Doctoral Dissertation
Doctoral Program in Aerospace Engineering (31th Cycle)

‘Safety Management System’ for light RPAS

Analysis of a real case: study on the safety and the integration in the civil airspace with an evaluation of the regulatory impact in Italy

Federica Bonfante
* * * * * *

Supervisors
Prof. ssa M. Battipede, Supervisor
Prof. P. Maggiore, Co-Supervisor
Prof. F. Grimaccia, Co-Supervisor

Doctoral Examination Committee:
Prof. A.B. , Referee, University of….
Prof. C.D. , Referee, University of…
Prof. E.F. , Referee, University of….
Prof. G.H. , Referee, University of…
Prof. I.J. , Referee, University of….

Politecnico di Torino
February 29, 2123

I hereby declare that, the contents and organisation of this dissertation constitute my own original work and does not compromise in any way the rights of third parties, including those relating to the security of personal data.

…….....

Federica Bonfante

Turin, February 29, 2123

Summary

This Doctoral Thesis sums up the carrying out of the research work and the results obtained from the safety analysis starting from the concept of 'Safety Management System' applied to Remotely Piloted Aircraft Systems (RPAS). With reference to the incoming integration of RPAS into not segregated airspaces, the future real case of specific category flight operations within the U-Space has been more precisely considered and studied.

The basic idea for the research derived from the guidelines issued by ICAO in the Annex 19 (2013) stating that every aeronautical operator shall implement a 'Safety Management System' within its own organization to be authorized to fly into the civil airspace: this indication applies to incoming RPAS operators too (ICAO Document 10019).

The Remotely Piloted Aircraft Systems are a subset of unmanned aerial systems composed of the unmanned aerial segment (the aircraft), the ground segment (a station or a remote portable radio controller) and the command and control radio link (C2) used by the human pilot to control and manage the aerial platform from ground.

The aviation authorities and, in general, the aviation community, guessing the potential high economic value of RPAS flight operations recognized that it could be adequately exploited only allowing their full integration into the civil airspaces.

Starting from these premises, a comprehensive safety analysis has been performed identifying and assessing safety hazards and possible mitigation provisions and thus implementing two risk matrices: the first one has been draft reasoning on the safety hazards related to the full integration of RPAS into uncontrolled airspaces (U-Space served); the second one has been draft reasoning on the safety hazards related to the full integration of RPAS into controlled airspaces (ATM served).

In accordance with the definition of Safety Management System (the continuous activity of identifying, assessing and mitigating risks to maintain their effects at or below an acceptable level), the content of the U-Space risk matrix has been used to layout a more advanced risk mitigation provision modelled as a rule-based 'Expert System'. The model has been focused on the implementation of the basic stage of an 'Expert System', that is its knowledge basis built as a collection of rules. The rules have been designed to be activated or not by specific precursors of previously analysed hazards and to alert the remote pilot on incoming risks in real time. In addition, they have been thought to provide him/her or the RPA flight control system (in case of fully automated RPAS flight operations) with real time decisional support about the most proper mitigation action to apply against the hazard occurring during a specific category flight mission in the not segregated airspace below 500 feet.

The above mentioned steps of the research have been used to define a proposal for a comprehensive RPAS functional architecture oriented towards mitigation of flight risks in the U-Space and to critically review the current technical solutions proposed to operatively deploy the incoming U-Space service.

The research on safety analysis on RPAS has been completed with an example of application of the STPA ('System-Theoretic Process Analysis') hazards analysis technique to show more recent methodologies beside the traditional and consolidated ones used in this research.

Finally, the impacts of the performed safety analysis on Italian RPAS regulation have been evaluated through a critical review of its state of art performed in the light of the results got from the safety analysis object of the research.

Beside the above described main topic of this work, considerations on safety and operative requirements for hybrid RPAS fed by hydrogen fuel cells have been carried out due to the necessity of enhancing remotely piloted aircraft systems endurance and range to really allow their full integration into civil non segregated airspaces.

The following points are hereinafter definitely highlighted as original added values of this work: starting from a regulation gap and, at the moment of performance of the present study, poor literature availability about, the performed study is an example of a safety analysis starting from a real case study and capable to fit with multiple RPAS in the U-space.

Acknowledgment

At the end of this work my acknowledgement is for my Tutors, Professor Paolo Maggiore (Politecnico di Torino), Professor Manuela Battipede (Politecnico di Torino) and Professor Francesco Grimaccia (Politecnico di Milano) for their advices and guidance while overviewing me during the performance of all the activities foreseen by the Ph. D. course and for Engineer Edoardo Filippone (CIRA) for his courtesy and availability to support me to better understand the deepest contents and aims of the incoming integration of RPAS into the civil airspace.

This work is dedicated to Irene and Noemi: follow your dreams until they will come true.

'If Winter comes, can Spring be far behind?'

From the 'Ode to the West Wind'
Percy Bysshe Shelley, 1792 - 1822

Contents

List of Tables

List of Figures

List of units of measure

Ft.	Feet
K	Kelvin degrees
Kg	Kilograms
MPa	MegaPascal

List of abbreviations and acronyms

3D	Dull, Dirty and Dangerous
4D	Four dimensions
4G	Fourth Generation
5G	Fifth Generation
ABAS	Aircraft Based Augmentation System
ACAS	Airborne Collision Avoidance System
ADS-B	Automatic Dependent Surveillance – Broadcast
AND	AND Boolean Logical Operator
ATC	Air Traffic Control
ATM	Air Traffic Management
ATZ	Aerodrome Traffic Zone
BAT	Buster Air Traffic
BIT	Built In Test
BITE	Built In Test Equipment
BRLOS	Beyond Radio Line of Sight
C2L	Command and Control link
CA	Control Action
CIRA	Centro Italiano Ricerche Aerospaziali
CNS	Communication Navigation and Surveillance
CONOPS	Concept of Operations
CR	Close Range
CRM	Crew Resource Management
CTR	Control Traffic Region
DAA	Detect and Avoid
DC	Direct Current
DEC	Decoy

DN	Detectability Number
Doc.	ICAO Document
EASA	European Safety Aviation Agency
ECU	Engine Control Unit
EGNOS	European Geostationary Navigation Overlay System
ENAC	Ente Nazionale Aviazione Civile
ENAV	Ente Nazionale Assistenza al Volo
ESC	Electronic Speed Control
ETA	Event Tree Analysis
ETSO	European Technical Standard Order
EU	European Union
EUROCAE	European Organization for Civil Aviation Equipment
EUSCG	European UAS Standards Coordination Group
EVLOS	Extended Visual Line of Sight
EXO	Exo-stratospheric
FCC	Flight Control Computer
FHA	Fault Hazard Analysis
FL	Flight Level
FLARE	Flying Lab for Experimental Research
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes and Effects and Criticality Analysis
FMS	Flight Management System
FPV	First Person View
FTA	Fault Tree Analysis
FTS	Flight Termination System
GATM	Global Air Traffic Management
GBAS	Ground-Based Augmentation System
GCS	Ground Control Station
GEO	Geostationery Earth Orbit
GLONASS	Global'naja Navigacionnaja Sputnikovaja Sistema

GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HALE	High Altitude Long Endurance
HAZOPS	Hazard and Operability Studies
HFACS	Human Factor Analysis and Classification System 2000
HMI	Human Machine Interface
IAS	Indicated Airspeed
ICAO	International Civil Aviation Organization
IFR	Instrumented Flight Rules
IMU	Inertial Measurement Unit
IoT	Internet of things
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
LADP	Low Altitude Deep Penetration
LALE	Low Altitude Long Endurance
LIDAR	Laser Imaging Detection and Ranging
LiPo	Lithium Polymer
LTE	Long Term Evolution
MALE	Moderate Altitude Long Endurance
MATS	Malta Air Navigation Service
MCC	Mission Control Centres
MR	Moderate Range
MRE	Moderate Range Endurance
MTBF	Mean Time Between Failure
MTOW	Max Take Off Weight
MTTR	Mean Time To Repair
NASA	National Aeronautics and Space Administration
NDZ	No-Drone Zone
NextGen	Next Generation Air Transportation System
NLES	Navigation Land Earth Stations
NOTAMs	Notices to Airmen

NPA	Notice of Proposed Amendment
OPV	Optionally Piloted Vehicle
OR	OR Boolean Logical Operator
PBN	Performance Based Navigation
PN	Probability Number
PSR	Primary Surveillance RADAR
RADAR	Radio Detection and Ranging
RAID	RPAS-ATM Integration Demonstration
RIMs	Ranging & Integrity Monitoring Stations
RLOS	Radio Line of Sight
RNAV	Area Navigation
RNP	Required Navigation Performance
RPA	Remote Piloted Aircraft.
RPAS	Remotely Piloted Aircraft. Systems
RPS	Remote Pilot Station
SARPS	Standard and Recommended Practices
SBAS	Satellite-Based Augmentation System
SESAR	Single European Sky ATM Research
SESAR1	Single European Sky ATM Research 1
SESAR-JU	Single European Sky Air Traffic Management Research Joint Undertaking
SHELL	Software Hardware Environment Liveware Liveware
SIDs	Standard Instrument Departures
SMS	Safety Management System
SN	Severity Number
SOL	Safety of Life
SONAR	Sound Navigation and Ranging
SPACE	Space
SR	Safety requirement
SR	Short Range

SSP	State Safety Program
SSR	Secondary Surveillance RADAR
STAMP	System-Theoretic Accident Model and Processes
STARs	Standard Instrument Arrivals
STPA	System Theoretic Process Analysis
STRATO	Stratospheric
UAS	Unmanned Aircraft System
UCA	Unsafe Control Action
UCAV	Unmanned Combat Aerial Vehicle
UIR	Upper Flight Information Region
US	United States
USA	United States of America
UTM	Unmanned Traffic Management
VDB	VHF Data Broadcast
VFR	Visual Flight Rules
VHL	Very High Level
VLA	Very Light Aircraft
VLL	Very Low Level
VTOL	Vertical Take Off Landing
XOR	XOR Boolean Logical Operator

Chapter 1

Introduction

1.1 Objective of the research

The present research work takes origin from the idea of implementing a 'Safety Management System' (SMS) for Remotely Piloted Aircraft Systems (RPAS). RPAS are aircraft without the pilot on board, but located on a remote pilot station and remotely conducting the flight operations through a portable radio command or a ground station and using commands, controls and displays (fed by telemetry data sent by the aerial platform) similar to those installed in the cockpit of manned aircraft.

According to the new vision of ICAO Annex 19, in addition to the historical eighteen annexes already in use, aircraft and aerial operations safety management is elevated at the level of State responsibility and every user of the airspace shall demonstrate to have implemented and to routinely apply an SMS to manage safety of own assets and aerial activity [1]. RPAS operators undergo these guidelines as manned aircraft operators.

More precisely, the idea of implementing a 'Safety Management System' for RPAS descends from the ICAO regulation reported at paragraph 7.3.2 of Doc. 10019, 'Manual on Remotely Piloted Aircraft System (RPAS)' issued in 2015 [2] and stating that:

'7.3.2 Irrespective of the type of operation (e.g. private, corporate, commercial), all RPAS operators must be certified by the State. One of the requirements for certification is expected to be that the RPAS operator has implemented an effective SMS.'

The responsibility for safety is inferred to the State [1] which has to issue a State Safety Program (SSP) that every aeronautical operator has to comply with to

be authorized to use the civil airspace. An SSP is an integrated set of regulations and activities aimed at improving safety. This obligation is now extended to RPAS operators too as incoming new actors of the current aviation scenario. The RPAS operators are equalized to any other operator of the manned aviation community and the RPAS safety shall be managed as for manned aircraft.

The 'Safety Management System' or SMS is a comprehensive and systematic approach to safety management. In aeronautics it started to be applied from the mid-1990s [3]. It relies on the systematic and continuous identification of the performed activity safety hazards (ground and aerial) and on keeping the related safety risks under a proper acceptable level defined in terms of probability of occurrence and severity of consequences [3].

As furtherly stated by Doc. 10019 at paragraph 6.2.2. [2]:

'*The RPAS operator must comply with all requirements established by the State of the Operator regarding its operation. These requirements should be consistent with the size, structure and complexity of the RPAS operator's.*'

The safety requirements issued by the State of Registry of the RPAS and the related applicable SMS shall fit the RPAS operator type and category and structure of operations size and complexity: remote piloted aircraft systems deeply differ from manned aircraft in terms of size and technical features and in terms of type and way of conduction of flight operations. This aspect will be properly highlighted in this work when necessary.

The definition of 'Safety Management System' and the contingent need for the implementation of an SMS suitable for RPAS organizations and operators have been recognized as a proper topic for a new research work: the performance of the safety analysis of the risks and mitigation actions related to the integration of RPAS into the civil airspace.

This thesis consists of seven Chapters and eight sections in Appendix (Appendixes A ÷ H). The First Chapter describes the concept of RPAS, the aviation operating scenario where they will be integrated in, the approach chosen by the European Aviation Authorities to manage their incoming in the civil not segregated airspace. The Second Chapter sums up the theoretical fundamentals of safety risk analysis in aviation that has been used in the safety analysis object of the research. The Third Chapter reports the content of the performed safety risk analysis considering both operations in the uncontrolled not segregated airspace (between 0 and 500 feet of altitude) managed by the U-Space service and operations in the controlled not segregated airspace managed by 'Air Traffic Management' (ATM). From this point onwards, the thesis has been focused on the flight operations that will be performed in the uncontrolled space served by the U-Space: in fact, this scenario will be the first to be arranged by the European Aviation Authority (EASA) and therefore, at the moment, it has been of cogent interest for this research. The Fourth Chapter introduces the 'Expert Systems' focusing on the rule-based ones and describes the design of the knowledge basis derived from the U-Space risk matrix. The Fifth Chapter describes and discusses

the proposal of an RPAS architecture oriented to safety risk mitigation of specific category flight operations under the U-Space service; further, it reviews current proposals of infrastructures elaborated in Europe to operatively deploy the U-Space service. The Sixth Chapter describes and discuss an example of application of the 'System Theoretic Process Analysis' (STPA) safety analysis methodology to the RPAS flying into non segregated airspaces hazard scenario. The Seventh Chapter, critically reviews the current Italian RPAS regulation on the basis of the performed safety analysis. Finally, the 'Conclusion' Chapter reconsiders the performed research work highlighting novelties with respect to current state of art about the research topic, limitations of the carried out choices and possible future developments.

With reference to the sections in Appendix: Appendix A reports the FMECA analysis results; Appendix B reports the RPAS safety of operations related human factor analysis results; Appendix C reports the FTA analysis results; Appendix D reports the safety risks analysis results (U-Space and ATM risk matrices). As above stated, after the risk matrixes implementation, the research has been focused on the flight operations that will be performed in the uncontrolled space served by the U-Space: therefore from this point onwards, Appendix E reports the Bow Tie schemes on mitigation provisions with reference to the U-Space risks (the most significant hazards have been considered only); the Appendix F reports the rules composing the 'Expert System' knowledge basis derived from the U-Space safety risk matrix. As additional topics to the main theme of the performed research, Appendix G reports the results of the application of the STPA hazard analysis to an example of specific hazard scenario; the Appendix H reports and discusses a proposal for operative and safety requirements for an hybrid RPAS (fed by hydrogen fuel cells) model.

1.2 Remotely Piloted Aircraft System (RPAS)

A 'Remote Piloted Aircraft System' (RPAS) is an aircraft conducted by a pilot remotely located (typically on ground, or also on other aircraft) and not on board the aircraft through a command and control (C2) radio link. The RPAS are a subset of 'Unmanned aircraft systems' (UAS) [4]. In fact, UAS can be manually, automatically or fully autonomously piloted: in the first case the aircraft is remotely controlled by the human pilot; in the second case it is managed by the on board autopilot, but with the pilot able to take the control of the aircraft in unexpected conditions; in the last one the flight is performed without allowing any pilot intervention. With reference to this categorization, the research object of this thesis has been performed in accordance with the following ICAO regulation [2]:

As a general consideration, Article 8 of the 'Convention on International Civil Aviation':

'No aircraft. capable of being flown without a pilot shall be flown without a pilot over the territory of a contracting State without special authorization by that State and in accordance with the terms of such authorization….'.

As a further more detailed guideline, paragraph 2.2 of [4]:

'Only the remotely-piloted aircraft (RPA), …, will be able to integrate into the international civil aviation system in the foreseeable future. The functions and responsibilities of the remote pilot are essential to the safe and predictable operation of the aircraft as it interacts with other civil aircraft and the air traffic management (ATM) system. Fully autonomous aircraft operations are not being considered in this effort, nor are unmanned free balloons nor other types of aircraft which cannot be managed on a real-time basis during flight.'

The RPAS are composed of the 'Remote Piloted Aircraft' (RPA), in this thesis also referred to as aerial segment or aerial platform, the 'Remote Pilot Station' (RPS), in this thesis also referred as the ground segment, the 'Command and Control Radio Link' (C2L) ([2], [4]). The remote pilot can operate the aerial platform using a hand-held portable radio controller, simpler (Figure 1 [5]), for RPAS comparable to toys or (Figure 2 [6]) more advanced, for RPAS for civil professional/commercial use, or a complete remote ground control station (even a multi-console one) (Figure 3 [7]), this last one typical of RPAS for military use, at the moment. The RPS hosts the controls to fly the RPAS and manage the flight (also on the basis of displays of telemetry data, sent by the RPA on the downlink channel). The RPS can be located inside or outside, stationery or mobile (that is installed in a moving vehicle/ship/aircraft, again with reference to military applications in most cases, at the moment) [4]. The radio link can be simple or redundant; it mainly consists of the uplink channel to send command signals to the RPA and the downlink channel to receive telemetry data from the RPA; it can be designed to control and manage the aircraft from direct 'Radio Line of Sight' (RLOS) to 'Beyond Radio Line of Sight' (BRLOS) [4]. In RLOS case the RPAS transmitting and receiving antennas are within mutual radio link coverage and signals can be exchanged in a comparable timeframe. In BRLOS, the radio link is supported by satellite systems or terrestrial networks to maintain the ground and aerial segments in contact and in some applications (military ones) more RPS can be used to manage very complex and long endurance operations; the necessary timeframe to make RPA and RPS communicate is further beyond the one of the RLOS case. The BRLOS operations are characterized by a higher communication delay than RLOS ones [2]. The interruption of communication between the ground and the aerial segments is indicated as 'lost link' condition.

Figure 1 – Example of RPAS portable remote controller [5]

Figure 2 – Example of rugged RPAS portable remote controller [6]

Figure 3 – Example of RPAS Ground Control Station [7]

An RPA system usually comprehends the following subsystems [2]:

- The Launch and Recovery equipment for RPA take-off and landing (like, for example: catapult, winch, rocket, net, parachute, airbag)
- The Flight Control Computer (FCC), the Flight Management Subsystem (FMS) and the Autopilot
- The Navigation Subsystem
- The Propulsion Subsystem

- The Communication Subsystem, including equipment to allow the remote pilot to communicate with Air Traffic Control (ATC), and systems to support Radionavigation
- Surveillance subsystem, to allow the RPA to be tracked by primary and secondary surveillance systems or through the use of 'Automatic Dependent Surveillance – Broadcast' (ADS-B) equipment
- The Power subsystem
- The Electrical Distribution subsystem
- The Structures
- The Health Monitoring Subsystem
- The 'Flight Termination Subsystem' (FTS) designed to manage an intentional controlled RPA flight termination in case of emergency

The RPAS are a more diversified technology than manned aircraft as shown by the categorizations reported hereinafter:

- With reference to weight and performances reachable with current technology, the RPAS are classified as shown in Table 1 [8]:

  From Table 1 [8], a more synthetic classification of RPAS according to MTOW can be derived as follows [9]:

  - Mini RPAS: MTOW from 0 up to 14 kg
  - Small RPAS: MTOW from 15 up to 199 kg
  - Medium RPAS: MTOW from 200 up to 1999 kg
  - Heavy RPAS: MTOW above 2000 kg

  The Light RPAS are considered in this thesis; with reference to the above reported list; 'Light RPAS' are those ranging from Mini to Moderate RPAS with upper limit equal to 150 kg MTOW, according to European/Italian regulation.

- With reference to the wing configuration, the RPAS are classified as follows ([9], Figure 4 [9]):

  - Fixed wing RPAS
  - Free wing RPAS
  - Rotary wing RPAS
  - Tilt wing/rotor RPAS
  - Tail sitters

Table 1 – UAS/RPAS classification [8]

UAS/RPAS Category	Acronym	Range [km]	Flight altitude [m]	Endurance [hours]	MTOW [Kg]	Currently flying
TACTICAL						
Nano	η	< 1	100	< 1	< 0,025	YES
Micro	μ or 'Micro'	< 10	250	1	< 5	YES
Mini	Mini	< 10	From 150 to 300	< 2	< 30	YES
Close Range	CR	From 10 to 30	3000	2 to 4	150	YES
Short Range	SR	From 30 to 70	3000	3 to 6	200	YES
Moderate Range	MR	From 70 to 200	5000	6 to 10	1250	YES
Moderate Range Endurance	MRE	> 500	8000	10 to 18	1250	YES
Low Altitude Deep Penetration	LADP	> 250	From 50 to 9000	0.5 to 1	350	YES
Low Altitude Long Endurance	LALE	> 500	3000	> 24	< 30	YES
Moderate Altitude Long Endurance	MALE	> 500	14000	24 to 48	1500	YES
STRATEGIC						
High Altitude Long Endurance	HALE	> 2000	20000	24 to 48	12000	YES
SPECIAL PURPOSE						
Unmanned Combat Aerial Vehicle	UCAV	Around 1500	10.000	Around 2	10000	YES
Lethal	LETH	300	4000	3 to 4	250	NO
Decoy	DEC	From 0 to 500	5000	< 4	250	NO
Stratospheric	STRATO	> 2000	Within 20000 and 30000	> 48	TBD	NO
Exo-stratospheric	EXO	TBD	> 30000	TBD	TBD	TBD
SPACE	SPACE	TBD	TBD	TBD	TBD	TBD

Figure 4 – RPAS classification according to wing configuration [9]

- Finally, with reference to the propulsion subsystem configuration, the RPAS can be classified as follows [10] and [11]:
  - Turbojet fixed wing RPAS

- Turboprop fixed wing RPAS
- Reciprocating fixed wing propeller (electric propulsion) RPAS
- Vertical Take-Off and Landing RPAS (VTOL RPAS)
- Airship (Lighter than Air)

1.2.1 Economic added value expected from RPAS

The integration of RPAS with manned aircraft is strongly encouraged by the scientific, technical and industrial community both for the 'disruptive' features of this technology and for the economic added value expected from it. The lack of the pilot on board RPAS opens the way to more different airframe configurations and more risky applications than manned aircraft: this issue potentially allows valuable developments of the RPAS market with expected economic return around 10 billion Euro annually by 2035 and over 15 billion Euro annually by 2050 ([12], [13]).

The possibility to fly aircraft without the pilot on board goes back to the years of the Second World War. In 1944 ICAO officially acknowledged the existence of UAS in the Chicago Convention. After the war, since 1950s, such aerial vehicles have been used almost exclusively for military purposes. Recent conflicts and peace-keeping operations around the world have further demonstrated and confirmed their operational capabilities from a military point of view. Consequently, during the European Summit on the Future Defence Policy hold on the 19th December 2013 a formal commitment was made to further enhance the European RPAS military assets capability but a new interest has been clearly expressed for civil use of RPAS [14].

Years from 2005 to present day have been a very fertile period to make RPAS tecnology feasible and more economically viable and competitive in the civil market thanks to the introduction of novel lighter and more resistant materials and thanks to new software, communication, data processing and miniaturisation tecniques applicable to RPAS too [13].

The remotely piloted aircraft are expected to bring benefits from their extensive application in many sectors (agriculture, infrastructures monitoring, etc.), allowing the decrease of human beings fatal injuries or death when aerial works must be performed; the expected birth of new professional figures (remote pilots, remote aircraft manufacturers, analysts of RPAS payload data, etc) and extension of interests of exixting economic sectors into remotely piloted aircraft industrial sector have been already occurring (like, for example, insurances) [14].

The key to reach such economic advantages will be the full and safe integration of RPAS into not segregated airspace alongside manned aircraft ([12] and [14]) unifying and uniforming the different rules and industrial standards in force across the European Union states and, in addition, enforcing the continental RPAS market with respect to other markets in the world. In fact, the current European RPAS market still suffers from the fact that the regulations for RPAS below 150 kg of MTOW (light RPAS) is fragmentary having been left to the responsibility of the single Member States [14], while the 'European Aviation

Safety Agency' (EASA) takes care for RPAS above 150 kg of MTOW only [15]. In the next future it is intention of the European Union to regulate all RPAS used in the Member States and strongly fostering the light RPAS market for civil use [15].

Hence, the current work of European Aviation Authorities is addressed both to identify affordable risk models to face and mitigate the hazards related to the integration of RPAS with manned aircraft and to create a new set of common regulations, industry standards and market product requirements to allow the industrial development, distribution and safe flight operations of RPAS across Europe.

According to its formal mission, ICAO is addressing RPAS regulatory framework at worldwide level. It has set-up a specific panel to prepare SARPS for RPAS integration into the airspaces. Following the first available guidelines issued by ICAO on RPAS, the 'European UAS Standards Coordination Group' (EUSCG), including, among the others, the 'Single European Sky ATM Research' (SESAR), the 'Joint Authorities for Rulemaking on Unmanned Systems' (JARUS) and the 'European Organization for Civil Aviation Equipment' (EUROCAE) (mainly for the definition of industry standards) are working to issue a common regulation for RPAS safe flight operations in Europe ([12]).

This work on regulation will allow the concrete development of a new European global and competitive RPAS market; this will also overcome other difficulties like the fact that, at the moment, third countries, such as the United States, do not accept the European validation process and consequently the RPAS products, especially if carried out by non-aviation authorities [14].

The European RPAS industries, go from start-ups to small/medium sized companies arriving until global players. This layout reflects the wide range of available unmanned systems from micro aerial platforms of few tens of grams of maximum take-off weight to those of size and performance comparable to an Airbus 320 commercial liner aircraft [14].

In conclusion, RPAS represents a great potential to change the civil aviation and society [16], provided that aviation authorities, governments and industries will develop the best regulatory framework to allow their full but safe integration with manned aircraft.

1.2.2 RPAS applications

With reference to civilian applications, RPAS have been basically conceived to carry out the so called '3D' duties that is operations that can be 'Dull', 'Dirty' or 'Dangerous' [4] for the human pilot of manned aircraft. The civilian applications of RPAS have been successively extended to commercial, scientific and security sectors developing and sharpening monitoring, communication and imaging functions [4] through the use of more and more sophisticated payload sensors.

The following are typical civilian applications of RPAS technology [17]: monitoring/inspection of pipelines, railroads, highways, traffic flows, coastlines, solar or windmill plants, oil rigs, oil spills, flood risk, forestry, snow pack avalanches, ice packs, clouds, volcanoes, nuclear plants; logistics for the delivery of goods; wildlife inventory, through the performance of aerial mapping and survey, cinematography, fire prevention and assessment, biological agents detection, archaeology, crop dusting, sport or music events surveillance, photogrammetry, tidal zones mapping, meteorology; performance of public safety, search and rescue and security operations.

1.2.3 Full integration into the civil airspace

Currently, the RPAS are authorized to fly into segregated airspaces that is limited portions of airspace outside and separated from manned aircraft routes in such a way that interference with manned aircraft and the risk of mid-air collisions with them is maintained at a reasonable acceptable low level or it is potentially completely avoided.

The change requested to really achieve the economic benefits expected from the RPAS market is the complete merging of RPAS with manned traffic, that is the RPAS full integration into the civil not segregated airspace. As previously stated, for the moment, in accordance with ICAO guidelines (paragraph 2.2 of [4]), remotely piloted aircraft managed on a real time basis during flight operations only will be fully integrated in the civil airspace. Automatic or semiautomatic operations (a mixture of automatic and manual operations) will be allowed in the civil airspaces, but not fully autonomous operations. Operations of autonomous RPAS will be allowed in the civil airspaces only if strictly necessary, under special provisions and/or using segregated subspaces (paragraph 2.2 of [4]); in any case, this arrangement will not be equivalent to a full integration of RPAS into civil airspace and it has not been considered in this thesis.

Within the integration of RPAS with manned aircraft, compensations for the absence of the human pilot on board shall be put in action in order to replicate his/her ‘See and Avoid’ capability that is the capability to see other aircraft or ground-based natural and man-made obstacles during flight operations and avoid collisions with them. The human pilot of manned aircraft usually accomplishes such task relying on his/her sight and on board flight instruments (like TCAS for example) or being supported by air traffic controllers who provide the on board crew with proper flight levels and instructions to maintain proper separation from other traffic.

The full integration of RPAS into the civil airspaces will be addressed by the following general principles: it will be gradual but it will occur in the medium term (within 2030 according to [12]); the manned aircraft transport system will not adequate to RPAS: the opposite will occur; RPAS will have to adequate to manned aircraft transport system rules [18]; a minimum set of safety requirements will have to be met by RPAS to safely operate with manned aircraft [4]; the

presence of RPAS alongside manned aircraft shall not impact the current safety level reached by the aerial transport sector.

1.2 The current operating aerial scenario

The current aerial operating scenario where in the medium term RPAS will be fully integrated with manned aircraft has been gone under deep changes in the last years mainly due to the increase of commercial traffic.

The civil airspace management is changing to fit with a new global management strategy due to the mentioned expected growth of commercial traffic volumes: the 'Global Air Traffic Management' (GATM) [19]. The novel elements of GATM that are of interest for RPAS integration into the airspace are hereinafter reminded and briefly described because these issues will be involved in some cases in the safety risk assessment object of this thesis.

The integration of RPAS into the civil airspace is a matter of management of these new users flight operations within the airspace. Currently the civil airspace is divided into two main subcategories: controlled airspaces and uncontrolled airspaces [20]. Within the controlled airspaces the air traffic controller has the responsibility to support the pilots to maintain recommended horizontal and vertical separations from other aircraft, from ground, from bodies of water and from any other natural or man-made obstacle along the flown track. In this case, the pilot has to follow the controller clearances/instructions. Further, the pilot periodically communicates with the controller about the relevant circumstances of interest during the given phase of flight. In the uncontrolled airspace, without ATC service, the pilot is responsible for the safe conduct of the aircraft using available flight information and advisory traffic services [20]. As it will be better described in the next paragraphs, RPAS will fly both within controlled and uncontrolled airspaces according to the type of planned sortie. The lack of the human pilot on board the RPAS introduces relevant safety critical issues to the above described scenarios.

Notwithstanding the new management strategies to optimize the use of the civil airspace facing the expected traffic volume increase, the safety of navigation always remains the main priority; the following sums up the novel elements brought by the GATM guidelines.

The new global airspace will act as an integrated single continuum airspace able to host both manned and remotely piloted aircraft up to transiting space-vehicles; it will be arranged to overcome current limitations like congested voice communications or too much rigid structured routes; the airspace, the airdromes and the human operators, supported by more advanced decisional tools based on real time technology and accurate information will provide a flexible and scalable integrated service. Manned or unmanned vehicles trajectories will be managed as dynamic four dimensions (4D) trajectories; the interactions among them or other issues will be managed as temporary hazards to achieve the best outcome with the minimal deviation from the user-requested flight trajectory, whenever possible. The new integrated service will be adaptable to accommodate a variety of air

activities, volumes of traffic and levels of service. The restrictions to the use of a volume of airspace will be assimilated to transitory conditions; the airspace boundaries will be adjusted to traffic flows and not accordingly to national boundaries anymore. Aerodromes, as integral part of the system, will be managed in order to reduce runaway occupancy and optimizing on air flight time. The airspaces and aerodromes demand and capacity will be balanced through an efficient management of air-traffic flow, weather and assets information. The mid-air conflict management, potentially further enhanced by the incoming integration of RPAS, will be a critical aspect of this balance and will influence the traffic synchronization, the separation provision and the collision avoidance. All the airspaces will be matter of the ATM and will be thought as usable resources. Its allocation and organization will be flexible and based on the principles of access and equity [19].

The conflict management will be managed following a three levels strategy: the first level of strategic conflict management will be achieved balancing the airspace organization and management, demand and capacity, and traffic synchronization components; the second level of conflict management will be the separation, that is the tactical process of keeping manned and unmanned aircraft one away from the other applying the appropriate separation minima; the third level of conflict management will be the collision avoidance and it will have to be activated when the separation mode (above mentioned second level) has been compromised. Technological surveillance systems based on cooperative aerial traffic like 'Automatic Dependance Surveillance - Broadcast' (ADS-B) or traditional ground-based surveillance systems suitable for not cooperative traffic too will support the real time traffic management between cooperative/not cooperative RPAS and manned aircraft [19].

The meteorological information service will be a function integrated in the ATM system and it will be exploited to optimise flight trajectories [19].

The evolution of 'Area Navigation' (RNAV) procedures will furtherly play a primary role. In fact, they are navigation procedures which permit aircraft operations on any desired flight path within the coverage of a station-referenced navigation aid or within the limits of the capability of self-contained aids, or according to a combination of them. With RNAV advent, aircraft are no more constrained to an airway [21]. This issue specifically addresses more and more to leave rigid structured routes towards an optimised use of the airspace volume and thus helping to easily host the future expected growth of commecial traffic. 'Required Navigation Performance' (RNP) certified equipment are necessary on board the aircraft to fly RNAV procedures and following the desired more efficient path with exceptional accuracy and with noticeable saving of fuel [20]. The RNAV procedures are a subset of 'Performance Based Navigation' (PBN) procedures that defines aircraft RNAV equipment performance in terms of accuracy, integrity, availability, continuity and functionality required for the given operation in the context of a particular airspace concept, when supported by the appropriate navigation infrastructure [22]. A different level of accuracy is required to RNAV/PBN navigation system depending on whether the considered

route is an oceanic one or the route leading the aircraft during the approach phase towards an aerodrome (Figure 5 [22]). Among such equipment, the 'Global Navigation Satellite System' (GNSS) [23] is of interest for the RPAS safety analysis object of this thesis. The Global Navigation Satellite Systems are satellite based navigation systems. Thanks to their higher precision and lower costs are successfully supporting traditional ground based navigation aids like Primary and Secondary Surveillance RADARs (PSR and SSR, respectively) [24]. The navigation satellite systems rely on GPS and GLONASS costellations (managed by USA and Russian Federation respectively), both compliant with ICAO Annex 10 performance requirements on aeronautical telecommunications [25]. They broadcasts a timing signal and a data message that includes the satellite ephemeris data. The aircraft are equipped with GNSS receivers that use these signals to calculate their range from each satellite in view, and to fix their three-dimensional position and time. A GNSS receiver is mainly composed of an antenna and a processor to compute position, time and, eventually, other information depending on the application. The receiver needs measurements from a minimum of four satellites to establish three-dimensional position and time. The accuracy depends on the precision of the measurements from the satellites and the relative positions and geometry of the satellites used [25]. The current exixting core satellite constellations alone do not meet strict aviation requirements. In order to reach this aim for each phase of flight, the core satellites need for technological enhancements. Three solutions are currently avalable [25] named 'Aircraft.-Based Augmentation System' (ABAS), 'Ground-Based Augmentation System' (GBAS) and 'Satellite-Based Augmentation System' (SBAS), the last one of interest for RPAS and considered in the safety analysis object of this thesis. as follows [25]. Satellite-Based Augmentation Systems uses ground stations to verify the validity of satellite signals and calculate corrections to enhance accuracy; then it delivers those data to the users via 'Geostationery Earth Orbit' (GEO) satellites. In Europe, the Satellite-Based Augmentation System in use is the SBAS EGNOS; the level required for aviation is indicaed as 'Safety of Life' (SOL) service level [26]. It provides a very precise satellite guide to aircraft into the European Airspace with a lateral/vertical accuracy of 16/20 meters against a 220/400 meters of traditional navigation aids and an horizontal alert limit/vertical alert limit of 40/50 meters against 556 meters/'not applicable' of traditional navigation aids respectively. The signal availability is 99% [25]. The EGNOS system, composed of a Space and a Ground segment, is more accurate than other navigation aids beause it collects data from the GPS constellation through the network of ground stations located in Europe and named 'Ranging & Integrity Monitoring Stations' (RIMs). Each GPS satellite is monitored by multiple RIMs. The monitorig stations transmit the GPS data to four 'Mission Control Centres' (MCC) that generate the augmented signal; this one, that is the signal with accuracy enhanced by the corrections and the integrity messages is transmitted by the six 'Navigation Land Earth Stations' (NLES) to the EGNOS geostationary satellites to be broadcasted to the users. The users aircraft shall be equipped with an EGNOS receiver on board. In space, the EGNOS is supported by three telecommunication geostationary satellites [25].

With reference to PBN requirements, the EGNOS accuracy is defined as the difference between the measured and the real position, speed or time of the receiver (measured on 95% of the time of use); the EGNOS continuity is the capability of the system to provide confidence thresholds as well as alarms in the event that anomalies (confidence threshold bigger than alarm limits for a period of 15 sec) occur in the positioning data; the EGNOS integrity is the capability of the system to work without any interruption; the EGNOS availability is the percentage of time during which the signal fulfils the accuracy, integrity and continuty criteria [26].

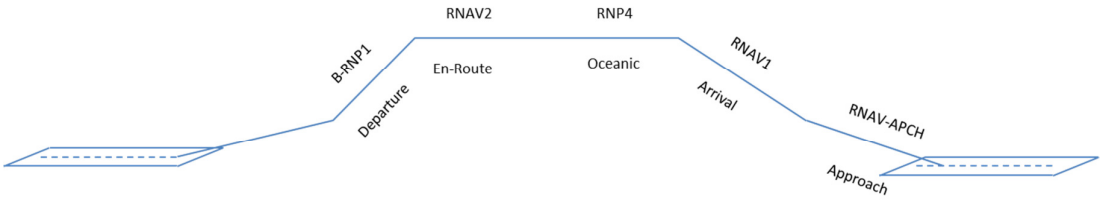


Figure 5 – An example of RNAV/PBN requirements application [22]

1.3 Integration of RPAS in Europe: the EASA risk centric approach

In Europe, the 'European Aviation Safety Agency' (EASA) regulates safety of aerial transport and within this issue it cares for RPAS safe integration into the airspace. In 2017 EASA officialised its approach on this topic issuing a 'Notice of Proposed Amendment' (NPA) to prepare the emission of a new RPAS Basic Regulation [26].

EASA proposes an approach to the integration of RPAS into the airspace based on the following hypotheses [12]:

- It will be an operation-centric risk-based approach based on safety risk evaluation
- It will be gradual but it will be completed in a relatively short period of time (2035)
- It will be performance-based
- It will be sensitive to privacy, data protection and security issues

With reference to the operation and risk-centric approach, EASA defines three categories ([18], [27] and [28]) of RPAS flight operations that will be described in the next paragraphs:

A. Open category
B. Specific category
C. Certified category

The ‘State’ RPAS, that is RPAS used for military, customs, police, firefighting and other similar applications are not included into the EASA regulation [27] and will not be included in the risk analysis discussed in this thesis.

The three above mentioned categories have been defined taking into account the ground and air risks that can be introduced by the integration of RPAS into not segregated airspaces ([27] and [28]. Due to the absence of the pilot on board, the risks introduced by RPAS are shifted outside the aircraft, while for manned aircraft the risk is evaluated both for people inside the aircraft and for people that can be killed and infrastructures that can be damaged/destroyed in case of catastrophic accidents occurrence. The RPAS ground risk refers to the risk of collision with natural obstacles or man-made (eventually sensitive) infrastructures and with the risk of injury or death of people on ground if hit by an RPAS or by parts or debris of an RPAS. The RPAS air risk refers to the mid-air collision risk with another manned or remotely piloted aircraft. In the last years, the air risk has increased in parallel with the greater and greater diffusion of RPAS both for professional use and for leisure.

1.3.1 Open category

The open category operations will be those performed using model aircraft or small RPAS of maximum take-off weight until 25 kg for leisure and conducted until 400 feet of altitude and in RLOS only ([27], [28] and [29]). If the RPAS operation will exceed one or more of these limitations, it will be classified as a specific category operation.

Thanks to the above mentioned prescriptions, the open category operations are intended as low risk operations by definition and therefore they will not be discussed in this thesis.

1.3.2 Specific category

The specific category operations will be those exceeding at least one of the limitations defined for the open category ones. The typical commercial operations expected from RPAS will undergo this category. The specific category operations will be characterized by a risk level to be assessed case by case to gain the authorization to perform it ([27], [28]). Proper standard risk scenarios with associated mitigation actions are under definition by EASA ([27], [28]) to alleviate the Member State from administrative burden for providing authorizations to operators.

The specific category operation is object of the risk analysis discussed in this thesis.

1.3.3 Certified category

According to EASA, the certified category will comprehend very complex operations characterised by very high risk comparable to those of manned aircraft,

like, for example, operations involving large or complex RPAS operating continuously over unsheltered crowd of people or operating beyond visual line of sight (BRLOS) in high-density airspaces; RPAS used for people transportation or used for dangerous goods transportation, etc. ([27], [28]).

1.3.4 EASA/EUROCONTROL concept of operations

The operation-centric approach proposed by EASA ([27], [28]) is further detailed by the 'Concept of operations' (CONOPS) proposed by EUROCONTROL [18]. The roles of the two distinct Authorities is hereinafter highlighted: EASA will manage and care for the rules the RPAS will have to respect to enter and safely use the civil airspace; EUROCONTROL is designing a proper concept of operation to assure the safety of RPAS navigation into the airspace as summed up in Figure 6 [18].

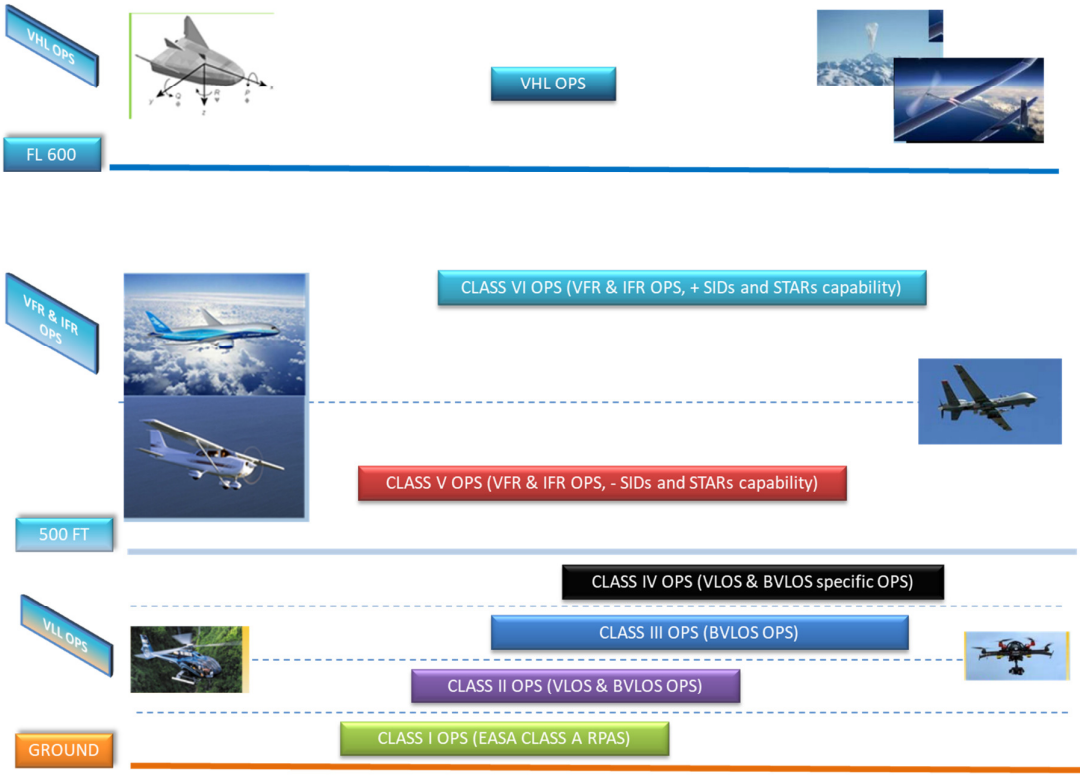


Figure 6 – RPAS integration in the civil airspace: EUROCONTROL concept of operation [18]

The civil airspace has been ideally arranged in three subspaces where the RPAS operations will be allocated as follows:

- The subspace between 0 and 500 feet from ground; it will be called 'Very Low Level' (VLL) subspace: the related flight operations will be performed not under ATC control in an uncontrolled airspace
- A subspace between 500 feet of altitude from ground and flight level FL600 (60000 feet/around 18300 meters of altitude): this subspace is a

controlled airspace served by ATC (in line with the services expected for the different airspace classes, from A to G)

- A subspace beyond FL600: it will be called 'Very High Level' (VHL) subspace; the operations will be performed beyond FL600 or UIR, that is beyond the conventional upper limit of the controlled airspace

From the EASA perspective (safety of flight operations), the following aspects of the afore mentioned EUROCONTROL concept of operations can be highlighted as follows ([18], [28] and [29]):

- 'Very Low Level' (VLL) subspace: the open category and specific category flight operations will be allocated in this portion of the uncontrolled airspace; as above indicated the open category operations are not of interest being categorized as low risk operations by definition; the specific operations will identify with RPAS commercial operations characterized by a medium level of operating risk. The adjective 'commercial' is also used to highlight the nature of these RPAS operations that will be deeply different from Open category operations
- Subspace between 500 feet of altitude from ground and flight level FL600: the RPAS certified operations, characterized by definition by a very high level of operational risk, will be mainly allocated in this portion of the airspace
- Subspace beyond FL600: certified category RPAS operations characterized by very high endurance and range (up to several months) will be mainly allocated in this portion of the airspace. The operations like those performed by Google balloons up to RPAS flying above Mach number airspeed are examples of the sorties allocated in this subspace

From the EUROCONTROL perspective (safety of flight navigation), the following further subdivision into classes of operations of the afore mentioned EUROCONTROL CONOPS can be highlighted as follows ([18] and [29]):

- 'Very Low Level' (VLL) operations subspace:
  - Class I operations: it will host EASA Open category operations performed by EASA Class A RPAS ([27] and [28]); the requirements for RPAS are the following ones:
    - The RPAS shall have 3D self-separation capability
    - The RPAS operations are conducted in RLOS only
    - The RPAS shall have geo fencing software functionality to ensure separation from No-Drone Zones (NDZ)
    - The declaration of operation is mandatory

        - The flights can be performed for recreational purpose only [29]
    - Class II operations: it will host EASA specific/certified category operations; the requirements for RPAS are the following ones:
        - The RPAS shall have 3D self-separation capability
        - The RPAS shall have surveillance capability through the use of 4G chips or other equivalent devices
        - The RPAS shall have free flight capability
        - The RPAS operations can be conducted in RLOS and/or in BRLOS
        - The RPAS shall be equipped with barometric measurement equipment for BRLOS operations
        - The declaration of operation is mandatory
        - The flight missions can be performed for survey, for video recording/photo shooting, search and rescue purposes and similar aims
    - Class III operations: it will host EASA specific/certified category operations; the requirements for RPAS are the following ones:
        - The RPAS shall have surveillance capability
        - The RPAS shall have free flight capability or it shall be capable of flying along structured routes
        - The RPAS operations can be conducted in BRLOS
        - The RPAS shall be equipped with barometric measurement equipment for BRLOS operations
        - The declaration of operation is mandatory
        - The flight missions can be performed mainly for transport purposes
    - Class IV operations: it will host EASA specific/certified category operations; the requirements for RPAS are the following ones:
        - The surveillance capability may be required or not according to the mission requirements
        - The RPAS will remain clear of manned traffic
        - The risk assessment will be required
        - The flight authorization will be released according to risk assessment results
        - These operations class will include very specialized sorties like civil, State or military very specific flight missions
- Operations between 500 feet of altitude from ground and flight level FL600 subspace:

- CLASS V operations: it will host EASA certified category operations only; the requirements for RPAS are the following ones:
  - The flight plan including information about the type of unmanned aircraft, the planned 'Contingency Procedure and a contact phone number shall be filed before starting the mission
  - The RPAS shall meet the CNS airspace requirements
  - The RPAS shall establish and maintain two way communication with ATC
  - RPAS operator ability to contact ATC in case of: C2 link loss, emergency and controlled termination of flight
  - The RPAS will remain clear of manned traffic
  - The RPAS will have detect and avoid capability cooperative with existing ACAS systems
  - The RPAS shall be able to perform VFR/IFR operations outside the pan-European network
  - The RPAS is not required to have SIDs and STARs capability
  - The RPAS operations at the aerodrome will be accommodated through separation of launch and recovery
  - These operations class will manly include missions for transport purposes and military sorties
- CLASS VI operations: it will host EASA certified category operations only; the requirements for RPAS are the following ones:
  - The flight plan including information about the type of unmanned aircraft, the planned 'Contingency Procedure and a contact phone number shall be filed before starting the mission
  - The RPAS shall meet the CNS airspace requirements
  - The RPAS shall establish and maintain two way communication with ATC
  - RPAS operator ability to contact ATC in case of: C2 link loss, emergency and controlled termination of flight
  - The RPAS will remain clear of manned traffic
  - The RPAS will have detect and avoid capability cooperative with existing ACAS systems
  - The RPAS shall be able to perform VFR/IFR operations within the pan-European network
  - The RPAS is required to have SIDs and STARs capability

        - Any kind of RPAS certified operation will be allowed in this class of operations
    - ‘Very High Level’ (VHL) operations subspace: it will host EASA certified category operations only:
        - The flight plan shall always be filed before mission starting
        - The RPAS shall meet the CNS airspace requirements
        - A regional centralised system shall overview the ongoing flight operations
        - The RPAS operator shall contact the ATC to inform them about emergency re-entry into controlled airspace
        - The RPAS operator shall contact the ATC to inform them about emergency re-entry modalities (deflating balloons or orbital descending)
        - This class of operations will be used to perform stratospheric commercial flight with unmanned aircraft of flight balloons
        - The departure and arrival procedures shall be defined

1.3.5 Traffic management service for RPAS

The integration of RPAS into the airspace will impact existing Air Traffic Control/Management infrastructures and operators within both not controlled and controlled airspaces. For this reasons, EASA and EUROCONTROL foresee two different levels of traffic management service for RPAS operations:

- The Specific operations within the VLL subspace will benefit from the so called U-space service; in the VLL subspace primary and secondary RADARs are not effective in tracking aircraft movements and in any case the tracked RPAS would appear as very small and cluttered bright dots on the air controllers displays thus resulting in totally ineffective images for safety purposes
- The Certified operations will start from the VLL subspace (take-off and climb), then they will continue in the controlled airspace (cruise) until eventually exceeding the upper limit of the controlled airspace (cruise) before the descending to conclude the mission: therefore they will fully benefit from the ATM service like manned aircraft and will be under RADAR or navigation satellites coverage

The main technical features of U-Space also referred as UTM (Unmanned Traffic Management service) and ATM services are of interest for the safety analysis object of this thesis, therefore they are hereinafter briefly described.

U-Space service

The U-space is defined by SESAR1 [30] as a set of new services and specific procedures defined to support the safe, secure and efficient access of a large number of RPAS to the civil airspace.

The U-space, that still does not exist, will rely on a high level of digitalisation and automation of functions, spread whether on ground and on board the RPAS. Its framework will provide proper services to support daily routine RPAS operations and a clear, safe and effective interface towards manned aviation, towards air traffic management and air navigation service providers and towards aviation authorities. In accordance with the ICAO concept of full integration of RPAS into the civil airspace [4], the U-space will not be a defined volume of airspace, segregated and designated for the use of remotely piloted aircraft only but it will be implemented to smoothly allow their operation within all possible operating environments and airspaces. For simplicity, in the first phases of the U-space deployment, that is the scenario considered in this thesis, it can be reasonably assumed that the U-space physically coincides with the above mentioned VLL subspace defined from ground level to 500 feet of altitude ([18], [29]).

The U-space will be functionally designed and technically implemented according to the following key principles [30]:

- To ensure the safe operation of RPAS users both in the airspace and on ground
- To provide a scalable, flexible and adaptable system to promptly respond to expected future evolution of RPAS operations demand, volume, technology, etc.
- To enable high-density operations with multiple automated RPAS under the supervision of fleet operators
- To guarantee an equal and fair access to all users to the airspace
- To encourage the exploitation for RPAS of up-to-date services addressed for the moment to manned aviation only like, for instance, GNSS-SBAS navigation services
- To guarantee a low cost enhancement of the U-Space through the adaptation to the aeronautical standards of infrastructures and services coming from other industrial sectors: for example, the 4G/LTE/5G networks, the cloud platforms and the ‘Internet of Things’ (IoT), accordingly moreover to the high level of automation and digitalization foreseen for the U-Space
- To ensure protection of RPAS from cyber threats
- To ensure a minimal environmental impact
- To ensure privacy protection

The U-space will host and facilitate RPAS flight operations from simple tasks like the delivery of goods, to aerial work to very complex services like the urban air mobility.

The U-space will be rolled up according to the following stages [30]:

- U1: Provision of the U-space foundation services of e-registration, e-identification and geo fencing
- U2: Provision of the U-space initial RPAS flight management services including, for example, flight planning, flight approval, flight tracking, airspace dynamic information service, and procedural interfaces with the air traffic control
- U3: Provision of the U-space advanced services to support more complex RPAS operations in dense areas and including capability for conflict detection management and assistance even using automated 'detect and avoid' (DAA) functionalities and more reliable communication datalinks
- U4: Provision of the U-space full services comprehensive of integrated interfaces with manned aviation, supporting the full operational capability of U-space and relying on very high level of automation, connectivity and digitalisation for both the RPAS and the U-space system

The following example taken from [30] is hereinafter briefly reported as a practical example of the type of operating scenarios where safety hazards object of the assessment discussed in this thesis can occur (Figure 7 [30]):

1. RPAS mission set up: the operator chooses an RPAS from his/her own fleet to deliver a package from a village to a urban centre 40 kilometres away. The RPAS will be e-registered; therefore ATM information like NOTAMs, forecasts etc. will be immediately available for the selected RPAS and matched with it and with its airworthiness and emergency mitigation features
2. Submission of the flight request and receipt of the acknowledgement: the proposed RPAS planned routes are compared to applicable regulations and airspace requirements and eventually reviewed to fit with other RPAS conflicting routes; the resulting 4D trajectory is proposed for acceptance; it is accepted by the RPAS operator with an acknowledgement and re-sent to him/her. During the flight the RPAS will broadcast its unique identifier to be tracked for all the sorties receiving update information and alerts on contingent traffic and meteorological conditions (for example)
3. Performance of the flight operation: the DAA functionality is available and usable for example to avoid birds or other contingent mid-air conflicting traffic; an alert about the presence on the RPAS route of a police state RPAS to monitor a cars accident and the approaching of

an helicopter ambulance is sent to the RPAS geo-fence system (consequently updated with reference to the given NOTAM) to prevent it to enter the temporary restricted area

4. RPAS mission completion: the RPAS safely reaches the planned destination and deliver the payload parcel; it can take-off again to perform the successive flight sortie

Figure 7 – U-space [30]

ATM service

In addition to the description of airpace incoming upgrade to a global full integrated service provider reported in Paragraph 1.2, the following information useful for the risk analysis of RPAS operations under ATM service are furterly detailed:

- The manned aircraft are currently identified using transponder codes that allow aircraft tracking by ground based RADAR systems; the next step will be equipping all airspace users with ADS-B devices; the aircraft (included RPAS) will be able to detect each other thanks to the broadcast surveillance capablity typical of this new kind of transponder. This functionality is supported by GNSS satellite-based system and in particular by GALILEO-EGNOS SOL service in the controlled airspace above Europe [31]
- According to [30] and [31], the manned aircraft flights are performed under 'Visual Flight Rules' (VFR flights) or 'Instrumental Flight Rules' (IFR flights). The VFR flights do not require the use of flight instrumentation; the IFR flights require the use of flight instrumentation. The ATC authorizes the execution of both VFR or IFR flights after having examinated the associated flight plan

- The ATC includes technical offices that provide meteorological forecasts to pilots. Meteorological forecasts are statement of expected meteorological conditions for a specified time or period, and for a specified area or portion of airspace [33]
- The airpaces are divided and ruled as follows (Table 2 [34]):

Table 2 – Airspace classes definition [34]

Class	Type of flight served	Service provided	Separation provided	Radio communication requirements	ATC clearance	Notes
A	IFR only	Air traffic control service	All aircraft	Continuous, two ways	Yes	Controlled airspace
B	IFR	Air traffic control service	All aircraft	Continuous, two ways	Yes	Controlled airspace
	VFR	Air traffic control service	All aircraft	Continuous, two ways	Yes	Controlled airspace
C	IFR	Air traffic control service	IFR from IFR IFR from VFR	Continuous, two ways	Yes	Controlled airspace
	VFR	- Air traffic control service for separation from IFR - VFR/VFR traffic information	VFR from IFR	Continuous, two ways	Yes	Controlled airspace
D	IFR	Air traffic control service including information about VFR flights (traffic avoidance on request)	IFR from IFR	Continuous, two ways	Yes	Controlled airspace
	VFR	Traffic information between VFR and IFR (traffic avoidance on request)	Nil	Continuous, two ways	Yes	Controlled airspace
E	IFR	Air traffic control service and traffic information about VFR flights	IFR from IFR	Continuous, two ways	Yes	Controlled airspace
	VFR	Traffic information as far as practical	Nil	Continuous, two ways	Yes	Controlled airspace
F	IFR	Air traffic advisory service; flight information service	IFR from IFR as far as practicable	Continuous, two ways	No	Uncontrolled airspace
	VFR	Flight information service	Nil	No	No	Uncontrolled airspace
G	IFR	Flight information service	Nil	Continuous, two ways	No	Uncontrolled airspace
	VFR	Flight information service	Nil	No	No	Uncontrolled airspace

1.3.6 The SESAR research program

Both in Europe and in the United States two similar research initiatives are on-going to study the reorganization of airspace management according to the

new guidelines issued by ICAO on the Global Air Traffic Management [23]. The European research program is the 'Single European Sky Air Traffic Management Research Joint Undertaking' [35] (SESAR-JU, now going on as SESAR1/SESAR2020); the US research program is called NextGen. This thesis will consider the European research program only with its relationship with the full integration of RPAS into the European not segregated airspace.

