1 m and Car length = 5 m. Note in this project phase, only Alert Limit in lateral direction is determined since AL lateral is more demanding due to the traffic lane width constrains.

In next sub-sections, basic automated car driving scenarios are described and related high-level user requirements justified. The scenarios include:

- Automated car driving on highway
- Automated car driving on local roads
- Automated car driving on narrow and curved roads

The main purpose of the analysis is to estimate basic values of Alert Limits and related Accuracies for HELMET position determination solutions. The main differentiator in these scenarios is a traffic lane width (W_lane). Since allowed velocity of vehicles depends on the lane width, the commonly used velocity intervals are allocated to the scenarios. At this high-level user requirements specification the impact of road/ lane arcs and curvatures is omitted because the main impact on AL and accuracy has a lane width.

It has been derived and described in HELMET D2.3 that the required Probability of Failure (PF) for car position determination related to GNSS (in composite fail-safety solution) can be 1 order higher than the related THR for train position determination, i.e. PF of 1e-5/ hr (for GNSS). The corresponding K-factor for Alert Limit / Accuracy determination is defined as AL= K * sigma, where sigma is standard deviation of GNSS position determination.

K – multiplier can be determined for Gaussian error distribution using Matlab as follows: abs(norminv(1e-5/2 ,0,1)) = 4.4172 ~ 4.4. In next subsections, a K value of 4.4 used for determination of GNSS accuracy (2*sigma) for all above operational scenarios.

In this report, Alert Limit (in lateral direction) is calculated for a passenger car with a typical car width (W_c) of 2.1 m. Alert Limit in longitudinal direction is not calculated for these high-level user requirements because Alert Limit in lateral direction is much more demanding than in longitudinal or vertical direction.

Note:
It is still questionable if the same level of robustness (safety integrity) of the position determination function required for high speed scenarios (e.g. on highways) is also required for scenarios with much lower allowed car velocities (e.g. on narrow roads) where the associated safety risk is also much lower. It creates a space for relaxing demands on accuracy of GNSS-based position and it could also lead higher allowed values of sigma for car positioning. This question will be discussed in later phases of the HELMET project.

3.2.1 Automated driving on highway

A usual width of traffic lane (W_lane) on highway is 3.6 m. The corresponding car velocity on highway is usually in a range of 80 - 130 km/ hr.

Alert Limit (lateral)
W_c = 2.1 m; W_lane = 3.6 m
AL = (W_lane – W_c)/ 2 = (3.6 – 2.1)/2 = 0.75 m

*GNSS accuracy for car position determination (2*sigma)*
AL = K * sigma → 4.4 * sigma
0.75 = 4.4 * sigma → sigma = 0.75/4.4 = 0.1705 m
Accuracy = 2*sigma = 2 * 0.1705 = 0.3409 m ~ 34 cm

Time-to Alert (TTA)
TTA < 1 s. This estimate is based on the experience with high-safety integrity railway systems.

Automotive safety Integrity Level (ASIL)
It is estimated and justified in the deliverable D2.3 (Systems requirements) that ASIL D is required for car position determination - as a whole system.

Availability
HIGH availability of car position determination function is required because availability has the direct impact on car safety in this safety-critical (fault-tolerant) system. It results from the analysis of safety concepts elaborated in the HELMET deliverable D2.2 (CONOPS).

Security
Security of car position determination function shall be HIGH in order to preserve related RAMS attributes and confidentiality.

3.2.2 Automated driving on local roads

A usual width of lane (W_lane) on a local road is 3 m. The corresponding car velocity on a local road is usually in a range of 60 - 90 km/ hr, depending on local conditions.

Alert Limit (lateral)
W_c = 2.1 m; W_lane = 3.0 m
AL = (W_lane – W_c)/ 2 = (3.0 - 2.1)/2 = 0.45 m

*GNSS accuracy for car position determination (2*sigma)*
AL = K * sigma → 4.4 * sigma
0.45 = 4.4 * sigma → sigma = 0.45/4.4 = 0.1023 m
Accuracy = 2*sigma = 2 * 0.1023 = 0.2046 m ~ 20 cm

Time-to Alert (TTA)
TTA < 1 s. This estimate is based on the experience with high-safety integrity railway systems.

Automotive safety Integrity Level (ASIL)

It is estimated and justified in the deliverable D2.3 (Systems requirements) that ASIL D is required for car position determination - as a whole system.

Availability

HIGH availability of car position determination function is required because availability has the direct impact on car safety in this safety-critical (fault-tolerant) system. It results from the analysis of safety concepts elaborated in the HELMET deliverable D2.2 (CONOPS).

Security

Security of car position determination function shall be HIGH in order to preserve related RAMS attributes and confidentiality.

3.2.3 Automated driving on narrow and curved roads

A usual width of lane (W_lane) on a narrow and curved roads is 2.5 m. The corresponding car velocity on a local road (or temporarily narrowed lane during road repair) is usually in a range of 20 - 60 km/ hr, depending on local conditions.

Alert Limit (lateral)

W_c = 2.1 m; W_lane = 2.5 m
AL = (W_lane – W_c)/ 2 = (2.5 - 2.1)/2 = 0.2 m

*GNSS accuracy for car position determination (2*sigma)*

AL = K * sigma → 4.4 * sigma

0.2 = 4.4 * sigma → sigma = 0.2/4.4 = 0.0455 m

Accuracy = 2*sigma = 2 * 0.0455 = 0.0909 m ~ 9 cm

Time-to Alert (TTA)

TTA < 1 s. This estimate is based on the experience with high-safety integrity railway systems.

Automotive safety Integrity Level (ASIL)

It is estimated and justified in the deliverable D2.3 (Systems requirements) that ASIL D is required for car position determination - as a whole system.

Availability

HIGH availability of car position determination function is required because availability has the direct impact on car safety in this safety-critical (fault-tolerant) system. It results from the analysis of safety concepts elaborated in the HELMET deliverable D2.2 (CONOPS).

Security

Security of car position determination function shall be HIGH in order to preserve related RAMS attributes and confidentiality.

3.2.4 Speed accuracy

In many countries the legislated error in speedometer readings is ultimately governed by the United Nations Economic Commission for Europe (UNECE) Regulation 39 (2017), which covers those aspects of vehicle type approval that relate to speedometers.

European Union member states must also grant type approval to vehicles meeting similar EU standards. The ones covering speedometers are similar to the UNECE regulation in that they specify that:

- 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.

These requirements related to speed accuracy will be analysed in more details from the automated car driving viewpoint in the deliverable D2.3.

3.3 UAS/RPAS: OPERATIONAL SCENARIOS AND USER REQUIREMENTS FOR HELMET

3.3.1 General

This section provides the UAS/RPAS-PIT Station Segment selected Operational Scenarios involving the most representative rail and automotive Inspection, Monitoring and Traffic Management (IMTM) Applications that the Aerial Segment will serve so as to establish the related to such applications, HELMET User Requirements and those exclusively dedicated to the safe aerial operations. The UAS/RPAS-PIT Station Segment IMTM services shall enhance significantly the Reliability, Availability, Maintainability and Safety of both Rail and Automotive Operations at a cost-effective manner (Operations with UAS/RPAS often cost less than using manned aircraft) since UAS/RPAS operations are particularly effective for missions that are dangerous or tiring:

a) Humans are not put at risk
b) Continuous operations are possible

In various User Surveys on the use of UAS/RPAS on Rail and Road Assets IMTM services, they were specified the following most required services which shall apply as far as possible to the scenarios provided in this document:

1) Railway and Road Infrastructural Assets Construction Works Status Inspection and Monitoring
2) Inspection and Evaluation of damages, defects or deformations and cracks of bridges, tunnels, depot buildings, railway tracks, and road pavement conditions for accessibility;
3) Inspection for maintenance of high value rail and road assets;
4) Perform Aerial imaging to support Geographic Information System (GIS) database for Rail and Road assets;
5) Perform Rail and Road Assets/Property General Survey and Inventory Control for future Growth and Development Needs;
6) Surveying and Classifying plant species to be removed and/or relocated while constructing a future railway track and/or highway and/or Urban or Extra-Urban Road;
7) Monitoring for Improving safety of labour when working on railway, highways and roads;
8) Monitoring Highway, Road (Urban and Extra-Urban) Traffic Conditions, and Tracking Vehicle movements at important and/or statistically dangerous intersections;

9) Monitoring and/or Managing Emergency and/or Civil Protection Vehicle Guidance;
10) Tracking, Surveillance and Monitoring of Accidents and/or Post-Accident on railways and roads;
11) Traffic Data Collection and signage inventory;
12) Surveillance for acts of vandalism on rail and road assets/property, monitoring illegal acts (i.e. theft) and intrusions in segregated for safety and high value rail and road property.
13) Monitoring for obstacles on railway tracks and roads that will cause incidents and accidents.

3.3.2 Main IMTM UAS/RPAS Operational Scenarios Constraints

IMTM UAS/RPAS for railway and drone are expected to operate within a range of operational constraints, as follows:

a) Geofencing: Depending on UAS/RPAS size, weight (such as >100 g), speed, operating altitude and mission, it may be required to operate within specific geographic flight corridors or defined zones. A map-based UAS/RPAS flight restrictions have been imposed for flights around civilian and military airports, helipads and flight corridors. The more expensive UAS/RPAS have capability to have geofencing constraints programmed into the flight control system in order to prevent inadvertent incursion into unauthorised areas.
b) Weather**:** Due to their small size and relatively low weight compared to conventional aircraft, UAS/RPAS are more susceptible to wind, where loss of horizontal position control could pose safety risks. The more sophisticated and expensive UAS/RPAS will have some degree of automatic stabilisation and wind shear compensation built into the flight control system. While light rain may not constrain certain drone operations, if it is associated with low cloud and low-visibility conditions, it may affect line-of-sight (LOS) operations and degrade visual imaging payload data quality for certain missions (for example, video or imaging quality from surveys, asset inspection and security patrols).
c) Hours of Operation: Time constraints on UAS/RPAS operations may include restrictions on UAS/RPAS operation in the dark, as well as allowable hours of certain drone missions at night near residential areas out of hours, and over weekends and public holidays. This may also include limits on UAS/RPAS mission duration. Some flight operations are limited to daylight hours and visual line-of-sight (VLOS), unless otherwise agreed to with demonstrated controls in place. Security patrol missions at night may require prior local Civil Aviation Authority approval (at least for approving the generic patrol mission schedule).
d) Remote Operation Range: Depending on prior notification and agreement with local Civil Aviation Authority, UAS/RPAS may be constrained to VLOS, EVLOS and BVLOS remote operation. Additionally, UAS/RPAS are limited by the range of their wireless radio data link, both for flight control and for mission payload.
e) Endurance: UAS/RPAS operational endurance may be subject to constraints such as fuel limits or battery charge limits. This may affect range of operations and mission duration, including loiter time over the mission area and total range. Just like a larger sized aircraft, a UAS/RPAS faces a payload versus range trade-off, and this is currently a more pronounced issue with battery-powered UAS/RPAS until the technology improves. This may drive decisions to procure a larger long endurance UAS/RPAS, or to procure a fleet of smaller UAS/RPAS to be deployed in a relay as each UAS/RPAS consumes its fuel or energy supply. For the purpose of the HELMET project the development and employment of PIT Station Network has the specific purpose among others to provide and assure UAS/RPAS operational endurance and availability.
f) Weight and Size**:** UAS/RPAS weight and size limitations are regulated by EASA (as mentioned in previous sections of this document) in terms of licensing and restrictions on operations and depending on the particular use case and associated mission requirement, the UAS/RPAS size and weight may be relevant as an operational constraint in this project. However, for IMTM Railway and Road applications may be considered the employments of various small UAS/RPAS configurations for specific mission capabilities and performances.

g) Operational Altitude: EASA limits UAS/RPAS flight operations to 120 m above ground level (AGL) for most civilian UAS/RPAS including Railway and Road IMTM applications operations and will require prior EASA notification and approval to exceed this altitude constraints. However, the totality of the HELMET IMTM UAS/RPAS railway and road applications will require very low flight altitudes (approximately from 1m to 80m AGL).

h) Security: Depending on the particular use case and associated mission profiles for railway and road IMTM, UAS/RPAS will require some level of security against criminal attack, including both physical and cyber security controls. In addition to security constraints placed by local Civil Aviation Authorities on its UAS/RPAS operations, there are security constraints placed by third party agencies, including Defence, for operations close to security-sensitive sites.

i) Noise**:** UAS/RPAS IMTM railway and road operations may be constrained by environmental noise emission limits and how these may affect operations over or near residential areas and hospitals, as well as other areas where the noise may have adverse environmental effects on nesting birds and other animals. UAS/RPAS HELMET operations shall need to ensure compliance of their operations with the EU and EASA Protection of the Environment Operations Regulations.

j) Privacy**:** UAS/RPAS IMTM railway and road operations may be constrained by privacy requirements, such as in private residential areas, but even in public places there are requirements in the law that limit or prohibit the unauthorised video or imaging of private persons without their express authorisation. Mission plans will need to account for these privacy constraints as per EU and local State Member Regulations.

k) Human proximity**:** EASA limits UAS/RPAS flight operations to no less than 30 m from humans (other than the UAS/RPAS pilot, mission owner and other authorised staff). As mentioned in section 2.3.1 of this document, depending on particular use cases and UAS/RPAS weight constraints, an IMTM UAS/RPAS for railway and road applications may need to operate within the 30 m human proximity limit, provided it is operating within a controlled site with safe working arrangements including physical barriers, and authorised staff working with suitable personal protective equipment (such as hard hats, protective eyewear and gloves).

l) Human Factors: IMTM UAS/RPAS that require manual remote piloted operation will place constraints on the operator workload, situational awareness, and other human factors and ergonomic constraints that may limit safe and efficient operation within that use case. Increasing UAS/RPAS automation may improve this, but degraded and emergency modes will need to be considered where automated functions fail and result in reversion to human operation.

m) Safety Related Constraints: 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

Safety features such as obstacle avoidance and/or detect and avoid, automatic return to base (for this project such support base shall be the PIT Station) on low battery, prevention of injury in case of critical flight system failure, may need to be provisioned in UAS/RPAS regulations. UAS/RPAS, including fully autonomous ones equipped with pre-programmed routes, may suffer from poor visibility in some weather conditions, requiring regulations on flying in bad weather. Many of these safety constraints are addressed within other constraints imposed by EASA and/or Local Member EU State Civil Aviation Authorities, such as UAS/RPAS weight, operating height, proximity to humans, and line-of-sight.

3.3.3 Potential Sensor Technologies and Process Capabilities Required for the IMTM UAS/RPAS for Railway and Road Operational Applications.

In terms of payload sensor technology (see Fig. 26) for Urban/Sub-Urban roads, highways and railway IMTM applications, the following most common types of sensors are used depending on the mission and aerial work and purposes of the project CONOPs:

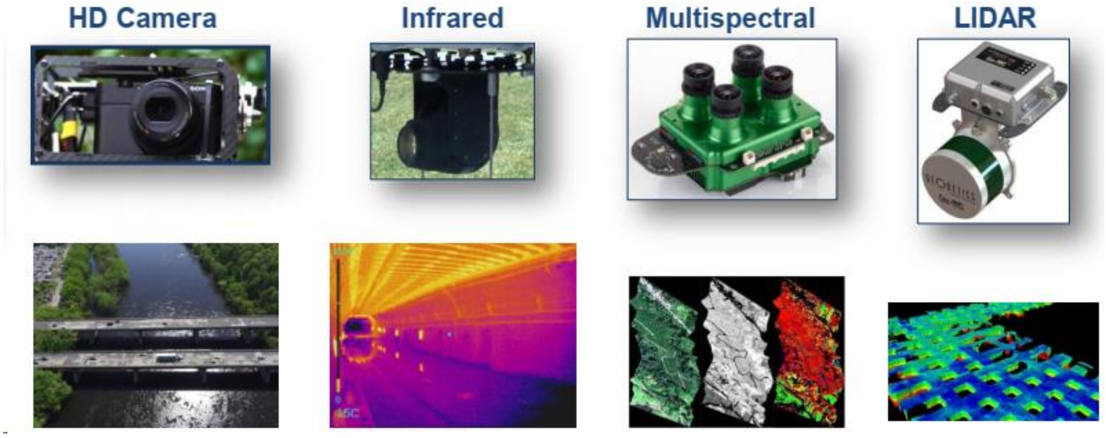


Figure 26. Example of payload sensor technology

a) High Definition (HD) Camera and/or Multispectral Sensor Visual Inspection and Monitoring – Railway Track, Highway/Road Pavements and Bridges Operational Scenarios, the main potential technologies and processes are:
   1) HD camera and/or Multispectral Sensor payload
   2) Live transmission
   3) Close up images
   4) Pre-planned flight
   5) Image Processing Methods:
      - ➢ Balanced Histogram Thresholding (BHT)
      - ➢ Hue Saturation Value (HSV)
      - ➢ P-Colour Threshold

b) Infrared Thermography for Inspection and Monitoring of Railway, Highway/Road Infrastructures (Pavements, Tracks, Bridges etc.) and Disaster Response Management Operational Scenarios, the main potential technologies and processes are:
   1) Infra-red camera payload
   2) Live transmission
   3) Defect inspection
      - ➢ Cracks
      - ➢ Holes
      - ➢ Leaks
   4) Disaster response management
      - ➢ Search and rescue (SAR)

c) Light Detection and Ranging (LiDAR) for Inspection and Survey of Railway, Highway/Road Infrastructures and Asset Management Operational Scenarios, the main potential technologies and processes are:
   1) Surface condition survey
   2) Crack detection
   3) 3D pothole geometry
   4) Grade model
   5) Rut model

6) Digital Elevation Model (DEM)
7) Building elevation model

d) Other: Robotic Arm Extender Holding Ultrasonic Equipment: for Inspection and Survey of Railway, Highway/Road Infrastructures and Asset Management Operational Scenarios, the main potential technologies and processes are:
1) Payload for Multi-rotor and/or Hybrid UAS/RPAS
2) Holds ultrasound equipment
3) Arm end holds transducer
4) Easy to manoeuvre around
5) 360 degree 3 axis movement
6) Extendable reach on walls
7) Allows safe distance between wall & UA/RPA
8) Controlled manually by ground station

3.3.4 Overview of the Common Required UAS/RPAS Operational Scenarios Framework for Railway and Road IMTM Applications

The required common UAS/RPAS Operational Framework for all Railway and Road IMTM Applications is based on the existing studies and can be classified into the following seven components:

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.

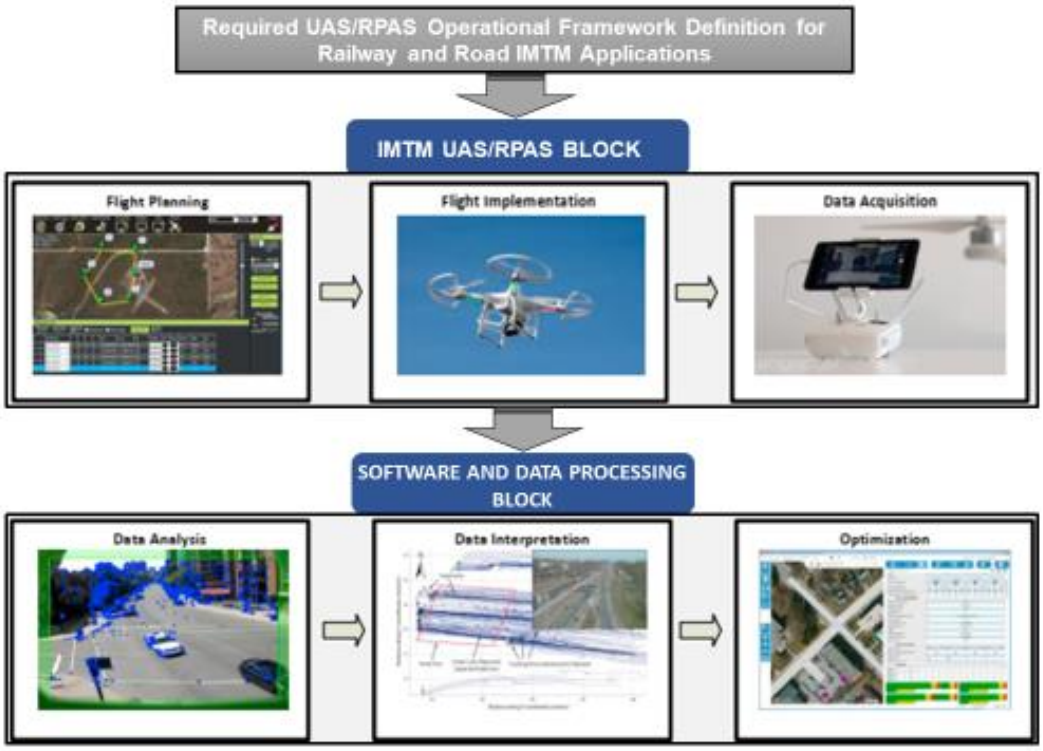

Required UAS/RPAS Operational Framework Definition for Railway and Road IMTM Applications
IMTM UAS/RPAS BLOCK
Flight Planning
Flight Implementation
Data Acquisition
SOFTWARE AND DATA PROCESSING BLOCK
Data Analysis
Data Interpretation
Optimization

Figure 27. Required UAS/RPAS Operational Framework for Railway and Road IMTM Applications Block Diagram

1) Operational Framework Definition: The first module of the Required UAS/RPAS Operational Framework for Railway and Road IMTM Applications involves the definition of the scope and identification of the specific operational mission to be conducted and its related scenario(s) - see Fig. 27. This is a critical step in defining the specific mission needs in terms of objectives, applicable regulations, standards, procedures and operational means. After the establishment of the above, the railways and road asset elements to be inspected, monitored and analysed are selected. This can be an intersection, a road or railway segment, a ramp, a bridge, a tunnel or a combination of them. In the Performance measures step, the parameters to be determined for the analysis are selected such as traffic volume, number of lane changes, vehicle and/or train classification, vehicle and/or train velocities, acceleration/deceleration, number of conflicts etc. The type of traffic parameters to be derived from the UAS/RPAS videos or other optical sensors shall also define the type of UA/RPA flight to be conducted e.g. extract the vehicle trajectories across the different legs of the intersection by just making the UA/RPA hover (constant altitude, zero velocity) above an intersection.

2) Flight Planning: The Flight Planning Stage involves the preparation for the implementation of the actual UAV flight for the collection of the required data. With the significant increase in the number of UAVs, state laws are now being formulated and implemented all over the world to avoid major mishaps. In this situation, the UAV flight planning step has become even more important. This implies that an in-depth flight planning, based on the project parameters or scope is essential. Based on the literature survey of the traffic related UAV studies, the whole process of the UAV flight planning may be classified into three main categories; safety, environment and route planning aspects, as shown in Fig. 28.

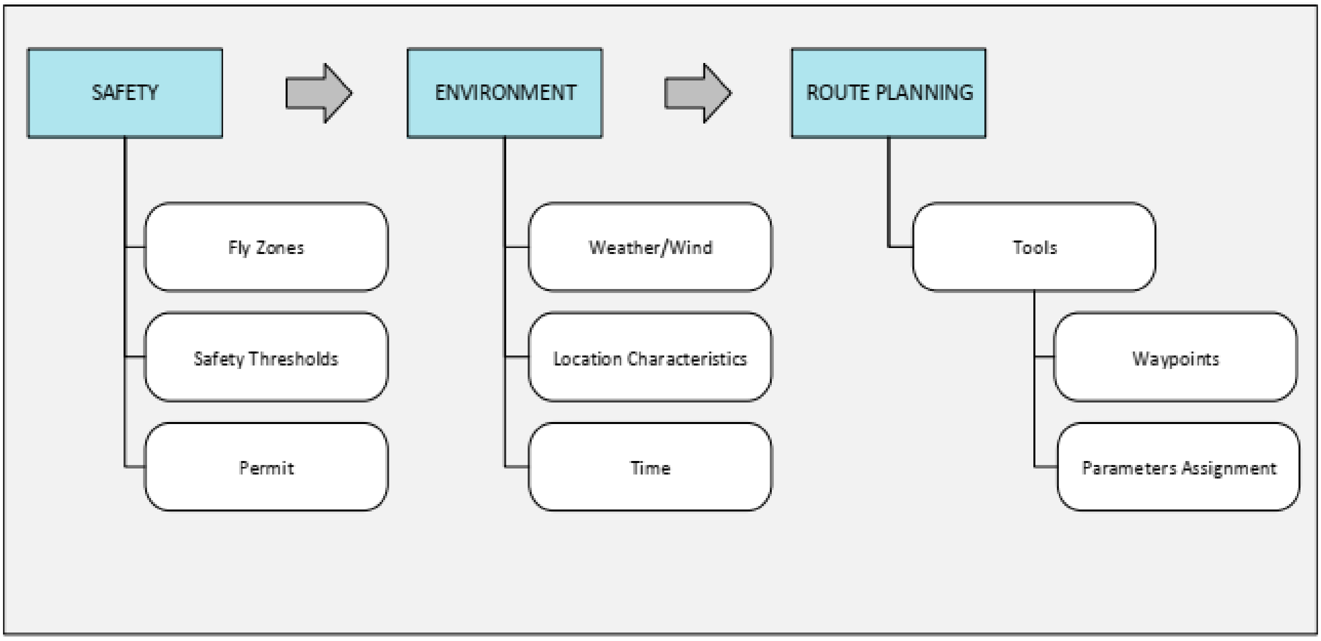


Figure 28. Flight Planning Process Steps

These three categories include all the aspects that are critical for ensuring a successful UA/RPA flight operation. First of all, the flying zone category must be evaluated with the help of the local flying zone maps. Also, a safe distance has to be maintained from the active airfields and from other sensitive installations. Based on the relevant flying zone, safety thresholds and other project characteristics, the flight parameters may be selected during the flight planning process. This is followed by an acquisition of a flight permit from the concerned department. This process shall become easier with the employment of UAS/RPAS local and global flight management platforms which shall automate a number of steps involved ensuring safety and attaining flight permits.

The specific location characteristics of the railway and road infrastructural environment where the flight operations will be performed must also be considered in quest for an optimal set of flight parameters including of alternatives or contingency plans in case of emergencies. Apart from the spatial planning for the UA/RPA flight, a temporal planning is also necessary. This requires a special deliberation towards the weather and wind conditions in the area of interest along with the optimal selection for the time of the day. For example, the conduct of UA/RPA flight operations at noon, as the shadows are minimal during this time of the day, ultimately can result in an easier and higher quality analysis of the sensor and/or video data. Also, the interference effects of electromagnetic emissions and the status of GNSS satellites especially in case of an automated and/or autonomous UA/RPA flight must also be considered during the planning phase.

With the advancement in the technology, UA/RPA flight planning tools have been developed that enable a more systematic and automated and/or autonomous flight operation. Using such tools, the users can mark the waypoints along the desired path. The users can plan and upload the exact route of the flight to the UA/RPA for an automated flight. Mission Planner and Command and Control ground stations are examples of such software. However, a backup certified pilot in line of sight (LOS) is compulsory even for automated UAV flights in the civilian domain due to security and insurance constraints.

3) Flight Implementation Stage: During the flight implementation Stage, the UA/RPA actually flies over an area of interest as per planned flight path/route. The specific flight shall be conducted on the basis of the parameters decided during the flight planning stage. The flight depending upon the user’s preference and flying expertise is controlled either manually via the radio controller or automatically via the auto-pilot function. This step in conjunction with the flight planning requires a number of safety and legal issues to be carefully addressed as mentioned in the previous procedure. During the UA/RPA flight implementation, it is also that the sensed data is of the highest quality thus not blurred or shaky or wobbly. While minor stability issues can be handled during the pre-processing stages, the payload sensor platform has to be stable enough to achieve a high quality video and/or imagery. For this purpose, most UAVs hold a gimbal (3-axis) which allows the rotation of the camera about a single axis only. The gimbal has its own motion sensors (similar to those that hold the UA/RPA stable) and small motors. It keeps the motion of the sensor independent (within certain limits) from the motions of the UA/RPA (motions from tilting to move forward or sideways, or when hit by a gust of wind). The payload operator shall be able to aim the sensor at will (overriding the ‘lock’ of the sensor position relative to the environment).

4) Data Acquisition: The acquisition of data from the UA/RPA shall also be a critical step of the IMTM operational framework and is largely dependent on the scope of the required railway and road specific applications. The data that has to be acquired from the UA/RPA includes the high quality UA/RPA sensed and recorded data of the area of interest by the payload sensors (infrared, thermal, ultrasonic etc.) mounted on the UA/RPA. In some cases, the flight telemetry data (altitude, horizontal speed, vertical speed along with the position and the orientation data) which is also acquired from the UA/RPA in order to calibrate the sensed data. The integration of position and orientation data generated by the navigation unit of the UA/RPA leads to a reduction of the number of physical control points that are required for the orientation and calibration of the UA/RPA sensed data. Overall, the scope specific data is acquired from the UAV and is then further treated and processed during the later stages of the operations framework. The data acquisition can be real-time or offline depending upon the requirements of the specific mission. Most of the known Inspection and Survey operations employ an offline processing approach in which the data is acquired and processed after the completion of the UA/RPA flight. On the other hand, the majority of the Monitoring and Traffic

Management (i.e. real time vehicle tracking and/or patrolling railway and road assets for surveillance) applications will be transmitting real time sensed data to the IMTM Operations Centre.

5) Data Processing & Analysis: Sensed Data Processing and Analysis is one of the critical steps of the operations framework that enables the IMTM railway and road operations personnel to easily collect detailed trajectory data and at the same time have a visual (real and/or non-real observation of the specific mission resulted work). However, the analysis of a traffic stream from a video recorded via an unstable aerial platform i.e. a UA/RPA is a relatively new topic. This process is more complex as compared to the analysis of a moving traffic stream from a stationary or fixed camera system. Multiple approaches have been employed in the existing literature for the processing and analysis of the UA/RPA based traffic data. These approaches can be broadly classified into two categories:

a) Semi-Automated Sensed Data Analysis: The semi-automated sensed data processing and analysis approach has been employed in a number of IMTM related UA/RPA operations. Such an approach is easy to set up and ensures a high level of accuracy and reliability. Also, no complex image processing algorithms are required which implies that far less computational power is needed. On the other hand, this approach is more laborious and generally requires more manpower as it generally involves the establishment of some physical ground control points (GCPs) or have certain lengths accurately measured on the site in order to calibrate the UA/RPA images.
b) Automated Sensed Data Analysis: An automated analysis of the UA/RPA acquired sensed data involves a series of advanced image processing filters and techniques in order to detect and track the relevant railway and road users. The automated sensed data analysis is gaining popularity especially for the real-time traffic monitoring and tracking applications. Although such an approach is quick and requires minimal manpower, it still has some limitations. Generally, the accuracy of such systems fluctuates dramatically with changes in conditions such as light, climate etc. Additionally, the automated system requires a high computational power and is difficult to initially set up as it involves complex algorithms for each sub-task of the analysis. In the case of the analysis of the UA/RPA-based traffic footage involves some pre-processing and stabilization procedures. These are necessary in order to make the video ready for the actual analyses steps. After the Geo-Referencing or calibration of the images to the real coordinate system, the detection and tracking of different railway and road users is carried out either automatically or semi-automatically as exposed earlier.

6) Data Interpretation: The interpretation of the processed IMTM sensed data is the next step in the operations framework. The interpretation shall be done with the help of different types of graphs and charts that are generated as an output of the data analysis procedures. This step too, along with the preceding steps of the present operations framework, is directly dependent on the scope of the specific railway and road applications. For instance, the trajectories of the vehicles or other road users extracted during the analysis part are displayed in x-y planar graphs to understand the behaviour and trend of the road users.

7) Optimized IMTM Applications: The optimized conclusion of the specifically planned IMTM operation(s) in accordance with its scope is the final step in the UA/RPA based analysis framework. The optimization of specific IMTM parameters determined during the analysis and interpretation steps shall be employed to improve the existing train and road IMTM models which they will ultimately also help in solving the real world traffic management situations. For example, this application dependent optimization may include a number of traffic related objectives such as traffic signal optimization, observation of drivers' behaviours, lane change manoeuvres etc. Moreover, a

real-time information system can optimize the traffic operation by sending alerts to the concerned departments in case of incidents and emergencies. By comparing the IMTM parameters obtained via the analysis of the UA/RPA acquired data with the IMTM parameters obtained via macro-simulation models.

3.3.5 IMTM UAS/RPAS Operational Environment Framework

The UAS/RPAS Operational Environment Framework applicable for IMTM railway and road applications is that of rail and road themselves and regards the GNSS PVT and Augmentation services performance under such environment. All the aerial operations in VLOS, EVLOS and BVLOS mode at VLL conditions considered herein are performed within the railway and road area of normal operations. Therefore, for the scenarios provided herein, the operational environment framework will be as follows:

1) Open Sky Regional and Sub-Urban IMTM UAS/RPAS Operational Environment: The Open Sky Environment for IMTM UAS/RPAS Operations is characterized by a good satellite visibility if the total number of GNSS satellites in view are appropriate for the PVT computation and are more than the minimum number for PVT computation. Moreover, an open sky environment is characterized by good satellite visibility if the overall geometry of the various GNSS satellites with respect to the user receiver results in a low DOP. Under the IMTM UAS/RPAS operational scenarios, these two conditions should be satisfied continuously with rare interruptions. In addition, an open sky environment also provides good EGNOS satellite visibility in terms of line of sight reception, with rare and limited reduction of such visibility.

2) Restricted Regional and Sub-Urban IMTM UAS/RPAS Operational Environment: The Restricted Environment is characterized by frequent interruptions of satellite visibility, and a significant reduction of the number of available GNSS satellites for PVT computation and consequently a large value of the DOP. A restricted environment is also characterized by a continuously changing visibility of individual satellites and GNSS signal multiple reflections (multipath) or also with no direct reception of the satellite signal (NLOS Non-Line Of Sight reception). In a restricted environment, the EGNOS satellites might only be visible sporadically. Typical restricted environment areas are:
    a) Tunnels, under bridges
    b) Vicinity to other Infrastructures such as Industrial Areas, Airports etc.
    c) Woods/Forests
    d) Mountains and Canyons

3) Urban/Local Operational Environment: The Urban/Local Environment is characterized by frequent interruptions of satellite visibility, with the number of available GNSS satellites for PVT computation significantly reduced, and a continuous changing visibility of individual satellites and consequently a continuously changing DOP value greater than a minimum number. This is combined with high probability of multipath and NLOS phenomena affecting GNSS signals, largely due to reflections and obstructions created by surrounding buildings.

It is important to stress that all of the above Operational Environments are subjected to variable intensity EMI phenomena caused naturally or are man-made together with the various other naturally occurring environmental conditions (temperature, rain, snow, wind, radiation etc.) which can influence the overall needed GNSS performance as two-way (up-link, downlink) interference.

3.3.6 Typical Flight Operative Modes Applicable to IMTM UAS/RPAS Operations

Herein is provided an overview of the most common operative modes available on off-the-shelf small UAS/RPAS. 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**.**

1) MANUAL: (UAS/RPAS attitude and height control only) In manual mode the pilot has full control of the aircraft; the FCU automatically controls the attitude of the UA/RPA on the horizontal plane to keep always a levelled flight and the height's control. No other control or software assistance is provided by the FCU in this flight mode. The pilot's commands are always mixed with the attitude and height control and are never overridden by on-board software in normal flight conditions. The integration of on-board SW is: Medium. The pilot's workload is: High**.**

2) ASSISTED: (Positioning, UAS/RPAS attitude and height control): In assisted mode the pilot has full control of the aircraft; the FCU automatically controls the attitude of the UA/RPA, the height and the horizontal position control. In this mode the UA/RPA is capable of hovering with outstanding precision in a fixed point in open sky. The wind's effect is autonomously corrected by using the on-board GNSS receiver. The pilot's commands are always mixed with on board software control the and never overridden by on-board navigation software in normal flight conditions. The integration of on-board SW is: High The pilot's workload is: Medium.

3) IOC (Intelligent Orientation Control): The IOC operating mode is a simplified flight mode useful to ease the pilot in normal and emergency flight manoeuvres and it is valuable for some VLOS operations. IOC can be switched only from Assisted mode with sufficient GNSS satellite coverage, used for UA/RPA position determination. In IOC flight mode the pilot's console control sticks are independent from aircraft's heading but are referred to the aircraft HOME point position. The integration of on-board SW is: High The pilot's workload is: Medium.

4) AUTO (Waypoint Navigation): In Auto (automatic) flight mode the pilot has no control of the aircraft during (autopilot) navigation, but he/she can always disengage autopilot system and take back full control of the aircraft in any moment. In this mode the aircraft is capable to implement an automatic flight plan with programmed waypoints. The integration of on-board SW is: High The pilot's workload is: Low.

Finally, there is an additional operational flight mode (*Failsafe*) which is handled internally by the FCU software. Failsafe is triggered by events or subsystems failures (*e.g. Loss of C2 link),* but it can also be switched by the pilot in emergency flight conditions forcing the aircraft to land or to return to home autonomously as it should be described in the emergency procedures of the UA/RPA manual. In Figure 29 it is reported a graph showing the possible transitions among different operational modes (aircraft status). The red dotted arrows stand for autonomous transitions handled by on board software, the black ones stands for pilot's driven operational modes changes.

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.

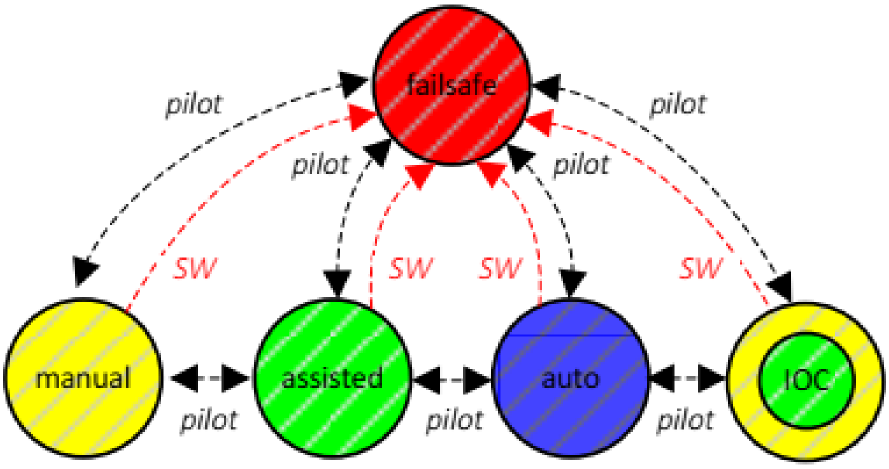


Figure 29. Possible Transitions among Different Flight Modes

In terms of IMTM UAS/RPAS-PIT Station Flight Operations for Railway and Road, the intended system architecture for all IMTM UAS/RPAS scenarios is shown in Figure 30.