The SESAR research program, following the European Commission's 'Roadmap for the integration of civil RPAS into the European aviation system' issued in 2013, launched its first research activity on RPAS integration into not segregated airspaces through nine demonstration projects [36]. Many universities, research centres and small/medium enterprises were called to take part to this initiative. The purpose was to perform real flight tests with RPAS in non-segregated airspace to identify and to assess potentialities and limitations of current regulations, technologies and infrastructures with respect to the incoming challenge of the integration of RPAS into controlled airspace.

Among the above mentioned projects, the RAID demo project[1] [37] will be hereinafter described more in detail as source for the idea of implementing a comprehensive risk matrix as first output of the safety analysis on hazards related to the integration of RPAS into not segregated airspaces.

The RAID demo project

The RAID demo project experimental activity was focused on simulation and flight testing activity of RPAS merged with manned aircraft in the controlled not segregated airspace. It has been performed by a consortium composed of the following actors:

---

[1] Disclosure note: *The activities hereinafter cited have been carried out in the frame of the project RAID and co-financed by the 'SESAR Joint Undertaking' (SJU) as part of RPAS Demo projects of the SESAR Program (2013 SESAR SJU/LC/0087-CFP). The opinions expressed in this thesis reflect the PhD Candidate views only and the SJU shall not be considered liable for them or for any use that may be made of the information contained herein.*

The PhD Candidate was not personally involved in the execution of the experimental activity described and discussed in the RAID demo project document reported in [37]; nevertheless, due to the topic of the PhD research activity, and by mean of the Supervisor Professor Francesco Grimaccia, She has been authorized by Engineer Edoardo Filippone from the 'Centro Italiano Ricerche Aerospaziali (CIRA) to access the RAID demo project final report content.

Professor Francesco Grimaccia and Engineer Edoardo Filippone took part to the RAID experimental activity as Advisor of Nimbus S.r.l. and as Responsible Manager for CIRA activities in the demo projects respectively.

- The 'Centro Italiano Ricerche Aeropaziali', (CIRA) Research Centre, which was also the coordinator responsible of the whole experimental activity
- The Malta Air Navigation Service Provider, MATS, which provided support to the activity for the aspects related to the air traffic control
- The University of Malta
- Nimbus S.r.l., an Italian small/medium enterprise, which provided the RPAS used during the experimental activity
- Deep Blue S.r.l., an Italian small/medium enterprise, which provided support to the activity for the aspects related to human factor and operations
- NAIS S.r.l., an Italian small/medium enterprise, which provided support to the activity for the aspects related to cybersecurity

The flight activity was performed from April 27th to May 6th 2016; each flight sortie started taking off from the airport of Capua close to the CIRA infrastructure and flying within the delimitated airspace shown in Figure 8 [37].

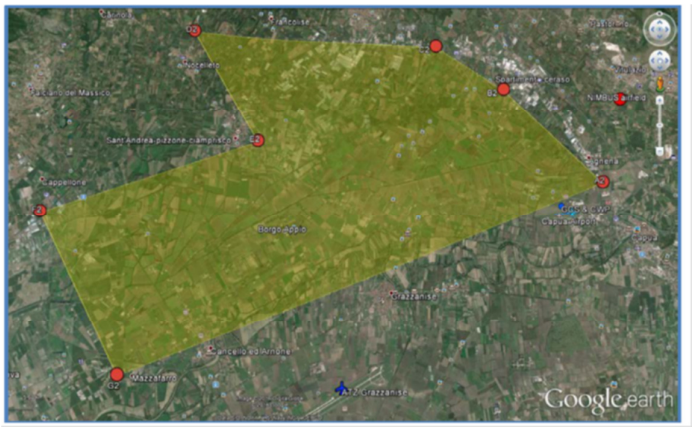


Figure 8 – RAID demo project flight test area (from [37])

Twelve flight tests were performed to collect data and information about a variety of elements related to the integration of RPAS with manned aircraft under ATC control. Among the others, the sudden intrusion of manned or unmanned aircraft on the RPAS route was physically tested as very critical scenario from a safety perspective. The aircraft used during the experimental activities were the following ones [37]:

- The CIRA Optionally Piloted Vehicle FLARE OPV TECNAM P92 Echo-S VLA aircraft: it was remotely piloted from ground or directly piloted by the human pilot on board to alternatively play the role of unmanned or manned aircraft flying in the airspace
- The Storm RG CS-VLA aircraft: it simulated the manned intruder
- The PPL 612 RPAS: it was provided by the Nimbus S.r.l.; it simulated the unmanned intruder

Table 3 shows the flight tests sorties where safety hazards occurred ([37], [38]).

Table 3 – RAID test sorties with elements relevant to safety ([37], [38])

Flight #*	Type of involved traffic	FLARE in RPAS Mode (Time window)	Safety hazards					
			DAA/ ADS-B failure	C2Link failure	Limitation in human performances	Weather and terrain + DAA/ADS-B failure	Weather and terrain + C2 link failure	Loss of GNSS, DAA and C2 Link Systems
1	FLARE A/C only	41‘	-	-	x	-	-	-
2	FLARE A/C only	22‘	-	-	x	-	-	-
3	FLARE A/C only	33‘	-	-	x	x	x	x
4	FLARE A/C & Mini RPAS	24‘	-	-	x	-	-	-
5	FLARE A/C & manned VLA	7‘	-	-	x	-	-	-
6	FLARE A/C & manned VLA	20‘	-	-	x	-	-	-

*Not original flight number.

Table 3 – RAID test sorties with elements relevant to safety ([37], [38]) (Cont'd)								
Flight #*	**Type of involved traffic**	**FLARE in RPAS Mode (Time window)**	**Safety hazards**					
			DAA/ ADS-B failure	**C2 Link failure**	**Limitation in human performances**	**Weather and terrain + DAA/ADS-B failure**	**Weather and terrain + C2 link failure**	**Loss of GNSS, DAA and C2 Link Systems**
8	FLARE A/C & manned VLA	25'	-	-	x	x	x	x
9	FLARE A/C & manned VLA	29'	x	x	x	x	x	x
10	FLARE A/C & manned VLA	31'	x	x	x	x	x	x
11	FLARE A/C & manned VLA	6'	x	x	x	x	x	x
12	FLARE A/C only	20'	x	x	x	x	x	x

The safety hazards of Table 3 ([37], [38]) have been assessed according to the criteria provided by ICAO Doc. 9859 [3] (these criteria will be described in Chapter 2) to draft a preliminary safety risk matrix (Table 4 [38]) as preliminary demo of the more comprehensive safety risk matrices implemented during the PhD research and reported in Appendix D.

Table 4 – Preliminary safety risk matrix [38]

Hazard	Risk assessment					
	Safety risk probability	**Safety risk severity**	**Safety risk assessment**	**Tolerability**	**Risk range description**	**Recommended action**
DAA/ ADS-B failure	Occasional (4)	Catastrophic (5 or A)	4A	Unacceptable	High risk	Cease or cut back operation promptly
C2 link failure	Occasional (4)	Catastrophic (5 or A)	4A	Unacceptable	High risk	Cease or cut back operation promptly
Human factor: ATC high workload	Occasional (4)	Hazardous (4 or B)	4B	Unacceptable	High risk	Cease or cut back operation promptly
Human factor: Remote pilot high workload	Occasional (4)	Hazardous (4 or B)	4B	Unacceptable	High risk	Cease or cut back operation promptly
Meteorological conditions*	-	-	-	-	-	-
Impact against terrain	Occasional (4)	Catastrophic (5 or A)	4A	Unacceptable	High risk	Cease or cut back operation promptly
Jamming/ spoofing with DAA/ADS-B in failure	Improbable (2)	Hazardous (4 or B)	2B	Acceptable based on risk mitigation	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable

* For safety reasons, all RAID sorties were performed under visual meteorological conditions [37].

1.4 The methodology

In the previous paragraphs the necessary premises for the safety analysis object of this thesis have been described and discussed. In this paragraph, the methodology followed to carry out the overall research is hereafter detailed:

A. Identification of the system to be studied and of its boundaries/interfaces with external environment: the system is the whole of the RPAS integrated with manned aircraft into the controlled/uncontrolled not segregated airspace. The elements of this ensemble are: the RPAS; the other manned or unmanned cooperative or not cooperative traffic also referred to as intruders; the airspace as infrastructure with its operating rules; the human factor intended as the RPAS remote pilot on ground, the manned aircraft pilot in command, the human beings on ground, the air traffic controllers; the third parties on ground intended both as natural obstacles and man-made infrastructures

B. Definition of the concept of operation of RPAS into the not segregated airspace: it is the one defined on the basis of EASA/EUROCONTROL state of art available documentation ([18], [28] and [29])

C. Hazards categorization definition: definition of a valuable hazards categorization following the RPAS functional guidelines defined by NASA and reported in [39]

D. Reliability analysis: performance of FMECA and FTA analyses to identify single and combined failure causes of RPAS potentially leading to contingent hazards

E. Human factor safety analysis: performance of RPAS related human factor safety analysis using SHELL and HFACS methodologies potentially leading to human factor related hazards for RPAS systems

F. Hazard logs draft: draft of two hazard logs following the categorization of RPAS functionalities proposed by NASA in [39]: one related to the hazards expected to occur during specific category RPAS flight operations performed within the U-Space, from ground to 500 feet of altitude, in an uncontrolled airspace and the other one related to the hazards expected to occur during certified category RPAS flight operations performed mainly beyond 500 feet of altitude, within controlled airspaces served by ATM.

G. Safety risk assessment execution: execution of the safety risk analysis and draft of two safety risk matrices named 'U-Space risk matrix' and 'ATM risk matrix'

H. From this point onwards, the safety analysis has been focused on the U-space due to the fact that the RPAS operations performed into the VLL will be the first ones allowed to be executed

I. Bow Tie analysis: the most significant hazards listed in the U-space matrix have been further analysed investigating threats that can cause the system operational drift from its baseline condition and the defences/barriers that can be applied to avoid catastrophic consequences occurrence; this stage of the safety analysis has been performed using the Bow Tie methodology [40]

J. Rule-based 'Expert System' knowledge basis implementation: the content of each hazard listed in the U-space matrix has been reconsidered and developed (when possible) into a rule or a set of rules composing the knowledge basis of a rule-based 'Expert System' [41]; the knowledge basis has been intended as fundamentals for the future implementation of a software based on artificial intelligence and capable of providing dynamic support to the remote pilot or directly to the RPAS (during fully automatic flight missions) in identifying precursors of high and medium risk hazards and mitigating their consequences thus avoiding catastrophic consequences occurrence

K. 'Expert System' knowledge basis rules coverage verification: verification of the 'Expert System' knowledge basis rules from the perspective of system engineering verifying the coverage and consistency of the

elaborated rules against the hazards and failure conditions identified with the safety analysis

L. RPAS high level functional architecture oriented towards in-flight hazards occurrence prevention and mitigation: drafting of a proposal for an RPAS high level functional architecture capable of counteract high and medium risk in flight hazards

M. Review of the first available U-Space infrastructure proposed in literature and on the web: a critical review of the first available U-Space infrastructure proposed in literature and on the web and studied during the research has been carried out on the basis of the performed safety risk analysis

N. Example of application of the 'System Theoretic Process Analysis' (STPA) [42] hazard methodology: an example of the application of this technique has been executed to directly evaluate its features as hazards analysis technique and to find out some examples of difference of this technique with respect to the traditional ones used in the research

O. Italian RPAS regulation: critical evaluation of Italian RPAS regulation from safety perspective on the basis of the analysis carried out during the research

P. Hybrid RPAS functional architecture proposal description and evaluation: performance of a brief digression on RPAS hybrid solutions to show and discuss safety and operative requirements for a high level hybrid RPAS functional architecture proposal

1.5 Conclusions

The full integration of RPAS into the civil not segregated airspace will allow a fruitful development of their European production both in Europe and worldwide. A common set of regulations and industry standards as well a comprehensive risk analysis to prevent the occurrence of catastrophic accidents are strictly necessary to support this integration.

Starting from the recent new recommendations issued by ICAO on Safety Management System for aeronautical operators and the safety hazards preliminarily identified by the consortium led by CIRA within the SESAR RAID demo project flight test activity, the idea raised up to focus the research activity of the Doctorate on the performance of a comprehensive safety analysis of the hazards related to the integration of RPAS into not segregated civil airspaces.

Chapter 2

Safety Management System: general overview

2.1 Safety in aviation

The safety in aviation is defined as the condition in which the possibility to harm human beings or to damage third parties properties is reduced to and maintained at or below an acceptable level using a continue process of hazard identification and safety risk management [3].

Being aviation a complex industrial sector that will never be completely free of risks for its nature, the safety management acts as a dynamic provision to continuously fit to the contingent hazards.

With time, safety in aviation has become a matter of culture as all the aviation stakeholders (manufacturers, commercial companies, etc.) are called to be responsible about safety continuously identifying and mitigating hazards.

During the Twentieth century, safety in aviation evolved from the technical era, when aircraft accidents where due to mechanical failures of equipment, passing through the human factor era, when after that reliability of parts had been enormously enhanced, the responsibility of safety was moved to the pilots, until arriving to the current organizational era where safety has become a responsibility of the aviation organization [3]. For instance, with reference to commercial aviation, this means that the whole of personnel managing aerodromes and their infrastructures, air companies crews and air traffic controllers are committed to maintain at a safe level their assets during both on ground and in flight operations. The accident of Linate (8^{th} September 2000) is an example of hazard occurrence with catastrophic consequences due to the lack of system safety at organizational level: the lack of RADARs to monitor Linate aerodrome ground movements, made the air traffic controllers miss the runaway incursion of a small aircraft that was hit by a commercial liner during its take-off run. Death of persons and damages to third parties on ground occurred as catastrophic level consequences.

Nowadays, safety in aviation is systematically managed applying 'Safety Management System' (SMS) criteria [3].

Remembering the above mentioned definition of SMS and the recent ICAO regulations on safety management cited in Chapter 1, the core idea considered in this Doctorate has been the assessment of safety risks related to the operations of RPAS into the civil not segregated airspace, alongside manned aircraft, identifying possible hazards and mitigation actions to maintain operational risk below or at an acceptable low level, according to a qualitative assessment as described in Chapter 3.

In this Chapter basic definitions of SMS concepts are exposed which have been used to perform the safety analysis object of this thesis and reported in Chapter 3.

2.2 The Safety Management System

The Safety Management System is based on four pillars [3]:

- Safety policy and objectives
- Safety risk management
- Safety assurance
- Safety promotion

with the following meaning: the safety policy and objectives is the whole of an aviation organization management commitment, responsibility and accountability for implementing safety and maintaining safety. It consists of the identification and assignment of responsibilities to designated key safety personnel. The safety risk management is the continuous process aimed to identify hazards and to analyse, assess and control the associated risks. The safety assurance is the set of processes addressed to verify if the organization meets or exceeds the committed safety performance objectives thus providing it a monitoring of the adopted safety policy effectiveness. The safety promotion is the whole of actions performed to improve the organizational safety culture and its continuous improvement.

The incoming of RPAS into the civil airspace will introduce disruptive changes in the aviation system that will have to be properly managed and mitigated. Considering the economic value of RPAS, the following applies (Figure 9 [3]): the best compromise shall be found between the provision of advanced mitigations solutions for safety of operations like avionic equipment and other technological solutions and the global RPAS economic value. The point is specifically crucial for light RPAS, that will be the first to be employed for commercial operations, and whose total cost (RPAS, operations, maintenance) shall have to remain strongly competitive with respect to manned aircraft (general aviation, helicopters) to allow their European market development fostering.

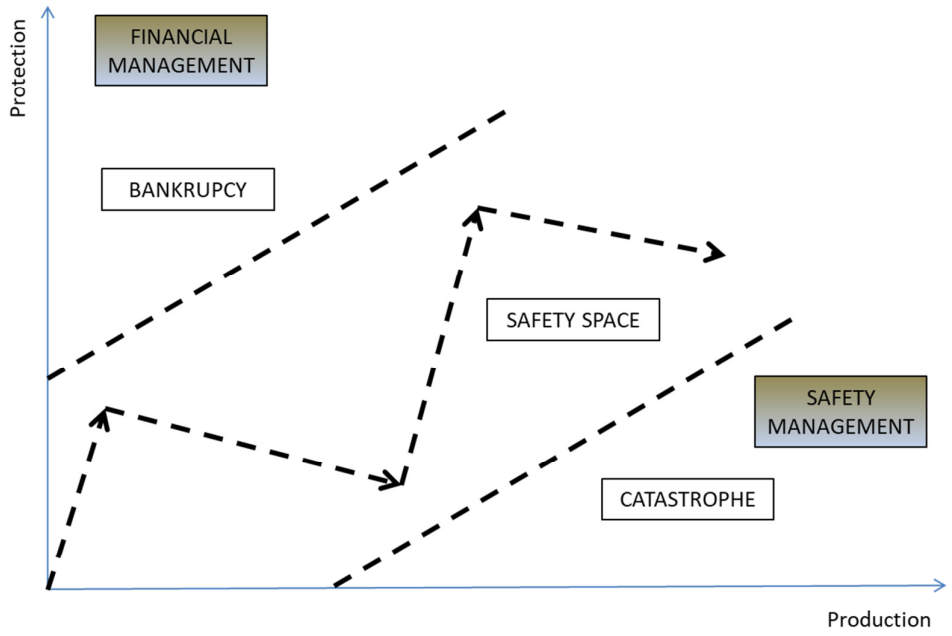


Figure 9 – Safety space definition [3]

2.3 The Safety Management Risk

The safety risk management is the former process of identification, assessment and mitigation of system safety risks. The crucial phase of the safety management process is the hazards elimination or mitigation (Figure 10 [3]).

The methodology for hazards identification can be reactive, proactive or predictive. The reactive methodology is based on the study of incidents and accidents reports issued after the given occurrence; the proactive approach is based on the voluntary report on real-time inconveniences, on precursors of hazards or on hazards; the predictive approach involves data gathering to identify new possible hazards and outcomes investigating on the processes and the environment where the system under analysis operates [3].

Considering that the integration of RPAS into the civil airspace is coming, but it is not yet a reality, the safety risk analysis reported in this document has been based on a predictive approach conjecturing the new hazards expected to occur when RPAS and manned aircraft will operate together in the same not segregated airspace.

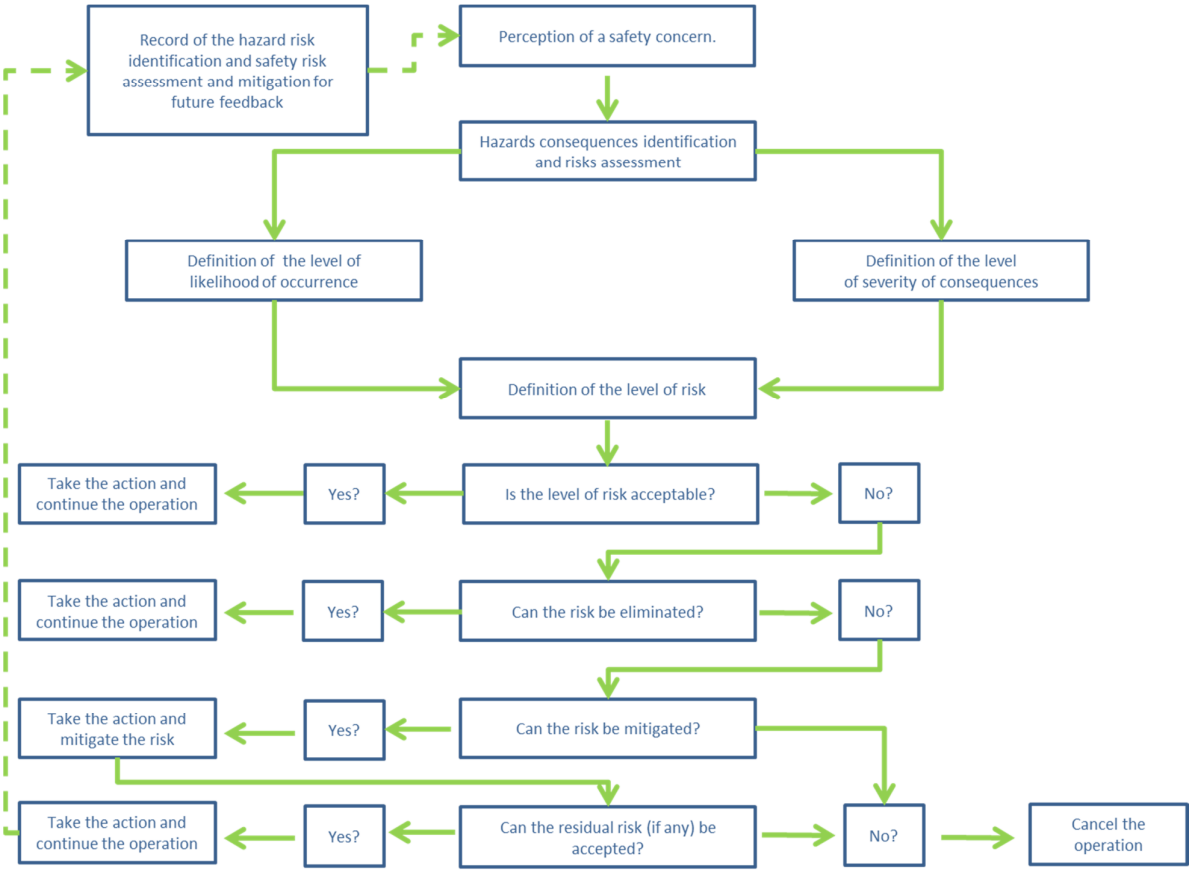


Figure 10 – Safety Risk Management process [3]

2.3.1 Risk analysis main definitions

The risk analysis main definitions used in this work are the following ([3] and [43]):

- Hazards: a hazard is the potential to cause harm; it can be a physical situation or a state of a system
- Risk: the risk is a measure of the exposure of the system to the hazard. The risk is expressed both in terms of the quantification of the hazard consequences severity and in terms of the quantification of the hazard probablility of occurrence (or likelihood). From a mathematical perspective, the risk associated to an hazard is the product of the consequence severity and the probablility of its occurrence
- Accident: an accident is an unintended event or sequence of events that causes harm
- Accident sequence: the accident sequence is the whole of a cause or initiating event that activates the hazard, the hazard occurrence, and finally the accident occurrence
- Drift: it is the deviation of the system performance from its baseline
- Practical drift: it is the deviation of the system behaviour from its baseline during its operation

- Mitigation actions: they are the barriers and the defences of the system against the hazard occurrence and its consequences severity

The above mentioned definitions are inextricably linked among them: the sudden failure of an equipment or system functionality or the violation of a procedure can provoke an hazard able to move the performance of the system from its baseline to a practical drift. If the hazard event occurs in such a way to trespass all the defences of the system, the incident or accident occurs.

2.3.2 Types of risk management

The risk assessment activity can be performed applying qualitative, semiquantitative or quantitative methodologies [43]:

- Qualitative risk assessment:
  - Risk based judment for relatively minor hazards
  - Hazard identification techniques characterized by a qualitative evaluation of significance of the hazards like Failure Modes and Effects and Criticality Analysis (FMECA)
  - Risk matrices with description of likelihood and consequences
- Semi qualitative risk assessment, giving order of magnitude estimation:
  - Risk matrices with descriptions of likelihood and consequences supported by numerical interpretation
  - Assessment of layers of protection
- Quantitative risk assessment:
  - Risks are numerical estimation in order to perform comparisons against numerical risk criteria at evaluation stages

2.3.3 The risk management and assessment process

The risk assessment is a decisional process The steps of the safety risk management process are the following ones (Figure 11 [3]):

- Hazard identification
- Risk analysis probability (likelihood) of occurrences evaluation
- Risk analysis severity evaluation
- Risk assessment
- Risk tolerability evaluation
- Risk mitigation/Risk control identification

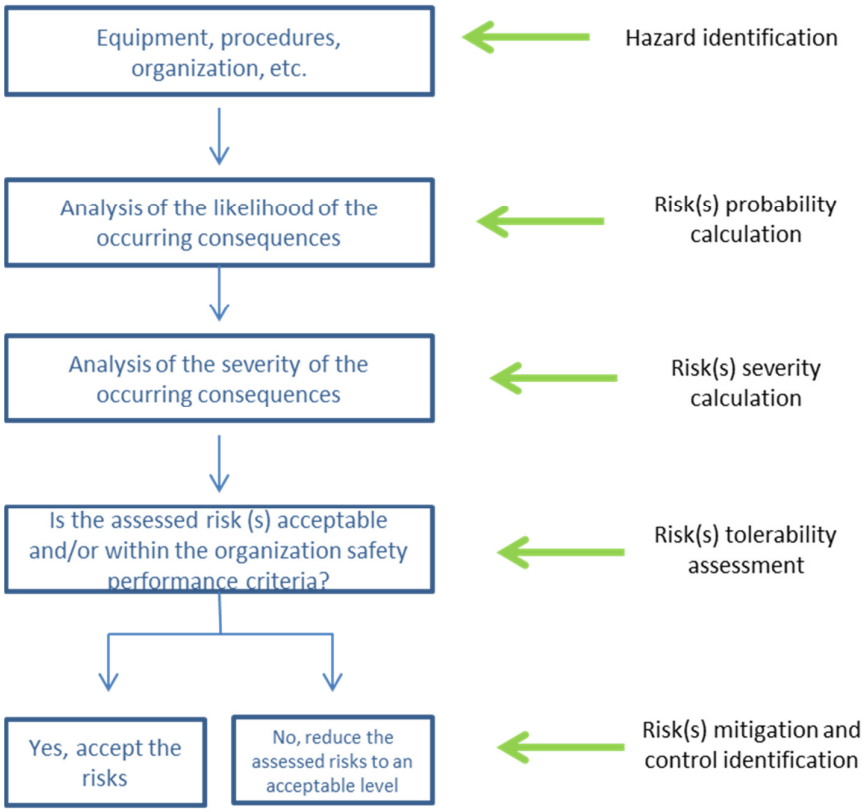


Figure 11 – Risk management process [3]

The hazard identification techniques

The hazard identification techniques are ([3], [43]):

- Empirical techniques:
  - Deductive techniques: Fault Tree Analysis (FTA), Accidents Investigation and Analysis, Fault Hazard Analysis (FHA)
  - Inductive techniques: Event Tree Analysis (ETA), Failure Modes and Effects Analysis (FMEA), Failure Modes and Effects and Criticality Analysis (FMECA)
- Creative/Intuitive techniques:
  - Hazard and Operability Studies (HAZOPS)
- Other techniques:

  Job Tasks Analysis, Operational Hazard Assessment, Scenario Analysis, What If Analysis

Risk assessment

For any given hazard, the safety risk assessment is function of the probability (likelihood) of occurrence and of the severity of its consequences.

For each safety hazard identified, the safety risk probability of occurrence shall be evaluated according to the content of Table 5 [3] considering possible valid scenarios.

Table 5 – ICAO safety risk probability table [3]		
Likelihood	**Meaning**	**Value**
Frequent	Likely to occur many times (has occurred frequently)	5
Occasional	Likely to occur sometimes (has occurred infrequently)	4
Remote	Unlikely to occur, but possible (has occurred rarely)	3
Improbable	Very unlikely to occur (not known to have occurred)	2
Extremely improbable	Almost inconceivable that the event will occur	1

For each safety hazard identified, the safety risk severity of consequences shall be evaluated according to the content of Table 6 [3]. The safety risk severity is ranked taking into account the potential worst realistic consequences conceivable for the hazard under analysis in terms of fatalities or injuries of human beings or damages of infrastructures.

Table 6 – ICAO safety risk severity of hazard occurrence consequences [3]		
Severity	**Meaning**	**Value**
Catastrophic	Equipment destroyed Multiple deaths	5
Hazardous	A large reduction in safety margins, physical distress or a workload such that the operators cannot be relied upon to perform their tasks accurately or completely Serious injury Major equipment damage	4
Major	A significant reduction in safety margins, a reduction in the ability of the operators to cope with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their efficiency Serious incident Injury to persons	3
Minor	Nuisance Operating limitations Use of emergency procedures Minor incident	2
Negligible	Few consequences	1

The determined safety indexes (Table 7 [3]) shall be compared against the reference safety tolerability indexes shown in Table 8 [3]/Table 9 [3].

Table 7 – Safety indexes [3]					
Risk probability	**Risk severity**				
	Catastrophic A	**Hazardous B**	**Major C**	**Minor D**	**Negligible E**
Frequent 5	5A	5B	5C	5D	5E
Occasional 4	4A	4B	4C	4D	4E
Remote 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Extremely improbable 1	1A	1B	1C	1D	1E

Table 8 – Safety risk tolerability matrix [3]

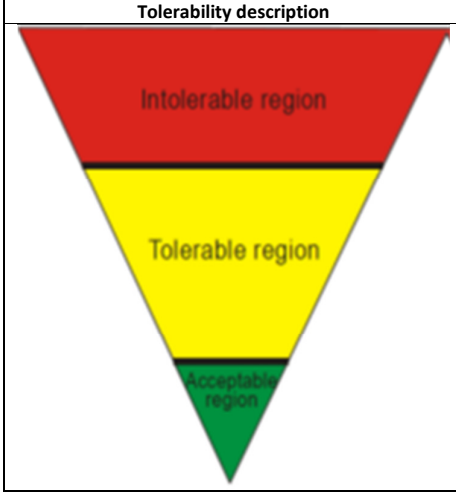
Tolerability description	Assessed risk index	Suggested criteria
	5A, 5B, 5C, 4A, 4B, 3A	Unacceptable under the existing circumstances
	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Acceptable based on risk mitigation. It may require management decision
	3E, 2E, 1E, 2D, 1D, 1B, 1C,	Acceptable

Table 9 – (Alternate) safety risk tolerability matrix [3]

Risk index range	Description	Recommended action
5A, 5B, 5C, 4A, 4B, 3A	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.
3E, 2E, 1E, 2D, 1D, 1B, 1C,	Low risk	Acceptable as it is. No further risk mitigation required.

Risk mitigation

The risk mitigations can be investigated using the Bow Tie methodology (Figure 12 [40]). It is as a qualitative structured risk analysis methodology chosen for its simplicity of use.

It combines the causes/threats and the consequences/defenses related to an hazard event; it logically links the fault tree analysis on the left side of the bow tie with the event analysis on the right side of it through the central knot depicted in the scheme. The knot represents the top event direcly related with the hazard under analysis. The physical meaning of the scheme is the following: the threats, if not balanced by the barriers can activate the hazard which can make the top event to occur; once the top event has occurred, the mitigation actions only can limitate the severity of consequences. Both on the side of the threats/causes and on the side of the consequences/effects, escalations factors can be considered for a deeper analysis.

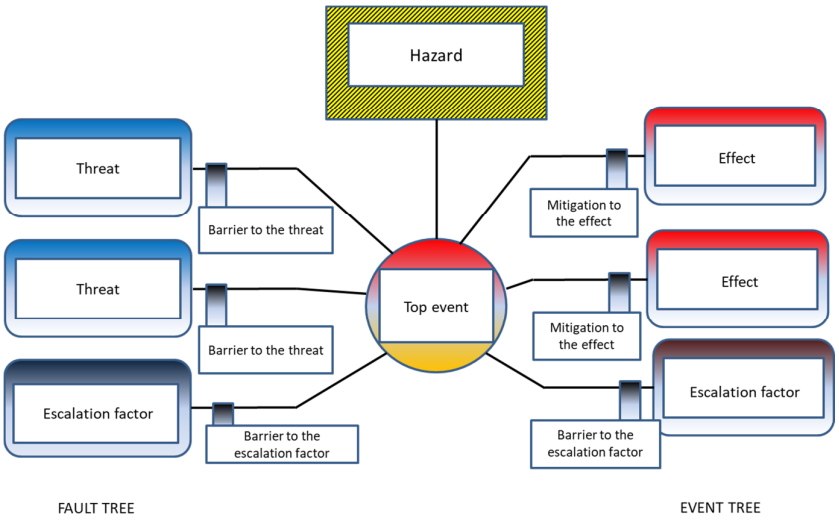


Figure 12 – Bow Tie scheme [40]

Residual risk

The residual risk [3] is the degree of safety risk that still remains after having applied the mitigation factors/defences to restrict the consequences of hazard occurrence. The residual risk may necessitate additional risk control measures.

The human factor: SHELL and HFACS models

The human factor is still present using RPAS even if the human pilot is not physically on board the aerial platform.

The human factor involved in the RPAS operations has been evaluated at high level from safety perspective using the SHELL ('Software, Hardware, Environment, Liveware, Liveware') model [3]; then the shades of the human behaviour that mostly can lead into hazards can be furtherly characterized using the HFACS model [44].

The SHELL model allows to identify the basic relationships between the human operator and the other system elements around him/her. This model reflets the fact that in a system every mismatch in the above listed relationships can cause a hazard (Figure 13 [3]). The boundaries of each block are not straight to indicate the adaptability (with limitations) of the human being to the system.

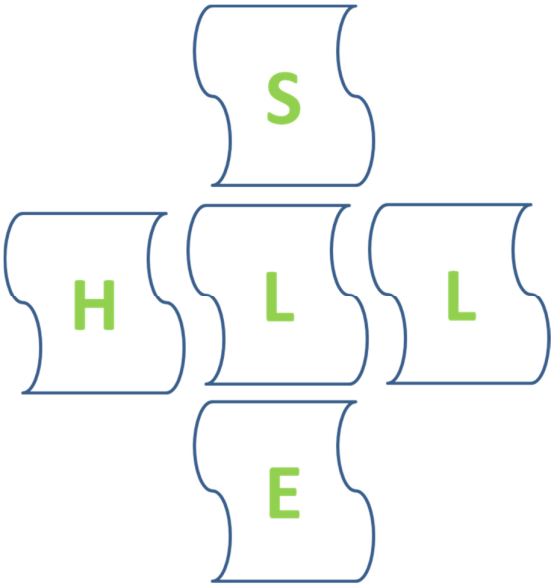


Figure 13 – SHELL model [3]

The possible relationships foreseen by the SHELL model are:

- Liveware – Hardware: this branch of the model deals with the relationships between the human operator and the physical attributes of equipment, machines and facilities
- Liveware – Software: this branch of the model deals with the relationships between the human operator and the supporting systems used in the workplace like, regulations, technical manuals, checklists, publications, standard operating procedures, computer software, etc. Further, it includes issues like, recency of experience, accuracy, format and presentation, vocabulary, clarity and symbology
- Liveware – Environment: this branch of the model deals with the relationships between the human operator and the internal and external environmental aspects of the workplace like, for example: light, noise, temperature, etc. (among the internal issues) and weather, vibrations, noise, etc. (among the external ones)
- Liveware – Liveware: this branch of the model deals with the relationships between the human operator in the work environment both among persons belonging to the same category (crews, ATC controllers, engineers, maintenance operators) and among persons afferent to different groups. The advent of the 'Crew Resource Management' (CRM) concept and its application to ATC and maintenance personnel too has acted during time as a mitigation factor against operational errors and malpractices caused by the human factor

The 'Human Factor Analysis and Classification System 2000' (HFACS), (Figure 14 [44]), provides a taxonomy to describe and classify human behaviour.

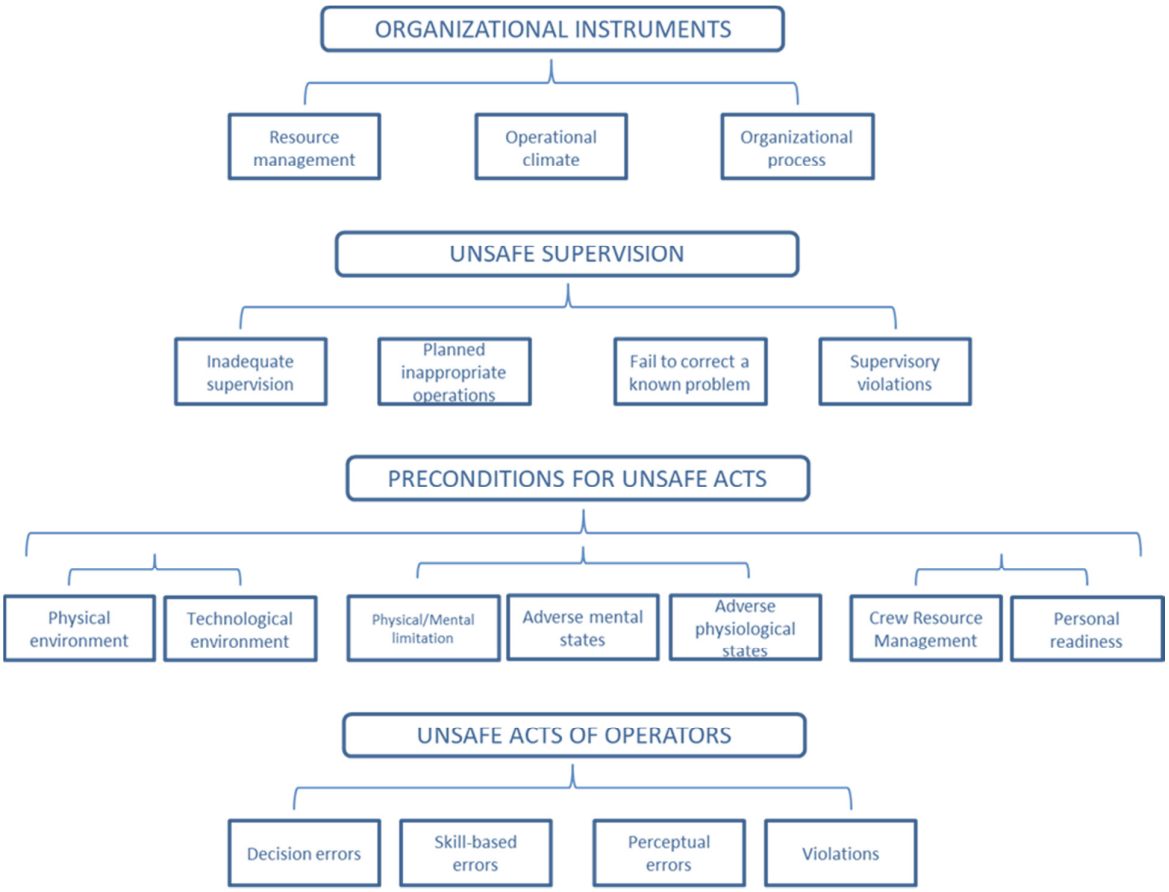


Figure 14 – HFACS scheme [44]

It was initially implemented by Professor James T. Reason and successively furtherly developed by two researchers Shappel and Wiegmann [44], after having analysed about 300 aerial accidents.

The human factor discipline studies the organizational factors, the crew behaviour, performance and management in terms of crew resource management, ergonomics and aeromedical issues, describing and systematically classifying them.

For the purpose of this work, the focus is mainly on human errors and violations (and related barriers/mitigation factors). The difference between them is in the intent. In fact, the error is always unintentional, while the violation is the deliberate performance of an unsafe act by-passing rules, procedures, protocols and established practices within an organization [3].

The consequence of errors and violations is usually a non-compliance with regulations or operative procedures potentially leading to a practical drift and to the generation of an hazard. Errors are actions or inactions performed by the operator leading to deviations from organizational or operator's intentions or expectations. Properly mitigation actions can be applied by the organisation to prevent operator errors from occurring even if human errors will always happen regardless of the level of technology used: rather they can be different or enhanced depending on the kind and complexity of available technology. Within

SMS application, the operators are encouraged by the organisation to report errors occurrence to analyse and classify them and provide proper barriers to reduce their occurrence [3].

Errors are mainly classified as ([3], [44] and [45]):

- Slips and lapses: they are failures in the execution of the intended action. Slips are actions that do no go as planned; lapses are faults of human beings memory
- Mistakes: they are errors in the plan of an action; they occur when the execution of the plan in correct, but it did not lead to the expected outcome

Possible safety strategies to prevent errors from occurrence or to try to eliminate them are the following ones [3]:

- Reductions strategies: they are put in action to reduce or eliminate the factors that can contribute to the error; for example: provision of ergonomic solutions for the aircraft crew
- Capturing strategies: assuming that errors will be made, such strategies are designed to prevent errors from occurring capturing them; for example: provision of checklists for aircraft pilots
- Tolerance strategies: they are those that lead to design the system so that it can accept the error and contain the effects of its consequences; for examples: rendundances on fault tolerant technological systems

The violations [3] are usually deliberate acts of wilful misconduct or omission resulting in deviations from established regulations, procedures, norms or practices. The cases in which the operators violate procedures looking for a shortcut are violations as well (violations in judgment: the operator performs the violation believing not to cause negative consequences with his or her actions).

They are classified as follows [3]:

- Situational violations caused by factors experienced in a specific context like time pressure or excessive workload
- Routine violations: they are violations of procedures due to practicality/workability issues that become, over the time, the normal way of performing a task within a working group. Such violations are committed in those cases when behaving in compliance with the established procedures makes difficult completing the task. This may be due to, deficiencies in human-technology interface design and other issues that cause persons to adopt workaround procedures, which eventually become routine
- Organizationally induced violations: they are such an extension of routine violations. They usually occur when an organization attempts

to meet increased output demands by ignoring or stretching its safety defences

2.4 Conclusions

The main definitions related to Safety Management System and Safety Risk Assessment have been presented in this Chapter.

They have been used to perform the safety analysis on RPAS integrated into the not segregated civil airspace for performance of specific category flight operations.

The complete safety analysis is described and discussed in the following Chapter 3.

Chapter 3

The safety analysis for RPAS flight operations

3.1 Introduction

The aim of the performed research has been the safety analysis of the light RPAS integration into the civil not segregated airspace. According to the definition of Safety Management System, the research has been addressed to identify safety possible hazards and mitigation provisions related to the system under analysis.

In this Chapter, the categorization and identification of hazards is presented and discussed until arriving to the implementation of the U-Space and ATM risk matrices.

Then, the analysis is focused on the U-space matrix only for the further assessment of threats and mitigation provisions applying the Bow Tie Methodology. At this stage of the research, it has been decided to concentrate on the U-Space scenario only because in the next future it will be the first one to host the initial phases of the integration of RPAS with manned aviation.

This part of the work is then preparatory for the implementation of the rules composing the rule-based 'Expert System' knowledge basis described in Chapter 4.

3.2 RPAS safety hazards categorization: a functional approach

As indicated in Paragraph 1.4 two distinct hazard risk matrices have been implemented in this work: the U-space matrix showing the safety assessment of hazards expected to occur during specific category flight operations in the VLL subspace (([18], [28], [29]); these missions will be carried out by light RPAS with maximum take-off weight between 25 and 150 kilograms under U-Space service;

the ATM matrix containing the safety assessment of hazards expected to occur during certified category flight operations mainly between 500 feet of altitude and FL600 and beyond, using RPAS with maximum take-off weight indicatively between 150 and 600 kilograms and flying under ATC control (Table 2).

A regulatory-based integrated system/functional approach has been chosen to categorize the groups of hazards and successively to identify them and proceeding with the analysis. This approach has been preferred due to the lack of historical data on RPAS for the relative infancy of this technology and the current variety of technical features of existing unmanned platforms. In literature, this choice is confirmed to be a proper one as highlighted by many Authors ([46], [47]). More precisely, the classification of RPAS functional requirements draft by NASA in [39] has been applied.

The integration of RPAS into the civil not segregated airspace will involve operational, functional, performance and design requirements [39]. The operational requirements define what is necessary to the RPAS to operate in the airspace. The functional requirements define what tasks and functions the RPAS shall necessarily perform. The performance requirements indicate how well the RPAS shall perform such tasks and functions. The design requirements indicate how the RPAS shall be implemented from the highest to the lowest physical level.

Derived from manned aeronautics, the following four main classes of functional requirements can be applied to the RPAS too with proper differences and peculiar characterizations (Figure 15 [39]):

- Aviate
- Navigate
- Communicate
- Avoid hazards

They includes all functional requirements necessary for a routinely and safely incremental integration of RPAS into the civil airspace. With respect to manned aviation, the RPAS are characterized by a fifth class of additional functionalities (cross-cutting functionalities) defined through the previous mentioned four ones.

Aviate', Navigate' and 'Communicate' are the basic functionality classes that every pilot must adhere to in order to use and properly manage an aircraft system [39]: the 'Aviate' functionality class deals with flying the aircraft; the 'Navigate' functionality class deals with flying the aircraft in the right direction from a starting point to an ending point; the 'Communicate' functionality class deals with communicating own intentions during the flight operations to others; the 'Avoid hazards' deals with the prevention of hazards occurrence with special care for the RPAS [39] due to the absence of the human pilot on board but with the intention nevertheless to ensure safety while integrating RPAS into the not segregated airspace; the 'Cross-cutting' functionality deal with the 'Command and Control' and 'Contingencies Management' functions [39].

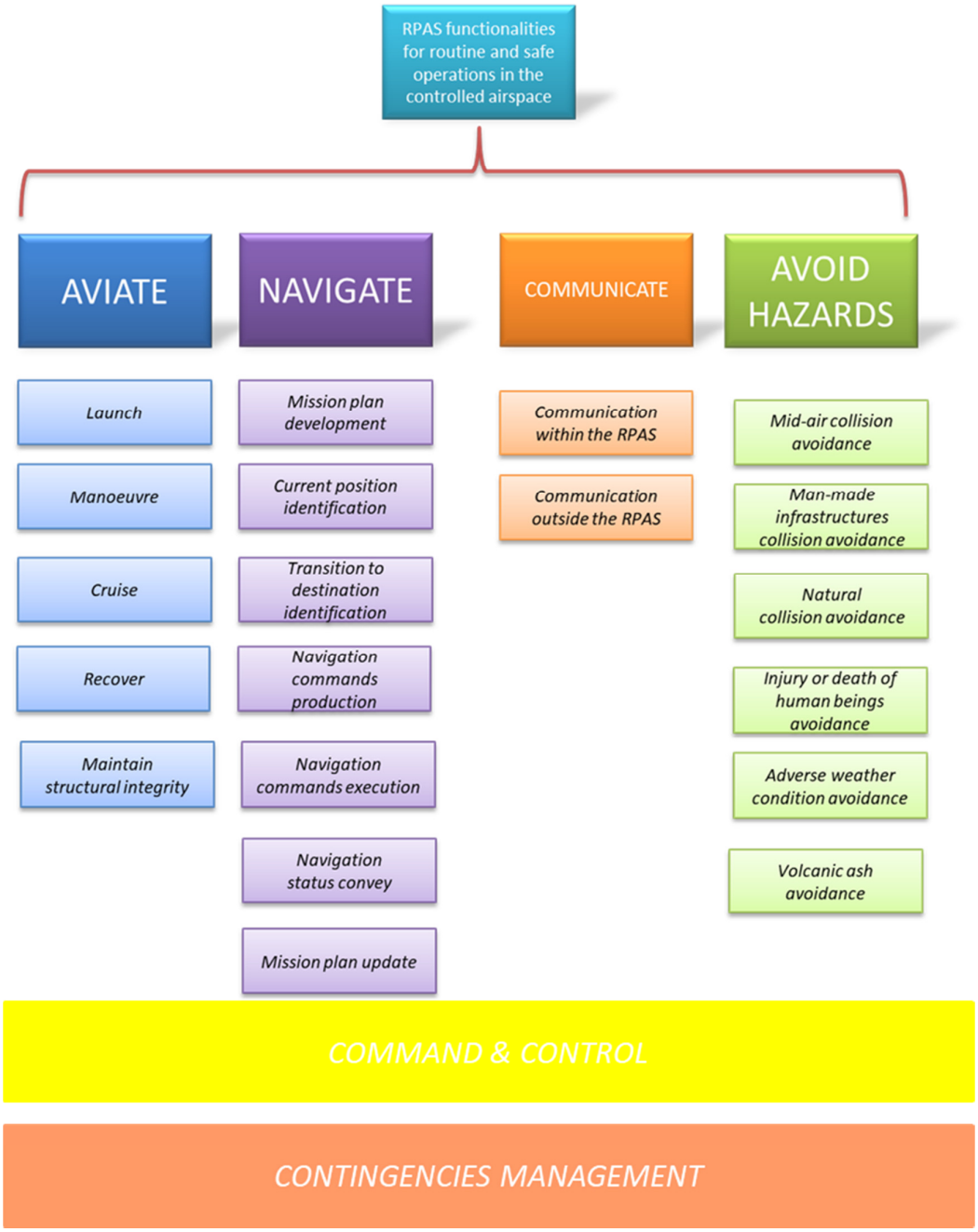


Figure 15 – RPAS functionalities for a routine and safe integration in the controlled airspace [39]

3.2.1 Aviate functionality

The aviate functionality [39] deals more in detail with the capabilities shown in Figure 16 [39].

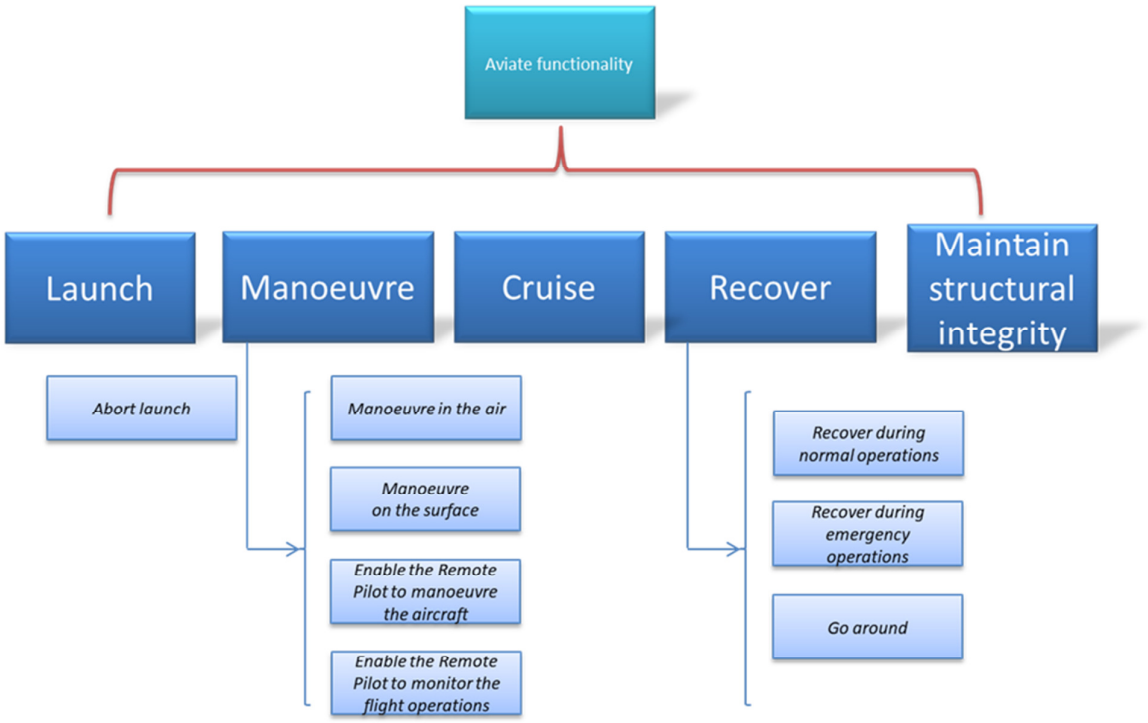


Figure 16 – Aviate functionality [39]

Under normal conditions, the RPA shall be able to take-off/to be launched (with reference to some fixed wing RPA) and abort take-off/launch if a sudden obstacle appears on the potential take-off/lunch trajectory of the aircraft.

The RPA manoeuvring functionality covers air and on ground manoeuvring capabilities. The first one consists of the aircraft capability to change its flight path in terms of heading, airspeed and altitude in the airspace, by mean of flight controls and of the propulsion subsystem. The second one deals with the capability of the aircraft to change its ground speed and path (direction of movement) with respect to the ground. The command signals to manoeuvre the RPA both on ground and on air are generated on ground by the remote pilot by mean of a proper human machine interface (HMI) and converted into radio signals to be sent to the aircraft via the Command and Control (C2) radio link. The HMI is represented by the longitudinal, lateral and directional flight controls and the throttle to manage the aircraft attitude angles and the engines respectively; the HMI can be usually implemented through a joystick and the pedals inside the ground station (Figure 1 [5]) or different level switches arranged on hand-held portable remote controllers (Figure 2 [6] or Figure 3 [7]). Within the aviate functionality, the remote pilot shall be able to monitor the flying aircraft through other HMI devices like displays fed by the RPA downlink telemetry to verify if the aircraft is operating as expected or if corrective actions commanded through on ground controls are requested.

The cruise functionality deals with the RPA capability to perform not accelerated flight in steady state conditions holding altitude or heading or airspeed

or climbing/descending according to contingent causes or ATC clearances and instructions.

The recovery functionality deals with the conclusion of the flight operation that the remotely piloted aircraft shall be able to perform both under normal and emergency conditions like a go around manoeuvre in case of aborted landing in final approach.

The structural integrity is intended as an embedded characteristic of the RPA that must be demonstrated for airworthiness and that shall be warranted during each flight sortie for the whole of its length.

3.2.2 Navigate functionality

The navigate functionality [39] accomplishes the navigation performance into the airspace: the RPA shall be able to go from the initial position of its route to the final destination following the chosen route in the assigned times. In other words, the RPA shall be able to follow the four dimensional navigation path in terms of latitude, longitude, altitude and time (Figure 17 [39]).

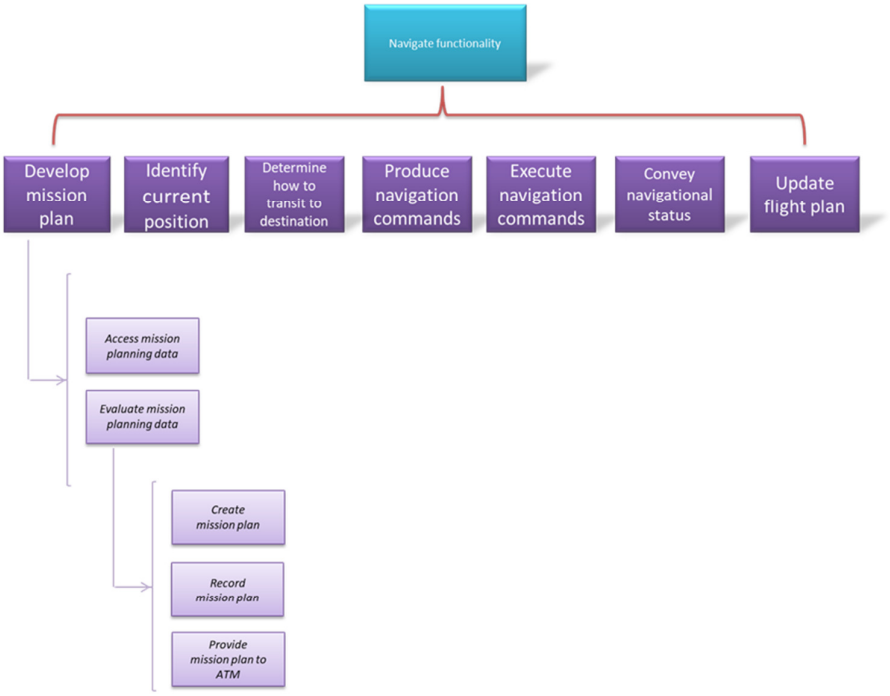


Figure 17 – Navigate functionality [39]

More in details (Figure 17 [39]), the RPAS system shall be able to manage and follow the mission plan to reach the final destination both in normal conditions and in case of contingencies and shall be able to manage them. The RPAS shall access the mission plan to identify the current navigation data, to use them and to modify them adding or erasing waypoints and routes to accomplish contingency or emergency variations to the given initial mission plan. Finally the mission plan shall be recorded and communicated to the traffic management service to interact with the controllers during the flight.

The RPA shall be able to identify its current position in the airspace. More specifically, very high accuracy will be requested to RPAS when flying specific category operations within urban or other kinds of highly congested scenarios; the same can be stated for RPAS requested to perform certified category missions performing for example up to IFR flights ([18], [29]).

The transition to destination is the capability to identify the next waypoint in the route according to the flight plan. Within the navigate functionality, the RPA shall produce and execute navigation command signals to follow the planned route both in normal and contingent or emergency conditions. The execution of navigation command signals is a subset of aviate functionalities: the navigate command signals are generated using flight controls.

The RPA shall convey to ground its navigational state so that the remote pilot or the ATM can verify if the aircraft is following the desired path in the airspace or if corrections are necessary.

Finally, the RPAS shall be able to update the flight plan during flight due to any variation with respect to the original one both during normal flight occurrences (adverse weather conditions, for instance) and during emergency flight occurrences (contingent failures, conflict management, etc.). The flight plan shall also be updated in case of missions lasting many hours or days as it could happen with HALE RPAS (intended in this work for civilian applications only and mainly regarding certified category operation only). This is a performance feature typical of RPAS only due to the absence of the human pilot on board; in this case, different crews would shift on ground to maintain the RPA operative in flight during the whole mission length.

3.2.3 Communicate functionality

The communicate functionality [39] deals with the ability to transmit/receive data voice or ADS-B transponder data with all the entities involved in any RPAS operation or impacted by it (other airspace users) so to perform the operation in a safe and reliable manner both for the RPAS and the other airspace users.

The communication is defined either as internal within the RPAS and external with the ATC or other airspace users (Figure 18 [39]).

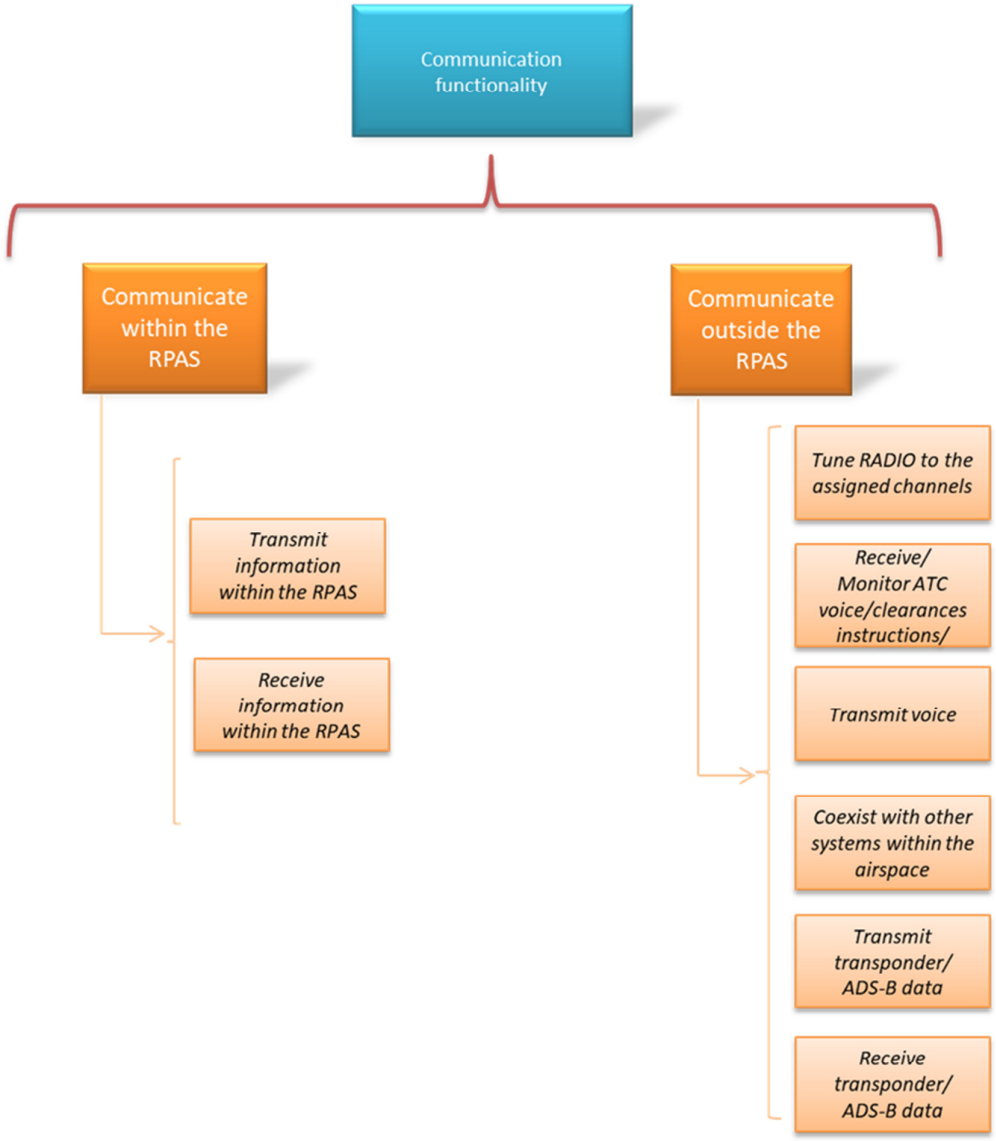


Figure 18 – Communicate functionality [39]

The communication internal to the RPAS is bi-directional: the command and control signals generated by the remote pilot are changed into signals to the RPA on the uplink channel. The RPA telemetry is transmitted from the RPA to the ground on the downlink channel. The RPA telemetry feed the on ground displays that help the remote operator to monitor the RPA and the flight. Among communication internal to the RPAS, a further separated channel shall be dedicated to flight termination functionality. Communication external to the RPAS is the one implemented to contact the ATC as required by EUROCONTROL concept of operations (with reference to certified operations in Class V and Class VI in the subspace between 500 Feet and FL600, and in Class VII in the subspace beyond FL600, [18] and [29]).

3.2.4 Avoid hazards functionality

The avoid hazards functionality [39] is implemented for RPAS through a larger use of advanced technology than for manned aircraft due to the absence of the pilot on board (Figure 19 [39]).

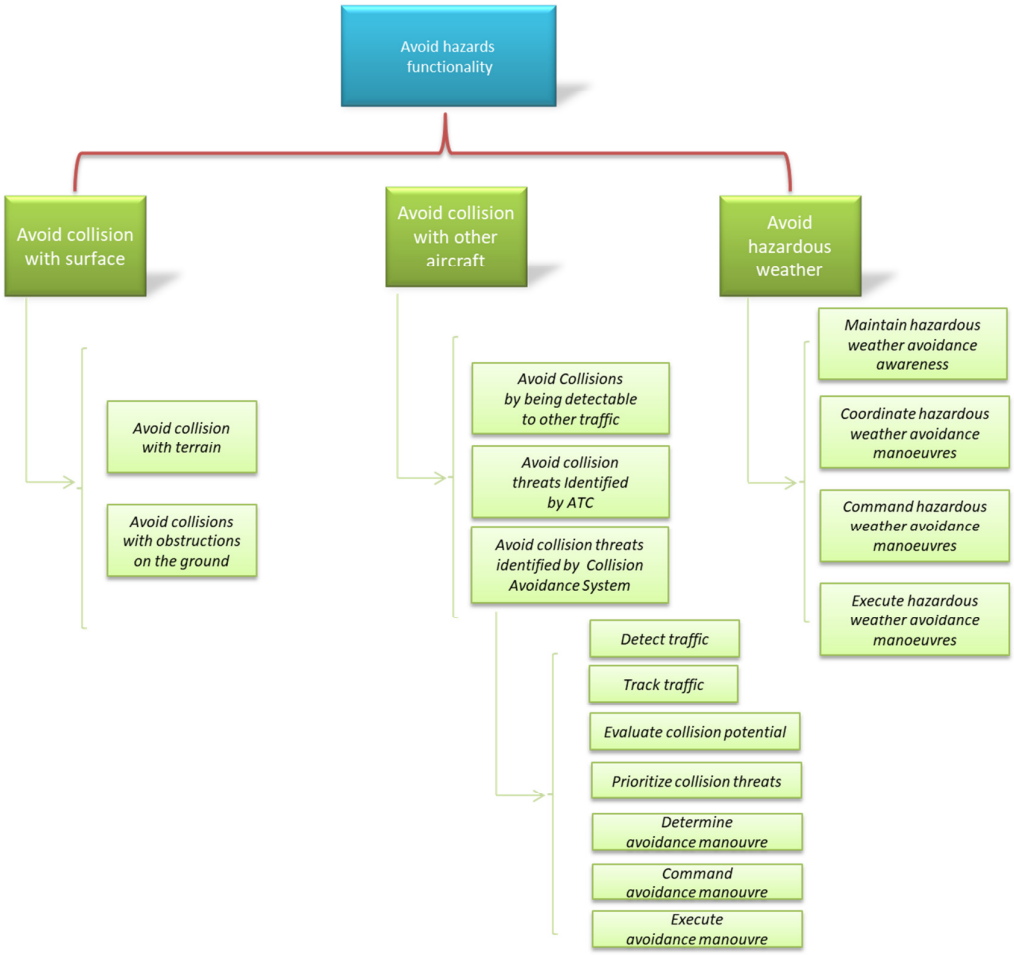


Figure 19 – Avoid hazards functionality [39]

The RPAS will be integrated into the civil not segregated airspace introducing proper mitigation action to avoid:

- Mid-air collision with manned aircraft
- Mid-air collision with other unmanned aircraft
- Collision with people on ground
- Collision with infrastructures and third properties on ground

With reference to Figure 19 [39], these concerns are reflected in the following functionalities: the avoidance of collisions with surfaces that deals with the risk of impact with terrain, bodies of water and obstructions on ground that is natural

obstacles like hills or mountains or man-made infrastructures like buildings, bridges, etc.; the RPA shall avoid mid-air collision with other aircraft in flight being detectable to other traffic so that other traffic too can avoid collision with it; furthermore the RPA shall be able to avoid the contingent threats indicated by the ATC or reported by the Collision Avoidance System installed on the RPA; the Collision Avoidance System shall detect potential conflicting traffic and track it; it shall evaluate the threats collision potential and prioritize them; finally, if it results necessary to avoid the collision in flight, it shall determine the correct avoidance manoeuvre, command it to the RPAS and make the aerial platform to execute it. The collision manoeuvre performance depends upon the RPAS aviate functionality with reference to the generation and execution of requested flight commands.

With reference to weather, the RPAS shall replicate the same capability of adverse weather monitoring and avoidance as the human pilot does with the support of on board instrumentation on manned aircraft. The adverse weather awareness shall be maintained during the whole flight sortie. In case of adverse weather occurrence on the route, the RPAS shall be able to avoid it coordinating the most proper avoidance manoeuvre, commanding it to the aircraft and executing it by mean of the aviate functionality. In the most complex operations the RPAS shall communicate the weather avoidance manoeuvre to the ATC through the 'Communicate' functionality (certified operations in Class V and Class VI in the subspace between 500 Feet and FL600, and in Class VII in the subspace beyond FL600, [18] and [29])

3.2.5 Cross-cutting functionalities

The cross-cutting functionalities [39] deal with the RPAS command and control (C2 radio link) and contingencies management functionalities (Figure 20 [39]).

The command and control functionality comprehends the information exchange, the control of the RPAS operations, the prevention of unauthorized operations to occur and the provision of the link connectivity.

The contingencies management functionality comprehends the RPAS health and status and contingencies management functionality in terms of system status monitoring and possible contingencies identification, prioritization and mitigation.

The information exchange functionality comprehends the uplink communication functionality to send undamaged and uncorrupted timely command signals and controls to the RPA and the downlink communication functionality to receive undamaged and uncorrupted timely telemetry on ground (in the Ground Control Station or to a portable hand held device). The command signals and controls and telemetry shall be exchanged as defined to effectively provide the remote pilot with necessary and correct data at the right time to conduct flight operation in a safe way.

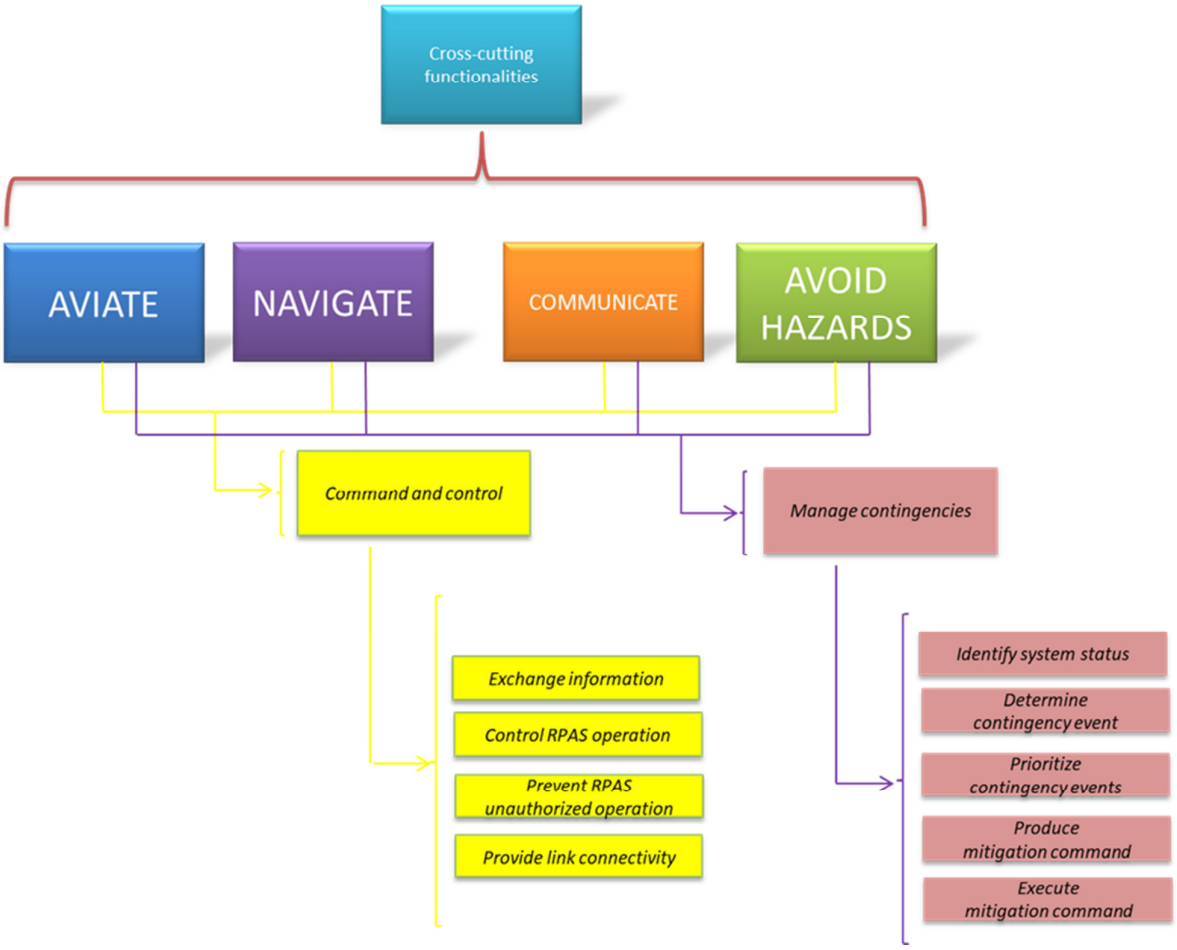


Figure 20 – Cross-cutting functionalities [39]

The uplink communication data include data like the command signals to manoeuvre and control the RPA, the autopilot flight modes, the command signals for the payload sensors and the flight termination in case of emergency condition during flight; the downlink communication data include the RPA subsystems data related to their nominal operation, data useful for the remote pilot situation awareness (alerts and warnings), health and status data from on board RPA subsystems and eventually other data as needed. The health and status parameters sent to the ground can contribute to enhance the remote pilot situational awareness and its safe conduct of the RPA during any flight mission.

The command and control radio link shall be capable of prioritizing the messages according to their importance for the safe conduct of the flight. The high priority messages shall be sent to the aircraft or towards ground before or with less delay than lower priority messages.

The C2 radio link shall not interfere with other telecommunication infrastructures present in the airspace and it shall be shielded from environment unintentional electromagnetic interferences neither it can result harmful to the current safety level of civilian radio communication (specifically within the airspace).

The C2 radio link shall allow the remote pilot, the ATC and any other operator of the airspace to distinguish the commanded and controlled RPA without any ambiguity.

The ground infrastructure or portable devices and the C2 radio link shall be implemented in order to prevent any physical interference with the remote pilot or unauthorized use of the RPAS as well as malicious interference like jamming or spoofing. These last issues deal more specifically with security of the RPAS even if potentially leading to loss of control of the RPA they can cause safety related events with catastrophic consequences (mid-air collision with other aircraft or with obstacles on ground, etc.).

The RPAS shall provide and maintain the C2 radio link connectivity during normal operating conditions against natural or manmade obstacles that can reduce the range of the radio signal and in any passage from 'Line of sight' to 'Beyond of Line of sight' conditions and vice versa or in case of RPAS control transition among ground control stations. This means that during the transition period itself from one ground station in control to another one the radio link with the RPA shall work correctly.

The contingencies management functionality deals with the management of contingent failures, malfunctions or inconveniences that can occur during the RPAS operations. The RPAS shall manage the contingencies to reduce the likelihood and the severity of the consequences with reference to the RPA loss of control. Within this functionality the RPAS shall be able to identify the health and status signals of all its flight critical subsystems and functionalities and convey these information to the remote pilot. The specific contingent event shall be promptly notified to the remote pilot so that contingencies can be prioritized and proper command signals generated, sent to the RPA and executed.

3.2.7 The safety risk assessment

Following the aforementioned regulation-based approach, after having defined the RPAS functionalities according to [39], the safety hazards have been categorized as follows:

- Safety hazards related to the RPAS aviate functionalities
- Safety hazards related to the RPAS navigate functionalities
- Safety hazards related to the RPAS communicate functionalities
- Safety hazards related to the RPAS hazard avoidance functionality
- Safety hazards related to the RPAS cross cutting functionality
    - Within cross cutting functionality, safety hazards caused by contingencies like:
        - Safety hazards deriving from single or combined technical failures
        - Safety hazards deriving from the human factor
        - Safety hazards derived from the weather

The contingent hazards due to RPAS single or multiple failures have been determined executing a complete 'Failure Mode and Effects analysis' (FMECA) and a 'Fault Tree Analysis' (FTA) on RPAS architecture respectively.

The contingent hazards derived from the human factor have been identified performing a structured analysis using the SHELL and HFACS models.

The use of a structured approach to lay down the basis for the safety hazards analysis is hereinafter further highlighted: the highest level hazards have been identified following a systematic categorization of RPAS functionality: hazards related to aviate, navigate, communicate and avoid hazards functionalities. The lowest level hazards caused by contingencies have been identified using structured analysis methodologies too: the FMECA analysis for single failures, the FTA analysis for multiple failures, the SHELL and HFACS model for human factor related hazards. A structured and systematic approach to RPAS hazard analysis helps to cover a wider spectrum of risk: in fact, many sources in literature confirm that incidents and/or accidents can be caused by a large variety of events among mechanical/electrical failures, human operator lacks and problems caused by adverse weather ([48], [49], [50])

The safety hazards analysis is focused on the system 'RPAS integrated in the civil not segregated airspace' not on a specific RPA model: hence, a theoretical RPAS architecture comprehending the most subsystems and equipment has been used for the analysis.

Failure Modes and Effects and Criticality Analysis (FMECA)

The Failure Modes and Effects and Criticality Analysis is a bottom-up analysis methodology that identifies the system components single failure modes, their effects on higher level of the system, and the detectability level and the resulting criticality level associated to each one of them.

In this work the FMECA analysis has been performed according to the Military Standard 1629 Revision A [51].

The RPAS architecture has been defined identifying each functional subsystem and equipment. The RPAS architecture under analysis has been defined from the highest to the lowest level as follows (Figure 21):

- The airborne segment: the aerial platform/the aircraft
- The radio link: the command and control radio link
- The ground segment: a Ground Control Station or a hand-held portable radio controller

Three kinds of architectures have been considered for the RPA (airborne segment) (Figure 21):

- Rotor wing RPA (airborne segment)
- Fixed wing RPA (airborne segment)
- Hybrid RPA (airborne segment)

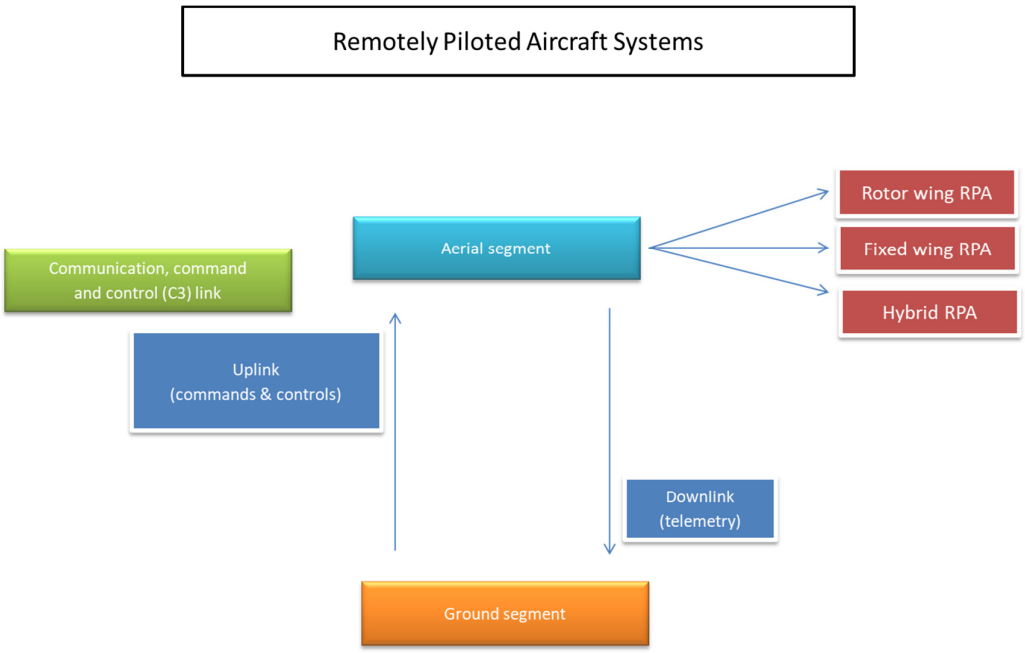


Figure 21 – RPAS higher level architecture

The architectures of each kind of RPA from Figure 21 has been completely defined until the single components. Performing the FMECA, the repetition of the reliability analysis of the common functionalities or equipment among different aerial segments has been avoided: the most comprehensive analysis has been performed for the rotor wing RPA; considering fixed wing or hybrid RPAS only subsystems different from rotor wing RPAS have been considered.

Following the guidelines of the standard 1629A [51], each RPA architecture indicated in Figure 21 has been detailed in terms of subsystems until arriving to the single equipment level definition (Appendix A: Figure 31, Figure 33 and Figure 35 respectively). A simple model for a typical specific category RPAS flight mission has been defined (Appendix A: Figure 32, Figure 34, Figure 36) to properly allocate RPA subsystems functionalities (Appendix A: Table 24, Table 47, Table 62). The failure modes identified for each equipment has been characterized in terms of probability of occurrence, severity of consequences, effects, detectability methods, resulting criticality level and indication for mitigation provisions, in accordance with the Standard 1629A [51]. The failure mode probability of occurrence level has been ranked according to Table 19 [51]; the failure modes severity of consequences has been ranked according to Table 18 [51]; the failure modes detectability has been ranked according to Table 20 [51]; the compensating provisions have been ranked according to Table 21 [51]; the criticality level has been ranked according to Table 22 [51].

The probability of occurrence level of the identified failure modes has been assessed searching for data among the following sources:

- Indications for reliability found in literature (papers): it has to be noted that in most of cases parts of an RPAS or specific functionalities only were object of the analysis
- Reliability data found in reliability handbooks like 'DTIC Not Electronic Parts Reliability Data' [52] and 'Handbook of reliability prediction procedures for mechanical equipment' [53] for mechanical/electrical components and 'Military Handbook 217 Revision F' [54] for electronic components
- 'Mean Time Between Failures' (MTBF) or 'Mean Time To Repair' (MTTR) data derived from RPAS equipment manufacturers data sheet
- Arbitrary reasonable estimations, if no other matching references were available

The above mentioned sources of reliability are referred to manned aeronautical systems or generally speaking mechanical systems; only data deriving from light RPAS equipment data sheet or found in literature inside papers where reliability analyses have been specifically performed on light RPAS did not need for correction to better represent light RPAS most probable reliability performances. In the other cases, proper corrective factors have been investigated and applied to take into account that the effects of environmental conditions induced by RPAS smaller dimensions with respect to hose of manned aircraft. In general it can be stated that current light RPAS failure rate are higher than heavier RPAS like the military ones; and the failure rate of military RPAS are in any case currently higher than for manned civil or military aircraft [55].

For each considered failure mode, the criticality ranking is given by the product of the probability of occurrence level else expressed as 'Probability Number' (PN), the severity of consequences ranking else expressed as 'Severity Number' (SN) and the detectability else expressed as 'Detection Number' (DN) as follows [48]:

$$\text{Criticality ranking} = PN \times SN \times DN \qquad (1)$$

The criticality ranking has been compared against the reference values of Table 22 [51] to classify the considered failure mode criticality as 'High' 'Moderate' or 'Low' ('Red', 'Yellow' and 'Green' respectively). The criticality level is a measure of the harmfulness of the given failure mode: the higher is the probability of occurrence, the higher is the severity of consequences and the more difficult is the failure mode occurrence detection in flight, the worst will be the practical/operational drift the RPAS will suffer during the flight operation until arriving to a catastrophic accident (with RPAS loss, deaths or damages to third parties and high economic loss).

The assessed criticality levels have been used to collect and rank the identified failure modes from the highest critical to the less critical in a final comprehensive list (Appendix A: Table 81). This list has been furtherly skimmed to identify contingent hazards potentially deriving from assessed single failure

mode and used to fill in the U-Space and ATM hazards logs among contingent hazards due to RPAS single failure modes.

The content of the FMECA analysis is reported hereinafter. The results of the complete analysis have been reported in Appendix A.

The rotor wing airborne segment

The rotor wing RPA/airborne segment is composed of the following subsystems (Figure 31):

- Propulsion Subsystem
- Power Subsystem
- Electrical Subsystem
- Flight Subsystem, subdivided into:
    - Navigation Subsystem
    - Air Data Subsystem
    - Flight Control Subsystem
    - Emergency Flight Subsystem
- Mission Data Subsystem
- Payload Data Subsystem
- Communication Subsystem
- Structures

The Propulsion Subsystem

The rotor wing RPAS Propulsion Subsystem is composed of rotor brushless electric motors fed by the electric current produced by the Lithium Polymer batteries. The electric motors angular speed is regulated commanding its variation by mean of the Electronic Speed Controls (ESCs). Each propeller is connected to the electric motor through a bearing spliced on the electric engine shaft. The propeller rotation generates the lift force to operate the rotor wing RPAS.

The failure modes of the following equipment have been analysed: the ESCs, the electric motors, and the propellers (Figure 31).

The failure modes of the ESCs can be (Table 25): seizing, degradation, overheating and burnout [56] (all the further relevant data and calculations have been collected in Table 79):

- The probability of occurrence level of ESC seizing has been estimated as C (Occasional): for reference this failure mode has been assimilated to item B.2-a of [57] for which the probability of occurrence level has been estimated as ‘Medium’/’Occasional’
- The probability of occurrence level of ESC degradation has been estimated as follows: the ESC has been assimilated to a PCB whose global failure rate has been estimated using the following formula

from [53]: $\lambda_p = \lambda_b \times [N_1 \times \pi_C + N_2 \times (\pi_C + 13)] \times \pi_Q \times \pi_E = 0{,}00041 \times [1{,}0 \times 1{,}0 + 1{,}0 \times (1 + 13)] \times 1{,}0 \times 19{,}0 = 0{,}12$ failures per million hours; according to [58] the failure rate reported in [53] and other similar technical documentation is referred to military components. The failure rate of the same component for a current RPAS will be different and it shall be re-sized. An indicative corrective factor equal to 29,31 has been chosen from [58] (figure 6; table 3, severity category 1B). Therefore a more realistic ESC failure rate will be 3,517 failures per million hours. The duration of a current typical RPAS mission can be 2 hours [58]. This value will be more accurate in future as soon as daily routine specific category RPAS mission will really occur. The calculated probability of occurrence of the ESC degradation is 7,03E-6. The overall ESC failure rate has been estimated as follows: from [58] (figure 6), the overall ESC corrected failure rate is 0,000125 failure per hour, that is 1,25E-04 failures per million hours. The resulting overall ESC probability of failure is 2,49E-04 (during a complete flight mission of 2 hours). The ESC degradation failure mode probability of occurrence level has been evaluated as 0,028 (7,03E-6/2,49E-04) that is C (Occasional)

- The probability of occurrence level of ESC overheating has been estimated as C (Occasional) due to the possibility of the electric motors prolonged use and assimilating this failure mode for reference to item B.2-a of [57] for which the probability of occurrence level has been estimated as 'Medium'/'Occasional'
- The probability of occurrence level of ESC burnout has been estimated as C (Occasional), assimilating this failure mode to item B.2-a or B.2-d of [57] for which the probability of occurrence level has been estimated in both cases as 'Medium'/'Occasional'

The loss or degradation of ESCs brings to degradation in rotor engines control of angular speed variation. This failure condition can lead to the loss of manoeuvrability of the rotor wing RPAS, therefore to its loss of control and ultimately to the system (RPA) loss. Hence, the severity of the consequences of the each ESCs single failure mode has been classified as 'Catastrophic'.

No means of detection of the above listed ESCs failure modes when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None' for the considered failure modes.

The resulting criticality level of ESCs failure modes is 'High' (Table 26).

The failure modes of the brushless electric motors can be due to (Table 25): stator housing (or casing) failure, bearing failure, windings failure, and armature shaft failure [53]; all the other further details and relevant data related to the calculations indicated hereinafter have been collected in Table 79:

- The brushless stator housing failure rate is 0,001 failures per million hours according to [53]. Applying the corrective factor [68] (figure 6; table 3, severity category 1B) and considering 2 hours of RPA flight mission, the brushless motor housing failure mode is 5,86E-08. The brushless electric motor overall failure rate has been estimated equal to 0,002125 failure/hours using figure 6 of [58]. The brushless electric motor overall probability of failure results equal to 4,25E-05 (considering a complete flight mission of 2 hours). The brushless electric motor stator housing failure mode level is about 0,0014 (5,86E-08/4,25E-05), that is D (Remote)
- The probability of occurrence level of electric motor bearing failure has been estimated as C (Occasional) ([57], with reference to item B.3-a, for example for wear due to bad or lack of lubrication [59] and for which the probability of occurrence level has been estimated as 'Medium'/'Occasional')
- The probability of occurrence level of windings open circuit and short circuit failure modes has been estimated as D (Remote) ([57], with reference to item B.3-c, for which the probability of occurrence level has been estimated as 'Low')
- The probability of occurrence level of the electric motor armature shaft failure has been estimated as D (Remote)

The loss or degradation of the RPAS electric motors brings to degradation and loss of engine trust, loss of aircraft lift and ultimately to the system (RPA) loss: for this reason the RPAS motors failure modes have been classified as 'Catastrophic'.

No means of detection of the above listed brushless electric motor failure modes when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None' for the considered failure modes.

The resulting criticality level of engine failure modes is 'Medium' (Table 26).

The failure modes of the propellers can be (Table 25): propeller structural failure, propeller connection failure and abrupt stop of the propeller [57]:

- The probability of occurrence level of the propeller structural failure has been estimated as E (Extremely unlikely) [57] (Table 79)
- The probability of occurrence level of the propeller connection failure been estimated as D (Remote) [57] (Table 79)
- The probability of occurrence level of the abrupt stop of the propeller has been estimated as E [57] (Table 79)

The loss of the propeller leads to the loss of lift and therefore to the loss of system manoeuvrability, system control and ultimately to the system (RPA) loss:

for this reason the severity of the consequences of the propeller failure modes has been classified as 'Catastrophic'.

No means of detection of the above listed propeller failure modes when the aircraft is in flight have been identified in literature. Therefore the detection method has been classified as 'None' for the considered failure modes.

The resulting criticality level of propeller failure modes 'Low' (Table 26).

The Power Subsystem

The rotor wing RPAS Power Subsystem consists of 'Lithium Polymer' (LiPo) batteries that generate DC current to supply the RPAS engines and all the other on board electrical equipment (Figure 31).

The failure modes of the following equipment have been analysed: LiPo batteries.

The failure modes of the LiPo batteries can be (Table 27): short circuit, mechanical damage and fire ([57], [60]).

- The probability of occurrence level of LiPo batteries short circuit has been estimated as C (Occasional) ([57], item B.1-a, with reference to internal short circuit and [57] item B.1-b, with reference to overcharging and over discharging and for which the probability of occurrence level has been estimated in both cases as 'Medium'/'Occasional') (Table 79)
- The probability of occurrence level of LiPo batteries mechanical damage has been estimated as C (Occasional) ([57], item B.1-b, with reference to mechanical damage and for which the probability of occurrence level has been estimated as 'Medium'/'Occasional') (Table 79)
- The probability of occurrence level of LiPo batteries fire has been estimated as C (Occasional) ([57], item B.1-b, with reference to extreme temperatures and for which the probability of occurrence level has been estimated as 'Medium'/'Occasional') (Table 79)

The degradation or loss of LiPo batteries leads to the loss of the RPAS electrical engines and ultimately to the loss of propulsion and ultimately system (RPA) loss; therefore the severity of the consequences of the LiPo batteries failure modes has been classified as 'Catastrophic'.

The LiPo batteries electrical can be detected using devices like LiPo battery voltage alarms or buzzers [61]; the alarm/buzzer failure will alert the remote pilot as soon as the LiPo voltage decreases below a minimum threshold; in this case the failure mode is expected to be detected in flight through a visible/audible warning system. For the other two LiPo batteries failure modes no specific detection methods have been identified in literature.

The resulting criticality level of LiPo batteries failure modes is 'High' (Table 28).

The Electrical Subsystem

The RPAS Electrical Subsystem mainly consists of balance cable, distribution cables and connectors to transport the electrical current from the LiPo batteries to all the RPAS electrical equipment/loads (Figure 31).

The failure modes of the following equipment have been analysed: the balance cables (that is the breakout wires to access each cell of the LiPo battery) [62], the distribution cables and the connectors (Table 29).

The failure modes of the balance cables can be short circuit and open circuit [63] (Table 29); all the other further details and relevant data related to the calculations indicated hereinafter have been collected in (Table 79):

- The cable short circuit failure rate is 3,0E-08 [64]. No corrective factors have been applied to cables failure rate, as suggested in [58]. The calculated probability of occurrence of this failure mode is equal 6,0E-08 (considering a complete flight mission of 2 hours). Assimilating the balance cables to generic electrical cables, the failure rate is equal to 0,6270 failures per million hours [52]. As said before, no corrective factors have been applied [58]. The calculated balance cable overall probability of failure is equal to 1,254E-06 (considering a complete flight mission of 2 hours). The balance cable short circuit failure mode probability of occurrence level is equal to 0,0478 (6,0E-08/1,254E-06), that is C (Occasional)
- The balance cable open circuit failure rate is 1,0E-05 [64]. No corrective factors have been applied to cables failure rate, as suggested in [58]. The calculated probability of occurrence of this failure mode is equal 1,999E-05 (considering a complete flight mission of 2 hours). Assimilating the balance cables to generic electrical cables, the failure rate is equal to 0,6270 failures per million hours [52]. As said before, no corrective factors have been applied [58]. The calculated balance cable overall probability of failure is equal to 1,254E-06 (considering a complete flight mission of 2 hours). The balance cable short circuit failure mode probability of occurrence level is equal to 15,949 (1,999E-05/1,254E-06), that is A (Frequent)

The degradation or loss of the electrical balance cables leads to the loss of the electrical current supply from the LiPo batteries; among the others, it leads to the loss of engines and ultimately to the system (RPA) loss. Therefore the severity of the consequences of the balance cables failure modes has been classified as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None' for the above mentioned failure mode.

The resulting criticality level of balance cables failure mode is 'High' (Table 30).

The failure modes of a generic distribution cable can be short circuit and open circuit (Table 29); all the other further details and relevant data related to the calculations indicated hereinafter have been collected in Table 79:

- The cable short circuit failure rate is 3,0E-08 [64]. No corrective factors have been applied to cables failure rate, as suggested in [58]. The calculated probability of occurrence of this failure mode is equal 6,0E-08 (considering a complete flight mission of 2 hours). Assimilating the balance cables to generic electrical cables, the failure rate is equal to 0,6270 failures per million hours [52]. As said before, no corrective factors have been applied [58]. The calculated balance cable overall probability of failure is equal to 1,254E-06 (considering a complete flight mission of 2 hours). The balance cable short circuit failure mode probability of occurrence level is equal to 0,0478 (6,0E-08/1,254E-06), that is C (Occasional)
- The balance cable open circuit failure rate is 1,0E-05 [64]. No corrective factors have been applied to cables failure rate, as suggested in [58]. The calculated probability of occurrence of this failure mode is equal 1,999E-05 (considering a complete flight mission of 2 hours). Assimilating the balance cables to generic electrical cables, the failure rate is equal to 0,6270 failures per million hours [52]. As said before, no corrective factors have been applied [58]. The calculated balance cable overall probability of failure is equal to 1,254E-06 (considering a complete flight mission of 2 hours). The balance cable short circuit failure mode probability of occurrence level is equal to 15,949 (1,999E-05/1,254E-06), that is A (Frequent)

The degradation or loss of the electrical distribution cables leads to the loss of the electrical current supply from the LiPo batteries; among the others, it leads to the loss of engines and ultimately to the system (RPA) loss. Therefore the severity of the consequences of the balance cables failure modes has been classified as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None' for the above mentioned failure mode.

The resulting criticality level of balance cables failure mode is 'High' (Table 30).

The failure mode of the connectors is electric arc due to mechanical disconnection (Table 29):

- The probability of occurrence level of this failure mode has been estimated as C (Occasional) (Table 79)

The sudden disconnection of cables form equipment (due to vibrations, fatigue or improper maintenance actions, etc.) can lead to electric arc and to fire on board the RPAS and ultimately to the system (RPA) loss. Therefore the severity of the consequences of the electrical connectors failure mode has been classified as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of the connectors failure mode is 'High' (Table 30).

The Flight Subsystem/Navigation Subsystem

The RPAS Navigation Subsystem mainly consists of the 'Inertial Measurement Unit' (IMU) and the 'Global Position System' (GPS) receiver (Figure 31).

The 'European Geostationary Navigation Overlay Service' (EGNOS) receiver and the 'Automatic Dependant Surveillance Broadcast' (ADS-B) receiver have been virtually added in the architecture of a remotely piloted aircraft Navigation Subsystem, even if at the moment they are not included, to perform the FMECA/FTA analyses on these equipment too and thus successfully deriving the related hazards for a more comprehensive safety evaluation. The EGNOS receiver is more accurate and advanced than the GPS one in aircraft position determination and currently starts to equip the most updated civil manned aircraft; as stated by other Authors [65], the EGNOS can effectively support RPAS in performing precision navigation within urban or very congested flight environments. The ADS-B equipment, that will be mandatory on manned aircraft from 2020 onwards [66], will be recommended to RPAS too as basic equipment of the 'Detect and Avoid' subsystem to avoid mid-air collision with other aircraft.

The failure modes of the following equipment have been analysed: the IMU, the GPS and EGNOS receivers and the ADS-B.

The failure modes of IMU can be (Table 31): circuitry overload and calibration loss [58]; all the other further details and relevant data related to the calculations indicated hereinafter have been collected in (Table 79):

- The probability of occurrence level of IMU circuitry overload failure mode has been estimated as D (Remote) ([57] with reference to item D.6-a and for which for which the probability of occurrence level has been estimated as 'Low') (Table 79)

- The probability of occurrence level of IMU loss of calibration failure mode has been estimated as C (Occasional) ([57], with reference to item D.6-b and for which for which the probability of occurrence level has been estimated as 'Medium'/'Occasional') (Table 79)

The degradation or loss of IMU leads to mission degradation. Therefore the severity of the consequences of the IMU failure modes has been classified as 'Marginal'.

No means of detection of the above mentioned failure modes when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of the connectors failure mode is 'Medium' and 'High' (Table 32).

The failure modes of the GPS receiver can be (Table 31): antenna failure, and malicious radio frequency interferences like jamming or spoofing; all the other further details and relevant data related to the calculations indicated hereinafter have been collected in Table 79:

- The probability of occurrence level of GPS antenna failure ([67] with reference to item AOA24) has been estimated as follows: the probability of occurrence of this failure mode is 1,0E-04 ([68] referring to item LOA-14 of the FTA); the failure rate of a GPS equipment installed on board an RPA is equal to 6,0E-03 ([69] with reference to air cargo MTBF datum equal to 6000 hours); this datum has been corrected according to [58] (corrective factor equal to 22,095 (2/0,105) from figure 6 and table 3); considering a standard flight mission of 2 hours, the probability of occurrence of the overall GPS failure has been estimated equal to 2,3290E-01; the GPS antenna failure mode is characterized by a probability of occurrence level equal to 0,0004294 (1,0E-04/2,3290E-01) that is E (Extremely Unlikely)
- The probability of occurrence level of GPS signal jamming ([67] with reference to item AOA14) has been estimated as follows: the probability of occurrence of this failure mode is 1,0E-13 ([68] referring to item LOA-15 of the FTA); considering the above calculated overall GPS equipment failure equal to 2,3290E-01 (as above calculated), the GPS signal jamming failure mode is characterized by a probability of occurrence level equal to 4,2936E-13 (1,0E-13/2,3290E-01) that is E (Extremely Unlikely)
- The probability of occurrence level of GPS signal spoofing has been estimated as B due to the current lack of effective cyber threats counter measures

The GPS antenna failure can lead to mission degradation. Therefore the severity of the consequences of this failure mode has been classified as 'Marginal'. The GPS signal jamming and/or spoofing failure modes can lead to the loss of RPA system control and ultimately to the system (RPA) loss; therefore the severity of their consequences has been ranked as 'Catastrophic'.

The GPS antenna failure mode is expected to be detected in flight by the remote pilot for example though visual or audible warning.

The GPS signal jamming consists of disrupting the control of the aerial platform using a transmitter tuned at the same frequency and modulation of the GPS receiver antenna installed on board the RPA, but characterized by such high power to override any signal sent to it [70]. It cannot be detected in flight, therefore 'None' detection method has been assigned to this GPS failure mode.

The GPS signal spoofing consists of deceiving a GPS receiver by broadcasting incorrect GPS signals but structured as a set of normal GPS signals, or by rebroadcasting toward the RPA to be spoofed a normal signal captured elsewhere or set at a different time. The result is that the GPS receiver estimates a spatial position that is not the real one as it was in a position other than where it really is or it estimates to be at the correct spatial position but at a time other than the real one; the hacker chooses how to manage the attack [71]. This failure mode can be detected in flight by the remote pilot passing from automatic to manual RPA flight mode and comparing the desired route to follow with the one really followed by the aircraft. Therefore the detection method related to this GPS failure mode has been ranked as 'Other methods'.

The resulting criticality level of the GPS antenna failure mode has been ranked as 'Low' (Table 32).

The resulting criticality level of the GPS jamming and spoofing failure modes have been ranked as 'Low' (Table 32).

The failure modes of the EGNOS receiver can be (Table 31) ([72] and [73]): EGNOS receiver failure, loss of EGNOS signal continuity, loss of EGNOS signal integrity and EGNOS signal delay; all the other further details and relevant data related to the calculations indicated hereinafter have been collected in Table 79:

- The EGNOS receiver failure rate is equal to 9,04E-06 ([74]; this datum has been corrected according to [58] (corrective factor equal to 22,095 (2/0,105) from figure 6 and table 3); considering a standard RPAS mission of 2 hours, the probability of occurrence of this failure mode has been estimated as 3,994E-04; the probability of occurrence of the overall EGNOS equipment failure has been determined as follows: the EGNOS MTBF is equal to 40.000 hours from [73]; the failure rate is equal to 25,0 failures per million hours; this datum has been corrected according to [58] (corrective factor equal to 22,095 (2/0,105) from figure 6 and table 3); considering a standard RPAS mission of 2 hours, the probability of occurrence of overall EGNOS equipment failure is 1,104E-03; the EGNOS receiver failure mode

probability of occurrence level is equal to 0,361 (3,994E-04/1,104E-03E-05), that is A (Frequent)

- The EGNOS loss of signal continuity probability of occurrence is equal to 9,04E-06 [73]; no corrective factors have been deemed to be applicable considering the properties of EGNOS signal as independent of the user; considering the above calculated overall EGNOS equipment probability of failure is 4,999E-05 during a standard RPAS mission, the EGNOS loss of signal continuity failure mode probability of occurrence level is equal to 0,08 (9,04E-06/4,999E-05), that is D (Remote)
- The EGNOS loss of signal integrity probability of occurrence is equal to 1,0E-09 [72]; no corrective factors have been deemed to be applicable considering the properties of EGNOS signal as independent of the user; considering the above calculated overall EGNOS equipment probability of failure is 4,999E-05 during a standard RPAS mission, the EGNOS loss of signal continuity failure mode probability of occurrence level is equal to 2,0E-05 (1,0E-09/4,999E-05), that is E (Extremely Unlikely)
- The EGNOS loss of signal delay probability of occurrence is equal to 3,2E-06 [74]; no corrective factors have been deemed to be applicable considering the properties of EGNOS signal as independent of the user; considering the above calculated overall EGNOS equipment probability of failure is 4,999E-05 during a standard RPAS mission, the EGNOS signal delay failure mode probability of occurrence level is equal to 0,0064 (3,2E-06/4,999E-05), that is D (Remote)

The consequence of EGNOS receiver degradation or loss can be the RPAS mission degradation. Therefore the severity of consequences of the above mentioned EGNOS failure modes has been ranked as ‘Marginal’.

The EGNOS failure modes are expected to be detected in flight, as it happens for EGNOS receivers installed on manned aircraft, through the use of ‘Built In Test’ devices and alerting systems [75].

The resulting criticality level of EGNOS failure modes is ‘High’, ‘Medium’ and ‘Low’ in accordance with the estimated level of probability of occurrence level (Table 32).

The failure modes of the ADS-B receiver can be (Table 31): loss of EGNOS position accuracy, GPS receiver unit failure, ADS-B out antenna failure, ADS-B out antenna deterioration, broadcast of distorted data, emitter/transponder failure, erroneous altitude data, data encoding error, loss of position data to be sent to the emitter, abrupt interruption of ADS-B service, abrupt lack of GPS data, degradation of accuracy of data sent by the satellite to the ADS-B, loss of satellite signal integrity, failure to detect manoeuvring aircraft, ground equipment failure, sudden loss of ADS-B data, ADS-B ground station failure, human error; all the

other further details and relevant data related to the calculations indicated hereinafter have been collected in Table 79:

- The probability of occurrence of ADS-B loss of EGNOS position accuracy ([67], item AOA-21) is equal to 5,0E-02 [68] (with reference to item COAP-5 of the FTA analysis); the MTBF of ADS-B is equal to 20,000 hours [76]; the failure rate is equal to 5,0E-05; this datum has been corrected according to [58] (corrective factor equal to 22,095 (2/0,105) from figure 6 and table 3); considering a standard RPAS mission of 2 hours, the probability of occurrence of this failure rate has been estimated as 2,207E-03; the ADS-B loss of position accuracy failure mode probability of occurrence level is equal to 22,654 (5,0E-02/2,207E-03), that is A (Frequent)
- The probability of occurrence of EGNOS receiver unit failure is equal to 9,04E-06 (as calculated for item NSS4b); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the ADS-B EGNOS receiver unit failure mode probability of occurrence level is equal to 0,1810 (5,0E-02/2,207E-03), that is B (Reasonably Probable)
- The probability of occurrence of ADS-B out antenna failure ([67], item AOA-25) is equal to 1,0E-04 [68] (with reference to item LOA-4 of the FTA analysis); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the ADS-B out antenna failure probability of occurrence level is equal to 0,045 (1,0E-04/2,207E-03), that is C (Occasional)
- The probability of occurrence of ADS-B out antenna deterioration ([67], item AOA-4) is equal to 1,2E-03 [68] (with reference to item COA-1 of the FTA analysis and solving the 'OR' Boolean operator); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the ADS-B out antenna deterioration probability of occurrence level is equal to 0,544 (1,2E-03/2,207E-03), that is A (Frequent)
- The probability of occurrence of ADS-B interruption of signal transmission due to RF interference ([67], item AOA-6) is equal to 1,0E-02 [68] (with reference to item CAA-9 of the FTA analysis); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the ADS-B interruption of signal transmission due to RF interference failure probability of occurrence level is equal to 4,530 (1,2E-03/2,207E-03), that is A (Frequent)
- The probability of occurrence of ADS-B emitter/transponder failure ([67], item AOA-7) is equal to 1,0E-04 [68] (with reference to item LOA-8 of the FTA analysis); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); ADS-B emitter/transponder failure mode probability of occurrence level is equal to 0,453 (1,0E-04/2,207E-03), that is A (Frequent)

- The probability of occurrence of altimeter erroneous altitude data ([67], item AOA-11) is equal to 1,0E-13 [68] (with reference to item COA-11 of the FTA analysis); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the altimeter erroneous altitude data failure mode probability of occurrence level is equal to 4,351E-11 (1,0E-13 /2,207E-03), that is E (Extremely Unlikely)
- The probability of occurrence of ADS-B data encoding error ([67], item AOA-10) is equal to 1,0E-13 [68] (with reference to item COA-11 of the FTA analysis); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the ADS-B data encoding error failure mode probability of occurrence level is equal to 4,351E-11 (1,0E-13/2,207E-03), that is E (Extremely Unlikely)
- The probability of occurrence of intentional/unintentional jamming of ADS-B signal ([67], item AOA-14) is equal to 1,0E-13 [68] (with reference to item LAA-8 of the FTA analysis); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the intentional/unintentional jamming of ADS-B signal failure mode probability of occurrence level is equal to 4,351E-11 (1,0E-13/2,207E-03), that is E (Extremely Unlikely)
- The probability of occurrence of lack of ADS-B service ([67], item AOA-16) is equal to 1,0E-13 [68] (with reference to item LAA-10 of the FTA analysis); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the lack of ADS-B service probability of occurrence level is equal to 4,351E-11 (1,0E-13/2,207E-03), that is E (Extremely Unlikely)
- The probability of occurrence of inaccurate position datum sent to the ADS-B emitter ([67], item AOA-21) is equal to 5,0E-02 [68] (with reference to item COAP-5 of the FTA analysis); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the inaccurate position datum sent to the ADS-B emitter failure mode probability of occurrence level is equal to 22,654 (5,0E-02/2,207E-03), that is A (Frequent)
- The probability of occurrence of degradation of accuracy and integrity of data sent by the satellite to the ADS-B ([67], item AOA-22) is equal to 1,0E-09 [72]; the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the inaccurate position datum sent to the ADS-B emitter failure mode probability of occurrence level is equal to 4,351E-07 (1,0E-09/2,207E-03), that is E (Extremely Unlikely)
- The probability of occurrence of failure of ADS-B transponder/emitter on the RPA ([67], item AOA-27) is equal to 1,0E-04 [68] (with reference to item COA-10 of the FTA analysis); the ADS-B overall

equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the failure of ADS-B transponder/emitter on the RPA failure mode probability of occurrence level is equal to 0,0453 (1,0E-04/2,207E-03), that is C (Occasional)

- The probability of occurrence of failure in detection of manoeuvring aircraft/RPA ([67], item AOA-23) is equal to 1,2E-03 [68] (with reference to item COAP-4 of the FTA analysis, solving the Boolean 'OR' operator); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the failure of ADS-B transponder/emitter on the RPA failure mode probability of occurrence level is equal to 0,544 (1,2E-03/2,207E-03), that is A (Frequent)
- The probability of occurrence of sudden loss of ADS-B data to ATC controllers without any notification ([67], item AOG-3) is equal to 1,0E-05 [68] (with reference to item LAA-4 of the FTA analysis); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the failure of ADS-B transponder/emitter on the RPA failure mode probability of occurrence level is equal to 0,00453 (1,0E-05/2,207E-03), that is D (Remote)
- The probability of ADSB-IN receiving antenna deterioration ([67], item AI1) is equal to 1,0E-04 [68] (with reference to item LAA-7 of the FTA analysis); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the failure of ADS-B transponder/emitter on the RPA failure mode probability of occurrence level is equal to 0,0453 (1,0E-04/2,207E-03), that is C (Occasional)
- The probability of ADS-B ground station failure is equal to 1,3E-04 [68] (with reference to item LAA-1 of the FTA analysis solving the Boolean 'OR' operator); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the failure of ADS-B transponder/emitter on the RPA failure mode probability of occurrence level is equal to 0,00453 (1,3E-04/2,207E-03), that is D (Remote)
- The probability of performance of wrong pre-flight procedures on ADS-B is equal to 2,0E-04 [68] (with reference to item LOA-1 of the FTA analysis solving the Boolean 'OR' operator); the ADS-B overall equipment failure probability of occurrence is equal to 2,207E-03 (as above calculated); the failure of ADS-B transponder/emitter on the RPA failure mode probability of occurrence level is equal to 0,0906 (2,0E-04/2,207E-03), that is C (Occasional)

The consequence of ADS-B equipment degradation or loss can lead to the degradation of 'Detect and Avoid' subsystem functionality and to the risk of

occurrence of mid-air collisions. Therefore the severity of consequences of the above mentioned ADS-B failure modes has been ranked as 'Catastrophic'.

Following the ADS-B analysis reported in [66], some of the ADS-B failure modes listed in Table 31 cannot be detected in flight; other ones can be detected in flight. In the first case 'None' detection method has been assigned to the considered failure modes; in the second case it has been supposed that those failure modes can be detected through visual or audible warning addressed to the remote pilot (Table 31).

The resulting criticality level of ADS-B failure modes has been ranked as 'High', 'Moderate' and 'Low' in accordance with the estimated level of probability of occurrence (Table 32).

The Flight Subsystem/Air Data Subsystem

The RPAS Air Data Unit Subsystem comprehends the equipment to measure airspeed and barometric altitude flight parameters (Table 31). The failure modes of the Air Data Unit are (Table 33) [53]: incorrect signal, loss of signal, signal error along the transmission line, error on output signal, loss of power supply; calibration error all the other further details and relevant data related to the calculations indicated hereinafter have been collected in Table 79:

- The probability of occurrence level of Air Data Unit incorrect signal has been estimated as follows: the related failure rate is equal to 2.0 failure per million hours ([53], with reference to pressure sensors sensing elements failure); this datum has been corrected according to [58] (corrective factor equal to 22,095 (2/0,105) from figure 6 and table 3); considering a standard RPAS mission of 2 hours, the probability of occurrence of this failure rate has been estimated as 8,837E-05. The Air Data Unit MTBF is equal to 400,000 hours [77]; this data is referred to manned aircraft equipment; the above mentioned corrective factor is applied to re-size this value; the estimated probability of overall Air Data Unit failure occurrence is equal to 1,105E-04; the Air Data Unit incorrect signal failure mode probability of occurrence level is equal to 0,8 (8,837E-05/1,105E-04), that is A (Frequent)
- The probability of occurrence level of Air Data Unit loss of signal has been estimated as follows: the related failure rate is equal to 2.0 failure per million hours ([53], with reference to pressure sensors sensing elements failure); this datum has been corrected according to [58] (corrective factor equal to 22,095 (2/0,105) from figure 6 and table 3); considering a standard RPAS mission of 2 hours, the probability of occurrence of this failure rate has been estimated as 8,837E-05. The Air Data Unit probability of overall Air Data Unit failure occurrence is equal to 1,105E-04 as above calculated; the Air Data Unit loss of

signal failure mode probability of occurrence level is equal to 0,8 (8,837E-05/1,105E-04), that is A (Frequent)

- The probability of occurrence level of Air Data Unit signal error along the transmission line has been estimated as follows: the related failure rate is: $\lambda_p = \lambda_b \times \pi_Q \times \pi_E = 0{,}026 \times 1 \times 16 = 0{,}416$ failure per million hours ([54], with reference to line failure rate); this datum has been corrected according to [58] (corrective factor equal to 22,095 (2/0,105) from figure 6 and table 3); considering a standard RPAS mission of 2 hours, the probability of occurrence of this failure rate has been estimated as 1,838E-06. The Air Data Unit probability of overall Air Data Unit failure occurrence is equal to 1,105E-04 as above calculated; the Air Data Unit error along the transmission line failure mode probability of occurrence level is equal to 0,0166 (1,838E-06/1,105E-04), that is C (Occasional)
- The probability of occurrence level of Air Data Unit signal error on output signal has been estimated as follows: the related failure rate is $\lambda_p = (C1 \times \pi_T + C2 \times \pi_E) \times \pi_E \times \pi_L = (0{,}24 \times 0{,}10 + 0{,}019 \times 8) \times 0{,}25 \times 2{,}0 = 0{,}088$ failure per million hours ([54], with reference to computational devices/microprocessors failure rate); this datum has been corrected according to [58] (corrective factor equal to 22,095 (2/0,105) from figure 6 and table 3); considering a standard RPAS mission of 2 hours, the probability of occurrence of this failure rate has been estimated as 3,888E-06. The Air Data Unit probability of overall Air Data Unit failure occurrence is equal to 1,105E-04 as above calculated; the Air Data Unit signal error on output signal failure mode probability of occurrence level is equal to 0,0352 (3,888E-06/1,105E-04), that is C (Occasional)
- The probability of occurrence level of Air Data Unit loss of power supply has been estimated as follows: from [52] the battery failure rate is 3,9453 failures per million hours; considering that on a rotor wing RPAS the power supply is made of LiPo batteries, it has been supposed that the loss of power supply rate can be assimilated to the battery failure rate. This value, applicable for ground based mechanical systems and in any case not for RPAS has been re-sized according to corrective factor equal to 29,324 (2,17/0,074) from [58] (figure 6 and table 3); considering an RPAS standard flight mission of 2 hours, the probability of Air Data Unit loss of power supply has been estimated as 2,3E-04. The Air Data Unit probability of overall Air Data Unit failure occurrence is equal to 1,105E-04 as above calculated; the Air Data Unit signal error on output signal failure mode probability of occurrence level is equal to 2,094 (2,3E-04/1,105E-04), that is A (Frequent)
- The probability of occurrence level of Air Data Unit calibration error has been estimated as follows: the related failure rate is $\lambda_p = (C1 \times \pi_T +$

C2× π_E) × π_E × π_L = (0,24 × 0,10 + 0,019 × 8) × 0,25 × 2,0 = 0,088 failure per million hours ([54], including this failure mode within those due to computational devices/microprocessors failure); this datum has been corrected according to [58] (corrective factor equal to 22,095 (2/0,105) from figure 6 and table 3); considering a standard RPAS mission of 2 hours, the probability of occurrence of this failure rate has been estimated as 3,888E-06. The Air Data Unit probability of overall Air Data Unit failure occurrence is equal to 1,105E-04 as above calculated; the Air Data Unit signal error on output signal failure mode probability of occurrence level is equal to 0,0352 (3,888E-06/1,105E-04), that is C (Occasional)

The degradation or loss of Air Data Unit leads loss of the RPAS barometric altitude and airspeed control, potentially leading to the system (RPA) loss. Therefore the severity of the consequences of the Air Data Unit failure modes has been classified as 'Catastrophic'.