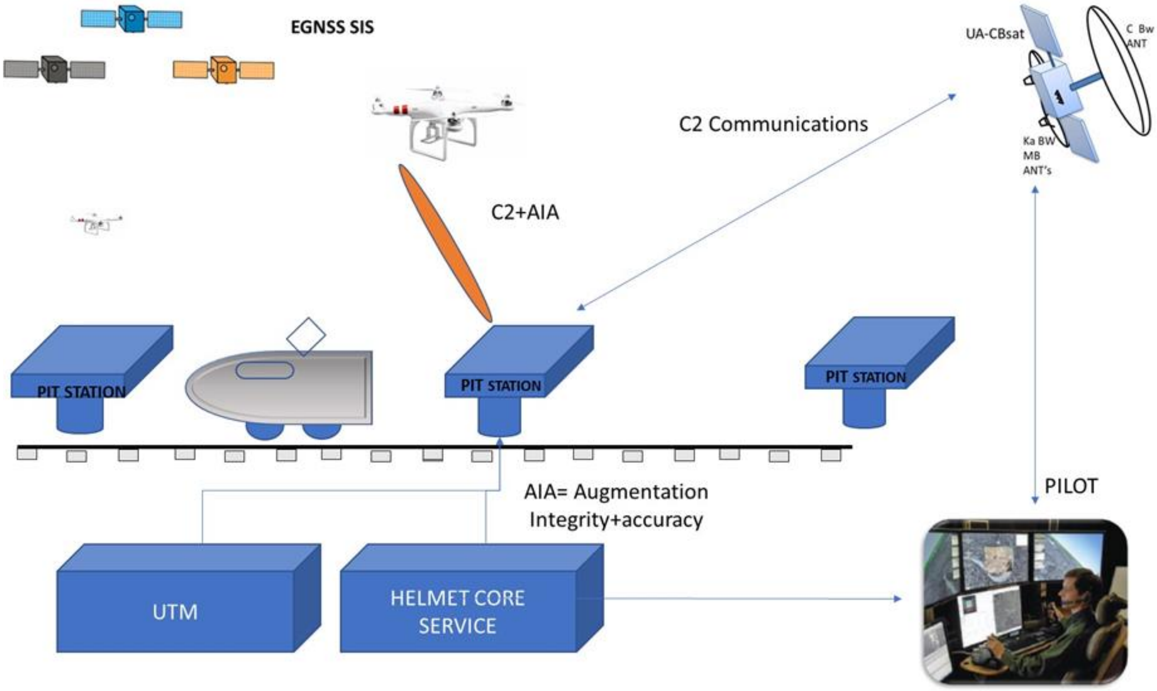


Figure 30. Overall IMTM UAS/RPAS-PIT Operational Scenario Application for HELMET

Figure 30 shows the generic operational architectural scheme for railway IMTM applications. However, the same architecture will be also applicable to the automotive road and highway assets. The entire IMTM UAS/RPAS Rail and Road operational scenarios shall be constrained by virtual fences, an example for railway UAS/RPAS operations is shown in Figure 31 below:

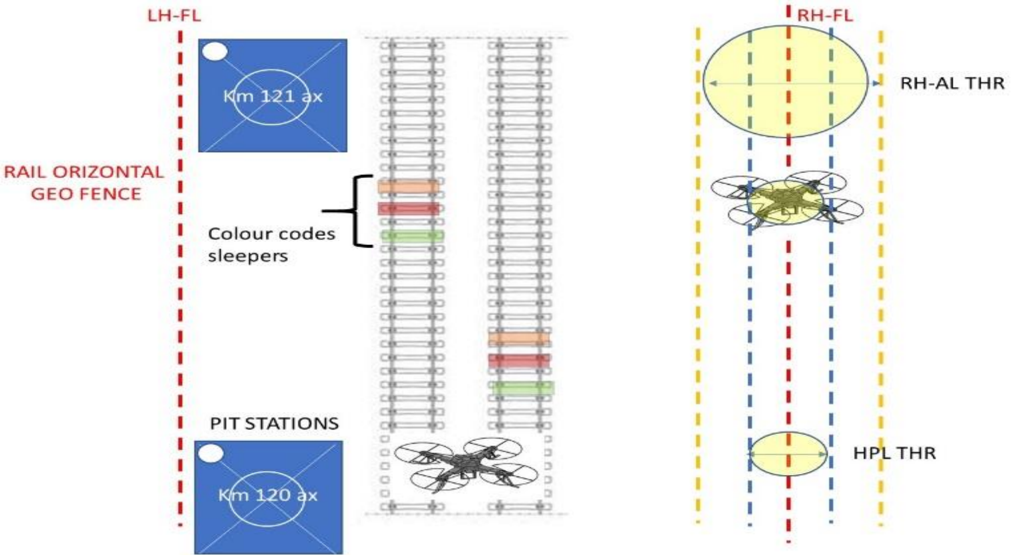


Figure 31. Example of IMTM UAS/RPAS Rail Operational Scenario with the Operational Area Constrained by Virtual Fences

For the time being it is proposed a study case of a UAS/RPAS that operates in a way that it will require at all times the pilot's presence and supervision in the fail-safe mode that could be accepted for initial service experimentation form designed institutions. UAS/RPAS avionics could be embedded with:

1) EGNSS rx with dual antenna for heading/ attitude control
2) IMU (accelerometer, gyro)
3) Magnetic compass, barometer
4) SW for position and navigation integration based on Kalman filter
5) Autopilot
6) On board SW controller with FDIR
7) Augmentation/UTM control communication link (can be included in the C2 link)
8) Remote C2 communication link
9) VBN (visual based navigation) on the basis of PIT station reference and sleeper coding, used for navigation check-point and attitude calibration.

The basic operation consists of transfer from the PIT station A to the PIT station B along the railway and road infrastructure. Figure 32 shows schematically the PIT to PIT Operation:

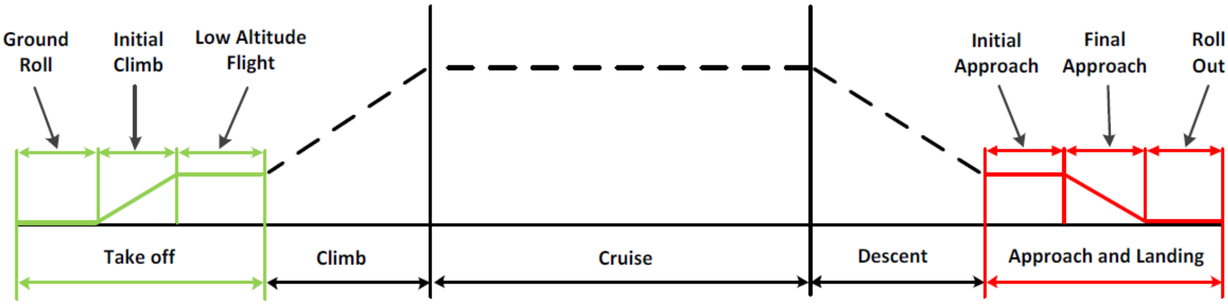


Figure 32. UAS/RPAS Operation PIT to PIT Schematic

The specific operations are:

1) **PIT Station A**

- Check and confirm the UAV identifier
- Refuel UAV
- Set local coordinate and target PIT coordinate
- Compute trajectory
- Select altitude and speed
- Select positioning accuracy AL and PL
- Set fence box vertical and horizontal limits
- Set recovery actions
- Set alternative reference positioning and navigation objects
- Set operative modes (i.e. observation, data gathering, etc.)
- Set communication operative frequencies and encryption keys
- Verify communication links operations
- Take-off on pilot command through local authorization (and UTM)

2) En-Route/Aerial Work

Then the UA/RPA takes off and reach the operative altitude. The trajectory is controlled by ha 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 autonomous means for controlling and commanding the UA/RPA as alternative to other systems. Because the small UA/RPA can't usually communicate directly with the Communications satellite the PIT station can operate as relay. The augmentation data comes form HELMET core service centre. In case there is a real time link between pilot and RPAS then it is possible to re-plan operation or take direct control of the RPAS.

Then the UA/RPA 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).

3) 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
- Landing
- Refuelling
- Dump acquired data for tx to Pilot or users via ground or space networks
- Check-up health
- Reprogram operation as for station A
- Goes next PIT stations

As mentioned before, the PIT stations tx to the UAV and pilot the integrity levels of position accuracy and receive back current position of UA/RPA that is then tx to the UTM. Any violation of trajectory or non-planned actions are immediately tx to the pilot. Basically, the UA/RPA operation area is thought not accessible for other UA/RPA or aircraft however a ADS-B tx only transponder 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.

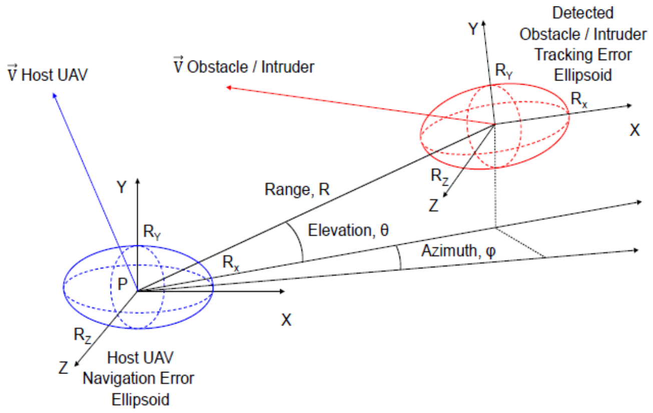


Figure 33. Obstacle detection by UAV

Any other activity in the operational aerospace shall be communicated to the pilot for flight re-planning.

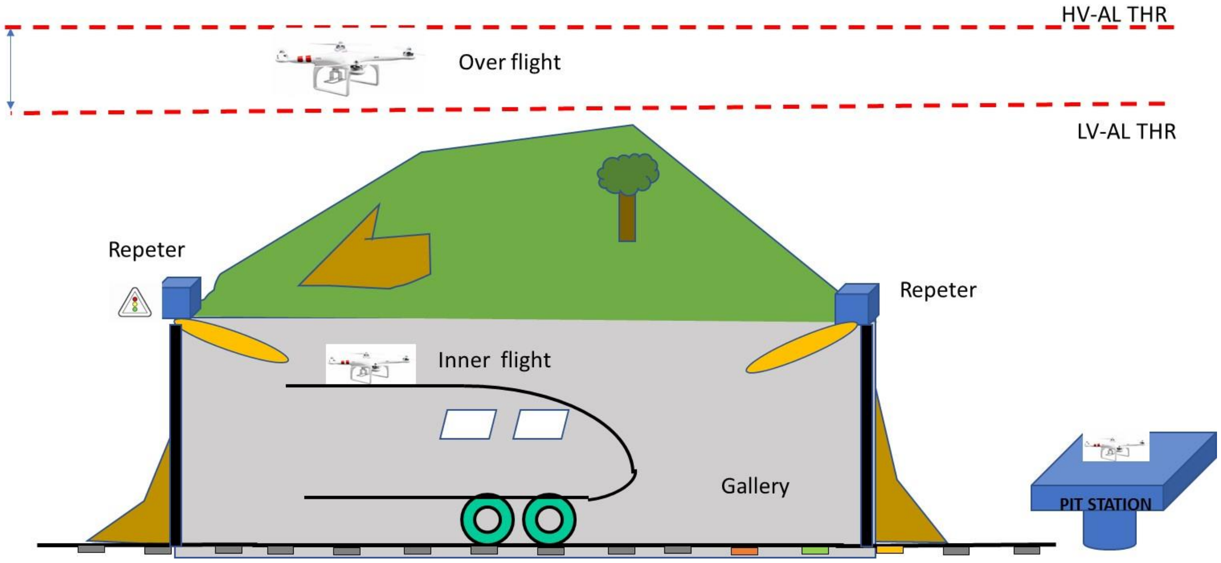


Figure 34. Example of UAS/RPAS Railway IMTM Application

3.3.7 UAS/RPAS IMTM Railway and Road Operational Scenarios

The following subsections provide a number of representative and not exhaustive scenarios for UAS/RPAS Railway and Road IMTM Applications within the Open Sky, Restricted and Urban/Local environmental operational conditions (see Fig. 33 and 34).

3.3.7.1 UAS/RPAS Inspection of Railway and Road Assets In Concurrent Operational Scenarios

A) SCENARIO: Three (3) small UAS/RPAS of the HELMET Support Services Network (which includes the PIT stations installed along the Railway and Road Systems) are involved in concurrent Inspection operations of a railway tunnel for maintenance, a railway metallic bridge structural condition and a road pavement condition in the UTM airspace under open sky, restricted and urban/local environmental operational conditions. The first UAS/RPAS is a small rotary wing (quad-copter) involved in the tunnel inspection mission performing an Infrared Thermography in VLOS flight mode in restricted operational environment conditions (tunnel). The second UAS/RPAS is also a small rotary wing as the first with a Robotic Arm Extender Holding Ultrasonic Equipment and it is involved in inspecting a metallic railway bridge in an urban/local area. The third UAS/RPAS is a fixed wing hybrid type equipped with a Light Detection and Ranging (LiDAR) sensor performing a road pavement condition inspection under open sky environmental conditions at BVLOS mode. All of the UAS/RPAS involved can be fully supported by the PIT Stations distributed in strategic locations within the HELMET Network service areas. All UAS/RPAS involved have a fail-safe flight mode capabilities and they have an approved flight plan by the local UTM and they aren't to exceed 100m altitude AGL during flight operations within the established geo-fencing restrictions.

B) SCENARIO FLIGHT PHASES, MISSION ENDURANCE AND RANGE: The Scenario Flight Phases for all UAS/RPAS involved are Pre-Flight, Take-off, Arrival to the mission area, Performance of the Planned Aerial Work and Return to Base (Landing), Post-Flight Operations. However, there are some slight differences on the planned aerial work. For the first two, most of the aerial work is at hovering conditions at low altitude from o.5m-20m (vertical) and lateral movements (25cm-10m) focusing at the inspection zone of the asset, while the third UAS/RPAS will have more complex flight trajectory going from straight flight up to 1km and back, to loitering and hovering periods around the target area at altitudes that can vary from 5m to 100m. All operational steps described in section 3.3.4 are applicable. Taking into account of the single UAS/RPAS involved in the above missions performance capabilities the mean endurance will be 90min (without PIT Station Support) while the range will be variable from 500m to 30km.

C) UAS/RPAS INSPECTION OPERATIONS GNSS REQUIREMENTS (see Table 17)

Table 17. Requirements for GNSS from viewpoint of UAS/RPAS inspection operations

INSPECTION MISSION (RAIL/AUTOMOTIVE)	ACCURACY HORIZONTAL	ACCURACY VERTICAL	INTEGRITY	TIME-TO-ALERT	CONTINUITY	AVAILABILITY
Position/Navigation	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

D) U-SPACE SERVICES:

1) U1: Pre-tactical Geofencing;
2) U2: Strategic Deconfliction; Flight Planning Management, Weather Information

E) ACTORS INVOLVED:

1) UTM Controller
2) UAS/RPAS Pilot, Aerial Services Management and Flight Line Support Personnel
3) HELMET Service Provider
4) Railway Assets Management
5) Road and Highway Assets Management

F) OTHER APPLICATIONS FEASIBLE UNDER THE SCENARIO:
Railway and Road Infrastructural Inspections

- ➢ Crack detection and inspection
- ➢ Rut and pothole detection
- ➢ Delamination detection
- ➢ Sight distance, slope, grade, and contours
- ➢ Ancillary and Support installations associated with railways and roads (water pipelines, electrical infrastructure, etc.

3.3.7.2 UAS/RPAS Monitoring of Railway and Road Assets Operational Scenarios

A) SCENARIO: A small Fixed Wing Hybrid UAS/RPAS of the HELMET Support Services Network (which includes the PIT stations installed along the Railway and Road Systems) is involved in Monitoring operations of a railway line and roads in the following missions:

a) Accident/Incident Occurrence;
b) Situational Awareness,
c) Difficult Terrain, Safety, or Manoeuvrability,
d) Natural Disaster Event;
e) Fatal Crash Scene Mapping

Under the conditions UTM airspace of open sky or restricted or urban/local environmental operational conditions. The UAS/RPAS is mainly equipped with a Video HD sensor performing the above operations (missions) in scheduled and/or non-scheduled flight planning (due to the nature of the operation of some sub-scenarios which evolve in a dynamic and non-foreseen ways) and transmitting in real-time and/or near-real-time the recorded events to the appropriate actors for action and/or information. The UAS/RPAS involved can be fully supported by the PIT Stations distributed in strategic locations within the HELMET Network service areas. This UAS/RPAS has a fail-safe flight mode capabilities, it will fly almost always at a BVLOS mode patrolling a big area within the railway and road assets perimeter (sometimes at 20-30km distance from base) and they have an approved flight plan by the local UTM and they aren't to exceed 120m altitude AGL during flight operations within the established geo-fencing restrictions.

B) SCENARIO FLIGHT PHASES, MISSION ENDURANCE AND RANGE: The Scenario Flight Phases for all UAS/RPAS involved are Pre-Flight, Take-off, Arrival to the mission area, Performance of the Planned Aerial Work and Return to Base (Landing), Post-Flight Operations. UAS/RPAS will have a complex flight trajectory composed of straight flight, loitering and hovering periods around the target area at altitudes that can vary from 10 to 120m. All operational steps described in section 3.3.4 are applicable. Taking into account of the single UAS/RPAS involved in the above missions performance capabilities the mean endurance will be 120min (without PIT Station Support) while the range will be variable from up to 30km.

C) UAS/RPAS MONITORING OPERATIONS GNSS REQUIREMENTS (see Table 18)

Table 18. Requirements for GNSS from viewpoint of UAS/RPAS monitoring operations

INSPECTION MISSION (RAIL/AUTOMOTIVE)	HORIZONTAL ACCURACY	VERTICAL ACCURACY	INTEGRITY	TIME-TO-ALERT	CONTINUITY	AVAILABILITY
Position/Navigation	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

D) U-SPACE SERVICES:

1) U1: Pre-tactical Geofencing;
2) U2: Strategic Deconfliction; Flight Planning Management, Weather Information

E) ACTORS INVOLVED:
1) UTM Controller
2) UAS/RPAS Pilot, Aerial Services Management and Flight Line Support Personnel
3) HELMET Service Provider
5) Rail, Road and Highway Assets Management

F) OTHER APPLICATIONS FEASIBLE UNDER THE SCENARIO:

- Visual location of victims on the accident scene
- Aerial damage assessment
- UA/RPA resource (food/water) delivery
- Medical first aid kit delivery
- UA/RPA with LiDAR damage monitoring and assessment
- Monitoring Natural Disaster

3.3.7.3 UAS/RPAS Traffic Management of Railway and Road Operational Scenario

The UAS/RPAS Traffic Management of Railway and Road Operational Scenario is a subset of the Monitoring Operations. However, Traffic Management has some peculiarities within the Monitoring task and thus will be assessed separately.

A) SCENARIO: A small Fixed Wing Hybrid or a Multi-Rotor UAS/RPAS of the HELMET shall Support Services Network (which includes the PIT stations installed along the Railway and Road Systems) involved in Traffic Management operations mainly for roads for the following specific missions:

1) Live traffic monitoring and control
2) Work zone management
3) Traffic data collection
4) Incident management at real time
5) Real-time traffic impact assessment
6) Monitoring congestion of roadways
7) Monitoring activities at traffic intersections
8) Assessment of traffic patterns
9) Crash investigation
10) Forensic mapping
11) Support Intelligent Transportation
12) System (ITS) application of highway and transportation infrastructure monitoring
13) Urban highway traffic monitoring
14) Level of Service (LOS) determination
15) Estimation of average annual daily travel
16) Measuring origin-destination flows
17) Traffic-related pollution monitoring

Under the conditions UTM airspace of open sky or restricted or urban/local environmental operational conditions. The UAS/RPAS is mainly equipped with a Video HD sensor or LIDAR performing the above operations (missions) in scheduled and/or non-scheduled flight planning (due to the nature of the operation of some sub-scenarios which evolve in a dynamic and non foreseen ways) and transmitting in real-time and/or near-real-time the recorded events to the appropriate actors for action and/or information. The UAS/RPAS involved can be fully supported by the PIT Stations distributed in strategic locations within the HELMET Network service areas. This UAS/RPAS has a fail-safe flight mode capabilities, it will fly almost always at a EVLOS and BVLOS modes patrolling a big area within mainly the road assets perimeter (sometimes at 20-30km distance from base) and they have an approved flight plan by the local UTM and they aren't to exceed 120m altitude AGL during flight operations within the established geo-fencing restrictions.

B) SCENARIO FLIGHT PHASES, MISSION ENDURANCE AND RANGE: The Scenario Flight Phases for all UAS/RPAS involved are Pre-Flight, Take-off, Arrival to the mission area, Performance of the Planned Aerial Work and Return to Base (Landing), Post-Flight Operations. UAS/RPAS will have a complex flight trajectory composed of straight flight, loitering and hovering periods around the target area at altitudes that can vary from 30 to 120m. All operational steps described in section 3.3.4 are applicable. Taking into account of the single UAS/RPAS involved in the above missions performance capabilities the mean endurance will be 120min (without PIT Station Support) while the range will be variable from up to 30km.

C) UAS/RPAS TRAFFIC MANAGEMENT OPERATIONS GNSS REQUIREMENTS (see Table 19)

Table 19. Requirements for GNSS from viewpoint of UAS/RPAS traffic management operations

TRAFFIC MANAGEMENT (RAIL/AUTOMOTIVE)	ACCURACY HORIZONTAL	ACCURACY VERTICAL	INTEGRITY	TIME-TO-ALERT	CONTINUITY	AVAILABILITY
Position/Navigation	10m / 30m	10m / 30m	1 – 2× 10–7	1s (HOT)-10 s(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

D) U-SPACE SERVICES:

1) U1: Pre-tactical Geofencing;
2) U2: Strategic Deconfliction; Flight Planning Management, Weather Information

E) ACTORS INVOLVED:

1) UTM Controller
2) UAS/RPAS Pilot, Aerial Services Management and Flight Line Support Personnel
3) HELMET Service Provider
5) Rail, Road and Highway Assets Management

4. SUMMARY OF HIGH-LEVEL USER REQUIREMENTS FOR HELMET

The summary of fundamental high-level user requirements related to HELMET solutions intended for multi-modal transportation is shown in Table 20 and Table 21, while Table 22 provides a summary of user requirements for UAS/RPAS as a segment and as support to railway and automotive safety applications.

Table 20. Summary of high-level user requirements for HELMET

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**

RAIL	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**
	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]):

User requirements for safety integrity of most demanding railway safety critical applications (i.e. Track identification, Odometry calibration, Cold movement detection) are sometimes expressed by Alert Limit of 7*sigma, where Gaussian position error is assumed. The corresponding Tolerable Hazard Rate / Probability of Failure (PF) can be estimated using MatLab cumulative distribution function normcdf as

PF = 2* (1 - P) =2* (1 - normcdf(7,0,1)) = 2.559730205575761e-12

It is evident that achievement of such very low probability is only valid under ideal normal error distribution. In practice, a correlation among subsequent GNSS samples exists and the error distribution is not perfectly Gaussian. It would not be easy to justify the above assumptions for AL of 7* sigma. Especially in tails of the Gaussian distribution. Moreover, it is not allowed to build a safety function compliant with SIL 3 and SIL 4 as a single function (EN 50129). A combination of diverse techniques must be used to exclude common causes of hazards. Fail-safety principle (e.g. composite fail-safety) must be used. It is the reason why it is assumed in Table 20, that composite fail-safety is applied and therefore less demanding requirements for Alert Limit and sigma are needed, i.e. AL ~ 5* sigma in case of composite fail-safety, instead of AL ~ 7* sigma .

Note [2]):

It is considered that car position in longitudinal direction could be determined by means of GNSS technology and in lateral by means of other techniques, such as computer vision, etc. It would reduce demanding requirements for GNSS.

Table 21 shows high level requirements for speed accuracy related to rail and automotive applications.

Table 21. Summary of high-level user requirements for HELMET (speed accuracy)

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**

It is evident from Table 20 that the most demanding user requirements regarding high-accuracy and high-safety integrity position determination are imposed by the road sector for automated car driving, where about 1 dm accuracy (2*sigma) and ASIL D for the position determination solution is necessary.

High availability is required because it has direct impact on car occupant's safety.

High security should be guaranteed as well, since preservation of functional safety (RAMS) and data confidentiality is required critical.

Table 22. Summary of High-Level UAS/RPAS Requirements for HELMET

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)-10 s(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**

5. HIGH-LEVEL SAFETY CONCEPTS

This section briefly summarises fundamental safety concepts, which will be used for safe architecture development and also for specification of system safety requirements. Land safety systems can be classified into two categories:

- fail-operational and
- fail-safe.

Fail-operational (or fault-tolerant) system requires except normal system state also functioning in degraded situations when some system parts are not working properly – 'rather some (incomplete) data than none'. Safety instrumented systems such as refineries, chemical processes, nuclear plants, etc. belong to this category. Immediate uncontrolled stopping could be dangerous. Safety is mainly maintained via high reliability and availability. It is also the case of airplane or ship controller. Fail-safe (fail-stop, fail-silent) system can be immediately brought into a predefined fail-safe state in case of failure – 'rather stop than fail'.

Safety-related systems such as railway signalling, machine control, etc. belong to this category. System with a fail-safe state is not operational (available) in case of dangerous failure, but it is acceptable for rare events.

It is evident that a fail-safe sate in process industry, i.e. spurious (false) trip has a different meaning than a fail-safe sate in safety-related systems (EN 61508; 2011). These safety concepts directly influence performance of multi-channel safety structures.

5.1 RAIL: RAILWAY SAFETY

5.1.1 Worst case approach

Railway traditionally belongs to very safe transportation systems. From the very beginning railway safety is based on conservative principles and worst-case approach. The worst-case approach takes into account many scenarios/ assumptions that are unlikely to occur simultaneously. One of them is e.g. brick-wall stop approach, which means that the minimum headway should be at least two stopping distances.

5.1.2 Fail-safe technique

Excepting the worst-case approach, the restrictive fail-safe technique has been also introduced to railway safety systems early at beginning of railway age. Fail-safety is the fundamental feature of railway signalling. It says that safety must be maintained in case of dangerous signalling system failure. As an example can mentioned a fail-safe train air brake invented by George Westinghouse in 1869 or a track circuit patented by its inventor William Robinson in 1872. Train brakes need energy to be released. If power supply (air pipe-line) is interrupted, brakes are activated. The track circuit is designed to indicate the presence of train also when failure occur. The fail-safe approach had been adopted by railways even before the first airplane took off (1903).

Train control systems are not generally designed to protect against all very rare hazardous events, e.g. fall of tree/ rock on rail, etc. – but they must be mitigated through other operational procedures. It means that suitable operational procedures can be used for reduction of sometimes very demanding initial safety requirements to make them more realistic.

5.1.3 Railway safety pillars

Safety of signalling is based on three main pillars:

- Functional safety – i.e. reliability of each safety function designed to mitigate a specific hazard.
- Technical safety – i.e. safe operation in case of dangerous failure. Each failure must be promptly enough detected and negated.
- High dependability – i.e. reliability and availability, because occasional irregularities in train operations due to degraded operational mode of signalling system with participation of a human factor may indirectly jeopardize railway safety.

5.1.4 Safety integrity concept

Railway safety integrity concept is related to the quality of system safety functions from the viewpoint of protection against dangerous faults and failures. The quality represents safeguards against:

- Hardware failures via HW safety integrity and
- Systematic faults via systematic safety integrity.

The safeguard against HW (random) failures is quantitatively achieved via tolerable hazard rate (THR). The safeguard against systematic faults means a safe function design, which is qualitatively achieved via an attribute called the Safety Integrity Level (SIL) and related guidelines.
Since the occurrence of deterministic systematic events cannot be quantified, a SIL table describing relation between SIL (1-4) and THR can be used. It is assumed that the systematic hazard cause may occur with a priory probability Pr = 1 (according to worst-case approach). SIL is identified from THR for a given safety function. SIL also indicates according to SIL table the THR interval for the systematic safety integrity for a given safety function.

5.1.5 Railway technical safety principles

Railway safety related systems to be compliant with SIL 3 or SIL 4 must ensure that they will remain safe in the event of any kind of single random HW fault. This principle is known as fail-safety and can be achieved by means of the following techniques – see Fig. 35:

- Inherent fail-safety,
- Composite fail-safety, or
- Reactive fail-safety.

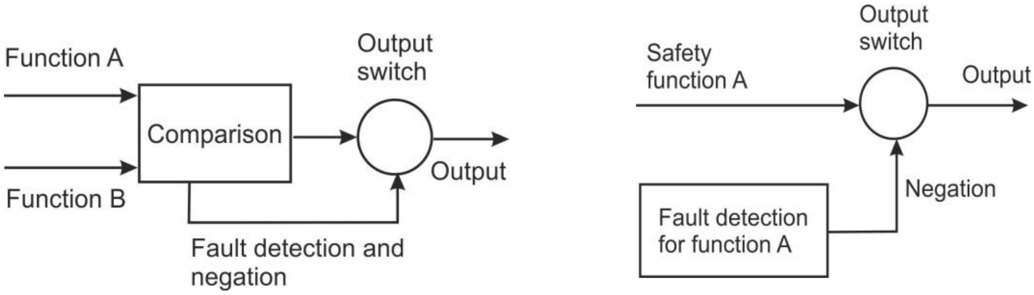


Figure 35. Fail-safe techniques according to CENELEC: (a) composite fail-safety, and (b) reactive fail-safety.

It is evident that implementation of these techniques not only determines which level of LDS safety will be achieved, but also how efficiently GNSS will be used within the LDS.

Inherent fail-safety allows a safety-related function to be performed by a single channel, provided that all the credible failure modes of the channel are not hazardous. It would be very difficult or impossible to make such evidence in case of complex GBAS or SBAS and therefore inherent fail-safety is not further considered for GNSS-based LDS.

Composite fail-safety allows a safety-related function to be performed by at least two independent channels. Hazardous fault in one channel shall be detected and negated sufficiently quickly to meet the required THR. The fault is detected by the comparison of the output values of these two or more channels, or also by means of an additional independent diagnosis. This technique could be used e.g. for improvement of GNSS safety integrity at dual/constellation LDS solution. However, very detailed Common Cause Failure/ Common Mode Failure (CCF/CMF) analysis should be performed to demonstrate SIL 4.

Finally, reactive fail-safety allows a safety-related function to be performed by a single channel, provided its safe operation is assured by fast detection and negation of any dangerous fault. This technique could be used for increase of THR requirement for GNSS. For example the current EGNOS SoL service could be used for virtual balise detection in combination with existing track circuits/ axle counters, ARAIM and safe ETCS odometry. The initial train position could be determined with the aid of track-side equipment to achieve the required THR < 1e-9/ 1 hr and the fast diagnosis would be performed using safe odometry and other techniques.

5.1.6 Common Safety Methods: EC regulation 402/2013

Each intended change in railway signalling represents a risk, which could threaten safety. In 2009 a new regulation regarding Safety Management has been implemented by the European Commission and European Union Agency for Railways (ERA) to harmonise risk assessment process for the European railway industry. This new approach is called Common Safety Method for Risk Evaluation and Assessment (CSM-RA). The CSM-RA approach is described in the revised Commission Regulation (EU) 402/2013 – see [8]. The CSM-RA shall be applied to any change (technical, operational organisational) in the railway system. The purpose of the CSM-RA is to maintain and improve the level of safety. A significant change becomes fundamental background for risk assessment process. If the change in signalling system is significant, then the proposer has to evaluate the associated risk according to the six criteria:

- Failure consequence: credible worst-case scenario;
- Novelty: innovative or new to organization;
- Complexity: the complexity of the change;
- Monitoring: the inability to monitor & intervene appropriately;
- Reversibility: the inability to revert to the original system;
- Additionality: to account for the sum of lots of minor changes.

The safety analysis must consider worst cases, not just the likely or expected case. The credible worst-case scenario in the event of failure of the system under assessment has also to take into account the existence of safety barriers outside the system.

The worst-case scenario is asking the question "What is the worst that could happen if the system behaves in an undesirable way following the introduction of the proposed change?" The CSM-RA should be evidently applied in case of GNSS employment for ERTMS/ETCS. It seems CSM-RA based on long-term experience has also large application potential in automotive safety systems.

5.2 AUTO: FAIL-SAFE VS. FAIL-OPERATIONAL AND FAULT-TOLERANT PRINCIPLES

5.2.1 Basic differences between ISO 26262 and IEC 61508/ EN 5012x

Automotive functional safety standard ISO 26262 and railway CENELEC safety standards and EN 5012x results from the same (mother) functional safety standard IEC 61508.

The standard IEC 61508 applies to safety-related systems that incorporate electrical and/or electronic and/or programmable electronic (E/E/PE) devices. The standard specifically covers hazards that occur when safety functions fail. The main goal of the safety standard is to reduce the risk of failure to a tolerable level. IEC 61508 is built on two fundamental pillars: 1) the safety life-cycle intended to reduce or eliminate failures due to systematic faults and 2) the safety integrity levels (SILs) to address random failures. The safety life cycle is defined as a process that includes all necessary steps to achieve the required functional safety. It is also called Functional Safety Management.

A safety integrity level is one of four levels (i.e. SIL 1, 2, 3 and 4), each corresponding to a range of target likelihood of failures of a safety function. SIL is a measure of performance of a safety function, which is designed as a safety guard (safety provision) against the specific hazard. SIL 4 is used to protect users against the highest risks. SIL is determined by the average probability of failure per 1 hour (PFH) for systems working in continuous or high demand mode of operation – i.e. also computer-based railway signalling systems. Note that a SIL is a property of a safety function rather than of a system or its part.

There are two basic differences between the IEC 61508 and ISO 26262 standards, which should be considered from viewpoint of safety management. First, IEC 61508 Safety Integrity (measured by SIL and PFH) was replaced with a qualitative attribute called Robustness, which is measured by the Automotive Safety Integrity Level (ASIL). Second, the ISO 26262 and IEC 61508 life-cycles are not fully identical because a system designed according to IEC 61508 / EN 50129 is installed first and then it is validated during operations, while a system designed according to ISO 26262 is validated and manufactured afterwards. The second differentiator is not applicable to the HELMET solution.

5.2.2 Fail-operational and fail-tolerant techniques

In case of automated car driving a critical parameter from viewpoint of safety also becomes reliability and availability. It has been already said above that high railway safety directly depends on high functional and technical safety, and indirectly on high dependability as well. It is because unreliable systems could cause interruptions of operations, which could finally impact safety in a degraded mode of operation due to engagement of unreliable human operator. Further, high system dependability is also required since is an important economical factor. The relation between safety and availability is depicted in Fig. 36.

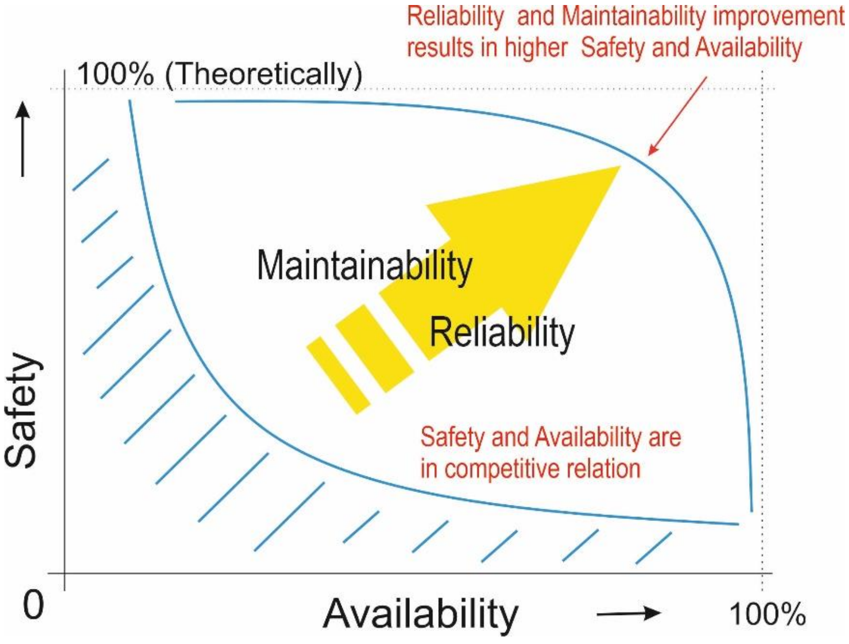


Figure 36. Relation between safety and availability – parameters are reliability and maintainability

In case of self-driving cars, the application of fail-safe (fail-stop) techniques could be very dangerous in some situations, especially when it is necessary to safely finish critical operations such as car overtaking or lane changing on a highway with busy traffic, etc. Interruption of such operations could have fatal consequences. Therefore, dependability and especially high system reliability and availability becomes a critical safety attribute for automated car driving. Automated car driving system become in fact a safety-critical system, which are also used in aviation or process industry (refineries, etc.). Safety-critical systems do not have defined a fail-safe state, because such systems must safely finish the process. The process interruption could be dangerous. Thus, high safety (of safety-critical systems) is achieved through high availability. It is necessary to distinguish such systems from so called safety-related systems, which have defined a fail-safe state (vehicle or electric saw stops). So high safety and also high dependability is generally achieved by fail-operational and fail-tolerant systems.

Fault-tolerance defined according to ISO 26262 is the ability to deliver specified functionality in the presence of one or more specified faults. Fail-operational means that a system continues to operate in case of a single failure in the control system – see Fig. 37. In other words, fault-tolerance or fail-operation is the property that enables a system to continue operating properly in the event of failure of some of its components.

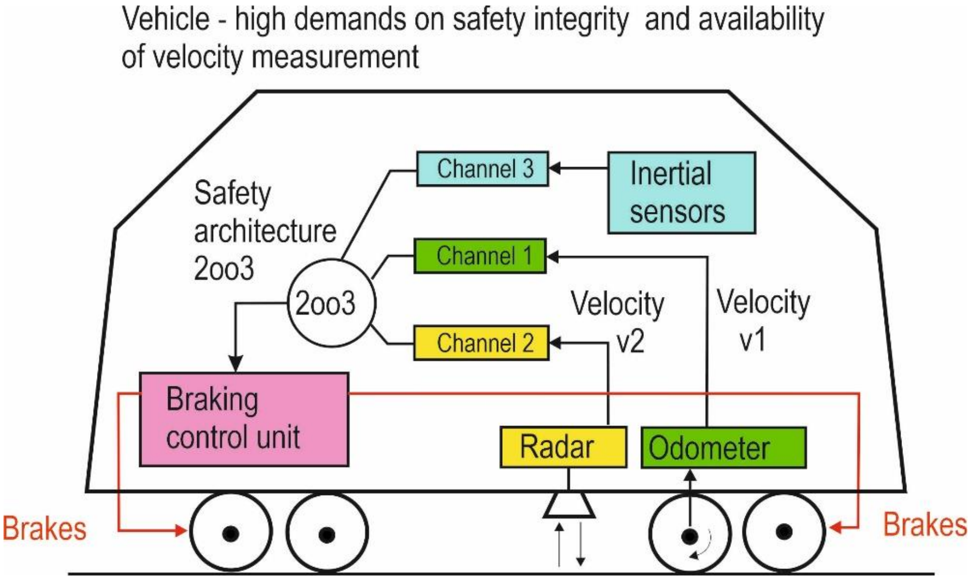
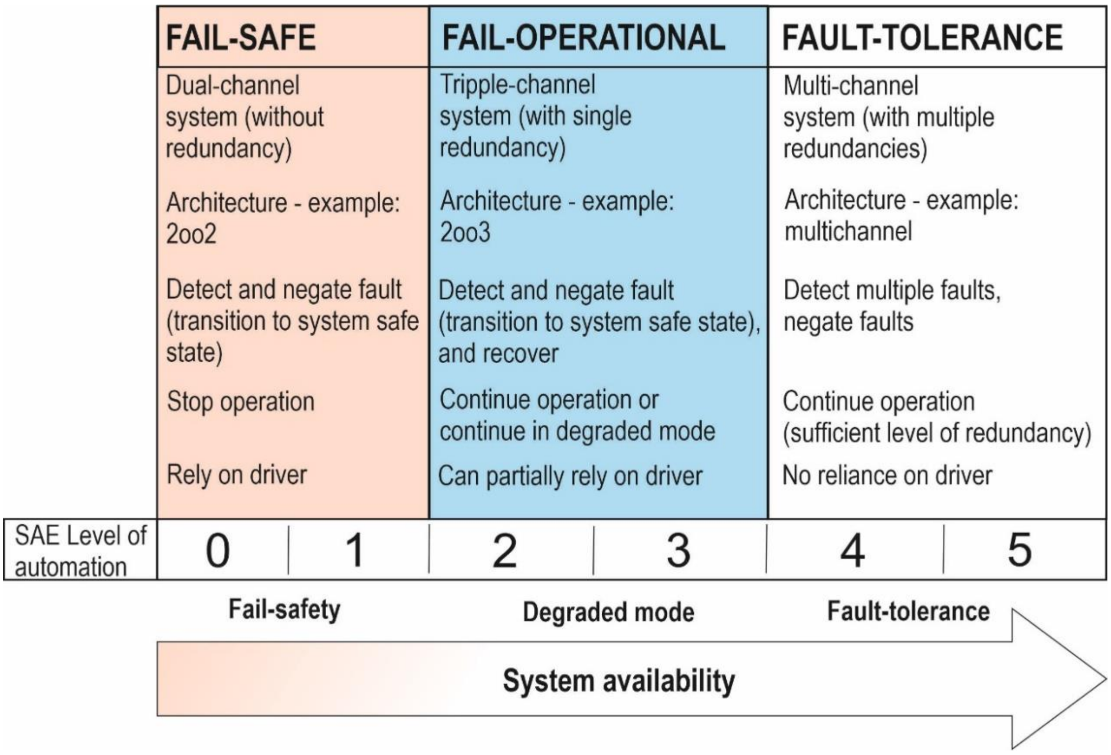


Figure 37. Example of fail-operational system for safe and dependable speed measurement

A comparison of safety techniques used for automated car driving with respect to the SAE automation levels is outlined in Table 23.