No means of detection of the above mentioned failure modes when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of Air Data Unit failure is 'High' (Table 34).

The Flight Subsystem/Flight Control Subsystem

The RPAS Flight Control Subsystem manages the flight command signals sent by the remote pilot to control the RPA.

A rotor wing RPAS Flight Control Subsystem is composed of the Autopilot and the 'Detect and Avoid' DAA subsystems (Figure 31).

The failure modes of the Autopilot are hardware failures like failure of weak joints [78] caused by over temperature, lack of power supply, software error due to the lack of pass/fail signals (Table 35):

- The probability of occurrence level of autopilot hardware failure has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of autopilot lack of power supply due to vibrations and damaged wiring has been estimated as D (Remote): for reference this failure mode has been assimilated to item D.5-b of [57] for which the probability of occurrence level has been estimated as 'Medium'/'Occasional' (Table 79)
- The probability of occurrence level of autopilot software failure has been estimated as D (Remote) (Table 79)

The degradation or loss of the Autopilot leads to the loss of RPA control and ultimately it leads to the system (RPA) loss. Therefore the severity of the consequences of the Autopilot failure modes has been classified as 'Catastrophic'.

The Autopilot failure modes are expected to be detected in flight, through visual or audible warning devices for the remote pilot.

The resulting criticality level of Autopilot failure modes is 'Medium' (Table 36).

The failure modes of the 'Detect and Avoid' (DAA) subsystem are: loss of ADS-B signal, EGNOS receiver failure and altimeter sensor failure:

- The probability of occurrence level of loss of ADS-B signal has been estimated as C (Occasional) (as for item NSS4r of the FMECA analysis reported in Appendix A) (Table 79)
- The probability of occurrence level of EGNOS receiver failure has been estimated as A (Frequent) (as for item NSS3a of the FMECA analysis reported in Appendix A) (Table 79)
- The probability of occurrence level of altimeter sensor failure has been estimated as E (Extremely unlikely) (as for item NSS4g of the FMECA analysis reported in Appendix A) (Table 79)

The degradation or loss of the DAA enhances the probability of missed detection in flight of other manned/unmanned intruders on the RPA mission track thus causing a higher probability of mid-air collision risk and ultimately of system (RPA) loss. Therefore the severity of the consequences of the DAA failure modes has been classified as 'Catastrophic'.

It is expected that the DAA failure modes can be detected in flight through visual or audible warnings addressed to the remote pilot.

The resulting criticality level of DAA failure modes is 'Low' and 'High' in accordance with the estimated probability of occurrence levels (Table 36).

The Flight Subsystem/Emergency Flight Subsystem

The RPAS Emergency Flight subsystem terminates the flight in case of emergency loss of control of the RPA thus providing a basic mitigation against the fact that the human pilot is not on board the aerial platform.

In case of loss of control, the flight of a rotor wing RPAS can be terminated cutting-off the power supply to the electric engines (use of the 'Flight Termination System' (FTS)) or activating the recovery parachute for a smoother falling down (if emergency occurs over urban/congested areas, for example) (Figure 31).

The FTS Emergency subsystem failure modes are (Table 37): loss of dedicated radio link, lack of functionality and unlawful interference on the dedicated radio link:

- The probability of occurrence level of the FTS loss of dedicated radio link failure has been estimated as C (Occasional) (Table 79)

- The probability of occurrence level of the FTS lack of functionality has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the FTS unlawful interference has been estimated as B (Reasonably probable) due to the current lack of active defences against cyber threats (Table 79)

The FTS Emergency Subsystem failure modes are expected to be detected in flight, through visual or audible warning devices for the remote pilot.

The resulting criticality level of the FTS Emergency Subsystem failure modes is 'High' and 'Medium' according to the above reported estimated failure modes probability of occurrence levels (Table 38).

The Recovery Parachute Emergency subsystem failure modes are (Table 37): loss of dedicated radio link, lack of functionality and unlawful interference on the dedicated radio link:

- The probability of occurrence level of the Recovery Parachute loss of dedicated radio link failure has been estimated as C (Occasional) (Table 79)
- The probability of occurrence level of the Recovery Parachute lack of functionality has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the Recovery Parachute unlawful interference has been estimated as B (Reasonably probable) due to the current lack of active defences against cyber threats (Table 79)

The Recovery Parachute Emergency Subsystem failure modes are expected to be detected in flight, through visual or audible warning devices for the remote pilot.

The resulting criticality level of the Recovery Parachute Emergency Subsystem failure modes is 'High' and 'Medium' according to the above reported estimated failure modes probability of occurrence levels (Table 38).

The Mission Control Subsystem

The RPAS Mission Control Subsystem manages the flight data (waypoints coordinates) and the flight plan.

It mainly consists of the mission data storage unit (Table 31) which failure modes are: the loss of mission data/software error and the physical unit damage/degradation (Table 39):

- The probability of occurrence level of the loss of mission data/software error has been estimated as C (Occasional) (Table 79)
- The probability of occurrence level of the mission data unit hardware failure/physical degradation has been estimated as C (Occasional) (Table 79)

The consequences of loss of mission data is mission degradation; therefore the severity of the consequences has been estimated as 'Marginal'.

The Mission Control subsystem failure modes are expected to be detected by the remote pilot observing the navigation displays, therefore the detection methods related to these failure modes have been ranked as 'Other methods' (Table 39).

The criticality of these failure modes is 'Low' (Table 40).

The Mission Payload Sensors Subsystem

The RPAS Mission Payload Sensors Subsystem is the whole of photo/video cameras and other specific sensors installed on board the RPA according to the technical purpose of the mission to record the data for which the specific commercial flight operation is performed: for example it can be an infrared photo/video camera to observe the thermal features of a building (Table 31).

The failure modes of payload sensors are defined according to the considered specific device (Table 41):

- The probability of occurrence level of the payload failure modes has been assessed as D (Remote) (Table 41); for reference these failure mode have been assimilated to item D.13-a/D13-b of [57] for which the probability of occurrence level has been estimated as 'Low' (Table 79)

The main consequences are loss of recorded data with no impact for the safety of the aircraft or degradation of the mission; therefore the severity of the consequences of the considered failure modes has been ranked as 'Minor'.

These failure mode are expected to be detected through automatic sensing devices.

The criticality of the Mission Payload failure modes is 'Low' (Table 42).

The Communication Subsystem

The RPAS Communication Subsystem allows to transmit command signals from ground to the aircraft and to receive telemetry data from the RPA. It consists of the transmitting/receiving antenna on board the RPA (Figure 31).

The Communication Subsystem failure modes are: failure of the transmitting antenna, the transmitter antenna fade; the receiver antenna failure and the receiver antenna fade (Table 43) [79]:

- The probability of occurrence level of the transmitting antenna failure has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of transmitting antenna fade has been estimated as C (Occasional ([57], with reference to item D.7-d

for which the probability of occurrence level has been estimated as 'Medium'/'Occasional' (Table 79)

The severity of consequences of RPAS transmitting antenna failure modes can potentially lead to the loss of the RPAS system; therefore it has been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure modes when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The criticality of this failure mode is 'Medium' and 'Low' in accordance with the estimated probability of occurrence levels (Table 44).

With reference to the receiving antenna [79].

- The probability of occurrence level of the receiving antenna failure has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of receiving antenna fade has been estimated as C (Occasional ([57], with reference to item D.7-d for which the probability of occurrence level has been estimated as 'Medium'/'Occasional' (Table 79)

The severity of consequences of RPAS receiving antenna failure modes can potentially lead to the loss of the RPAS system; therefore it has been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure modes when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The criticality of this failure mode is 'Medium' and 'Low' in accordance with the estimated probability of occurrence levels (Table 44).

The Structures Subsystem

The RPA Structural Subsystem has not been analysed using the FMECA methodology because this methodology is not recommended in literature to investigate structures failure modes.

Nevertheless, it is here highlighted that structural integrity shall be demonstrated and continuously maintained for the RPA airworthiness [39].

The fixed wing airborne segment

The fixed wing airborne segment is composed of the following subsystems (Figure 33):

- Propulsion Subsystem powered by a combustion jet engine or by a propeller engine
- Fuel Subsystem

- Power Subsystem
- Electrical Subsystem
- Flight Subsystem, subdivided into:
    - Navigation Subsystem
    - Air Data Subsystem
    - Flight Control Subsystem (with servo units actuators and flight surfaces)
    - Emergency Flight Subsystem
- Mission Data Subsystem
- Payload Data Subsystem
- Communication Subsystem
- Structures (with landing gear)

The FMECA analysis related to the above mentioned subsystems is hereafter described with reference to the typical elements of fixed wing RPAS airborne segment only: that is Propulsion Subsystem, Fuel Subsystem, Power Subsystem and Flight Control Subsystem. The FMECA analysis of equipment in common with rotor wing RPAS has not been duplicated.

The Propulsion Subsystem

The fixed wing RPAS Propulsion Subsystem can be of jet (jet engine with 'Engine Control Unit' (ECU)) or propeller type (engine with 'Engine Control Unit' (ECU) and the propeller).

The jet combustion engine consists of the engine and the 'Engine Control Unit' (ECU) (Figure 33).

The engine control unit failure modes can be (Table 48) [80]: software error (during software/firmware upgrade, for example), mechanical failure, loss of on board computer or carburetor failure:

- The probability of occurrence level of ECU software error has been estimated as D (Remote) [80] (Table 79)
- The probability of occurrence level of ECU mechanical failure has been estimated as B (Reasonably Probable) [80] (solving the 'OR' operator of the FTA reported in figure 5) (Table 79)
- The probability of occurrence level of on board computer has been estimated as E [80] (Table 79)
- The probability of occurrence level of carburetor failure has been estimated as C (Occasional) [80] (Table 79)

The ECU failure brings to the RPAS engines control loss and ultimately to the system (RPA) loss, therefore the severity of the consequences of the ECU failure modes has been classified as 'Catastrophic'.

No means of detection of the above mentioned failure modes when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of combustion jet engine ECU failure modes is 'High', 'Moderate' and 'Low' according to the failure modes estimated probability of occurrence (Table 49).

The jet combustion engine failure modes are (Table 48) [80]: engine control system failure, engine mechanical failure, engine fire, use of improper fuel, short circuit. A numerical value, has been associated to probability of occurrence level of single events from [80] to solve the above mentioned FTA. Such numerical level have been defined as average values from Military Standard 1629 Revision A guidelines for qualitative estimation of probability of occurrence levels (Table 10).

Table 10 – Numerical values associated to MIL-STD-1629 Revision A qualitative probability of occurrence level

A	Frequent	> 0,20 of the overall probability of failure during the item operating time interval	P > 2,0E-01
B	Reasonably probable	> 0,10 and < 0,20 of the overall probability of failure during the item operating time interval	P = 1,5E-01
C	Occasional	> 0,01 and < 0,10 of the overall probability of failure during the item operating time interval	P = 5,5E-02
D	Remote	> 0,001 and < 0,01 of the overall probability of failure during the item operating time interval	P = 5,5E-03
E	Extremely unlikely	< 0,001 of the overall probability of failure during the item operating time interval	P < 1,0E-01

- The probability of occurrence level of engine control system failure has been estimated as C (Occasional) [80] (solving the 'OR' Boolean operator of figure 6) (Table 79)
- The probability of occurrence level of engine mechanical failure has been estimated as A (Frequent) [80] (solving the Fault Tree of figure 5) (Table 79)
- The probability of occurrence level of engine fire has been estimated as D (Remote) [80] (Table 79)
- The probability of occurrence level of use of improper fuel has been estimated as D (Occasional) [80] (Table 79)

The loss of engine on fixed RPAS brings to the loss of control of the system and ultimately loss of (RPA) system: for this reason the severity of consequences of these failure modes has been classified as 'Catastrophic'.

It is expected that there are no ways to detect the engine failure modes when the aircraft is in flight except for the ECU failure and the engine fire failure modes for which it can be expected to have proper visual or audible warning devices. The resulting criticality level of combustion jet engine failure modes is 'High', 'Moderate' and 'Low' according to the failure modes estimated probability of occurrence levels (Table 49).

The combustion engine with propeller consists of the engine, the 'Engine Control Unit' (ECU) and the propeller.

The combustion engine and ECU failure modes are the same as for the jet engine. The propeller failure modes can be: propeller structural failure, propeller connection failure and abrupt stop of the propeller (Table 50):

- The probability of occurrence level of the propeller structural failure has been estimated as E (Extremely unlikely) [80] (Table 79)
- The probability of occurrence level of the propeller connection failure has been ranked as D (Remote) [80] (Table 79)
- The probability of occurrence level of the abrupt stop of the propeller has been estimated as E (Extremely unlikely) [80] (Table 79)

The loss of the propeller brings the loss of thrust, lift and ultimately the loss of the (RPA) system, therefore the severity of consequences of the related failure modes has been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure modes when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of propeller jet engine ECU and engine failure modes is 'High', 'Moderate' and 'Low' according to the failure modes estimated probability of occurrence levels (Table 51). The resulting criticality level of the propeller failure modes is 'Low' (Table 51).

The Fuel Subsystem

The fixed wing RPAS Fuel Subsystem consists of the fuel tanks, the pumps to pressurize the fuel and the pipelines to transport the fuel to the engines (Figure 33)

The fuel tank can be mainly affected by a structural failure (Table 52):

- The probability of occurrence level of fuel tank structural failure has been estimated as D (Remote) (Table 79)

The consequences of this failure mode ranges from the loss of the propulsion system until the loss of the (RPA) system; therefore this failure mode has been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of this failure is 'Low' (Table 53) due to the estimated probability of occurrence.

The fuel pump can be affected by mechanical failures (Table 52):

- The probability of occurrence level pump mechanical failures has been estimated as D (Remote) (Table 79)

The consequences of this failure mode ranges from the loss of the propulsion subsystem until the loss of the (RPA) system; therefore this failure mode has been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of this failure is 'Low' (Table 53) due to the estimated probability of occurrence.

The loss of the fuel pump is expected to be detected in flight using an automatic sensing device. The resulting criticality level of this failure mode is 'Moderate' (48).

The fuel pipelines can be mainly affected by structural failures (Table 52):

- The probability of occurrence level of fuel pipelines structural failures has been estimated as E (Extremely unlikely) (Table 79)

The consequences of this failure mode ranges from the loss of the propulsion subsystem until the loss of the aircraft system; therefore this failure mode has been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of this failure is 'Low' (Table 53) due to the estimated probability of occurrence.

The Power Generation Subsystem

The fixed wing RPAS Power Generation Subsystem consists of the alternator to generate the alternate current on board the aircraft, the rectifier unit to convert the alternate current into direct current and the emergency battery as power backup equipment (Figure 33).

The alternator failure mode is mechanical failures due to brushes/diodes failure occurrence (Table 54):

- The probability of occurrence level of the alternator mechanical failure has been estimated as C (Occasional) (Table 79)

The consequences of this failure is the loss of the (RPA) system; therefore this failure mode has been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of this failure mode is 'High' (Table 55).

The rectifier failure modes are overheating and chemical failure (Table 54):

- The probability of occurrence level of overheating has been estimated as C (Occasional) (Table 79)
- The probability of occurrence level of the chemical failure has been estimated as C (Occasional) (Table 79)

The consequences of these failure modes bring to the loss of the (RPA) system; therefore the consequences of each one of these failure mode have been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of this failure mode is 'High' (Table 55).

The emergency battery failure modes are mechanical failure, thermal failure, chemical failure, electrical failure (Table 54):

- The probability of occurrence level of the mechanical failure mode has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the thermal failure mode has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the chemical failure mode has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the electrical failure mode has been estimated as D (Remote) (Table 79)

The consequences of these failure modes bring to the loss of the (RPA) system; therefore the consequences of each one of these failure mode have been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of this failure mode is 'Medium (Table 55).

The Flight Subsystem/Air Data Subsystem

The RPAS Air Data Subsystem comprehends the pitot air probe to measure absolute and relative air pressure and the Air Data Unit equipment to measure airspeed and barometric altitude flight parameters (Figure 33).

The main failure mode of the air probe is clogging [57] due to ice or dust (Table 56):

- The probability of occurrence level of air probe clogging has been estimated as B (Reasonably Probable) from [57] with reference to item D.8-a for a fixed wing RPA, for which this failure mode probability of occurrence level has been ranked as 'High' (Table 79)

The clogging of the air probe leads to the loss of the RPAS barometric altitude and airspeed control, and potentially to the (RPA) system loss. Therefore, the severity of the consequences of this failure mode has been classified as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of Air Data Unit failure is 'High' (Table 57).

The failure modes of the Data Unit are [53]: incorrect signal, loss of signal, signal error along the transmission line, error on output signal, loss of power supply, calibration error (Table 56). The evaluations are the same as for the items ADSS1a÷f of previously considered for rotor wing airborne segments (Table 79).

The degradation or loss of Air Data Unit leads to the loss of the RPAS barometric altitude and airspeed control, potentially leading to the (RPA) system loss. Therefore the severity of the consequences of the Air Data Unit failure modes has been classified as 'Catastrophic' for fixed wing airborne segments too.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of Air Data Unit failure is 'High' and 'Medium' according to the estimated probability of occurrence levels (Table 57).

The Flight Subsystem/Flight Control Subsystem

The fixed wing RPAS Flight Control Subsystem manages the flight command signals sent by the remote pilot and transmit them to the flight surfaces to manoeuvring to reach the expected flight attitude.

A fixed wing RPAS Flight Control Subsystem is composed of the Autopilot, the servo-actuator units to command the flight surfaces and the 'Detect and Avoid' DAA subsystem (Figure 33).

The Autopilot and DAA have been already treated for the rotor wing RPAS; the servo-actuator units subsystem failure modes are hereinafter detailed.

The servo-units subsystem failure modes are (Table 58): bias, stuck surface, handover, floating surface, oscillatory modes, increased dead band/stiction, structural damage:

- The probability of occurrence level of servo-units bias has been estimated as C (Occasional) [81] (where the probability of occurrence level of the considered failure mode has been ranked as 'Medium') (Table 79)
- The probability of occurrence level of servo-units stuck-surface has been estimated as D (Remote) [81] (where the probability of occurrence level of the considered failure mode has been ranked as 'Low') (Table 79)
- The probability of occurrence level of servo-units hardover has been estimated as D (Remote) [81] (where the probability of occurrence level of the considered failure mode has been ranked as 'Low') (Table 79)
- The probability of occurrence level of servo-units floating surface has been estimated as C (Occasional) [81] (where the probability of occurrence level of the considered failure mode has been ranked as 'Medium') (Table 79)
- The probability of occurrence level of servo-units oscillatory modes has been estimated as D (Remote) [81] (where the probability of occurrence level of the considered failure mode has been ranked as 'Low') (Table 79)
- The probability of occurrence level of servo-units increased dead band/stiction has been estimated as D (Remote) [81] (where the probability of occurrence level of the considered failure mode has been ranked as 'Low') (Table 79)
- The probability of occurrence level of servo-units structural damage has been estimated as E (Extremely unlikely) (Table 79)

The severity of consequences of the above mentioned failure modes has been ranked as 'Catastrophic' because each failure mode brings to the loss of aircraft control and ultimately to the loss of the (RPA) system.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality is 'High', 'Moderate' and 'Low' according to the failure modes estimated probability of occurrence levels (Table 59).

The Structures Subsystem

The RPA Structural Subsystem has not been analysed using the FMECA methodology because from literature this methodology is not recommended to investigate structures failure modes.

Nevertheless, it is here highlighted that structural integrity shall be demonstrated and continuously maintained for the RPA airworthiness [39].

The rotor wing hybrid airborne segment

The fixed wing hybrid airborne segment is composed of the following subsystems (Figure 35):

- Propulsion Subsystem powered by electric motors fed by fuel cells and by the LiPo battery stack (as backup system)
- Hydrogen fuel Subsystem
- Power Subsystem
- Electrical Subsystem
- Flight Subsystem, subdivided into:
    - Navigation Subsystem
    - Air Data Subsystem
    - Flight Control Subsystem
    - Emergency Flight Subsystem
- Mission Data Subsystem
- Payload Data Subsystem
- Communication Subsystem
- Structures

The Propulsion Subsystem

The hybrid RPAS Propulsion Subsystem consists of the hydrogen fuel cell powered line and of the LiPo batteries powered line. The fuel cell powered line is composed of the hydrogen tank, the fuel cell and the DC to DC converter which provides the electrical loads with the current at the correct values of voltage and intensity; the LiPo powered line consists of the LiPo battery stack and the DC to DC converter; the DC to DC power bus distributes the produced electrical power to all the RPA electrical loads (Figure 35).

The hydrogen tank failure modes are structural damage and leakage (Table 63):

- The probability of occurrence level of the structural damage failure mode has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the leakage failure mode has been estimated as D (Remote) (Table 79)

The consequences of these failure modes can be fire on board the RPA due to the presence of hydrogen and ultimately the system (hybrid RPA) loss; therefore the severity of consequences of these failure modes has been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level of this failure mode is 'Medium' (Table 64) according to the estimated value of probability of occurrence level.

The fuel cell failure modes can be fuel cell membrane drying and water condensation inhibition [82] (Table 63):

- The probability of occurrence level of the fuel cell membrane drying has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the fuel cell water condensation inhibition has been estimated as D (Remote) (Table 79)

The consequences of these failure mode ranges from the loss of the fuel cell functionality to the loss of propulsion until the loss of the aircraft system; therefore this failure mode has been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level associated to these failure modes is 'Medium' according to the estimated value of probability of occurrence level (Table 64).

The hydrogen can cause fire in particular due to casual presence of explosive gases like chlorine [83] (Table 63):

- The probability of occurrence level of hydrogen fire has been estimated as C (Occasional) (Table 79)

The consequences of hydrogen fire are the (hybrid RPA) system loss; therefore the severity of consequences of hydrogen fire has been ranked as 'Catastrophic'.

It is expected that hydrogen fire can be detected in flight through audible or visual warnings.

The resulting criticality level of this failure mode is 'High' (Table 64) according to the estimated value of probability of occurrence level.

The LiPo batteries failure modes analysis is the same as for rotor wing RPAS power subsystem (Table 63).

The DC power bus failure modes can be electrical failure due to overvoltage or under voltage (Table 63):

- The probability of occurrence level has been estimated as C (Occasional) (Table 79)

The DC power Bus failure potentially leads to the lack of supplied power to the RPA electrical loads, therefore the severity of consequences of this failure mode has been classified as 'Catastrophic' potentially leading to the loss of the (hybrid RPA) system.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level associated to these failure modes is 'High' (Table 64) according to the estimated value of probability of occurrence level.

The DC to DC converter failure modes can be due to the failure of its internal components like capacitors or transistors (Table 63):

- The probability of occurrence level of DC to DC converter internal components failure has been estimated as C (Occasional) (Table 79)

The failure of the DC to DC converter leads to the lack of proper management of electrical current voltage to be provided to the RPA electrical loads. This fault scenario can potentially lead to the degradation of functionality of all other hybrid RPA electrical powered equipment and to the system (hybrid RPA) loss. Therefore, the severity of the consequences of these failure modes has been classified as 'Catastrophic'.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level associated to these failure modes is 'High' (Table 64) according to the estimated value of probability of occurrence level.

The Command and Control (C2) link

The Command and Control (C2) link is the radio link that allows the remote pilot to command and control/manage the RPA from ground (Figure 37).

The failure modes are signal degradation and signal loss (Table 65):

- The probability of occurrence level of the radio link signal degradation has been estimated as D (Remote) (Table 79)

The severity of this failure mode consequences has been estimated as 'Catastrophic' potentially leading to the loss of the (RPA) system.

Visual or audible warning devices are expected to be used as detection methods. The resulting criticality level is 'Medium' according to the estimated value of probability of occurrence level (Table 65).

- The probability of occurrence level of the radio link signal loss has been estimated as D (Remote) (Table 79)

The severity of this failure mode consequences has been estimated as 'Catastrophic' potentially leading to the loss of the (RPA) system.

Visual or audible warning devices are expected to be used as detection methods. The resulting criticality level is 'Medium' according to the estimated value of probability of occurrence level (Table 65).

The ground segment

The RPAS ground segment is composed of the following subsystems (Figure 38):

- The GCS Power Generation Subsystem
- The GCS Start-Up subsystem
- The GCS HMI Subsystem
- The GCS Flight Termination HMI Subsystem
- The GCS Payload Sensors HMI Subsystem
- The GCS Communication Subsystem

The Ground Control Station Power Generation Subsystem

For a more complex RPAS, the GCS Power Generation Subsystem mainly consists of a generator and ground emergency battery (Figure 38); for simpler RPAS it mainly consists of the battery which supplies the hand-held portable radio controller. For a more comprehensive analysis (applicable for civil RPAS capable of certified operations, for example), the more complex case is hereinafter debated.

The generator failure modes are missed start and sudden stop (Table 67):

- The probability of occurrence level of the missed start failure mode has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the sudden stop failure mode has been estimated as D (Remote) (Table 79)

The severity of consequences of these failure modes has been estimated as 'Catastrophic' because they can lead to the loss of GCS functionality, the loss of control of the airborne segment and ultimately to the loss of the airborne segment (RPA).

It is expected that audible or visual warnings can be used as failure detection methods.

The resulting criticality level is 'Low' (Table 68).

The ground emergency battery failure modes are low charge and lack of charge (Table 67); considering the emergency battery as a backup system, the following is expected:

- The probability of occurrence level of low charge failure mode has been estimated as E (Extremely unlikely) (Table 79)
- The probability of occurrence level of lack of charge failure mode has been estimated as E (Extremely unlikely) (Table 79)

The severity of consequences of these failure modes has been estimated as 'Catastrophic' because they can lead to the loss of GCS functionality, the loss of control of the airborne segment and ultimately to the loss of the airborne segment (RPA).

It is expected that audible or visual warnings can be used as failure detection methods.

The resulting criticality level is 'Low' (Table 68).

The Ground Control Station Start Up Subsystem

The GCS Start Up Subsystem mainly consists of the master switch (Figure 38) to power on the ground control segment (both for more complex and simpler RPAS).

The GCS Start Up Subsystem failure mode is missed start (Table 67):

- The probability of occurrence level of this failure mode has been estimated as E (Extremely unlikely) (Table 79)

The severity of consequences of these failure modes has been estimated as 'Minor' due to the impossibility to start and perform the aerial mission if this failure occurs.

No means of detection of the above mentioned failure have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level associated to these failure modes is 'Low' Table 70.

The Ground Control Station Human Machine Interface Subsystem

The GCS Human Machine Interface (Figure 38) consists (both for more complex and simpler RPAS) of: the control (usually a joystick) to command the RPA attitude variation along the longitudinal and directional axes, the control

(pedals for more complex RPAS or level switches for simpler RPAS) to command the RPA attitude variations on the lateral direction and the throttle to manage the thrust regime on board the RPA; the autopilot modes selection switch to choose the most proper RPA autopilot for each stage of flight; the GCS management software that receives the command signals generated by the remote pilot every time he/she operates an HMI control, converts them into electromagnetic signals according to given protocols and convey them towards the GCS communication subsystem to send them to the RPA via the radio uplink channel; the displays fed by telemetry data to monitor the status of on board RPA functional subsystems (Table 71).

The GCS joystick failure modes are (Table 71): lack of calibration, software error, missed start and sudden stop:

- The probability of occurrence level of the joystick hardware failure has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the joystick software error has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the joystick missed start has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the joystick sudden stop has been estimated as D (Remote) (Table 79)

The severity of consequences of these failure modes has been estimated as 'Catastrophic' because they can lead to the loss of longitudinal and lateral control of the airborne segment and ultimately to the loss of the airborne segment (RPA).

No means of detection of the above mentioned failure mode when the RPA is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level is 'Medium' (Table 72).

The GCS pedals failure modes are (Table 71): lack of calibration, software error, missed start and sudden stop:

- The probability of occurrence level of the pedals hardware failure has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the pedals software error has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the pedals missed start has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the pedals sudden stop has been estimated as D (Remote) (Table 79)

The severity of consequences of these failure modes has been estimated as 'Catastrophic' because they can lead to the loss of directional control of the airborne segment and ultimately to the loss of the airborne segment (RPA).

No means of detection of the above mentioned failure mode when the RPA is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level is 'Medium' (Table 72).

The GCS throttle failure modes are (Table 71): lack of calibration, software error, missed start and sudden stop:

- The probability of occurrence level of the throttle hardware failure has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the throttle software error has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the throttle missed start has been estimated as has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the throttle sudden stop has been estimated as D (Remote) (Table 79)

The severity of consequences of these failure modes has been estimated as 'Catastrophic' because they can lead to the loss of trust control of the airborne segment and ultimately to the loss of the airborne segment (RPA).

No means of detection of the above mentioned failure mode when the RPA is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level is 'Medium' (Table 72).

The Autopilot switch failure modes are (Table 71): mechanical failure, electrical failure and software error:

- The probability of occurrence level of the mechanical failure has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the electrical failure has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the autopilot switch signal error has been estimated as D (Remote) (Table 79)

The severity of consequences of these failure modes has been estimated as 'Catastrophic' because they can lead to the loss of control of the airborne segment (RPA) and ultimately to the loss of the airborne segment (RPA)

No means of detection of the above mentioned failure mode when the RPA is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level is 'Medium' (Table 72).

The GCS management software failure mode is software error (Table 71):

- The probability of occurrence level has been estimated as E (Extremely Unlikely) (Table 79)

The severity of consequences of these failure modes has been estimated as 'Catastrophic' because they can lead to the loss of control of the airborne segment (RPA) and ultimately to the loss of the airborne segment (RPA)

No means of detection of the above mentioned failure mode when the RPA is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level is 'Medium' (Table 72).

The GCS displays failure modes are (Table 71): electrical failure and software error:

- The probability of occurrence level of lack of power supply has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of the GCS displays software error has been estimated as D (Remote) (Table 79)

The severity of consequences of these failure modes has been estimated as 'Catastrophic' because they can lead to the loss of GCS monitoring capability of the RPA, the loss of control of the RPA and ultimately to the loss of the airborne segment (RPA).

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level is 'Medium (Table 72).

The Ground Control Station Emergency Flight Termination HMI Subsystem

The GCS Flight Termination HMI Subsystem consists of the FTS command switch and the Recovery Parachute deployment command switch (Figure 38).

The FTS command switch failure modes is the mechanical failure (Table 73):

- The probability of occurrence level of FTS command switch mechanical failure has been estimated as E (Extremely Unlikely) (Table 79)

The severity of consequences of this failure mode has been estimated as 'Catastrophic' because it leads to the loss of the airborne segment due to emergency on board failures.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level is 'Low' (Table 74).

The Emergency Parachute command switch failure modes is the mechanical failure (Table 73):

- The probability of occurrence level of Emergency Parachute switch mechanical failure has been estimated as E (Extremely Unlikely) (Table 79)

The severity of consequences of this failure mode has been estimated as 'Catastrophic' because it leads to the loss of the airborne segment due to emergency on board failures.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level is 'Low' (Table 74).

The Ground Control Station Payload Sensors HMI Switch Subsystem

The Ground Control Station Payload Sensors HMI Subsystem is the whole of the controls to manage the RPA on board payload sensors from ground. The payload sensors can be: photo/video cameras and/or other kinds of sensors according to the commercial mission aim (Figure 38Figure 38 – Ground Control Station [80]).

The photo/video cameras command switch failure mode is mechanical failure (Table 75):

- The probability of occurrence level of mechanical failure has been estimated as D (Remote) (Table 79)

The severity of consequences of this failure mode has been estimated as 'Minor' because it does not imply any safety related consequence on the RPAS.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level is 'Low' (Table 76).

The other payload command switch failure mode is mechanical failure (Table 75):

- The probability of occurrence level of mechanical failure has been estimated as D (Remote) (Table 79)

The severity of consequences of this failure mode has been estimated as 'Minor' because it does not imply any safety related consequence on the RPAS.

No means of detection of the above mentioned failure mode when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The resulting criticality level is 'Low' (Table 76).

The Ground Control Station Communication Subsystem

The GCS Communication Subsystem consists of the Transmitting Antenna, the Receiving Antenna and the ATC channel (Figure 38).

The GCS Communication Transmitting Subsystem failure modes are: transmitting antenna lack of signal processing and antenna fade (Table 77) [57]:

- The probability of occurrence level of transmitting lack of signal processing has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of transmitting antenna fade has been estimated as C (Occasional ([57], with reference to item D.7-d for which the probability of occurrence has been estimated as 'Medium'/'Occasional' (Table 79)

The severity of consequences of RPAS transmitting antenna failure modes can potentially lead to the loss of the RPA control and ultimately to the loss of the RPA system; therefore it has been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure modes when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The criticality of this failure mode is 'Medium' and 'Low' in accordance with the estimated probability of occurrence levels (Table 78).

The GCS Communication Receiving Subsystem failure modes are: receiving antenna lack of signal processing and antenna fade (Table 77) [57]:

- The probability of occurrence level of receiving lack of signal processing has been estimated as D (Remote) (Table 79)
- The probability of occurrence level of receiving antenna fade has been estimated as C (Occasional ([57], with reference to item D.7-d for which the probability of occurrence has been estimated as 'Medium'/'Occasional' (Table 79)

The severity of consequences of RPAS transmitting antenna failure modes can potentially lead to the loss of the RPA control and ultimately to the loss of the RPA system; therefore it has been ranked as 'Catastrophic'.

No means of detection of the above mentioned failure modes when the aircraft is in flight have been identified in literature. Therefore, the detection method has been classified as 'None'.

The criticality of this failure mode is 'Medium' and 'Low' in accordance with the estimated probability of occurrence levels (Table 78).

The failure mode of the ATC channel is the lack of communication with the ATC (Table 77):

- The probability of occurrence level of this failure mode has been estimated as C (Occasional) (Table 79)

The severity of the consequences has been ranked as 'Catastrophic' due to the possible loss of the aircraft (Table 79)

This failure mode is expected to be detected through visual or audible warning devices.

The criticality level of this failure mode is 'High' (Table 78).

FMECA analysis: pros and cons

The FMECA analysis has been performed to systematically investigate the possible single failure modes (that is simple events of failure not furtherly decomposable in other simpler events) of the components of each main segments of RPAS (the airborne segment, the radio link and the ground segment), that could abruptly occur during flight operations in the civil airspace; each failure can have impact on the RPAS itself and/or on third parties according to the operative scenario. This aspect is further investigated forward in this work in the safety hazards analysis.

The performed analysis has provided a wide basis to identify direct or indirect events that can cause the RPAS practical/operating drift from its baseline towards an incident/accident. The analysis results allow to confirm the benefit of the FMECA methodology for RPAS too as for manned aircraft as guideline for better addressed design choices.

The limitations of the performed analysis are summed up hereinafter:

- A qualitative analysis has been intentionally rather than a quantitative one because of the consistent lack of reliability data on RPAS due to the relatively recency of this technology
- The analysis has been intentionally performed on a generic theoretical RPAS functional architecture to lay down the basis for a more comprehensive analysis and because the RPAS technology is a quickly changing disruptive technology
- The analysis purpose has not been the evaluation of reliability of current given RPAS commercial equipment but looking forward the

safety hazard risk analysis on the system 'RPAS integrated in the controlled airspace' focus of this research work

- In general, the reliability of an RPAS equipment is not expected to be equal to the reliability of the same type of equipment designed to be installed on a civil aircraft mainly for the different level of environmental stress caused by strongly different airframe configurations, weight and sizes (much lower than manned aircraft) and altitudes of operation (until operating within urban environment): as initial expectations, a more stressing effect due to vibrations, temperature, humidity, wind gust, dust and debris are expected to more negatively affect RPAS equipment reliability. Proper technical documentation ([52], [53] and [54]) has been consulted to find out indications on corrective factors to be applied. In any case, in accordance with [51], quantitative values of RPAS equipment failure rate can be determined only running dedicated tests on the equipment reproducing the real operative conditions on board the RPAS
- Proper requirements and guidelines on RPAS equipment reliability are needed to be issued by Aviation Authorities for incoming specific category operations
- Proper requirements and guidelines on RPAS safety critical software functionalities are needed to be issued by Aviation Authorities for incoming specific category operations to avoid errors/bugs in the software modules embedded in the following equipment/subsystems: 'Detect and Avoid' (DAA), 'Flight Control Computer' (FCC), 'Flight Termination System' (FTS)
- Proper requirements and guidelines on the systematic performance of reliability tests for collection of RPAS historical reliability data are needed to be issued by Aviation Authorities

Fault Tree Analysis

The Fault Tree Analysis (FTA) is a top-down graphical deductive analysis methodology structured in terms of events. It is used to model faults in terms of failures, anomalies, malfunctions, and human errors. In this work, it has been applied to find out combinantions of FMECA sngle fault events (thus maintaining the direct correlation between the two analyses) potentially leading to a given equipment failure and, from there onwards, untill the complete loss of functionality of the associated RPAS subsystem. Going through the FTA, possbile fault paths can be identfied from initiating events; for any functionality, the initiating events have been chosen among failure modes causes. For each subsystem functionality a fault tree has been implemented; the descending truth tables have been solved combining the 'OR', 'AND' and 'XOR' Boolean operators assigned as deemed necessary to logically represent the expected real functional links among equipment. The failure modes qualitative probability of occurrence levels assigned in the FMECA analysis and combined in the truth

tables have been changed into numerical values (Table 80) (Table 81) following the assumptions of Table 10 and rearranged according to criticality level from those characterized by high criticality to those characterized by low criticality (Table 81). Once solved the truth tables related to intermediate multiple failures, an average value of their probability of occurrence level has been calculated (at the bottom of the related truth table) to give the same weight (without other available information) to each combination of failures that can lead to the partial or total loss of the overall subsystem functionality under analysis. The resulting estimated probability of occurrence level of loss of a given RPAS subsystem functionality has been calculated as a single value (A, B, C, D or E) or a range between two extreme values of an interval ('B → C', for example). Finally, these data have been used as an indication to assess the probability of occurrence the hazards due to a given RPAS subsystem loss of functionality.

Considering the current early stage of definition of RPAS operations in the not segregated airspace and related regulations, the above described approach has been deemed the most proper to be used at the moment. For the same reasons, during the FTA performance, the combinations up to six input variables to the truth tables have been extensively solved only; proper considerations have been introduced to simplify more complex cases (for instance: flight control subsystem FTA for fixed wing aerial segment).

The analysis has been carried on the following the aerial and ground segments subsystem functionalities as already defined for the FMECA analysis; again the fault trees of duplicated aerial segment subsystems (for example passing from rotor wing to fixed wing RPAS) has been avoided.

The FTA analysis has been carried out on the following RPAS subsystems:

- Rotor wing RPAS:
    - Propulsion Subsystem functionality (Figure 40, Table 82, Table 83, Table 84 and Table 85)
    - Power Subsystem functionality (Figure 41, Table 86)
    - Electrical Subsystem functionality (Figure 42, Table 87, Table 88 and Table 89)
    - Navigation Subsystem functionality (Figure 43, Table 90, Table 91, Table 92, Table 93 and Table 94)
    - Air Data Subsystem functionality (Figure 44, Table 95)
    - Flight Control Subsystem functionality (Figure 45, Table 96, Table 97 and Table 98)
    - Emergency Flight Termination Subsystem functionality (Figure 46, Table 99, Table 100 and Table 101)
    - Mission Control Subsystem functionality (Figure 47, Table 102)
    - Payload Sensors Subsystem functionality
    - On Board Communication Subsystem functionality (Figure 48, Table 103, Table 104 and Table 105)
- Fixed wing RPAS:

    - Propulsion with Combustion Engine Subsystem functionality (Figure 49, Table 106, Table 107 and Table 108)
    - Propulsion with Combustion Engine with Propellers Subsystem functionality (Figure 50, Table 110, Table 111, and Table 112)
    - Fuel Subsystem functionality (Figure 51, Table 113)
    - Power Generation Subsystem functionality (Figure 52, Table 117)
    - Air Data Subsystem functionality (Figure 53, Table 118 and Table 119)
    - Flight Control Subsystem functionality (Figure 54, Table 120)
- Hybrid RPAS:
    - Propulsion Subsystem functionality (Figure 55, Table 121, Table 122, Table 123, Table 124 and Table 125)
- Command and Control (C2) Radio Link:
    - Command and Control (C2) Radio Link Subsystem functionality (
    -
    -
    - Figure 56, Table 126)
- Ground Segment:
    - Ground Control Station Start-Up Subsystem functionality (Figure 57, Table 127 and Table 128)
    - Ground Control Station Power Generation Subsystem functionality (Figure 57, Table 129)
    - Ground Control Station HMI Subsystem functionality (Figure 58, Table 130, Table 131, Table 132, Table 133 and Table 134)
    - Ground Control Station Payload Sensors HMI Subsystem functionality
    - Ground Control Station Flight Termination HMI Subsystem functionalityv (Figure 59, Table 135)
    - Ground Control Station Communication Subsystem functionality (Figure 60, Table 136, Table 137 and Table 138)

The FTA analysis has been developed according to the 'Military Handbook 338 Revision B' [84]; the final results have been reported in Appendix B (Table 139).

The human factor model

The hazards caused by human factor in RPAS operations into civil non segregated airspace has been investigated using the SHELL and HFACS models. The mismatches precursors to hazards due to human behaviour with respect to the

surrounding operational environment have been identified using the SHELL model (Table 140). The mismatches have been defined considering as 'liveware' in turn each one of three categories of human actors potentially involved into RPAS operations in the not segregated airspace: the remote pilot, the pilot on board manned aircraft and the ATC controllers. The most comprehensive case has been considered where all of the three above mentioned human roles are involved. The analysis has been performed referring to a typical operational event where this condition can occur: the mid-air conflict between a remotely piloted aircraft and a manned intruder in the airspace under the overview of competent ATC. With reference to the concept of operations described in Figure 6, this can be a typical scenario for a certified category flight operation; without the involvement of the ATC it becomes a possible scenario for specific category RPAS operations.

In addition, the performance of the three above mentioned actors has been analysed according to the HFACS model to find other sources of hazards of interest (Table 141).

The human factor analysis and the results have been reported in Appendix C (Table 142) where a list of selected hazards related to human factor in RPAS operations in the not segregated have been collected with an associated qualitative assessment of the probability of occurrence, as hereinafter reported:

Hazard: ATC Communication error: according to [85], the measured rate of ATC communication error that can cause an accident is equal to 1.10E-07 per ATC communication; the assigned qualitative probability of occurrence of this hazard according to Table 5 [3] is Improbable (D) [85].

Hazard: Collision with natural/man made obstacle when the RPA is flown in manual mode: the collision could be caused by an error due to remote pilot low flight planning or his/her poor practice; the assigned probability of occurrence according to Table 5 [3] is Occasional (B).

Hazard: Confusing, misleading or cluttering of operational documentation, and checklists, etc.: this issue is particularly expected to be more frequent at the beginning of integration of RPAS into the not segregated airspace when a transitory period of adaptation of civil RPAS remote pilot to these well consolidated practices of manned aeronautics can occur; the assigned probability of occurrence according to Table 5 [3] is Frequent (A).

Hazard: Error to manage separations: this issue could be expected to be more frequent at the beginning of integration of RPAS into the not segregated airspace due to ATC adaptation to the new operational scenarios involving RPAS; the assigned probability of occurrence to Table 5 [3] is Occasional (B).

Hazard: Human senses limitation: the assigned probability of occurrence according to Table 5 [3] is Frequent (A) due to the location of the remote pilot not on board he RPA and receiving data from sensors not from his senses [86].

Hazard: Loss of remote pilot situational awareness; the assigned probability of occurrence according to Table 5 [3] is Frequent (A) particularly in complex operations in congested scenario due to the location of the remote pilot not on board he RPA and receiving data from sensors not from his senses [86].

Hazard: Insufficient or inappropriate operational procedure; this issue is expected to more frequent at the beginning of integration of RPAS into the not segregated airspace; the assigned probability of occurrence to Table 5 [3] is Occasional (B).

Hazard: Intentional violation of standard procedures; this issue is expected to be due to malicious act; the assigned probability of occurrence to Table 5 [3] is Remote (C).

Hazard: Lack of specific checklists, operational procedures; this issue is expected to more frequent at the beginning of integration of RPAS into the not segregated airspace when a transitory period of adaptation of civil RPAS (commercial) operators to these well consolidated practices of manned aeronautics can occur; the assigned probability of occurrence to Table 5 [3] is Frequent (A).

Hazard: Low manned aircraft crew resource management in case of mid-air conflict with an RPA; this hazard is expected to more frequent at the beginning of integration of RPAS into the not segregated airspace; the assigned probability of occurrence to Table 5 [3] is Occasional (B).

Hazard: Low remote pilot training; this hazard is expected to more frequent at the beginning of daily routine RPAS commercial operations RPAS into the not segregated airspace; the assigned probability of occurrence to Table 5 [3] is Occasional (B).

Hazard: Performance of no compliant procedures; this hazard is expected to more frequent at the beginning of daily routine RPAS commercial operations RPAS into the not segregated airspace; the assigned probability of occurrence to Table 5 is Occasional (B).

Hazard: Excessive workload due to the presence of RPAS in the airspace; this hazard can occur both to ATC personnel, to RPAS remote pilot and to the pilot of manned aircraft; the assigned probability of occurrence to Table 5 [3] is Occasional (B).

Hazard: Remote pilot reduced physical performance; the assigned probability of occurrence to Table 5 [3] is Remote (C).

Hazard: Remote pilot perceptual errors; the assigned probability of occurrence to Table 5 [3] is Frequent (A) due to the location of the remote pilot not on board he RPA and receiving data from sensors not from his senses [86].

Hazard: RPA flight through adverse weather conditions: the assigned probability of occurrence to Table 5 [3] is Occasional (B) due to the lack of weather RADARs on board the RPA [86].

Hazard: Unintentional violation of operational procedures: the assigned probability of occurrence to Table 5 [3] is Remote (C) due to eventual poor or lack of adequate training.

Hazard: Intentional violation of operational procedures: the assigned probability of occurrence to Table 5 [3] is Occasional (B) due to malicious acts.

Hazard: Unintentional violation of separations: the assigned probability of occurrence to Table 5 [3] is Remote (C) due to eventual poor or lack of adequate training.

Hazard: Intentional violation of separations: the assigned probability of occurrence to Table 5 [3] is Occasional (B) due to malicious acts.

3.2.8 The U-space hazard log

The U-Space hazard log (Table 11) has been draft according to the categorization of RPAS functionalities described in Paragraph 3.2 for the successive safety risk analysis. It reports the hazards expected to occur for specific category RPAS operations performed in the VLL subspace served by the U-Space according to EUROCONTROL/EASA definitions ([25], [26], [27]). The considered RPAS weight is between 25 and 150 kg (light RPAS).

Table 11 – Hazard analysis: U-Space hazard log

Hazard log	
Hazard #	**Definition**
Service: **U-Space**	
RPAS Aviate functionality related hazards	
H01	Loss of abort launch capability
H02	Loss of flight controls
H03	Loss of propulsion
H04	Loss of GCS HMI
H05	Deviation from steady-state (not-accelerating) flight condition
H06	Loss of Emergency Flight Termination System
H07	Loss of 'Return to home function'
RPAS Navigate functionality related hazards	
H08	Loss of mission plan
H09	Loss of GPS signal
H10	Loss of EGNOS signal
H11	Drift with respect to mission plan
RPAS Communicate functionality related hazards	
H12	Loss of uplink channel of the RPAS radio link
H13	Loss of downlink channel of the RPAS radio link
H14	Loss of ADS_B
RPAS hazards avoidance functionality related hazards	
H15	Presence of natural obstacles
H16	Presence of man-made manufactures
H17	Mid-air collision with other aircraft
H18	Loss of DAA capability
H19	No detectability from other airspace users
H20	Cooperative traffic intrusion
H21	Not cooperative traffic intrusion
H22	Missed cooperative traffic tracking
H23	Missed not cooperative traffic tracking
H24	Collision avoidance with cooperative traffic
H25	Collision avoidance with not cooperative traffic
H26	Missed performance of collision avoidance manoeuvre
H27	Missed monitoring of performance of collision avoidance manoeuvring
Hazard log	
Hazard #	**Definition**
Service: **U-Space**	
H28	Missed weather awareness capability
H29	Missed gathering of contingent weather information
H30	Missed avoidance of adverse weather
Cross-cutting functionalities related hazards	

H31	Loss of RPAS subsystems health and status monitoring
H32	Loss of communication while transiting from LOS to BRLOS and vice versa
H33	Unintentional radio link interference

Table 11 – Hazard analysis: U-Space hazard log (Cont'd)

H34	Malicious radio link jamming
H35	Malicious radio link spoofing
Contingencies → Failures related hazards	
H36	Fire
H37	Loss of RPAS autopilot
H38	Loss of electrical power
H39	Loss of inertial platform
H40	Loss of heading indication
H41	Loss of altitude indication
H42	Pressure sensor failure
H43	Misleading altitude indication
H44	Misleading airspeed indication
H45	Misleading indication of the angle of incidence
H46	Stall
Contingencies → Human factor related hazards	
H47	Loss of fuel cell
H48	Remote pilot low training
H49	Non-compliant operational procedures
H50	Remote pilot loss of situational awareness
H51	Human senses limitations
H52	Remote pilot excessive workload
Contingencies → Weather related hazards	
H53	Cloud cover
H54	Fog
H55	Freezing rain
H56	Glare
H57	Haze
H58	Humidity
H59	Ice
H60	Rain
H61	Snow
H62	Solar storms
H63	Temperature
H64	Turbulence
H66	Wind
H66	Lightning strike
H67	Hail
H68	Hurricanes
H69	Volcanic ash

The U-space risk assessment matrix

The risk matrix has been developed on the basis of the hazard log reported Table 11.

Each hazard has been characterized in terms of probability of occurrence and severity of consequences and safety assessment (tolerance, risk range description), mitigation actions and residual risk.

For each hazard:

- The probability of hazard consequence occurrence has been assigned in accordance with the ICAO guidance (ICAO ranking) reported in Table 5 [3] using the following sources of data:

- The probability of occurrence levels estimated for the FMECA analysis (Appendix A)
- The probability of occurrence levels estimated for the FTA analysis (Appendix B)
- The probability of occurrence levels estimated for the human factor analysis (Appendix C)
- Available literature
- Arbitrary assessment if no other matching references were available

  Note: as precized in [3] (Paragraphs 2.13.5 and 2.13.6), hazards shall not be confused with their consequences. In fact they are two distinct items, where the consequence is physically the outcome triggered by the hazard existence. In addition, more and different levels of consequences can be caused by the same hazardous event ranging from an immediate consequence to an ultimate consequence identifiable with an accident. In this work, due to the simplicity of RPAS for civil use and the uncertainty of data available at the moment of the research, a single consequence has been conjectured to be caused by each given hazard and the probability of hazard consequence occurrence has been defined in a qualitative way heavily basing on the above mentioned sources of probability of occurrence level of the related hazard event itself. In other words, due to the above remembered high simplicity of RPAS for civil use, it has been assumed that, as a first approximation, if the hazard occurs, the consequent/accident will occur, so the probability of occurrence of these two events can be assumed to be equal. The same assumption has been used to perform both the safety assessment reported in the U-space risk matrix (Table 143) and the safety assessment reported in the ATM risk matrix (Table 144)

- The severity of consequences and the safety assessment parameters, have been ranked or defined according to the content of Table 6 and Table 7 and Table 8/Table 9 [3], respectively
- The mitigation actions have been selected and assigned to downgrade the residual risk from initial high level to medium/low level risks and from initial medium level to low level

The analysis carried out to develop the U-Space safety matrix content is 0063hereinafter reported; the resulting matrix has been reported in Appendix D (Table 143).

H01 – 'Loss of abort launch capability': the probability of occurrence of hazard H01 consequences has been estimated as 'Remote' (3); the severity of H01 hazard consequences, potentially leading to RPA destruction, has been assessed as 'Catastrophic'; the risk associated to hazard H01 has been assessed as 'High' and

unacceptable; the proposed mitigation action is to immediately terminate the flight using FTS/Emergency parachute; the mitigation action shall reduce the probability of H01 hazard consequences occurrence from C to D (Improbable) and the residual risk from 'High' to 'Moderate' and acceptable.

H02 – 'Loss of flight controls': the probability of occurrence of hazard H02 consequences has been estimated as 'Occasional' (4): from the FTA analysis (Table 139), the probability of occurrence level of loss of RPA control hazard has been estimated included in the range D ÷ B for rotor wing RPA and equal to A for fixed wing RPA. Performing a precautionary evaluation, the probability of occurrence of hazard H02 consequences has been ranked as 'Occasional' (4) (from probability of occurrence level 'A'). The severity of H02 hazard consequences, potentially leading to RPA destruction, has been assessed as 'Catastrophic'. The risk associated to hazard H02 has been assessed as 'High' and unacceptable. The proposed mitigation action is to terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the entity of the hazard consequences severity from 'Catastrophic' to 'Minor', due to use of emergency procedures, and the residual risk from 'High' to 'Moderate' and acceptable.

H03 – 'Loss of propulsion': the probability of occurrence of hazard H03 consequences has been estimated as 'Occasional' (4): from the FTA analysis (Table 139), the probability of occurrence level of loss of RPA propulsion hazard has been estimated included in the range D ÷ B both for rotor wing and fixed wing RPA. Performing a precautionary evaluation, the probability of occurrence of hazard number H02 has been ranked as 'Occasional' (4). The severity of hazard H03 consequences, potentially leading to RPA destruction, has been assessed as 'Catastrophic'. The risk associated to hazard H03 has been assessed as 'High' and unacceptable. The proposed mitigation action is to terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the entity of the hazard consequences severity from 'Catastrophic' to 'Minor', due to use of emergency procedures, and the residual risk from 'High' to 'Moderate' and acceptable.

H04 – 'Loss of GCS HMI': the probability of occurrence of hazard H04 consequences has been estimated as 'Remote' (3): the probability of occurrence level of GCS HMI loss has been estimated as D in the FMECA analysis with reference to GCS HMI single failure modes (Table 71) and as B in the FTA analysis, with reference to loss of longitudinal, lateral, direction and trust control hazards (Table 139); an intermediate value has been chosen, 'Remote' (3). The severity of hazard H04 consequences, potentially leading to RPA destruction, has been assessed as 'Catastrophic'. The risk associated to hazard H04 has been assessed as 'High' and unacceptable. The proposed mitigation action is to terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The FTS HMI is intended to be implemented as a separate control from other GCS HMIs (Figure 38). The mitigation action shall reduce the entity of the hazard consequences severity from

'Catastrophic' to 'Minor', due to use of emergency procedures, and the residual risk from 'High' to 'Moderate' and acceptable.

H05 – 'Deviation from steady-state (not-accelerating) flight condition': the probability of occurrence of hazard H05 consequences has been assessed as 'Remote' (3). The severity of hazard H05 consequences has been assessed as 'Catastrophic' assimilating this hazard to a loss of RPAS control hazard. The proposed mitigation action is to terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Minor', due to use of emergency procedures, and the residual risk from 'High' to 'Moderate' and acceptable.

H06 – 'Loss of Emergency Flight Termination System': the probability of occurrence of hazard H06 consequences has been estimated as 'Remote' (3): the probability of occurrence level of FTS/Emergency Parachute loss has been estimated as C/D in the FMECA analysis (Table 37) and included within B and A in the FTA analysis (Table 139); an intermediate value has been chosen, 'Remote' (3), both considering the above mentioned data and also expecting a general higher reliability from these RPA subsystems being emergency subsystems. The severity of H06 hazard consequences, potentially leading to RPA destruction, has been assessed as 'Catastrophic'. The risk associated to hazard H06 has been assessed as 'High' and unacceptable. The proposed mitigation action is an operational procedure to immediately interrupt the sortie setting the autopilot to 'landing' flight mode. The mitigation action shall reduce the consequences severity of the hazard from 'Catastrophic' to 'Minor', due to use of emergency procedures, and the residual risk from 'High' to 'Moderate' and acceptable.