Table 23. Characteristic features of safety techniques applicable to automated car driving



	FAIL-SAFE	FAIL-OPERATIONAL	FAULT-TOLERANCE
	Dual-channel system (without redundancy)	Tripple-channel system (with single redundancy)	Multi-channel system (with multiple redundancies)
	Architecture - example: 2oo2	Architecture - example: 2oo3	Architecture - example: multichannel
	Detect and negate fault (transition to system safe state)	Detect and negate fault (transition to system safe state), and recover	Detect multiple faults, negate faults
	Stop operation	Continue operation or continue in degraded mode	Continue operation (sufficient level of redundancy)
	Rely on driver	Can partially rely on driver	No reliance on driver
SAE Level of automation	0 1	2 3	4 5

Fail-safety

Degraded mode

Fault-tolerance

System availability

5.3 UAV: HIGH LEVEL SAFETY CONCEPTS FOR UAS/UAS/RPAS-PIT STATION

5.3.1 General

For the purposes of this Project the High Level Safety Concept and Procedures to be applied shall be mainly those of ICAO Doc 9859 AN/474 “Safety Management Manual (SMM)” for manned civil aviation operations which are also applicable to a degree to UAS/RPAS and on specific and/or peculiar to UAS/RPAS issues those of JARUS (Joint Authorities for Rulemaking of Unmanned Systems) “Working Group 6 – Safety & Risk Assessment AMC UAS/RPAS.1309, Issue 2 Safety Assessment of Remotely Piloted Aircraft Systems which shall apply only to HELMET UAS/UAS/RPAS-PIT Station to “Specific” depending on the type of operations and the nature of the risks involved and all “Certified” Category operations.

In addition, the general public’s acceptance (societal acceptance) of civil UAS/RPAS in terms of safety is the subject to many and varying factors including; safety, noise, intrusion/privacy, etc. This type of safety issue is treated in section 2.3.1 of this document while herein the focus is placed on the design and airworthiness aspects of safety.

5.3.2 The Concept of Safety in Aviation: Background and Impact on UAS/RPAS

Depending on the perspective, the concept of safety in aviation may have different connotations, such as:

a) zero accidents or serious incidents
b) freedom from hazards, i.e. those factors which cause or are likely to cause harm;
c) attitudes of employees of aviation organizations towards unsafe acts and conditions;
d) error avoidance; and
e) regulatory compliance.

Whatever the connotation, they all have one underlying commonality: the possibility of absolute control. Zero accidents, freedom from hazards, and so forth, convey the idea that it would be possible (by design or intervention) to bring under control, in aviation operational contexts, all variables that can precipitate bad or damaging outcomes. However, while the elimination of accidents and/or serious incidents and the achievement of absolute control is certainly desirable, they are unachievable goals in open and dynamic operational contexts. Hazards are integral components of aviation operational contexts. Failures and operational errors will occur in aviation, in spite of the best and most accomplished efforts to prevent them. No human activity or human-made system can be guaranteed to be absolutely free from hazards and operational errors. Safety is therefore a concept that must encompass relatives rather than absolutes, whereby safety risks arising from the consequences of hazards in operational contexts must be acceptable in an inherently safe system. The key issue still resides in control, but relative rather than absolute control. As long as safety risks and operational errors are kept under a reasonable degree of control, a system as open and dynamic as commercial civil aviation is considered to be safe. In other words, safety risks and operational errors that are controlled to a reasonable degree are acceptable in an inherently safe system.

Conventional manned aircraft system safety assessment and criteria, referred to as the ‘1309’ criteria, is a general airworthiness requirement used for the certification of aircraft, and aims to ensure that an aircraft is capable of continued safe flight and landing following a failure or multiple failures of systems. The methodologies applied and resulting analysis focus both on the protection of people on-board aircraft and third party risks to people and property on the ground; third party protection being by virtue of maintaining continued safe flight and landing of the aircraft.

With the introduction of UAS/RPAS and the absence of a pilot on-board, the safety analysis has to be adapted to focus on the specific characteristics of UAS/RPAS. For example, in manned aviation, application of a safety analysis (1309) to aircraft systems considers the presence of the flight crew as a means of mitigation in order to manage system failures. Depending on the complexity of the UAS/RPAS and its reliance on automatic functions, the on-board systems may now undertake a larger proportion of what were traditionally flight crew functions, including automatic decision making. Even on relatively simple UAS/RPAS, reliance on the remote crew to manage failures may no longer be realistic (e.g. following failure of the command & control link). It is therefore expected that even in a relatively small and simple UAS/RPAS, some functions may require a complex flight management system to gain type-certification.

The UAS/RPAS is called to provide fault management capabilities equivalent to that of a manned aircraft. UAS/RPAS have some advantages in this regard e.g. may not be susceptible to disorientation, be predictable, provide a more rapid response, and could continuously monitor flight and system parameters etc. However, they may also be subject to some limitations e.g. still susceptible to errors (from the control station, programming, interference, etc.), and may not have a human's capability to adapt to unusual situations as it will be reliant on programmed scenarios. It is also likely that an UAS/RPAS may lack situational awareness due to the limited sensors available to fully replicate those of an onboard pilot's sensory perception – e.g. sight, smell, feel and hearing.

5.3.3 The UAS/RPAS Safety Process Logic Overview

In its essence, the UAS/RPAS Safety Process shall mainly follow the Manned Aviation Procedures and Requirements whatever is the method of Safety Risk Analysis and Assessment such as the JARUS SORA for the "specific" UAS category, and as such it shall consist of eight (8) elements as per Fig. 38 below which depicts the typical logic sequence of the process which may also require iteration between steps.

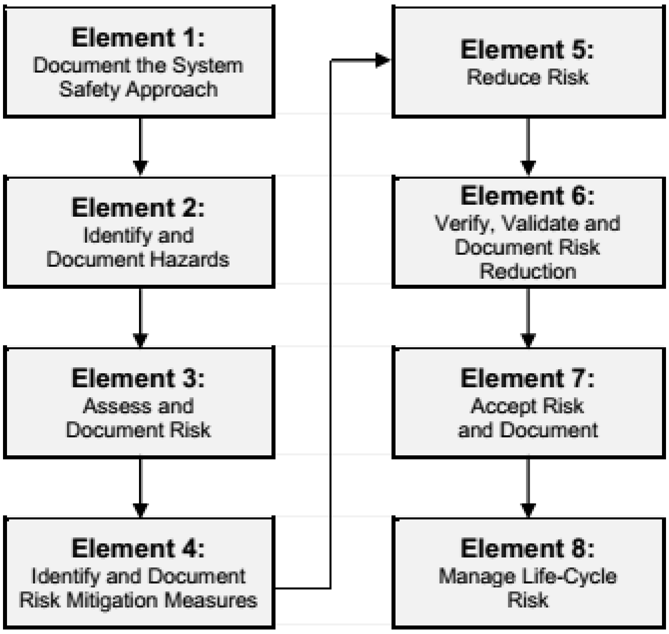


Figure 38. Eight Elements of the Aviation System Safety Process

5.3.4 Failure Condition Classification

The familiar failure condition classifications (Catastrophic, Hazardous, Major, Minor and No safety effect) have been retained from manned aviation requirements. The classification of a failure condition does not depend on whether a system or function is required by specific regulation. Some systems required by regulation, such as position lights and transponders, may have the potential for only minor failure conditions. Conversely, other systems not required by any specific regulation, such as automatic take-off and landing systems may have the potential for Catastrophic failure conditions. Failure Conditions for UAS/RPAS are classified according to the severity of their effects as follows:

1) No Safety Effect: Failure conditions that would have no effect on safety. For example, failure conditions that would not affect the operational capability of the UAS/RPAS or increase remote crew workload.
2) Minor**:** Failure conditions that would not significantly reduce UAS/RPAS safety and that involve remote pilot actions that are within their capabilities. Minor failure conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in remote crew workload, such as flight plan changes.
3) Major**:** Failure conditions that would reduce the capability of the UAS/RPAS or the ability of the remote pilot to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins, functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote pilot efficiency.
4) Hazardous**:** Failure conditions that would reduce the capability of the UAS/RPAS or the ability of the remote pilot to cope with adverse operating conditions to the extent that there would be the following:
   a) Loss of the UA/RPA where it can be reasonably expected that a fatality will not occur, or
   b) A large reduction in safety margins or functional capabilities, or
   c) High workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely.

5) Catastrophic**:** Failure conditions that could result in one or more fatalities.

An inverse relationship must exist between the average probability per flight hour of a failure condition occurring and its likely consequence, such that;

1) Failure Conditions with No safety Effect have no probability requirement.
2) Minor Failure Conditions may be Probable.
3) Major Failure Conditions must be no more frequent than Remote.
4) Hazardous Failure Conditions must be no more frequent than Extremely Remote.
5) Catastrophic Failure Conditions must be Extremely Improbable.

It is foreseen that as part of the tailoring process required to turn a manned airworthiness code into one applicable to UAS/RPAS, existing CS/FAR xx.1309 will require the need for a Special Condition to be raised to reflect the novel features of UAS/RPAS and to capture the specific certification needs that would be applied to UAS/RPAS equipment, systems and installations.

Whilst this AMC details "what needs to be addressed, the development of the safety assessment process and material providing guidance on "how to" comply with this Special Condition has not been fully completed in this issue of this document. This will be further developed after confirmation that the approach adopted is acceptable. One source of "how-to" guidance is published in ARP 4754A/ED-79A. This might form the basis of material to be developed.

For some simple UAS/RPAS, a qualitative analysis might be acceptable provided that current commonly accepted industry practices are adopted. Salient points to note in the definitions and example failure condition classifications are given below.

Note: These examples are for illustrative purposes only and may vary depending on the individual UAS/RPAS design. An applicant will need to establish the failure classification on a case-by-case basis as part of a functional hazard assessment.

1) No Safety Effect: A 'No safety Effect' might be used for a payload system failure condition that has no effect on the airworthiness of the UAS/RPAS.
2) Minor: Examples of 'a slight reduction in safety margins or functional capabilities' might include: a Loss of a single redundancy in a multi-redundant system.
3) Major: Possible examples of '*a significant reduction in safety margins or functional capabilities*' might include: Total loss of communications with UTM/ATC.
4) Hazardous: Possible examples of '*a large reduction in safety margins or functional capabilities*' might include:
   a) Potential loss of safe separation (e.g. loss of DAA, incorrect altitude reporting);
   b) Activation of an emergency recovery capability potentially resulting in loss of the UAS/RPAS where a fatality is not expected to occur.
5) Catastrophic: This refers to one or more fatalities that can occur either in the air (mid-air collision) or on the ground. Where type-certification does not stipulate any limitations on type of airspace to be used and areas to be overflown, the design assumption must be that any failure condition leading to a rash, mid-air collision or forced landing, is potentially fatal. Examples of potentially Catastrophic failure conditions include:
   a) Loss of control over a populated area leading to impact with the surface outside of an approved safe area;
   b) Loss of control leading to the inability of a RPA to be contained within a pre-defined segregated area;
   c) Malfunction of a DAA system that actively guides the RPA towards neighbouring traffic.

An emergency recovery capability may be used as a means of mitigating Catastrophic failure conditions. Where an emergency recovery function is used as mitigation for what would otherwise be a Catastrophic failure condition, the systems and equipment that supports this functionality would be required to undergo safety analysis to ensure a level of performance acceptable to the certifying authority.

5.3.4 Overview of Hazards Identification and Assessment for UAS/RPAS Operations

The small UAS/RPAS in low-altitude UTM airspace which have been proposed for the HELMET rail and road applications a paradigm shift from single-UAS visual operations in restricted airspace to multi-UAS/RPAS beyond visual line of sight operations with increasing use of autonomous systems and operations under increasing levels of urban development and airspace usage. Ensuring the safety of UAS/RPAS IMTM operations requires an understanding of the associated current, future and combined hazards. This is challenging for UAS/RPAS operations due to insufficient mishap (accident and incident) reporting for UAS/RPAS and the rapid growth of new UAS/RPA IMTM applications (our use cases) that have not yet been implemented as provided in this CONOPS. A first set of current, future and combined identified and assessed Hazards are found in Tables 24 to 37 in this subsection. These Tables will be completed with further assessments during the HELMENT UAS/RPAS-PIT Station Preliminary Design, where is required, and then the results shall be used to develop a set of combined (current and future) hazards for assessing risks for each IMTM selected operations using the JARUS LORA Method (Refer to subsection 2.3 of this document) for the case of "Specific" UAS/RPAS Category while (if required) the possible use of "Certified" UAS/RPAS for HELMET then the Risk Assessment will follow the manned aircraft methods in accordance with the EASA regulations.

The UAS/RPAS IMTM operations for rail and road will increasingly require interactions with an array of existing and future users of the airspace – other UAS/UAS/RPAS, general aviation aircraft, helicopters, gliders, balloons, and even parachutists. However, the safety of these existing operations cannot be reduced by the introduction of the ever more or new UAS/RPAS operations. Currently, there is no automation infrastructure to accommodate the widespread use of UAS/RPAS operations in uncontrolled airspace. The EU-EASA UAS/RPAS Traffic Management (UTM) Project seeks to facilitate the safe use of low-altitude airspace (below 400 feet) by operators of small UAS/RPAS (25Kg MTOM or less) for a wide variety of applications. The UTM system will enable safe and efficient low-altitude airspace operations by providing services such as airspace design, corridors, dynamic geo-fencing, severe weather and wind avoidance, congestion management, terrain avoidance, route planning, re-routing, separation management, sequencing, spacing, and contingency management. UTM is essential to enable the accelerated development and use of civilian UAS applications. In its most mature form, the UTM system will be developed using automaticity characteristics, which will include self-configuration, self-optimization and self-protection.

Associated with the proliferation of civil applications for UAS/RPAS is a paradigm shift from single-UAS/RPAS remotely piloted within visual line of sight operations in remote locations to multi-UAS/RPAS BVLOS (beyond visual line of sight) operations with increasing use of autonomous systems and operations under increasing levels of urban development and airspace usage. Along with increasing levels of operational complexity and sophistication come increasing complexity of hazards sources and levels of safety / risk impacts. Ensuring safety can therefore be thought of as a multidimensional problem, and visualized in a 3-dimensional problem space as depicted in Fig. 39 below.

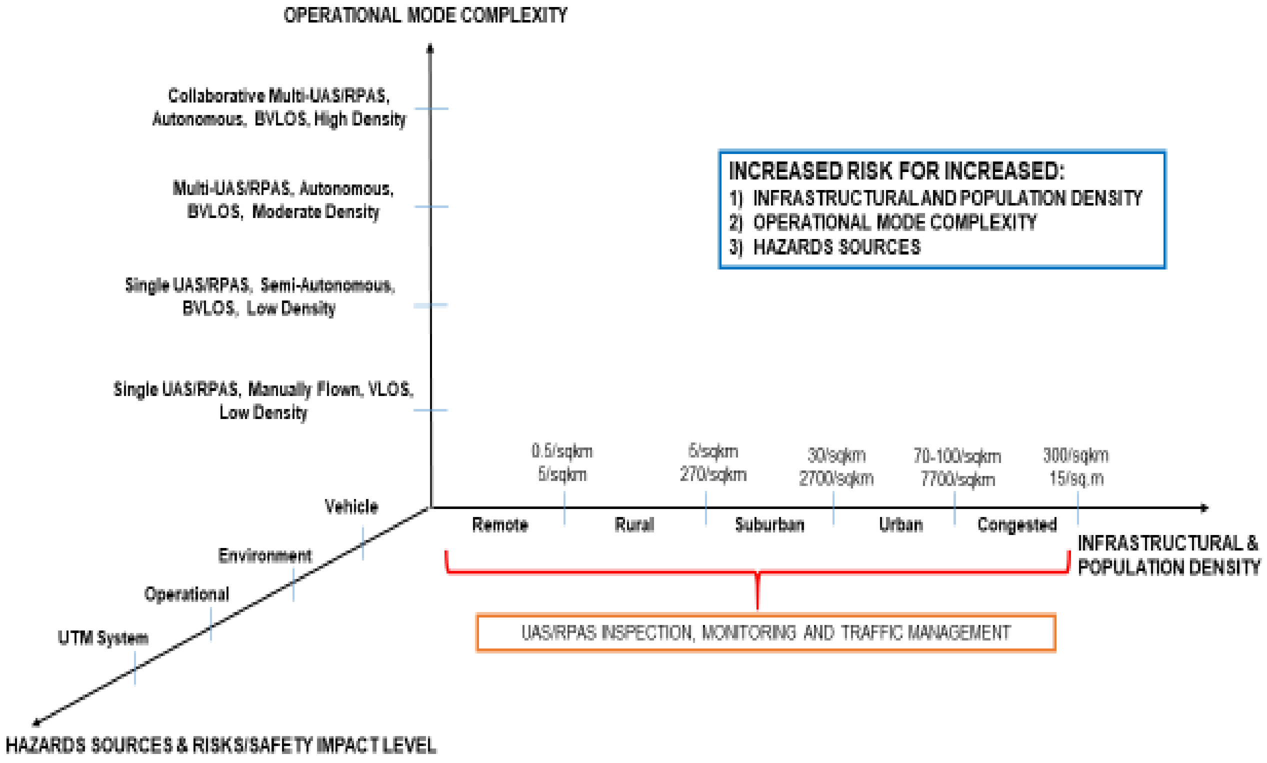
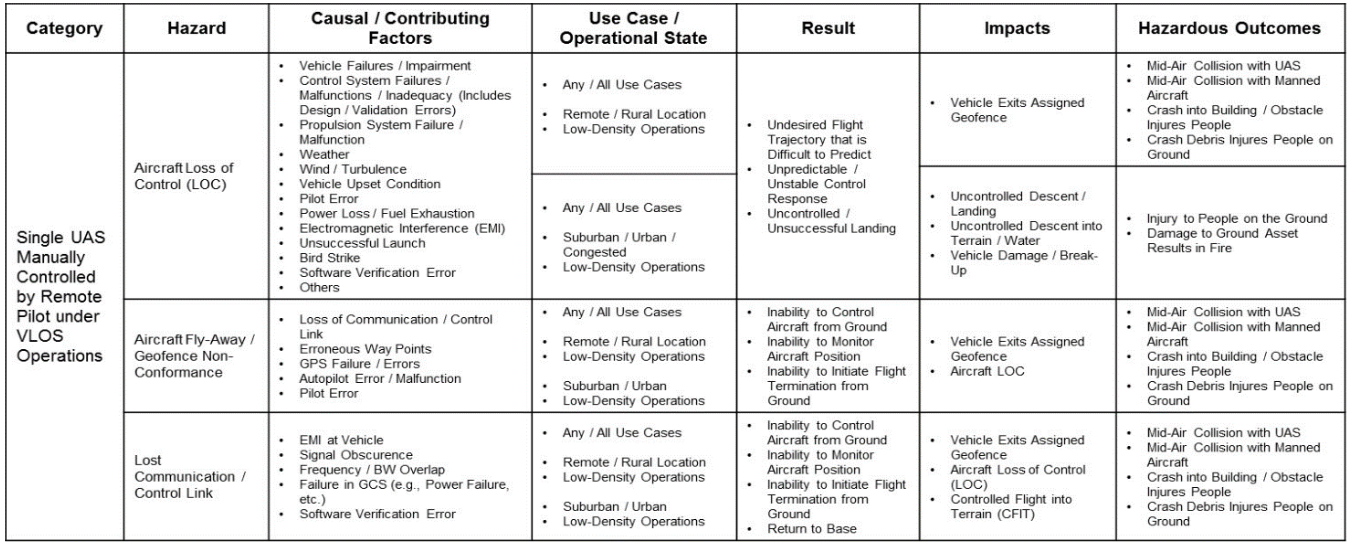
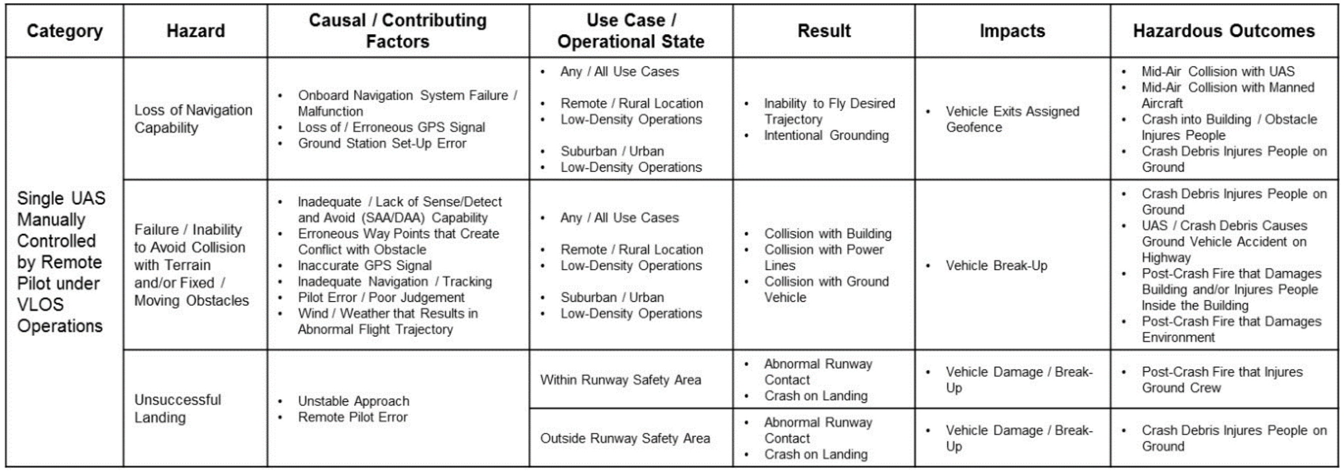

OPERATIONAL MODE COMPLEXITY
Collaborative Multi-UAS/RPAS, Autonomous, BVLOS, High Density
Multi-UAS/RPAS, Autonomous, BVLOS, Moderate Density
Single UAS/RPAS, Semi-Autonomous, BVLOS, Low Density
Single UAS/RPAS, Manually Flown, VLOS, Low Density
INCREASED RISK FOR INCREASED:
1) INFRASTRUCTURAL AND POPULATION DENSITY
2) OPERATIONAL MODE COMPLEXITY
3) HAZARDS SOURCES
0.5/sqkm 5/sqkm
5/sqkm 270/sqkm
30/sqkm 2700/sqkm
70-100/sqkm 7700/sqkm
300/sqkm 15/sq.m
Remote
Rural
Suburban
Urban
Congested
INFRASTRUCTURAL & POPULATION DENSITY
UAS/RPAS INSPECTION, MONITORING AND TRAFFIC MANAGEMENT
Vehicle
Environment
Operational
UTM System
HAZARDS SOURCES & RISKS/SAFETY IMPACT LEVEL

Figure 39. Multidimensional Problem Space for Assessing Risk and Ensuring the Safety of UAS and UTM Operations

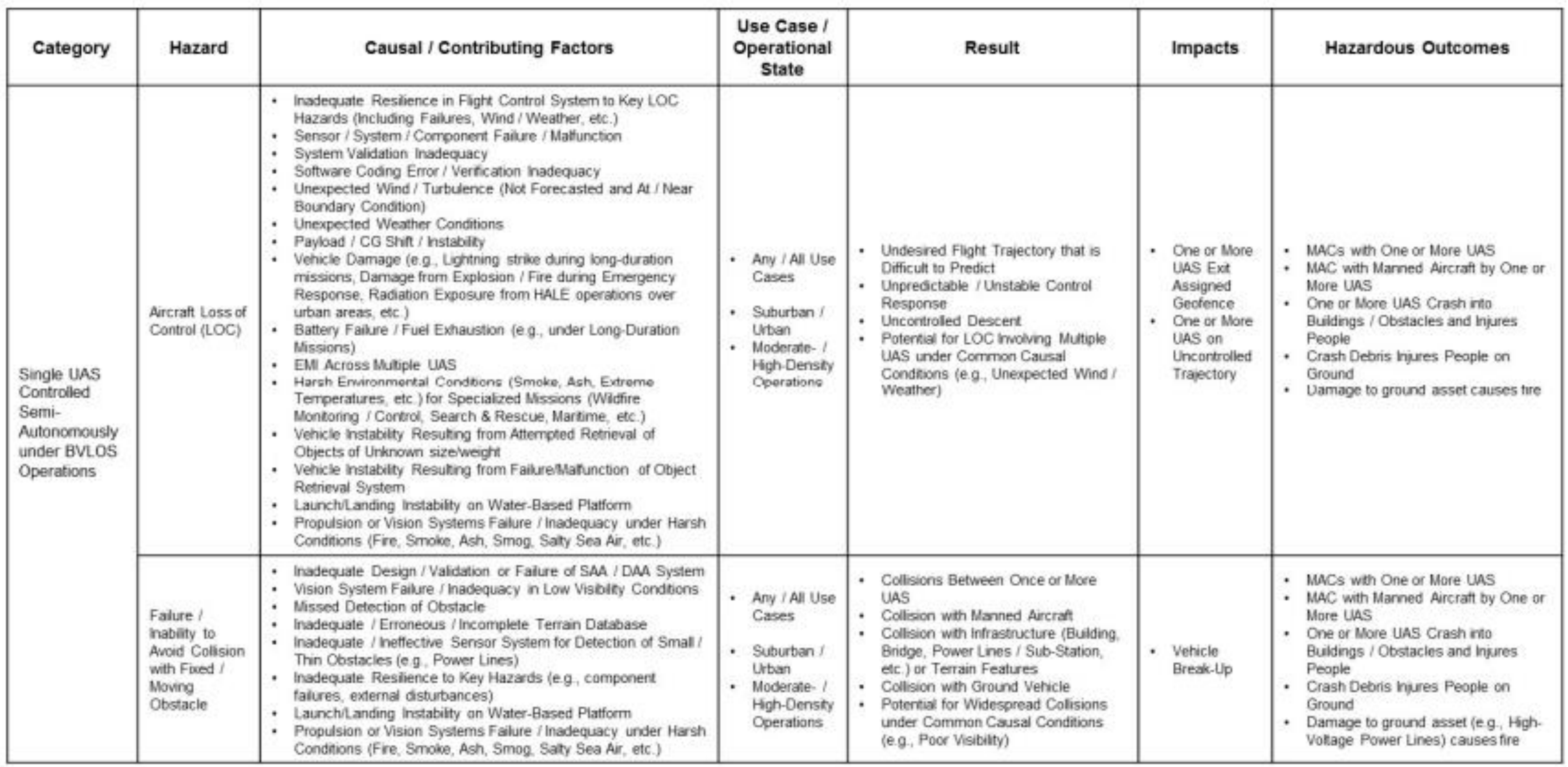
As indicated in Fig. 39 above one dimension of the safety process concept involves operational mode complexity, which increases with increasing numbers of UAS/RPAS operations by a single operator, increasing use of autonomous systems and operations, and increasing density of operations within the UTM airspace (i.e., from low to high density of operations). Another dimension of the safety problem involves the infrastructural and population density (including remote, rural, suburban, urban, and congested) of the operational environment encounter in both rail and road, and the proliferation of IMTM applications for UAS/RPAS being considered. An attempt is made in Fig. 39 at mapping the various UAS/RPAS applications (or use cases) across the operational environments envisioned. The third dimension depicted in Fig. 39 represents the hazards sources and levels of associated safety / risk impact, including but not limited to at the vehicle level, environment, operational, and the UTM system. It should be noted that hazards at one level can affect not only that level but also others along this dimension. For example, a hazard at the vehicle level can impact safety and risk at the operational level. The identification of safety hazards and associated risk is challenging for the emerging UAS/RPAS operations.

Table 24. UAS/RPAS Current Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)

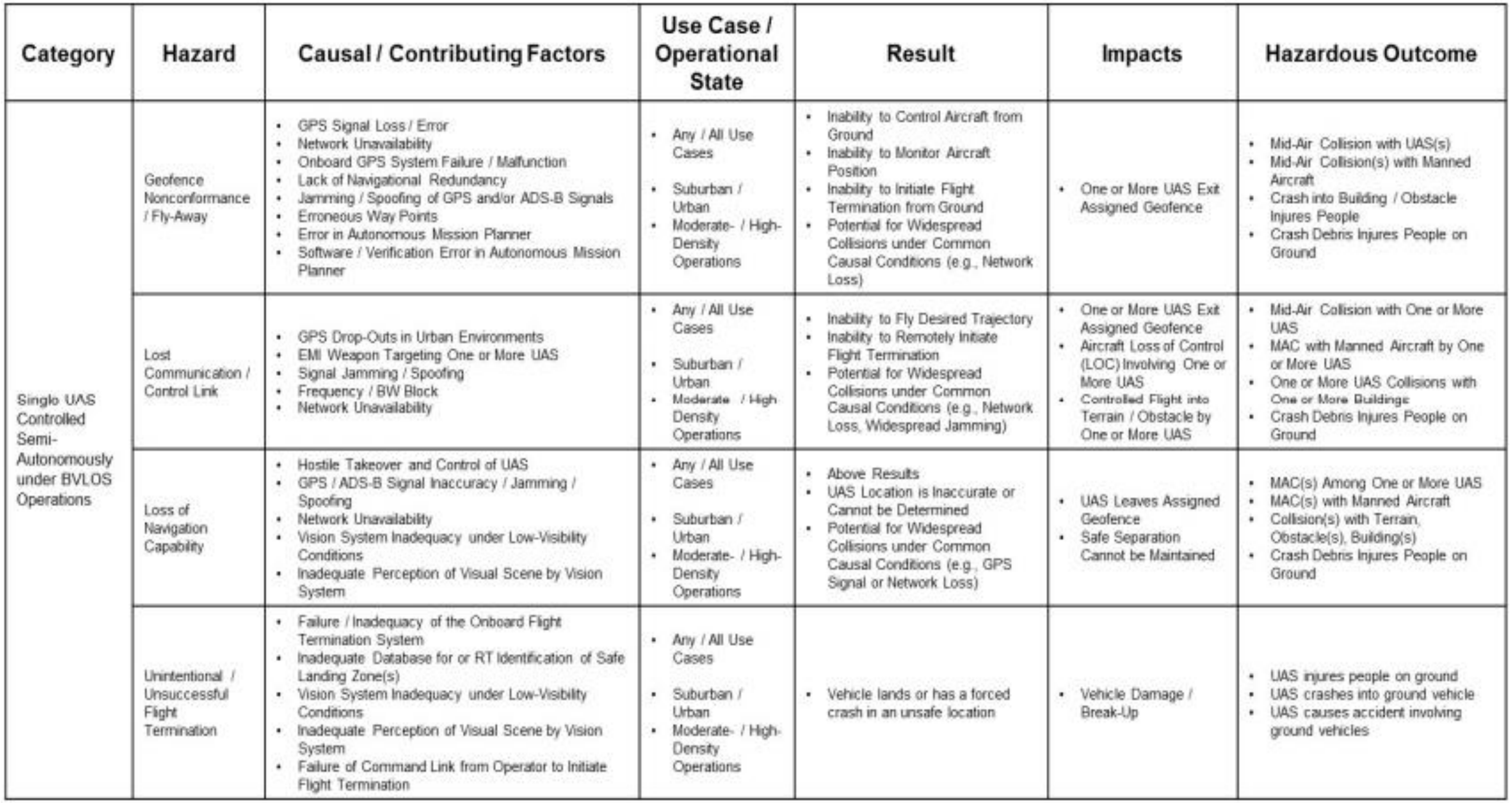
Category	Hazard	Causal / Contributing Factors	Use Case / Operational State	Result	Impacts	Hazardous Outcomes
Single UAS Manually Controlled by Remote Pilot under VLOS Operations	Aircraft Loss of Control (LOC)	• Vehicle Failures / Impairment • Control System Failures / Malfunctions / Inadequacy (Includes Design / Validation Errors) • Propulsion System Failure / Malfunction • Weather • Wind / Turbulence • Vehicle Upset Condition • Pilot Error • Power Loss / Fuel Exhaustion • Electromagnetic Interference (EMI) • Unsuccessful Launch • Bird Strike • Software Verification Error • Others	• Any / All Use Cases • Remote / Rural Location • Low-Density Operations	• Undesired Flight Trajectory that is Difficult to Predict • Unpredictable / Unstable Control Response • Uncontrolled / Unsuccessful Landing	• Vehicle Exits Assigned Geofence	• Mid-Air Collision with UAS • Mid-Air Collision with Manned Aircraft • Crash into Building / Obstacle Injures People • Crash Debris Injures People on Ground
			• Any / All Use Cases • Suburban / Urban / Congested • Low-Density Operations		• Uncontrolled Descent / Landing • Uncontrolled Descent into Terrain / Water • Vehicle Damage / Break-Up	• Injury to People on the Ground • Damage to Ground Asset Results in Fire
	Aircraft Fly-Away / Geofence Non-Conformance	• Loss of Communication / Control Link • Erroneous Way Points • GPS Failure / Errors • Autopilot Error / Malfunction • Pilot Error	• Any / All Use Cases • Remote / Rural Location • Low-Density Operations • Suburban / Urban • Low-Density Operations	• Inability to Control Aircraft from Ground • Inability to Monitor Aircraft Position • Inability to Initiate Flight Termination from Ground	• Vehicle Exits Assigned Geofence • Aircraft LOC	• Mid-Air Collision with UAS • Mid-Air Collision with Manned Aircraft • Crash into Building / Obstacle Injures People • Crash Debris Injures People on Ground
	Lost Communication / Control Link	• EMI at Vehicle • Signal Obscurence • Frequency / BW Overlap • Failure in GCS (e.g., Power Failure, etc.) • Software Verification Error	• Any / All Use Cases • Remote / Rural Location • Low-Density Operations • Suburban / Urban • Low-Density Operations	• Inability to Control Aircraft from Ground • Inability to Monitor Aircraft Position • Inability to Initiate Flight Termination from Ground • Return to Base	• Vehicle Exits Assigned Geofence • Aircraft Loss of Control (LOC) • Controlled Flight into Terrain (CFIT)	• Mid-Air Collision with UAS • Mid-Air Collision with Manned Aircraft • Crash into Building / Obstacle Injures People • Crash Debris Injures People on Ground
Single UAS Manually Controlled by Remote Pilot under VLOS Operations	Loss of Navigation Capability	• Onboard Navigation System Failure / Malfunction • Loss of / Erroneous GPS Signal • Ground Station Set-Up Error	• Any / All Use Cases • Remote / Rural Location • Low-Density Operations • Suburban / Urban • Low-Density Operations	• Inability to Fly Desired Trajectory • Intentional Grounding	• Vehicle Exits Assigned Geofence	• Mid-Air Collision with UAS • Mid-Air Collision with Manned Aircraft • Crash into Building / Obstacle Injures People • Crash Debris Injures People on Ground
	Failure / Inability to Avoid Collision with Terrain and/or Fixed / Moving Obstacles	• Inadequate / Lack of Sense/Detect and Avoid (SAA/DAA) Capability • Erroneous Way Points that Create Conflict with Obstacle • Inaccurate GPS Signal • Inadequate Navigation / Tracking • Pilot Error / Poor Judgement • Wind / Weather that Results in Abnormal Flight Trajectory	• Any / All Use Cases • Remote / Rural Location • Low-Density Operations • Suburban / Urban • Low-Density Operations	• Collision with Building • Collision with Power Lines • Collision with Ground Vehicle	• Vehicle Break-Up	• Crash Debris Injures People on Ground • UAS / Crash Debris Causes Ground Vehicle Accident on Highway • Post-Crash Fire that Damages Building and/or Injures People Inside the Building • Post-Crash Fire that Damages Environment
	Unsuccessful Landing	• Unstable Approach • Remote Pilot Error	Within Runway Safety Area	• Abnormal Runway Contact • Crash on Landing	• Vehicle Damage / Break-Up	• Post-Crash Fire that Injures Ground Crew
			Outside Runway Safety Area	• Abnormal Runway Contact • Crash on Landing	• Vehicle Damage / Break-Up	• Crash Debris Injures People on Ground

Table 25. UAS/RPAS Future Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



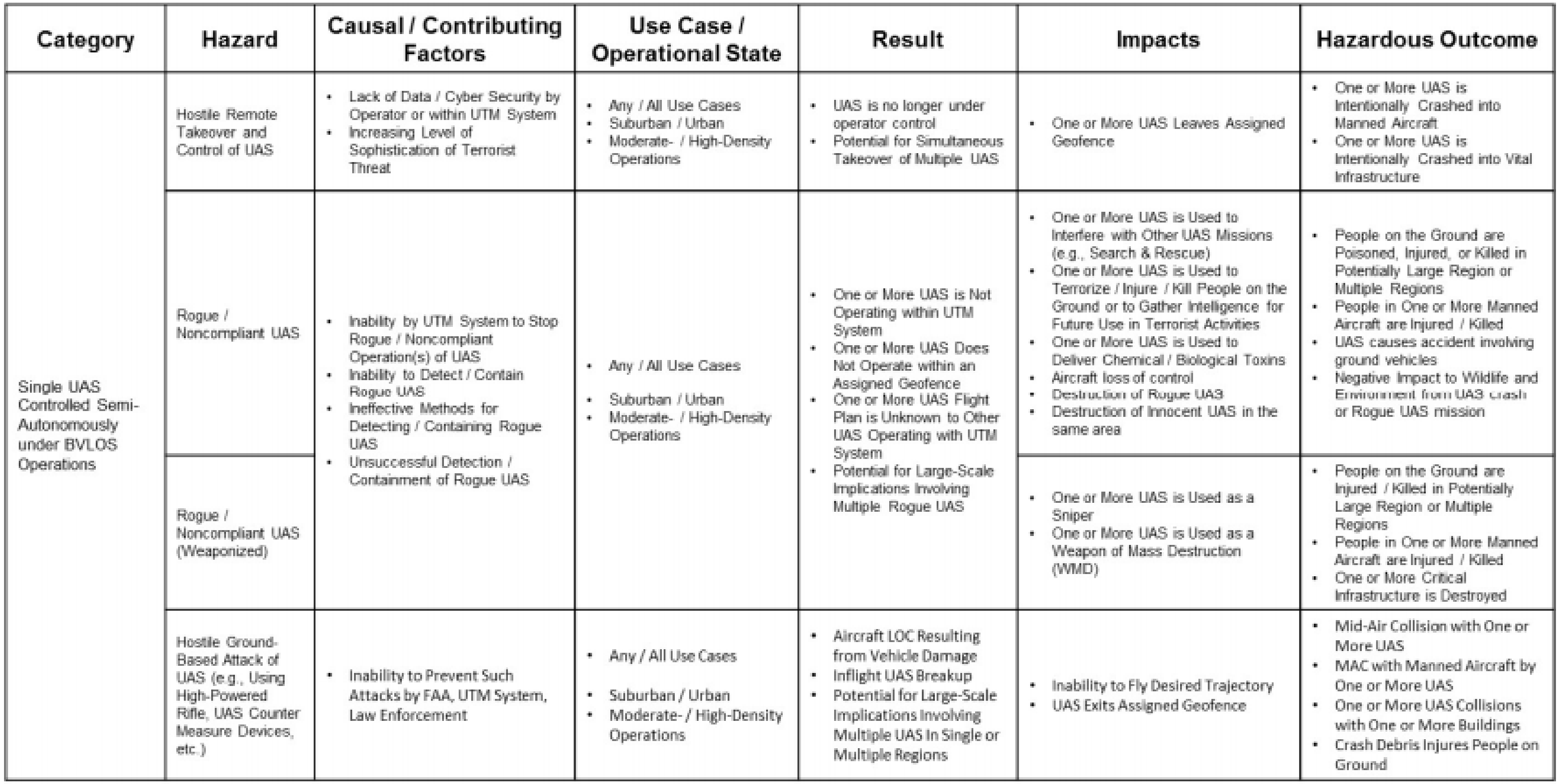
Category	Hazard	Causal / Contributing Factors	Use Case / Operational State	Result	Impacts	Hazardous Outcomes
Single UAS Controlled Semi-Autonomously under BVLOS Operations	Aircraft Loss of Control (LOC)	• Inadequate Resilience in Flight Control System to Key LOC Hazards (Including Failures, Wind / Weather, etc.) • Sensor / System / Component Failure / Malfunction • System Validation Inadequacy • Software Coding Error / Verification Inadequacy • Unexpected Wind / Turbulence (Not Forecasted and At / Near Boundary Condition) • Unexpected Weather Conditions • Payload / CG Shift / Instability • Vehicle Damage (e.g., Lightning strike during long-duration missions, Damage from Explosion / Fire during Emergency Response, Radiation Exposure from HALE operations over urban areas, etc.) • Battery Failure / Fuel Exhaustion (e.g., under Long-Duration Missions) • EMI Across Multiple UAS • Harsh Environmental Conditions (Smoke, Ash, Extreme Temperatures, etc.) for Specialized Missions (Wildfire Monitoring / Control, Search & Rescue, Maritime, etc.) • Vehicle Instability Resulting from Attempted Retrieval of Objects of Unknown size/weight • Vehicle Instability Resulting from Failure/Malfunction of Object Retrieval System • Launch/Landing Instability on Water-Based Platform • Propulsion or Vision Systems Failure / Inadequacy under Harsh Conditions (Fire, Smoke, Ash, Smog, Salty Sea Air, etc.)	• Any / All Use Cases • Suburban / Urban • Moderate- / High-Density Operations	• Undesired Flight Trajectory that is Difficult to Predict • Unpredictable / Unstable Control Response • Uncontrolled Descent • Potential for LOC Involving Multiple UAS under Common Causal Conditions (e.g., Unexpected Wind / Weather)	• One or More UAS Exit Assigned Geofence • One or More UAS on Uncontrolled Trajectory	• MACs with One or More UAS • MAC with Manned Aircraft by One or More UAS • One or More UAS Crash into Buildings / Obstacles and Injures People • Crash Debris Injures People on Ground • Damage to ground asset causes fire
	Failure / Inability to Avoid Collision with Fixed / Moving Obstacle	• Inadequate Design / Validation or Failure of SAA / DAA System • Vision System Failure / Inadequacy in Low Visibility Conditions • Missed Detection of Obstacle • Inadequate / Erroneous / Incomplete Terrain Database • Inadequate / Ineffective Sensor System for Detection of Small / Thin Obstacles (e.g., Power Lines) • Inadequate Resilience to Key Hazards (e.g., component failures, external disturbances) • Launch/Landing Instability on Water-Based Platform • Propulsion or Vision Systems Failure / Inadequacy under Harsh Conditions (Fire, Smoke, Ash, Smog, Salty Sea Air, etc.)	• Any / All Use Cases • Suburban / Urban • Moderate- / High-Density Operations	• Collisions Between Once or More UAS • Collision with Manned Aircraft • Collision with Infrastructure (Building, Bridge, Power Lines / Sub-Station, etc.) or Terrain Features • Collision with Ground Vehicle • Potential for Widespread Collisions under Common Causal Conditions (e.g., Poor Visibility)	• Vehicle Break-Up	• MACs with One or More UAS • MAC with Manned Aircraft by One or More UAS • One or More UAS Crash into Buildings / Obstacles and Injures People • Crash Debris Injures People on Ground • Damage to ground asset (e.g., High-Voltage Power Lines) causes fire