H07 – 'Loss of "Return to Home" function': the probability of occurrence of hazard H07 consequences has been estimated as 'Improbable' (2) with reference to Autopilot software error probability of occurrence level estimated as D (Remote) (Table 35, item FCSS1c of the FMECA analysis). The severity of hazard H07 consequences, potentially leading to RPA destruction (for example in case of loss of link within urban environment without the possibility to use the "Return to Home" function), has been assessed as 'Catastrophic'. The risk associated to hazard H07 has been assessed as 'Moderate' and acceptable. The proposed mitigation action is to terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the entity of the hazard consequences severity from 'Catastrophic' to 'Minor', due to use of emergency procedures, and the residual risk from 'Moderate' to 'Low' and fully acceptable.

H08 – 'Loss of mission plan functionality': the probability of occurrence of hazard H08 consequences has been estimated as 'Remote' (3) with reference to 'Loss of mission software' (item MCSS1a of the FMECA analysis) which probability of occurrence level has been estimated as C (Occasional) (Table 39) and 'Loss of RPAS Mission Control subsystem functionality' with probability of occurrence level estimated between C and B. The severity of hazard H08 consequences, has been assessed as 'Minor' potentially involving operating

limitations and/or use of emergency procedures. The risk associated to hazard H08 has been assessed as 'Moderate' and acceptable. The proposed mitigation action is to use the 'Return to Home' autopilot software functionality. The mitigation action shall reduce the hazard consequences probability of occurrence from 'Remote' to 'Improbable' (2), the hazard consequences severity from 'Minor' to 'Negligible', and the residual risk from 'Moderate' to 'Low' and fully acceptable.

H09 – 'Loss of GPS signal': the probability of occurrence of hazard H09 consequences has been estimated as 'Occasional' (4). The severity of hazard H09 consequences, has been assessed as 'Minor' potentially involving operational limitations and/or use of emergency procedures. The risk associated to hazard H09 has been assessed as 'Moderate' and acceptable. The proposed mitigation action is to switch on EGNOS service, to use inertial navigation or to activate the "Return to Home" function. The mitigation action shall reduce the hazard consequences severity from 'Minor' to 'Negligible', and the residual risk from 'Moderate' to 'Low' and fully acceptable.

H10: 'Loss of EGNOS signal': the probability of occurrence of hazard H10 consequences has been estimated as 'Remote' (3) from item NSS3b of the FMECA analysis (Table 31) which probability of occurrence level has been estimated as 'D' (Remote); further more robustness/reliability is expected from EGNOS service if compared to current GPS service. The severity of hazard H10 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction if the case of RPA flying within urban or congested environment is considered with the occurrence of loss of EGNOS signal. The risk associated to hazard H10 has been assessed as 'High' and unacceptable. The proposed mitigation action is to switch on GPS service, to use inertial navigation or to activate the "Return to Home" function. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Minor', due to use of emergency procedures, and residual the risk from 'High' to 'Moderate' and acceptable.

H11 – 'Drift from the mission plan': the probability of occurrence of hazard H11 consequences has been estimated as 'Remote' (3). The severity of hazard H11 consequences, has been assessed as 'Hazardous' with reference to a potential large reduction in safety margin potentially. The risk associated to hazard H11 has been assessed as 'Moderate' and acceptable. The proposed mitigation action to further decrease the risk is to use the "Return to Home" function or to terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the hazard consequences severity from 'Hazardous' to 'Minor', due to use of emergency procedures, and the residual risk from 'Moderate' to 'Low' and fully acceptable.

H12 – 'Loss of uplink channel of the RPAS radio link': the probability of occurrence of hazard H12 consequences has been estimated as 'Occasional' (4) as intermediate evaluation between items C2LSS1a and C2LSS1b probability of occurrence level estimated as 'D' (Remote) from the FMECA analysis (Table 65) and hazard 'Degradation or loss of uplink command link with the RPA'

probability of occurrence level estimated as included within B and A from the FTA analysis (Table 139). The severity of hazard H12 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction due to the complete loss of RPA remote control in case of loss of uplink channel. The risk associated to hazard H12 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide a redundant uplink channel, to use the "Return to Home" function or to terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Minor' due to use of emergency procedures, and the residual risk from 'High' to 'Moderate' and acceptable.

H13 – 'Loss of downlink channel of the RPAS radio link': the probability of occurrence of hazard H13 consequences has been estimated as 'Occasional' (4) as intermediate evaluation between items C2LSS1a and C2LSS1b probability of occurrence level estimated as 'D' (Remote) from the FMECA analysis (Table 31) and hazard 'Degradation or loss of downlink telemetry link from the RPA' probability of occurrence level estimated as included within B and A from the FTA analysis (Table 139). The severity of hazard H13 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction due to the complete loss of RPA remote control in case of loss of uplink channel. The risk associated to hazard H13 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide a redundant uplink channel, to use the "Return to Home" function or to terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Minor' due to use of emergency procedures, and the residual risk from 'High' to 'Moderate' and acceptable.

H14 – 'Loss of ADS-B': the probability of occurrence of hazard H14 consequences has been estimated as 'Occasional' (4) as intermediate evaluation between items NSS4o probability of occurrence level estimated as 'C' (Occasional) from the FMECA analysis (Table 31) and hazard 'Degradation or loss of ADS-B functionality on board the RPAS' probability of occurrence level estimated as 'A' from the FTA analysis (Table 139). The severity of hazard H14 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction: in fact the loss of ADS-B causes lack of RPA surveillance from other airspace users, hence enhancing the probability of mid-air conflict/collision occurrence for the given RPA. The risk associated to hazard H14 has been assessed as 'High' and unacceptable. The proposed mitigation action is to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Minor', due to use of emergency procedures, and the residual risk from 'High' to 'Moderate' and acceptable.

H15 – 'Presence of natural obstacles': the probability of occurrence of hazard H15 consequences has been estimated as 'Frequent' (5). The severity of hazard

H15 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction if mid-air collision of an RPA against a natural obstacle occurs. The risk associated to hazard H15 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide the RPA with on board collision avoidance systems based on the use of downward LIDAR/SONAR sensor and/or to provide the RPA mission planner software with terrain profile data from mapping services (like Google Map). The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Negligible' (few consequences) and the residual risk from 'High' to 'Moderate' and acceptable.

H16 – 'Presence of man-made manufactures': the probability of occurrence of hazard H16 consequences has been estimated as 'Frequent' (5). The severity of hazard H16 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction if mid-air collision of an RPA against a natural obstacle occurs. The risk associated to hazard H16 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide the RPA with on board collision avoidance systems based on the use of downward LIDAR/SONAR sensor and/or to provide the RPA mission planner software with terrain profile data from mapping services (like Google Map); in addition geofence software functionality is suggested to completely avoid RPA to fly nearby sensitive buildings, airport infrastructures forbidden areas, etc. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Negligible' (few consequences) and the residual risk from 'High' to 'Moderate' and acceptable.

H17 – 'Mid-air collision with other aircraft': the probability of occurrence of hazard H17 consequences has been estimated as 'Occasional' (4). The severity of hazard H17 consequences has been assessed as 'Catastrophic' leading to RPA destruction if mid-air collision of an RPA against another RPA or manned aircraft occurs; further human beings severe injury or death can potentially in case of mid-air collision with manned aircraft. The risk associated to hazard H17 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide the RPA with on board 'Detect and Avoid' systems against mid-air conflict with cooperative traffic and to provide the RPA with LIDAR/SONAR sensor against mid-air conflict with not cooperative traffic. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Negligible' (few consequences) and the residual risk from 'High' to 'Moderate' and acceptable.

H18 – 'Loss of DAA capability': the probability of occurrence of hazard H18 consequences has been estimated as 'Remote' (3) starting from the calculated probability of occurrence level of DAA multiple failures of Table 97. The severity of hazard H18 consequences, has been assessed as 'Catastrophic' leading to RPA destruction if mid-air collision of an RPA against another RPA or manned aircraft occurs; further human beings severe injury or death can potentially occur if an RPA collides with a manned aircraft. The risk associated to hazard H18 has been assessed as 'High' and unacceptable. The proposed mitigation action is to terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Minor' (due to use of

emergency procedures), and the residual risk from 'High' to 'Moderate' and acceptable.

H19 – 'No detectability from other airspace users': the probability of occurrence of hazard H19 consequences has been estimated as 'Frequent' (5) due to the reduced size of RPA with respect to manned aviation. The severity of hazard H19 consequences, has been assessed as 'Catastrophic' leading to RPA destruction if mid-air collision of an RPA against another RPA or manned aircraft occurs; further human beings severe injury or death can potentially occur if an RPA collides with a manned aircraft. The risk associated to hazard H19 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide the RPA with on board ADS-B to be detectable by other U-Space users equipped with DAA functionalities. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Minor' (due to use of emergency procedures), and the residual risk from 'High' to 'Moderate' and acceptable.

H20 – 'Cooperative traffic intrusion': the probability of occurrence of hazard H20 consequences has been estimated as 'Occasional' (4). The severity of hazard H20 consequences, has been assessed as 'Catastrophic' leading to RPA destruction if mid-air collision of an RPA against another RPA or manned aircraft occurs; further human beings severe injury or death can potentially occur if an RPA collides with a manned aircraft. The risk associated to hazard H20 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide the RPA with on board ADS-B and DAA equipment against cooperative traffic intrusion in the VLL subspace. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Minor' (due to use of emergency procedures), and the residual risk from 'High' to 'Moderate' and acceptable.

H21 – 'Not cooperative traffic intrusion': the probability of occurrence of hazard H21 consequences has been estimated as 'Occasional' (4). The severity of hazard H21 consequences, has been assessed as 'Catastrophic' leading to RPA destruction if mid-air collision of an RPA against another RPA or manned aircraft occurs; further human beings severe injury or death can potentially occur if an RPA collides with a manned aircraft. The risk associated to hazard H21 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide the RPA with LIDAR/SONAR sensors as secondary (with respect to DAA subsystem) collision avoidance system against not cooperative traffic intrusion in the VLL subspace. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Minor' (due to use of emergency procedures), and the residual risk from 'High' to 'Moderate' and acceptable.

H22 – 'Missed cooperative traffic tracking': the probability of occurrence of hazard H22 consequences has been estimated as 'Occasional' (4). The severity of hazard H22 consequences, has been assessed as 'Catastrophic' leading to RPA destruction if mid-air collision of an RPA against another RPA or manned aircraft occurs; further human beings severe injury or death can potentially occur if an RPA collides with a manned aircraft. The risk associated to hazard H22 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide the RPA with on board ADS-B and DAA equipment. The mitigation action shall

reduce the hazard consequences severity from ‘Catastrophic’ to ‘Minor’, and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H23 – ‘Missed not cooperative traffic tracking’: the probability of occurrence of hazard H23 consequences has been estimated as ‘Occasional’ (4). The severity of hazard H23 consequences, has been assessed as ‘Catastrophic’ leading to RPA destruction if mid-air collision of an RPA against another RPA or manned aircraft occurs; further human beings severe injury or death can potentially occur if an RPA collides with a manned aircraft. The risk associated to hazard H23 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to provide the RPA with on board LIDAR/SONAR sensors (also as secondary, with respect to DAA, surveillance and anti-collision systems). The mitigation action shall reduce the hazard consequences severity from ‘Catastrophic’ to ‘Minor’, and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H24 – ‘Collision with cooperative traffic’: the probability of occurrence of hazard H24 consequences has been estimated as ‘Occasional’ (4). The severity of hazard H24 consequences, has been assessed as ‘Catastrophic’ leading to RPA destruction if mid-air collision of an RPA against another RPA or manned aircraft occurs; further human beings severe injury or death can potentially occur if an RPA collides with a manned aircraft. The risk associated to hazard H24 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to provide the RPA with DAA equipment to detect cooperative traffic in the VLL subspace. The mitigation action shall reduce the hazard consequences severity from ‘Catastrophic’ to ‘Minor’ (due to use of emergency procedures), and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H25 – ‘Collision with not cooperative traffic’: the probability of occurrence of hazard H25 consequences has been estimated as ‘Occasional’ (4). The severity of hazard H25 consequences, has been assessed as ‘Catastrophic’ leading to RPA destruction if mid-air collision of an RPA against another RPA or manned aircraft occurs; further human beings severe injury or death can potentially occur if an RPA collides with a manned aircraft. The risk associated to hazard H25 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to provide the RPA with LIDAR/SONAR sensors as secondary (with respect to DAA subsystem) collision avoidance system to detect not cooperative traffic in the VLL subspace. The mitigation action shall reduce the hazard consequences severity from ‘Catastrophic’ to ‘Minor’ (due to use of emergency procedures), and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H26 – ‘Missed performance of avoidance collision manoeuvre’: the probability of occurrence of hazard H26 consequences has been estimated as ‘Occasional’ (4). The severity of hazard H26 consequences, has been assessed as ‘Catastrophic’ leading to RPA destruction when avoidance mid-air collision of an RPA against another RPA or manned aircraft occurs due to missed performance of avoidance manoeuvre; further human beings severe injury or death can potentially occur if an RPA collides with a manned aircraft. The risk associated to hazard H26 has been assessed as ‘High’ and unacceptable. Assuming that hazard H26 occurs for DAA failure, the proposed mitigation action is to provide the RPA

with a secondary collision avoidance system based on LIDAR/SONAR sensors capable as DAA to provide the Flight Control Subsystem with proper data to make the RPA perform anti-collision evasive manoeuvre. The mitigation action shall reduce the hazard consequences probability of occurrence from 'Occasional' to 'Remote', hazard consequences severity from 'Catastrophic' to 'Minor' (due to use of emergency procedures), and the residual risk from 'High' to 'Moderate' and acceptable.

H27 – 'Missed monitoring of performance of collision avoidance manoeuvre': the probability of occurrence of hazard H27 consequences has been estimated as 'Occasional' (4). The severity of hazard H27 consequences, has been assessed as 'Hazardous' leading to large reduction in RPA safety margins. The risk associated to hazard H27 has been assessed as 'High' and unacceptable. The proposed mitigation action is to increase the remote pilot training in monitoring collision avoidance manoeuvring. The mitigation action shall reduce the hazard consequences probability of occurrence from 'Occasional' to 'Remote', and the residual risk from 'High' to 'Moderate' and acceptable.

H28 – 'Missed weather awareness capability': the probability of occurrence of hazard H28 consequences has been estimated as 'Remote' (3). The severity of hazard H28 consequences, has been assessed as 'Hazardous' potentially leading to large reduction in RPA safety margins. The risk associated to hazard H28 has been assessed as 'Moderate' and acceptable. The proposed mitigation action to further decrease the risk is to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the hazard consequences severity from 'Hazardous' to 'Minor' (due to use of emergency procedures), and the residual risk from 'Moderate' to 'Low' and fully acceptable.

H29 – 'Missed gathering of contingent weather information': the probability of occurrence of hazard H29 consequences has been estimated as 'Remote' (3). The severity of hazard H29 consequences, has been assessed as 'Hazardous' potentially leading to large reduction in RPA safety margins. The risk associated to hazard H29 has been assessed as 'Moderate' and acceptable. The proposed mitigation action to further decrease risk is to increase on ground routine maintenance/checks for weather information gathering HMI. The mitigation action shall reduce the hazard consequences probability of occurrence from 'Remote' to 'Improbable' and the risk from 'Moderate' to 'Low' and fully acceptable.

H30 – 'Missed avoidance of adverse weather': the probability of occurrence of hazard H30 consequences has been estimated as 'Occasional' (4). The severity of hazard H30 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction. The risk associated to hazard H30 has been assessed as 'High' and unacceptable. The proposed mitigation action to provide support to the remote pilot through the installation of an on board miniaturized weather Doppler RADAR. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Negligible', and the risk from 'High' to 'Moderate' and acceptable.

H31 – ‘Loss of RPAS subsystems health and status monitoring’: the probability of occurrence of hazard H31 consequences has been estimated as ‘Occasional’ (4). The severity of hazard H31 consequences, has been assessed as ‘Hazardous’ potentially leading to large reduction in RPA safety margins. The risk associated to hazard H31 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to use the “Return to Home” function or to terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the hazard consequences severity from ‘Hazardous’ to ‘Minor’, due to use of emergency procedures, and the risk from ‘High’ to ‘Low’ and fully acceptable.

H32 – ‘Loss of communication while transiting from LOS to BRLOS and vice versa’: the probability of occurrence of hazard H32 consequences has been estimated as ‘Frequent’ (5) on the basis of probability of occurrence levels estimated between B and A for the hazards ‘Degradation or loss of uplink command link with the RPA’/‘Degradation or loss of downlink telemetry link from the RPA’ (Table 139). The severity of hazard H32 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction. The risk associated to hazard H32 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to perform an accurate pre-flight mission planning in accordance with the RPAS radio link range capability. The mitigation action shall reduce hazard H32 probability of consequences occurrence from ‘Occasional’ to ‘Remote’, hazard H32 consequences severity from ‘Hazardous’ to ‘Minor’, due to use of emergency procedures, and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H33 – ‘Unintentional radio link interference’: the probability of occurrence of hazard H33 consequences has been estimated as ‘Remote’ (3) with reference to items C2LSS1a and C2LSS1b which probability of occurrence level has been estimated equal to ‘D’ (Remote) in the FMECA analysis (Table 65). The severity of hazard H33 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction. The risk associated to hazard H33 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to provide a redundant radio link on another radio frequency band. The mitigation action shall reduce the hazard consequences probability of occurrence from ‘Remote’ to ‘Improbable’, and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H34 – ‘Malicious radio link jamming’: the probability of occurrence of hazard H34 consequences has been estimated as ‘Occasional’ (4). The severity of hazard H34 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction. The risk associated to hazard H34 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to provide a redundant radio link on another radio frequency band or to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce hazard H34 consequences probability of occurrence from ‘Occasional’ to ‘Remote’, hazard H34 consequences severity from ‘Catastrophic’ to ‘Minor’ (due to use of emergency procedures) and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H35 – ‘Malicious radio link jamming’: the probability of occurrence of hazard H35 consequences has been estimated as ‘Occasional’ (4). The severity of hazard H35 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction. The risk associated to hazard H35 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to provide a redundant radio link on another radio frequency band or to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce hazard H35 probability of occurrence from ‘Occasional’ to ‘Remote’, hazard H35 consequences severity from ‘Catastrophic’ to ‘Minor’ (due to use of emergency procedures) and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H36 – ‘Fire’: the probability of occurrence of hazard H36 consequences has been estimated as ‘Occasional’ (4) on the basis of the evaluations performed on different RPAS subsystems: fire caused by LiPo batteries short circuit with probability of occurrence level estimated as ‘B’; fire due to electrical cables short circuit with probability of occurrence level estimated as ‘A’, fire on board fixed wing RPAS with probability of occurrence level estimated between ‘B’ and ‘A’, fire on board hybrid RPAS with probability of occurrence level estimated between ‘C’ and ‘B’ (from the FTA analysis, Table 139). The severity of hazard H36 consequences, has been assessed as ‘Catastrophic’ leading to RPA destruction. The risk associated to hazard H36 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to perform proper routine maintenance actions on LiPo batteries, electrical, fuel and hydrogen fuel cells subsystems to prevent hazard H36 from occurring; the suggested mitigation action is to immediately terminate the flight using the FTS. The mitigation action shall reduce the hazard consequences severity from ‘Catastrophic’ to ‘Hazardous’ (due large reduction of safety margins) and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H37 – ‘Loss of RPAS autopilot’: the probability of occurrence of hazard H37 consequences has been estimated as ‘Remote’ (3) on the basis of the evaluations performed in for items FCSS1a, FCSS1b, FCSS1c in the FMECA analysis (Table 35). The severity of hazard H37 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction. The risk associated to hazard H37 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to switch on a redundant autopilot and/or to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce hazard H37 probability of occurrence from ‘Remote’ to ‘Improbable’ (switching on redundant autopilot), hazard H37 consequences severity from ‘Catastrophic’ to ‘Minor’ (due to use of the flight termination emergency procedures) and the residual risk from ‘High’ to ‘Low’ and fully acceptable.

H38 – ‘Loss of electrical power’: the probability of occurrence of hazard H38 consequences has been estimated as ‘Frequent (5) on the basis of the evaluations performed for the following hazards ‘Degradation or loss of rotor wing RPAS power functionality’ with probability of occurrence level estimated as ‘B’ and/or ‘Degradation or loss of fixed wing RPAS power functionality’ with probability of

occurrence level included between ‘B’ and ‘A’ in the FTA analysis (Table 139). The severity of hazard H38 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction. The risk associated to hazard H38 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the hazard consequences severity from ‘Catastrophic’ to ‘Minor’ (due to the use of emergency procedures) and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H39 – ‘Loss of inertial platform’: the probability of occurrence of hazard H39 consequences as ‘Occasional’ (4) on the basis of items NSS1a and NSS1b probability of occurrence levels estimated as ‘D’ and ‘C’ respectively in the FMECA analysis (Table 31). The severity of hazard H39 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction. The risk associated to hazard H39 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to switch on a redundant inertial platform or to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce hazard H39 consequences probability of occurrence from ‘Occasional’ to ‘Remote’ (switching on the redundant inertial platform), hazard H39 consequences severity from ‘Catastrophic’ to ‘Minor’ (due to the use of flight termination emergency procedures) and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H40 – ‘Loss of heading indication’: the probability of occurrence of hazard H40 consequences has been estimated as ‘Occasional’ (4) on the basis of items NSS1a and NSS1b probability of occurrence levels estimated as ‘D’ and ‘C’ respectively in the FMECA analysis (Table 31). The severity of hazard H40 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction. The risk associated to hazard H40 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to switch on a redundant inertial platform or to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce hazard H40 consequences probability of occurrence from ‘Occasional’ to ‘Remote’ (switching on the redundant inertial platform), hazard H40 consequences severity from ‘Catastrophic’ to ‘Minor’ (due to the use of flight termination emergency procedures) and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H41 – ‘Loss of altitude indication’: the probability of occurrence of hazard H41 consequences has been estimated as ‘Improbable’ (2) on the basis of the evaluations of item NSS4g probability of occurrence level estimated as ‘E’ in the FMECA analysis (Table 31) performed in the FMECA analysis. The severity of hazard H41 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction. The risk associated to hazard H41 has been assessed as ‘Moderate’ and acceptable. The proposed mitigation action is to provide a redundant altimeter or to immediately terminate the flight using the FTS if far

from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce hazard H41 consequences probability of occurrence from 'Improbable' to 'Extremely improbable' (switching on the redundant altimeter), hazard H41 consequences severity from 'Catastrophic' to 'Minor' (due to the use of flight termination emergency procedures) and the residual risk from 'Moderate' to 'Low' and fully acceptable.

H42 – 'Pressure sensor failure: the probability of occurrence of hazard H42 consequences has been estimated as 'Frequent' (5) on the basis of the hazard 'Pressure sensor failure' probability of occurrence level estimated as A in the FTA analysis (Table 139). The severity of hazard H42 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction. The risk associated to hazard H42 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide a redundant pressure sensor or to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce hazard H42 consequences probability of occurrence from 'Frequent' to 'Occasional' (switching on the redundant pressure sensor), hazard H42 consequences severity from 'Catastrophic' to 'Minor' (due to the use of flight termination emergency procedures) and the residual risk from 'High' to 'Moderate' and acceptable.

H43 – 'Misleading altitude indication': the probability of occurrence of hazard H43 consequences has been estimated as 'Frequent' (5) on the basis of the hazard 'Misleading altitude indication' probability of occurrence level estimated as A in the FTA analysis (Table 139). The severity of hazard H43 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction. The risk associated to hazard H43 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide a redundant pressure sensor or to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce hazard H43 consequences probability of occurrence from 'Frequent' to 'Occasional' (switching on the redundant altimeter), hazard H43 consequences severity from 'Catastrophic' to 'Minor' (due to the use of flight termination emergency procedures) and the residual risk from 'High' to 'Moderate' and acceptable.

H44 – 'Misleading airspeed indication': the probability of occurrence of hazard H44 consequences has been estimated as 'Frequent' (5) on the basis of the hazard 'Misleading airspeed indication' probability of occurrence level estimated as A in the FTA analysis (Table 139). The severity of hazard H44 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction. The risk associated to hazard H44 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide a redundant pressure sensor or to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce hazard H44 consequences probability of occurrence from 'Frequent' to 'Occasional' (switching on the redundant pressure sensor), hazard H44 consequences severity from 'Catastrophic' to 'Minor' (due to the use of flight

termination emergency procedures) and the residual risk from 'High' to 'Moderate' and acceptable.

H45 – 'Misleading indication of the angle of incidence': the probability of occurrence of hazard H45 consequences has been estimated as 'Frequent' (5) on the basis of the hazard 'Fixed wing RPAS misleading angle of attack indication' probability of occurrence level estimated as included between B and A in the FTA analysis (Table 139). The severity of hazard H45 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction. The risk associated to hazard H45 has been assessed as 'High' and unacceptable. The proposed mitigation action is to provide a redundant pressure sensor or to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce hazard H45 consequences probability of occurrence from 'Frequent' to 'Occasional' (switching on the redundant pressure sensor), hazard consequences severity from 'Catastrophic' to 'Minor' (due to the use of flight termination emergency procedures) and the residual risk from 'High' to 'Moderate' and acceptable.

H46 – 'Stall': the probability of occurrence of hazard H46 consequences has been estimated as 'Frequent' (5) on the basis of the hazard 'Fixed wing RPAS stall' probability of occurrence level estimated as included between B and A in the FTA analysis (Table 139). The severity of hazard H46 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction. The risk associated to hazard H46 has been assessed as 'High' and unacceptable. The proposed mitigation action is to promptly execute a diving manoeuvre or to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce hazard H46 consequences severity from 'Catastrophic' to 'Minor' (due to the use of emergency procedures) and the residual risk from 'High' to 'Moderate' and acceptable.

H47 – 'Loss of fuel cell': the probability of occurrence of hazard H47 consequences has been estimated as 'Remote' (3) on the basis of items HPSS2a and HPSS2b probability of occurrence levels estimated equal to 'D' in the FMECA analysis (Table 63). The severity of hazard H47 consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction. The risk associated to hazard H47 has been assessed as 'High' and unacceptable. The proposed mitigation action is to switch on redundant LiPo batteries. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Minor' (due to use of emergency procedures) and the residual risk from 'High' to 'Moderate' and acceptable.

H48 – 'Lack or not appropriate remote pilot training': the probability of occurrence of hazard H48 consequences has been estimated as 'Occasional' (4) on the basis of the human factor related hazard 'Low remote pilot training' with probability of occurrence estimated as 'Occasional' (Table 142). The severity of hazard H48 consequences, has been assessed as 'Hazardous', potentially leading to a large reduction in safety margins. The risk associated to hazard H48 has been assessed as 'High' and unacceptable. The proposed mitigation action is to increase

and improve the remote pilot training. The mitigation action shall reduce hazard H48 probability of occurrence from 'Occasional' to 'Remote', hazard H48 consequences severity from 'Hazardous' to 'Minor' (nuisance) and the residual risk from 'High' to 'Moderate' and acceptable.

H49 – 'Lack of compliant operational procedures, checklist, etc.': the probability of occurrence of hazard H49 consequences has been estimated as 'Frequent' (5) on the basis of the 'Lack of specific checklists, operational procedures' human factor related hazard with probability of occurrence estimated as 'Frequent' (Table 142). The severity of hazard H49 consequences, has been assessed as 'Hazardous', potentially leading to a large reduction in safety margins. The risk associated to hazard H49 has been assessed as 'High' and unacceptable. The proposed mitigation action is the provision of proper operational procedures and checklists. The mitigation action shall reduce hazard H49 consequences probability of occurrence from 'Frequent' to 'Remote', hazard H49 consequences severity from 'Hazardous' to 'Minor' (nuisance) and the residual risk from 'High' to 'Moderate' and acceptable.

H50 – 'Loss of remote pilot situational awareness': the probability of occurrence of hazard H50 consequences has been estimated as 'Frequent' (5) on the basis of the 'Loss of remote pilot situational awareness' human factor related hazard with probability of occurrence estimated as 'Frequent' (Table 142). The severity of hazard H50 consequences, has been assessed as 'Hazardous', potentially leading to a large reduction in safety margins. The risk associated to hazard H50 has been assessed as 'High' and unacceptable. The proposed mitigation action is the increase the remote pilot training. The mitigation action shall reduce hazard H50 consequences probability of occurrence from 'Frequent' to 'Remote', hazard H50 consequences severity from 'Hazardous' to 'Minor' (nuisance) and the residual risk from 'High' to 'Moderate' and acceptable.

H51 – 'Human senses limitation': the probability of occurrence of hazard H51 consequences has been estimated as 'Frequent' (5) on the basis of the 'Human senses limitation' human factor related hazard with probability of occurrence estimated as 'Frequent' (Table 142). The severity of hazard H51 consequences, has been assessed as 'Catastrophic', potentially leading to RPA destruction. The risk associated to hazard H51 has been assessed as 'High' and unacceptable. The proposed mitigation action is the increase the remote pilot training. The mitigation action shall reduce hazard H51 consequences probability of occurrence from 'Frequent' to 'Remote', hazard H51 consequences severity from 'Catastrophic' to 'Minor' (nuisance) and the residual risk from 'High' to 'Moderate' and acceptable.

H52 – 'Remote pilot excessive workload': the probability of occurrence of hazard H52 consequences has been estimated as 'Occasional' (4) on the basis of the 'Human senses limitation' human factor related hazard with probability of occurrence estimated as 'Occasional' (Table 142). The severity of hazard H52 consequences, has been assessed as 'Major', potentially leading to a significant reduction in safety margins. The risk associated to hazard H52 has been assessed as 'High' and unacceptable. The proposed mitigation action is the increase the

remote pilot training. The mitigation action shall reduce hazard H52 consequences probability of occurrence from 'Occasional' to 'Remote', hazard H52 consequences severity from 'Major' to 'Minor' (nuisance) and the residual risk from 'High' to 'Moderate' and acceptable.

H53 – 'Cloud cover': the probability of occurrence of hazard H53 consequences has been estimated as 'Frequent' (5). The severity of hazard H53 consequences, has been assessed as 'Major' [87]. The risk associated to hazard H53 has been assessed as 'High' and unacceptable. The proposed mitigation action is to interrupt the flight mission and to apply the "Return to Home" function. The mitigation actions shall reduce the hazard consequences severity from 'Major' to 'Minor' (with reference to nuisance/use of emergency procedures) and the residual risk from 'High' to 'Moderate' and acceptable.

H54 – 'Fog': the probability of occurrence of hazard H54 consequences has been estimated as 'Occasional' (4). The severity of hazard H54 consequences, has been assessed as 'Major' [87]. The risk associated to hazard H54 has been assessed as 'Moderate' and acceptable. Nevertheless, the proposed mitigation action to further decrease the risk associated to this hazard is to interrupt the flight mission and to apply the "Return to Home" function. The mitigation actions shall reduce the hazard consequences severity from 'Major' to 'Negligible' (few consequences); the residual risk remains 'Moderate' and acceptable.

H55 – 'Freezing rain': the probability of occurrence of hazard H55 consequences has been estimated as 'Remote' (3). The severity of hazard H55 consequences, has been assessed as 'Hazardous' leading to a large reduction in safety margins. The risk associated to hazard H55 has been assessed as 'Moderate' and acceptable. Nevertheless, the proposed mitigation action to further decrease the risk associated to this hazard is to interrupt the flight mission and to apply the "Return to Home" function. The mitigation actions shall reduce the hazard consequences severity from 'Hazardous' to 'Negligible' (few consequences) and the residual risk from 'Moderate' to 'Low' and fully acceptable.

H56 – 'Glare': the probability of occurrence of hazard H56 consequences has been estimated as 'Occasional' (4). The severity of hazard H56 consequences, has been assessed as 'None' due to the absence of the pilot on board the RPAS. The risk associated to hazard H56 has been assessed as 'Moderate' and acceptable without the necessity for further mitigation actions required.

H57 – 'Haze': the probability of occurrence of hazard H57 consequences has been estimated as 'Occasional' (4). The severity of hazard H57 consequences, has been assessed as 'Major' [87]. The risk associated to hazard H57 has been assessed as 'Moderate' and acceptable. Nevertheless, the proposed mitigation action to further decrease the risk associated to this hazard is to interrupt the flight mission and to apply the "Return to Home" function. The mitigation actions shall reduce the hazard consequences severity from 'Hazardous' to 'Negligible' (few consequences) and the residual risk from 'Moderate' to 'Low' and fully acceptable.

H58 – ‘Humidity’: the probability of occurrence of hazard H58 consequences has been estimated as ‘Frequent’ (5). The severity of hazard H58 consequences, has been assessed as ‘Hazardous’ [87]. The risk associated to hazard H58 has been assessed as ‘High’ and unacceptable. Nevertheless, the proposed mitigation action is to forbid the flight mission until the air humidity values are above the RPAS limits indicated in the operational manual. The mitigation action shall reduce the hazard consequences severity from ‘Hazardous’ to ‘Negligible’ (few consequences) and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H59 – ‘Ice’: the probability of occurrence of hazard H59 consequences has been estimated as ‘Occasional’ (4). The severity of hazard H59 consequences, has been assessed as ‘Hazardous’ [87]. The risk associated to hazard H59 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to forbid the flight mission until when optimal weather conditions are restored. The mitigation action shall reduce the hazard consequences severity from ‘Hazardous’ to ‘Negligible’ (few consequences) and the residual risk from ‘High’ to ‘Low’ and fully acceptable.

H60 – ‘Rain’: the probability of occurrence of hazard H60 consequences has been estimated as ‘Frequent’ (5). The severity of hazard H60 consequences, has been assessed as ‘Hazardous’ [87]. The risk associated to hazard H60 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is the provision of an on board miniaturized weather Doppler RADAR to identify the rain and the successive application of the “Return to Home” function to save the RPA. The mitigation action shall reduce the hazard consequences severity from ‘Hazardous’ to ‘Negligible’ (few consequences) and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H61 – ‘Snow’: the probability of occurrence of hazard H61 consequences has been estimated as ‘Frequent’ (5). The severity of hazard H61 consequences, has been assessed as ‘Hazardous’ [87]. The risk associated to hazard H61 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is the provision of an on board miniaturized weather Doppler RADAR to identify the rain and the successive application of the “Return to Home” function to save the RPA. The mitigation action shall reduce the hazard consequences severity from ‘Hazardous’ to ‘Negligible’ (few consequences) and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H62 – ‘Solar storm’: the probability of occurrence of hazard H62 consequences has been estimated as ‘Remote’ (3). The severity of hazard H62 consequences, has been assessed as ‘Hazardous’ [87]. The risk associated to hazard H62 has been assessed as ‘Moderate’ and acceptable. Nevertheless, due to the potential occurrence of loss or degradation of the radio link caused by excessive solar activity, the proposed mitigation action is to apply the “Return to Home” function and save he RPA. The mitigation action shall reduce the hazard consequences severity from ‘Hazardous’ to ‘Negligible’ (few consequences) and the risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H63 – ‘Temperature’: the probability of occurrence of hazard H63 consequences has been estimated as ‘Frequent’ (5). The severity of hazard H63

consequences, has been assessed as 'Hazardous' [87]. The risk associated to hazard H63 has been assessed as 'High' and unacceptable. The proposed mitigation action is to forbid the flight mission until the temperature values are above the RPAS limits indicated in the operational manual. The mitigation action shall reduce the hazard consequences severity from 'Hazardous' to 'Negligible' (few consequences) and the residual risk from 'High' to 'Moderate' and acceptable.

H64 – 'Turbulence': the probability of occurrence of hazard H64 consequences has been estimated as 'Occasional' (4). The severity of hazard H64 consequences, has been assessed as 'Hazardous' [87]. The risk associated to hazard H64 has been assessed as 'High' and unacceptable. The proposed mitigation action is to forbid the flight mission until that optimal operational conditions are restored. The mitigation action shall reduce the hazard consequences severity from 'Hazardous' to 'Negligible' (few consequences) and the residual risk from 'High' to 'Moderate' and acceptable.

H65 – 'Wind': the probability of occurrence of hazard H65 consequences has been estimated as 'Frequent' (5). The severity of hazard H65 consequences, has been assessed as 'Hazardous' [87]. The risk associated to hazard H65 has been assessed as 'High' and unacceptable. The proposed mitigation action is to forbid the flight mission until that optimal operational conditions are restored. The mitigation action shall reduce the hazard consequences severity from 'Hazardous' to 'Negligible' (few consequences) and the residual risk from 'High' to 'Moderate' and acceptable.

H66 – 'Lightning strike': the probability of occurrence of hazard H66 consequences has been estimated as 'Occasional' (4). The severity of hazard H65 consequences, has been assessed as 'Catastrophic' [87]. The risk associated to hazard H66 has been assessed as 'High' and unacceptable. The proposed mitigation action is to forbid the flight mission until that optimal operational conditions are restored. The mitigation action shall reduce the hazard consequences severity from 'Hazardous' to 'Negligible' (few consequences) and the residual risk from 'High' to 'Moderate' and acceptable.

H67 – 'Hail': the probability of occurrence of hazard H67 consequences has been estimated as 'Occasional' (4). The severity of hazard H67 consequences, has been assessed as 'Catastrophic' [87]. The risk associated to hazard H67 has been assessed as 'High' and unacceptable. The proposed mitigation action is to forbid the flight mission until when optimal weather conditions are restored. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Negligible' (few consequences) and the risk from 'High' to 'Moderate' and fully acceptable.

H68 – 'Hurricane': the probability of occurrence of hazard H68 consequences has been estimated as 'Remote' (3). The severity of hazard H68 consequences, has been assessed as 'Catastrophic' [87]. The risk associated to hazard H68 has been assessed as 'High' and unacceptable. The proposed mitigation action is to forbid the flight mission until when optimal weather conditions are restored. The mitigation action shall reduce the hazard consequences severity from

'Catastrophic' to 'Negligible' (few consequences) and the risk from 'High' to 'Low' and fully acceptable.

H69 – 'Volcanic ash': the probability of occurrence of hazard H69 consequences has been estimated as 'Remote' (3) ([88], Appendix 4). The severity of hazard H69 consequences, has been assessed as 'Catastrophic'. The risk associated to hazard H69 has been assessed as 'High' and unacceptable. The proposed mitigation action is to forbid the flight mission until when optimal weather conditions are restored. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Negligible' (few consequences) and the risk from 'High' to 'Low' and fully acceptable.

3.2.9 The ATM hazard log

The ATM hazard log (Table 12) has been draft according to the categorization of RPAS functionalities described in Paragraph 3.2 for the successive safety risk analysis. It reports the hazards expected to occur in the subspace above 500 Feet of altitude until FL600 and beyond under ATM service where the certified category operations involving RPAS with maximum take-off weight between 150 and 600 kg (HALE RPAS) are expected to be host ([18], [27], [28] and [29]).

Table 12 – Hazard analysis: ATM hazard log

Hazard log	
Hazard #	**Definition**
Service: **ATM**	
RPAS Aviate functionality related hazards	
H01	Impossibility to perform manoeuvres on ground
H02	Loss of abort launch capability
H03	Loss of flight controls
H04	Loss of propulsion
H05	Loss of GCS HMI
H06	Loss of GCS monitoring displays
H07	Deviation from steady-state (not-accelerating) flight condition
H08	Loss of Emergency Flight Termination System
H09	Loss of 'Return to home function'
H10	Impossibility to perform a 'go around' manoeuvre
RPAS Navigate functionality related hazards	
H11	Loss of mission plan
H12	Loss of GPS signal
H13	Loss of EGNOS signal
H14	Drift from the mission plan
H15	Loss of mission plan updating software functionality
H16	Lack of communication of mission plan updating to ATC
RPAS Communicate functionality related hazards	
Hazard log	
Hazard #	**Definition**
Service: **ATM**	
H17	Loss of uplink channel of the RPAS radio link
H18	Loss of downlink channel of the RPAS radio link
H19	Loss of ADS_B
H20	Loss of communication with ATC
RPAS hazards avoidance functionality related hazards	

Table 12 – Hazard analysis: ATM hazard log (Cont'd)	
H21	Presence of natural obstacles
H22	Presence of man-made manufactures
H23	Mid-air collision with other aircraft
H24	Loss of DAA functionality
H25	No detectability from other airspace users
H26	Cooperative traffic intrusion
H27	Not cooperative traffic intrusion
H28	Missed cooperative traffic tracking
H29	Missed not cooperative traffic tracking
H30	Collision with cooperative traffic
H31	Collision with not cooperative traffic
H32	Missed performance of collision avoidance manoeuvre
H33	Missed monitoring of performance of collision avoidance manoeuvring
H34	Missed weather awareness capability
H35	Missed gathering of contingent weather information
H36	Missed avoidance of adverse weather
Cross-cutting functionalities related hazard	
H37	Loss of RPAS subsystems health and status monitoring
H38	Loss of communication while transiting from LOS to BRLOS and vice versa
H39	Unintentional radio link interference
H40	Malicious radio link jamming
H41	Malicious radio link spoofing
Contingencies → Failures related hazards	
H42	Fire
H43	Loss of RPAS autopilot
H44	Loss of electrical power
H45	Loss of inertial platform
H46	Loss of heading indication
H47	Loss of altitude indication
H48	Loss of airspeed indication
H49	Pressure sensors failure
H50	Misleading altitude indication
H51	Misleading airspeed indication
H52	Misleading indication of the angle of incidence
H53	Stall
H54	Loss of fuel cell
H55	Loss of fuel
Contingencies → Human factor related hazards	
H56	Remote pilot low training
H57	Non-compliant operational procedures
H58	Remote pilot loss of situational awareness
H59	Human senses limitations
H60	Remote pilot excessive workload
H61	Loss of separation provision from the ATC
H62	Loss of separation provision from the remote pilot
H63	Erroneous separation instruction provision from the ATC
H64	Erroneous execution of the separation provision instruction from the remote pilot
H65	The RPAS does not comply or incorrectly responds to separation provision instruction issued by ATC
H66	Remote pilot delayed response to separation instruction provision from ATC
Hazard log	
Hazard #	**Definition**
Service: **ATM**	
H67	Excessive number of intentional deviations from separation provision instruction
H68	Missed submission of flight plan to ATC
Contingencies → Weather related hazards	
H69	Cloud cover

Table 12 – Hazard analysis: ATM hazard log (Cont'd)	
H70	Fog
H71	Freezing rain
H72	Glare
H73	Haze
H74	Humidity
H75	Ice
H76	Rain
H77	Snow
H78	Solar storms
H79	Temperature
H80	Turbulence
H81	Wind
H82	Lightning strike
H83	Hail
H84	Hurricanes
H85	Volcanic ash

The ATM risk assessment matrix

The ATM risk matrix has been developed following the same criteria as for the U-Space risk matrix.

The analysis carried out to develop the ATM safety matrix content is hereinafter reported; the differences only in the analysis of the ATM hazard log and implementation of the descending risk matrix with respect to the above described U-space hazard log and risk matrix analysis are hereinafter reported and described.

The resulting ATM safety risk matrix has been reported in Appendix D (Table 144).

H01 – 'Impossibility to perform manoeuvers on ground': the probability of occurrence of hazard H01 consequences has been estimated as 'Remote' (3); the severity of H01 hazard consequences, has been assessed as 'Hazardous' leading to a large reduction in safety margins on ground; the risk associated to hazard H01 has been assessed as 'High' and unacceptable; the proposed mitigation action is to increase RPA maintenance; the mitigation action shall reduce the probability of hazard H01 consequences occurrence from 'Remote' to 'Improbable' and the residual risk from 'High' to 'Moderate' and acceptable.

H02 – 'Loss of abort launch capability': as for hazard H01 in the U-space matrix.

H03 – 'Loss of flight controls': as for hazard H02 in the U-space matrix, but the probability of hazard H03 consequences occurrence has been assessed as 'Remote' (3) due to the operation of RPAS expected to be technically more advanced. The proposed mitigation actions shall reduce the residual risk from 'High' to 'Moderate' and acceptable.

H04 – 'Loss of propulsion': as for hazard H03 in the U-space matrix, but the probability of hazard H04 consequences occurrence has been assessed as 'Remote' (3) due to the operation of RPAS expected to be technically more advanced. The proposed mitigation actions shall reduce the residual risk from 'High' to 'Moderate' and acceptable.

H05 – ‘Loss of GCS HMI’: as for hazard H04 in the U-space matrix, but the probability of hazard H05 consequences occurrence has been assessed as ‘Improbable’ (2) and the risk as ‘Moderate’ due to the operation of RPAS expected to be technically more advanced. The proposed mitigation actions shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H06 – ‘Loss of GCS monitoring displays’: the probability of occurrence of hazard H06 consequences has been estimated as ‘Remote’ (3) on the basis of items GCSHMISS6a and GCSHMISS6b with estimated probability of occurrence level estimated as D (Remote) in the FMECA analysis (Table 71) and on the basis of the hazard ‘Loss of RPA on board systems monitoring/telemetry due to GCS displays failure’ with probability of occurrence estimated as ‘B’. The severity of hazard H06 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction; the risk associated to hazard H06 has been assessed as ‘Moderate’ and acceptable; to further decrease the risk, the proposed mitigation action is to immediately terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not; the mitigation action shall reduce the hazard H06 consequences severity from ‘Catastrophic’ to ‘Minor’ (with reference to the use of emergency procedures) and the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H07 – ‘Deviation from steady-state (not-accelerating) flight condition’: as for hazard H05 in the U-space matrix, but the probability of hazard H07 consequences occurrence has been assessed as ‘Improbable’ (2) and the risk as ‘Moderate’ due to the operation of RPAS expected to be technically more advanced. The proposed mitigation actions shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H08 – ‘Loss of Emergency Flight Termination System’: as for hazard H06 in the U-space matrix, but the probability of hazard H08 consequences occurrence has been assessed as ‘Improbable’ (2) and the risk as ‘Moderate’ due to the operation of RPAS expected to be technically more advanced. The proposed mitigation actions shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H09 – ‘Loss of “Return to Home” function’: as for hazard H07 in the U-space matrix.

H10 – ‘Impossibility to perform a go-around manoeuver’: the probability of occurrence of this hazard consequences has been estimated as ‘Occasional’ (4). The severity of hazard H10 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction; the risk associated to hazard H10 has been assessed as ‘High’ and unacceptable; the proposed mitigation action is to immediately terminate the flight using the parachute for smoother landing; the mitigation action shall reduce hazard H10 consequences severity from ‘Catastrophic’ to ‘Minor’ (with reference to the use of emergency procedures) and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H11 – ‘Loss of Mission plan’: as for hazard H08 in the U-space matrix, but the probability of hazard H11 consequences occurrence has been assessed as

‘Improbable’ (2) and the risk as ‘Low’ due to the operation of RPAS mission software expected to be more advanced and reliable.

H12 – ‘Loss of GPS signal’: as for hazard H09 in the U-space matrix.

H13 – ‘Loss of EGNOS signal’: as for hazard H10 in the U-space matrix.

H14 – ‘Drift from the mission plan’: as for hazard H11 in the U-space matrix, but the probability of hazard H14 consequence occurrence has been assessed as ‘Improbable’ (2) and the risk as ‘Moderate’ due to the operation of RPAS expected to be technically more advanced. The proposed mitigation actions shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H15 – ‘Loss of mission plan updating software functionality’: the probability of occurrence hazard H15 consequences occurrence has been estimated as ‘Remote’ (3). The severity of hazard H15 consequences, has been assessed as ‘Hazardous’ potentially leading to a large reduction in safety margins; the risk associated to hazard H15 has been assessed as ‘Moderate’ and acceptable; the proposed mitigation action is to immediately terminate the flight using the parachute for smoother landing; the mitigation action shall reduce the probability of H15 hazard consequences from ‘Hazardous’ to ‘Minor’ (with reference to the use of emergency procedures) and the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H16 – ‘Lack of communication of mission plan updating to ATC’: the probability of occurrence of hazard H16 consequences has been estimated as ‘Remote’ (3). The severity of hazard H16 consequences, has been assessed as ‘Hazardous’ potentially leading to a large reduction in safety margins; the risk associated to hazard H16 has been assessed as ‘Moderate’ and acceptable; the proposed mitigation action is to increase the remote pilot training; the mitigation action shall reduce the probability of occurrence of H16 hazard probability of occurrence from ‘Remote’ to ‘Improbable’ and the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H17 – ‘Loss of uplink channel of the RPAS radio link’: as for hazard H12 in the U-space matrix, but the probability of occurrence of hazard H17 consequences has been assessed as ‘Remote’ (3) due to the operation of RPAS expected to be technically more advanced and, with reference to hazard H17 with a more robust radio link. The proposed mitigation actions shall reduce the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H18 – ‘Loss of downlink channel of the RPAS radio link’: as for hazard H13 in the U-space matrix, but the probability of occurrence of hazard H18 consequences has been assessed as ‘Remote’ (3) due to the operation of RPAS expected to be technically more advanced and, with reference to hazard H18 with a more robust radio link. The proposed mitigation actions shall reduce the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H19 – ‘Loss of ADS-B’: as for hazard H14 in the U-space matrix, but the probability of occurrence of hazard H19 consequences has been assessed as ‘Improbable’ (2) and the risk as ‘Moderate’ due to the operation of RPAS expected to be technically more advanced. The proposed mitigation actions is to provide a redundant ADS-B on board the RPA; the proposed mitigation actions

shall reduce the hazard H19 consequences probability of occurrence from 'Improbable' to 'Extremely improbable'; the residual risk remains 'Moderate' and acceptable.

H20 – 'Loss of communication with ATC': the probability of occurrence of this hazard consequences has been estimated as 'Remote' (3). The severity of H20 hazard consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction; the risk associated to hazard H20 has been assessed as 'High' and unacceptable; the proposed mitigation action is to switch and immediately and rely on controller-pilot data link communication channel; the mitigation action shall reduce hazard H20 consequences probability of occurrence from 'Remote' to 'Improbable' and the residual risk from 'High' to 'Moderate' and acceptable.

H21 – 'Presence of natural obstacle': as for hazard H15 in the U-space matrix.

H22 – 'Presence of man-made manufactures': as for hazard H16 in the U-space matrix.

H23 – 'Mid-air collision with other aircraft': as for hazard H17 in the U-space matrix.

H24 – 'Loss of DAA functionality': the probability of occurrence of this hazard consequences has been estimated as 'Improbable' (2). The severity of H20 hazard consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction; the risk associated to hazard H20 has been assessed as 'High' and unacceptable; the proposed mitigation action is to switch on redundant DAA subsystem; the mitigation action shall reduce the probability of occurrence of hazard H20 consequences from 'Improbable' to 'Extremely improbable'; the residual risk remains 'Moderate' and acceptable.

H25 – 'No detectability from other airspace users': the probability of occurrence of this hazard consequences has been estimated as 'Remote' (3). The severity of H20 hazard consequences, has been assessed as 'Catastrophic' potentially leading to RPA destruction; the risk associated to hazard H20 has been assessed as 'High' and unacceptable; the proposed mitigation action is to equip RPA with ADS-B equipment; the mitigation action shall reduce the consequences severity of hazard H20 from 'Catastrophic' to 'Minor' (nuisance) and the residual risk from 'High' to 'Moderate' and acceptable.

H26 – 'Cooperative traffic intrusion': as for hazard H20 in the U-space matrix, but the probability of hazard H26 consequences occurrence has been assessed as 'Remote' (3) and the risk as 'Moderate' and acceptable due to the expected operation of more skilled crews. The proposed mitigation actions shall reduce the residual risk from 'High' to 'Moderate' and acceptable.

H27 – 'Not cooperative traffic intrusion': as for hazard H21 in the U-space matrix, but the probability of hazard H27 consequences occurrence has been assessed as 'Remote' (3) and the risk as 'Moderate' and acceptable due to the expected operation of more skilled crews. The proposed mitigation actions shall reduce the residual risk from 'High' to 'Moderate' and acceptable.

H28 – 'Missed cooperative traffic tracking': as for hazard H22 in the U-space matrix, but the probability of hazard H28 consequences occurrence has been

assessed as ‘Improbable’ (2) and the risk as ‘Moderate’ and acceptable due to the operation of RPAS expected to be technically more advanced. The proposed mitigation actions shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H29 – ‘Missed not cooperative traffic tracking’: as for hazard H23 in the U-space matrix, but the probability of hazard H29 consequences occurrence has been assessed as ‘Improbable’ (2) and the risk as ‘Moderate’ and acceptable due to the operation of RPAS expected to be technically more advanced. The proposed mitigation actions shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H30 – ‘Collision with cooperative traffic’: as for hazard H24 in the U-space matrix, but the probability of hazard H30 consequences occurrence has been assessed as ‘Improbable’ (2) and the risk as ‘Moderate’ due to the operation of RPAS expected to be technically more advanced. The proposed mitigation actions shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H31 – ‘Collision with not cooperative traffic’: as for hazard H24 in the U-space matrix, but the probability of hazard H31 consequences occurrence has been assessed as ‘Improbable’ (2) and the risk as ‘Moderate’ and acceptable due to the operation of RPAS expected to be technically more advanced. The proposed mitigation actions shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H32 – ‘Missed performance of collision avoidance manoeuvre’: as for hazard H26 in the U-space matrix, but the probability of hazard H32 consequences occurrence has been assessed as ‘Remote’ (3) due to the operation of RPAS expected to be technically more advanced and the risk as ‘High’. The proposed mitigation actions shall reduce the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H33 – Missed monitoring of performance of collision avoidance manoeuvring: as for hazard H27 in the U-space matrix, but the probability of occurrence of hazard H33 consequences occurrence has been assessed as ‘Remote’ (3) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Moderate’and acceptable. The proposed mitigation actions shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H34 – ‘Missed weather awareness capability’: as for hazard H28 in the U-space matrix, but the probability of occurrence of hazard H34 consequences has been assessed as ‘Improbable’ (2) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Moderate’ and acceptable. The proposed mitigation actions shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H35 – ‘Missed gathering of contingent weather information’: as for hazard H28 in the U-space matrix, but the probability of occurrence of hazard H35 consequences has been assessed as ‘Improbable’ (2) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Moderate’. The

proposed mitigation actions shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H36 – ‘Missed avoidance of adverse weather’: as for hazard H30 in the U-space matrix, but the probability of occurrence of hazard H36 consequences has been assessed as ‘Improbable’ (2) due to the operation of RPAS expected to be technically more advanced as ‘Moderate’ and acceptable. The proposed mitigation actions shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H37 – ‘Loss of RPAS subsystems health and status monitoring’: as for hazard H31 in the U-space matrix, but the probability of occurrence of hazard H37 consequences has been assessed as ‘Improbable’ (2) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Moderate’ and acceptable. The proposed mitigation actions is to increase RPAS health subsystem maintenance on ground; the proposed mitigation action shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H38 – ‘Loss of communication while transiting from LOS to BRLOS and vice versa’: the probability of occurrence of this hazard consequences has been estimated as ‘Extremely improbable’ (1) due to the operation of RPAS expected to be technically more advanced. The severity of hazard H38 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction. The risk associated to hazard H38 has been assessed as ‘Moderate’ and acceptable. No further mitigation actions has been provided due to assigned probability of occurrence.

H39 – ‘Unintentional radio link interference’: as for hazard H33 in the U-space matrix, but the probability of occurrence of hazard H39 consequences has been assessed as ‘Improbable’ (2) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Moderate’. The proposed mitigation actions is to increase RPAS health subsystem maintenance on ground; the proposed mitigation action shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H40 – ‘Malicious radio link jamming’: as for hazard H34 in the U-space matrix, but the probability of occurrence of hazard H40 consequences has been assessed as ‘Remote’ (3) due to the operation of RPAS expected to be technically more advanced and the risk as ‘High’. The proposed mitigation actions is to increase RPAS health subsystem maintenance on ground; the proposed mitigation action shall reduce the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H41 – ‘Malicious radio link spoofing’: as for hazard H35 in the U-space matrix, but the probability of occurrence of hazard H41 consequences has been assessed as ‘Remote’ (3) due to the operation of RPAS expected to be technically more advanced and the risk as ‘High’. The proposed mitigation actions is to increase RPAS health subsystem maintenance on ground; the proposed mitigation action shall reduce the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H42 – ‘Fire’: as for hazard H36 in the U-space matrix, but the probability of occurrence of hazard H42 consequences has been assessed as ‘Extremely improbable’ (1) due to the operation of RPAS expected to be technically more

advanced and the risk as ‘Moderate’. The proposed mitigation shall reduce the residual risk from ‘High’ to ‘Low’ and fully acceptable.

H43 – ‘Loss of RPAS autopilot’: as for hazard H37 in the U-space matrix, but the probability of occurrence of hazard H43 consequences has been assessed as ‘Extremely improbable’ (1) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Moderate’. The proposed mitigation shall reduce the residual risk from ‘High’ to ‘Low’ and fully acceptable.

H44 – ‘Loss of electrical power’: as for hazard H38 in the U-space matrix, but the probability of occurrence of hazard H44 consequences has been assessed as ‘Extremely improbable’ (1) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Moderate’. The proposed mitigation shall reduce the residual risk from ‘High’ to ‘Low’ and fully acceptable.

H45 – ‘Loss of inertial platform’: as for hazard H39 in the U-space matrix, but the probability of occurrence of hazard H45 consequences has been assessed as ‘Extremely improbable’ (1) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Low’. No further mitigation actions are requested.

H46 – ‘Loss of heading indication’: as for hazard H40 in the U-space matrix, but the probability of occurrence of hazard H46 consequences has been assessed as ‘Extremely improbable’ (1) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Low’. No further mitigation actions are requested.