Table 26. UAS/RPAS Future Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



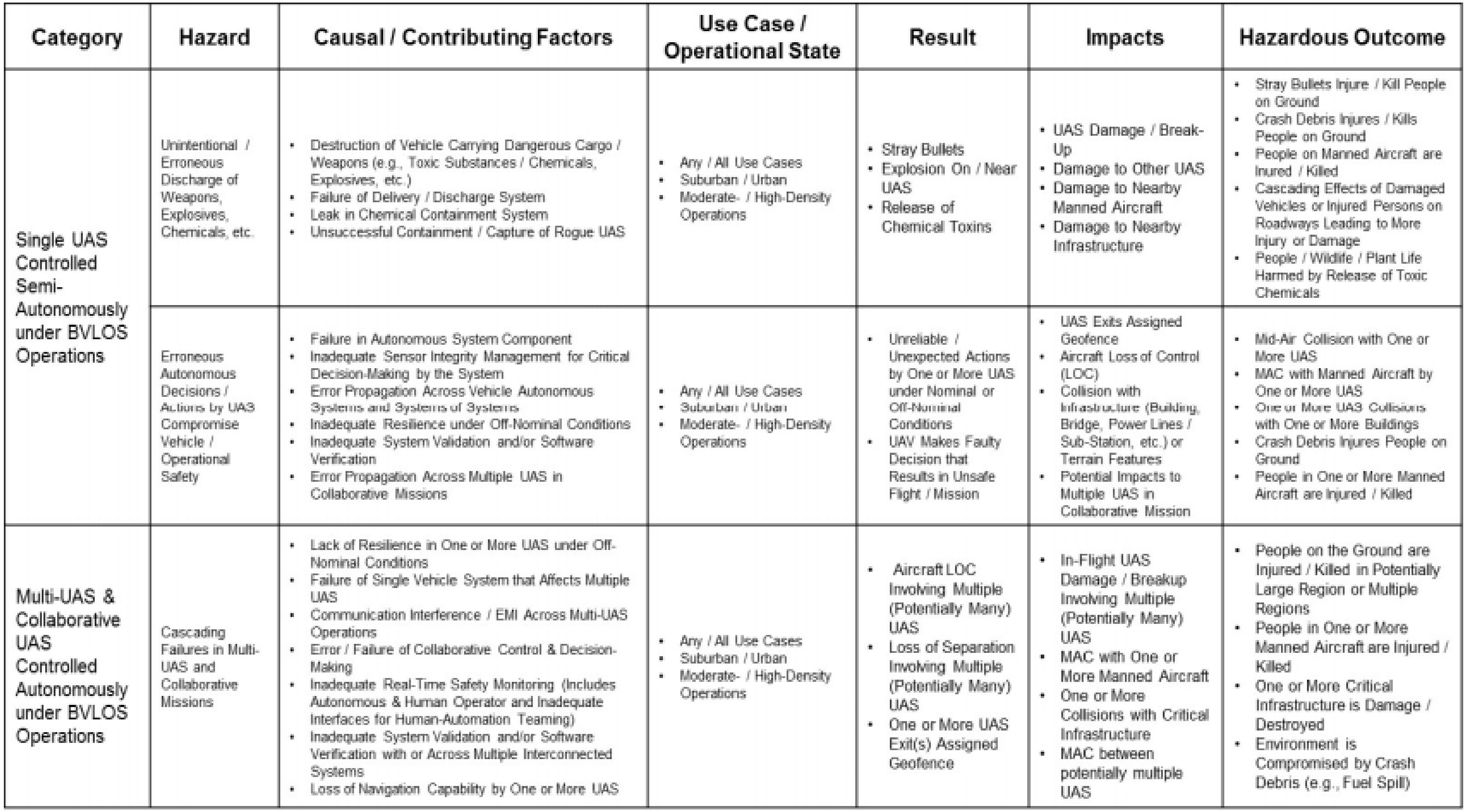
Category	Hazard	Causal / Contributing Factors	Use Case / Operational State	Result	Impacts	Hazardous Outcome
Single UAS Controlled Semi-Autonomously under BVLOS Operations	Geofence Nonconformance / Fly-Away	• GPS Signal Loss / Error • Network Unavailability • Onboard GPS System Failure / Malfunction • Lack of Navigational Redundancy • Jamming / Spoofing of GPS and/or ADS-B Signals • Erroneous Way Points • Error in Autonomous Mission Planner • Software / Verification Error in Autonomous Mission Planner	• Any / All Use Cases • Suburban / Urban • Moderate- / High-Density Operations	• Inability to Control Aircraft from Ground • Inability to Monitor Aircraft Position • Inability to Initiate Flight Termination from Ground • Potential for Widespread Collisions under Common Causal Conditions (e.g., Network Loss)	• One or More UAS Exit Assigned Geofence	• Mid-Air Collision with UAS(s) • Mid-Air Collision(s) with Manned Aircraft • Crash into Building / Obstacle Injures People • Crash Debris Injures People on Ground
	Lost Communication / Control Link	• GPS Drop-Outs in Urban Environments • EMI Weapon Targeting One or More UAS • Signal Jamming / Spoofing • Frequency / BW Block • Network Unavailability	• Any / All Use Cases • Suburban / Urban • Moderate / High Density Operations	• Inability to Fly Desired Trajectory • Inability to Remotely Initiate Flight Termination • Potential for Widespread Collisions under Common Causal Conditions (e.g., Network Loss, Widespread Jamming)	• One or More UAS Exit Assigned Geofence • Aircraft Loss of Control (LOC) Involving One or More UAS • Controlled Flight into Terrain / Obstacle by One or More UAS	• Mid-Air Collision with One or More UAS • MAC with Manned Aircraft by One or More UAS • One or More UAS Collisions with One or More Buildings • Crash Debris Injures People on Ground
	Loss of Navigation Capability	• Hostile Takeover and Control of UAS • GPS / ADS-B Signal Inaccuracy / Jamming / Spoofing • Network Unavailability • Vision System Inadequacy under Low-Visibility Conditions • Inadequate Perception of Visual Scene by Vision System	• Any / All Use Cases • Suburban / Urban • Moderate- / High-Density Operations	• Above Results • UAS Location is Inaccurate or Cannot be Determined • Potential for Widespread Collisions under Common Causal Conditions (e.g., GPS Signal or Network Loss)	• UAS Leaves Assigned Geofence • Safe Separation Cannot be Maintained	• MAC(s) Among One or More UAS • MAC(s) with Manned Aircraft • Collision(s) with Terrain, Obstacle(s), Building(s) • Crash Debris Injures People on Ground
	Unintentional / Unsuccessful Flight Termination	• Failure / Inadequacy of the Onboard Flight Termination System • Inadequate Database for or RT Identification of Safe Landing Zone(s) • Vision System Inadequacy under Low-Visibility Conditions • Inadequate Perception of Visual Scene by Vision System • Failure of Command Link from Operator to Initiate Flight Termination	• Any / All Use Cases • Suburban / Urban • Moderate- / High-Density Operations	• Vehicle lands or has a forced crash in an unsafe location	• Vehicle Damage / Break-Up	• UAS injures people on ground • UAS crashes into ground vehicle • UAS causes accident involving ground vehicles

Table 27. UAS/RPAS Future Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



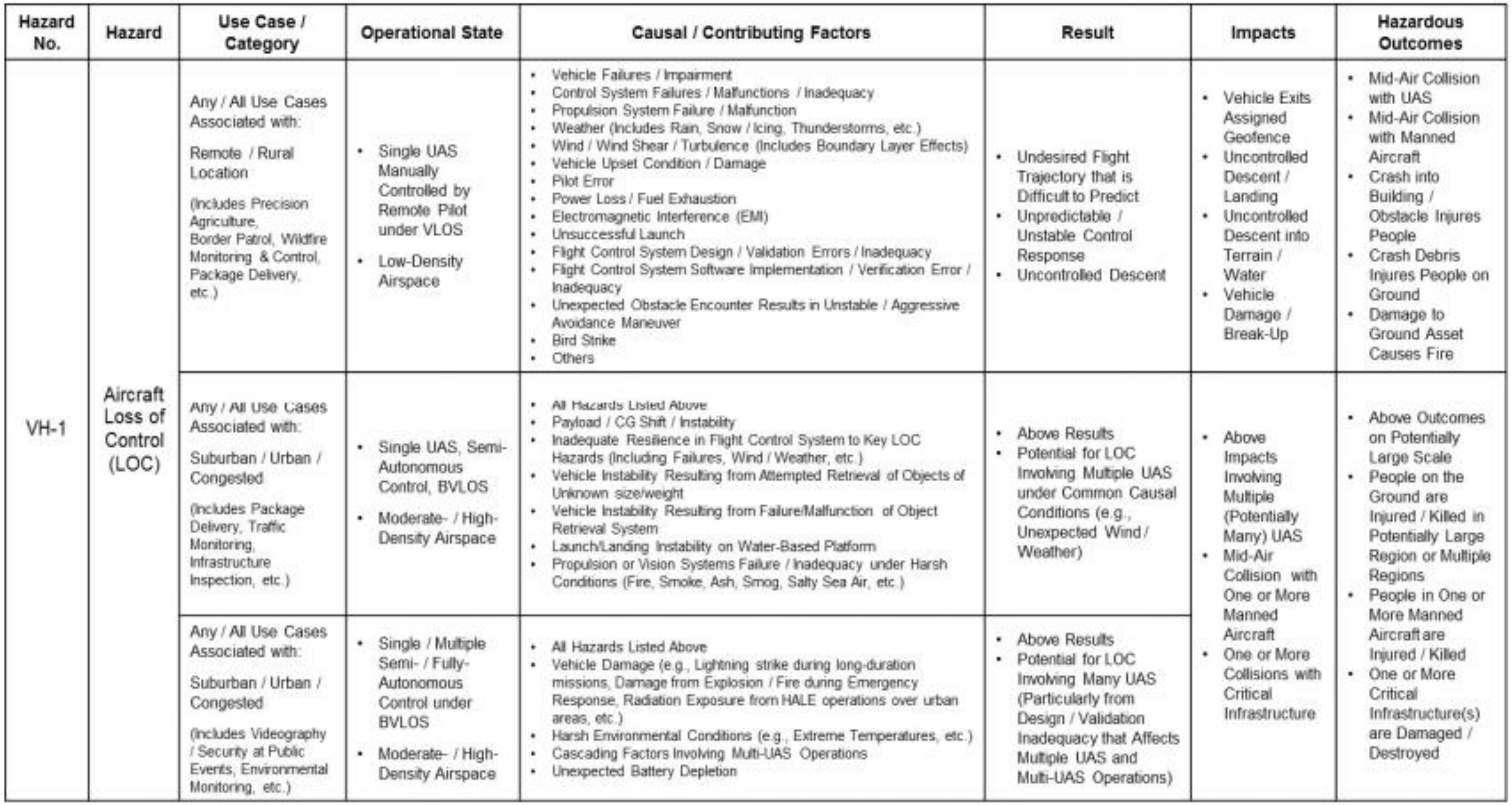
Category	Hazard	Causal / Contributing Factors	Use Case / Operational State	Result	Impacts	Hazardous Outcome
Single UAS Controlled Semi-Autonomously under BVLOS Operations	Hostile Remote Takeover and Control of UAS	• Lack of Data / Cyber Security by Operator or within UTM System • Increasing Level of Sophistication of Terrorist Threat	• Any / All Use Cases • Suburban / Urban • Moderate- / High-Density Operations	• UAS is no longer under operator control • Potential for Simultaneous Takeover of Multiple UAS	• One or More UAS Leaves Assigned Geofence	• One or More UAS is Intentionally Crashed into Manned Aircraft • One or More UAS is Intentionally Crashed into Vital Infrastructure
	Rogue / Noncompliant UAS	• Inability by UTM System to Stop Rogue / Noncompliant Operation(s) of UAS • Inability to Detect / Contain Rogue UAS • Ineffective Methods for Detecting / Containing Rogue UAS • Unsuccessful Detection / Containment of Rogue UAS	• Any / All Use Cases • Suburban / Urban • Moderate- / High-Density Operations	• One or More UAS is Not Operating within UTM System • One or More UAS Does Not Operate within an Assigned Geofence • One or More UAS Flight Plan is Unknown to Other UAS Operating with UTM System • Potential for Large-Scale Implications Involving Multiple Rogue UAS	• One or More UAS is Used to Interfere with Other UAS Missions (e.g., Search & Rescue) • One or More UAS is Used to Terrorize / Injure / Kill People on the Ground or to Gather Intelligence for Future Use in Terrorist Activities • One or More UAS is Used to Deliver Chemical / Biological Toxins • Aircraft loss of control • Destruction of Rogue UAS • Destruction of Innocent UAS in the same area	• People on the Ground are Poisoned, Injured, or Killed in Potentially Large Region or Multiple Regions • People in One or More Manned Aircraft are Injured / Killed • UAS causes accident involving ground vehicles • Negative Impact to Wildlife and Environment from UAS crash or Rogue UAS mission
	Rogue / Noncompliant UAS (Weaponized)				• One or More UAS is Used as a Sniper • One or More UAS is Used as a Weapon of Mass Destruction (WMD)	• People on the Ground are Injured / Killed in Potentially Large Region or Multiple Regions • People in One or More Manned Aircraft are Injured / Killed • One or More Critical Infrastructure is Destroyed
	Hostile Ground-Based Attack of UAS (e.g., Using High-Powered Rifle, UAS Counter Measure Devices, etc.)	• Inability to Prevent Such Attacks by FAA, UTM System, Law Enforcement	• Any / All Use Cases • Suburban / Urban • Moderate- / High-Density Operations	• Aircraft LOC Resulting from Vehicle Damage • Inflight UAS Breakup • Potential for Large-Scale Implications Involving Multiple UAS In Single or Multiple Regions	• Inability to Fly Desired Trajectory • UAS Exits Assigned Geofence	• Mid-Air Collision with One or More UAS • MAC with Manned Aircraft by One or More UAS • One or More UAS Collisions with One or More Buildings • Crash Debris Injures People on Ground

Table 28. UAS/RPAS Future Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



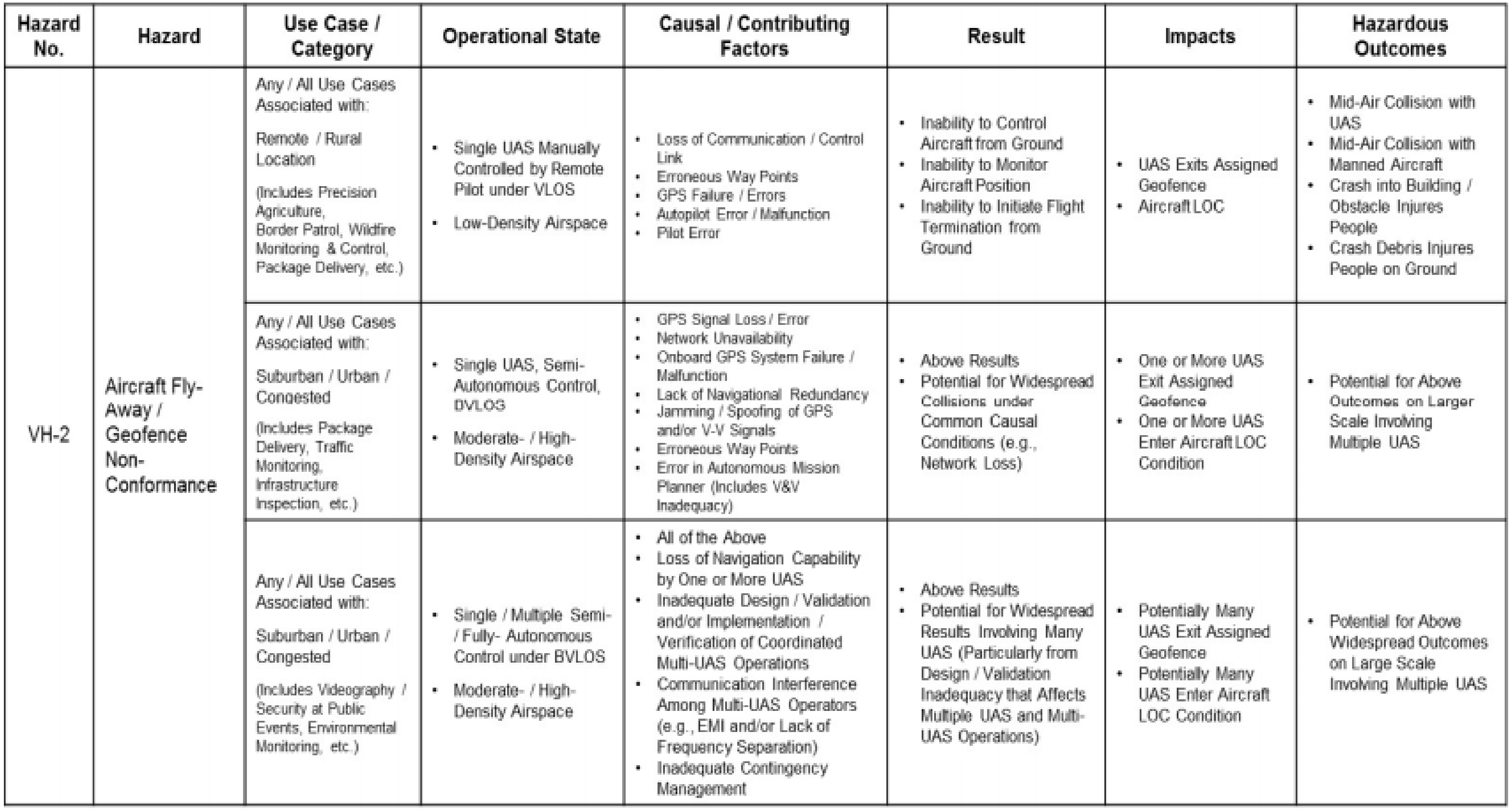
Category	Hazard	Causal / Contributing Factors	Use Case / Operational State	Result	Impacts	Hazardous Outcome
Single UAS Controlled Semi-Autonomously under BVLOS Operations	Unintentional / Erroneous Discharge of Weapons, Explosives, Chemicals, etc.	• Destruction of Vehicle Carrying Dangerous Cargo / Weapons (e.g., Toxic Substances / Chemicals, Explosives, etc.) • Failure of Delivery / Discharge System • Leak in Chemical Containment System • Unsuccessful Containment / Capture of Rogue UAS	• Any / All Use Cases • Suburban / Urban • Moderate- / High-Density Operations	• Stray Bullets • Explosion On / Near UAS • Release of Chemical Toxins	• UAS Damage / Break-Up • Damage to Other UAS • Damage to Nearby Manned Aircraft • Damage to Nearby Infrastructure	• Stray Bullets Injure / Kill People on Ground • Crash Debris Injures / Kills People on Ground • People on Manned Aircraft are Inured / Killed • Cascading Effects of Damaged Vehicles or Injured Persons on Roadways Leading to More Injury or Damage • People / Wildlife / Plant Life Harmed by Release of Toxic Chemicals
	Erroneous Autonomous Decisions / Actions by UAS Compromise Vehicle / Operational Safety	• Failure in Autonomous System Component • Inadequate Sensor Integrity Management for Critical Decision-Making by the System • Error Propagation Across Vehicle Autonomous Systems and Systems of Systems • Inadequate Resilience under Off-Nominal Conditions • Inadequate System Validation and/or Software Verification • Error Propagation Across Multiple UAS in Collaborative Missions	• Any / All Use Cases • Suburban / Urban • Moderate- / High-Density Operations	• Unreliable / Unexpected Actions by One or More UAS under Nominal or Off-Nominal Conditions • UAV Makes Faulty Decision that Results in Unsafe Flight / Mission	• UAS Exits Assigned Geofence • Aircraft Loss of Control (LOC) • Collision with Infrastructure (Building, Bridge, Power Lines / Sub-Station, etc.) or Terrain Features • Potential Impacts to Multiple UAS in Collaborative Mission	• Mid-Air Collision with One or More UAS • MAC with Manned Aircraft by One or More UAS • One or More UAS Collisions with One or More Buildings • Crash Debris Injures People on Ground • People in One or More Manned Aircraft are Injured / Killed
Multi-UAS & Collaborative UAS Controlled Autonomously under BVLOS Operations	Cascading Failures in Multi-UAS and Collaborative Missions	• Lack of Resilience in One or More UAS under Off-Nominal Conditions • Failure of Single Vehicle System that Affects Multiple UAS • Communication Interference / EMI Across Multi-UAS Operations • Error / Failure of Collaborative Control & Decision-Making • Inadequate Real-Time Safety Monitoring (Includes Autonomous & Human Operator and Inadequate Interfaces for Human-Automation Teaming) • Inadequate System Validation and/or Software Verification with or Across Multiple Interconnected Systems • Loss of Navigation Capability by One or More UAS	• Any / All Use Cases • Suburban / Urban • Moderate- / High-Density Operations	• Aircraft LOC Involving Multiple (Potentially Many) UAS • Loss of Separation Involving Multiple (Potentially Many) UAS • One or More UAS Exit(s) Assigned Geofence	• In-Flight UAS Damage / Breakup Involving Multiple (Potentially Many) UAS • MAC with One or More Manned Aircraft • One or More Collisions with Critical Infrastructure • MAC between potentially multiple UAS	• People on the Ground are Injured / Killed in Potentially Large Region or Multiple Regions • People in One or More Manned Aircraft are Injured / Killed • One or More Critical Infrastructure is Damage / Destroyed • Environment is Compromised by Crash Debris (e.g., Fuel Spill)

Table 29. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



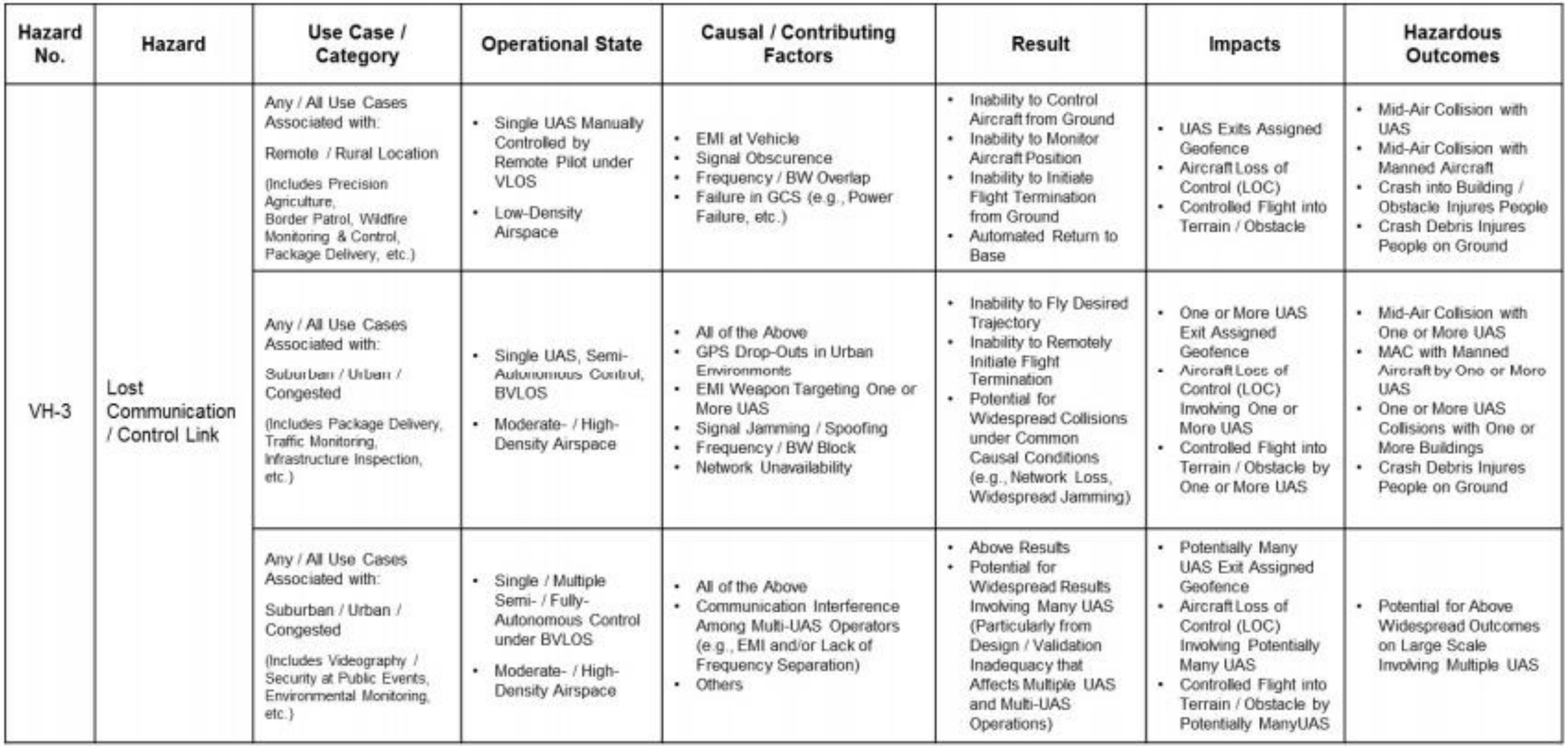
Hazard No.	Hazard	Use Case / Category	Operational State	Causal / Contributing Factors	Result	Impacts	Hazardous Outcomes
VH-1	Aircraft Loss of Control (LOC)	Any / All Use Cases Associated with: Remote / Rural Location (Includes Precision Agriculture, Border Patrol, Wildfire Monitoring & Control, Package Delivery, etc.)	• Single UAS Manually Controlled by Remote Pilot under VLOS • Low-Density Airspace	• Vehicle Failures / Impairment • Control System Failures / Malfunctions / Inadequacy • Propulsion System Failure / Malfunction • Weather (Includes Rain, Snow / Icing, Thunderstorms, etc.) • Wind / Wind Shear / Turbulence (Includes Boundary Layer Effects) • Vehicle Upset Condition / Damage • Pilot Error • Power Loss / Fuel Exhaustion • Electromagnetic Interference (EMI) • Unsuccessful Launch • Flight Control System Design / Validation Errors / Inadequacy • Flight Control System Software Implementation / Verification Error / Inadequacy • Unexpected Obstacle Encounter Results in Unstable / Aggressive Avoidance Maneuver • Bird Strike • Others	• Undesired Flight Trajectory that is Difficult to Predict • Unpredictable / Unstable Control Response • Uncontrolled Descent	• Vehicle Exits Assigned Geofence • Uncontrolled Descent / Landing • Uncontrolled Descent into Terrain / Water • Vehicle Damage / Break-Up	• Mid-Air Collision with UAS • Mid-Air Collision with Manned Aircraft • Crash into Building / Obstacle Injures People • Crash Debris Injures People on Ground • Damage to Ground Asset Causes Fire
		Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Package Delivery, Traffic Monitoring, Infrastructure Inspection, etc.)	• Single UAS, Semi-Autonomous Control, BVLOS • Moderate- / High-Density Airspace	• All Hazards Listed Above • Payload / CG Shift / Instability • Inadequate Resilience in Flight Control System to Key LOC Hazards (Including Failures, Wind / Weather, etc.) • Vehicle Instability Resulting from Attempted Retrieval of Objects of Unknown size/weight • Vehicle Instability Resulting from Failure/Malfunction of Object Retrieval System • Launch/Landing Instability on Water-Based Platform • Propulsion or Vision Systems Failure / Inadequacy under Harsh Conditions (Fire, Smoke, Ash, Smog, Salty Sea Air, etc.)	• Above Results • Potential for LOC Involving Multiple UAS under Common Causal Conditions (e.g., Unexpected Wind / Weather)	• Above Impacts Involving Multiple (Potentially Many) UAS • Mid-Air Collision with One or More Manned Aircraft • One or More Collisions with Critical Infrastructure	• Above Outcomes on Potentially Large Scale • People on the Ground are Injured / Killed in Potentially Large Region or Multiple Regions • People in One or More Manned Aircraft are Injured / Killed • One or More Critical Infrastructure(s) are Damaged / Destroyed
		Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Videography / Security at Public Events, Environmental Monitoring, etc.)	• Single / Multiple Semi- / Fully-Autonomous Control under BVLOS • Moderate- / High-Density Airspace	• All Hazards Listed Above • Vehicle Damage (e.g., Lightning strike during long-duration missions, Damage from Explosion / Fire during Emergency Response, Radiation Exposure from HALE operations over urban areas, etc.) • Harsh Environmental Conditions (e.g., Extreme Temperatures, etc.) • Cascading Factors Involving Multi-UAS Operations • Unexpected Battery Depletion	• Above Results • Potential for LOC Involving Many UAS (Particularly from Design / Validation Inadequacy that Affects Multiple UAS and Multi-UAS Operations)		

Table 30. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



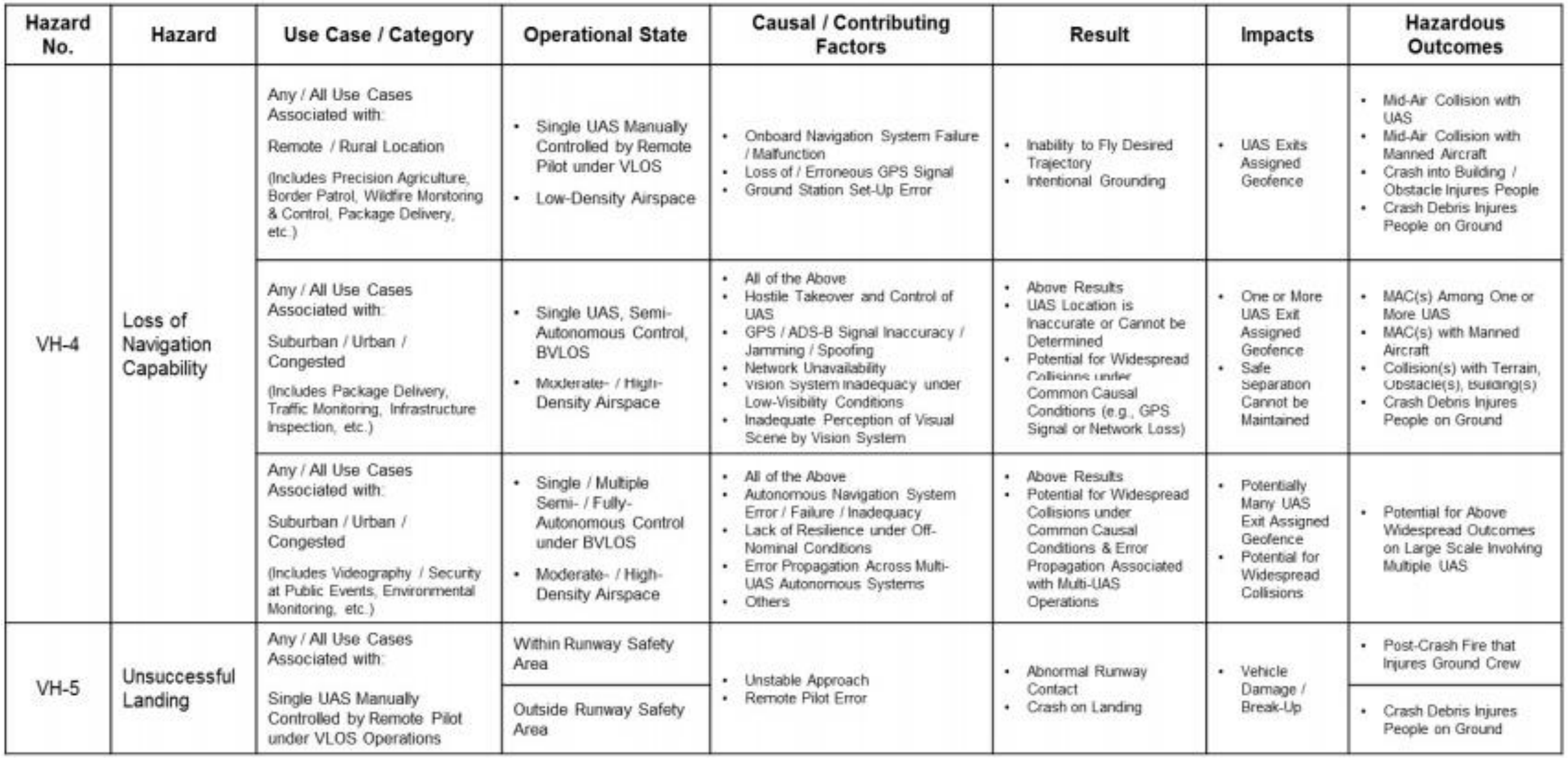
Hazard No.	Hazard	Use Case / Category	Operational State	Causal / Contributing Factors	Result	Impacts	Hazardous Outcomes
VH-2	Aircraft Fly-Away / Geofence Non-Conformance	Any / All Use Cases Associated with: Remote / Rural Location (Includes Precision Agriculture, Border Patrol, Wildfire Monitoring & Control, Package Delivery, etc.)	• Single UAS Manually Controlled by Remote Pilot under VLOS • Low-Density Airspace	• Loss of Communication / Control Link • Erroneous Way Points • GPS Failure / Errors • Autopilot Error / Malfunction • Pilot Error	• Inability to Control Aircraft from Ground • Inability to Monitor Aircraft Position • Inability to Initiate Flight Termination from Ground	• UAS Exits Assigned Geofence • Aircraft LOC	• Mid-Air Collision with UAS • Mid-Air Collision with Manned Aircraft • Crash into Building / Obstacle Injures People • Crash Debris Injures People on Ground
		Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Package Delivery, Traffic Monitoring, Infrastructure Inspection, etc.)	• Single UAS, Semi-Autonomous Control, BVLOS • Moderate- / High-Density Airspace	• GPS Signal Loss / Error • Network Unavailability • Onboard GPS System Failure / Malfunction • Lack of Navigational Redundancy • Jamming / Spoofing of GPS and/or V-V Signals • Erroneous Way Points • Error in Autonomous Mission Planner (Includes V&V Inadequacy)	• Above Results • Potential for Widespread Collisions under Common Causal Conditions (e.g., Network Loss)	• One or More UAS Exit Assigned Geofence • One or More UAS Enter Aircraft LOC Condition	• Potential for Above Outcomes on Larger Scale Involving Multiple UAS
		Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Videography / Security at Public Events, Environmental Monitoring, etc.)	• Single / Multiple Semi- / Fully- Autonomous Control under BVLOS • Moderate- / High-Density Airspace	• All of the Above • Loss of Navigation Capability by One or More UAS • Inadequate Design / Validation and/or Implementation / Verification of Coordinated Multi-UAS Operations • Communication Interference Among Multi-UAS Operators (e.g., EMI and/or Lack of Frequency Separation) • Inadequate Contingency Management	• Above Results • Potential for Widespread Results Involving Many UAS (Particularly from Design / Validation Inadequacy that Affects Multiple UAS and Multi-UAS Operations)	• Potentially Many UAS Exit Assigned Geofence • Potentially Many UAS Enter Aircraft LOC Condition	• Potential for Above Widespread Outcomes on Large Scale Involving Multiple UAS

Table 31. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



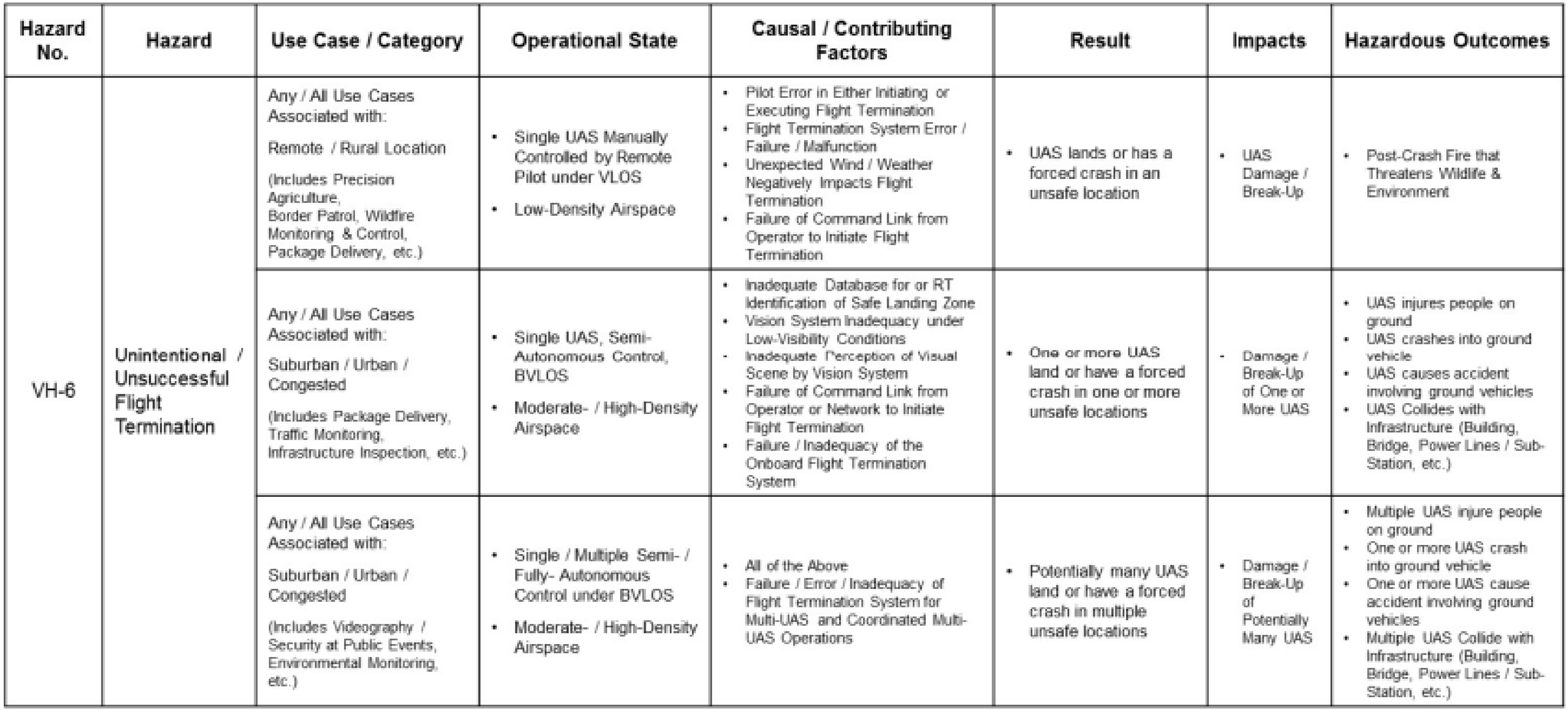
Hazard No.	Hazard	Use Case / Category	Operational State	Causal / Contributing Factors	Result	Impacts	Hazardous Outcomes
VH-3	Lost Communication / Control Link	Any / All Use Cases Associated with: Remote / Rural Location (Includes Precision Agriculture, Border Patrol, Wildfire Monitoring & Control, Package Delivery, etc.)	• Single UAS Manually Controlled by Remote Pilot under VLOS • Low-Density Airspace	• EMI at Vehicle • Signal Obscurence • Frequency / BW Overlap • Failure in GCS (e.g., Power Failure, etc.)	• Inability to Control Aircraft from Ground • Inability to Monitor Aircraft Position • Inability to Initiate Flight Termination from Ground • Automated Return to Base	• UAS Exits Assigned Geofence • Aircraft Loss of Control (LOC) • Controlled Flight into Terrain / Obstacle	• Mid-Air Collision with UAS • Mid-Air Collision with Manned Aircraft • Crash into Building / Obstacle Injures People • Crash Debris Injures People on Ground
		Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Package Delivery, Traffic Monitoring, Infrastructure Inspection, etc.)	• Single UAS, Semi-Autonomous Control, BVLOS • Moderate- / High-Density Airspace	• All of the Above • GPS Drop-Outs in Urban Environments • EMI Weapon Targeting One or More UAS • Signal Jamming / Spoofing • Frequency / BW Block • Network Unavailability	• Inability to Fly Desired Trajectory • Inability to Remotely Initiate Flight Termination • Potential for Widespread Collisions under Common Causal Conditions (e.g., Network Loss, Widespread Jamming)	• One or More UAS Exit Assigned Geofence • Aircraft Loss of Control (LOC) Involving One or More UAS • Controlled Flight into Terrain / Obstacle by One or More UAS	• Mid-Air Collision with One or More UAS • MAC with Manned Aircraft by One or More UAS • One or More UAS Collisions with One or More Buildings • Crash Debris Injures People on Ground
		Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Videography / Security at Public Events, Environmental Monitoring, etc.)	• Single / Multiple Semi- / Fully-Autonomous Control under BVLOS • Moderate- / High-Density Airspace	• All of the Above • Communication Interference Among Multi-UAS Operators (e.g., EMI and/or Lack of Frequency Separation) • Others	• Above Results • Potential for Widespread Results Involving Many UAS (Particularly from Design / Validation Inadequacy that Affects Multiple UAS and Multi-UAS Operations)	• Potentially Many UAS Exit Assigned Geofence • Aircraft Loss of Control (LOC) Involving Potentially Many UAS • Controlled Flight into Terrain / Obstacle by Potentially ManyUAS	• Potential for Above Widespread Outcomes on Large Scale Involving Multiple UAS