H47 – ‘Loss of altitude indication’: as for hazard H41 in the U-space matrix, but the probability of occurrence of hazard H47 consequences has been assessed as ‘Extremely improbable’ (1) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Moderate’. The proposed mitigation action is to switch on redundant altimeter; the proposed mitigation action shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H48 – ‘Loss of airspeed indication: the probability of occurrence of hazard H48 consequences has been assessed as ‘Extremely improbable’ (1) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Low’. No further mitigation actions are requested.

H49 – ‘Loss of pressure sensor failure’: as for hazard H42 in the U-space matrix, but the probability of occurrence of hazard H49 consequences has been assessed as ‘Extremely improbable’ (1) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Moderate’. The proposed mitigation action is to switch on redundant pressure sensor; the proposed mitigation action shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H50 – ‘Misleading altitude indication’: as for hazard H43 in the U-space matrix, but the probability of occurrence of hazard H50 consequences has been assessed as ‘Remote’ (3) due to the operation of RPAS expected to be technically more advanced and the risk as ‘High’. The proposed mitigation action is to switch on redundant alitmeter; the proposed mitigation action shall reduce the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H51 – ‘Misleading airspeed indication’: as for hazard H44 in the U-space matrix, but the probability of occurrence of hazard H51 consequences has been assessed as ‘Remote’ (3) due to the operation of RPAS expected to be technically more advanced and the risk as ‘High’. The proposed mitigation action is to switch on redundant altimeter; the proposed mitigation action shall reduce the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H52 – ‘Misleading indication of the angle of incidence’: as for hazard H45 in the U-space matrix, but the probability of occurrence of hazard H52 consequences has been assessed as ‘Improbable’ (2) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Moderate’. The proposed mitigation action is to switch on redundant pressure sensors or to immediately terminate the flight; the proposed mitigation action shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H52 – ‘Stall’: as for hazard H46 in the U-space matrix, but the probability of occurrence of hazard H52 consequences has been assessed as ‘Improbable’ (2) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Moderate’. The proposed mitigation action is to perform a proper diving corrective manoeuvre or to immediately terminate the flight; the proposed mitigation action shall reduce the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H54 – ‘Loss of fuel cell’: as for hazard H47 in the U-space matrix, but the probability of occurrence of hazard H54 has been assessed as ‘Improbable’ (2) due to the operation of RPAS expected to be technically more advanced and the risk as ‘Moderate’ and acceptable. The proposed mitigation action is to switch on LiPo batteries; the proposed mitigation action shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H55 – ‘Loss of fuel’: the probability of occurrence of this hazard consequences has been estimated as ‘Remote’ (3) with reference to item FSS1 of the FMECA analysis, ‘Structural damage’ of the fuel tank, that causes loss of fuel (Table 52). The severity of hazard H55 consequences, has been assessed as ‘Catastrophic’ potentially leading to RPA destruction. The risk associated to hazard H55 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to immediately terminate the flight using the FTS. The mitigation action shall reduce the hazard consequences from ‘Catastrophic’ to ‘Minor’ (due to the use of emergency procedures) and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H56 – ‘Remote pilot low training’: as for hazard H48 in the U-space matrix, but the probability of occurrence of hazard H56 consequences has been assessed as ‘Remote’ (3) due to the expected operation of more skilled crews and the risk as ‘Moderate’ and acceptable. The proposed shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H57 – ‘Non-compliant operational procedures’: as for hazard H49 in the U-space matrix, but the probability of occurrence of hazard H57 consequences has been assessed as ‘Remote’ (3) due to the expected operation of more skilled crews

and the risk as ‘Moderate’ and acceptable. The proposed shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H58 – ‘Remote pilot loss of situational awareness’: as for hazard H50 in the U-space matrix, but the probability of occurrence of hazard H58 consequences has been assessed as ‘Remote’ (3) due to the expected operation of more skilled crews and the risk as ‘Moderate’ and acceptable. The proposed shall reduce the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H59 – ‘Human senses limitations’: as for hazard H51 in the U-space matrix.

H60 – ‘Remote pilot excessive workload’: as for hazard H52 in the U-space matrix.

H61 – ‘Loss of separation provision from the ATC’: the probability of occurrence of this hazard consequences has been estimated as ‘Remote’ (3): the severity of H61 hazard consequences, potentially leading to a large reduction in safety margins, has been assessed as ‘Hazardous’. The risk associated to hazard H61 has been assessed as ‘Moderate’ and acceptable. The proposed mitigation action is to provide DAA/LIDAR sensor on board the RPA against mid-air conflict/collision risks. The mitigation action shall reduce the entity of the hazard consequences from ‘Catastrophic’ to ‘None’, and the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H62 – ‘Loss of separation provision from the remote pilot’: the probability of occurrence of this hazard consequences has been estimated as ‘Occsional’ (4): the severity of H62 hazard consequences, potentially leading to a large reduction in safety margins, has been assessed as ‘Hazardous’. The risk associated to hazard H62 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to provide DAA/LIDAR sensor on board the RPA against mid-air conflict/collision risks. The mitigation action shall reduce the entity of the hazard consequences from ‘Catastrophic’ to ‘Negligible’, and the residual risk from ‘High’ to ‘Moderate’ and fully acceptable.

H63 – ‘Loss of separation provision from the remote pilot’: the probability of occurrence of this hazard consequences has been estimated as ‘Extremely improbable’ (1) with reference to hazard ‘ATC communication errors’ from human factor analysis (Table 141): the severity of H63 hazard consequences, potentially leading to a large reduction in safety margins, has been assessed as ‘Hazardous’. The risk associated to hazard H63 has been assessed as ‘Low’ and fully acceptable. No further mitigation actions are required.

H64 – ‘Erroneous execution of the separation provision instruction from the remote pilot’: the probability of occurrence of this hazard consequences has been estimated as ‘Occasional’ (4): the severity of H64 hazard consequences, potentially leading to a large reduction in safety margins, has been assessed as ‘Hazardous’. The risk associated to hazard H64 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to provide DAA/LIDAR sensor on board the RPA against mid-air conflict/collision risks and to increase the remote pilot training. The mitigation action shall reduce the probabilty of hazard H64 occurrence (increase of remote pilot training) and hazard H64 severity of

consequences from ‘Catastrophic’ to ‘Minor’ (due to the use of emergency procedures), and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H65 – ‘The RPAS does not comply or incorrectly responds to separation provision instruction issued by ATC’: the probability of occurrence of this hazard consequences has been estimated as ‘Remote’ (3): the severity of H65 hazard consequences, potentially leading to RPA destruction, has been assessed as ‘Catastrophic’. The risk associated to hazard H65 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to terminate the flight using the FTS if far from congested areas or using the parachute for smoother landing if not. The mitigation action shall reduce the hazard consequences from ‘Catastrophic’ to ‘Minor’ (due to the use of emergency procedures), and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H66 – ‘Remote pilot delayed response to separation provision instruction from ATC’: the probability of occurrence of this hazard consequences has been estimated as ‘Occasional’ (4): the severity of H66 hazard consequences, a significant reduction in safety margins, has been assessed as ‘Major’. The risk associated to hazard H66 has been assessed as ‘Moderate’ and acceptable. The proposed mitigation action is to increase the remote pilot training. The mitigation action shall reduce the hazard consequences severity from ‘Major’ to ‘Negligible’ (due to the use of emergency procedures), and the residual risk from ‘Moderate’ to ‘Low’ and fully acceptable.

H67 – ‘Excessive number of intentional deviations from separation provision instructions’: the probability of occurrence of this hazard consequences has been estimated as ‘Frequent’ (5): the severity of H65 hazard consequences, has been assessed as ‘Major’ with reference to a significant reduction in safety margins. The risk associated to hazard H67 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to increase the remote pilot training. The mitigation action shall reduce the hazard consequences probability of occurrence from ‘Frequent’ to ‘Remote’, and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H68 – ‘Missed submissionof flight plan to ATC’: the probability of occurrence of this hazard consequences has been estimated as ‘Occasional’ (4): the severity of H68 hazard consequences, has been assessed as ‘Hazardous’ with reference to a large reduction in safety margins. The risk associated to hazard H68 has been assessed as ‘High’ and unacceptable. The proposed mitigation action is to increase the remote pilot training. The mitigation action shall reduce the hazard consequences probability of occurrence from ‘Occasional’ to ‘Remote’, and the residual risk from ‘High’ to ‘Moderate’ and acceptable.

H69 – ‘Cloud’: the probability of occurrence of this hazard consequences has been estimated as ‘Frequent’ (5): the severity of H69 hazard consequences, has been assessed as ‘Negligible’ for IFR flights and ‘Minor’ (nuisance) for VFR flights. The risk associated to hazard H69 has been assessed as ‘Moderate’ and acceptable both for IFR and for VFR flights. The proposed mitigation action is to use the autopilot “Return to Home” function. The mitigation action shall reduce

the hazard consequences severity from ‘Minor’ to ‘Negligible’ for VFR flights; the residual risk remains ‘Moderate’ and acceptable both for IFR and VFR flights.

H70 – ‘Fog’: the probability of occurrence of this hazard consequences has been estimated as ‘Occasional’ (4): the severity of H70 hazard consequences, has been assessed as ‘Negligible’ for IFR flights and ‘Minor’ (nuisance) for VFR flights. The risk associated to hazard H70 has been assessed as ‘Moderate’ and acceptable both for IFR and for VFR flights. The proposed mitigation action is to use the autopilot “Return to Home” function. The mitigation action shall reduce the hazard consequences severity from ‘Minor’ to ‘Negligible’ for VFR flights; the residual risk remains ‘Moderate’ and acceptable both for IFR and VFR flights.

H71 – ‘Freezing rain’: the probability of occurrence of this hazard consequences has been estimated as ‘Remote’ (5): the severity of H71 hazard consequences, has been assessed as ‘Catastrophic’ both for IFR and VFR flights. The risk associated to hazard H71 has been assessed as ‘High’ and unacceptable both for IFR and for VFR flights. The proposed mitigation action is to use the autopilot “Return to Home” function. The mitigation action shall reduce the hazard consequences severity from ‘Catatrophic’ to ‘Negligible’ and the residual risk from ‘High’ to ‘Low’ and fully acceptable both for IFR and VFR flights.

H72 – ‘Glare’: the probability of occurrence of this hazard consequences has been estimated as ‘Occasional’ (4): the severity of H72 hazard consequences, has been assessed as ‘Negligible’ both for IFR and VFR flights due to the absence of the remote pilot onboard. The risk associated to hazard H72 has been assessed as ‘Moderate’ and unacceptable both for IFR and for VFR flights. The proposed mitigation action is to use the autopilot “Return to Home” function. The mitigation action shall reduce the hazard consequences severity from ‘Catatrophic’ to ‘Negligible’ and the residual risk from ‘High’ to ‘Low’ and fully acceptable both for IFR and VFR flights.

H73 – ‘Haze’: the probability of occurrence of this hazard consequences has been estimated as ‘Occasional’ (4): the severity of H73 hazard consequences, has been assessed as ‘Negligible’ for IFR flights and ‘Minor’ (nuisance) for VFR flights. The risk associated to hazard H73 has been assessed as ‘Moderate’ and acceptable both for IFR and for VFR flights. The proposed mitigation action is to use the autopilot “Return to Home” function. The mitigation action shall reduce the hazard consequences severity from ‘Minor’ to ‘Negligible’ for VFR flights; the residual risk remains ‘Moderate’ and acceptable both for IFR and VFR flights.

H74 – ‘Humidity’: the probability of occurrence of this hazard consequences has been estimated as ‘Frequent’ (5): the severity of H73 hazard consequences, has been assessed as ‘Negligible’ for the RPA expected to fly certified operations. The risk associated to hazard H73 has been assessed as ‘Moderate’ and acceptable. No further mitigation actions have been foreseen.

H75 – ‘Ice’: the probability of occurrence of this hazard consequences has been estimated as ‘Occasional’ (4): the severity of H73 hazard consequences, has been assessed as ‘Catastrophic’ both for IFR and VFR flights. The risk associated to hazard H73 has been assessed as ‘High’ and unacceptable. For both IFR and VFR flights, the proposed mitigation action is to forbid the flight mission until

when optimal weather conditions are restored. The mitigation action shall reduce the hazard consequences severity from 'Catastrophic' to 'Negligible' (few consequences) and the residual risk from 'High' to 'Moderate' and acceptable.

H76 – 'Rain': as for Hazard H60 of the U-space matrix with reference to both IFR and VFR flights.

H77 – 'Snow': as for Hazard H61 of the U-space matrix with reference to both IFR and VFR flights.

H78 – 'Solar storm': as for Hazard H62 of the U-space matrix with reference to both IFR and VFR flights.

H79 – 'Temperature': as for Hazard H63 of the U-space matrix with reference to both IFR and VFR flights; but the severity of consequences of hazard H79 have been considered negligible the RPA expected to fly certified operations. The risk associated to hazard H79 has been ranked as 'Moderate'; no futher mitigation provision has been foreseen.

H80 – 'Turbulence': as for Hazard H64 of the U-space matrix with reference to both IFR and VFR flights.

H81 – 'Wind': as for Hazard H65 of the U-space matrix with reference to both IFR and VFR flights.

H82 – 'Lightning strike': as for Hazard H66 of the U-space matrix with reference to both IFR and VFR flights.

H83 – 'Hail': as for Hazard H67 of the U-space matrix with reference to both IFR and VFR flights.

H84 – 'Hurricanes': as for Hazard H68 of the U-space matrix with reference to both IFR and VFR flights.

H85 – 'Volcanic ash': as for Hazard H69 of the U-space matrix with reference to both IFR and VFR flights.

3.3 RPAS risk mitigation strategies

The general indications for mitigation strategies are reported in the U-Space and ATM risk matrices (Table 143 and Table 144). Further evaluations better specifying threats and escalation factors have been carried out using the Bow Tie Methodology.

3.3.1 Residual risk

With reference to both the U-Space and the ATM risk matrices, the mitigation provisions have been determined in such a way that the residual risk was ultimately downgraded to an acceptable level (low or moderate, Table 143 and Table 144).

3.3.2 The Bow Tie methodology

The whole of the U-Space and ATM risk matrices accomplishes the identification of hazard risks for operations of RPAS integrated in the civil not

segregated airspace from ground to flight level FL600 and beyond covering both uncontrolled and controlled airspace. From this point onwards, starting from the Bow Tie analysis, the research has been focused on RPAS capable of specific category operations in the VLL subspace under U-Space service only. In fact, this scenario involving light RPAS will be the most representative one in the nearest future: following EASA work intentions, the specific category RPAS operations will immediately cover routine commercial flights; the certified category operations are defined theoretically only at the moment and, by definition, for they high complexity, they need more advanced regulations and operational infrastructures to be performed maintain hazards at or below an acceptable level.

The Bow Tie Analysis has been performed considering for each main group of hazards of Table 143 the most significant one identifying the top event related to the given hazard and the associable treats/barriers and escalation factors/barriers.

The analysis has been carried out following the conceptual scheme reported in Figure 12; the results have been reported in Appendix E (Figure 61 ÷ Figure 74).

3.4 Conclusions

In accordance with the definition of Safety Management System in aviation [3] and in accordance with the ICAO regulations for which every aeronautical operator shall manage the safety of its assets and operations according to a Safety Management System ([1] and [2]), the risk analysis described in this chapter has identified safety hazards and mitigation provisions to maintain risks generated by the integration of RPAS into the civil not segregated airspaces at or below an acceptable level.

The analysis has been further developed focusing on the concern of mitigating safety hazards. From this stage on, the work has been focused on the specific category RPAS operations scenario only, as the first one that will be deployed n the next future.

This second part of the research work starts considering the ‘Expert Systems’, as described in Chapter 4.

Chapter 4

‘Expert Systems’

4.1 Introduction

The U-Space risk matrix content has been exploited to implement the knowledge basis for a rule-based ‘Expert System’. It has been deemed that an ‘Expert System’ can provide the basis for an effective active mitigation provision to be integrated with autopilot software functionalities to support the remote pilot decision making process in case of in-flight hazard occurrence during specific category RPAS flight operations or to act autonomously in case of certified category RPAS flight operations.

An ‘Expert System’ is a software programmed to emulate the human experts judgment in a field of knowledge. An ‘Expert System’ initial stage (basis of knowledge) has been developed starting from the U-space risk matrix to provide the remote pilot with a dynamic and flexible tool to support his/her decision making process about the solution of RPAS in-flight safety hazards in case of their occurrence.

4.2 ‘Expert Systems’

The ‘Expert Systems’ are a sub-set of computer systems programmed with ‘Artificial Intelligence’ software capable of emulating the human experts: in fact they are designed and implemented to provide the user with support in decision-making thanks to the experience gained in a field (or domain) of knowledge. Further, similarly to experienced human beings, the ‘Expert Systems’ can find the solution of complex problems operating on the acquired body of knowledge [89].

The architecture of an ‘Expert System’ is mainly composed of (Figure 22 [90]):

- The knowledge basis
- The inference engine

- The user, who cannot be expert of the considered domain of knowledge

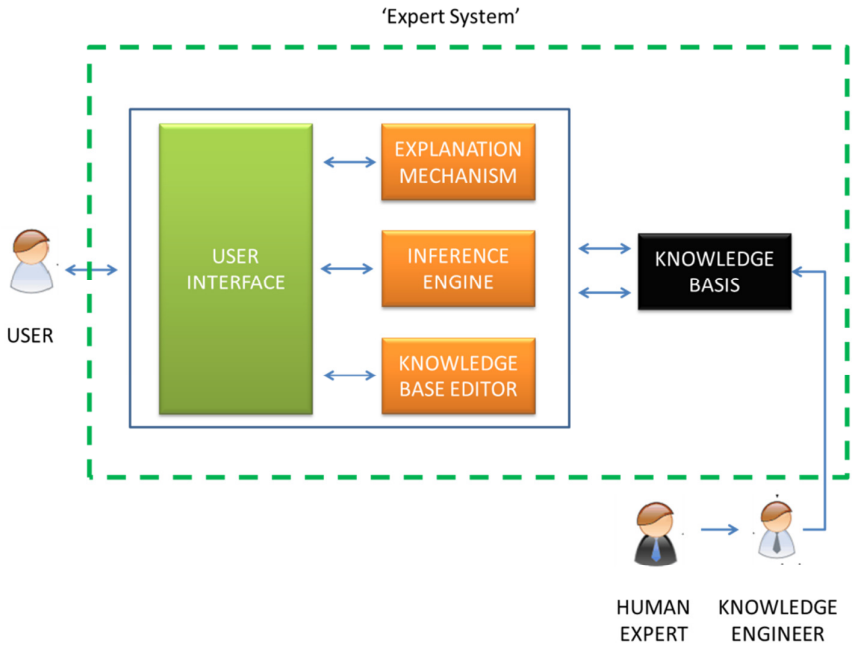


Figure 22 – 'Expert System' concept [90]

An 'Expert System' is high performant, understandable, reliable and high responsive. In general they are programmed to be capable of emulating human processes like advising, assisting human persons in decision making against very complex problems, deriving solutions, performing diagnoses, providing explanations, interpreting inputs, predicting results, justifying conclusions or suggesting alternative conclusion for a given problem. On the contrary, the 'Expert Systems' are not able to substitute the human being in taking decision, to possess human capabilities, to autonomously take decision or to autonomously refine their knowledge on issues related to a domain they have not been properly taught about [89].

The knowledge basis comprehends facts, data, as collection of facts, and information based on data and facts. The knowledge based on information is classified as factual; the knowledge based on practice, judgment, one's ability to evaluate and guessing is classified as heuristic [91]. The process of instructing the 'Expert System' through the acquisition of knowledge is actuated using simple 'rules' formally expressed according to the logical sequence 'IF - THEN'. This statement subtends 'IF a given condition occurs', 'THEN this action will follow'. The knowledge database made up as above described are defined 'rule-based' 'Expert Systems' class and they are of interest for this work. Other 'Expert Systems' implemented according to different criteria are out of the scope of this work.

The ‘Expert System’ deduces new facts from previous ones through the deduction processes implemented in the inference engine. The inference engine can be assimilate to the reasoning part of the ‘Expert System’ [92]: in fact the ‘inference’ refers to the logical process of explicitly ‘drawing a consequence’; conceptually, it is a logical process opposite to the ‘implication’ which implicitly attains to a consequence. Two typologies of inference processes can be applied while implementing an ‘Expert System’: forward chaining and backward chaining (Figure 23) [91]. In the first case the inference engine leads the user from the facts to the conclusion through the rules; in the latter the facts are deduced from the conclusion though the rules.

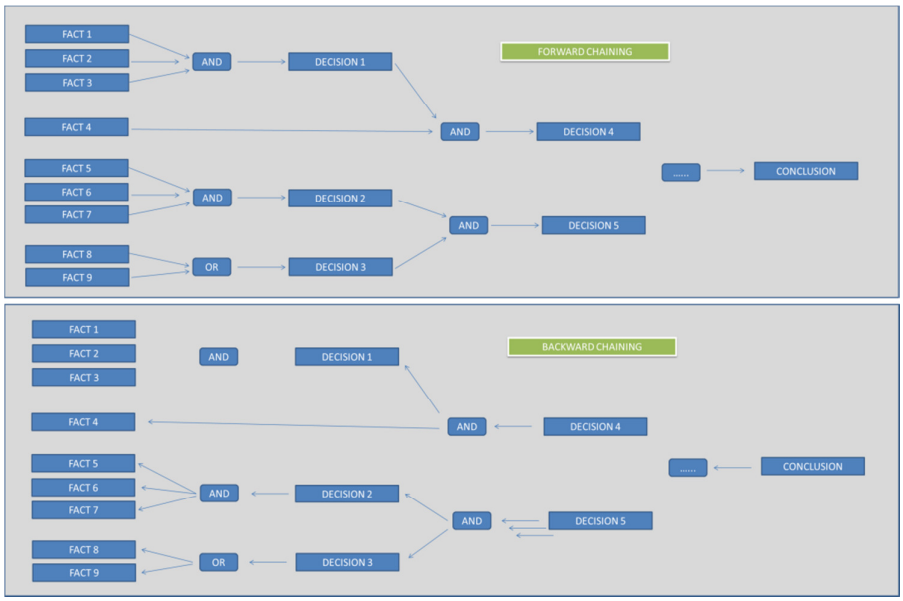


Figure 23 – ‘Expert System’ inference engine forward/backword chaining [91]

In general, opportunistic strategies consisting of mixing some forward chaining with some other backward chaining in an adaptable way are recommended to get more flexibility of the ‘Expert System’ associated to the designed inference engine [92]. Further, the inference engine can reiterate the inference process to obtain facts generating new facts and thus increasing the level of knowledge of the ‘Expert System’ [91]. In case of conflicts caused by multiple rules applied to the same case, the inference engine is able to solve them. On a secondary level, the ‘Expert Systems’ include the ‘explanation’ sub-system responsible of providing the explanation for a given inference rule [92].

The user, usually a person who is not expert of the given domain of knowledge, approaches the ‘Expert System’ to solve a problem by mean of a user interface towards the machine. The user interface shall be friendly and simple to be operated like for instance an interactive dialogue system which asks questions to the ‘Expert System’ and this one forwards the answers as ‘information’ or ‘facts’ to the inference engine for further processing [92] outputting a conclusion for the user decisional process. The inference rules are previously stored in the

knowledge database by the knowledge engineer who determines the architecture of the database, identifies the rules and implements the knowledge database [92].

The following main 'Expert Systems' operational limitations are presented and discussed because of interest for this research work. There are limitations on the level of knowledge in a given domain: the knowledge can be incomplete or affected by uncertainty for which mitigation measures like weight age factors or statistical approaches are used to compensate knowledge incompleteness and uncertainty. With reference to the level of knowledge, the implementation of an 'Expert System' for each possible task within a domain is impossible; the 'Expert Systems' are not able to identify erroneous facts or information introduced in the knowledge database; the 'Expert Systems are not able to know and be aware about their own state, scope and limitations. The unit of measure of 'Expert Systems' size is the 'rule'; the highest is the database size, the highest is the number of rules that compose it and the highest will be the time to attain a conclusion and to take a decision from the user perspective [93] and the more complex will be the maintenance as well as development costs [92]. The 'Expert System' maintenance consists of the existing source code updating/debugging and of knowledge basis upgrading according to the eventual latest development occurred in the domain of knowledge the 'Expert System' refers to. The updating of knowledge can further include new interfaces addition with other information systems if any [92].

The advantages in the 'Expert Systems' are that they work in a similar way to the human reasoning, but, with time, they do not become old and make mistakes and, in general, the probability of risk occurring in evaluations is lower than relying on human beings mind; further, they operate without getting motional, tensed or fatigued [93]. Finally, the 'Expert Systems' can be used in dangerous environment (as RPAS, Paragraph 1.2.2) thus avoiding human beings exposure; on the other hand, their adaptability depends upon the knowledge basis architecture design.

The rule-based 'Expert Systems' based on 'IF – THEN' statements are usually programmed with the 'CLIPS' tool developed by NASA [94].

4.3 Why 'Expert Systems' for RPAS

It has been conceived to draft the knowledge basis of a rule-based 'Expert System' as basis for the future implementation of affordable mitigation provisions based on artificial intelligence to support the RPAS remote pilot decision making process when a hazard occurs within the scenario of specific category flight operations into the VLL uncontrolled subspace under the U-Space service.

4.4 Architecture of the proposed 'Expert Systems'

The rule-based 'Expert System' proposed in this work is directly correlated with the U-Space risk matrix: the content of each hazard of the matrix (Table 143) has been developed into one or more 'IF – THEN' statements allowing to develop

a set of rules to be activated or de-activated according to the indications and warnings issued by the RPAS about occurring in flight hazards.

The high level architecture of the 'Expert System' merged with the RPAS is showed in Figure 24.

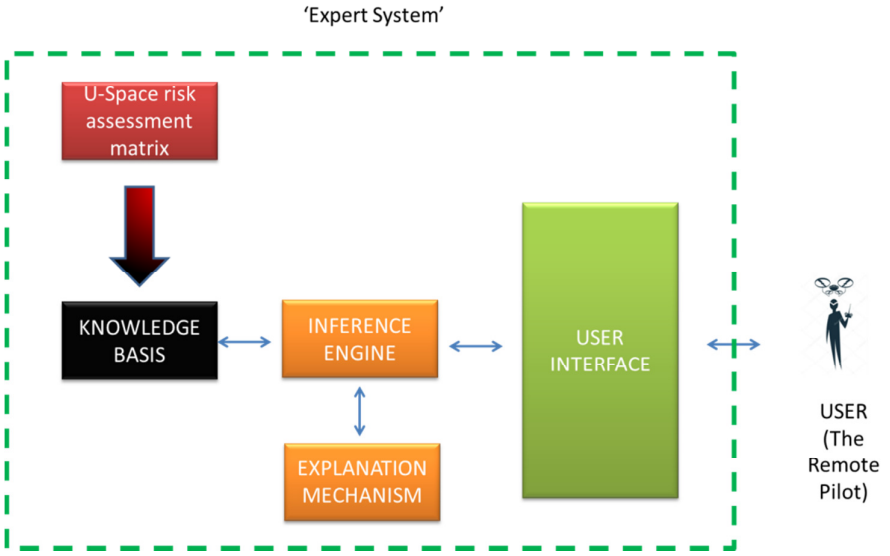


Figure 24 – RPAS 'Expert System' high level architecture

4.4.1 The knowledge basis

The knowledge basis of the considered 'Expert System' has been implemented with rules derived from the U-Space risk matrix content (Table 143). Each assessed hazard has been transposed into a 'IF – THEN' statement with the following meaning: 'IF <condition> THEN <statement>'. The 'condition' is the hazard content expressed with other conditions; the 'statement' or 'conclusion' corresponds to the mitigation action proposed by the risk matrix even integrated with further suggestions derived from the Bow Tie analysis (Table 143 and Appendix E contents, respectively). The 'conclusion' also reports the warn about the resulting initial and residual hazard classification.

All the U-Space hazards have been transposed into a rule or a set of rules except the following ones: hazards related to electromagnetic interference (Hazard H33), hazards related to cybersecurity (Hazards H34 and H35), hazards related to human factor (Hazards number H27, H28, and Hazards H48 ÷ H52), hazards not applicable to the hybrid rotor wing RPAS model conjectured to implement the rules and finally some hazards related to adverse weather conditions (Hazards H53 ÷ H59 and Hazards H63 ÷ H69).

In these cases, other solutions rather than an 'Expert System' rule have been judged as more proper to be implemented to mitigate risks for the mentioned hazards:

- Unintentional electromagnetic interference: geofence or proper operational procedures can be foreseen to avoid altogether RPAS

operations nearby VORs, airports (as already requested by current RPAS national regulations), television broadcasting stations and similar infrastructures

- Jamming and spoofing attacks: proper cybersecurity strategies at electronic, information and telecommunication level shall be designed to avoid random malicious control of the RPAS; the scientific and technical community is actively working on this concern
- Human factor: wearable sensors to measure and monitor physiological parameters related to fatigue and emotional stress can be used to warn the remote pilot on potential hazardous conductance and management of the flight operation; an 'Expert System' tailored on human physiology and human factor correlated with unmanned flight operations is an example of future works on issues generated by the incoming intensive use of RPAS for aerial work. Another possible solution for mitigation of hazards related to human factor, often suggested in this work (FMECA analysis, Appendix A), is the provision of proper training for remote pilot/crew to become more and more familiar with remote aircraft piloting techniques and hidden pitfalls

An index has been defined and used in Appendix F (Table 145) to take into consideration the ground risk component of RPAS specific category operations. This index is derived from the ground risk assessment elaborated by JARUS within the 'Specific Operations Risk Assessment' (SORA) documentation package ([95], Paragraph 3.2.3, Figure 2). Such index considers both the combination of the following flight modalities:

- RLOS operations: operations conducted in Visual Line of Sight of the remote pilot with respect to the RPA
- BRLOS operations: operations conducted with the RPA flying Beyond Visual Line of Sight with respect to the remote pilot

and the characteristics of the overflown area, in terms of controlled/not controlled areas and population density, foreseeing and distinguishing the following cases:

- Controlled area, located inside a sparsely populated environment
- Sparsely populated environment (overflown areas uniformly inhabited)
- Controlled area, located inside a populated environment
- Populated environment
- Areas with gathering of people

Further, depending the ground risk depends on the characteristic size of the flying RPA, four ranges of types of RPA representative characteristic sizes have been defined; then the intrinsic ground risk has been described accordingly. These

conditions have been combined according to an increasing risk-based criterion and mixed with the safety related content of the draft rules (Appendix F).

All the variables used to write the rules have been defined and reported in Appendix F before the list of rules.

All the draft rules have been collected in Appendix F.

4.4.2 The inference engine

In the present case a simple forward chaining approach has been used for the inference engine: each rule starts with a series of conditions explicitly including the hazard content and ends with the final conclusion that notifies the gravity of the hazard to the remote pilot and suggests him/her the proper recommended mitigation to reduce the consequences of the hazard occurrence.

4.4.3 The integration of the 'Expert System' with the RPAS

A proposal for the integration of an 'Expert System' with the RPAS autopilot software capable of performing specific operations is shown in Figure 25.

According to the external inputs, the 'Expert System' activates or deactivates the rule(s) related to a given hazard predefined and stored in the knowledge basis and suggests the remote pilot the best conclusion/mitigation action to solve the contingent risk situation on the basis of proper assigned control variables. The control variables physically can be signals generated by monitoring or failure sensors properly arranged in advance on board the RPAS (Figure 25).

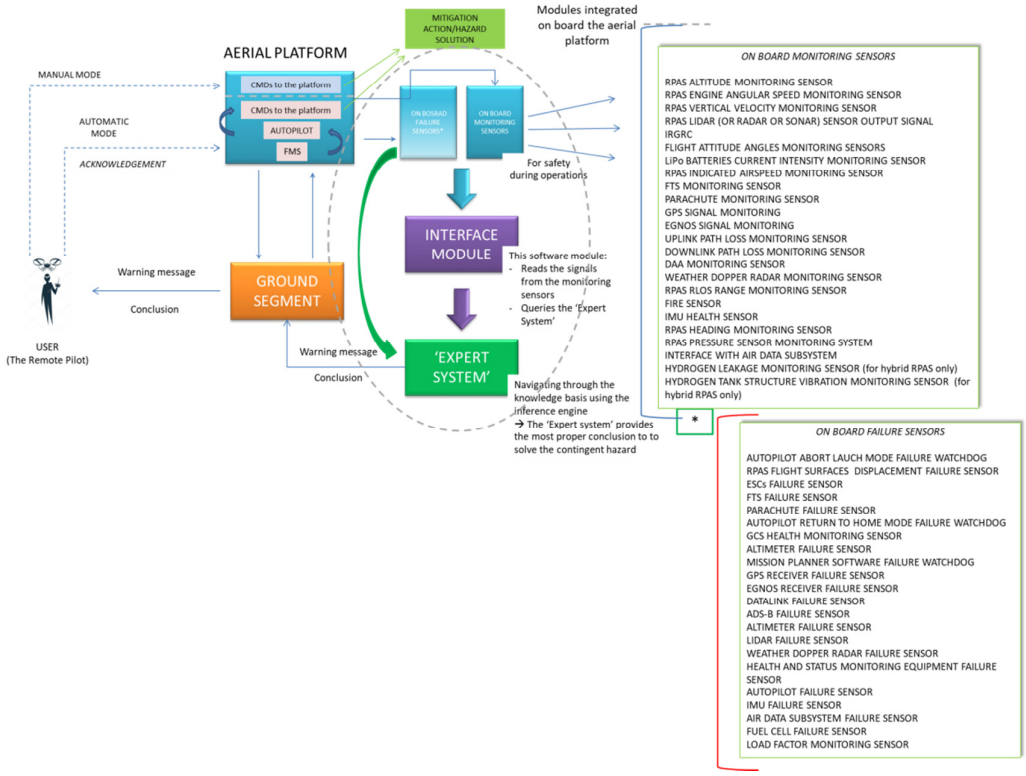


Figure 25 – Integration of the 'Expert system' with the RPAS autopilot software

An on board monitoring unit interfaces with safety critical equipment/subsystems sensors. The signals generated by the monitoring sensors indicated in Figure 25 replicate the input variables used into the rules (Appendix F).

Each variable is monitored during flights and sent to the interface module which plays the role of the user querying the 'Expert System'. According to the combination of values of the monitored variables, navigating through the knowledge basis, the inference engine generates a warning message and a conclusion. Both these information are sent to the remote pilot on ground to warn him on what is happening to the platform, the related risk range description (as assessed in Table 143) and the proposed conclusion/hazard mitigation provision (as assessed in Table 143). From the perspective of the remote pilot the conclusion identified by the 'Expert System' is the suggested mitigation action to solve the hazard and preserve the RPA from an accident occurrence.

Two levels of integration of 'Expert Systems' with RPAS autopilots software have been conceived:

- A basic level of integration, where the remote pilot holds the full remote manual control of the flying RPA. The 'Expert System' supports as above described the remote pilot in solving the in-flight hazards, but the remote pilot and not the autopilot remains in command of the aerial platform
- An advanced level of integration, where the RPA automatically solves the in-flight hazards: the autopilot dialogues with the 'Expert Systems' and directly acts on the aerial platform; this solution has been deemed more suitable for very complex flight missions where a more promptly and quick solution of the hazards than human capability could save the RPA from hazards consequences effects

4.4.3 The verification of the knowledge basis of the 'Expert System'

From the perspective of the system engineering, the knowledge basis is the most critical component of the 'Expert System' for which a good design is necessary. The operation of the 'Expert System' relies on the truth, completeness, correctness and consistency of the knowledge basis.

At this very early stage of RPAS operations, a coverage/consistency verification of the rules content with respect to the hazard conditions identified as main core of the performed safety analysis on RPAS has been carried out. The FMECA, FTA and human factor analyses results have been used in support of the verification in object.

4.4.4 Rules coverage verification: results and discussion

Table 13 sums up the results of rules consistency and coverage verification.

Table 13 – 'Expert System' rules coverage/consistency verification against U-space matrix content

Hazard #	Definition	Rule	Control variables	Coverage/Consistency
RPAS Aviate functionality related hazards				
H01	Loss of abort launch capability	Hazard 01 Rules 1, 2	RPAS_ALT RPAS_ENGINE_OMEGA RPAS_RATE_OF_CLIMB RPAS_LIDAR_SENSOR_OUTPUT **RPAS_AUTOPILOT_ABORT_LAUNCH_MODE** IRGRC RPAS_RECOVERY_PARACHUTE_CMD	The loss of abort launch capability during take-off/launch in presence of a sudden obstacle has been considered → OK
H02	Loss of flight controls	Hazard 02 Rules 1, 2, 3, 4, 5, 6	**PITCH_CMD_LONGITUDINAL_SHIFT** **PITCH_CMD_ELECTRICAL_SIGNAL** **ROLL_CMD_LONGITUDINAL_SHIFT** **ROLL_CMD_ELECTRICAL_SIGNAL** **YWA_CMD_LONGITUDINAL_SHIFT** **YAW_CMD_ELECTRICAL_SIGNAL** RPAS_ENGINE_OMEGA RPAS_ALT IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	Pitch, roll and yaw commands have been considered → Ok
H03	Loss of propulsion	Hazard 03 Rules 1, 2, 3, 4, 5, 6	RPAS_ALT RPAS_ENGINE_OMEGA **RPAS_LIPO_BATTERY_CURRENT** **RPAS_ESC_FAILURE_SENSOR** IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	Loss of LiPo battery and ESC failure in case of LiPo battery correct operations have been considered → Ok
H04	Loss of GCS HMI	Hazard 04 Rules 1,2,3,4,5,6	**PITCH_CMD_LONGITUDINAL_SHIFT** **PITCH_CMD_ELECTRICAL_SIGNAL** **ROLL_CMD_LONGITUDINAL_SHIFT** **ROLL_CMD_ELECTRICAL_SIGNAL** **YWA_CMD_LONGITUDINAL_SHIFT** **YAW_CMD_ELECTRICAL_SIGNAL** RPAS_ALT RPAS_ENGINE_OMEGA IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The loss of Pitch, Roll and Yaw commands have been considered while the RPA is flying → Ok
H05	Deviation from steady-state (not-accelerating) flight condition	Hazard 05 Rules 1, 2, 3, 4, 5, 6, 7, 8	**WP_ALT** **RPAS_IAS** **RPAS_ALT** IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The cases of constant altitude with not constant airspeed and vice versa have been considered → Ok
H06	Loss of Emergency Flight Termination System	Hazard 06 Rules 1, 2	**RPAS_FTS_BIT** **RPAS_RECOVERY_PARACHUTE_BIT** **IRGRC** RPAS_AUTOPILOT_LANDING_MODE	The cases of recovery parachute and FTS failures have been considered → Ok
H07	Loss of "Return to home function"	Hazard 07 Rules 1, 2	**RPAS_AUTOPILOT_RETURN_TO_HOME_MODE** IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The error of autopilot "Return to Home" mode has been considered → Ok
RPAS Navigate functionality related hazards				
H08	Loss of mission plan	Hazard 08 Rules 1, 2	**RPAS_MISSION_PLAN** IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The loss of the mission plan functionality has been considered → Ok
H09	Loss of GPS signal	Hazard 09 Rules 1, 2, 3	**GPS_LAT** **GPS_LONG** **GPS_ALT** IRGRC RPAS_AUTOPILOT_RETURN TO HOME_MODE RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The freezing of GPS data has been considered → Ok
H10	Loss of EGNOS signal	Hazard 10 Rules 1, 2, 3	**EGNOS_LAT** **EGNOS_LONG** **EGNOS_ALT** IRGRC RPAS_AUTOPILOT_RETURN TO HOME_MODE RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The freezing of EGNOS data has been considered → Ok

Table 13 – 'Expert System' rules coverage/consistency verification against U-space matrix content (Cont'd)

Hazard #	Definition	Rule	Control variables	Coverage/Consistency
H11	Drift with respect to mission plan	Hazard 10 Rules 1, 2	**RPAS_LAT** **PLANNED_WP_LAT** **RPAS_LONG** **PLANNED_WP_LONG** **RPAS_ALT** **PLANNED_WP_ALT** IRGRC RPAS_AUTOPILOT_RETURN TO HOME_MODE RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The difference between the RPAS current position and the planned one has been considered → Ok
RPAS Communicate functionality related hazards				
H12	Loss of uplink channel of the RPAS radio link	Hazard H12 Rule 1	**RPAS_UPLINK_PATH_LOSS** RPAS_AUTOPILOT_RETURN TO HOME_MODE	The loss of uplink channel has been considered → Ok
H13	Loss of downlink channel of the RPAS radio link	Hazard H12 Rule 1	**RPAS_DOWNLINK_PATH_LOSS** RPAS_AUTOPILOT_RETURN TO HOME_MODE	The loss of uplink channel has been considered → Ok
H14	Loss of ADS_B	Hazard H13 Rule 1, 2	**RPAS_ADS-B_BIT** IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The falure diagnosis of ADS-B has been considered → Ok
RPAS hazards avoidance functionality related hazards				
H15	Presence of natural obstacles	Hazard H14 Rule 1	**RPAS_LIDAR_SENSOR_OUTPUT** **RPAS_DISTANCE_FROM_OBSTACLE**	The ue of LIDAR has been considered → Ok
H16	Presence of man-made manufactures	Hazard H15 Rule 1	**RPAS_LIDAR_SENSOR_OUTPUT** **RPAS_DISTANCE_FROM_OBSTACLE**	The ue of LIDAR has been considered → Ok
H17	Mid-air collision with other aircraft	Hazard H17 Rule 1	**RPAS_DAA_OUTPUT** **RPAS_LIDAR_SENSOR_OUTPUT** **RPAS_DISTANCE_FROM_OBSTACLE**	The ue of DAA and LIDAR has been considered → Ok
H18	Loss of DAA capability	Hazard H8 Rule 1, 2, 3, 4, 5, 6	**RPAS_ADS-B_BIT** **RPAS_ALTIMETER_BIT** **RPAS_EGNOS_BIT** IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The cases of at least aech DAA component failure has been considered → Ok
H19	No detectability from other airspace users	Hazard H18 Rule 1, 2	**RPAS_DAA_OUTPUT** **RPAS_LIDAR_SENSOR_OUTPUT** **RPAS_DISTANCE_FROM_OBSTACLE**	The ue of DAA and LIDAR has been considered → Ok
H20	Cooperative traffic intrusion	Hazard H19 Rule 1	**RPAS_DAA_OUTPUT** **RPAS_DISTANCE_FROM_OBSTACLE**	The ue of DAA has been considered → Ok
H21	Not cooperative traffic intrusion	Hazard H21 Rule 1	**RPAS_LIDAR_SENSOR_OUTPUT** **RPAS_DISTANCE_FROM_OBSTACLE**	The ue of LIDAR has been considered → Ok
H22	Missed cooperative traffic tracking	Hazard H22 Rule 1	**RPAS_DAA_OUTPUT** **RPAS_DISTANCE_FROM_OBSTACLE**	The ue of DAA has been considered → Ok
H23	Missed not cooperative traffic tracking	Hazard H23 Rule 1	**RPAS_LIDAR_SENSOR_OUTPUT** **RPAS_DISTANCE_FROM_OBSTACLE**	The ue of LIDAR has been considered → Ok
H24	Collision avoidance with cooperative traffic	Hazard H24 Rule 1	**RPAS_DAA_OUTPUT** **RPAS_DISTANCE_FROM_OBSTACLE**	The ue of DAA has been considered → Ok
H25	Collision avoidance with not cooperative traffic	Hazard H25 Rule 1	**RPAS_LIDAR_SENSOR_OUTPUT** **RPAS_DISTANCE_FROM_OBSTACLE**	The ue of LIDAR has been considered → Ok
H26	Missed performance of collision avoidance manoeuvre	Hazard H26 Rules 1, 2	**RPAS_DAA_OUTPUT** **RPAS_LIDAR_SENSOR_OUTPUT** **RPAS_DISTANCE_FROM_OBSTACLE** RPAS_FTS_CMD	The ue of DAA and LIDAR has been considered → Ok
	Missed monitoring of performance of collision avoidance manoeuvring			
H27	Missed performance of collision avoidance manoeuvre monitoring	This is an hazard condition related to human factor performance; no Expert System rules are deemed applicable in this case		
H28	Missed weather awareness capability	Hazard condition related to human factor performance: no Expert System rules are deemed applicable in this case		
H29	Missed gathering of contingent weather information	Hazard H29 Rules 1, 2	**WEATHER_DOPPLER_RADAR_BIT** RPAS_ENGINE_OMEGA RPAS_ALT IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The diagnosis of weather Doppler RADAR has been considered → Ok
H30	Missed avoidance of adverse weather	Hazard condition that can be verified on ground performing pre-flight briefing, checklists, etc.; no 'Expert System' rules are deemed to be applicable in this case		Ok

Table 13 – 'Expert System' rules coverage/consistency verification against U-space matrix content (Cont'd)

Hazard #	Definition	Rule	Control variables	Coverage/Consistency
Cross-cutting functionalities related hazards				
H31	Loss of RPAS subsystems health and status monitoring	Hazard H30 Rules 1, 2	**HEALTH_AND_STATUS_MONITORING_BIT** RPAS_ENGINE_OMEGA RPAS_ALT IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The diagnosi of RPA health and status monitoring subsystem has been considered → Ok
H32	Loss of communication while transiting from LOS to BRLOS and vice versa	Hazard H31 Rules 1, 2	**RPAS_RANGE** **RPAS_RANGE_RLOS** RPAS_ENGINE_OMEGA RPAS_ALT **RPAS_UPLINK_PATH_LOSS** **RPAS_DOWNLINK_PATH_LOSS** RPAS_AUTOPILOT_RETURN TO HOME_MODE	The loss of up/downlink with RPAS variation with time has been considered → Ok
H33	Unintentional radio link interference	Hazard condition that can be solved using operational procedures; no 'Expert System' rules are deemed to be applicable in this case		Ok
H34	Malicious radio link jamming	Hazard condition that can be solved using operational procedures: switching on secondary redundant radio frequency band or immediately terminate the flight; no 'Expert System' rules are deemed to be applicable in this case		Ok
H35	Malicious radio link spoofing	Hazard condition that can be solved using operational procedures: switching on secondary redundant radio frequency band or immediately terminate the flight; no 'Expert System' rules are deemed to be applicable in this case		Ok
Contingencies → Failures related hazards				
H36	Fire	Hazard H36 Rule 1	**RPAS_FIRE_WARNING** RPAS_ENGINE_OMEGA RPAS_ALT IRGRC RPAS_FTS_CMD	The on board RPAS fire when the RPA is in flight has been considered → Ok
H37	Loss of RPAS autopilot	Hazard H37 Rule 1, 2	**RPAS_AUTOPILOT_FAILURE_WARNING** RPAS_ENGINE_OMEGA RPAS_ALT IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The falure of on board RPAS autopilot when the RPA is in flight has been considered → Ok
H38	Loss of electrical power	Hazard H38 Rules 1, 2	**LIPO_BATTERY_CURRENT** RPAS_ENGINE_OMEGA RPAS_ALT IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The loss of RPAS electrical power when the RPA is in flight has been considered → Ok
H39	Loss of inertial platform	Hazard H39 Rules 1, 2	**RPAS_IMU_BIT** RPAS_ENGINE_OMEGA RPAS_ALT IS GREATER THAN ZERO feet IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The loss of RPAS IMU when the RPA is in flight has been considered → Ok
H40	Loss of heading indication	Hazard H40 Rules 1, 2	**RPAS_HDG1** **RPAS_HDG2** RPAS_ENGINE_OMEGA RPAS_ALT IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The loss of RPAS heading when the RPA is in flight has been considered → Ok
H41	Loss of altitude indication	Hazard H41 Rules 1, 2	**RPAS_ALT1** **RPAS_ALT2** RPAS_ENGINE_OMEGA – RPAS_ALT IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The loss of RPAS altitude when the RPA is in flight has been considered → Ok
H42	Pressure sensor failure	Hazard H42 Rules 1, 2	**RPAS_PRSR1** **RPAS_PRSR2** RPAS_ENGINE_OMEGA – RPAS_ALT IS IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The loss of RPAS pressuer sensor when the RPA is in flight has been considered → Ok
H43	Misleading altitude indication	Hazard H43 Rules 1, 2	**RPAS_ALT1** **RPAS_ALT2** RPAS_ENGINE_OMEGA RPAS_ALT IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The loss of RPAS altitude when the RPA is in flight has been considered → Ok

Table 13 – 'Expert System' rules coverage/consistency verification against U-space matrix content (Cont'd)

Hazard #	Definition	Rule	Control variables	Coverage/Consistency
H44	Misleading airspeed indication	Hazard H44 Rules 1, 2	**RPAS_IAS1** **RPAS_IAS2** RPAS_ENGINE_OMEGA RPAS_ALT IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The loss of RPAS altitude when the RPA is in flight has been considered → Ok
H45	Misleading indication of the angle of incidence	Hazard not applicable to the hybrid rotor wing RPAS model used to implement the rules		Ok
H46	Stall	Hazard not applicable to the hybrid rotor wing RPAS model used to implement the rules		Ok
Contingencies → Human factor related hazards				
H47	Loss of fuel cell	Hazard H44 Rules 1, 2	**RPAS_FUEL_CELL_CURRENT** RPAS_ENGINE_OMEGA RPAS_ALT IRGRC RPAS_RECOVERY_PARACHUTE_CMD RPAS_FTS_CMD	The loss of RPAS altitude when the RPA is in flight has been considered → Ok
H48	Remote pilot low training	Hazard condition due to human factor issues: 'Expert System' rules are deemed not applicable		
H49	Non-compliant operational procedures	Hazard condition due to human factor issues: 'Expert System' rules are deemed not applicable		Ok
H50	Loss of remote pilot situational awareness	Hazard condition due to human factor issues: 'Expert System' rules are deemed not applicable		Ok
H51	Human senses limitations	Hazard condition due to human factor issues: 'Expert System' rules are deemed not applicable		Ok
H52	Remote pilot excessive workload	Hazard condition due to human factor issues: 'Expert System' rules are deemed not applicable		Ok
Contingencies → Weather related hazards				
H53	Cloud cover	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok
H54	Fog	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok
H55	Freezing rain	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok
H56	Glare	Hazard condiion deemed to cause moderate acceptable risk due to the fact that the remote pilot is not on board the RPA		Ok
H57	Haze	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok
H58	Humidity	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok
H59	Ice	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok
H60	Rain	Hazard H60 Rule 1	**WEATHER_DOPPLER_RADAR_IMAGE** RPAS_ENGINE RPAS_ALT RPAS_AUTOPILOT_RETURN TO HOME_MODE	When the weather Doppler RADAR identifies 'rain' during a mission flight, the RPAS shll return home → Ok
H61	Snow	Hazard H60 Rule 1	**WEATHER_DOPPLER_RADAR_IMAGE** RPAS_ENGINE RPAS_ALT RPAS_AUTOPILOT_RETURN TO HOME_MODE	When the weather Doppler RADAR identifies 'snow' during a mission flight, the RPAS shll return home → Ok
H62	Solar storms	Hazard H62 Rule 1	**GPS_LAT** **GPS_LONG** **GPS_ALT** **EGNOS_LAT** **EGNOS_LONG** **EGNOS_ALT** RPAS_AUTOPILOT_RETURN TO HOME_MODE	When the weather Doppler RADAR identifies 'snow' during a mission flight, the RPAS shll return home → Ok

Table 13 – 'Expert System' rules coverage/consistency verification against U-space matrix content (Cont'd)

Hazard #	Definition	Rule	Control variables	Coverage/Consistency
H63	Temperature	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok
H64	Turbulence	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok
H66	Wind	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok
H66	Lightning strike	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok
H67	Hail	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok
H68	Hurricanes	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok
H69	Volcanic ash	Hazard condition that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission		Ok

With reference to performed verifications, the following issues are considered:

- The consistency of the knowledge basis relies on the safety analysis correctness
- The coverage of the knowledge basis rules relies on how much the safety analysis has been deepen and articulated and correct; its correctness leans on FMECA and FTA as consolidated reliability and safety analyses methodologies and on the confidence on the derived results:
    - The confidence on the FMECA results is as much high as the failure rates are correct and as the analyst has a clear and deepen knowledge of the equipment characteristics, way of operation, and how it is connected and interface with adjacent equipment
    - The confidence on the FTA results is correlated with the FMECA quality of execution: for a given system, the initiating events and single failure events identify with failure mode causes and failure modes themselves listed in the analysis.
    - In terms of risk ranking ('High risk', 'Moderate risk' and 'Low risk'), the safety assessment leans on the correctness of the evaluation of the failure modes probability of occurrence when the hazards derives from a failure occurrence and rely on the evaluation of the hazards probability of occurrence in the other cases. Similarly, the evaluation of the consequences of the

hazards shall be correct, that is the heaviest one among the possible ones.

- The reference parameters for the evaluation are supposed to be correct by definition: they are issued by ICAO (Table 5, Table 6, Table 7 and Table 8/Table 9 [3]) and accepted by the scientific and technical community after continuous application for aerospace

For any hazard occurrence, Table 13 shows the rules that are activated and triggered by control variables (highlighted in bold) which can be monitored by dedicated sensors (Figure 25).

According to safety management general principles [3], the defence of the system from all possible hazards is impossible: every change in the RPAS mission or every variation in its physical configuration will introduce new hazards. This issue strengthens the nature of safety management activities that are a continuous and dynamic process (SMS safety assurance pillar) to fit with new system conditions; from the 'Expert Systems' perspective this fact brings back to the problem of their maintenance/upgrade and to the size of the associated knowledge basis that can be increased but searching for the best compromise between the numer of rules, the performance of the 'Expert System' and its regular maintenance/debug.

4.4 Conclusions

The 'Expert Systems' have been proposed as a dynamic and flexible support to remote pilot decision making process in case of RPAS in-flight safety hazards occurrence.

The knowledge basis of a rule-based 'Expert Systems' has been draft exploiting the content of the U-space safety risks matrix.

A proposal for an 'Expert System' integrated with RPAS autopilot software has been proposed for more advanced real time solution of in-flight hazards for RPAS involved in specific category operations.

A coverage/consistency verification of the knowledge basis rules content with respect to the hazards collected in the U-space matrix has been performed.

Chapter 5

RPAS safety oriented architectures and review of U-space infrastructures

5.1 Introduction

The performed safety analysis and the introduction of the 'Expert System' have been used to define a proposal of a high level RPAS architecture oriented towards safe specific category operations in the VLL.

Beside this topic, a critical review of technical proposals for U-Space service deployment available in literature and on the web has been performed from a safety perspective and reported in this Chapter.

5.2 Safety oriented RPAS functional architectures: a proposal

As anticipated in Chapter 1, a typical specific category RPAS flight mission can be the following one: the operator sends the request for authorization to perform the mission and receive the acknowledge from the authority; the RPAS takes-off from outside a town and flies until arriving over the urban area; there it has to modify its route due to a NOTAM warning on the temporary presence of a police helicopter to monitor the area on a car accident; the RPAS avoids the mid-air conflict with the manned aircraft, arrive to destination and land to deliver the payload. Among the relevant elements, during the above mentioned example of mission the RPAS flies over at least two different scenarios: a rural one and a more congested one and it has to manage a contingent mid-air conflict. These issues highlights the need for RPAS architectures capable of dynamically adapting to changing scenarios but preserving operational safety.

Considering these premises, the performed safety analysis and the concept of 'Expert Systems' integrated with RPAS, a proposal for a functional high level architecture for an RPAS capable of safety risks mitigation is hereinafter presented and discussed.

5.2.1 External airframe and size

As already stated, light RPAS until 150 kilograms (payload included) have been considered for operations in the VLL subspace. With reference to the RPAS external airframe and size, the most challenging scenario is the urban/congested one. In literature, Authors suggest contained sizes up to 1.80 meters for fixed wing RPAS, and 1 meter for rotary wing RPAS [96].

5.2.1 Internal functional architecture

The VLL upper limit of 500 feet assures separation from operations of manned aircraft acting as a first line of risk mitigation. Nevertheless, the mid-air conflicts can occur and therefore, the mid-air collision risk shall be prevented/mitigated due to the presence in the VLL of sports and recreational air traffic, air ambulances, police 'Buster Air Traffic' (BAT) or helicopters/aircrafts involved in fire extinguishing/rescue operations, etc. In addition all other hazards capable of causing the RPAS operation going out of control shall be considered and mitigated in the VLL subspace as well.

Starting from these premises, the following RPAS high level functional architecture is proposed (Figure 26) as applications of the results of the performed safety analysis: it is an hybrid/electric powered RPAS with rotor engines (four ones for example) composed of the following subsystems: the airframe structures, the Propulsion Subsystem, the Power Subsystem, the Flight Management Subsystem, the Payload Sensors Subsystem, the Communication Subsystem; at its turn, the Flight Management Subsystem includes the Navigation Subsystem, the Air Data Subsystem, the Flight Control Subsystem and the Flight Termination Subsystem; the aerial segment communicates with the Ground Segment through a redundant Data Link Subsystem.

The above mentioned subsystems are hereinafter described highlighting the provisions derived from the performed safety analysis.

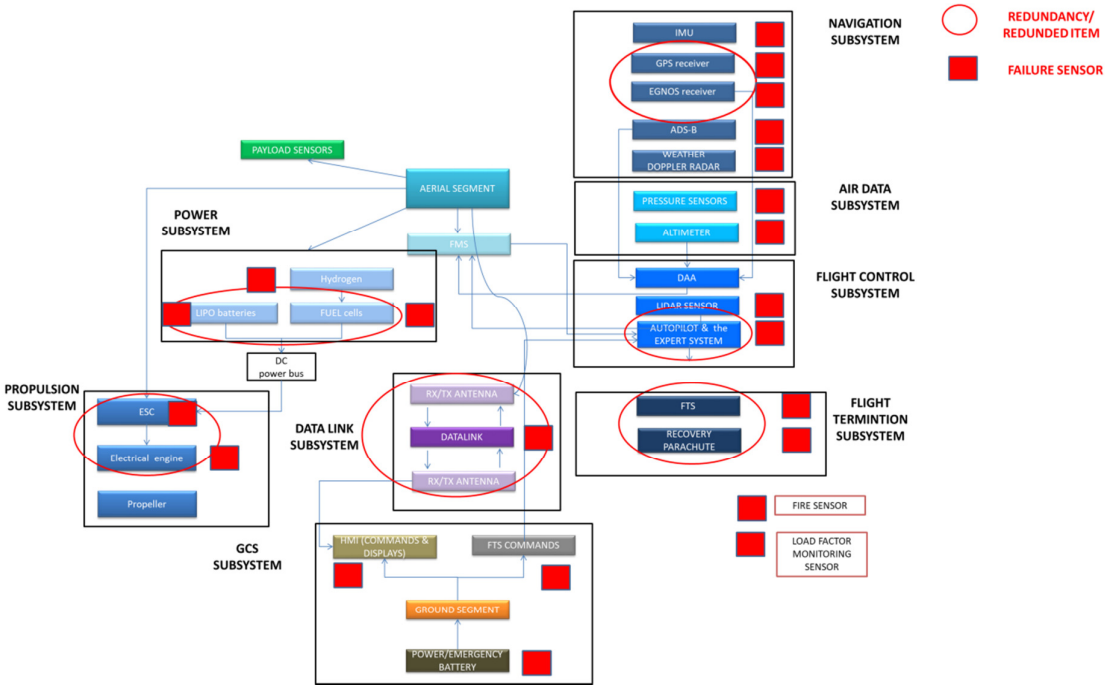


Figure 26 – Light RPAS high level safety oriented architecture

The Power and the Propulsion Subsystem

The electrical engines are supposed to be powered by hydrogen fuel cells to enhance the RPA endurance and range. The fuel cell is the main source of energy. The LiPo batteries are provided as a redundancy in case of fuel cells system failure (Hazard H47, FMECA items HPSS1a, HPSS1b, HPSS2a, HPSS2b and FTA Table 121, Table 122, Table 123, Table 124 and Table 125) and to promptly provide energy in case of high demanding manoeuvers (a sudden evasive manoeuvre to avoid mid-air collision, for example).

The Flight Management Subsystem/Navigation Subsystem

The Flight Management Subsystem/Navigation Subsystem is supposed to be provided with the EGNOS SoL (Safety of Life Service) receiver as primary navigation aid coupled with the GPS receiver as backup solution (Hazard H10, FMECA items NSS3a, NSS3b, NSS3c, NSS3d and FTA Table 94). The EGNOS is proposed as main navigation aid due to its higher accuracy and continuity of service with respect to GPS. This provision is fundamental for RPAS to safely operate within urban and congested environments as they will routinely requested to do in civilian applications; this idea is supported by Authors in literature too as reported, for instance, in [65].

Two redundant Inertial Measurement Units are foreseen in accordance with the reliability and safety analyses indications (Hazard H39, FMECA items NSS1a and NSS1b, and FTA Table 90).

The ADS-B transponder and a LIDAR sensor are proposed as fundamental equipment for subsystems to avoid mid-air collisions with other aircraft (Hazards

from H15 to H25). The 'Automatic Dependent Surveillance – Broadcasting' (ADS-B) is a transponder that relies on the Mode S at 1090 MHz (according to EASA ETSO-2C112b), on 'Global Navigation Satellite Systems' (GNSS) service (according to EASA ETSO C-129 and ETSO C-145/C-146) and on the deployment of ground-based surveillance systems capable of broadcasting enhanced sets of aircraft surveillance data to the ATM service and other airspace users [66]. These surveillance data (for example: position, track and speed) are much more accurate than those provided by ground based RADAR systems currently in use. The ADS-B introduction will allow manned aviation to perform more accurate navigation thus optimizing the allocation in the airspace available volume, saving more fuel and allowing to host the expected traffic increase in the next yeas ([1], [66]). According to the European Commission Regulation No 1207/2011 (22th November 2011), from the 7th June 2020, all aircraft with maximum take-off weight beyond 5.700 kilograms or capable of a maximum cruise speed greater than 250 knots, shall be equipped with ADS-B devices to be authorized to operate in the European airspace [66]. No similar regulations currently apply for RPAS, but when it will happen, the RPAS traffic will benefit the same flexibility and safety in navigation as manned aviation.

Further, the ADS-B is the focal equipment around which the RPAS 'Detect and Avoid' (DAA) systems are built. The provision of DAA subsystems ([36], [37], [38]) provides effective mitigations against mid-air collision risk with other cooperative traffic; 'cooperative traffic' means that the intruder on the RPAS route is equipped with the ADS-B equipment too; the RPAS DAA receives the signal broadcasted by the intruder ADS-B, elaborates it and use it to command the evasive manoeuvre to the given RPAS and make it execute o effectively avoid the collision. If the intruder is 'not cooperative', that is without the ADS-B installed on board, the DAA function is performed using sensors like the LIDAR. In order to protect the RPAS from the risk of mid-air collision with other both cooperative and not cooperative traffic, DAA subsystem and LIDAR sensors have been foreseen in the architecture under discussion (Figure 26).

The weather Doppler RADAR is provided (Figure 26) as mitigation provision to monitor weather changes in real time during flight operations specifically in case of long endurance operations; a weather Doppler RADAR can be useful in particular against the contingent occurrence of rain and snow (Hazards H30, H60 and H61) .

A final observation on navigation equipment applies: as foreseen by literature (Figure 9 [3]), the best compromise shall be reached between the need for enhanced safety, RPAS size, weight constraints and power availability and costs of advanced avionics: in fact, the RPAS shall accomplish safety of operations and competitive global costs with respect to manned fixed wing/rotor wing aviation. Given these elements, valid solutions will be probably provided by miniaturization techniques and nanotechnology as shown, for example, by

Figure 27 [97].

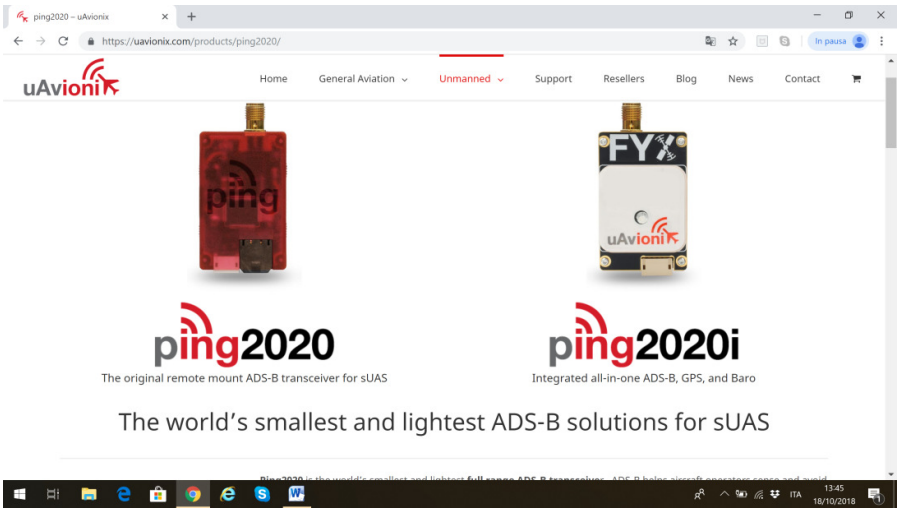


Figure 27 – ADS-B for Light RPAS [97]

The Air Data Subsystem

The Air Data Subsystem is composed of redundant pressure sensors and altimeters according to the safety and reliability analyses results (Hazards H41, H42, H43, H44, FMECA items from ADSS1 to ADSS6 and FTA Table 95).

The Flight Control Subsystem

The Flight Control Subsystem mainly includes a redundant autopilot in accordance with the safety and reliability analyses results (Hazard H37, FMECA, items FCSS1a, FCSS1b, FCSS1c and FTA Table 98), the ESCs (having supposed to consider a hybrid/electric powered RPAS with electrical motors) and the anti-collision subsystems based on DAA subsystem and LIDAR sensor previously described. As anticipated in Chapter 4, the autopilot has been supposed to be supported by a very simple rule-based 'Expert System' for real time management of in-flight hazard risks; the 'Expert System' triggered by the following signals (Table 13): Autopilot 'Abort Launch Mode', Pitch Command, Pitch Command HMI Longitudinal Shift, Pitch Command HMI Electrical Signal, Roll Command, Roll Command HMI Lateral Shift, Roll Command HMI Electrical Signal, Yaw Command, Yaw Command HMI Directional Shift, Yaw Command HMI Electrical Signal, LiPo Battery Current, ESC Failure Sensor, Waypoint Altitude, RPAS Indicated Airspeed (IAS), RPAS Altitude, FTS Built in Test (BIT), Recovery Parachute Built In Test (BIT), Autopilot "Return to Home" mode monitor, RPAS Mission Plan, GPS Latitude, GPS Longitude, GPS Altitude, EGNOS Latitude, EGNOS Longitude, EGNOS Altitude, RPAS Latitude, Planned Waypoint Latitude, RPAS Longitude, Planned Waypoint Longitude, Planned Waypoint Altitude, RPAS Uplink Path Loss, RPAS Downlink Path Loss, RPAS ADS-B BIT, RPAS LIDAR Sensor Output, RPAS Distance from obstacle, RPAS DAA output, RPAS Altimeter BIT (Built In Test), RPAS EGNOS BIT (Built In Test), Weather Doppler RADAR BIT (Built In Test), Health and Status Monitoring BIT (Built In Test), RPAS Range, RPAS Range RLOS, RPAS Fire

Warning, RPAS Autopilot Failure Warning, LiPo Battery Current, RPAS IMU BIT (Built In Test), RPAS Heading Indication 1, RPAS Heading Indication 2, RPAS Altitude Indication 1, RPAS Altitude Indication 2, RPAS Pressure Sensor Indication 1, RPAS Pressure Sensor Indication 2, RPAS Indicated Airspeed 1, RPAS Airspeed Indication 2, RPAS Fuel Cell Current, Weather Doppler RADAR Image.

The Flight Termination Subsystem

The Flight Termination System is composed of both the functionality to cut-off all the RPAS engines and to deploy the emergency parachute for smooth landing over congested/populated environments (Hazard H06, FMECA items EFSS1a, EFSS1b, EFSS1c and items EFSS2a, EFSS2b, EFSS2c and FTA Table 99, Table 100 and Table 101).

The radio link

The radio link allows to:

- Command and control the RPA in uplink
- Monitor the RPA telemetry data in downlink
- Command and control the payload in uplink
- Monitor the payload telemetry data sent in downlink including images, videos and the 'First Person View' (FPV) data

From a safety perspective, two redundant bands are proposed to be used for uplink and downlink channels (Hazards H12, H13, FMECA items C2LSS1a, C2LSS1b and FTA Table 126). One non redundant band is proposed for the payload management because the loss of payload is expected to affect the scope of the flight mission (FMECA items MPYSS1 and MPYSS2) but not the safety of the RPA or of third parties on ground.

The Ground Segment

The Ground segments includes the human machine interface to generate the flight command signals to be sent to the RPA in uplink, the monitoring displays mechanized by the signals sent from the RPA in downlink, the Flight Termination System HMI, the Payload HMI and the communication subsystem.

From a safety perspective the provision for monitoring sensors is indicated in Figure 26 to alert the remote pilot if failures on HMI controls occur.

In addition, a whole of systematic and well-structured safety alerts in terms of cautions and warnings fed by the RPA on board safety monitoring sensors is suggested to be implemented in the ground control station or on hand-held portable radio controller to enhance the remote pilot situational awareness on precursors of RPAS in-flight hazards.

5.3 U-space service infrastructures for implementation in Europe: a critical review from a safety perspective

Besides the above reported description of a light RPAS safety oriented high level architecture for the performance of routinely specific category operations in the VLL subspace, the main features of U-space service infrastructures implementation in Europe found in literature/on the web (in most of cases) are hereinafter reported (Table 14 [98]) and reviewed from a safety perspective; in particular the following items are detailed:

- The name of the considered infrastructure/platform
- The European state/company where it has been developed
- A brief description of its technical features/provided functionalities
- The main category of technological solution it can be ascribed to
- An evaluation from safety of RPAS operations perspective in terms of added value and possible limitations

Table 14 – Infrastructures/platforms developed in Europe to operatively deploy the U-Space service [98]

Infrastructure/ platform name	Origin	Description/Provided functionalities	Technological category	Considerations about safety	
				Added value	Limitations
Guardian UTM	Altitude Angel (United Kingdom)	Provision of traffic management capabilities Need for preliminary flight plan filing Use of open standards and protocols Customisable and modular Capable of manned traffic, and unmanned cooperative and not cooperative traffic tracking	Cloud-based platform	Manned and unmanned cooperative/not cooperative traffic management capability Preliminary flight planning filing ATC situational awareness Modularity Scalability	Potential lack of use of certified cartography approved for aeronautical use Potential lack of provisions and real time upgrade of further service information like weather Potential remote pilot situational awareness enhancement Potential low cyber security (due to the use of open protocols)
Drone-Flight-Check	Colibrex (Germany)	RPAS information RPAS traffic management database App for enhanced safety and regulation	Solution based on the use of telecommunication networks	Better RPAS monitoring into volume of airspaces not covered by ground-based RADAR systems Possibility of capillary monitoring of RPAS traffic due to the use of telecommunication infrastructures	Potential poor technical solution with lack of modularity Potential lack of mid-air collision risk mitigations Potential low cyber security Potential low radio link robustness against unintentional or malicious radio frequencies interferences
UTM	DFS (Germany)	Location of RPAS flying BRLOS using the mobile telecommunications network Incorporation of the traffic located into an air situation display Transmission of RPAS position to the controller using the mobile network RPAS equipped with an LTE modem, a GPS module and a mobile transmitter Generation of an air situation display from these position data Surrounding traffic, warning of conflicts, prohibited areas etc. are shown to the controller operator Detection of in-flight RPAS up to 100 meters of altitude can detect unmanned aircraft systems up to a height of 100 metres. Traffic monitoring through the use of multi sensor RADAR systems Adaptation of visualization on the controller displays of the monitored RPAS traffic Link to existing air traffic control systems Integration of chart material, prohibited areas and meteorological information Addition of data from detection systems to identify intrusive RPAS	Solution based on the use of telecommunication networks	Better RPAS monitoring into volume of airspaces not covered by ground-based RADAR systems Possibility of capillary monitoring of RPAS traffic due to the use of telecommunication infrastructures RPAS remote pilot situational awareness ATC situational awareness Possibility of capillary monitoring of RPAS traffic due to the use of telecommunication infrastructures Detection of RPAS between ground and 100 meter of altitude Use of cartography approved for aeronautical use Identification of intrusive RPAS traffic.	Potential low cyber security Potential low radio link robustness against unintentional or malicious radio frequencies interferences

Table 14 – Infrastructures/platforms developed in Europe to operatively deploy the U-Space service [98] (Cont'd)

Infrastructure/ platform name	Origin	Description/Provided functionalities	Technological category	Considerations about safety	
				Added value	Limitations
Blueprint Concept for Urban Airspace Integration	DLR (Germany)	Allowance to fly according to the technical sophistication of the considered RPAS; such degree of sophistication is visually represented with a small or large polygon (less of more sophistication) Assignment of a full simulated and risk-minimised flight path which takes into account airspace users that are already airborne, avoids critical areas on the ground, and results in a flight route with the less number of deviations as possible from the ideal path	Other technical solution	RPAS remote pilot situational awareness ATC situational awareness	Potentially complicated system, potential low scalability Potentially low manned and unmanned cooperative/ not cooperative traffic management capability Potential lack of use of certified cartography approved for aeronautical use Potential lack of provisions and real time upgrade of further service information like weather
DAMS	Drone Radar (Polish)	DAMS: Drones Aware and Monitoring System Fully integrated with the Polish Air Navigation Services Agency (PANSA) Analysis of the airspace using information and data shared with the PANSA Two ways not verbal communication between the ATC operators and the RPAS operator Bi-directional emergency communication with the RPAS operator to immediately land the unmanned aircraft when necessary	Other technical solution	Use of data shared with the national ATC Communication of the RPAS operator with the ATC during ordinary flight activity and during emergency, with immediate land of the RPAS if necessary	Potentially low manned and unmanned cooperative/not cooperative traffic management capability/strategies
DroNav	Dronsystems (United Kingdom)	Self-learning platform based on the use of software and hardware elements Capability of offering redundancy, fail-safe algorithms for conflict prevention/resolution and management. Scalable and easily deployable system capable of allowing the safe management of concurrent operations of a large number of RPAS in the same airspace	Other technical solution	Conflict prevention/resolution/management Scalability	Potential low ATC situational awareness Potential low RPAS remote pilot situational awareness Potential lack of use of certified cartography approved for aeronautical use Potential lack of provisions and real time upgrade of further service information like weather Potential low cyber security
UTM portal	Exponent Technology Services (United Kingdom)	Portal coupled with the Exponent's SkyCommander Tracker, Allowance to manage a host of UAV/RPAS flight operation functions from a single operational console Overlay with dedicated ADS-B civil air traffic data Near real time monitoring of RPAS separation, with automated alerts generated based upon customizable metrics as defined by the regulator. Storage of flight data: data can be made available for successive audits; data can be exported and integrated with third party tools; report generation Extendibility to allow new applications via API to enable payload data visualization and analytics	Cloud-based platform	Use of a single operational console ATC situational awareness Monitoring of ADS-B civil air data Provision of near real time monitoring of RPAS separation Storage of data for successive possible safety analysis/Collection of RPAS safety/reliability related data	Potential low remote pilot situational awareness Potential risk to have to manage too much data on a single console and for one of few ATC operators

Table 14 – Infrastructures/platforms developed in Europe to operatively deploy the U-Space service [98] (Cont'd)

Infrastructure/ platform name	Origin	Description/Provided functionalities	Technological category	Considerations about safety	
				Added value	Limitations
Urban ATM	GLVI (Germany)	Modular, redundant and expandable system Designed for urban environments and areas without clear lines-of-sight, and with atmospheric disturbances (fog, rain, or dust) Designed to work with high traffic densities The system does not distinguish between remotely piloted and software-in-control unmanned aircraft The system is able to consider both airspace users able to cooperate with the system and others which are not able to like pedestrians, leisure drones, or birds.	Other technical solution	Modularity and scalability of the system Design for urban environments (one of the most challenging for RPAS due to the presence of a variety of obstacles) System designed to manage high traffic densities Capability to manage both cooperative and not cooperative traffic	Potential lack of care for ATC situational awareness Potential lack of care for RPAS remote pilot situational awareness Potential lack of use of certified cartography approved for aeronautical use Potential lack of provisions and real time upgrade of further service information like weather Potential low cyber security
DREAMS	IDS (Italy)	Web-based system for airspace management and information Provision for e-registration, identification and tracking Single point of entry for all RPAS stakeholders Provision of tailored services and interfaces No-fly zone, airspace and flight planning management and reservation Flight validation and scheduling Flight awareness, RPAS tracking and notification to ATC for potential conflicts Recording and playback for safety investigation	Cloud-based platform	Modularity and scalability of the system Potential use of cartography approved for aeronautical use ATC and remote pilot flight situational awareness Data recording for successive possible safety analysis and safety and reliability historical data collection	Potential low cyber security
Involi.live	Involi (Switzerland)	Collection of real time data from low altitude traffic equipped with ADS-B and aircraft transponders The system is able to process these data and to transmit them to the UTM system to share in real time information with all the airspace users Implementation of automated micro-control tower capable of operating without the intervention of the human operator	Other technical solution	High automation in RPAS traffic management	Potential low care for ATC and remote pilot situational awareness Potential low cyber security Potential low radio link robustness against unintentional or malicious radio frequencies interferences
Automated UTM system	Leonardo Company S.p.A. (Italy)	Automated UTM system Provision of public register of RPAS, communication, route and mission planning, dynamic geo fencing Provision of a scalable cloud platform according to the architecture 'Platform as service' Fusion of information from the UTM and the ATM and sharing with the remote users Provision of a mission safety processor capable of warning operators on safety related events	Cloud-based platform	Automation Scalability Mission planning Fusion of information between the ATM and the RPAS traffic management system Sharing of information with remote users Use of the safety processor to warn the operators on safety related events	Potential lack of provisions for cyber security

Table 14 – Infrastructures/platforms developed in Europe to operatively deploy the U-Space service [98] (Cont'd)

Infrastructure/ platform name	Origin	Description/Provided functionalities	Technological category	Considerations about safety	
				Added value	Limitations
Drones Solutions	Lufthansa Systems (Germany)	Use of APPs based on Lufthansa aeronautical certified data shared among RPAS users to warn them in case of safety related events	Cloud-based platform	Use and sharing of aeronautical certified data among the airspace users	Potential lack of measures to prevent mid-air collisions events with both cooperative and not cooperative traffic Potential low care for ATC and remote pilot situational awareness Potential low cyber security
Drone Assist	NATS (United Kingdom)	Interactive map of areas used by commercial aircraft Use of the 'Fly now' feature to share RPAS locations and reduce the risk of RPAS related incidents	Other technical solution	Use and sharing of data among the airspace users	Potential lack of the use of certified aeronautical data Potential lack of measures to prevent mid-air collisions events with both cooperative and not cooperative traffic Potential low care for ATC and remote pilot situational awareness Potential low cyber security
AlphaOne, One Sky Connect	OneSky (Involi, Switzerland)	Provision of a system of micro control towers Provision of an internet platform to manage RPAS separations, conflicts and geo fencing	Other technical solution	See 'Involi.live'	See 'Involi.live'
Low Level RPAS Traffic Management (LLRTM)	ONERA (France)	Provision of the LLRTM (Low Level RPAS Traffic Management). Platform to manage RPAS traffic in uncontrolled airspace and to interface with traffic within controlled airspaces Coordination of traffic monitoring with the ATC within controlled airspaces Ground-based system to manage RPAS sorties within VLL subspace (airspace classes E and G), though the use of a combination airborne collaborative alerting sensors and ground sensor	Other technical solution	Interface with ATC and coordination with them within controlled airspaces Use of airborne and ground-based monitoring sensors	Potential lack of the use of certified aeronautical data Potential low cyber security
ECOSystem	THALES (France)	Software application capable of real-time validation of RPAS flight plans Provision of a decision support platform for advanced aviation operations	Other technical solution	Provision for flights plan validation Provision for cyber security ATC situational awareness Probable provision and sharing of certified aeronautical data and real time updated weather information	Not tailored for RPAS only Not sensitive to specific operational environments like the urban scenarios Possible lack of specific measures for the mitigation of mid-air risk collision avoidance Possible lack of the remote pilot situational awareness

Table 14 – Infrastructures/platforms developed in Europe to operatively deploy the U-Space service [98] (Cont'd)

Infrastructure/ platform name	Origin	Description/Provided functionalities	Technological category	Considerations about safety	
				Added value	Limitations
RPAS VLLOC	VITO, Luciad and FlightPlus (Belgium)	RPAS 'Very Low Level Operation Coordination' (RPAS VLLOC) platform suitable for safe planning of RPAS VLL operations The platform has been designed to provide control over operations and the possibility to cancel them if necessary Compliant with the EUROCONTROL SWIM service	Other technical solution	RPAS mission planning ATC situational awareness	Possible lack of specific measures for the mitigation of mid-air risk collision avoidance Possible lack of the remote pilot situational awareness Possible lack of use of certified aeronautical data Possible lack of real time update of weather information Possible lack of cyber security
Swiss wide U-Space	FOCA (Switzerland) [99]	High digitalization solution for RPAS electronic registration, identification and geo fence	Other technical solution	High automation in RPAS traffic management RPAS mission planning ATC situational awareness	Possible lack of specific measures for the mitigation of mid-air risk collision avoidance Possible lack of the remote pilot situational awareness Possible lack of use of certified aeronautical data Possible lack of real time update of weather information Possible lack of cyber security
Use of sim cards on RPAS and of 4G/LTE networks	VODAFONE UK (United Kingdom) [100]	RPAS monitoring and control solutions based on the use of sim cards like those equipping mobile phones and the 4G/LTE network	Solution based on the use of telecommunication networks	Better RPAS monitoring into volume of airspaces not covered by ground-based RADAR systems Possibility of capillary monitoring of RPAS traffic due to the use of telecommunication infrastructures	Potential low care for ATC and remote pilot situational awareness Potential low cyber security Potential low radio link robustness against unintentional or malicious radio frequencies interferences
Web-based cloud system for RPAS collision and Avoidance [101]	Example from literature	RPAS monitoring and control and collision avoidance solutions relying on web-based cloud systems	Cloud-based platform	Scalability Provision of mid-air collision risk mitigation Use of certified aeronautical data	Potential low cyber security Potential low care for ATC and remote pilot situational awareness Potential low care for the remote pilot situational awareness Potential lack for real time updated weather information

Some basic requirements for the operational deployment of the U-Space service in the VLL subspace have been derived from the review reported in Table 14 (Table 15):

Table 15 – Basic requirements for the U-Space service in the VLL subspace

Requirement	Motivation/Notes
RPAS electronic registration	He need for the electronic registration (e-registration) to allow the identification of the operating RPAS
RPAS electronic identification	The need for the electronic identification (e-identification) to know who is flying through the knowledge of the remote pilot contacts, his/her identity verification capability and through the knowledge of the RPAS data
RPAS geo fence	The need for The whole of digital boundaries on air maps with associated rules for access with real time status upgrade and sharing among the VLL users
RPAS mission planning	Necessary for awareness on the number of flying RPAS in the VLL
One common source/database for mission plan filing	Necessary for better control of the number of the VLL subspace users
RPAS mission plan visualization	Necessary for ATC/remote pilot situational awareness enhancement
RPAS mission plan cancellation	Necessary for ATC situational awareness enhancement
Modularity	Necessary for an easier and dynamic management of the VLL
Scalability	Necessary to easily add new users to the VLL subspace monitoring
Cyber security	Necessary to avoid intentional malicious interference with RPAS operations to catch the remote control of the flying RPAS
Prevention of intentional RPAS loss of link (spoofing, jamming)	Necessary to avoid intentional malicious interference with RPAS operations to catch the remote control of the flying RPAS like, more specifically, performing spoofing, jamming, etc.
Prevention of unintentional RPAS loss of link (for instance caused by flight over radio transmitting stations, VORs, etc.)	Necessary to avoid electromagnetic interference if the RPAS operates near powerful sources of radio waves like telecommunication antennas, VORs, etc.
Interface of the U-Space service with the ATM service	Necessary for manned traffic identification of RPAS traffic
Sharing of RPAS flight data between the U-Space service with the ATM service in the VLL subspace	Necessary for ATC situational awareness with respect to RPAS traffic
Availability of real time updated weather information	Necessary to prevent weather related hazards from occurring
Use for RPAS of certified aeronautical data/charts/map	Necessary to properly implement geo fence
Geofence implemented on the basis of certified aeronautical data/charts/map	Necessary to properly prevent RPAS traffic from entering prohibited areas like aerodromes or sensitive areas, etc.
Prevention of mid-air conflict risk with cooperative RPAS traffic	Necessary for prevention of mid-air collision hazard with cooperative RPAS traffic
Prevention of mid-air conflict risk with not cooperative RPAS	Necessary for prevention of mid-air collision hazard with not cooperative RPAS traffic
Avoidance collision in case of mid-air conflict risk with cooperative RPAS	Necessary for avoidance of mid-air collision hazard with cooperative RPAS traffic
Avoidance collision in case of mid-air conflict risk with not cooperative RPAS	Necessary for avoidance of mid-air collision hazard with not cooperative RPAS traffic
Aerial traffic resolution	Necessary for resolution of conflicts among RPAS traffic or between unmanned and manned traffic
Aerial traffic management	Necessary for management of ordinary RPAS operations
Facilitation of RPAS remote pilot situational awareness in the VLL subspace	Necessary to enhance general safety of RPAS operations
Facilitation of ATC controllers situational awareness towards RPAS traffic merged with manned traffic	Necessary to enhance a safer management of RPAS traffic from the perspective of he ATC personnel
Two ways voice communication with ATC	Necessary to communicate with the ATC for ordinary reasons
Two ways voice emergency communication with ATC	Necessary to communicate with the ATC in case of emergency on board the RPAS
Monitoring of RPAS flight not identifiable by ground RADAR	Necessary for monitoring of RPAS at altitudes at which ground RADAR are not capable of identifying/controlling the RPAS
Capillary monitoring of high volumes of RPAS traffic	Necessary for precise monitoring of a high number of concurrently operating RPAS
Use of ADS-B on small RPAS	Necessary for cooperative RPAS traffic identification
Use of LIDAR/SONAR on small RPAS	Necessary for not cooperative RPAS traffic identification
Use of weather RADAR on small RPAS	Necessary for real time updating of weather information
RPAS flight data recording for safety analyses	Necessary to collect safety related data for safety analysis/evaluation of compliance with key safety targets

Table 15 – Basic requirements for the U-Space service in the VLL subspace (Cont'd)	
Requirement	**Motivation/Notes**
RPAS data recording for reliability analyses/identification and collection of historical data	Necessary to collect reliability related data for historical databases
Automation for RPAS traffic management	Necessary to alleviate ATC personnel workload and enhance RPAS flight operations management
Use of distributed micro control towers	Necessary to alleviate ATC personnel workload and enhance RPAS flight operations management
Use of airborne and ground-based monitoring sensors	Necessary to alleviate ATC personnel workload and enhance RPAS flight operations management

5.4 Conclusions

A proposal for a light RPAS high level functional architecture oriented towards operational risk mitigation in the VLL airspace has been presented and discussed in this chapter.

In addition, the first available proposals of technical solutions to deploy the U-space service have been presented and review from a safety of RPAS operations perspective, identifying possible useful requirements to manage light remotely piloted aircraft systems flight operations in the VLL subspace.

Chapter 6

Complex systems safety analysis

6.1 Introduction

The FMECA, FTA and Bow Tie used as basis to derive hazards for the safety analysis of the system 'RPAS integrated in the civil airspace' are event based models.

From safety perspective, the operating scenario of RPAS integrated in the not segregated airspaces can be assimilated to a complex system where the identification of systemic accidents precursors is capable of providing additional data for a more effective Safety Management System.

The complex systems are object of study of the 'System Theory': the 'System-Theoretic Process Analysis' (STPA) hazard analysis derived from the 'System-Theoretic Accidents Model Process' (STAMP) methodology is hereinafter described and applied to a selected accident scenario to show its potentialities to integrate traditional safety analysis methodologies.

6.2 Complex systems and the systems theory

The FMECA and FTA are probabilistic event based analysis techniques based on the probability of occurrence of single components failure that can trigger an accident occurrence. For this reason, according to more recent trends in safety analysis, they do not completely match with the reality: the paradox can occur that all of the system components are confirmed to be reliable but an accident occur to the system, that is the system has not resulted to be safe in reality.

The 'Complex Systems' theory proposes extended causality models that allow the investigation of interactions among the system components and found out system hazards; the system hazards cannot be identified by traditional event based safety analysis methodologies [42] thus revealing an important limitation. These issues are overcome by 'Complex Systems' derived methodologies thus helping the analyst to get complementary data and positively supporting the

implementation of more effective safety management systems. Using complex systems techniques, the safety problem is reformulated in terms of a control problem rather than in terms of a reliability issue. The theoretical foundation of this approach is the 'Systems Theory'. The expression 'System Theory' deals with approaching the system under study as a whole, rather than considering its components singularly. Further, the 'System Theory' operates not only on the system components but also on their mutual interactions according to proper control laws [42].

6.2.1 STAMP methodology

Within the 'System Theory', the 'System-Theoretic Process Analysis' (STPA) hazard analysis methodology derived from the 'System-Theoretic Accidents Model Process' (STAMP) is hereinafter proposed and discussed.

6.2.2 The STPA safety hazard analysis

The 'System Theoretic Process Analysis' is a hazard analysis technique based on the STAMP methodology; therefore it describes the system in terms of control loops foreseeing a controller who observes the behaviour of the controlled process through measured variables and manipulates it through the injection in the loops of controlled variables (Figure 28 [42]).

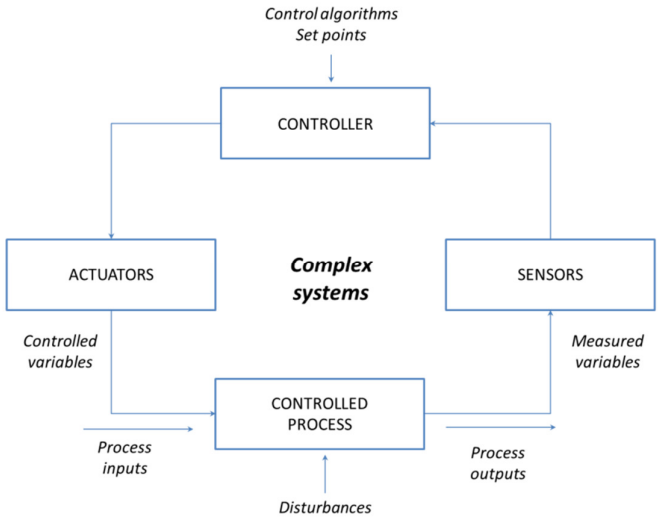


Figure 28 – Complex systems control loop [42]

Passing through a control problem strategy rather than single components failure, the STPA identifies hazards due to unsafe and unintended interactions occurring among the system components even if none of them is affected by failures and lead to identify the process causing the accident scenario. To reach this aim, the STPA methodology uses further causal factors like behaviour, omissions, decisions, etc. [42] to include hazards of other nature caused by sub-system interactions, design errors, software errors, human beings behaviour and

decision making process errors, and social, management and organizational related factors. The accident is conceived as the result of the violation of system constraints in one or more control loops [102].

The STPA methodology is applied following these steps ([42], [102], [103]); Figure 29 ([42], [103]) shows a standard control loop associated to the above reported steps:

a) Safety constraints definition: the hazards are transposed into safety constraints
b) Safety control loops definition: the system structure is transposed into tailored safety control loops
c) Potentially inadequate control actions identification: it is the identification of the whole of the ways according to which the system can get into safety hazards conditions; the inadequate control actions can belongs to one of the following four categories:
    - A control action required to maintain safety is not provided
    - An incorrect or unsafe control action is provided thus inducing a loss in the system
    - Potentially correct or adequate control actions are provided too early, too late, or out of sequence
    - A correct control action is stopped too early
d) Identification of causes of inadequate controls: it is the determination of how each potential identified hazardous action can occur with reference to: management of change procedures, verification if safety constraints are changing accordingly; audits performance; detection of unplanned changes that can violate the constraints; accident and incident analysis to trace anomalies to the hazards and to the system design

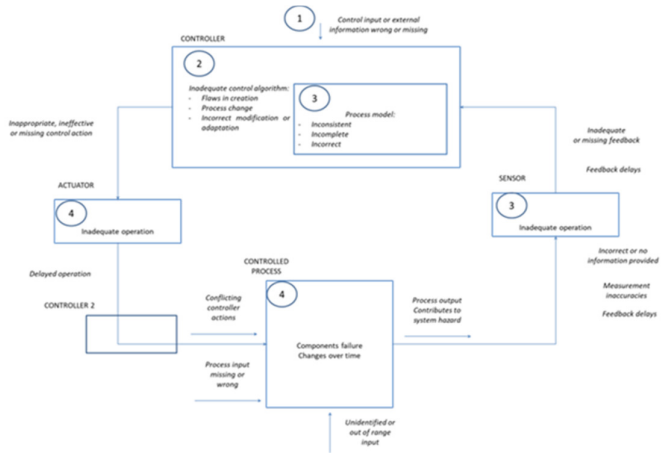


Figure 29 – A standard control loop and associated factors ([42], [103])

6.2.3 The STPA safety analysis of the system 'RPAS integrated in the civil airspace'

The safety analysis of the system 'RPAS integrated in the civil airspace' applying the STPA method has been performed with reference to a specific accident scenario to show the essence of this methodology and, on this basis, to evaluate its potentiality/differences with the traditional safety analysis techniques used in this research.

Three main risks shall be properly managed when during and RPAS sortie:

- Mid-air collision with manned aircraft
- Fatal injury to persons on ground
- Damage to third parts on ground

The 'mid-air collision with manned aircraft' is chosen in this case to show how the STPA method works.

According to the above mentioned methodology steps the following is set up:

a) Safety constraints definition: the high level hazards and high level safety requirements (SR) necessary to apply the STPA methodology are reported in Table 16 [103]
b) Figure 30 ([102], [103]) shows the standard control loops tailored to this case
c) Potentially inadequate control actions are identified in Table 16 [103]
d) The results of the application of the STPA technique with the identification of the hazards have been reported in Appendix G ([103] Table 147 [103] and Table 148 [103])

Table 16 – STPA methodology: set up of the investigated scenario and analysis parameters [103]

Investigated scenario: Mid-air collision of an RPAS in the VLL with a cooperative manned aircraft	
High level safety hazards	**High level safety requirements (SR):**
H01: unsafe separation from a cooperative manned aircraft	SR01: the RPAS shall maintain safe separation from manned aircraft
H02: loss of RPAS control	SR02: the remote pilot shall maintain safe separation from manned aircraft
H03: Detect and Avoid subsystem failure	SR03: the Detect and Avoid subsystem shall prevent the RPAS from collision occurrence with other airspace users

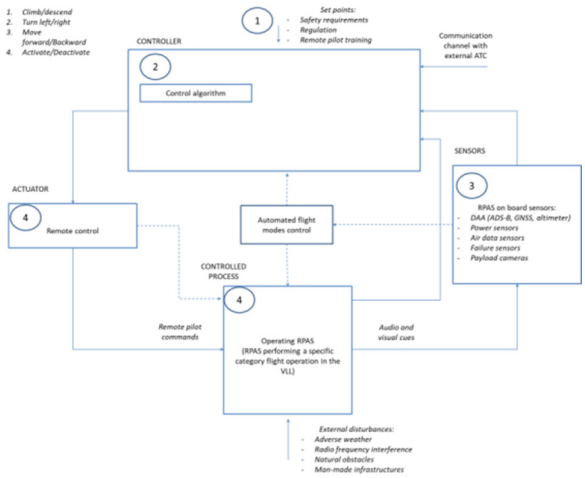


Figure 30 – Light RPAS operations in VLL airspace: STPA control loop [103]

6.2.4 Discussion

The operational accident scenario used in Appendix G is that of the mid-air collision risk between the operated RPA and a cooperative (ADS-B equipped) manned intruder in the VLL airspace.

The possible control actions (CA) related to the given accident scenario are: climb/descend, left/right turn, move backward/forward, increase/decrease airspeed, deactivate/reactivated. The controlled actions can be performed by the RPA commanded by the remote pilot or through automated flight modes acting on the RPA control algorithm.

The control actions trigger hazardous/unsafe control actions (UCA) effectively causing hazards or not. If they cause an hazardous state, this is explicitly indicated recalling one or more of the high level hazards of interest (Table 16 [103]) capable to lead to the accident scenario under examination (Table 148 [103]).

The identified control actions of interest (Table 147 [103]) are reconsidered and classified according to possible causal factors (Table 148 [103]); the following case is described more in detail for example: starting from control action 1 ‘Climb’, if it is performed according to DAA proposed manoeuvre to resolve the mid-air conflict, the RPA will avoid the collision with the intruder; if not, the accident scenario with the intruder will occur; the CA1 ‘Climb’ cannot be performed because the RPA does not correctly execute the DAA commanded evasive manoeuvre ([UCA2]) or because the remote pilot, bypassing the DAA, commands an inappropriate/wrong manoeuvre to the RPA ([UCA3]). Going through the unsafe control actions causal factors (Table 148 [103]): the RPA cannot correctly execute the DAA manoeuvre due to inadequate command signals generated by the control algorithm or due to inadequate communication link between the remote controller and the RPA or due to misleading information shown by on ground displays. Therefore, using the STPA technique, safety

hazards related to the following topics can be argued more easily and directly than using only FMECA/FTA methodologies [42]:

- Design errors (including software flaws): they can apply to ground control displays content; if the requirements for their mechanization are poor, the displays will provide misleading information to the remote pilot affecting his/her situational awareness, decisions and consequent recovery actions
- Cognitively complex human decision-making errors: the RPAS operator can decide to perform an action on the basis of an unexpected external input; but the actions reveals to be detrimental for the RPAS
- Social, management or organizational factors contributing to cause accidents: it could be the case of inadequate regulation issued by the authority; it can be the case of a regulation that is intrinsically affected by error or which is not clearly formulated; the same could be said about wrong or improper procedure contained in the operational manual of the RPAS operator and still not having been properly amended

The above described example of application of the STPA method shows how it allows to identifies more hazard events than traditional reliability based methods including those caused by lack of system components reliability as well ([42], [102]). The integration of traditional and STPA safety hazards analyses can provide a more extended spectrum of safety risks allowing the implementation of more effective safety management systems for RPAS. Further, according to the basic definition of safety management system for which the search for new hazards never stops but dynamically fits with the system to be managed, it can be stated that such advanced methodologies like the STPA hazard analysis can adequately support this activity and as the system becomes more and more complex it helps the analyst to easily going through it and identifying the deepest and most hidden causes of incidents/accidents. Nevertheless, the safety analysis reported in this dissertation has been based on traditional analysis methodologies like FMECA and FTA due to their consolidated recognized reliability against the high level of novelties brought by the RPAS technology and their incoming integration into the civil not segregated airspace. Further, the investigation on RPAS equipment reliability has been judged fundamental because no systematic and extended reliability and safety analysis have been found in literature.

Among the causal factors not related to simple lack of system components reliability, the system components interaction and the use of software [42] to manage the RPAS operations can be separately discussed. The system components interaction is still early to be considered in depth due to the current early stage of integration of RPAS and developments of related regulation. With reference to software modules largely used on board RPAS, the STPA

methodology can provide significant more support in the analysis of software functionalities than traditional event based techniques.

Finally, if the STPA is appreciated because it provides great support to the safety analyses during the initial phases of design when the system neither exists, FMECA and FTA gain usefulness with the increase of RPA operative life, when failures due to the physiological decrease of components reliability start to more and more affect the system safety of operation.

In conclusion, the above reported considerations highlight the utility of both event based and system based hazards analysis techniques.

6.3 Conclusions

The safety analysis methodology STPA ('System-Theoretic Process Analysis') derived from the 'Systems Theory' has been introduced in this Chapter because it is as a powerful technique to integrate hazards identified applying traditional safety analysis techniques.

The STPA, focusing on system components interactions rather than on single components reliability, provides the possibility to identify systemic hazards.

A practical case based on a selected accident scenario has been presented and discussed as an example of the results obtainable using the STPA methodology.

The application of both traditional and STPA techniques on the system 'RPAS integrated in the civil airspace', can lead to a more comprehensive, better structured and effective Safety Management System for RPAS.

Chapter 7

Evaluation of impacts of the safety analysis on RPAS Italian regulation

7.1 Introduction

The Remotely Piloted Aircraft Systems are regulated in Italy by the 'Ente Nazionale Aviazione Civile', ENAC. The state of art of Italian applicable regulation for RPAS operations is mainly composed of the following documentation:

- Remotely Piloted Aircraft Systems, Second Edition, issued on the 16th July 2015; amendment 4 (21st May 2018) [104]
- Standard scenarios prescriptions in accordance with EASA Opinion 01/2018 but defined for open category RPAS operations only for the moment [105], as it can be argued by the weight category of involved RPAS (MTOW less than 2 kilograms, MTOW included between 2 and 4 kilograms, MTOW included between 4 and 25 kilograms) and the indicated operational limitations; for this reason this document is not hereinafter further analysed

Hence, the above mentioned main RPAS Italian regulation [104] is considered against the performed research activity on RPAS safety and reviewed to evaluate the impacts of the analysis on them.

7.2 RPAS Italian regulation

The main contents of the Italian RPAS regulations are hereinafter recalled.

The Remotely Piloted Aircraft Systems regulation [104] rules the operations of RPAS until 150 kilograms maximum take-off weight. Indoor operations of RPAS or free balloons are excluded. The Italian regulation is focused on safety requirements to operate the RPAS outdoor within the Italian boundaries. The possible kinds of operations are the commercial ones and those performed for scientific/research purposes under RLOS, ERLOS (extended RLOS with the support of technological devices) and BRLOS conditions.

Three categories are identified according to the RPAS maximum take-off weight:

- RPAS with maximum take-off weight until 25 kilograms: the operations are further classified as critical or not critical according to the correlated risk level (low or medium/high, respectively)
- RPAS with maximum take-off weight between 25 and 150 kilograms: they shall be identifiable through the assignment registration marks and they undergo the issuance of a permit to fly to operate within the national airspace
- RPAS with maximum take-off weight below 2 kilograms; the sorties performed with these RPAS are always considered as low risk operations

The survey of crowds of people during sport events or similar are always forbidden in Italy.

A design certification document is foreseen if a manufacturer wants to make industrial production of an RPAS model.

The standard scenario prescriptions [105] identify the safety prescriptions to mitigate the risks for each one of the proposed scenario in accordance with the roadmap foreseen by EASA [28]: the aim at the basis of this process is to simplify the formal procedures for the operators to get the flight authorizations and to alleviate burden of Authorities in evaluating requests to fly.

7.2.1 Evaluation of safety analyses impacts on ENAC RPAS regulation

The evaluation on the basis of the performed safety analysis of the above mentioned Italian regulation is hereinafter reported; the evaluation is performed specifically indicating each article and comma of interest of the considered regulation and related comments.

The following items of the ENAC RPAS regulation [104] have been considered evaluations on the basis of the safety analysis performed during the research:

Article 7, comma 4, with reference to ‘Extended Visual Line of Sight’ (EVLOS) operations (that is operations beyond VLOS conditions and for which the remote pilot uses supporting technical devices and operators (other remote pilot) to maintain the visual contact and the control of the RPAS): this also means

that the radio link shall be effectively maintained when the aerial platform control is passed from one remote pilot to another one. It is deemed that hazard H32 from the U-space risk matrix (Table 143) is applicable even if more precisely it deals with BRLOS condition (that is beyond ERLOS condition); as shown in Table 143, the lack of capability to maintain the radio link leads to a high risk; an accurate pre-flight planning is suggested as mitigation action during which the ground and aerial segments communication equipment (on ground/on board transmitting/receiving antennas and devices) are properly verified with reference to range performances; in case of lost link hazard condition, the emergency flight termination can be recommended as further recovery action.

Article 8, comma 5, with reference to altimeter for altitude holding: the use of the altimeter shall be highlighted in the RPAS operational manual as safety prescription.

Article 8, comma 6, with reference to the installation and use of lights or other devices to facilitate the recognition of the operating RPAS from other airspace users in not-segregated airspaces: the not recognition of RPAS from other airspace users involves a high risk (U-space matrix, hazard H19, Table 143); the implementation and correct use of the above mentioned devices shall be highlighted in the RPAS operational manual as a safety prescription; a redundant power supply line for lights shall be implemented in the RPAS.

Article 10, comma 5, with reference to the activation of the Flight Termination System: the use of parachute systems rather than the cut off of motors/engines is suggested to better control the RPAS fall particularly within urban/congested environments. The loss of the Emergency Termination Subsystem or of the HMI to manage the its activation involves high risk (U-space matrix, hazard H06 and H04 respectively, Table 143); sensors for on board automatic activation can be foreseen both as redundancy of manual activation from ground and as redundancy in case of loss of ground Emergency Termination Subsystem HMI (FMECA Table 75 and FTA Table 135) or loss of overall ground segment functionality (FMECA Table 54 and FTA Table 129, Table 130, Table 131, Table 132, Table 133, Table 134 and Table 135); the provision of an independent emergency battery to power the Emergency Flight Termination System is recommended in case of loss of on board main power supply or in case of on board fire.

Article 10, comma 6, letter b: with reference to mitigation provisions in case of loss link occurrence during RLOS operations over urban scenarios: the loss of link involves a high risk (U-space matrix, hazard H12 for loss of uplink channel and H13 for loss of downlink channel respectively, Table 143); the use of redundant channels on two different radio frequency bands; the provision for ‘Return to home function’ among autopilot automatic flight modes; the termination of flight using FTS or parachute systems.

Article 24, comma 4, with reference to avoidance for SAPR to perform flight operations nearby airports and ATZ/CTR (‘Aerodrome Traffic Zone/Control Traffic Region) areas: the implementation of geofence software functionality can help RPAS accomplishing this requirement (U-space matrix hazard H16, Table

143); the implementation of geofence systems based on aeronautical official and up-to-date cartography is recommended.

Article 26, comma 1: with reference to BRLOS operations. The separation from other airspace users shall be assured/maintained; mid-air conflicts scenarios are always high risk scenarios (U-space matrix hazards H15 ÷ H25, Table 143) and collision avoidance software functionality shall be implemented on board the RPAS using DAA subsystems based on ADS-B surveillance transponder against cooperative traffic and RADAR, LIDAR or SONAR based subsystems against not cooperative traffic (natural or man-made infrastructures are intended to be included in this statement); such functionalities are also expected to provide support to maintain separations in flight

7.3 Discussion

Within the integration of RPAS into not segregated airspaces, regulation plays a basic role: as clearly shown by EASA documentation ([27] and [28]) and as it is confirmed by Authors ([46] and [47], for example), future RPAS regulations will follow a risk-based approach to identify airworthiness requirements for RPAS. A proper unambiguous link shall be established between the requirement indicated by the regulation and the assessed risk of reference [46] to further proceed with a solid basis for RPAS airworthiness certification and legal authorization to enter the airspace.

The effectiveness of the this approach depends on how much the risk analysis is comprehensive and accurate. The following elements are almost consolidated among Authors [46]: the risks posed by RPAS are different in nature from those posed by manned aircraft due to the absence of the pilot on board and the high variety of configurations of RPAS with respect to manned aircraft: fixed wing RPAS, rotor wing RPAS, the possibility to be launched by hand or by a catapult rather than the possibility to take-off and landing like an helicopter or like a manned fixed wing aircraft; the possibility that the RPAS is manually piloted from ground or it is flown in automatic modes, etc. A systematic regulation-based approach to the safety analysis like the one performed in this research work (based on general functional requirements [39], [47] and then gradually detailed using FMECA, FTA and human factor models) is hence confirmed in its correctness.

7.4 Conclusions

Current RPAS Italian regulation has been critically evaluated according to the content of the performed safety assessment of RPAS operations in the civil not segregated airspace.

The basic importance of a regulation-based approached focused on risk assessment is confirmed in its correctness due to the high variety of RPAS technology configurations.

Conclusions

The research work object of this Dissertation consists of the following main parts and contribuitions:

- In 2013 ICAO issued the Annex 19 on safety management thus stressing the necessity for a new global and integrated approach to safety in aviation. This has been due to the expectation for a duplication of volume of civil air traffic. With the Annex 19, the safety in aviation is officially elevated to a State responsibility and the obligation to implement a Safety Management System is extended to all aeronautical operators both of manned and remotely piloted aircraft systems to be allowed to enter the airspace
- Starting from the first experimental test flights on remotely piloted aircraft operating beside manned traffic performed under the SESAR1 RAID research demo project (under CIRA responsibility), a preliminary risk matrix on hazards identified during the cited activity has been draft. Successively, the idea arose to study safety management systems for RPAS focusing on safety risk analysis and extending the concept of risk matrix to more comprehensive cases. Hence, following the guidelines provided by EASA on the risk based categorization of RPAS operations (open, specific and certified category operations according to a growing risk) and merging it with the concept of operations issued by EUROCONTROL (open and specific category operations to be performed until 500 feet of altitude from ground, within an uncontrolled subspace served by U-space infrastructures and certified operations allowed beyond 500 feet of altitude from ground within controlled subspaces served by ATM infrastructures) two extended risk matrices have been implemented
- After having investigated which hazards can be generated from the operation of both manned and unmanned aircraft in the same controlled/uncontrolled airspace, the attention has been focused on the provision of solutions to mitigate the effects of the identified hazards. The concept of 'Expert System' and the proposal for a high level functional RPAS architecture oriented towards safety of specific operations have been carried out
- Finally evaluations on more recent safety analysis techniques, impacts on the performed safety analysis on current Italian RPAS regulation, and on hybrid RPAS have been performed

In the following Table 17 we finally summarize the main engineering results gained during the research work, the main novelties introduced by these results against the current state of art of knowledge about RPAS, the main limits of the methodology adopted to perform this research work and the main possible future developments of the engineering results described in this Dissertation.