Table 32. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



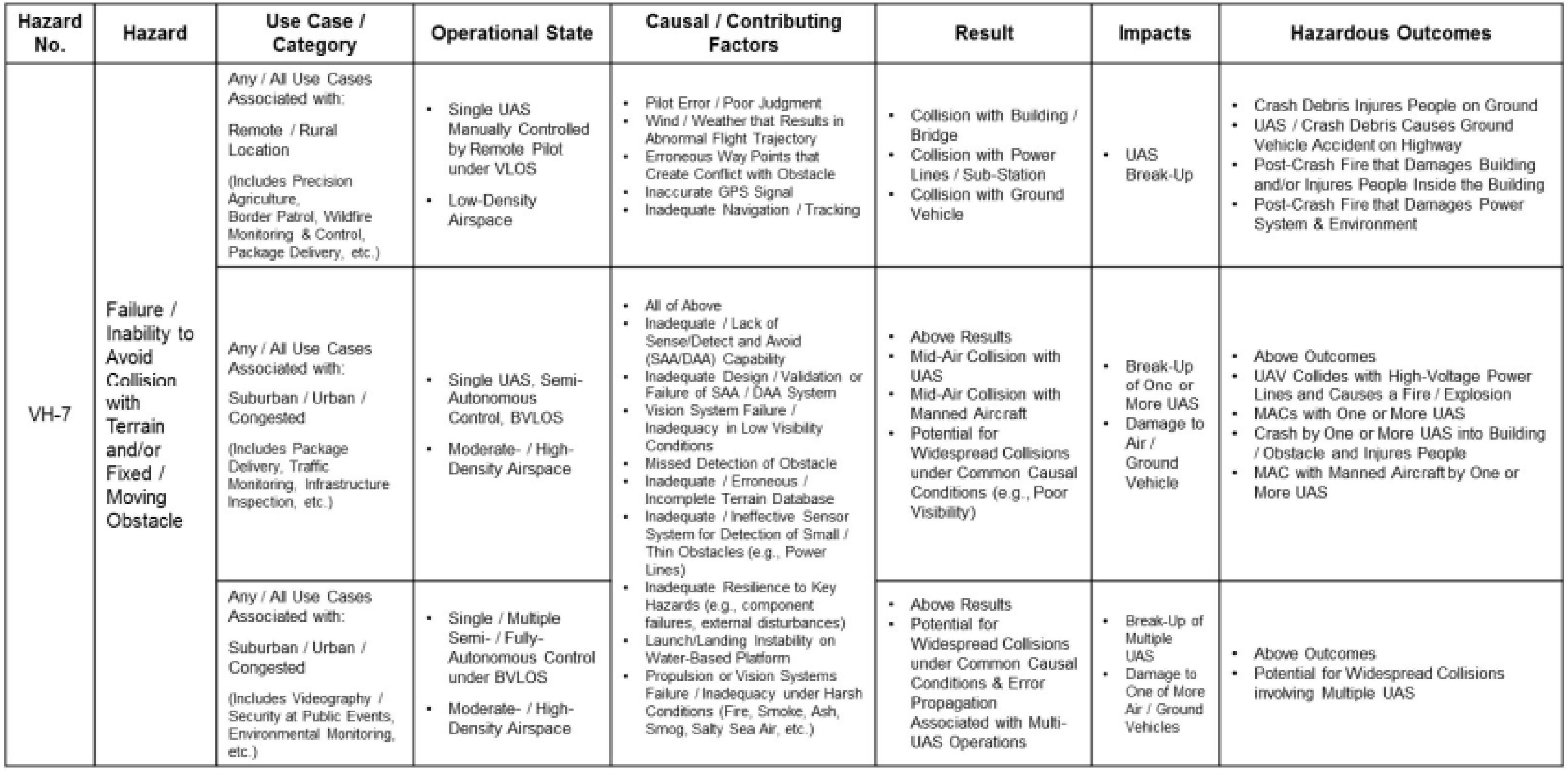
Hazard No.	Hazard	Use Case / Category	Operational State	Causal / Contributing Factors	Result	Impacts	Hazardous Outcomes
VH-4	Loss of Navigation Capability	Any / All Use Cases Associated with: Remote / Rural Location (Includes Precision Agriculture, Border Patrol, Wildfire Monitoring & Control, Package Delivery, etc.)	• Single UAS Manually Controlled by Remote Pilot under VLOS • Low-Density Airspace	• Onboard Navigation System Failure / Malfunction • Loss of / Erroneous GPS Signal • Ground Station Set-Up Error	• Inability to Fly Desired Trajectory • Intentional Grounding	• UAS Exits Assigned Geofence	• Mid-Air Collision with UAS • Mid-Air Collision with Manned Aircraft • Crash into Building / Obstacle Injures People • Crash Debris Injures People on Ground
		Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Package Delivery, Traffic Monitoring, Infrastructure Inspection, etc.)	• Single UAS, Semi-Autonomous Control, BVLOS • Moderate- / High-Density Airspace	• All of the Above • Hostile Takeover and Control of UAS • GPS / ADS-B Signal Inaccuracy / Jamming / Spoofing • Network Unavailability • Vision System Inadequacy under Low-Visibility Conditions • Inadequate Perception of Visual Scene by Vision System	• Above Results • UAS Location is Inaccurate or Cannot be Determined • Potential for Widespread Collisions under Common Causal Conditions (e.g., GPS Signal or Network Loss)	• One or More UAS Exit Assigned Geofence • Safe Separation Cannot be Maintained	• MAC(s) Among One or More UAS • MAC(s) with Manned Aircraft • Collision(s) with Terrain, Obstacle(s), Building(s) • Crash Debris Injures People on Ground
		Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Videography / Security at Public Events, Environmental Monitoring, etc.)	• Single / Multiple Semi- / Fully-Autonomous Control under BVLOS • Moderate- / High-Density Airspace	• All of the Above • Autonomous Navigation System Error / Failure / Inadequacy • Lack of Resilience under Off-Nominal Conditions • Error Propagation Across Multi-UAS Autonomous Systems • Others	• Above Results • Potential for Widespread Collisions under Common Causal Conditions & Error Propagation Associated with Multi-UAS Operations	• Potentially Many UAS Exit Assigned Geofence • Potential for Widespread Collisions	• Potential for Above Widespread Outcomes on Large Scale Involving Multiple UAS
VH-5	Unsuccessful Landing	Any / All Use Cases Associated with: Single UAS Manually Controlled by Remote Pilot under VLOS Operations	Within Runway Safety Area	• Unstable Approach • Remote Pilot Error	• Abnormal Runway Contact • Crash on Landing	• Vehicle Damage / Break-Up	• Post-Crash Fire that Injures Ground Crew
			Outside Runway Safety Area				• Crash Debris Injures People on Ground

Table 33. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



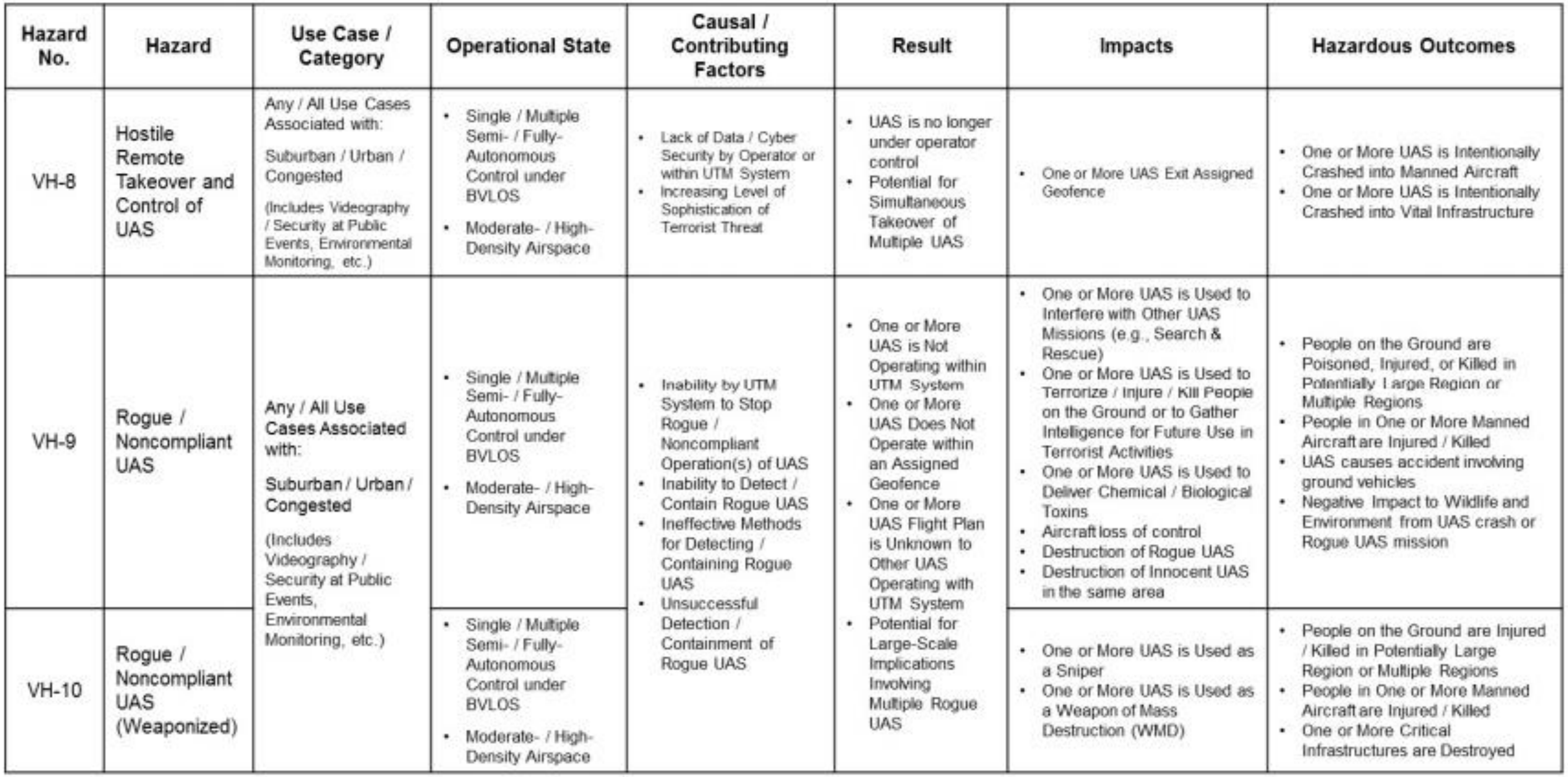
Hazard No.	Hazard	Use Case / Category	Operational State	Causal / Contributing Factors	Result	Impacts	Hazardous Outcomes
VH-6	Unintentional / Unsuccessful Flight Termination	Any / All Use Cases Associated with: Remote / Rural Location (Includes Precision Agriculture, Border Patrol, Wildfire Monitoring & Control, Package Delivery, etc.)	• Single UAS Manually Controlled by Remote Pilot under VLOS • Low-Density Airspace	• Pilot Error in Either Initiating or Executing Flight Termination • Flight Termination System Error / Failure / Malfunction • Unexpected Wind / Weather Negatively Impacts Flight Termination • Failure of Command Link from Operator to Initiate Flight Termination	• UAS lands or has a forced crash in an unsafe location	• UAS Damage / Break-Up	• Post-Crash Fire that Threatens Wildlife & Environment
		Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Package Delivery, Traffic Monitoring, Infrastructure Inspection, etc.)	• Single UAS, Semi-Autonomous Control, BVLOS • Moderate- / High-Density Airspace	• Inadequate Database for or RT Identification of Safe Landing Zone • Vision System Inadequacy under Low-Visibility Conditions - Inadequate Perception of Visual Scene by Vision System • Failure of Command Link from Operator or Network to Initiate Flight Termination • Failure / Inadequacy of the Onboard Flight Termination System	• One or more UAS land or have a forced crash in one or more unsafe locations	- Damage / Break-Up of One or More UAS	• UAS injures people on ground • UAS crashes into ground vehicle • UAS causes accident involving ground vehicles • UAS Collides with Infrastructure (Building, Bridge, Power Lines / Sub-Station, etc.)
		Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Videography / Security at Public Events, Environmental Monitoring, etc.)	• Single / Multiple Semi- / Fully- Autonomous Control under BVLOS • Moderate- / High-Density Airspace	• All of the Above • Failure / Error / Inadequacy of Flight Termination System for Multi-UAS and Coordinated Multi-UAS Operations	• Potentially many UAS land or have a forced crash in multiple unsafe locations	• Damage / Break-Up of Potentially Many UAS	• Multiple UAS injure people on ground • One or more UAS crash into ground vehicle • One or more UAS cause accident involving ground vehicles • Multiple UAS Collide with Infrastructure (Building, Bridge, Power Lines / Sub-Station, etc.)

Table 34. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



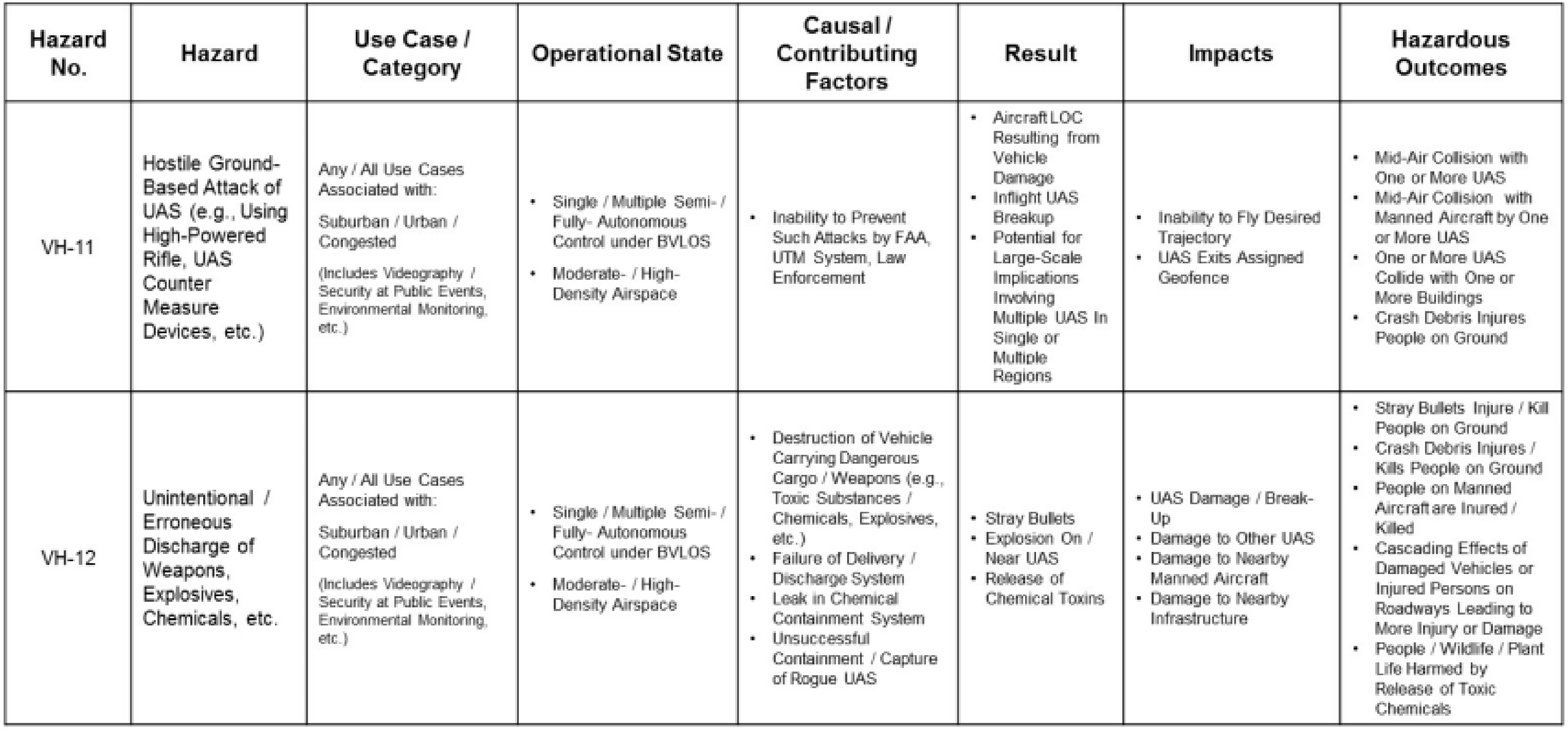
Hazard No.	Hazard	Use Case / Category	Operational State	Causal / Contributing Factors	Result	Impacts	Hazardous Outcomes
VH-7	Failure / Inability to Avoid Collision with Terrain and/or Fixed / Moving Obstacle	Any / All Use Cases Associated with: Remote / Rural Location (Includes Precision Agriculture, Border Patrol, Wildfire Monitoring & Control, Package Delivery, etc.)	• Single UAS Manually Controlled by Remote Pilot under VLOS • Low-Density Airspace	• Pilot Error / Poor Judgment • Wind / Weather that Results in Abnormal Flight Trajectory • Erroneous Way Points that Create Conflict with Obstacle • Inaccurate GPS Signal • Inadequate Navigation / Tracking	• Collision with Building / Bridge • Collision with Power Lines / Sub-Station • Collision with Ground Vehicle	• UAS Break-Up	• Crash Debris Injures People on Ground • UAS / Crash Debris Causes Ground Vehicle Accident on Highway • Post-Crash Fire that Damages Building and/or Injures People Inside the Building • Post-Crash Fire that Damages Power System & Environment
		Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Package Delivery, Traffic Monitoring, Infrastructure Inspection, etc.)	• Single UAS, Semi-Autonomous Control, BVLOS • Moderate- / High-Density Airspace	• All of Above • Inadequate / Lack of Sense/Detect and Avoid (SAA/DAA) Capability • Inadequate Design / Validation or Failure of SAA / DAA System • Vision System Failure / Inadequacy in Low Visibility Conditions • Missed Detection of Obstacle • Inadequate / Erroneous / Incomplete Terrain Database • Inadequate / Ineffective Sensor System for Detection of Small / Thin Obstacles (e.g., Power Lines) • Inadequate Resilience to Key Hazards (e.g., component failures, external disturbances) • Launch/Landing Instability on Water-Based Platform • Propulsion or Vision Systems Failure / Inadequacy under Harsh Conditions (Fire, Smoke, Ash, Smog, Salty Sea Air, etc.)	• Above Results • Mid-Air Collision with UAS • Mid-Air Collision with Manned Aircraft • Potential for Widespread Collisions under Common Causal Conditions (e.g., Poor Visibility)	• Break-Up of One or More UAS • Damage to Air / Ground Vehicle	• Above Outcomes • UAV Collides with High-Voltage Power Lines and Causes a Fire / Explosion • MACs with One or More UAS • Crash by One or More UAS into Building / Obstacle and Injures People • MAC with Manned Aircraft by One or More UAS
		Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Videography / Security at Public Events, Environmental Monitoring, etc.)	• Single / Multiple Semi- / Fully-Autonomous Control under BVLOS • Moderate- / High-Density Airspace		• Above Results • Potential for Widespread Collisions under Common Causal Conditions & Error Propagation Associated with Multi-UAS Operations	• Break-Up of Multiple UAS • Damage to One of More Air / Ground Vehicles	• Above Outcomes • Potential for Widespread Collisions involving Multiple UAS

Table 35. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



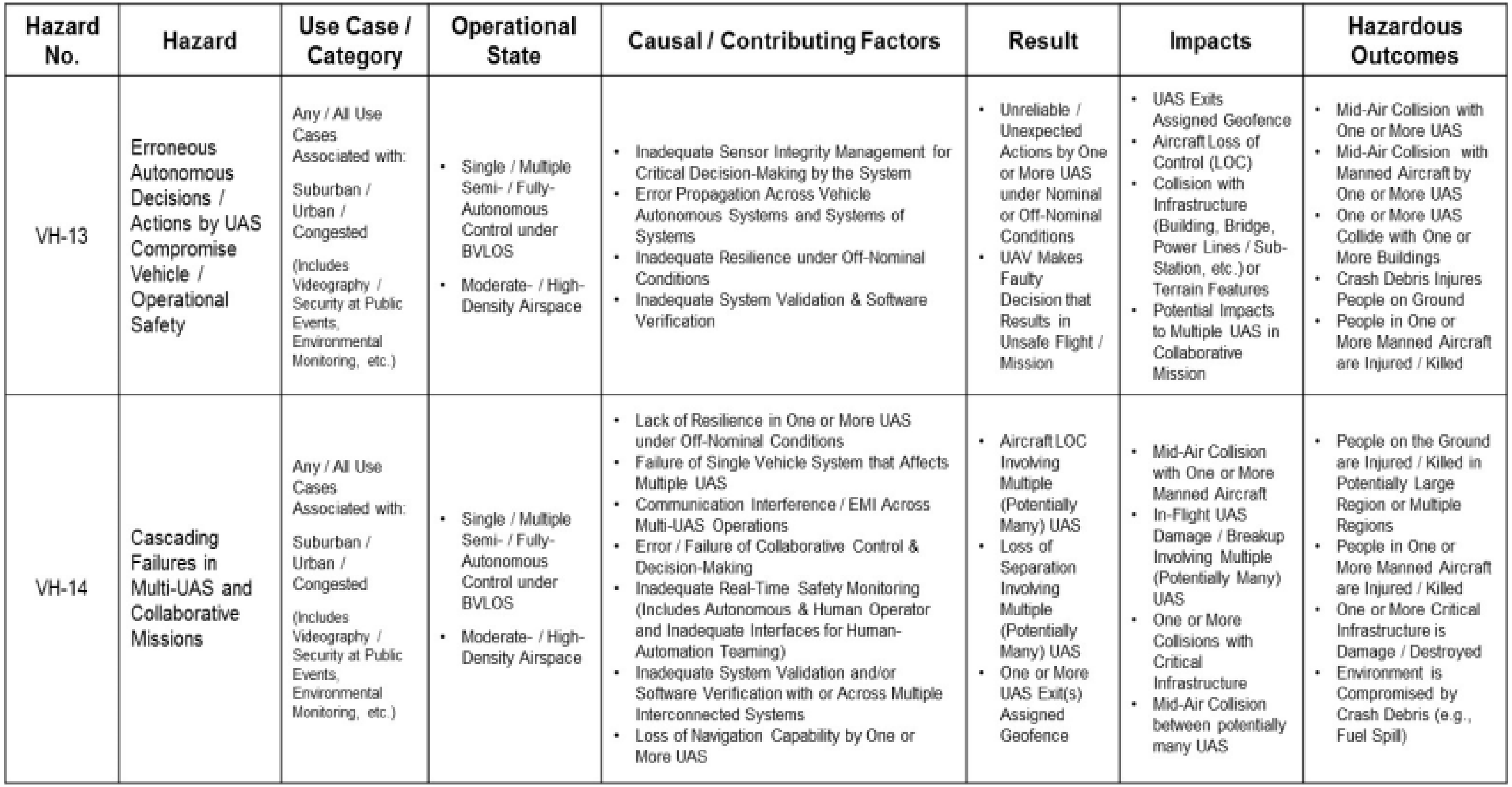
Hazard No.	Hazard	Use Case / Category	Operational State	Causal / Contributing Factors	Result	Impacts	Hazardous Outcomes
VH-8	Hostile Remote Takeover and Control of UAS	Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Videography / Security at Public Events, Environmental Monitoring, etc.)	• Single / Multiple Semi- / Fully-Autonomous Control under BVLOS • Moderate- / High-Density Airspace	• Lack of Data / Cyber Security by Operator or within UTM System • Increasing Level of Sophistication of Terrorist Threat	• UAS is no longer under operator control • Potential for Simultaneous Takeover of Multiple UAS	• One or More UAS Exit Assigned Geofence	• One or More UAS is Intentionally Crashed into Manned Aircraft • One or More UAS is Intentionally Crashed into Vital Infrastructure
VH-9	Rogue / Noncompliant UAS	Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Videography / Security at Public Events, Environmental Monitoring, etc.)	• Single / Multiple Semi- / Fully-Autonomous Control under BVLOS • Moderate- / High-Density Airspace	• Inability by UTM System to Stop Rogue / Noncompliant Operation(s) of UAS • Inability to Detect / Contain Rogue UAS • Ineffective Methods for Detecting / Containing Rogue UAS • Unsuccessful Detection / Containment of Rogue UAS	• One or More UAS is Not Operating within UTM System • One or More UAS Does Not Operate within an Assigned Geofence • One or More UAS Flight Plan is Unknown to Other UAS Operating with UTM System • Potential for Large-Scale Implications Involving Multiple Rogue UAS	• One or More UAS is Used to Interfere with Other UAS Missions (e.g., Search & Rescue) • One or More UAS is Used to Terrorize / Injure / Kill People on the Ground or to Gather Intelligence for Future Use in Terrorist Activities • One or More UAS is Used to Deliver Chemical / Biological Toxins • Aircraft loss of control • Destruction of Rogue UAS • Destruction of Innocent UAS in the same area	• People on the Ground are Poisoned, Injured, or Killed in Potentially Large Region or Multiple Regions • People in One or More Manned Aircraft are Injured / Killed • UAS causes accident involving ground vehicles • Negative Impact to Wildlife and Environment from UAS crash or Rogue UAS mission
VH-10	Rogue / Noncompliant UAS (Weaponized)		• Single / Multiple Semi- / Fully-Autonomous Control under BVLOS • Moderate- / High-Density Airspace			• One or More UAS is Used as a Sniper • One or More UAS is Used as a Weapon of Mass Destruction (WMD)	• People on the Ground are Injured / Killed in Potentially Large Region or Multiple Regions • People in One or More Manned Aircraft are Injured / Killed • One or More Critical Infrastructures are Destroyed

Table 36. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



Hazard No.	Hazard	Use Case / Category	Operational State	Causal / Contributing Factors	Result	Impacts	Hazardous Outcomes
VH-11	Hostile Ground-Based Attack of UAS (e.g., Using High-Powered Rifle, UAS Counter Measure Devices, etc.)	Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Videography / Security at Public Events, Environmental Monitoring, etc.)	• Single / Multiple Semi- / Fully- Autonomous Control under BVLOS • Moderate- / High-Density Airspace	• Inability to Prevent Such Attacks by FAA, UTM System, Law Enforcement	• Aircraft LOC Resulting from Vehicle Damage • Inflight UAS Breakup • Potential for Large-Scale Implications Involving Multiple UAS In Single or Multiple Regions	• Inability to Fly Desired Trajectory • UAS Exits Assigned Geofence	• Mid-Air Collision with One or More UAS • Mid-Air Collision with Manned Aircraft by One or More UAS • One or More UAS Collide with One or More Buildings • Crash Debris Injures People on Ground
VH-12	Unintentional / Erroneous Discharge of Weapons, Explosives, Chemicals, etc.	Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Videography / Security at Public Events, Environmental Monitoring, etc.)	• Single / Multiple Semi- / Fully- Autonomous Control under BVLOS • Moderate- / High-Density Airspace	• Destruction of Vehicle Carrying Dangerous Cargo / Weapons (e.g., Toxic Substances / Chemicals, Explosives, etc.) • Failure of Delivery / Discharge System • Leak in Chemical Containment System • Unsuccessful Containment / Capture of Rogue UAS	• Stray Bullets • Explosion On / Near UAS • Release of Chemical Toxins	• UAS Damage / Break-Up • Damage to Other UAS • Damage to Nearby Manned Aircraft • Damage to Nearby Infrastructure	• Stray Bullets Injure / Kill People on Ground • Crash Debris Injures / Kills People on Ground • People on Manned Aircraft are Inured / Killed • Cascading Effects of Damaged Vehicles or Injured Persons on Roadways Leading to More Injury or Damage • People / Wildlife / Plant Life Harmed by Release of Toxic Chemicals

Table 37. UAS/RPAS Combined Hazards (Ref. Hazards Identification and Analysis for UAS Operations, AIAA AVIATION Forum)



Hazard No.	Hazard	Use Case / Category	Operational State	Causal / Contributing Factors	Result	Impacts	Hazardous Outcomes
VH-13	Erroneous Autonomous Decisions / Actions by UAS Compromise Vehicle / Operational Safety	Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Videography / Security at Public Events, Environmental Monitoring, etc.)	• Single / Multiple Semi- / Fully-Autonomous Control under BVLOS • Moderate- / High-Density Airspace	• Inadequate Sensor Integrity Management for Critical Decision-Making by the System • Error Propagation Across Vehicle Autonomous Systems and Systems of Systems • Inadequate Resilience under Off-Nominal Conditions • Inadequate System Validation & Software Verification	• Unreliable / Unexpected Actions by One or More UAS under Nominal or Off-Nominal Conditions • UAV Makes Faulty Decision that Results in Unsafe Flight / Mission	• UAS Exits Assigned Geofence • Aircraft Loss of Control (LOC) • Collision with Infrastructure (Building, Bridge, Power Lines / Sub-Station, etc.) or Terrain Features • Potential Impacts to Multiple UAS in Collaborative Mission	• Mid-Air Collision with One or More UAS • Mid-Air Collision with Manned Aircraft by One or More UAS • One or More UAS Collide with One or More Buildings • Crash Debris Injures People on Ground • People in One or More Manned Aircraft are Injured / Killed
VH-14	Cascading Failures in Multi-UAS and Collaborative Missions	Any / All Use Cases Associated with: Suburban / Urban / Congested (Includes Videography / Security at Public Events, Environmental Monitoring, etc.)	• Single / Multiple Semi- / Fully-Autonomous Control under BVLOS • Moderate- / High-Density Airspace	• Lack of Resilience in One or More UAS under Off-Nominal Conditions • Failure of Single Vehicle System that Affects Multiple UAS • Communication Interference / EMI Across Multi-UAS Operations • Error / Failure of Collaborative Control & Decision-Making • Inadequate Real-Time Safety Monitoring (Includes Autonomous & Human Operator and Inadequate Interfaces for Human-Automation Teaming) • Inadequate System Validation and/or Software Verification with or Across Multiple Interconnected Systems • Loss of Navigation Capability by One or More UAS	• Aircraft LOC Involving Multiple (Potentially Many) UAS • Loss of Separation Involving Multiple (Potentially Many) UAS • One or More UAS Exit(s) Assigned Geofence	• Mid-Air Collision with One or More Manned Aircraft • In-Flight UAS Damage / Breakup Involving Multiple (Potentially Many) UAS • One or More Collisions with Critical Infrastructure • Mid-Air Collision between potentially many UAS	• People on the Ground are Injured / Killed in Potentially Large Region or Multiple Regions • People in One or More Manned Aircraft are Injured / Killed • One or More Critical Infrastructure is Damage / Destroyed • Environment is Compromised by Crash Debris (e.g., Fuel Spill)

5.3.4 Safety Objectives

When defining UAS/RPAS safety objectives, the equivalence with manned aircraft per category principle is applied. The starting point is therefore to establish a range of target levels of safety for manned aircraft. This can be based either on current practice (quantitative target levels of safety are available in AMC 25.1309 and AC-23.1309-1E), or from a knowledge of actual accident rates. For aircraft categories where no target level of safety is defined, actual accident statistics have been established from published data, in this case UK-CAA CAP 780, and is summarized below in Table 38.

Table 38. Manned Aircraft Accident Rates

Aircraft Category	Accident Rate (per flight hour) All Causes	Source data
Large transport (CS-25)	1 x 10-6	AMC 25.1309
Normal Utility (CS-23, Class I)	1 x 10-4	AC 23.1309-1E
Large public transport aeroplane	4.8 x 10-6	UK-CAA CAP 780
Small public transport aeroplane	5.3 x 10-5	
Public transport helicopters	1.91 x 10-5	
Non-public transport conventional aircraft < 5700 kg	1.79 x 10-4	
Non public transport helicopters < 5,700 kg	1.27 x 10-4	
Microlights	3.1 x 10-4	

With the introduction of UAS/UAS/RPAS, it is expected that light UA/RPA will replace or augment existing manned aircraft performing a similar role. The resulting effect will probably be a shift in the balance of the fleet towards lower category aircraft, and hence lower average safety targets. To counter this trend and prevent an overall increase in the accident rate (all categories), a minimum target level of safety of 1x10^{-4}/fh (all causes) is established commensurate with the lowest safety target applied to manned aircraft. Those UAS/RPAS that have no direct equivalence with manned aircraft due to their lower weights will therefore need to meet this minimum target level of safety. A review of this policy may be necessary as the UAS/RPAS fleet expands.

A target level of safety is made up of both airworthiness and operational elements. As UAS/RPAS are more dependent on systems to ensure safety of flight and less on human interaction (in part due to the reliability of the data link), it is appropriate that the operational/airworthiness balance to achieving the overall target level of safety is reassessed and adjusted, where necessary, in favour of higher airworthiness standards to achieve the same accident rate per category.

Manned aircraft system safety assessment was developed for large aircraft based on the fatal accident rate at the time (10^{-6}/fh), an observation that approximately 10% of accidents were the result of a systems failure primary causal factor, and an assumption that complex systems installed in CS-25 aircraft had in the order of 100 potentially Catastrophic failure conditions at aircraft level. Summing these values leads to the familiar and acceptable quantitative probability value <10^{-9}/fh for each Catastrophic failure condition.

A difference between manned aircraft and UAS/RPAS is the increased reliance on aircraft systems. UAS/RPAS may need to incorporate some advanced systems, including fly-by-wire and Command & Control data links. Furthermore, in the case of complex UAS/RPAS (Complexity Levels II), additional systems to enable automatic capability, together with Detect & Avoid and flight management systems, will also need to be installed. In making parallels with manned aircraft, the level of system complexity in Level II is seen as more akin to large aircraft and so it is appropriate that the same rational is used in deriving safety objectives. To maintain the manned aircraft surface impact accident rate, UAS/RPAS of Complexity Level II will be required to enhance the quantitative safety objectives of applicable systems by one order of magnitude over and above that of the equivalent manned aircraft but no more than the maximum corresponding with CS/part-25 values. Therefore, already complex aircraft such as CS/part 25 or 29 will see no difference. For UAS/RPAS of Complexity Levels I there will be no change to the quantitative safety objectives from their manned equivalent.

Table 39 illustrates the approach adopted for a range of manned aircraft and the equivalent UAS/RPAS. Note that the column titled 'Number of Potential Failure Conditions' (shown in grey), which is key in differentiating between manned aircraft and UAS/RPAS.

Table 39. Derived Quantitative Systems Availability and Integrity Required to Maintain Safe Flight and Landing (excluding loss of safe separation) [JARUS AMC RPAS.1309. Issue 2, November 2015]

Aircraft Type	**UAS/RPAS Complexity Level**	**Accident Rate (pfh) All Causes**	**% Due to Systems** (10%)	**No. of Potential Catastrophic Failure Conditions**	**Probability of a Catastrophic Failure Condition (pfh)**
Manned CS-25		1x10-6	1x10-1	100 (10-2)	1x10-9
RPAS CS-25	N/A	1x10-6	1x10-1	100 (10-2)	1x10-9
Manned CS-29		1x10-6	1x10-1	100 (10-2)	1x10-9
RPAS CS-29	N/A	1x10-6	1x10-1	100 (10-2)	1x10-9
Manned CS-23 Class I		1x10-4	1x10-1	10 (10-1)	1x10-6
RPAS CS-23 Class I	I	1x10-4	1x10-1	10 (10-1)	1x10-6
	II	1x10-4	1x10-1	100 (10-2)	1x10-7
Manned CS-23 Class II		1x10-5	1x10-1	10 (10-1)	1x10-7
RPAS CS-23 Class II	I	1x10-5	1x10-1	10 (10-1)	1x10-7
	II	1x10-5	1x10-1	100 (10-2)	1x10-8
Manned CS-23 Class III		1x10-6	1x10-1	10 (10-1)	1x10-8
RPAS CS-23 Class III	I	1x10-6	1x10-1	10 (10-1)	1x10-8
	II	1x10-6	1x10-1	100 (10-2)	1x10-9
Manned CS-23 Class IV		1x10-6	1x10-1	100 (10-2)	1x10-9
RPAS CS-23 Class IV	N/A	1x10-6	1x10-1	10 (10-2)	1x10-9
Manned CS-27		1x10-4	No quantitative criteria defined		
RPAS CS-27	I	1x10-4	No quantitative criteria defined		
	II	1x10-4			
Manned CS-VLA		No data	No quantitative criteria defined		
RPAS CS-LUAS	I	1x10-4	1x10-1	10 (10-1)	1x10-6
	II	1x10-4	1x10-1	100 (10-2)	1x10-7
Manned CS-VLR		No data	No quantitative criteria defined		
RPAS CS-LURS	I	1x10-4	1x10-1	10 (10-1)	1x10-6
	II	1x10-4	1x10-1	100 (10-2)	1x10-7

5.3.5 Certification Targets

The full classification of failure conditions, including Design Assurance Levels (DALs) and probability targets to maintain safe flight and landing for each UAS/RPAS class and complexity level, is presented in Table 40 below.

Table 40. Relationship among Aircraft Classes, Probabilities, Severity of Failure Conditions and Software and Complex hardware DALs, required to maintain safe flight and landing to that of equivalent manned aircraft (excluding loss of safe separation) [JARUS AMC RPAS.1309. Issue 2, November 2015]

Classification of failure Conditions				
No Safety Effect	**Minor**	**Major**	**Hazardous**	**Catastrophic**
Allowable Qualitative Probability				
No Probability Requirement	**Probable**	**Remote**	**Extremely Remote**	**Improbable Extremely**

Classes of RPAS	**Complexity Levels (CL)**	**Allowable Quantitative Probabilities and DAL (Note 2)**				
RPAS-25	**N/A**	See AMC 25.1309				
RPAS-29	**N/A**	See AC 29-2C, AC 29.1309				
RPAS-23 Class I (SRE under 6,000lbs)	**I**	No probability/DAL Requirement	**<10-3** P=D, S=D (Notes 1 & 4)	**<10-4** P=D, S=D (Notes 1 & 4)	**<10-5** P=C, S=D (Note 4)	**<10-6** P=C, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**<10-3** DAL=D (Note 1)	**<10-5** DAL=C (Note 1)	**<10-6** DAL=C	**<10-7** DAL=B (Note 3)
RPAS-23 Class II (MRE, STE or MTE under 6000lbs)	**I**	No probability/DAL Requirement	**<10-3** P=D, S=D (Notes 1 & 4)	**<10-5** P=C, S=D (Notes 1 & 4)	**<10-6** P=C, S=C (Notes 4)	**<10-7** P=B, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**<10-3** DAL=D (Note 1)	**<10-5** DAL=C (Note 1)	**<10-7** DAL=B	**<10-8** DAL=B (Note 3)
RPAS-23 Class III (SRE, MRE, STE or MTE > 6000lbs)	**I**	No probability/DAL Requirement	**<10-3** P=D, S=D (Notes 1 & 4)	**<10-5** P=C, S=D (Notes 1 & 4)	**<10-7** P=B, S=C (Notes 4)	**<10-8** P=B, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**<10-3** DAL=D (Note 1)	**<10-5** DAL=C (Note 1)	**<10-7** DAL=B	**<10-9** DAL=A (Note 3)
RPAS-23 Class IV	**N/A**	See AC 23.1309-1E				
CS-LUAS, or **CS-LURS**	**I** (Note 6)	No probability/DAL Requirement	**<10-3** P=D, S=D (Notes 1 & 4)	**<10-4** P=D, S=D (Notes 1 & 4)	**<10-5** P=C, S=D (Note 4)	**<10-6** P=C, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**<10-3** DAL=D (Note 1)	**<10-5** DAL=C (Note 1)	**<10-6** DAL= C	**<10-7** DAL=B (Note 3)
RPAS-27 (Note 5)	**I**	No probability/DAL Requirement	**<10-3** P=D, S=D (Notes 1 & 4)	**<10-4** P=D, S=D (Notes 1 & 4)	**<10-5** P=C, S=C (Note 4)	**<10-6** P=C, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**<10-3** DAL=D (Note 1)	**<10-5** DAL=C (Note 1)	**<10-6** DAL=C	**<10-7** DAL=B (Note 3)

Notes pertaining to Table 40

Note 1: Numerical values indicate an order of probability range and are provided here as a reference. The applicant is usually not required to perform a quantitative analysis for minor and major failure conditions.
Note 2: The symbology denotes the typical DALs for primary systems (P) and secondary system (S). For example, DAL Level A on primary system is noted by P=A.
Note 3: At RPAS functional level, no single failure will result in a catastrophic failure condition.
Note 4: Secondary system (S) may not be required to meet probability goals. If installed, S should meet stated requirements.
Note 5: These values are not currently aligned with AC 27-1B. Current certification practice applied to manned rotorcraft may change these values depending on the intended type of operation (e.g. VFR/IFR) and the type-certification basis of the rotorcraft.
Note 6: Irrespective of the probability and DAL levels assigned, a CL I RPAS that requires real-time communication with the remote pilot station to maintain basic vehicle stability and control is unlikely to be granted type-certification.

6. DERIVATION OF HIGH-LEVEL SAFETY REQUIREMENTS

6.1 RAIL: GENERIC PROCESS FOR DERIVATION OF SAFETY REQUIREMENTS FOR RAILWAY SAFETY-RELATED SYSTEMS

A generic process for derivation of safety requirements starts from system definition which is followed by hazard identification and risk analysis – see Fig. 40. It applies to a new system.

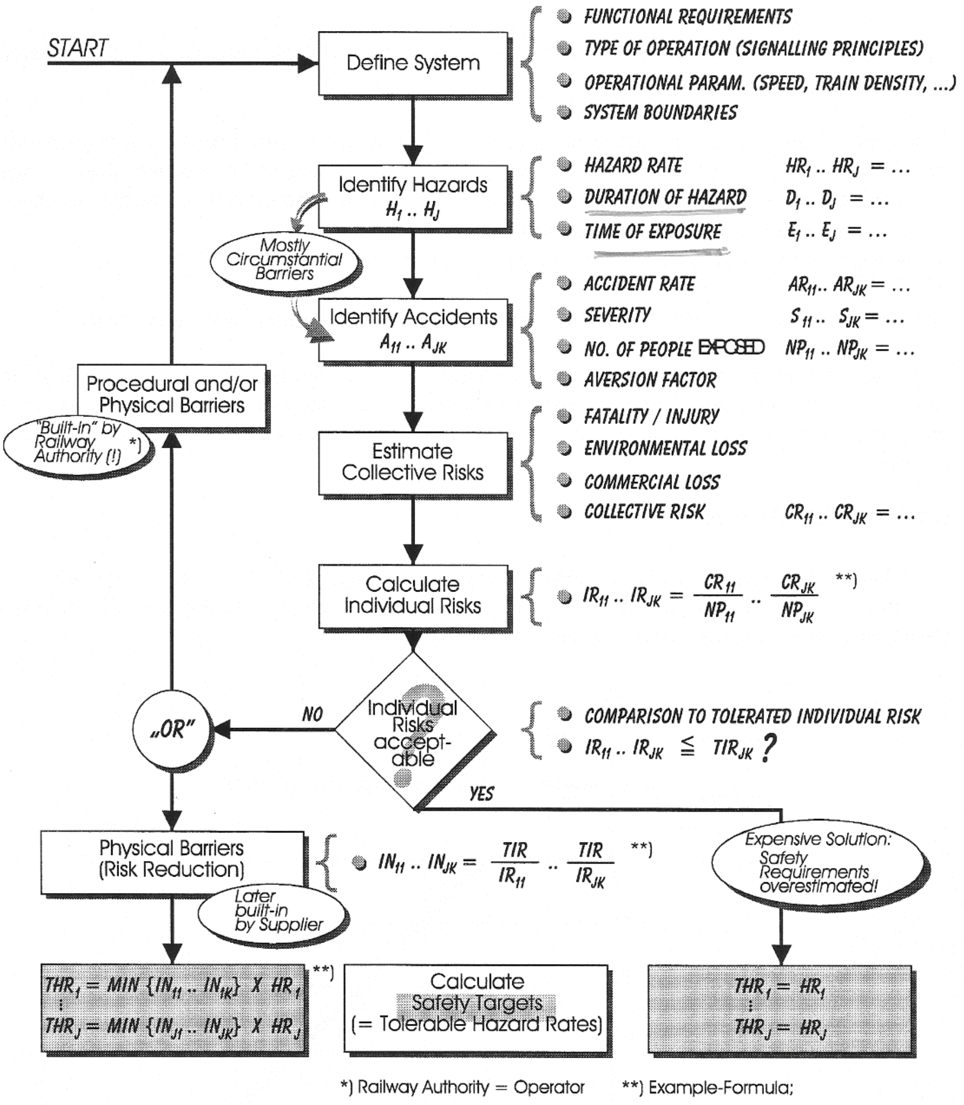

START
Define System
FUNCTIONAL REQUIREMENTS
TYPE OF OPERATION (SIGNALLING PRINCIPLES)
OPERATIONAL PARAM. (SPEED, TRAIN DENSITY, ...)
SYSTEM BOUNDARIES
Identify Hazards $H_1 .. H_J$
HAZARD RATE $HR_1 .. HR_J = ...$
DURATION OF HAZARD $D_1 .. D_J = ...$
TIME OF EXPOSURE $E_1 .. E_J = ...$
Mostly Circumstantial Barriers
Identify Accidents $A_{11} .. A_{JK}$
ACCIDENT RATE $AR_{11} .. AR_{JK} = ...$
SEVERITY $S_{11} .. S_{JK} = ...$
NO. OF PEOPLE EXPOSED $NP_{11} .. NP_{JK} = ...$
AVERSION FACTOR
Procedural and/or Physical Barriers
"Built-In" by Railway Authority (!) *)
Estimate Collective Risks
FATALITY / INJURY
ENVIRONMENTAL LOSS
COMMERCIAL LOSS
COLLECTIVE RISK $CR_{11} .. CR_{JK} = ...$
Calculate Individual Risks
$IR_{11} .. IR_{JK} = \frac{CR_{11}}{NP_{11}} .. \frac{CR_{JK}}{NP_{JK}}$ **)
Individual Risks accept-able
NO
YES
„OR"
COMPARISON TO TOLERATED INDIVIDUAL RISK
$IR_{11} .. IR_{JK} \leqq TIR_{JK}$?
Physical Barriers (Risk Reduction)
$IN_{11} .. IN_{JK} = \frac{TIR}{IR_{11}} .. \frac{TIR}{IR_{JK}}$ **)
Later built-in by Supplier
Expensive Solution: Safety Requirements overestimated!
$THR_1 = MIN\{IN_{11} .. IN_{1K}\} \times HR_1$ **)
$THR_J = MIN\{IN_{J1} .. IN_{JK}\} \times HR_J$
Calculate Safety Targets (= Tolerable Hazard Rates)
$THR_1 = HR_1$
$THR_J = HR_J$
*) Railway Authority = Operator
**) Example-Formula;

Figure 40. Example of risk analysis process for safety requirements derivation [19]

However, in case of HELMET we have already identified the purpose of high-accuracy and high-integrity position determination based on GNSS and therefore it is not necessary to start from the scratch regarding safety requirements specification. Thus, we can directly focus our attention on ERTMS/ETCS as it is defined in HELMET operational scenarios for rail and for completeness' sake describe a way how high-level safety target for ERTMS/ETCS was derived.

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 (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.

6.2 AUTO: DERIVATION OF HIGH-LEVEL SAFETY REQUIREMENTS FOR SELF-DRIVING CARS

Derivation of high-level safety requirements for SDCs is based on the harmonised risk acceptance approach. The harmonisation of risk acceptance is a way to achieve widely acceptable requirements for SDCs. In HELMET, the proposed methodology for safety requirements derivation consists of following 7 steps:

1. Determination of societal needs for SDCs safety compared to generally acceptable safety levels of additional means of transport. To answer to question: >> How much safe should driverless vehicles be to be accepted by society? <<;
2. Use of real safety performances selected as the safest means of transport (i.e. rail and aviation) for determination of safety targets for SDCs;
3. Selection of a suitable travel safety performance measure (time vs. km/miles);
4. Transition from fatality measures in transport (per 1 hour or km) to car crash (per 1 hour) and subsequent (average) system Probability of Failure per 1 hour (PF);
5. Consideration of impacts and potential safety gap(s) related to determination of safety requirements according to the automotive functional safety standard ISO 26262. Application of quantitative approach for high-level system requirements specification for SDCs is proposed in parallel to the ISO 26262 ASIL qualitative approach;
6. Application of suitable Risk Acceptance Principles (RAP) and Risk Acceptance Criteria (RAC) for the target Probability of Failure (per 1 hour) harmonisation;
7. Allocation of the target system PF to SDC subsystems including position determination/ localization GNSS based.

Explanation of steps 1-6 is performed in Sections 6 and 8 of this document (D2.2), while the PF allocation to SDC subsystems will be described in D2.3.

6.2.1 Derivation of high-level safety requirements in aviation

This section briefly outlines how aviation Target Level of Safety (TLS) and integrity and continuity requirements for aviation GNSS SoL service were derived. It is mentioned here because derivation of safety requirements for SDCs described in [20] partially follows the aviation approach. It is explained why this approach cannot be used for derivation of safety requirements for SDCs.

Allocation of aviation TLS to GNSS integrity and continuity risks

Requirements for GNSS integrity and continuity risks were derived from the Target Level of Safety (TLS) [21] as evident in Fig. 41. The TLS in aviation is expressed in the units of hull losses per aircraft flight hour. The TLS is derived from the ICAO historical statistical data of commercial airplane accidents in a given period of time. The average hull loss per mission has been expressed as 431 hull loss accidents / 230 million flights = 1.87x10^{-6}/1 flight. After the TLS improvement (e.g. due to air traffic increasing), the value of 1.5 x10^{-7} per mission (i.e. per 1.5 hour) was set. Finally, the risk of hull loss for individual operations was allocated in terms of probability per duration operation. For example, the risk (probability) of 1 x10^{-8} was allocated from the total TLS to final approach with the average duration of 150 s. Therefore, the integrity and continuity risks, which were derived from the risks for individual flight operations, were also expressed in terms of probability per operation.

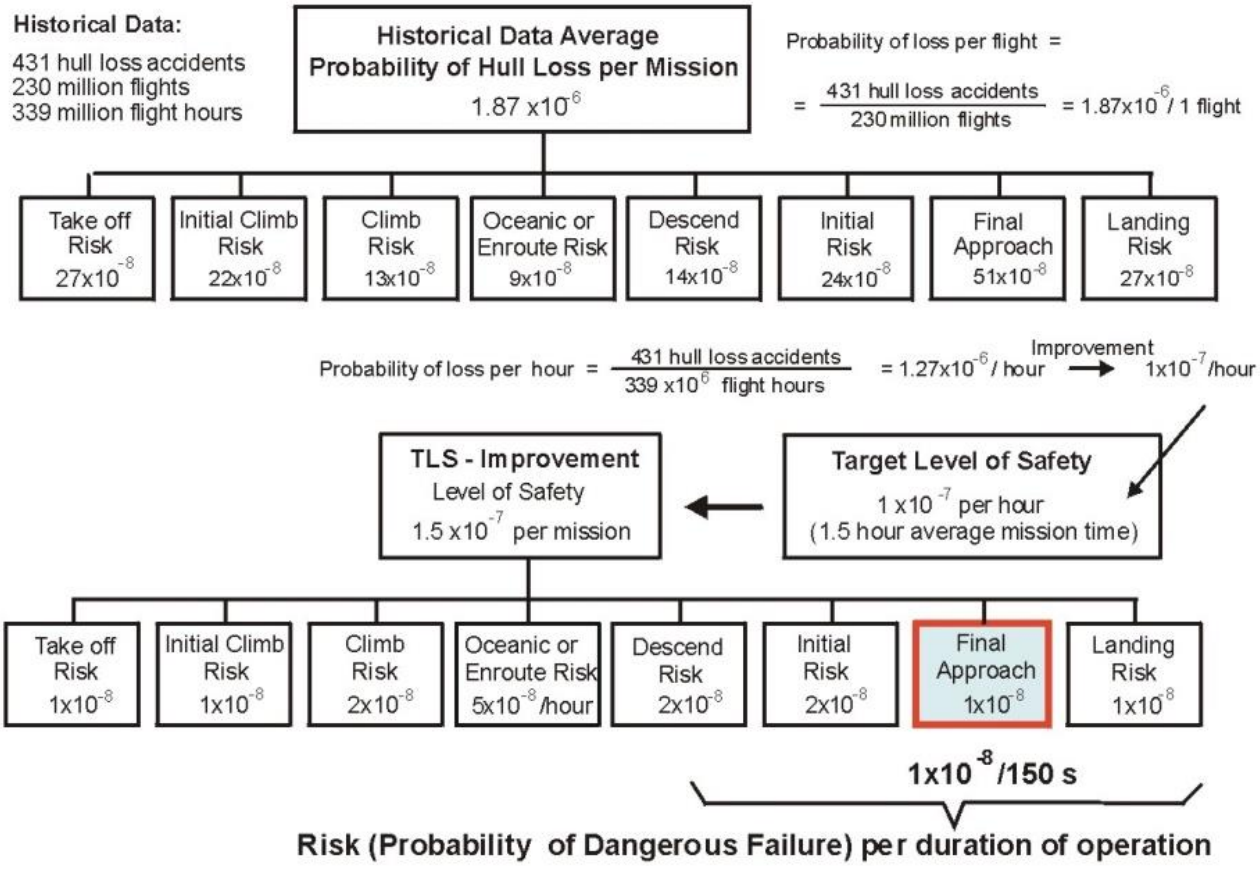


Figure 41. Target Level of Safety for GNSS in Aviation

The only difference is that the integrity risk (latent failure) covers the whole operation while the continuity risk (detected failure) covers the most critical part of the safety operation. Thus, for the above mentioned final approach the integrity risk is defined per 150 s and the continuity risk per 15 s (last 15 s before a decision height is the most critical part of the operation since pilot must make decision if to continue in landing or to initiate missed approach).

GNSS SIS integrity and continuity risks requirements were derived accordingly to the fault tree analysis from allocated risk for a given operation [21]. The following considerations are related to final approach and start from risk of 1 x10^{-8} / 150 s, as evident from diagram in Fig. 42. The fact that not every hazardous event will lead to an accident gives the reduction of the initial TLS with ratio of 1:10. The corresponding risk value of 1 x10^{-7} / approach is equally sub-allocated among the total system integrity and continuity risks.

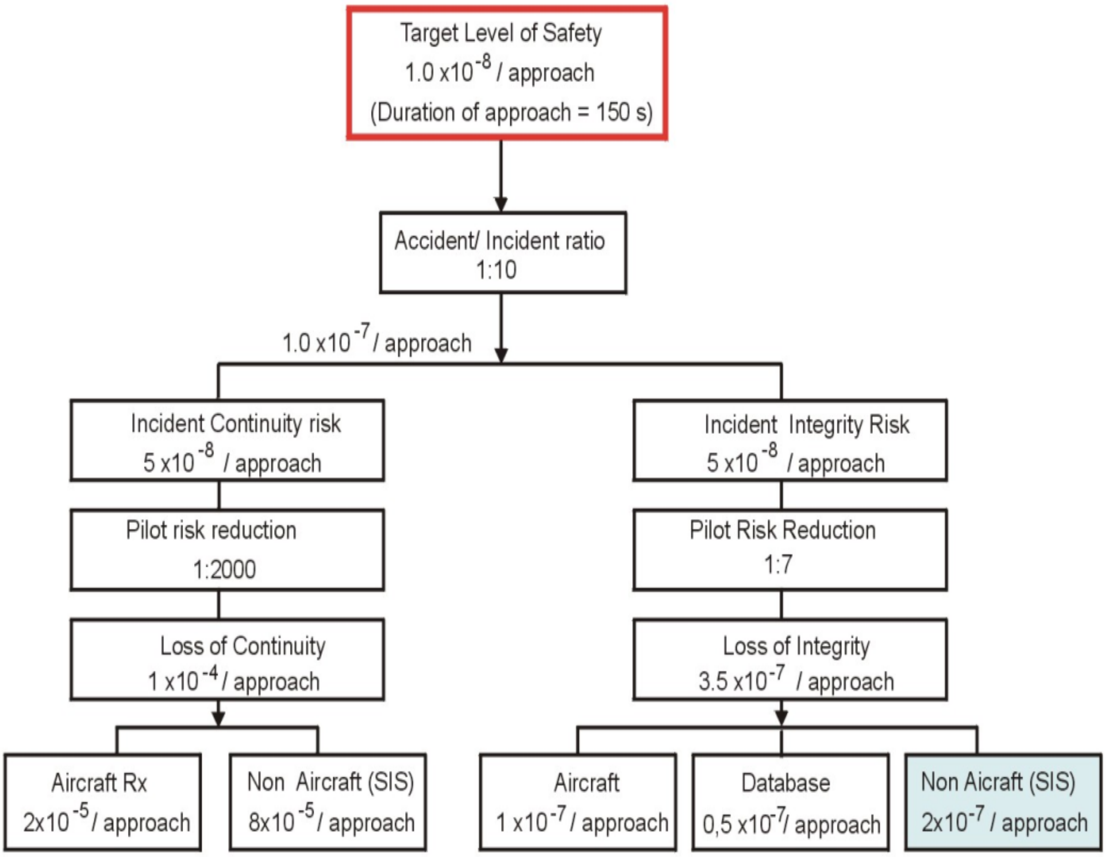


Figure 42. Aviation Target Level of Safety allocation to integrity and continuity risks

The integrity and continuity risks are subsequently reduced by the pilot [21]. Finally, the loss of integrity of 3.5 x10^{-7} / 150 s is sub-allocated among the SIS integrity risk IR_{SIS} = 2 x10^{-7} / 150 s, the integrity risk of GNSS receiver on airplane IR_{Rx} = 5 x10^{-8} / 150 s and the database integrity risk IR_{DBS} = 1 x10^{-7} / 150 s. Similarly, the loss of continuity CR = 1 x10^{-5} / 15 s is sub-allocated among the SIS continuity risk CR_{SIS} = 8 x10^{-6} / 15 s and the continuity risk of onboard GNSS receiver CR_{Rx} = 2 x10^{-6} / 15 s. Note: CR_{SIS} = 8 x10^{-6} / 15 s = 8 x10^{-5} / 150 s (i.e. per approach).
Although this procedure has been used to derive GNSS Safety-of-Life service requirements for aviation safety operations, it is not suitable for specifying safety requirements for self-driving cars.

There are two reasons for it. First, aviation Target Level of Safety (TSL) is not expressed by fatalities of passengers, but only through number of hull losses. It is not evident from the statistics, how many people died in average during a hull accident. Second, TLS is derived for the most demanding safety operations (approach, landing) per duration of operation and not per 1 hour, as it is common in land safety-related systems. Specification of duration of operation is not applicable to SDCs.

Derivation of catastrophic failure rate target in aviation

Another approach for derivation of aviation risk target is described in [22]. Historical evidence based on statistical data indicates that a risk of serious accident due to operational and airframe related causes happen approximately 1 per million flights (1e-6 per flight hour). This risk of accident approximately corresponds to the statistical hull loss data mentioned in previous section. 10% of this risk is allocated to an aircraft system failure. A rate of the aircraft system failure then is 1e-7 per flight hour. Further it is assumed that there are about 100 potential failure states in an airplane which would prevent continued safe flight and landing. This leads to a maximum tolerable frequency of 1e-9 per flight hour per catastrophic failure state. Catastrophic failure state can cause loss of multiple lives.

Although this procedure for derivation of the aviation target failure rate is quite straightforward, it would be hardly applicable for derivation of safety requirements for self-driving cars because it doesn't reflects individual risk fatality data, which is necessary for derivation of safety requirements for land safety-related systems (rail, industry). Airplane hull (car) loss as a measure of risk is not sufficient.

Classification of catastrophic and hazardous/ critical failures

System safety requirements derivation in aviation and on railway usually takes into account the following failure consequences/ function failures:

Aviation:

- Catastrophic failure consequences resulting in multiple fatalities usually with loss of plane (thus impacting all occupants) should not exceed an occurrence of 1e-9/ flight hour. Failure consequences are extremely improbable in this case.
- Hazardous failure consequences reducing capability of air-plane, large reduction in safety margins, physical distress or excessive workload on crew and impacting a relatively small number of occupants should not exceed an occurrence of 1e-7/ flight hour. Failure consequences are extremely remote in this case.

Railways:

- Failures of functions having possibility to affect whole train (i.e. all occupants) and resulting in fatalities should not exceed an occurrence of 1–9 / 1 hour. Failure consequences are catastrophic in this case.
- Failures of functions having possibility to affect a limited area of train (thus a relatively small number of occupants) and resulting in at least one fatality should not exceed an occurrence of 1e-7 / 1 hour. Failure consequences are classified as critical in this case.

Catastrophic safety risks are generally controlled with safety-related systems compliant with SIL 4 and critical safety risks by systems compliant with SIL 3. It is evident that failure occurrences and consequences in aviation and on railways are classified in a very similar way. Thus it seems the failure consequences classification can be also utilised for specification of safety requirements for SDCs.

Application of Common Safety Method Design Targets (CSM-DT) [9] based on the above failure classification and originally developed for harmonised requirements specification of railway safety-related systems is proposed in this document below for harmonisation of safety requirements of SDCs.

6.2.2 Travel safety measures: Time versus Distance

In railway sector Target Individual Risk of fatality (TIR) and also resulting tolerable rate or probability of failure are specified per 1 hour. It is because it would be very difficult or impossible to specify and classify duration of different railway operations (such as shunting, ride between stations, etc.). The same applies to cars.

A different situation is in the civil aviation where such approach it is possible. For example, it is possible to estimate duration of CAT I precision approach, landing operations CAT II, CAT IIIa, CAT IIIb, etc. – see Fig 43. It is the reason why aviation requirements for different GNSS SoL service (SBAS, LAAS, etc.) were defined per duration of operations. For less dangerous aviation operations (than e.g. landing) like En-route or Terminal operations are GNSS integrity measures also traditionally scaled by 1 one hour, because it would be difficult to estimate a duration of such operations.

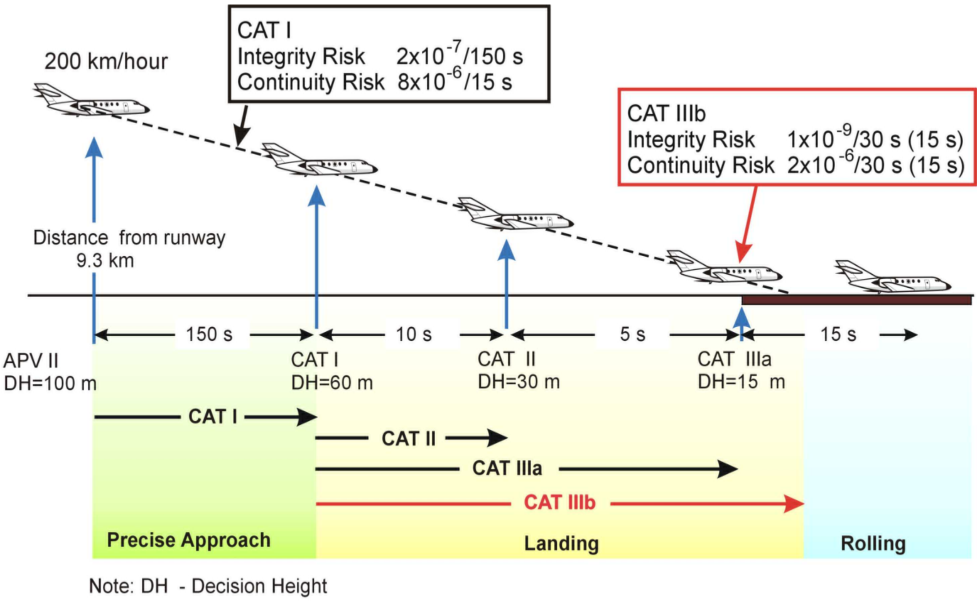


Figure 43. Duration of operation for Integrity Risk specification

One of the above-mentioned Risk Acceptance Principles (RAP)/ Criteria (RAC) called Minimum Endogenous Mortality (MEM), which is also recommended in the railway CENELEC standard EN 50126 [5], expresses acceptable individual mortality of persons per time (e.g. 1 year or 1 hour).

It is more common to evaluate safety of persons per time unit (1 year or 1 hour) than per a distance travelled, although safety of travel is being also statistically expressed per km or mile. Therefore, derivation of safety requirements should also start from fatality risk per 1 hour. For example, the road Traffic Fatality Rate (TFR) mentioned in Section 1 is also measured per time (year) and not per km/ miles travelled - see also [23]. It can be demonstrated by the following example. Let's derive THR for safety-related functions to be performed by a technical system from the socially acceptable Target Individual Risk of fatality (TIR), which is defined per time – see Fig. 44.

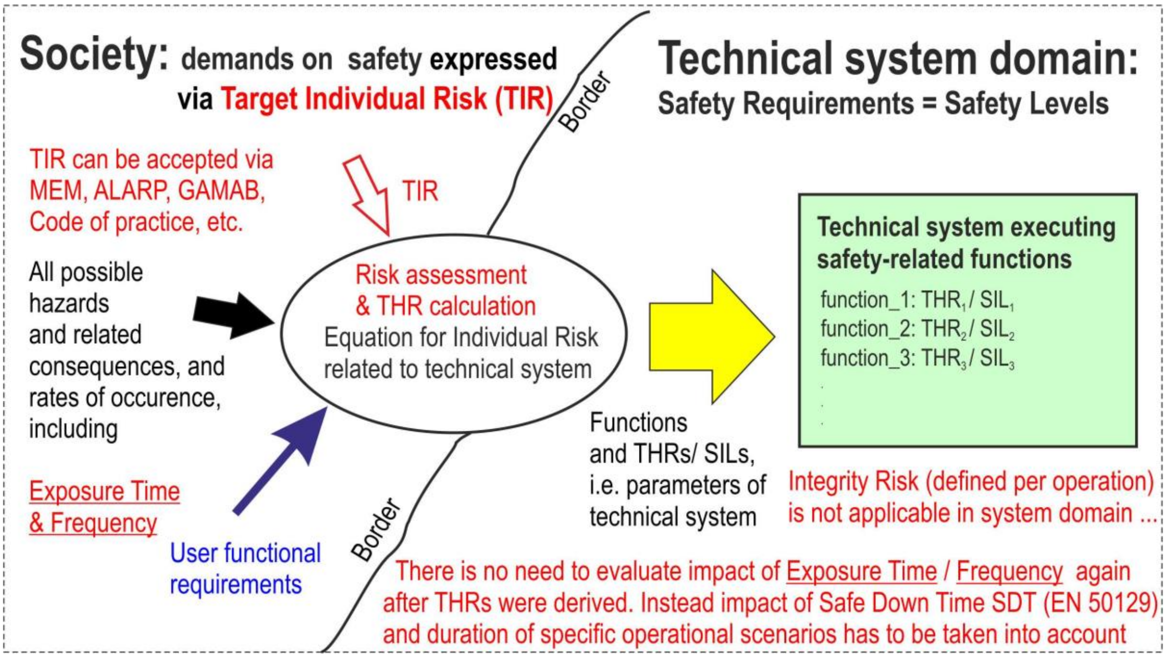

Society: demands on safety expressed via Target Individual Risk (TIR)
Border
Technical system domain:
Safety Requirements = Safety Levels
TIR can be accepted via MEM, ALARP, GAMAB, Code of practice, etc.
TIR
All possible hazards and related consequences, and rates of occurence, including
Risk assessment & THR calculation
Equation for Individual Risk related to technical system
Technical system executing safety-related functions
function_1: THR1 / SIL1
function_2: THR2 / SIL2
function_3: THR3 / SIL3
Exposure Time & Frequency
User functional requirements
Functions and THRs/ SILs, i.e. parameters of technical system
Integrity Risk (defined per operation) is not applicable in system domain ...
Border
There is no need to evaluate impact of Exposure Time / Frequency again after THRs were derived. Instead impact of Safe Down Time SDT (EN 50129) and duration of specific operational scenarios has to be taken into account

Figure 44. Transition from Target Individual Risk to THRs of safety-related functions to be implemented by technical system

To solve the problem, the equation for Individual Risk of Fatality can be used for HR (THR) calculation [19]

$$IRF_i = \sum_{all\_hazards\_H_j} \overset{\text{Exposure frequency}}{N_i} \left[\underset{\text{THR/ SIL for a given hazard/ safety function}}{HR_j} \cdot (D_j + \overset{\text{Exposure time}}{E_{ij}}) \cdot \sum C_j^k \cdot F_i^k \right] \tag{1}$$

where *IRF*IRF_i - individual risk of fatality (per time) for particular *i*-th user of the system, N_i - individual usage profile (number of usages per time), HR_j - hazard rate of safety function protecting against hazard H_j, D_j - duration of hazardous of failure in system, E_{ij} - exposure time for individual user (i) and hazard (j) , C_{jk} – external risk reduction probability (e.g. by driver) and F_{ik} – probability of fatality (of e.g. driver) for *k*-th accident. The sum *ΣC*$_{jk}$**F*$_{ik}$ represents the risk matrix for user / driver of the system [-].

If *IRF*$_i$ is limited by *TIR*, then the hazard rate for the individual safety-related function becomes the Tolerable Hazard Rate *THR*. In case that only one hazard is considered, then (1) can be rewritten as

$$IRF_i = N_i \left[THR_1 \cdot (D_1 + E_{i1}) \cdot \sum_{accidents\, A_k} C_{1k} \cdot F_{ik} \right] \leq TIR \qquad (2)$$

THR per 1 hour is obtained from equation (2). Probability of failure per 1 hour is required for safety-related systems with high-demand or continuous mode of operation (according to IEC 61508). The high-demand / continuous mode of operation is also considered for THR.

It is evident from the example that THR per 1 hour can be directly calculated from the IRF and TIR, also measured per unit time. TIR expressed per travelled distance would only complicate the THR solution.

Since the average Probability of Failure (PH) per 1 hour as a measure of automotive safety shall be derived, it is recommended in HELMET to start the PH derivation from the selected safety performance of travel (rail and airline) expressed per 1 hour as well – not per km/miles travelled. A related safety risk measured per time unit (1 hour) is closer to risk acceptance criterium like MEM.

6.2.3 Risk acceptance principles and criteria on European railways

Railway stakeholders have to manage safely all changes of the European railway system – including GNSS positioning, hybrid GNSS positioning and other sensors integration with ERTMS. Common Safety Method for Risk evaluation and Assessment (CSM-RA) must be used according to European railway regulations if a safety-related change in a system is significant – see Fig. 45 [8]. It is also the case of application of GNSS for Virtual Balise detection within ERTMS.

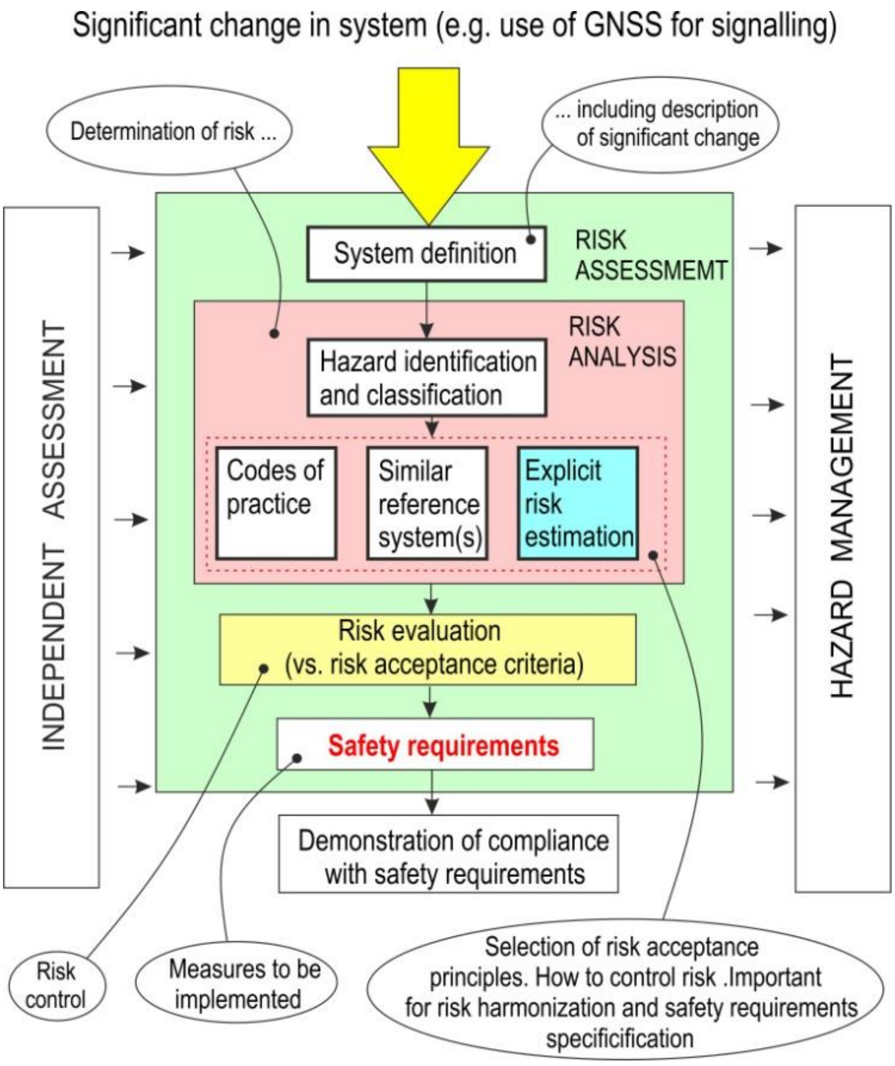

Significant change in system (e.g. use of GNSS for signalling)
Determination of risk ...
... including description of significant change
System definition
RISK ASSESSMEMT
RISK ANALYSIS
Hazard identification and classification
Codes of practice
Similar reference system(s)
Explicit risk estimation
Risk evaluation (vs. risk acceptance criteria)
Safety requirements
Demonstration of compliance with safety requirements
INDEPENDENT ASSESSMENT
HAZARD MANAGEMENT
Risk control
Measures to be implemented
Selection of risk acceptance principles. How to control risk .Important for risk harmonization and safety requirements specificification

Figure 45. Common Safety Method for risk evaluation and Assessment (CSM-RA)

CSM-RA supports risk harmonization and also harmonised safety requirements derivation. Harmonisation of safety requirements is also important task for SDCs. In next sections there is outlined a way how safety requirements for SDCs could be harmonised.

6.2.4 Risk harmonization of railway technical systems

Harmonization of risk acceptance and safety requirements specification in land transport like rail or road is critical not only from viewpoint of required safety, but also from the required system efficiency. Railways have (compared to automated cars) a long-term experience with harmonisation of risk acceptance including the whole certification and safety approval process for developed Technical Systems (TS). It is because TS shall be safe as it is required by society – but TS must not be exceedingly safe because they would be too expensive, and nobody would use them. European railway sector utilises the above mentioned CSM-RA for harmonisation of risk acceptance. The harmonization and mutual recognition of safety requirements is performed via Risk Acceptance Principles (RAP) and Risk Acceptance Criteria (RAC) [8].

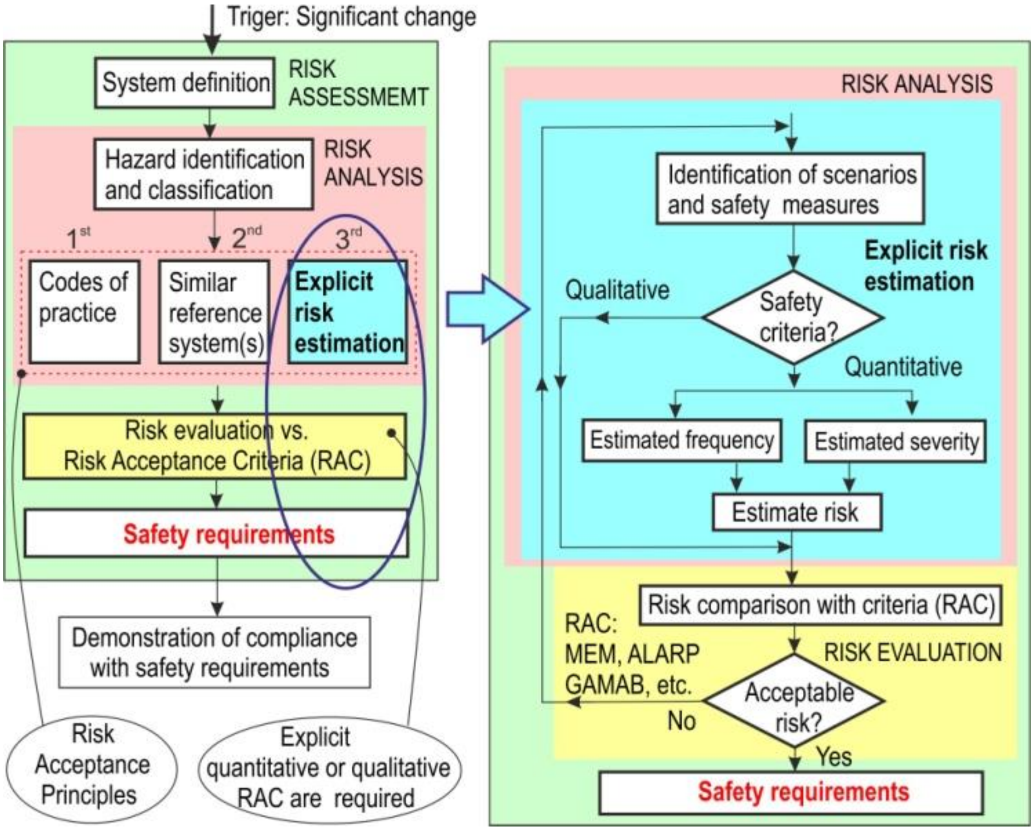

Triger: Significant change
System definition
RISK ASSESSMEMT
Hazard identification and classification
RISK ANALYSIS
1st
2nd
3rd
Codes of practice
Similar reference system(s)
Explicit risk estimation
Risk evaluation vs. Risk Acceptance Criteria (RAC)
Safety requirements
Demonstration of compliance with safety requirements
Risk Acceptance Principles
Explicit quantitative or qualitative RAC are required
RISK ANALYSIS
Identification of scenarios and safety measures
Explicit risk estimation
Qualitative
Safety criteria?
Quantitative
Estimated frequency
Estimated severity
Estimate risk
Risk comparison with criteria (RAC)
RAC:
MEM, ALARP
GAMAB, etc.
RISK EVALUATION
Acceptable risk?
No
Yes
Safety requirements

Figure 46. Explicit risk estimation and evaluation within CSM

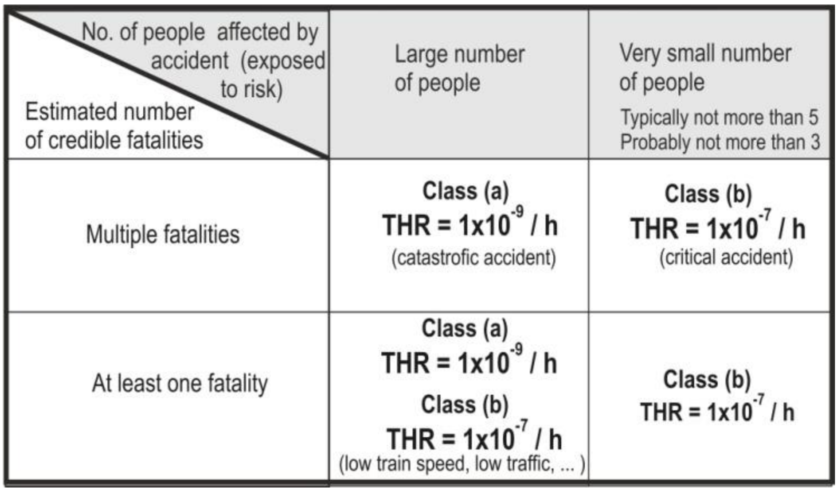
Widely acceptable Codes of Practice (CoP) such as ERTMS TSIs, CENELEC standards, etc., used as RAP enable to harmonise risk and thus railway safety requirements across Europe – see Fig. 46. These CoP have been elaborated based on a long-term experience with designing of railway safety-related systems. Reference systems can be used as Risk Acceptance Principles in a very similar way as Codes of Practice because a reference system is a system that has been proven in practice to have an acceptable safety level. Both Code of Practice and similar Reference Systems used as Risk Acceptance Principles can be also considered at the same time as Risk Acceptance Criteria.

If enough experience with a specific safety system design and assessment is missing, which is also the case of high-safety integrity steering systems for SDCs, then explicit risk estimation as RAP must be applied. Then specific railway Risk Acceptance Criteria are also needed – e.g. MEM, ALARP, GAMAB, etc. [5]. Problem is that these RACs are not harmonised in Europe. Thus, the related risk cannot be acceptable in all EU countries. It means that resulting safety requirements for TS cannot not be harmonised as well. Widely acceptable harmonised RAC are needed, as it is outlined in next Section.

6.2.5 Design safety targets as harmonised risk acceptance criteria

In rail domain it was obviously needed to ensure a mutual recognition of risk assessment of Technical Systems (TS) when also the explicit risk estimation as 3rd Risk Acceptance Principle is used.

Table 41. Harmonised CSM Design Targets for railway technical systems



No. of people affected by accident (exposed to risk) Estimated number of credible fatalities	Large number of people	Very small number of people Typically not more than 5 Probably not more than 3
Multiple fatalities	Class (a) THR = 1x10^{-9} / h (catastrofic accident)	Class (b) THR = 1x10^{-7} / h (critical accident)
At least one fatality	Class (a) THR = 1x10^{-9} / h Class (b) THR = 1x10^{-7} / h (low train speed, low traffic, ...)	Class (b) THR = 1x10^{-7} / h

In order to harmonise safety requirements for design of E/E/PE (Electric/ Electronic/ Programmable Electronic Safety-related Systems) as TS, CSM – Design Targets (CSM-DT) [9] have been introduced by ERA (EU Agency for Railways) – see Table 41. The goal of the harmonised CSM-DT is to assure that designed TS will be safe enough, as it is required by society. At the same time TS will not be safer than actually needed.

CSM-DT was derived on basis of current experience and best practice with railway safety-related system design. CSM-DT represents harmonised functional safety requirements for TS, i.e. safety levels. CSM-DT can be used as quantitative safety requirements for random HW failures of E/E/EP technical systems. And how can be the harmonised design targets used? Hazard rate of a specific functional hazardous failure of a technical system should be estimated first. The use of techniques such as FMECA or fault tree analysis (FTA) can involve for this purpose. The estimated hazard rate is then compared with the required CSM-DT. If the compliance of TS with the CSM-DT is not assured, then changes in safety design must be performed.

For example, in case of ERTMS with Virtual Balises (VBs) detected by GNSS, harmonised Risk Acceptance Principles (RAP) and harmonised Risk Acceptance Criteria (RAC) in the form of e.g. ERTMS TSI (Technical Specifications for Interoperability) can be utilised to specify safety requirements for VB detection. In case that any harmonised RAP (e.g. Code of Practice or similar Reference System) is not available, then it is recommended to use harmonised CSM-DT.

A long-term experience with high-safety integrity E/E/EP systems in the field of automated car driving (compared to rail) is missing. There are neither available harmonised Risk Acceptance Principles (RAP) and harmonised Risk Acceptance Criteria (RAC), which could be used for specification of widely acceptable high-level safety requirements for self-driving cars. Due to this reason railway CSM-DT approach is proposed here for specification of safety requirements in the automotive sector – see Fig. 47.

Note: Railway CSM Design Targets well comply with the aviation failure classification described in Section 6.2.1 of this report.

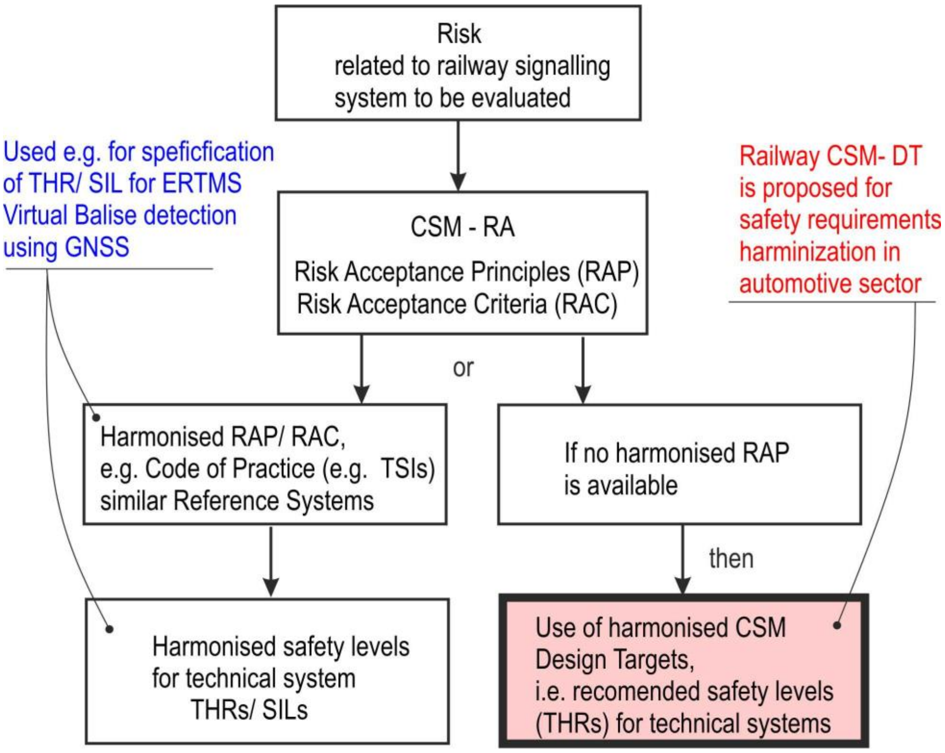


Figure 47. Harmonised approach for risk evaluation and determination of high safety integrity requirements for railway technical systems

The quantitative railway CSM-DT are proposed in this HELMET report as a complement to the qualitative ISO 26262 ASIL determination approach in order to fill-in the identified safety gap disabling direct application of socially acceptable individual risk of fatality for derivation of safety requirements for automated driving systems – see below.

6.2.6 Derivation of system safety requirements according to functional safety standards (IEC 61508, CENELEC and ISO 26262)

This section compares procedures for derivation of system safety requirements according to following safety standards: IEC 61508 (functional safety generally), railway CENELEC standards (EN 50126 -RAMS)/ EN 50129 (railway signalling) and ISO 26262 (automobile functional safety).

IEC 61508

IEC 61508 generally assumes that a safety system consists of EUC (Equipment Under Control) and EUC safety-related system. Safety functions with Continuous or High Demand modes of operations are considered, since there are also used in case of railway signalling or control system of self-driving cars, where EUC is tightly integrated with EUC safety-related system. Probability of failure per 1 hour (PFH) is determined quantitatively for safety-related function (s) first, e.g. using equation (1) from the acceptable Target Individual Risk (TIR) and then the corresponding Safety Integrity Level (SIL), which is qualitative integrity measure, is assigned to the specified PFH(s). Note: Automotive functional safety standard IEC 26262 doesn’t know notion Safety Integrity. Term Robustness instead of Safety Integrity is used in IEC 26262.

CENELEC EN 50126 & EN 50129

Railway CENELEC safety standards are focused on a railway-safety related system. Risk linked with the system is evaluated in view of identified hazards for a given operational scenario. It means that Hazardous Event is considered within the Hazard Analysis and Risk Assessment (HARA). This concept is also in line with ISO 26262. Since CENELEC standards represent a modification of the IEC 61508 for the railway safety systems, then the applied procedure for derivation of the quantitative tolerable measure of failure occurrence, i.e. Tolerable Hazard Rate (THR), can be similar of that used for PFH determination according to IEC 61508 – e.g. according to eqn. (1). At the beginning of the hazard analysis and risk assessment, when there is not enough information about the system to be designed, a qualitative approach for specification of system safety requirements is used.

In many cases the above generic explicit risk analysis approach for THR/SIL derivation can be replaced with widely acceptable (harmonised) Risk Acceptance Principles such as Codes of Practice (TSIs, similar reference systems) or also harmonised CSM – Design targets. These widely used approaches for specification of system safety requirements are based on long-term railway experience with safety systems. It is also the case of ERTMS based on GNSS, where ERTMS TSI and related technical subsets containing safety requirements for baseline ERTMS have been used for specification of safety requirements for virtual balises and GNSS.

ISO 26262

The process of safety requirements determination for the vehicle Item /System/ fFunction starts from hazard analysis and risk assessment – see Fig. 48.

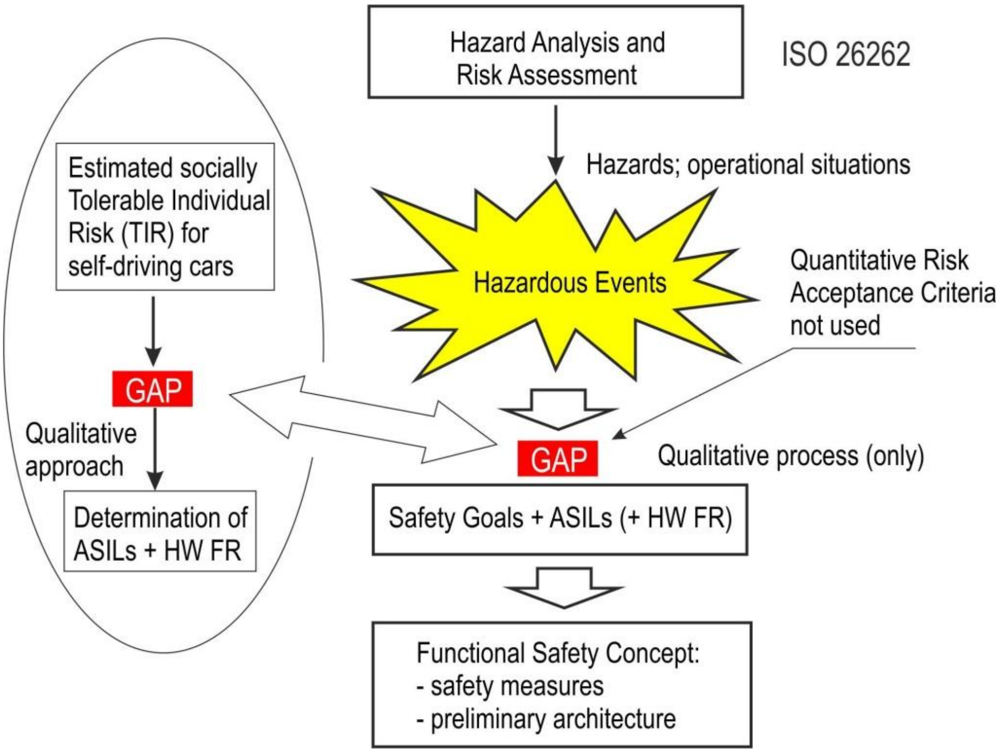

Hazard Analysis and Risk Assessment
ISO 26262
Hazards; operational situations
Estimated socially Tolerable Individual Risk (TIR) for self-driving cars
Hazardous Events
Quantitative Risk Acceptance Criteria not used
GAP
Qualitative approach
GAP
Qualitative process (only)
Determination of ASILs + HW FR
Safety Goals + ASILs (+ HW FR)
Functional Safety Concept:
- safety measures
- preliminary architecture

Figure 48. Determination of safety requirements for automotive systems

Safety requirements for the automotive Item, i.e. Safety Goals (description of safety measures) & ASIL (Automotive Safety Integrity Level) are determined for a given Hazardous Event, which is a combination of Hazard and Operational Situation. ASIL as a measure of Robustness of the Item is determined qualitatively according to ISO 26262-3 Table 4 as follows:

$$\text{ASIL} \Leftarrow f\,(E, C, S) \qquad (3)$$

where E – Exposure, C – Controllability by driver or other persons and S- Severity. Target value of Probability of Failure (PF) per 1 hour for equipment is determined from ASIL. This procedure is completely opposite to safety requirements (THR/ SIL) derivation for safety function for railway systems (EN 50129; also IEC 61508), where THR (or PFH) is (usually) quantitatively estimated first and after that qualitative SIL is assigned.

ASIL is a qualitative measure of risk. It means that ASIL is only based on the qualitative risk assessment. ASIL classifies a safety goal for a given hazardous event resulting from a specific hazard during an operational situation. On railway, the qualitative analysis is usually used at the beginning of the risk assessment, when there is not enough experience with quantitative risk description. Afterwards quantitative analysis is used. It is especially needed in case of high safety integrity requirements.

Note: In some cases ASIL derivation for specific applications may not be sufficiently clear – see [24]. It can be due the fact that ISO 26262 doesn't provide specific methodologies or processes for clear classification of the three properties (E, C, S). It can be also the case of safety requirements specification for GNSS-based position determination for self-driving cars. A socially acceptable individual risk of fatality as a starting point for hazard mitigation within a given operational scenario is not utilized according to ISO 26262.

6.2.7 Quantitative or qualitative way for high level safety requirements derivation for SDCs?

A significant gap in the process related to derivation of safety requirements for automotive systems in sense of ISO 26262 has been identified – see red box in Fig. 48. This gap means that a process for derivation of safety requirements is not able to reflect current society needs for acceptable or tolerable risk of fatality formulated by feature users/ owners of self-driving cars. In Section 2.2 there was estimated on the basis of the public survey that the socially acceptable road target fatality rate (TFR_reduced) for self-driving car should be less than $1\text{x}10^{-9}$/ h. However, there is not possible to utilise this demand in the requirements specification process because ASIL has to be derived quantitatively according to ISO 26262 based on f(E, C, S) evaluation – see formulae (3).

It is not evident from ISO 26262 which Risk Acceptance Principles/ Criteria were utilised for ASIL concept development.

The process for railway safety requirements determination according to EN 50126/ EN 50129, CSM-RA and CSM-DT seems much more transparent because it results from clearly defined and harmonised (in Europe) Risk Acceptance Criteria on which basis THR is qualitatively derived and subsequently the corresponding SIL is allocated (by means of the SIL table in EN50129).

6.2.8 Proposal for harmonization of automotive safety requirements based on railway experience

It was proposed on the basis of the identified gap in the safety requirements derivation according to ISO 26262 that the railway concept of CSM Design Targets could significantly clarify and simplify the specification of safety requirements for automobiles with safety functions – mainly those where high robustness is required – see Fig. 49.

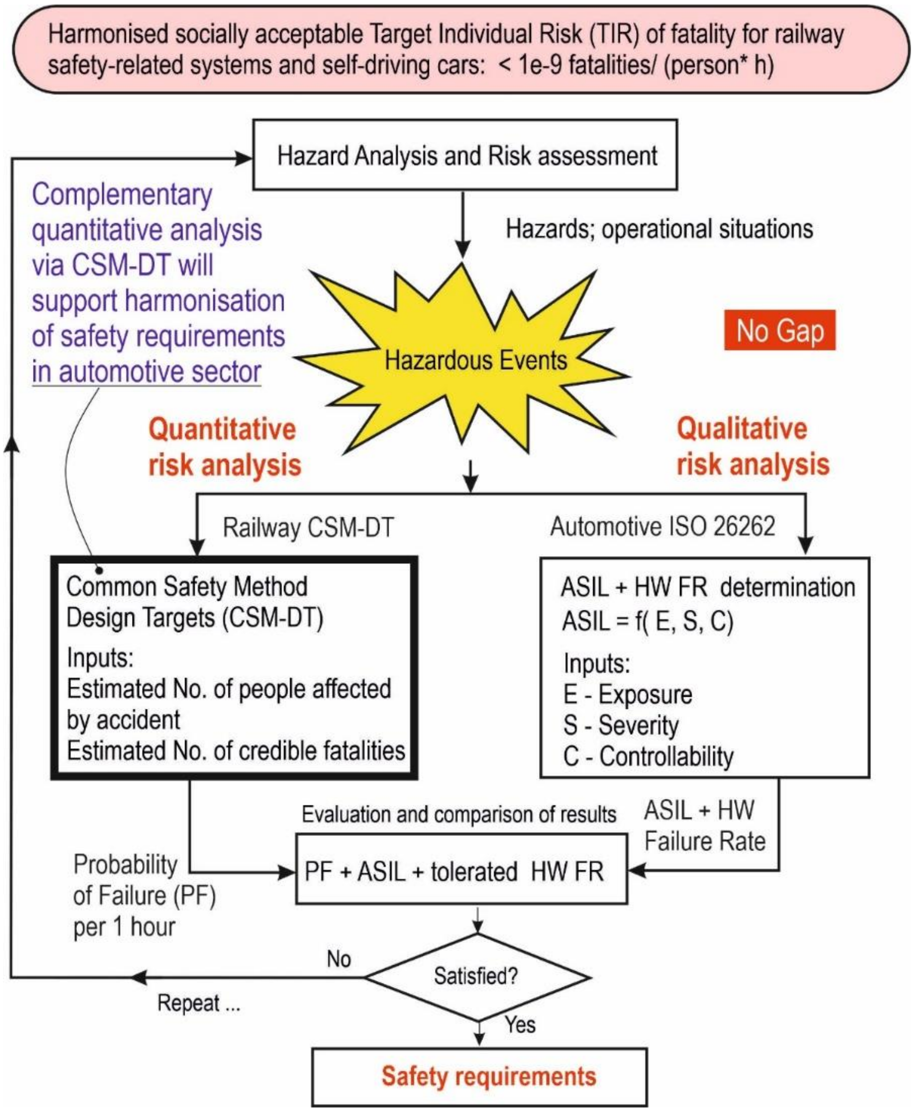

Harmonised socially acceptable Target Individual Risk (TIR) of fatality for railway safety-related systems and self-driving cars: < 1e-9 fatalities/ (person* h)
Hazard Analysis and Risk assessment
Complementary quantitative analysis via CSM-DT will support harmonisation of safety requirements in automotive sector
Hazards; operational situations
Hazardous Events
No Gap
Quantitative risk analysis
Qualitative risk analysis
Railway CSM-DT
Automotive ISO 26262
Common Safety Method Design Targets (CSM-DT)
Inputs:
Estimated No. of people affected by accident
Estimated No. of credible fatalities
ASIL + HW FR determination
ASIL = f(E, S, C)
Inputs:
E - Exposure
S - Severity
C - Controllability
Evaluation and comparison of results
ASIL + HW Failure Rate
Probability of Failure (PF) per 1 hour
PF + ASIL + tolerated HW FR
No
Satisfied?
Repeat ...
Yes
Safety requirements

Figure 49. Proposed use of railway quantitative CSM-DT as a complementary method to the qualitative ASIL determination procedure in order to support harmonization of safety requirements for self-driving cars.

The initial work regarding ISO 26262 development started by individual automotive companies around 2003 and the first draft of requirement specification appeared in 2005. In that time railways already had available a very consolidated set of CENELEC standards based on very long-term railway experience – in terms of both qualitative and quantitative risk assessment approach resulting from clearly quantified socially acceptable risk.

The ASIL concept (ISO 26262) has arisen as the modification of SIL concept with the intention to guarantee the highest safety requirements while the development cost of the automotive system should be kept as **minimum**. Application of railway CSM-DT, which also compliant with aviation classification of (catastrophic and hazardous) failures, could contribute to this effort.

In Section 7.2 there is outlined how the CSM-DT approach can utilised for harmonisation of safety requirements specification for SDCs.

6.3 UAVS/RPAS: DERIVATION OF HIGH-LEVEL SAFETY REQUIREMENTS

The derivation of High-Level Safety Requirements for UAS/RPAS follows the derivation of requirements for civil aviation outlined in sub-sections 2.3 and 6.2.1 of this document.

7. HIGH-LEVEL USER SAFETY REQUIREMENTS

7.1 RAIL: HIGH-LEVEL SAFETY TARGET FOR HELMET EXPLOITATION IN ERTMS

The quantitative ERTMS/ETCS safety target of 2e-9/ hr/ train, whose derivation is outlined in Section 6.1, is considered as a high-level safety requirement for ERTMS/ETCS applications in the HELMET project.

In the HELMET deliverable D2.3 (System Requirements Specification), detailed safety requirements for the railway operational scenarios will be derived. For this purpose, procedures and techniques used for safety requirements specification related to the ERTMS virtual balise detection, which were developed within recent projects and activities (3InSat, NGTC, ERSAT EAV RHINOS, ERSAT GGC, etc.), will be recapitulated.

7.2 AUTO: HIGH-LEVEL SAFETY TARGET DERIVATION FOR SELF-DRIVING CARS

A procedure for derivation of high-level safety target for self-driving cars is outlined in Fig. 50. It is based on information presented in Sections 5-7. The application of the harmonised risk acceptance approach based on CSM Design Targets (and aviation failure classification) is aiming at the derivation of really widely acceptable safety target for self-driving cars.

The procedure starts from the road world Traffic Fatality Rate (TFR), which is a measure of road safety - see Fig. 5 [3]. 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 a public survey/ inquiry on estimation of required safety level for self-driving car are recapitulated [2]. 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 [11].

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 [23] 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 [20], then also average speed of airplane should be also considered, otherwise the initial value of TLS would be overestimated.

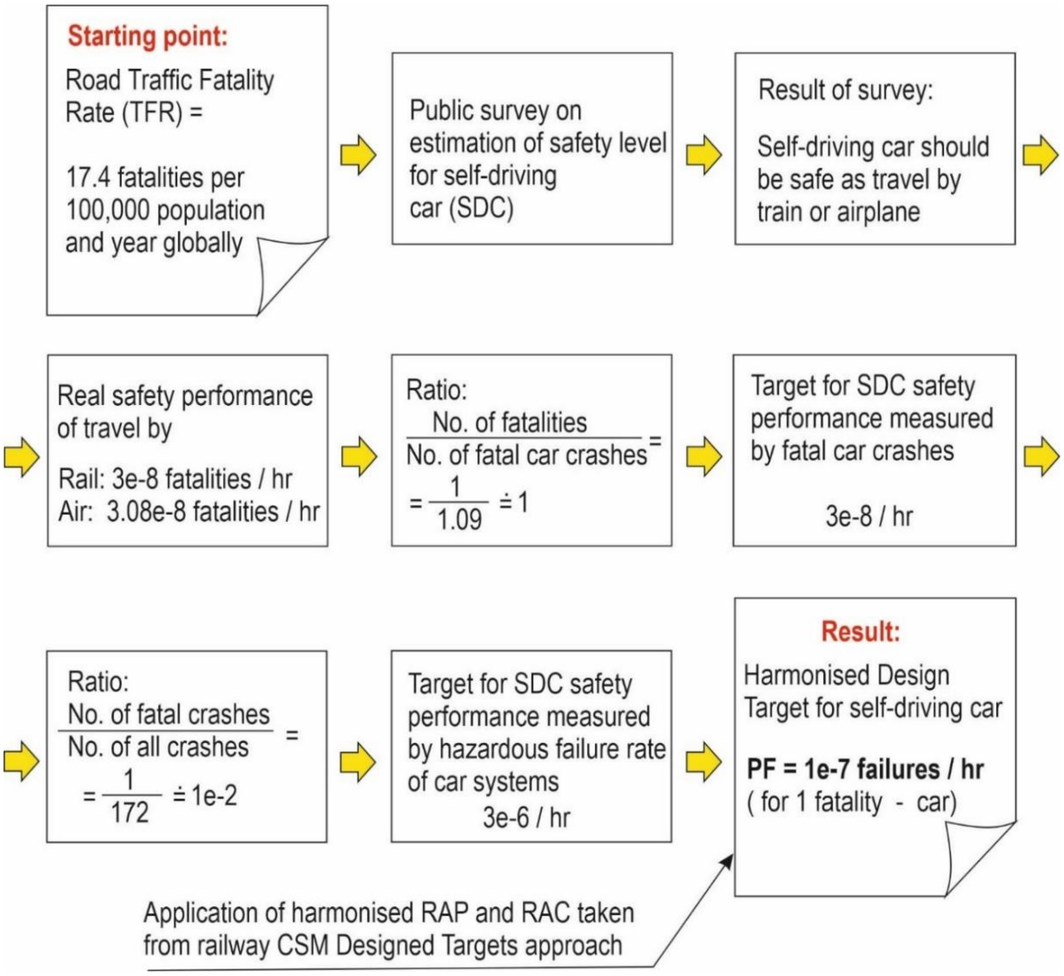

Starting point:
Road Traffic Fatality Rate (TFR) =
17.4 fatalities per 100,000 population and year globally
Public survey on estimation of safety level for self-driving car (SDC)
Result of survey:
Self-driving car should be safe as travel by train or airplane
Real safety performance of travel by
Rail: 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 50. Derivation of harmonised design target for self-driving cars

Note: An aviation risk of 2e-10 fatalities/ mile chosen in [20] as TLS corresponds to 2e-10 fatalities per time interval of 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 [20] 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 according to Table 2 , or 7.5e-8/ hr - see above) than widely acceptable safety (i.e. risk of 1e-9/ hr or less).

Since this requirements derivation process starts from 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 (safety) Design 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 risk analysis process – see Fig. 50.

The 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 [20]. It can be also considered as a way to get widely acceptable / harmonised safety requirements for SDCs.

Based on car accident statistics one can assume that approximately 1 fatal accident cause 1 fatality [20]. It means that probability of occurrence of fatal accident could be 3e-8/ hr, see Fig 50. 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 ratio in aviation TLS derivation, which is 1:10 (see Fig. 42). In the case of a car, a critical failure may not cause a fatal accident. It is stated in [20] that an automotive fatal accident to accident ratio based on statistical evaluation is 1:172. This ratio is conservatively chosen as 1:100 in [20]. The same figure is also used in Fig. 50.

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 $\Sigma C_{jk}*F_{ik}$ in 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 widely 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 a 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 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.

7.3 UAS/RPAS: HIGH-LEVEL SAFETY TARGET DERIVATION

The derivation of High-Level Safety Target Requirements for UAS/RPAS follows the derivation of requirements for civil aviation outlined in sub-section 6.2.1 of this document.

8. REGULATORY REQUIREMENTS FOR CERTIFICATION AND AUTHORIZATION

8.1 RAIL: DESCRIPTION OF CERTIFICATION PROCESS

This subsection briefly describes the certification and safety approval process, which is currently applied to railway safety-related systems on European Railways. The intention is to provide an inspiration to the automobile sector which could be similarly applied to type-approval process for future automated car driving supported by a digital road-side infrastructure.

Certification and for railway safety-related systems is outlined here via an example of ERTMS, which was developed for signalling and traffic management in Europe. The European Train Control System (ETCS), which is a part of ERTMS, employs track balises with known position for safe train position determination. These physical balises are detected on board of train by means of a so called Balise Transmission Module (BTM) – see Fig. 51.

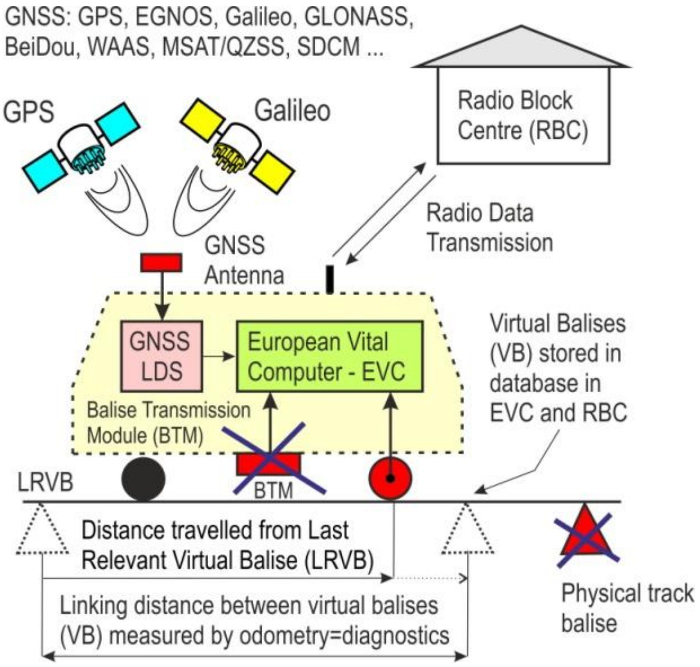

GNSS: GPS, EGNOS, Galileo, GLONASS, BeiDou, WAAS, MSAT/QZSS, SDCM ...
GPS
Galileo
Radio Block Centre (RBC)
Radio Data Transmission
GNSS Antenna
GNSS LDS
European Vital Computer - EVC
Virtual Balises (VB) stored in database in EVC and RBC
Balise Transmission Module (BTM)
LRVB
BTM
Distance travelled from Last Relevant Virtual Balise (LRVB)
Linking distance between virtual balises (VB) measured by odometry=diagnostics
Physical track balise

Figure 51. European train control system with virtual balises detected by GNSS

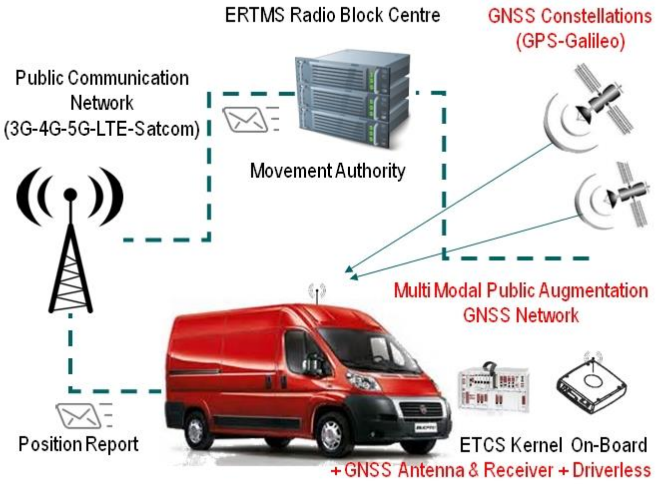


Figure 52. Example of using the ERTMS for connected car

The ERTMS is a centralised command and control system which authorizes the train to move until a predetermined point once the train position has been detected and all the safety conditions are fulfilled. Train positioning is determined by a SIL 4 on-board odometer whose errors are reset periodically with transponders (balises) deployed along the railways. This architecture is well consolidated and operational since more than 15 years, cumulating billions of Km travelled without accidents due to a technical failure Nowadays the ERTMS is evolving to adopt the GNSS positioning, hybrid telecom networks and autonomous driving, making it similar to the Connected car architecture (Fig. 52). These changes will undergo the approved certification and authorization process [26], [4], [27] in order to guarantee the safety levels. Furthermore, hybrid positioning systems (GNSS + IMU) are being developed in order to increase the availability of the vehicle's positioning. The objective is to demonstrate a THR better than 10^{-9}/ h. A cross-check with an independent non-GNSS localizer, i.e. IMU as the Function B shown in Fig. 24, has been defined in the RHINOS project [25].

A key feature of the ERTMS is to ensure the interoperability among on-board and track-side subsystems shared between different actors, mainly Infrastructure Managers (IM) and Railway Undertakings (RU). A similar scenario is applied for car manufactures and road infrastructure managers. High safety and dependability requirements (i.e. RAMS – Reliability, Availability, Maintainability and Safety) for ERTMS must be met - also in cases when track balises are replaced with virtual balises and detected by GNSS positioning – see e.g. ERSAT GGC project [28]. Therefore it to necessary to pass the certification and approval process that guarantees all requirements for ERTMS (i.e. safety standards CENELEC EN 5012x [5], [29], [30] Technical Specifications for Interoperability (TSIs), EU regulations, directives, etc.) are met. The EU Directive 2016/797 [4] extends authorization process of Control Command Systems (CCS) to the entire railway system - it supports concept of “Cross Acceptance“ as a stepping stone to the interoperability within the Trans European Network. The whole framework for certification and safety authorization of ERTMS based on GNSS has been described in [31].

Excepting Verification and Validation (V&V), Safety Case elaboration (for on-board, track-side and integrated track-side and on-board equipment) and Independent Safety Assessment (ISA), the system compliance with ERTMS TSIs should be checked within the certification process [31].

Railway actors have to manage safely all changes of the European railway system – including GNSS positioning, hybrid GNSS positioning and other sensors integration with ERTMS. Common Safety Method for Risk evaluation and Assessment (CSM-RA) must be used according to European railway regulations if a safety-related change in a system is significant – see Fig. 45 [8], [32], [33].

The CSM-RA shall cover the whole CENELEC lifecycle including safety evaluation during system operations. The above mentioned activities such as V&V, Safety Case elaboration, Independent Risk Assessment and Conformity Assessment with respect to TSI's (i.e. certification) cover only part of the safety life-cycle according to CENELEC EN 50126 [5] and [32], [34]. As is it outlined in [31], CSM-RA creates a framework for the whole certification and safety approval process for European railway systems. The safety monitoring during real system operations is not covered by the activities mentioned above. Therefore CSM-RA requires a separate Safety Management System (SMS) to be implemented and performed within Railway Undertaking (RU) and Infrastructure Manager (IM) activities to fill in the safety gap mentioned above – see Fig. 53. The European Common Safety Targets [26] for the whole railway system are used for safety evaluation within the SMS.

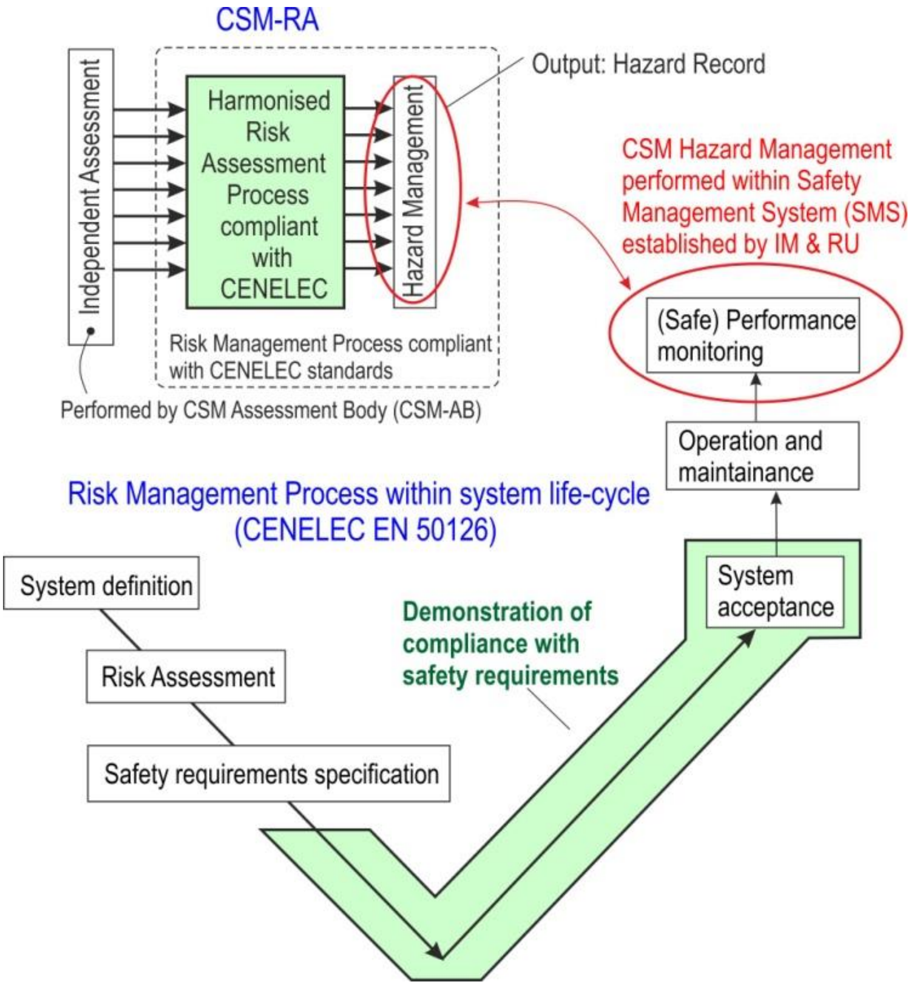

CSM-RA
Independent Assessment
Harmonised Risk Assessment Process compliant with CENELEC
Hazard Management
Output: Hazard Record
Risk Management Process compliant with CENELEC standards
Performed by CSM Assessment Body (CSM-AB)
CSM Hazard Management performed within Safety Management System (SMS) established by IM & RU
(Safe) Performance monitoring
Operation and maintainance
Risk Management Process within system life-cycle (CENELEC EN 50126)
System definition
Risk Assessment
Safety requirements specification
Demonstration of compliance with safety requirements
System acceptance

Figure 53. Relation between CSM-RA and CENELEC life cycle.

The aim of European railway authorities and European railway industry is to develop interoperable railway systems based on common regulations. The cross-acceptance of safety approvals for sub-systems and equipment by the different national railway authorities is essential. The cross-acceptance becomes e.g. also critical in the area of exploitation of the aviation GNSS Safety-of-Life (SoL) service as the Generic and Specific Application for ERTMS – see [31]. In this sense a Safety Case is a very important part of the conformity assessment documenting the achieved safety levels. The cross-acceptance of GNSS SoL service can be demonstrated via two following Generic Safety Cases from the EN 50129 [30] safety cases family: 1) Generic Product Safety Case - independent of railway application, and 2) Generic Application Safety Case - for a class of applications.

It seems the important element in this GNSS/ EGNOS SoL service cross-acceptance process is a so-called 'pre-existing' item originally introduced in IEC 61508 (2010) and adopted later by CENELEC EN 50129 (2018). The idea [51] consists in fact that e.g. the EGNOS SoL service would be adopted and certified via a so-called 'pre-existing' item in terms of the standards EN 50129/ IEC 61508. Important is that EGNOS can be fully cross-accepted according to CENELEC railway safety standards and so this significant (safety) change in ERTMS can be fully controlled using CSM Risk Management Process in compliance with the CENELEC life cycle. It means that there is no need to develop a new EGNOS safety case specifically for rail safety applications according to CENELEC, which would not even be possible. This proposal opens the door to the EGNOS certification for railway safety systems compliant with SIL 4. In addition, the idea can be also utilised for GNSS SoL services adoption and certification in other land GNSS-based safety applications, such as self-driving cars, machine control, mobile robots, etc.

8.2 AUTO: CERTIFICATION PROCESS FOR SELF-DRIVING CARS

8.2.1 Need for certification of self-driving cars

Safety certification and authorization process for road vehicles in Europe is historically based on a so called Type-approval process [35]-[37]. The National Safety Authority in a given EU Member State usually entrusts the national Technically Services to perform tests and other verification and validation of a vehicle prototype. After the tests have been successfully completed, the National Safety Authority issues the vehicle type-approval to the vehicle manufacturer. On this basis the vehicle manufacturer issues the Certificate of Conformity (birth-certificate) [38] which must accompany each manufactured vehicle.

In recent years the development and type-approval process for automated vehicles is getting more complicated when Automatically Commanded Steering Functions (ACSF) are being introduced into operations [39]. Higher categories ACSF systems (B2 - *Hands-off lane guidance systems* and E - *Lane change system without driver input*) will require among others much higher safety levels for car position determination, as it is also common in aviation or railway sectors. For example on railway, the compliance with Safety Integrity Level (SIL) 4 with THR < 1e-9/ h is required for train position determination function. Furthermore, a clear certification and safety approval process for these high safety levels should be specified. Otherwise it would be impossible to use cars with ACSF due to lack of trust from the passenger side.

To solve the above tasks numerous activities have been performed within the UN ECE expert groups (United Nations Economic Commission for Europe) and other working parties. However, usable conclusions and recommendations on ACSF certification are still missing, although examples for such process have also been searched in sectors with traditionally very high safety target levels like aviation, nuclear energy and railway – see [40] and [41]-[49].

8.2.2 Shorter vehicle lifecycle on road-side digital infrastructure

Demonstration of compliance with regulations and standards for a large civil aircraft can take more than 5 years. Duration of safety authorization in case of complex railway signalling such as ERTMS is similar to the process duration for airplane. The situation in automobile industry is different, because the conformity assessment process usually takes less than 1 year [40]. It is not expected it will take longer for cars with automated driving functions satisfying higher safety levels than existing car assistants. It is because the current trend tends to shortening of car lifecycle to about 3 years. Furthermore, these cars will be much more dependent on a way-side communications-based infrastructure. It will be necessary not only to demonstrate the required safety of automated car, but all significant changes in future road automated transport systems must be safely managed as well – including road-side infrastructure for connected cars.

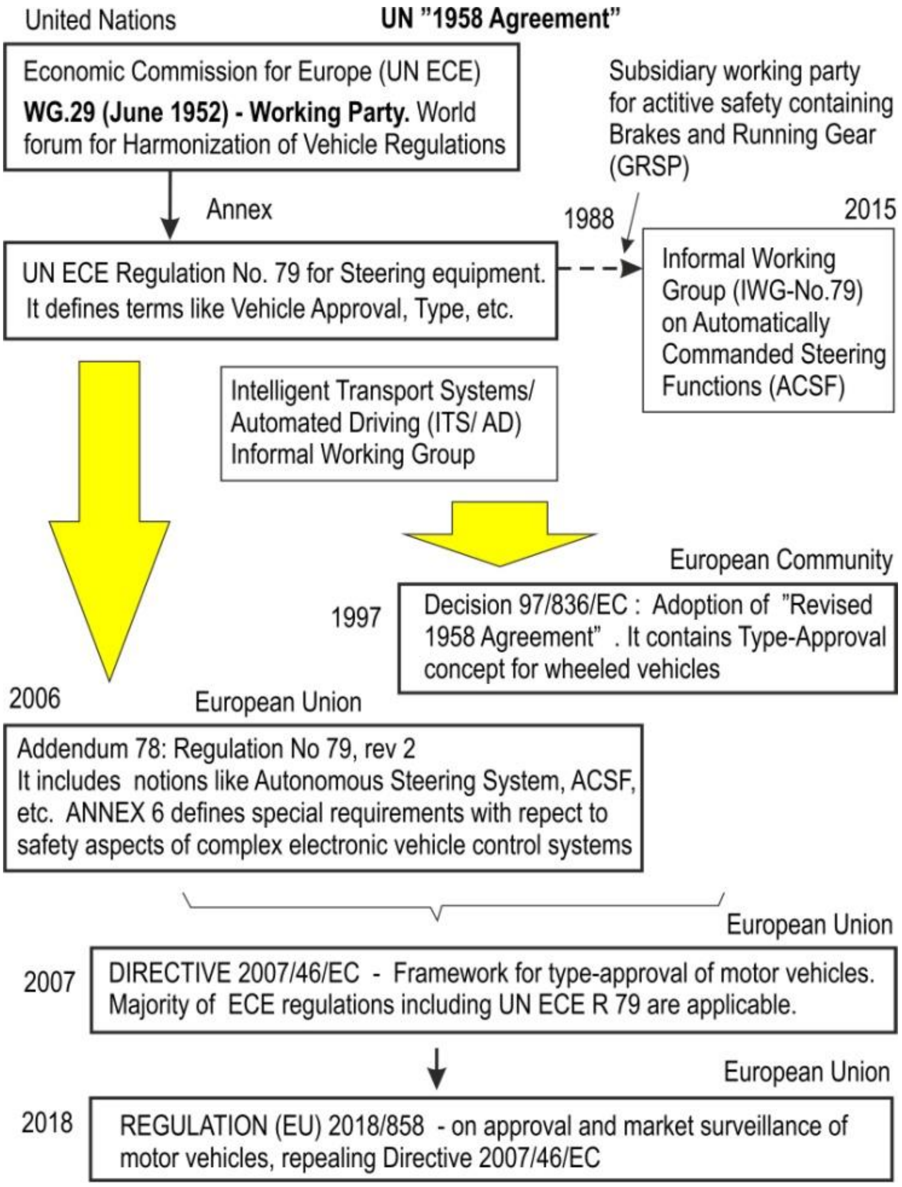
The absence of a widely acceptable methodology for management of relatively frequent safety-related changes in vehicles with implemented ACSF represents currently a significant gap in terms of safety for automated vehicles world-wide. Future SDC operating companies and road infrastructure managers will not be simply able without a suitable Risk Management Process to safely control system changes and enable to guarantee a high safety level which is e.g. common in aviation or on railway. The absence of such clearly defined process also has a negative impact in society. Every accident of not properly approved automated car due to technical failures contributes to the mistrust towards this new technology in society. Nevertheless, railway stakeholders know how to manage safely changes on European railways. That's why it is proposed to utilise this railway experience as an example and motivation for setting up the risk management process for SDCs.

8.2.3 Type-approval framework for cars in EU

Before a new model of vehicle is to be placed on the EU market, it must pass through a so-called type-approval process, i.e. homologation. Within this process national authorities in EU Member states certify that the model of a vehicle (or its part) satisfies all EU safety, environmental and production requirements. This type-approval process shall be performed according to the Regulation (EU) 2018/858 of May 2018 [38], which establishes the harmonised framework for approval of motor vehicles.

The manufacturer shall submit according to the above regulation the application accompanied by the information folder to the approval authority in each Member State. If all relevant requirements are met, the national authority delivers an EC type-approval certificate to the manufacturer authorizing the sale of the vehicle type in EU. After that the manufacturer issues a Certificate of Conformity, which accompanies every produced vehicle. The certification process is based on a mutual recognition, i.e. cross-acceptance of approvals by national approval authorities in EU Member States.

The above EU regulation has been formulated in accordance with the 1958 United Nations Economic Commission for Europe (UN ECE) agreement [35] and additional subsequent regulations as it is outlined in Fig. 54. The World Forum for Harmonization of Vehicle Regulations is a working party (WP.29) of the UN ECE. It is tasked with creating a uniform system of regulations, called UN Regulations, for vehicle design to facilitate international trade. WP.29 was established in June 1952


United Nations
UN "1958 Agreement"

Economic Commission for Europe (UN ECE)
WG.29 (June 1952) - Working Party. World forum for Harmonization of Vehicle Regulations

Subsidiary working party for actitive safety containing Brakes and Running Gear (GRSP)

Annex

1988

2015

UN ECE Regulation No. 79 for Steering equipment. It defines terms like Vehicle Approval, Type, etc.

Informal Working Group (IWG-No.79) on Automatically Commanded Steering Functions (ACSF)

Intelligent Transport Systems/ Automated Driving (ITS/ AD) Informal Working Group

European Community

1997

Decision 97/836/EC : Adoption of "Revised 1958 Agreement" . It contains Type-Approval concept for wheeled vehicles

2006

European Union

Addendum 78: Regulation No 79, rev 2
It includes notions like Autonomous Steering System, ACSF, etc. ANNEX 6 defines special requirements with repect to safety aspects of complex electronic vehicle control systems

European Union

2007

DIRECTIVE 2007/46/EC - Framework for type-approval of motor vehicles. Majority of ECE regulations including UN ECE R 79 are applicable.

European Union

2018

REGULATION (EU) 2018/858 - on approval and market surveillance of motor vehicles, repealing Directive 2007/46/EC

Figure 54. Chronology of regulations towards type-approval process of vehicles with ACSF in Europe

as the "Working Party of experts on technical requirement of vehicles", while its current name was adopted in year 2000. The forum works on regulations covering vehicle safety, environmental protection, energy efficiency and theft-resistance.

The approval of vehicles with regard to steering equipment is included in UN ECE regulation No. 79 [36] that is effective from 1988. This regulation is annexed to the UN 1958 agreement regarding adoption of technical prescriptions on equipment of wheel vehicles and mutual recognition of the approval.

However, the Regulation No. 79 did not cover primary steering transmissions purely based on electric means. In 1997 European Community adopted a so called Revised 1958 Agreement (97/836/EC) [37] concerning the adoption of uniform technical prescriptions for wheeled vehicles including mutual recognition of approvals (type-approvals).

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

In 2007 the EU directive 2007/46/EC [50] establishing a harmonised framework for the approval of vehicles in EU Member States was adopted. No technical requirements are contained in the directive. However, it is stated in the Appendix IV, that the majority of ECE Regulations, including Regulation No. 79 are applicable. Regulation (EU) 2018/858 [38] repeals the Directive 2007/46/EC.

8.3 UAS/RPAS: REQULATORY FRAMEWORK AND REQUIREMENTS

In the present work all UAS/RPAS Regulations for Civil Aviation Operations are related to those of the EU (ECAC Region) Regulatory Bodies such as EASA, International such as ICAO and ITU and Operational Standards emanated from EUROCONTROL and JARUS Standards. In particular the IMTM UAS/RPAS Operations will be confined within the future European UTM System and its related Regulatory Frame. Current Regulatory Issues and Operational Limitations of UAS/RPAS and for the purposes of the HELMET project shall be assessed the use of small UAS/RPAS from more than 1Kg to 25Kg Maximum Take-off Mass-MTOM.

In the wake of the World Radio-communication Conferences WRC-12, WRC-15 (Res.155), and WRC-19 (Res.155) the actual spectrum resources and requirements are explored and imposed, regarding the RLOS and BRLOS operations of the Civil Aviation UAS/RPAS in the non-segregated and segregated airspace under aviation safety conditions so as to achieve standard, and certifiable data links supplying UAS/RPAS safe Command, Control and Communications over which an UAS/RPAS Remote Pilot (RP) can control and monitor the Remote Piloted Aircraft (UAS/RPAS) operations.

The UAS/RPAS can operate over terrestrial radio links within radio line-of-sight (RLOS) while for beyond radio line-of-sight (BRLOS), two options exist: a deployment of networked terrestrial stations covering the entire area of expected UAS/RPAS operations, or satellite communications. A complete network of terrestrial stations covering all possible operational locations is unlikely to be realized, especially considering remote and over-water locations. Hence, satellite communications (including NAVAID) will need to be a significant component of the Link infrastructure for UAS/UAS/RPAS.

The International Civil Aviation Organization (ICAO) has determined that the C2 link must operate over protected aviation spectrum. Therefore, protected aviation spectrum must be allocated for this function, approved through the processes of the International Telecommunications Union Radio-communication Sector (ITU-R). Actions taken at the ITU-R 2012 World Radio-communication Conference (WRC-12) have established spectrum resources to address the RLOS spectrum requirement among others also in the C-Band, at 5030-5091 MHz. At the ITU-R 2015 WRC (WRC-15), BRLOS spectrum requirements were addressed by providing allocations specifically for UAS/RPAS in Ku-Band and Ka-Band in Fixed Satellite Service (FSS) allocations Revised and Confirmed in Resolution 155 WRC-19 (incl. Annexures 1 and 2) as Regulatory provisions related to earth stations on board unmanned aircraft which operate with geostationary-satellite networks in the fixed-satellite service in certain frequency bands not subject to a Plan of Appendices 30, 30A and 30B for the control and non-payload communications of unmanned aircraft systems in non-segregated airspaces. The FSS allocation is not aviation safety spectrum, hence the use of these bands for C2 links will require a number of special considerations in order to meet an equivalent level of safety.

In this document the operational aspects of UAS/RPAS C2 links for both RLOS and BRLOS conditions for the operation of UAS/RPAS CNPC links are provided as a basis to be further reviewed during the project implementation, as well as the data transfer requirements, bandwidth requirements and link technical characteristics.

It is noted that ICAO identified the conditions required for UAS/RPAS C2 use of FSS bands to meet an equivalent level of safety in non-segregated airspaces. ICAO identified the required conditions in the ICAO Position in WRC-15 and WRC-19. Taking into account the ICAO conditions, WRC-15 and WRC-19 were able to come to an agreement to make new allocations in the FSS Ku and Ka frequency bands, identifying over 2.2 GHz of spectrum in WRC-15 Resolution 155 and WRC-19 Rev. Resolution 155. The Resolution specifies that these frequency bands can be used for the UAS C2 links in non-segregated but also segregated airspace under certain conditions and any other airspace under the control of civil aviation authorities. This use is contingent on the successful ongoing development of ICAO SARPs. The Resolution goes into considerable detail to protect the current FSS environment against being disrupted by the introduction of a service that is virtually the same as an aviation safety service. The Resolution requires ICAO to report on its progress in the development of SARPs for the UAS/RPASC2 link to WRC-23, including identification of any problems in the application of the Resolution and potential means by the WRC to address those. The Resolution will come fully into force by WRC-23.

On request by the European Commission, Member States and other stakeholders, EASA has developed an operation centric, proportionate, risk- and performance-based regulatory framework for all unmanned aircraft (UA) establishing three categories with different safety requirements, proportionate to the risk, namely:

1) “Open” (low risk) is an UAS/RPAS operation category that, considering the risks involved, does not require a prior authorization by the competent authority before the operation takes place; The ‘Open’ category UA/RPA has a maximum take-off mass (MTOM) of less than 25kg, and flies below a height of 21m in Visual Line of Sight (VLOS), far from aerodromes. Thus, the Regulation in this category considers the following:
    a) Low risk operations
    b) Without involvement of aviation authority
    c) Limitations (visual line of sight, maximum altitude, distance from airport and sensitive zones)
    d) Flight over people is possible in sub-class A0 with drones in classes C1 and C0 only (less than 911g or 81J)
    e) No overflying of crowds
    f) CE marking
    g) Training and passing a test are mandatory for all remote pilots of drones above 251g.

The Open category is further sub-divided into three sub-categories:

- a) A0: flights over people (but not over open-air assemblies of people) intended for hobby users flying UAs under 911g (or 81J) - class C1 or C0;
- b) A2: flights close to people, but a safe distance from them for heavier UAs - class C2 - and require passing a recognised theory test;
- c) A0: flights far from people – generally intended for model aircraft clubs - class C0 and C4.

2) 'Specific' (medium risk) is an UAS/RPAS operation category that, considering the risks involved, requires an authorization by the competent authority before the operation takes place and takes into account the mitigation measures identified in an operational risk assessment, except for certain standard scenarios where a declaration by the operator is sufficient; 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 the majority of professional flying in VLL will be considered Specific operations. U-Space.

3) 'Certified' (high risk) is an UAS/RPAS operation category that, considering the risks involved, requires the certification of the UAS/UAS/RPAS, a licensed remote pilot and an operator approved by the competent authority, in order to ensure an appropriate level of safety. The related regulatory requirements are comparable to those for manned aviation. Oversight by an NAA (issue of licences and approval of maintenance, operations, training, ATM and aerodromes organisations) and by EASA (design and approval of foreign organisations). Thus, the Regulation in this category considers the following:

- a) High risk
- b) Comparable to manned aviation
- c) Type certificate (TC), Certificate of airworthiness, noise certificate, approved organisations, licences
- d) C2 link equipment and the remote pilot station could have separate TCs

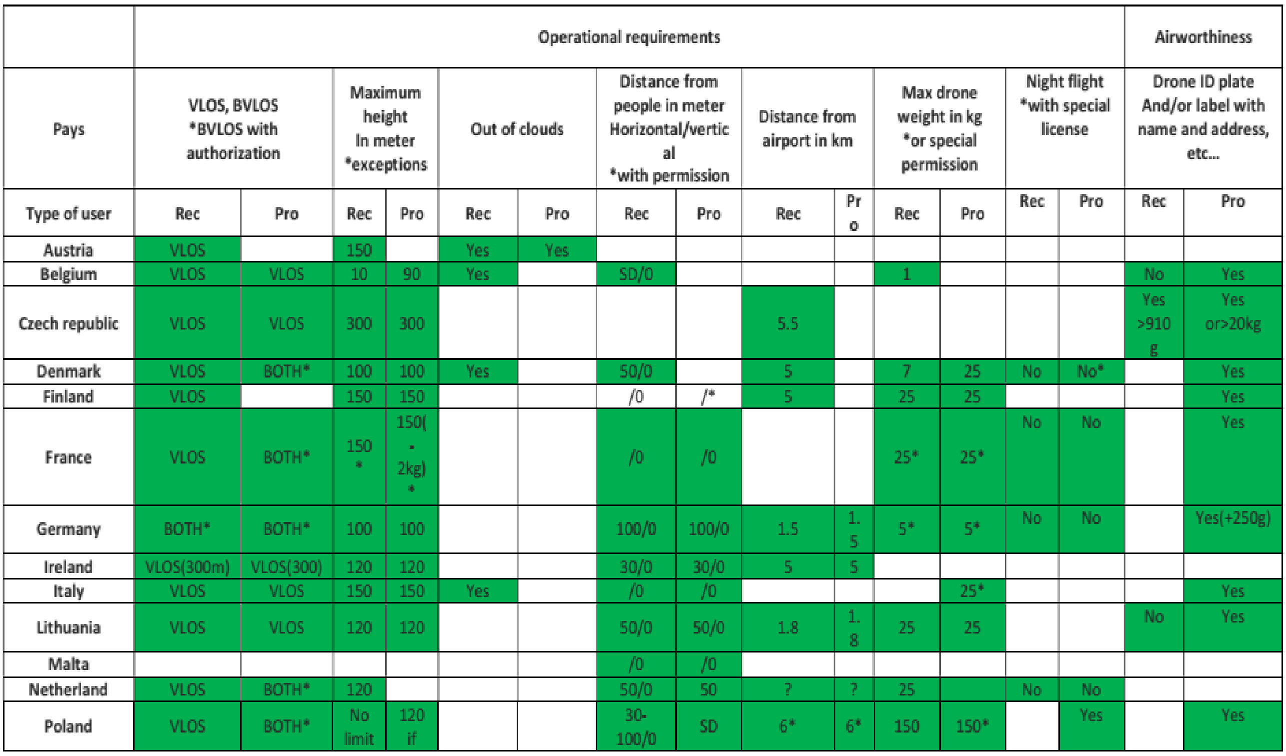
Note that the majority of the UAS/RPAS to be employed for HELMET IMTM work will be of the "Specific" Category and thus they will be regulated by EASA to operate in the U-Space environment after they have met the requirements for operations as assessed for risks by the SORA methodology.

EASA has developed proposals for an operation centric, proportionate, risk- and performance-based Regulatory framework for all unmanned aircraft (UA), which has been outlined in Section 2.3.1 of this document. The Current Regulatory Frame of EASA (EU State Members Civil Aviation Regulatory Institutions) and Operational Limitations are related to small UAS/RPAS to up 25kg TOW. This concept focuses on safety risks but recognises the importance of risks to privacy and security. The safety risks considered must take into account:

- a) Mid-air collision with manned aircraft and/or other UAS/RPAS
- b) Harm to people, and
- c) Damage to property in particular critical and sensitive infrastructure.

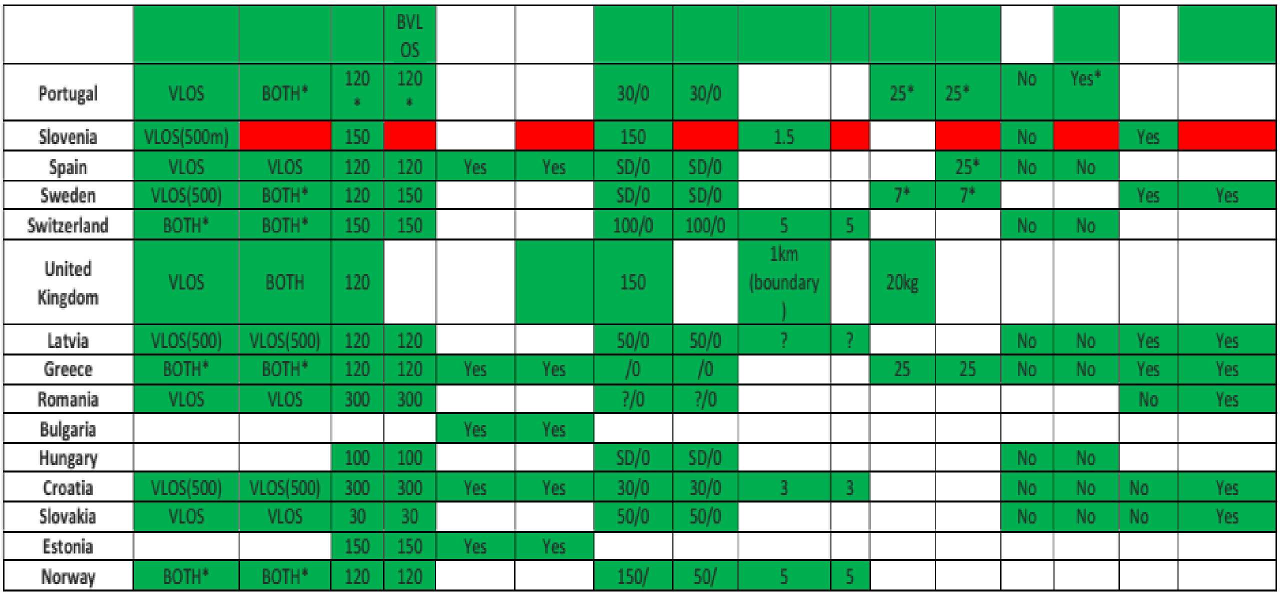
Tables 4 and Tables 42 (a)-(d) summarize some EU Member States' Regulations on UAV/ UAS/ RPAS up to 25kg MTOW, operational, legal and other constraints.

Table 42 (a-d). Overview of some EU Member States' Regulations on UAV/UAS/RPAS up to 25kg TOW
(Ref. EASA A-NPA 2015-10 and CORUS U-space CONOPS Annex J: Current regulatory environment of Europe).



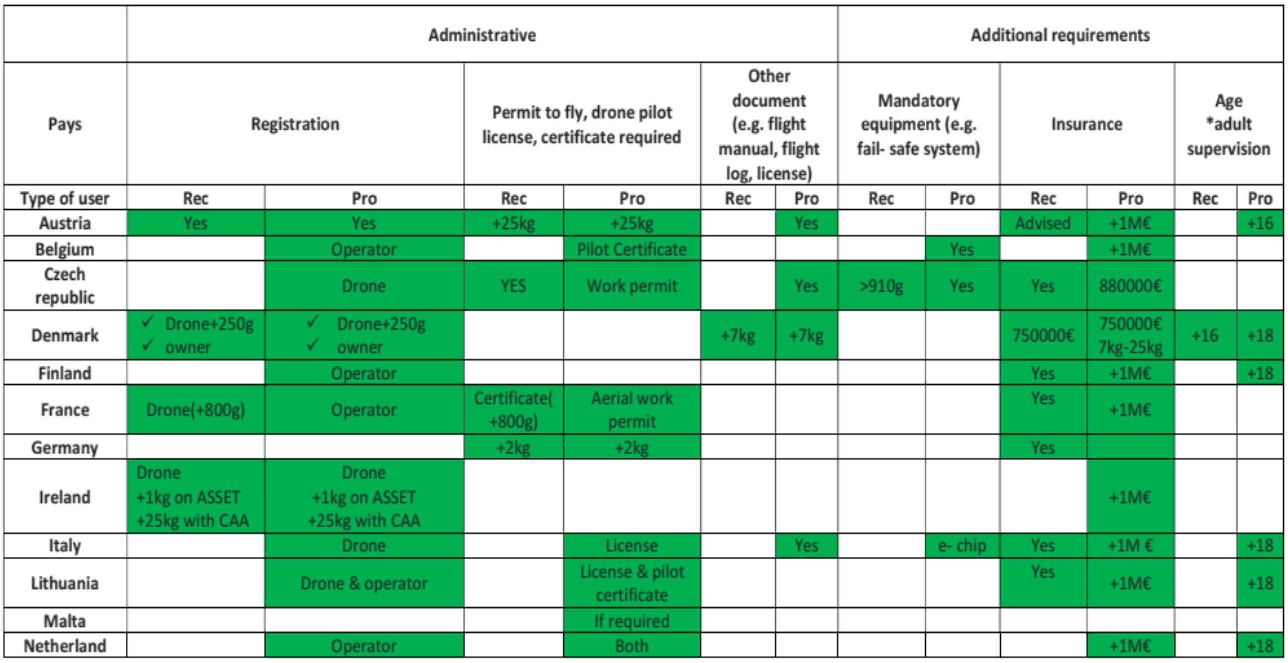
	Operational requirements														Airworthiness	
Pays	VLOS, BVLOS *BVLOS with authorization		Maximum height In meter *exceptions		Out of clouds		Distance from people in meter Horizontal/vertical *with permission		Distance from airport in km		Max drone weight in kg *or special permission		Night flight *with special license		Drone ID plate And/or label with name and address, etc...	
Type of user	Rec	Pro	Rec	Pro	Rec	Pro	Rec	Pro	Rec	Pro	Rec	Pro	Rec	Pro	Rec	Pro
Austria	VLOS		150		Yes	Yes										
Belgium	VLOS	VLOS	10	90	Yes		SD/0				1				No	Yes
Czech republic	VLOS	VLOS	300	300					5.5						Yes >910g	Yes or>20kg
Denmark	VLOS	BOTH*	100	100	Yes		50/0		5		7	25	No	No*		Yes
Finland	VLOS		150	150			/0	/*	5		25	25				Yes
France	VLOS	BOTH*	150*	150(-2kg)*			/0	/0			25*	25*	No	No		Yes
Germany	BOTH*	BOTH*	100	100			100/0	100/0	1.5	1.5	5*	5*	No	No		Yes(+250g)
Ireland	VLOS(300m)	VLOS(300)	120	120			30/0	30/0	5	5						
Italy	VLOS	VLOS	150	150	Yes		/0	/0				25*				Yes
Lithuania	VLOS	VLOS	120	120			50/0	50/0	1.8	1.8	25	25			No	Yes
Malta							/0	/0								
Netherland	VLOS	BOTH*	120				50/0	50	?	?	25		No	No		
Poland	VLOS	BOTH*	No limit	120 if			30-100/0	SD	6*	6*	150	150*		Yes		Yes

(a)



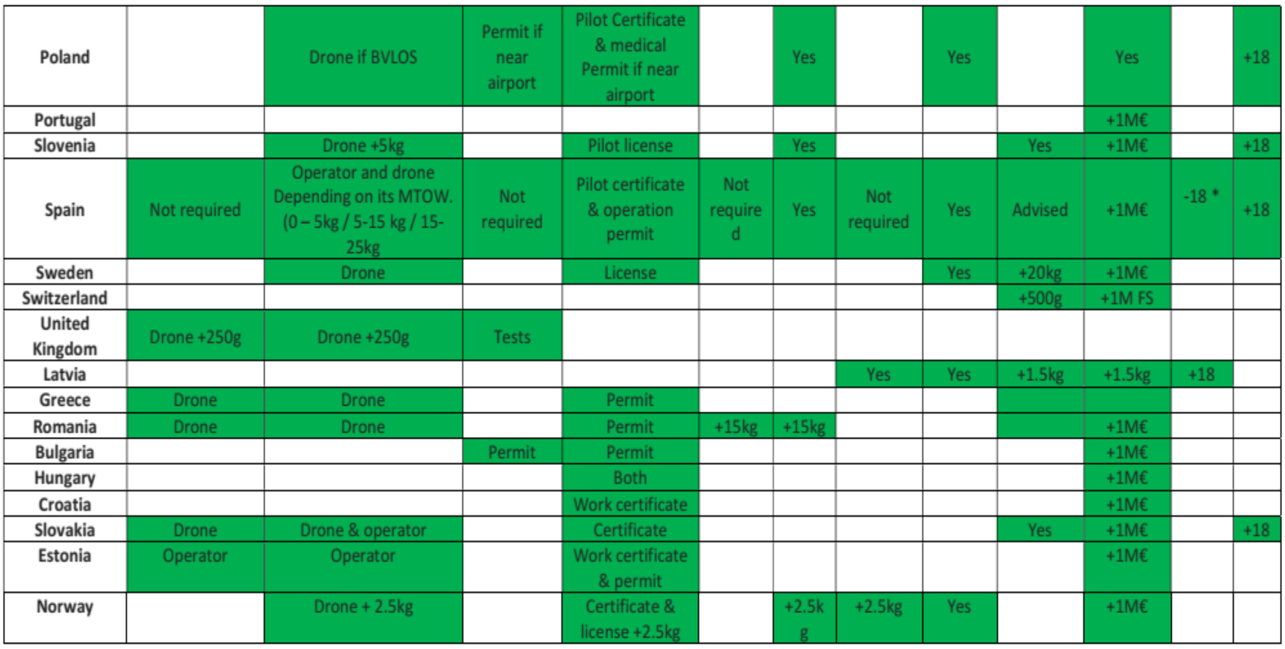
	🟩	🟩	🟩	BVLOS			🟩	🟩	🟩	🟩	🟩	🟩		🟩		🟩
Portugal	VLOS	BOTH*	120*	120*			30/0	30/0			25*	25*	No	Yes*		
Slovenia	VLOS(500m)	🟥	150	🟥		🟥	150	🟥	1.5	🟥		🟥	No	🟥	Yes	🟥
Spain	VLOS	VLOS	120	120	Yes	Yes	SD/0	SD/0				25*	No	No		
Sweden	VLOS(500)	BOTH*	120	150			SD/0	SD/0			7*	7*			Yes	Yes
Switzerland	BOTH*	BOTH*	150	150			100/0	100/0	5	5			No	No		
United Kingdom	VLOS	BOTH	120			🟩	150		1km (boundary)		20kg					
Latvia	VLOS(500)	VLOS(500)	120	120			50/0	50/0	?	?			No	No	Yes	Yes
Greece	BOTH*	BOTH*	120	120	Yes	Yes	/0	/0			25	25	No	No	Yes	Yes
Romania	VLOS	VLOS	300	300			?/0	?/0							No	Yes
Bulgaria					Yes	Yes										
Hungary			100	100			SD/0	SD/0					No	No		
Croatia	VLOS(500)	VLOS(500)	300	300	Yes	Yes	30/0	30/0	3	3			No	No	No	Yes
Slovakia	VLOS	VLOS	30	30			50/0	50/0					No	No	No	Yes
Estonia			150	150	Yes	Yes										
Norway	BOTH*	BOTH*	120	120			150/	50/	5	5						

(b)



	Administrative						Additional requirements					
Pays	Registration		Permit to fly, drone pilot license, certificate required		Other document (e.g. flight manual, flight log, license)		Mandatory equipment (e.g. fail- safe system)		Insurance		Age *adult supervision	
Type of user	Rec	Pro	Rec	Pro	Rec	Pro	Rec	Pro	Rec	Pro	Rec	Pro
Austria	Yes	Yes	+25kg	+25kg		Yes			Advised	+1M€		+16
Belgium		Operator		Pilot Certificate				Yes		+1M€		
Czech republic		Drone	YES	Work permit		Yes	>910g	Yes	Yes	880000€		
Denmark	✓ Drone+250g ✓ owner	✓ Drone+250g ✓ owner			+7kg	+7kg			750000€	750000€ 7kg-25kg	+16	+18
Finland		Operator							Yes	+1M€		+18
France	Drone(+800g)	Operator	Certificate(+800g)	Aerial work permit					Yes	+1M€		
Germany			+2kg	+2kg					Yes			
Ireland	Drone +1kg on ASSET +25kg with CAA	Drone +1kg on ASSET +25kg with CAA								+1M€		
Italy		Drone		License		Yes		e- chip	Yes	+1M €		+18
Lithuania		Drone & operator		License & pilot certificate					Yes	+1M€		+18
Malta				If required								
Netherland		Operator		Both						+1M€		+18

(c)



Poland		Drone if BVLOS	Permit if near airport	Pilot Certificate & medical Permit if near airport		Yes		Yes		Yes		+18
Portugal										+1M€		
Slovenia		Drone +5kg		Pilot license		Yes			Yes	+1M€		+18
Spain	Not required	Operator and drone Depending on its MTOW. (0 – 5kg / 5-15 kg / 15-25kg	Not required	Pilot certificate & operation permit	Not require d	Yes	Not required	Yes	Advised	+1M€	-18 *	+18
Sweden		Drone		License				Yes	+20kg	+1M€		
Switzerland									+500g	+1M FS		
United Kingdom	Drone +250g	Drone +250g	Tests									
Latvia							Yes	Yes	+1.5kg	+1.5kg	+18	
Greece	Drone	Drone		Permit								
Romania	Drone	Drone		Permit	+15kg	+15kg				+1M€		
Bulgaria			Permit	Permit						+1M€		
Hungary				Both						+1M€		
Croatia				Work certificate						+1M€		
Slovakia	Drone	Drone & operator		Certificate					Yes	+1M€		+18
Estonia	Operator	Operator		Work certificate & permit						+1M€		
Norway		Drone + 2.5kg		Certificate & license +2.5kg		+2.5k g	+2.5kg	Yes		+1M€		

(d)

NOTE:

**=with permission/registration*
SD=safe distance
?=restriction but no distance.
For the distance from airport, the reference of the distance is not always specified (e.g. from the perimeter fence, the centre of the airport or the runway).

In conclusion related to UAS/RPAS, several decisions are embedded in the EU regulations. These are summarized as follows:

a) An UAS/RPAS operation is categorised as Open, Specific or Certified. Each category combines a risk level for the operation, and an appropriate risk assessment and mitigation approach.

b) UAS/RPAS that are to be supplied as suitable for Open operations fall into one of five classes, C0, C1, C2, C3 or C4, depending on various technical parameters.

c) The Open category is divided into three sub-categories, A1, A2 and A3, that refer to the different UAS/RPAS classes C0 to C4 referred to above.

d) Preparation of a Specific operation should usually include a risk assessment using the JARUS SORA method, or any other assessment method, compliant with the Acceptable Means of Compliance (AMC).1 However, it is expected that many current operations in the lower end of the Specific category will be covered by standard scenarios, which already include the minimum set of requirements (in addition to those in the regulation) to be complied with, and will not therefore require the operator to perform the SORA process.

e) EASA will publish a "pre-defined risk assessment" as an AMC. This will contain requirements based on a pre-application of SORA, to guide operators in their operational authorisation process.

9. CONCLUSIONS

The purpose of the deliverable D2.2 CONOPS was to describe the operational needs, views, visions and expectations of the user's groups without provision of technical details on HELMET.

The HELMET CONOPS includes:

- Identification of different operational modes/ scenarios for RAIL, AUTO and UAVs applications;
- Identification of various operational environments and constrains;
- Derivation of High-level User Requirements for HELMET solutions;
- Overview of High-level User Requirements for HELMET;
- High-level safety concepts;
- Derivation of High-level safety requirements;
- High-level User safety requirements;
- Regulatory requirements for certification and authorization process.

The main output from the HELMET D2.2 CONOPS deliverable are the High-level User requirements – which have been also extracted from D2.2 and included a separate deliverable D2.1 User Requirements Specifications.

The HELMET CONOPS serves as a basis for specification of high-level functional and system requirements (to be done in D2.3) and related technical specifications. Further, user needs and performance measures identified in the CONOPS are the fundamental information for the HELMET Requirements Traceability Matrix and Validation Plan elaboration to be used to validate the HELMET concept at the end of this concept development phase. The overview of the regulatory requirements for certification and authorization process in given application areas (RAIL, AUTO and UAVs) will be utilised for standardization activities of HELMET solutions, to be performed within WP6.

10. REFERENCES

[1] 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.

[2] Liu, P., Yang, R., Xu, Z.: 'How Safe Is Safe Enough for Self-Driving Vehicles?' Risk Analysis Vol. 0, No. 0, 2018, 11 pages.

[3] Global status report on road safety 2015. https://www.who.int/violence_injury_prevention/road_safety_status/2015/en/

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

[5] EN 50126 'Railway Applications: The Specification and Demonstration of Dependability Reliability, Availability, Maintainability and Safety (RAMS)'. CENELEC European standard, 2002.

[6] Mokkapati, C.: 'A practical risk and safety assessment methodology for safety–critical systems'. Proc. of the AREMA 2004 C&S Technical Conference, Nashville, Tennessee, May 17-18, 2004, 18 pages.

[7] Braband, J.: 'Risk-oriented apportionment of safety integrity requirements – an example'. Signal + Draht (92) 1+2/2000, pp. 35-39.

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

[9] Jovicic, D.: 'Guideline for the application of harmonised design targets (CSM-DT) for technical systems as defined in (EU) Regulation 2015/1136 within the risk assessment process of Regulation 402/2013'. ERA, Doc. ref. ERA-REC-116-2015-GUI, Valenciennes Cedex, France, 23/12/2016, 139 pages.

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

[11] Aviation safety. https://en.wikipedia.org/wiki/Aviation_safety

[12] Comparison of transport modes: trains safer than buses and cars (2017) . https://www.allianz-pro-schiene.de/en/press-releases/comparison-of-transport-modes-trains-safer-than-buses-and-cars/

[13] Fourth Railway Package Still Divides Member States (2014). https://epthinktank.eu/2014/12/03/fourth-railway-package-still-divides-member-states/

[14] 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.

[15] Rail Cyber Security. RISSB (Rail Industry Safety and Standards Board) Safety Standars, Ref: AS 7770: 2018.

[16] Ref: ERTMS/ETCS Baseline 3 Onboard Subsystem Requirements: New Trains. Rail Industry Standard RIS-0798-CCS Issue: One, RSSB UK, September 2018.

[17] Ref: ERTMS/ETCS – Class 1, SUBSET-036: FFFIS for Eurobalise, 2007.

[18] ERTMS Users Group, Localisation Working Group (LWG): Railway Localisation System, High Level User's Requirements, Ref: 18E112, 28/01/2019, 17 pages.

[19] CENELEC Report R009-009, Ref.: No. R009-004:2001 E, 2001

[20] 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

[21] Manual for Validation of GNSS in Civil Aviation, EC DG Tren, Sept. 2000.

[22] Final Report – Risk Acceptance Criteria for Technical Systems and Operational Procedures. Report for European Railway Agency Report No: 24127328/03 Rev: 02, 22 January 2010.

[23] Higgins, Ch.: Travel Safety: Time versus Distance. Int. J. of Humanities and Social Science, vol. 5, No. 7(1), July 2015, pp. 132-133.

[24] Jang, H., A. et al.: A Study on Situation Analysis for ASIL Determination. J. of Industrial and Intelligent Information Vol 3., No. 2, June 2015, pp. 152 – 157.

[25] Rispoli, F., Neri, A., Stallo, C. et al.: 'Synergies for trains and cars era of virtual networking automation in the era of virtual networking'. J. of Transportation Technologies, Scientific Research Publishing, No. 8, 2018, pp. 175-193. https://file.scirp.org/pdf/JTTs_2018053115032399.pdf

[26] Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety.

[27] 'Report on the certification of ERTMS equipment'. The European Railway Agency, 14th April 2011, Document reference: ERA/REP/2011-08/ERTMS, 51 pages.

[28] Website of H2020 'ERSAT-GGC' project ; http://www.ersat-ggc.eu/

[29] EN 50128 'Railway Applications: Communications, signalling and processing systems – Software for railway control and protection systems'. CENELEC European standard, 2003.

[30] EN 50129 'Railway Applications: Safety related electronic systems for signalling'. CENELEC European standard, 2003.

[31] Filip, A., Sabina, S., Rispoli, F.: 'A Framework for Certification of Train Location Determination System Based on GNSS for ERTMS/ETCS'. Int. J. of Transport Development and Integration, WIT Press, Southampton, UK, Vol. 2, No. 3 (2018), pp. 284–297.

[32] Jovicic, D.: 'CSM for risk assessment: Proactive decision making instrument Consequences and benefits of latest changes'. Safety Conference of Danish Transport and Construction Agency - Copenhagen, 28th October 2015, presentation, 56 slides.

[33] Jovicic, D.: 'Explanatory note on the CSM Assessment Body referred to in Regulation (EU) N°402/2013 and in OTIF UTP GEN-G of 1.1.2014 on the Common Safety Method (CSM) for risk assessment'. The *European Railway Agency.* Document reference: ERA/GUI/01-2014/SAF, 17 pages.

[34] 'Collection of examples of risk assessments and of some possible tools supporting the CSM Regulation'. The European Railway Agency, 06/01/2009, Reference: ERA/GUI/02-2008/SAF, version 1.0, 105 pages.

[35] United Nations Regulation No. 79 on Uniform provisions concerning the approval of vehicles with regard to steering equipment, with effect from 29 January 1989. Annexed to the Agreement of 20 March 1958 concerning the adoption of uniform conditions of approval and

reciprocal recognition of approval for motor vehicle equipment and parts - done at Geneva, on 20 March 1958.

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

[37] 97/836/EC 'Revised 1958 Agreement'. UN ECE Agreement concerning the adoption of uniform technical prescriptions for wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles and the conditions for reciprocal recognition of approvals granted on the basis of these prescriptions.

[38] Regulation (EU) 2018/858 of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC.

[39] Frost, B.: ‘Automated Driving UNECE International Harmonization’. Presentation 2018, 12 slides. http://www.jasic.org/j/14_automated-driving/pdf/sympo3.pdf

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

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

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

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

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

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

[46] Lång, K. E: ‘Collaborative Approach Needed For Big Business’. Innovation Bazaar, RISE Viktoria, Vehicle ICT Arena 2018-02-08, 20 slides. https://vehicle.lindholmen.se/sites/default/files/content/bilder/1._victa_bazaar_-ad_collaborative_approach_needed_kent_eric_lang_rise_viktoria_180208_1.pdf

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

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

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

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

[51] Filip, A.: ‘Certification of EGNOS Safety-of-Life service for ERTMS according to IEC 61508 and EN 50129‘. Prepared for the COMPRAIL 2020 conference, organized by the Wessex Institute of Technology, originally scheduled in Berlin on 1-3 July 2020. Version 03/04/2020, 12 pages.

--- END OF FILE ---