Table 17 – Conclusions

	Engineering results	Novelties vs. RPAS state of art	Limits	Future works
Safety Management System for RPAS integrated in the not segregated airspace	Functional categorization of safety hazards introduced by RPAS operations within not segregated airspace	Performance of an extensive reliability and safety analysis on RPAS functional architecture and operations The lack of reliability data deriving from the absence of consistent historical databases and due to the fact that currently no extensive reliability tests have never been performed and results systematically collected (too much recent technology) has been recognised and highlighted	The reliability and safety analyses have been performed using qualitative methodologies due to the lack of RPAS reliability data The safety analysis has been performed using traditional methodologies based on system components single failure events as causal factors	Integration of the performed safety analysis with more recent system based hazards analysis methodologies like the STPA technique from 'Complex Systems' theory Development of a software based on artificial intelligence (with respect to which the 'Expert Systems' are precursors) integrating the designed 'Expert System' with an inference engine Functional integration of the artificial intelligence with the RPAS autopilot/Flight Management System and the RPAS failure sensor monitoring system for a real time effective mitigation of safety risk even during complex RPAS flight operations in the not segregated airspace Identification of valuable criteria to manage uncertainty of strategies to assess safety risk
	Allocation of hazards according to the EASA risk-based categorization of RPAS operations of interest (specific and certified)			
	Allocation of hazards according to the EUROCONTROL CONOPS (risks related to specific category operations in the VLL subspace; risks related to the certified category operations in the subspace between 500 feet of altitude from ground and FL600 and beyond)			
	Performance of the FMECA analysis on a complete RPAS functional architecture			
	Performance of the FTA analysis on a complete RPAS functional architecture			
	Performance of the analysis of some examples of hazards related to the human factor involved in the RPAS operations into the not segregated airspace			
	Full implementation of the risk matrices for RPAS operations both into uncontrolled and controlled airspaces			
	Evaluation of barriers/defences to prevent/mitigate the effects of safety hazards though the Bow Tie Method	Identification of mitigation strategies according to the basic definition of 'Safety Management System' (The continuous identification of safety hazards and application of mitigation strategies to maintain the risk level of the given system at or below an acceptable level)	The effectiveness of the 'Expert System' depends on the size hat is the number of rules composing the knowledge basis; this item, at its turn, depend on the level of detail of the correlated risk model	
	Design of the knowledge basis of an 'Expert System' to support the decision making process of the remote pilot on ground during RPAS specific category operations			
	Identification of a high level RPAS functional architecture oriented towards the mitigation of safety hazards during specific category operations			
	Evaluations of solutions for the operational deployment of the U-Space service from a safety perspective	Evaluation of U-space infrastructure in the light of the performed safety analysis		
	Identification of safety requirements for the deployment of the U-space service			
	Evaluation from a safety perspective of current RPAS Italian regulation	Evaluation of Italian RPAS regulation in the light of the performed safety analysis		

References

[1] International Civil Aviation Organization (ICAO), *Annex 19 presentation, https://www.icao.int/safety/SafetyManagement/Documents/Annex%2019%20-%20ICAO%20presentation%20-%20self%20instruction%2024September2013.pdf, 24th September 2013,* accessed on the web on the 05th November 2018

[2] International Civil Aviation Organization (ICAO), *Doc. 10019/AN 507, Manual on Remotely Piloted Aircraft. Systems (RPAS),* Montreal (Canada), First Edition, 2015

[3] International Civil Aviation Organization (ICAO), *Doc. 9859/AN 474, Safety Management Manual (SMM)*, Montreal (Canada), Third Edition, 2013

[4] International Civil Aviation Organization (ICAO), *Circular 328/AN 190, Unmanned Aerial Systems (UAS)*, Montreal (Canada), 2011

[5] *https://www.riseabove.com.au/products/futaba-14sg-flight-radio.html*, accessed on the web on the 18th February 2018

[6] *https://products.embention.com/veronte/control-station/hcs-suitcase*, accessed on the web on the 18th February 2018

[7] *http://www.ga-asi.com/advanced-cockpit-gcs*, accessed on the web on the 18th February 2018

[8] 2011-2012 UAS Yearbook, *UAS: the global perspective*, Pages 151/216, Ed. Blyenburgh&Co, Ninth Edition, June 2011 and *www.uvs-info.com*, accessed on the web on the 16th July 2018

[9] Prof. K. P. Valavanis, University of Denver, Colorado, United States of America, *UAS navigation and controls, a comprehensive approach, Lecture 'Hystory of UAS: Basics'*, Politecnico di Torino, Scuola Di Dottorato, Third Level Training Course, 8th_17th May 2018

[10] Radio Technical Commission for Aeronautics (RTCA), *DO-304, Guidance Material and Considerations for Unmanned Aircraft*, Systems, 2007

[11] European Organization for Civil Aviation Equipment (EUROCAE), *ER-0004 Volume 1, General considerations for civilian operation of Unmanned Aircraft*, November 2010

[12] Single European SKY ATM Research (SESAR), *European ATM Master Plan, Roadmap for the safe integration of drones in all classes of airspaces*

[13] *SESAR Drones Outlook Study*, *http://www.sesarju.eu/sites/default/*

files/documents/reports/European_Drones_Outlook_Study_2016.pdf, accessed on the web on the 12th October 2018

[14] European Commission, Commission Staff Working Document, *Impact Assessment, accompanying the Proposal for a Regulation of the European Parliament and of the Council on common rules in the field of civil aviation and establishing a European Civil Aviation Safety Agency, and repealing regulation (EC) number 216/2008 of the European Parliament and of the Council*, Brussel (Belgium), 2015

[15] European Parliament and Council, *Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC*, Brussel (Belgium), 2008

[16] Završnik, A., *Drones & UAV, Legal and social implications for security and surveillance*, Springer, 2016, https://doi.org/10.1007/978-3-319-23760-2

[17] Prof. K. P. Valavanis, University of Denver, Colorado, United States of America, *UAS navigation and controls, a comprehensive approach, Lecture 'UAS applications'*, Politecnico di Torino, Scuola Di Dottorato, Third Level Training Course, 8th_17th May 2018

[18] European Organisation for the Safety of Air Navigation (EUROCONTROL), *RPAS ATM CONOPS*, Edition 4.0, 21st February 2017

[19] International Civil Aviation Organization (ICAO), *Doc. 9854, Global Air Traffic Management Concept*, First Edition, Montreal (Canada), 2005

[20] Sándor, Z., *Challenges Caused by the Unmanned Aerial Vehicle in the Air Traffic Management*, Periodica Polytechnica Transportation Engineering, 47(2), pp. 96-105. DOI: https://doi.org/10.3311/PPtr.11204

[21] Universal Avionics Systems Corporation, *Understanding Required Navigation Performance (RNP) and Area Navigation (RNAV) operations*, White Paper, Document No.WHTP-2013-16-10, October 2013

[22] International Civil Aviation Organization (ICAO), *Doc. 9613/AN937, Performance Navigation Based (PBN) manual*, Third Edition, Montreal, (Canada), 2008

[23] International Civil Aviation Organization (ICAO), *Doc. 9849/AN457, Global Navigation Satellite System (GNSS) manual*, Second Edition, Montreal (Canada), 2012

[24] *Wikipedia, https://en.wikipedia.org/wiki/Primary_radar*, accessed on the Web on the 07th May 2018

[25] Todaro, G., *Study, integration and risk analysis of Augmentation Systems*, Master Thesis, Politecnico di Torino, March 2018

[26] European Space Agency, *EGNOS brochure*, BR-284, ISBN 978-92-9221-012-0, ISSN 0250-1589, 2009

[27] European Safety Aviation Agency (EASA), *Notice for Proposed Amendment 2017-05(A)*, RMT.0230, 4th May 2017

[28] European Safety Aviation Agency (EASA), *Opinion No. 01/2018, Introduction of a regulatory framework for the operation of unmanned aircraft systems in the 'open' and 'specific' categories, Related NPA/CRD: 2017-05(A)*, RMT.0230, 6th February 2018

[29] European Organisation for the Safety of Air Navigation (EUROCONTROL) and European Safety Aviation Agency (EASA), *UAS ATM integration, Operational concept*, Edition 1.0, 27th November 2018

[30] SESAR Joint Undertaking, *U-Space Blueprint*, Luxembourg, 2017, DOI:10.2829/335092

[31] International Civil Aviation Organization, NACC/DCA/08 - IP/12, *Automatic Dependant Surveillance Broadcast (ADS-B out): ensuring preparedness for the 2020 equipage mandate*, Information Paper, 5th September 2017

[32] International Civil Aviation Organization (ICAO), *Annex 2, Rules of the Air*, Tenth Edition, Montreal (Canada), July 2005

[33] International Civil Aviation Organization (ICAO), *Doc. 4444, Procedures for Air Navigation Services, Air Traffic Management*, Sixteenth Edition, Montreal (Canada), November 2016

[34] Burdett, H., Stoker, J., Simpson A., *Functional Hazard Assessment (FHA) Report for Unmanned Aircraft Systems*, EBENI Limited, Issue 2, 22nd November 2009

[35] *https://www.sesarju.eu/node/2993*, accessed on the web on the 5th February 2019

[36] Single European Sky ATM Research Joint Undertaking (SESAR JU), *Demonstrating RPAS integration in the European aviation system, A summary of SESAR drone demonstration projects results*, SESAR Joint Undertaking, Bruxelles (Belgium), 2016

[37] Centro Italiano Ricerche Aerospaziali (CIRA), *SESAR Joint Undertaking RPAS 0.3 RAID Demonstration Report, SESAR Joint Undertaking*, First Edition, Bruxelles (Belgium), 2016

[38] Grimaccia, F., Bonfante, F., Battipede, M., Maggiore, P., Filippone, E., *Risk analysis of the future implementation of a Safety Management System for multiple RPAS based on first demonstration flights*, Electronics, MDPI, 2017, DOI: 10.3390/electronics6030050

[39] National Aeronautics and Space Administration (NASA), *Functional requirements document for HALE UAS operations in the NAS Step 1*, Version 3, January 2006

[40] *http://downloads.bowtiepro.com/Bowtie%20Pro%20Methodology.pdf*, accessed on the web on the 10th April 2018

[41] *http://www.clipsrules.net/*, accessed on the web on the 21st August 2018

[42] Leveson, N. G., *Engineering a safer world: systems thinking applied to safety*, The MIT Press, Cambridge MA (United States of Americ), 2011;

available online at the URL: http://mitpress.mit.edu/books/engineering-safer-world, accessed on web on the 24th June 2017

[43] Dr. Simon Place, *Hazard identification and risk management, risk management notes* 'Safety in Aviation', Cranfield University, United Kingdom, Short Course, 4th_8th September 2017, Lecture hold on the 7th September 2017

[44] Deloitte Consulting S.r.l. Aviation & Transportation, *HFACS human factors approach to accident analysis classification system prevention*, Short Course, 2016

[45] https://www.researchgate.net/figure/The-HFACS-framework_fig1_255713130, accessed on the web on the 27th March 2018

[46] Washington, A., Reece, A. C., Jose, S., *A review of unmanned aircraft system ground risk models*, Progress in Aerospace Science, Volume 95, pp 24-44, Elsevier, November 2017, https://doi.org/10.1016/j.paerosci.2017.10.001

[47] Luxhøj, J. T., Öztekin, A., *A regulatory-based approach to safety analysis of Unmanned Aircraft Systems*, Department of Industrial and Systems Engineering, Rutgers University, Piscataway NJ (United States of America)

[48] Williams, K. W., *A summary of Unmanned Aircraft Accident/Incident data: human factors implications*, FAA Civil Aerospace Medical Institute, Oklahoma City OK (United States of America)

[49] *https://dronewars.net/drone-crash-database/*, accessed on the web on the 16th September 2018

[50] National Transportation Safety Board, *Customs and border protection Predator B accident*, Safety report, Nogales AZ (United States of America), 25th April 2006

[51] *Military Standard 1629 Revision A*, Department of Defence, United States of America, 1980

[52] Denson, W., Chandler, G., Crowell, W., Wanner, R., *DTIC, Non electronic parts reliability data*, Reliability Analysis Centre, Rome NY (United States of America), 1991

[53] Tyrone L. J., *Handbook of reliability prediction procedures for mechanical equipment*, Revision A, Naval Surface Warfare Centre, Carderok Division, West Bethesda MD (United States of America), 2nd May 2006

[54] Military Handbook 217 Revision F, *Reliability prediction of electronic equipment*, Revision F, Department of Defence, United States of America, 1991

[55] Petritoli, E., Leccese, F., Ciani, L., *Reliability and maintenance analysis of Unmanned Aerial Vehicles*, Sensors, MDPI, 19th September 2018, DOI:10.3390/s18093171

[56] Olson, I. J., Atkins, E. M., *Qualitative failure analysis for a small quadrotor Unmanned Aircraft System*, University of Michigan MI (United States of America), 2013, DOI: 10.2514/6.2013-4761

[57] Freeman, P. M., *Reliability assessment for low-cost Unmanned Aerial Vehicles*, Ph.D. Dissertation, University of Minnesota MN (Unites States of America), November 2014

[58] Reimann, S., Amos, J., Bergquist, E., Cole, J., Phillips, J., Shuster, S., Professor P. Seiler (Advisor), *UAV for reliability*, AEM 4331 – Aerospace Vehicle Design. 19th December 2013

[59] *http://www.uesystems.com/news/the-50-failure-modes-of-electric-motors*, accessed on the web on the 06th August 2018

[60] Doughty, D. H., *Failure mechanisms of Li-ion batteries*, Battery Safety Consulting Inc. Presentation to National Transportation Safety Board, Albuquerque NM (Unites States of America), April 11th 2013

[61] *https://oscarliang.com/monitor-measure-battery-voltage-alarm-drone/*, accessed on the web on the 8th January 2019

[62] *http://www.tjinguytech.com/charging-how-tos/balance-connectors*, accessed on the web on the 9th January 2019

[63] *https://www.igus.ca/_wpck/pdf/US_en/TechTalk-6-Common-Cable-Failure-Modes.pdf*, accessed on the 8th January 2019

[64] International Atomic Energy Agency (IAEA), *Component reliability data for use in probabilistic safety assessment*, Wien, 1988

[65] Bijjahalli, S., Gardi, A., Sabatini, R., *GNSS performance modelling for positioning and navigation in urban environments*, Conference Paper, 5th IEEE International Workshop on Metrology for AeroSpace, June 2018, DOI: 10.1109/MetroAeroSpace.2018.8453544

[66] European Aviation Safety Agency (EASA), *Seasonal Technical Communication*, June 2018

[67] Syd Ali, B., Ochieng, W., Majumdar, A., Schuster, W., Kian Chiew, T. (2014), *ADS-B system failure modes and models*, Journal of Navigation, 67(6), pp 995-1017, DOI:10.1017/S037346331400037X

[68] Ali, B., Ochieng, W., Majumdar, A., (2017), *ADS-B: probabilistic safety assessment, Journal of Navigation*, 70(4), pp 887-906, DOI:10.1017/S0373463317000054

[69] *https://www.unmannedsystemstechnology.com/wp-content/uploads/2013/05/SDN500-INS-GPS-Datasheet.pdf*, accessed on the web on the 19th January 2019

[70] *https://en.wikipedia.org/wiki/Radio_jamming*, accessed on the 18th September 2018

[71] *https://en.wikipedia.org/wiki/Spoofing_attack#Preventing_GPS_spoofing*, accessed on the 18th September 2018

[72] European Global Navigation Satellite System Agency, *EGNOS Safety of Life (SoL) service definition document*, 26th September 2016

[73] Pullen, S., *Augmented GNSS: fundamentals and keys to integrity and continuity*, Department of Aeronautics and Astronautics, Stanford University, CA (United States of America), 16th September 2011

[74] Shin, K., H., Shin, D, Joung, E., J., Kim, Y., G., *The reliability and safety enhancement method of GNSS for train control application*, Proceedings of the 23rd International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2008), Japan

[75] Cobham Avionics Integrated Systems, *GPS - WAAS receiver data sheet Texas, United States of America, 2008, https://www.cobham.com/media/153262/gps-waas_datasheet.pdf*, accessed on the web on the 07th February 2019

[76] Gables Engineering, *G7614 Series ATC/TCAS/Flight ID with ADS-B Fault Annunciator, https://www.gableseng.com/gei/wp-content/uploads/2017/08/G7614-Series-ADSB-Fact-Sheet-Rev-03-Final.pdf*, accessed on the web on the 07th February 2019

[77] Defence and Space Electronic Systems, Honeywell International Inc., *Air Data Unit Product family data sheet, 2003, https://aerocontent.honeywell.com/aero/common/documents/myaerospacecatalog-documents/MilitaryAC/Air_Data_Products.pdf*, Minneapolis MN (United States of America), accessed on the web on the 07th February 2019

[78] Yang, Z., Lin, F., Chen, B.M., *Survey of autopilot for multi-rotor unmanned aerial vehicles, Conference paper*, IECON 2016, 23th_26th October 2016, DOI: 10.1109/IECON.2016.7793820,

[79] Bogucki, J., Wielowieyska, E., *Reliability of line-of-sight radio-relay systems*, Journal of Telecommunication and Information Technology, 2006

[80] De Oliveira Martins Franco, B. J., Sandoval Góes, L. C., *Failure analysis methods in Unmanned Aerial Vehicles*, Proceedings of COBEM 2007, 19th International Congress of Mechanical Engineering, ABCM, 2007

[81] Freeman, P., Balas, G. J., *Actuation Failure Modes and Effects Analysis for a Small UAV A*, American Control Conference (ACC), 978-1-4799-3271-9, Portland OR (United States of America) June 4th-6th, 2014

[82] Höflinger, J., Hofmann, P., *Thermal management of a fuel cell range-extended electric vehicle*, Springer, 2017, DOI 10.1007/978-3-658-19224-2_7

[83] Töpler, J., Lehmann, J., *Hydrogen and fuel cell technologies and market perspectives*, Springer, 2016, DOI 10.1007/978-3-662-44972-1

[84] Department of Defence, *Military Handbook 338 Revision B*, United States of America, 1998

[85] Kirwan, B., *Technical basis for a human reliability assessment capability for air traffic safety management*, EUROCONTROL, 2007

[86] McCarley, J. S., Wickens, C. D., *Human factor concerns in UAV flight*, University of Illinois IL (United States of America)

[87] Ranquist, E., Steiner, A. M., Argrow, B., *Exploring the range of weather impacts on UAS operations*, University of Colorado Boulder, CO (Unites States of America), 2017

[88] International Civil Aviation Organization (ICAO), *Doc. 9974/ANB 487, Flight safety and volcanic ash*, First edition, Montreal (Canada), 2012

[89] *https://en.wikipedia.org/wiki/Expert_system*, accessed on the web on the 3rd October 2018

[90] Kaczor, K., Bobek, S., Nalepa, G. J., *Overview of expert system shells*, Institute of Automatics, AGH University of Science and Technology, Inzynieria wiedzy, Kraków (Poland), 12.05.2010, http://geist.agh.edu.pl

[91] *https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_expert_systems.htm*, accessed on the web on the 3rd October 2018

[92] Dutta, A., Bhattacharyya, A., *Expert Systems*, IETE Journal of Education, 2006, DOI: 10.1080/09747338.2006.11415860

[93] *http://psych.utoronto.ca/users/reingold/courses/ai/cache/expert.htm*, accessed on the web on the 4th October 2018

[94] *http://www.clipsrules.net/*, accessed on the web on the 3rd October 2018

[95] Joint Authorities for Rulemaking on Unmanned Systems (JARUS), *JARUS guidelines on Specific Operations Risk Assessment (SORA)*, Document identifier JAR-DEL-WG6-D.04, Edition 1.0, 26th June 2017

[96] Capello, E., Dentis, M., Guglieri, G., Novaro Mascarello, L., Spanò Cuomo L., *An innovative cloud-based supervision system for the integration of RPAS in urban environments*, Transportation Research Procedia, Volume 28, pp 191-200, Open access, 2017, https://doi.org/10.1016/j.trpro.2017.12.185

[97] *https://uavionix.com/products/ping1090/,* accessed on the web on the 20th October 2018

[98] *The Unmanned Air System Traffic Management (UTM) directory by www.Unmannedairspace.info*, accessed on the web on the 8th December 2018

[99] *https://www.airmap.com/utm/*, accessed on the web on the 18th October 2018

[100] *https://www.vodafone.com/content/index/media/vodafone-group-releases/2018/iot-drone-tracking.html#*, accessed on the web on the 20th October 2018

[101] Itkin, M., Kim, M., Park, Y., *Development of cloud-based RPAS monitoring and management system*, Sensors, 16, 1913, 15th November 2016, DOI:10.3390/s161119133

[102] Ishimatsu, T., Levenson, N., Thomas J., Katahira M., Miyamoto, Y., Nakao H., *Modeling and hazard analysis using STPA*, Proceedings of the 4th IAASS Conference, Making Safety Matter, 19th–21st May 2010, Huntsville AL (United States of America)

[103] Plioutsias, A., Karanikas, N., Chatzimihailidou, M. M., *Hazard analysis and safety requirements for small drone operations: to what extent do popular drones embed safety? Risk Analysis*, Volume 38, No. 3, 2018, DOI: 10.1111/risa.12867

[104] Ente Nazionale Aviazione Civile (ENAC), *Remotely Piloted Aircraft Systems regulation*, Second Edition, 16th July 2015; Fourth amendment, 21st May 2018

[105] *https://www.enac.gov.it/la-normativa/normativa-enac/note-informative/ni-2017-007*, accessed on the web on the 22nd October 2018

[106] Colucci, M., *Electric propulsion for sports use (Propulsione elettrica per uso portivo)*, Master Degree Thesis, Politecnico di Torino, 2013

[107] Bonfante F., Dalla Vedova, M. D. L., *Evaluations on hydrogen fuel cells as a source of energy for specific operations category civil RPAS systems*, WSEAS Transactions on Environment and Development, Volume 14, E-ISSN: 2224-3496, April 2018

[108] Sammes, N., *Fuel cell technology reaching towards commercialization*, Springer, 2006

[109] Valavanis, K. P., Vachtsevanos, G. J., *Handbook of Unmanned Aerial Vehicles*, Springer, 2015

[110] SAE international, *Innovative all-electric motor glider project*, 2012. http://papers.sae.org/2013-01-2114

[111] Höflinger, J., Hofmann, P., *Thermal management of a fuel cell range-extended electric vehicle*, Springer, 2017, DOI: 10.1007/978-3-658-19224-2_7

[112] Osenar, P., Sisco, J., Reid, C., *Advanced propulsion for small Unmanned Aerial Vehicles, The role of fuel cell based energy systems for commercial* UAVs, Ballard White Paper, 2017

[113] Töpler, J. Lehmann, J., *Hydrogen and fuel cell technologies and market perspectives*, Springer, 2016, DOI 10.1007/978-3-662-44972-1

Appendix A – Failure Modes and Effects and Criticality Analysis (FMECA) – Results

System definition: see the following sections of FMECA analysis
System mission phases definition: see the following sections of FMECA analysis

FMECA analysis: performed according to Military Standard 1629 Revision A [51]
Classification of occurrences according to the following severity ranking:

Table 18 – Severity ranking [51]

Description	Classification	Mishap definition	Severity number (SN)
Catastrophic	I	Death or system loss	4
Critical	II	Severe injury/Major property damage/Major system damage resulting in system loss	3
Marginal	III	Minor injury/Minor property damage/Minor system damage with delay or loss of system availability or mission degradation	2
Minor	IV	Failure not serious enough to cause injury, property damage or system damage, but which will result in unscheduled maintenance or repair	1

Classification of occurrences according to the following occurrence probability ranking:

Table 19 – Probability of occurrence [51]

Level	Occurrence	Description	Occurrence number	Probability number (PN)
A	Frequent	High probability of occurrence	> 0,20 of the overall probability of failure during the item operating time interval	5
B	Reasonably probable	Moderate probability of occurrence	> 0,10 and < 0,20 of the overall probability of failure during the item operating time interval	4
C	Occasional	Occasional probability of occurrence	> 0,01 and < 0,10 of the overall probability of failure during the item operating time interval	3
D	Remote	Unlikely probability of occurrence	> 0,001 and < 0,01 of the overall probability of failure during the item operating time interval	2
E	Extremely unlikely	Essentially zero	< 0,001 of the overall probability of failure during the item operating time interval	1

Detectability ranking:

Table 20 – Detectability ranking [51]

Detection method	Ranking
Visual or audible warning devices	1
Automatic sensing devices	2
Sensing instrumentation	3
Other methods	4
None	5

Compensating provisions:

Table 21 – Compensating provisions [51]	
Compensating provision	**Design solutions:**
	Provision of a design that foresees redundant items that allow continued and safe operation
	Provision of safety or relief devices such as monitoring or alarm provisions which permit effective operation or limit damage
	Provision of alternative modes of operation such as backup or standby items or systems
	Operator actions:
	Compensating provisions which require operator action to circumvent or mitigate the effect of the postulated failure. The compensating provision that best satisfies the indication(s) observed by an operator when the failure occurs shall be determined. This may require the investigation of an interface system to determine the most correct operator action(s) . The consequences of any probable incorrect action(s) by the operator in response to an abnormal indication should be considered and recorded

Criticality matrix (from Military Standard 1629 Revision A [51]):

Table 22 – Criticality level [51]

Probability of occurrence / Severity level	CATEGORY IV - MINOR	CATEGORY III - MARGINAL	CATEGORY II - CRITICAL	CATEGORY I - CATASTROPHIC
LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				
LEVEL D – REMOTE				
LEVEL E – EXTREMELY UNLIKELY				

Criticality increase

System definition: rotor wing RPAS:

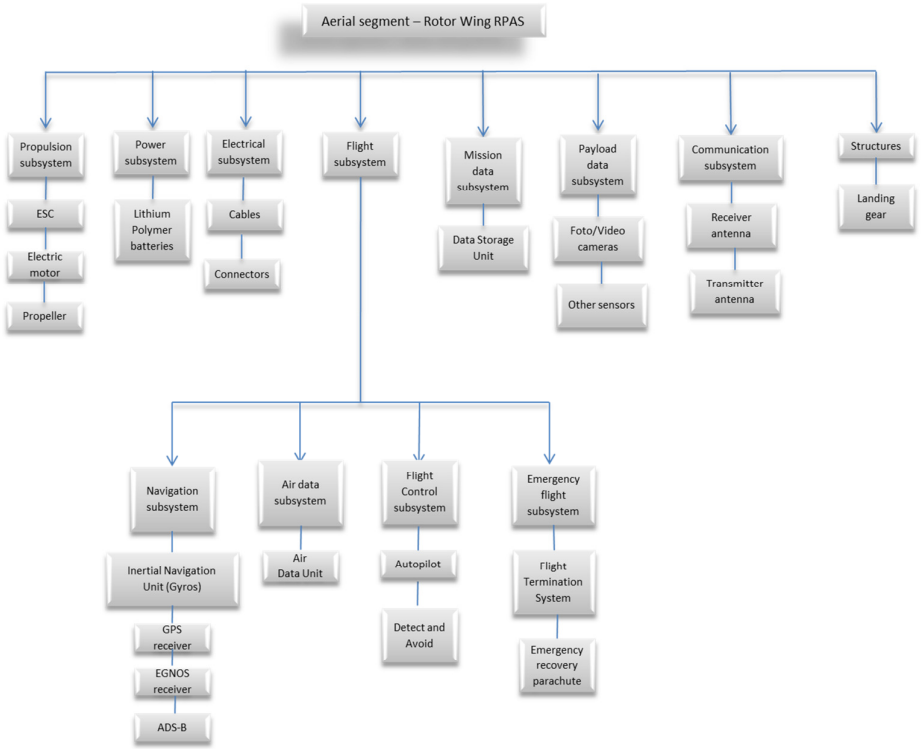


Figure 31 – Rotor wing RPAS

Mission phases: rotor wing RPAS:

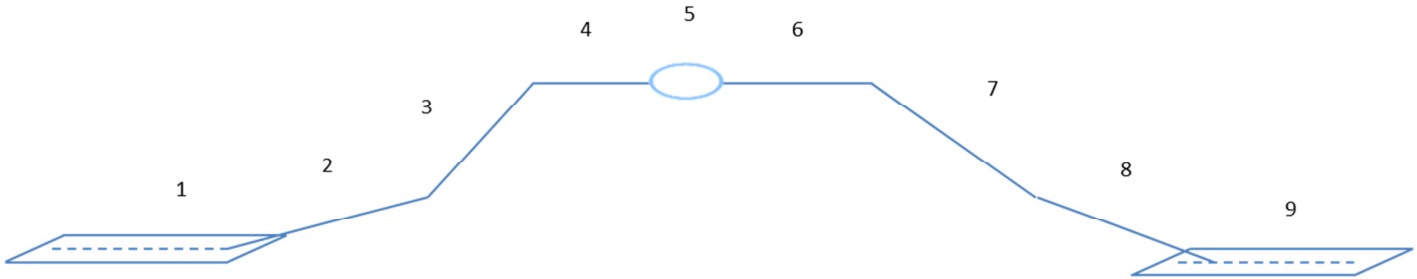


Figure 32 – Rotor wing RPAS mission phases [80]

Table 23 – RPAS mission phases [80]

Mission phase number	Mission phase name
1	Taxi – Engines power on
2	Take-off
3	Climb
4	Cruise
5	Loiter – Use of payload in the mission area
6	Cruise
7	Descent
8	Landing
9	Taxi – Engines shutdown

Table 24 – Mission phases [80]

RPAS Flight functionality potentially involved	Mission phases (Rotor wing RPAS)						
	1, 2	3	4	5	6	7	8, 9
Start-up subsystem	X	X	X	X	X	X	X
Structures	X	X	X	X	X	X	X
Propulsion subsystem	X	X	X	X	X	X	X
Power subsystem	X	X	X	X	X	X	X
Electrical subsystem	X	X	X	X	X	X	X
Flight Navigation subsystem	-	X	X	X	X	X	-
Flight Information subsystem	-	X	X	X	X	X	-
Flight control subsystem	-	X	X	X	X	X	-
Emergency flight subsystem	-	X	X	X	X	X	-
Mission data subsystem	X	X	X	X	X	X	X
Payload data subsystem	-	-	-	X	-	-	-
Communication Command and Control subsystem	X	X	X	X	X	X	X
Ground Control Station subsystem	X	X	X	X	X	X	X

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 25 – Subsystem: Propulsion Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Electronic Speed Control (ESC)	To allow aerial segment maneuverability	PSS1a	ESC seizing	Improper ESC startup sequence/ Catching in environment hazard/Full degradation/ Burnt out ESC	2, 3, 4, 5, 6, 7, 8	-	Loss of engine speed control	System loss	Catastrophic	4	C	3	None	4	12	48	Design solution (Provision of an RPM sensing device [56])	-
Electronic Speed Control (ESC)	To allow aerial segment maneuverability	PSS1b	ESC degradation	Prolonged use/ Particles in motor housing	2, 3, 4, 5, 6, 7, 8	-	Loss of engine speed control	System loss	Catastrophic	4	C	3	None	4	12	48	Operator actions (Performance of proper maintenance on ground [56])	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 25 – Subsystem: Propulsion Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Electronic Speed Control (ESC)	To allow aerial segment maneuverability	PSS1c	ESC overheating	Prolonged use/Seized motors/ Overdraw on current/ Poor air circulation/ Hot environment	2, 3, 4, 5, 6, 7, 8	-	Loss of engine speed control	System loss	Catastrophic	4	C	4	None	5	4	20	Design solution (Proper length of testing on ground [56])	-
Electronic Speed Control (ESC)	To allow aerial segment maneuverability	PSS1d	ESC burnout	Prolonged overheating	2, 3, 4, 5, 6, 7, 8	-	Loss of engine speed control	System loss	Catastrophic	4	C	3	None	5	12	60	Design solution (Provision of an RPM sensing device [56])	-
Electrical brushless motor	Thrust generation	PSS2a	Cranked stator housing	Fatigue/ External shock/ Vibration	2, 3, 4, 5, 6, 7, 8	Loss of engine	Loss of thrust	System loss	Catastrophic	4	D	2	None	5	16	80	Operator actions (Performance of proper maintenance on ground [59])	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 25 – Subsystem: Propulsion Subsystem (Con't)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Electrical brushless motor	Thrust generation	PSS2b	Worn bearings	Poor lubrication/ Contamination/ Overloading/ High temperature	2, 3, 4, 5, 6, 7, 8	Loss of engine	Loss of thrust	System loss	Catastrophic	4	C	3	None	5	12	60	Operator actions (Performance of proper maintenance on ground [59])	-
Electrical brushless motor	Thrust generation	PSS2c	Windings open circuit	Excessively high temperature	2, 3, 4, 5, 6, 7, 8	Loss of engine	Loss of thrust	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (Performance of proper maintenance on ground [59])	-
Electrical brushless motor	Thrust generation	PSS2d	Armature shaft structural damage	Fatigue/ Misalignment/ Bearing failure	2, 3, 4, 5, 6, 7, 8	Loss of engine	Loss of thrust	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (Performance of proper maintenance on ground [59])	-

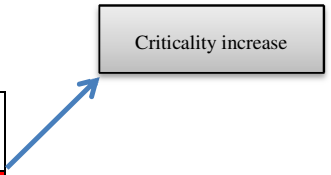
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 25 – Subsystem: Propulsion Subsystem (Con't)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Propeller	Lift generation	PSS3a	Propeller structural failure	Fatigue/ Vibration/ Collision with an obstacle	2, 3, 4, 5, 6, 7, 8	Loss of propeller	Loss of thrust	System loss	Catastrophic	4	E	1	None	5	4	20	Design solutions (Provision of redundant equipment)	-
Propeller	Lift generation	PSS3b	Propeller connection failure	Fatigue/ Vibration	2, 3, 4, 5, 6, 7, 8	Loss of propeller	Loss of thrust	System loss	Catastrophic	4	D	2	None	5	8	40	Design solutions (Provision of redundant equipment)	-
Propeller	Lift generation	PSS3c	Abrupt stop of the propeller	Friction/ Wear/Lack of lubrication/ Low or improper lubrication	2, 3, 4, 5, 6, 7, 8	Loss of propeller	Loss of thrust	System loss	Catastrophic	4	E	1	None	5	4	20	Operator actions (Performance of proper maintenance on ground)	-

Table 26 – Propulsion Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				ESC seizing (PSS1a) ESC degradation (PSS1b) ESC overheating (PSS1c) ESC burn out (PSS1d) Worn bearings (PSS2b)
LEVEL D – REMOTE				Cranked stator housing (PSS2a) Windings open circuit (PSS2c) Armature shaft structural failure (PSS2d) Propeller connection failure (PSS3b)
LEVEL E – EXTREMELY UNLIKELY				Propeller structural failure (PSS3a) Abrupt stop of the propeller (PSS3c)
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 27 – Subsystem: Power Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
LiPo battery	Electrical power generation	PWSS1a	Short circuit	Heat/ External overheating/ High rate operation (causing overheat)/ Internal short circuit (hot spot)/ External short circuit/Over charge/Over discharge	2, 3, 4, 5, 6, 7, 8	Loss of battery	Loss or decrease of electrical power/ Loss of thrust	System loss	Catastrophic	4	C	3	Visual or audible warning devices [61]	1	12	12	Design solutions (Provision of redundant equipment)	-
LiPo battery	Electrical power generation	PWSS1b	Mechanical damage	Crush/Nail Penetration/ Drop/ Mechanical Shock/ Vibration /Water Immersion	2, 3, 4, 5, 6, 7, 8	Loss of battery	Loss or decrease of electrical power/Loss of thrust	System loss	Catastrophic	4	C	3	None	5	12	60	Design solutions (Provision of redundant equipment)	-

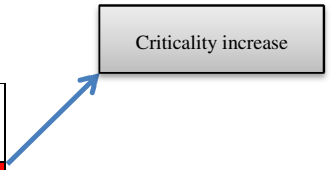
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 27 – Subsystem: Power Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
LiPo battery	Electrical power generation	PWSS1c	Fire	Overheat/ Thermal ramp/Fire	2, 3, 4, 5, 6, 7, 8	Loss of battery	Loss or decrease of electrical power/Loss of thrust	System loss	Catastrophic	4	C	3	None	5	12	60	Design solutions (Provision of redundant equipment)	-

Table 28 – Power Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				Short circuit (PWSS1a) Mechanical damage(PWSS1b) Fire (PWSS1c)
LEVEL D – REMOTE				
LEVEL E – EXTREMELY UNLIKELY				
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 29 – Subsystem: Electrical Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
JST/XH balance cables	Electrical power distribution	ESS1a	Short circuit	Insulation breakdown/ Fatigue	2, 3, 4, 5, 6, 7, 8	-	Loss or decrease of electrical power	System loss	Catastrophic	4	C	3	None	5	12	60	Operator actions (Performance of proper maintenance on ground)	-
JST/XH balance cables	Electrical power distribution	ESS1b	Open circuit	Fatigue/ Vibrations/ Mechanical shock	2, 3, 4, 5, 6, 7, 8	-	Loss or decrease of electrical power	System loss	Catastrophic	4	A	5	None	5	20	100	Operator actions (Performance of proper maintenance on ground)	-
Distribution cables	Electrical power distribution	ESS2a	Short circuit	Insulation breakdown/ Fatigue	2, 3, 4, 5, 6, 7, 8	-	Loss or decrease of electrical power	System loss	Catastrophic	4	C	3	None	5	12	60	Operator actions (Performance of proper maintenance on ground)	-

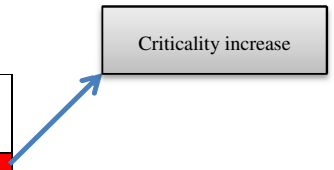
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 29 – Subsystem: Electrical Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Distribution cables	Electrical power distribution	ESS2b	Open circuit	Fatigue/ Vibrations/ Mechanical shock	2, 3, 4, 5, 6, 7, 8	-	Loss or decrease of electrical power	System loss	Catastrophic	4	A	5	None	5	20	100	Operator actions (Performance of proper maintenance on ground)	-
Connectors	Electrical power distribution	ESS3	Electric arc	Mechanical disconnection /Fatigue/ Vibrations/ Shock	2, 3, 4, 5, 6, 7, 8	-	Loss or decrease of electrical power	System loss	Catastrophic	4	C	3	None	5	12	60	Operator actions (Performance of proper maintenance on ground)	-

Table 30 – Electrical Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				Open circuit (ESS1b) Open circuit (ESS2b)
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				Short circuit (ESS1a) Short circuit (ESS2a) Electric arc (ESS3)
LEVEL D – REMOTE				
LEVEL E – EXTREMELY UNLIKELY				
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Inertial Measurement Unit	Measurement of angular rates and of translation accelerations	NSS1a	Circuitry overload	Power surge/ Electric static discharge	2, 3, 4, 5, 6, 7, 8	Inaccurate inertial measurements	Incorrect data reported to the flight computer	Inaccurate flight data/ Mission degradation	Marginal	2	D	2	None	5	4	20	Design solutions (Provision of redundant equipment, use of surge protection, use of proper ground circuit)	-
Inertial Measurement Unit	Measurement of angular rates and of translation accelerations	NSS1b	Calibration loss	Reset to factory default/ Vibrations on equipment connections/ Cables damage/ Disconnection from power surge	2, 3, 4, 5, 6, 7, 8	Inaccurate inertial measurements	Incorrect data reported to the flight computer	Inaccurate flight data/ Mission degradation	Marginal	2	C	3	None	5	6	30	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
GPS	System navigation in 3D space	NSS2a	GPS antenna failure	Amplifier oscillation	2, 3, 4, 5, 6, 7, 8	-	-	Mission degradation	Marginal	2	E	1	Visual or audible warning devices	1	4	4	Design solutions (Provision of redundant equipment)	-
GPS	System navigation in 3D space	NSS2b	GPS signal jamming	External malicious interference	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	E	1	None	5	4	20	Design solutions (Design against cyber threats)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
GPS	System navigation in 3D space	NSS2c	GPS signal spoofing	External malicious interference	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	B	4	Other methods	4	16	64	Design solutions (Design against cyber threats)/ Operator actions (Operator actions: training on manual RPAS flight parameters monitoring; switching from automatic to manual flight mode)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
European Geostationary Navigation Overlay System (EGNOS)	System navigation in 3D space	NSS3a	EGNOS receiver failure	Receiver cables disconnected or damaged/ Damaged RX ports/ Wrong antenna polarization settings	2, 3, 4, 5, 6, 7, 8	EGNOS receiver functionality degradation	ADS-B functionality degradation	Mission degradation	Marginal	2	A	5	Visual or audible warning devices	1	10	10	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-
European Geostationary Navigation Overlay System (EGNOS)	System navigation in 3D space	NSS3b	Loss of EGNOS signal continuity	Environmental conditions (ionosphere effects)/ Unscheduled satellite outages	2, 3, 4, 5, 6, 7, 8	EGNOS receiver functionality degradation	ADS-B functionality degradation	Mission degradation	Marginal	2	D	2	Visual or audible warning devices	1	4	4	Design solutions (Provision of redundant equipment)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
European Geostationary Navigation Overlay System (EGNOS)	System navigation in 3D space	NSS3c	Loss of EGNOS signal integrity	The error associated to the position is larger than the alert limits defined for the intended operation	2, 3, 4, 5, 6, 7, 8	EGNOS receiver functionality degradation	ADS-B functionality degradation	Mission degradation	Marginal	2	E	1	Visual or audible warning devices	1	2	2	Design solutions (Provision of redundant equipment)	-
European Geostationary Navigation Overlay System (EGNOS)	System navigation in 3D space	NSS3d	EGNOS signal delay	Ionosphere dispersion effect	2, 3, 4, 5, 6, 7, 8	EGNOS receiver functionality degradation	ADS-B functionality degradation	Mission degradation	Marginal	2	D	2	Visual or audible warning devices	1	4	4	Design solutions (Provision of redundant equipment)	-
ADS-B	In flight surveillance	NSS4a	Loss of EGNOS position accuracy	Equipment aging	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	A	5	None [67]	5	20	100	Operator actions (Performance of proper maintenance on ground [67]))	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
ADS-B	In flight surveillance	NSS4b	EGNOS receiver unit failure	Lack of calibration/ Maintenance	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	B	2	Visual or audible warning devices [67]	1	8	8	Design solutions (Provision of redundant GPS receiver [67])	-
ADS-B	In flight surveillance	NSS4c	ADS-B OUT antenna failure	Equipment aging	2, 3, 4, 5, 6, 7, 8	Incorrect data broadcast	-	System loss	Catastrophic	4	C	3	None [67]	5	12	60	Operator actions (Check for ADS-B data integrity validation [67])	-
ADS-B	In flight surveillance	NSS4d	ADS-B OUT antenna deterioration	Lak of maintenance/ Lack of calibration	2, 3, 4, 5, 6, 7, 8	Incorrect data broadcast	-	System loss	Catastrophic	4	A	5	None [67]	5	20	100	Operator actions (Check for ADS-B data integrity validation [67])	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
ADS-B	In flight surveillance	NSS4e	Signal interruption	Intentional/ unintentional RF interference	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	A	5	None [67]	5	20	100	Operator actions (Check for ADS-B data integrity validation [67])	-
ADS-B	In flight surveillance	NSS4f	Emitter/ transponder failure	Lak of maintenance/ Lack of calibration	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	A	5	None [67]	5	20	100	Operator actions (Check for ADS-B data integrity validation [67])	-
ADS-B	In flight surveillance	NSS4g	Erroneous altitude data	Altimeter failure/ Altitude encoder failure/Pitot tube failure	2, 3, 4, 5, 6, 7, 8	Erroneous data transmission to the ADS-B emitter	-	System loss	Catastrophic	4	E	1	None [67]	5	4	20	Operator actions (Performance of proper maintenance on ground [67])	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
ADS-B	In flight surveillance	NSS4h	Data encoding error	Software error/ Encoder error	2, 3, 4, 5, 6, 7, 8	Incorrect altitude data transmitted to the ADS-B emitter	-	System loss	Catastrophic	4	E	1	None [67]	5	4	20	Operator actions (Performance of proper maintenance on ground [67])	-
ADS-B	In flight surveillance	NSS4i	Intentional/ unintentional jamming of ADS-B signal	Loss of position data to be sent to the emitter	2, 3, 4, 5, 6, 7, 8	Loss of position data to be transmitted to the ADS-B emitter	-	System loss	Catastrophic	4	E	1	Visual or audible warning devices [67]	1	4	4	Design solutions (Provision of other backup on board navigation system like, for example – Inertial Navigation System (INS) [67])	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
ADS-B	In flight surveillance	NSS4I	Lack of ADS-B service	Satellite failure	2, 3, 4, 5, 6, 7, 8	Loss of ADS-B service	-	System loss	Catastrophic	4	E	1	Visual or audible warning devices [67]	1	4	4	Design solutions (Provision of other backup on board navigation system like, for example – Inertial Navigation System (INS) [67])	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
ADS-B	In flight surveillance	NSS4m	Inaccurate position datum sent to the ADS-B emitter	EGNOS receiver malfunction/ EGNOS loss of accuracy	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	A	5	Visual or audible warning devices [67]	1	20	20	Design solutions (Provision of other backup on board navigation system like, for example – Inertial Navigation System (INS) [67])	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
ADS-B	In flight surveillance	NSS4n	Degradation of accuracy and integrity of data sent by the satellite to the ADS-B	EGNOS failure	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	E	1	Visual or audible warning devices [67]	1	4	4	Design solutions (The ADS-B emitter shall reject corrupted position data relying on position accuracy indicator (HFOM) from EGNOS [67])	-
ADS-B	In flight surveillance	NSS4o	Failure of ADS-B transponder/ emitter on the RPA	Short circuit	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	C	3	Visual or audible warning devices [67]	1	12	12	Design solutions (Provision of redundant emitter/ transponder [67])	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
ADS-B	In flight surveillance	NSS4p	Failure in detection of maneuvering aircraft/RPA	EGNOS antenna loss of sensitivity	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	A	5	Visual or audible warning devices [67]	1	20	20	Design solutions (Provision of redundant INS or EGNOS receiver [67])	-
ADS-B	In flight surveillance	NSS4q	Sudden loss of ADS-B data to ATC controllers without any notification	Ground equipment failure/ Loss of power supply	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	D	2	Visual or audible warning devices [67]	1	8	8	Design solutions (Provision of redundant power supply source for the ADS-B station [67])	-
ADS-B	In flight surveillance	NSS4r	ADS-B IN receiving antenna deterioration	Poor maintenance/ Lack of antenna calibration	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	C	3	Visual or audible warning devices [67]	1	12	12	Operator action (Performance of proper maintenance and calibration on ground [67])	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 31 – Subsystem: Flight Subsystem/Navigation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
ADS-B	In flight surveillance	NSS4s	ADS-B ground station failure	Poor maintenance	2, 3, 4, 5, 6, 7, 8	Incorrect data displayed to the ATC controller	-	System loss	Catastrophic	4	D	2	None [67]	5	8	40	Operator actions (Performance of proper maintenance on ground of ADS-B ground segment [67])	-
ADS-B	In flight surveillance	NSS4t	Performance of wrong preflight procedures on ADS-B	Remote pilot human error/Lack of preflight checks	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	D	3	None [67]	5	12	60	Operator actions (Performance of more training)	-

Criticality increase

Table 32– Flight Subsystem/Navigation Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				EGNOS receiver failure (NSS3a) Loss of EGNOS position accuracy (NSS4a) Inaccurate position datum sent to the ADS-B emitter (NSS4m) Failure in detection of manoeuvring aircraft/RPA (NSS4p)
LEVEL B – REASONABLY PROBABLE				EGNOS receiver unit failure (NSS4b) ADS-B OUT antenna deterioration (NSS4d) Signal interruption (NSS4e)
LEVEL C – OCCASIONAL				Calibration loss (NSS1b) ADS-B OUT antenna failure (NSS4c) Emitter/transponder failure (NSS4f) Failure of ADS-B transponder/ emitter on the RPA (NSS4o) ADS-B IN receiving antenna deterioration (NSS4r)
LEVEL D – REMOTE				Circuitry overload (NSS1a) Loss of EGNOS signal continuity (NSS3b) EGNOS signal delay (NSSd) Sudden loss of ADS-B data to ATC controllers without any notification (NSS4q) ADS-B ground station failure (NSS4s) Performance of wrong preflight procedures on ADS-B (NSS4t)
LEVEL E – EXTREMELY UNLIKELY				GPS antenna failure (NSS2a) GPS signal jamming (NSS2b) GPS signal spoofing (NSS2c) Loss of EGNOS signal integrity (NSS3c) Erroneous altitude data (NSS4g) Data encoding error (NSS4h) Intentional/unintentional jamming of ADS-B signal (NSS4i) Lack of ADS-B service (NSS4l) Degradation of accuracy and integrity of data sent by the satellite to the ADS-B (NSS4n)
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 33– Subsystem: Flight Subsystem/Air Data Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Air Data Unit	Measurement and provision of airspeed and barometric altitude	ADSS1a	Incorrect signal	Reduction of signal level/Impedance mismatch/Analogue to digital conversion failure	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurement	Incorrect air data reported to computer	System loss	Catastrophic	4	A	5	None	5	20	100	Design solutions (Provision of redundant GPS for altitude measurement)/ Operator action (Performance of proper maintenance on ground)	-
Air Data Unit	Measurement and provision of airspeed and barometric altitude	ADSS1b	Loss of signal	Chip failure/ Corrosion	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurement	Incorrect air data reported to computer	System loss	Catastrophic	4	A	5	None	5	20	100	Design solutions (Provision of redundant GPS for altitude measurement)/ Operator action (Performance of proper maintenance on ground)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 33 – Subsystem: Flight Subsystem/Air Data Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Air Data Unit	Measurement and provision of airspeed and barometric altitude	ADSS1c	Signal error along the transmission line	Interference on the line	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurement	Incorrect air data reported to computer	System loss	Catastrophic	4	C	3	None	5	12	60	Design solutions (Provision of redundant GPS for altitude measurement)/ Operator action (Performance of proper maintenance on ground)	-
Air Data Unit	Measurement and provision of airspeed and barometric altitude	ADSS1d	Error on output signal	Error in the sensor algorithm	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurement	Incorrect air data reported to computer	System loss	Catastrophic	4	C	3	None	5	12	60	Design solutions (Provision of redundant GPS for altitude measurement)/ Operator action (Performance of proper maintenance on ground)	-

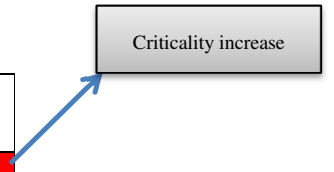
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 33 – Subsystem: Flight Subsystem/Air Data Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Air Data Unit	Measurement and provision of airspeed and barometric altitude	ADSS1e	Loss of power supply	Failure in power supply/Mechanical disconnection from power supply	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurement	Incorrect air data reported to computer	System loss	Catastrophic	4	A	5	None	5	20	100	Design solutions (Provision of redundant GPS for altitude measurement)/ Operator action (Performance of proper maintenance on ground)	-
Air Data Unit	Measurement and provision of airspeed and barometric altitude	ADSS1f	Calibration error	Error in the sensor algorithm	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurement	Incorrect air data reported to computer	System loss	Catastrophic	4	C	3	None	5	12	60	Design solutions (Provision of redundant GPS for altitude measurement)/ Operator action (Performance of proper maintenance on ground)	-

Table 34 – Subsystem/Air Data Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				Incorrect signal (ADSS1a) Loss of signal (ADSS1b) Loss of power supply (ADSS1e)
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				Signal error along the transmission line (ADSS1c) Error on output signal (ADSS1d) Calibration error (ADSS1f)
LEVEL D – REMOTE				
LEVEL E – EXTREMELY UNLIKELY				
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 35 – Subsystem: Flight Subsystem/Flight Control Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Autopilot Unit	Vehicle flight control and management	FCSS1a	Failure of weak joints	Over-temperature	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	D	2	Visual or audible warning devices	1	8	8	Design solutions (Provision of a redundant item)	-
Autopilot Unit	Vehicle flight control and management	FCSS1b	Lack of power supply	Vibrations/ Damaged wiring	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	D	2	Visual or audible warning devices	1	8	8	Design solutions (Provision of a redundant item)	-
Autopilot Unit	Vehicle flight control and management	FCSS1c	Software error	Lack of pass/fail signal	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	D	2	Visual or audible warning devices	1	8	8	Design solutions (Provision of a redundant item)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 35 – Subsystem: Flight Subsystem/Flight Control Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Detect and Avoid	Mid-air collision avoidance	FCSS2a	ADS-B IN receiving antenna deterioration	Poor maintenance/ Lack of antenna calibration	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	C	3	Visual or audible warning devices [67]	1	12	12	Operator action (Performance of proper maintenance and calibration on ground [67])	-
Detect and Avoid	Mid-air collision avoidance	FCSS2b	EGNOS receiver failure	Receiver cables disconnected or damaged/ Damaged RX ports/ Wrong antenna polarization settings	2, 3, 4, 5, 6, 7, 8	EGNOS receiver functionality degradation	ADS-B functionality degradation	Mission degradation	Marginal	2	A	5	Visual or audible warning devices	1	10	10	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-

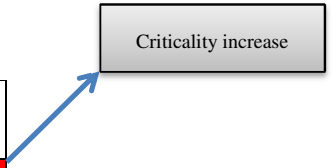
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 35 – Subsystem: Flight Subsystem/Flight Control Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Detect and Avoid	Mid-air collision avoidance	FCSS2c	Erroneous altitude data	Altimeter failure/ Altitude encoder failure/Pitot tube failure	2, 3, 4, 5, 6, 7, 8	Erroneous data transmission to the ADS-B emitter	-	System loss	Catastrophic	4	E	1	None [67]	5	4	20	Operator actions (Performance of proper maintenance on ground [67]	-

Table 36 – Flight Subsystem/Flight Control Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				EGNOS receiver failure (FCSS2b)
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				ADS-B IN receiving antenna deterioration (FCSS2a)
LEVEL D – REMOTE				Failure of weak joints (FCSS1a) Lack of power supply (FCSS1b) Software error (FCSS1c)
LEVEL E – EXTREMELY UNLIKELY				Erroneous altitude data (FCSS2c)
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 37 – Subsystem: Flight Subsystem/Emergency Flight Termination Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Flight Termination System	To allow minimization of risks for people/ infrastructures on ground during emergency flight mission plan termination	EFSS1a	Loss of dedicated radio link	Electro-magnetic interference	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	C	3	Visual or audible warning devices	1	12	12	Design solutions (Provision of redundant radio link)	-
Flight Termination System	To allow minimization of risks for people/ infrastructures on ground during emergency flight mission plan termination	EFSS1b	Lack of functionality	Loss of power supply	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	D	2	Visual or audible warning devices	1	8	8	Design solutions (Provision of redundant item)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 37 – Subsystem: Flight Subsystem/Emergency Flight Termination Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Flight Termination System	To allow minimization of risks for people/ infrastructures on ground during emergency flight mission plan termination	EFSS1c	Unlawful interference on dedicated radio link (jamming)	Intentional malicious interference	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	B	4	Visual or audible warning devices	1	16	16	Design solutions (Provision of protections against electromagnetic interference)	-
Emergency recovery parachute	To allow minimization of risks for people/ infrastructures on ground during emergency flight mission plan termination	EFSS2a	Loss of dedicated radio link	Electro-magnetic interference	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	C	3	Visual or audible warning devices	1	12	12	Design solutions (Provision of redundant radio link)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 37 – Subsystem: Flight Subsystem/Emergency Flight Termination Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Emergency recovery parachute	To allow minimization of risks for people/ infrastructures on ground during emergency flight mission plan termination	EFSS2b	Lack of functionality	Loss of power supply	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	D	2	Visual or audible warning devices	1	8	8	Design solutions (Provision of redundant item)	-
Emergency recovery parachute	To allow minimization of risks for people/ infrastructures on ground during emergency flight mission plan termination	EFSS2c	Unlawful interference on dedicated radio link (jamming)	Intentional malicious interference	2, 3, 4, 5, 6, 7, 8	-	-	System loss	Catastrophic	4	B	4	Visual or audible warning devices	1	16	16	Design solutions (Provision of protections against electromagnetic interference)	-

Table 38 – Flight Subsystem/Emergency Flight Termination Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				Unlawful interference on dedicated radio link (jamming) (EFSS1c) Unlawful interference on dedicated radio link (jamming) (EFSS2c)
LEVEL C – OCCASIONAL				Loss of dedicated radio link (EFSS1a) Loss of dedicated radio link (EFSS2a)
LEVEL D – REMOTE				Lack of functionality (EFSS1b) Lack of functionality (EFSS2b)
LEVEL E – EXTREMELY UNLIKELY				
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC

Criticality increase

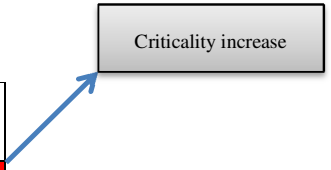
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 39 – Subsystem: Mission Control Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Data Storage Unit	Storage of mission data	MCSS1a	Loss of mission software	Electromagnetic interference	3, 4, 5, 6, 7	Loss of mission data	-	Mission degradation	Marginal	2	C	3	Other methods	4	6	24	Operator action (Performance of preflight checks)	-
Data Storage Unit	Storage of mission data	MCSS1b	Physical unit degradation	Vibrations/ Mechanical shock/ Electric shock	3, 4, 5, 6, 7	Loss of mission data	-	Mission degradation	Marginal	2	C	3	Other methods	4	6	24	Operator action (Performance of preflight checks)	-

Table 40 – Mission Control Subsystem failure modes criticality matrix

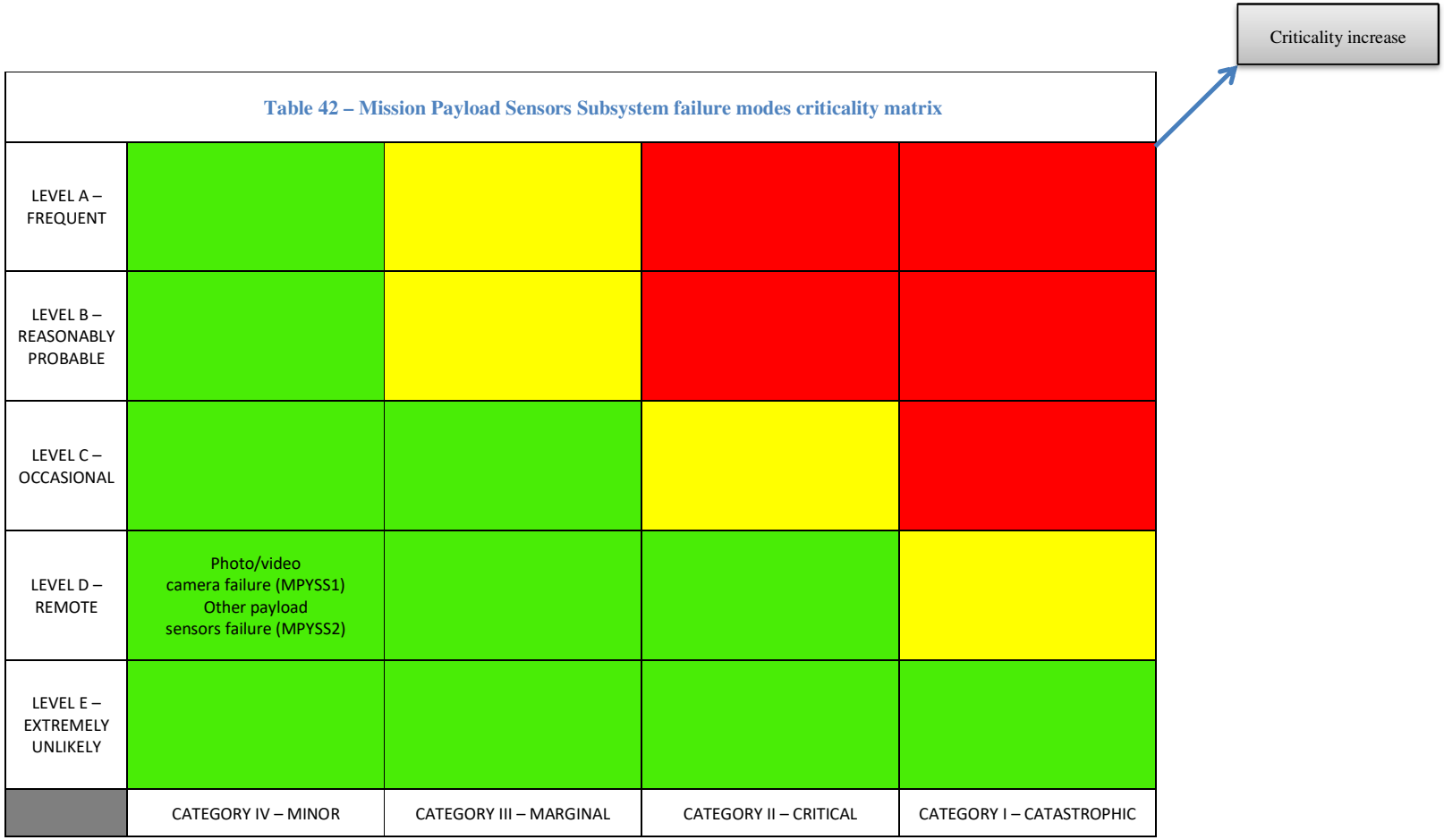
LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL		Loss of mission data software (MCSS1a) Physical unit degradation (MCSS1b)		
LEVEL D – REMOTE				
LEVEL E – EXTREMELY UNLIKELY				
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 41 – Subsystem: Mission Payload Sensors Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Payload Photo/video camera sensors	Photo/ video data recording	MPYSS1	According to sensor type and technology	According to sensor type and technology	5	Loss of functionality	Loss of payload data	-	Minor	1	D	2	Visual or audible warning devices	1	2	2	Operator actions (Performance of proper maintenance on ground)	-
Other payload sensors	Other functions depending on the sensor used	MPYSS2	According to sensor type and technology	According to sensor type and technology	5	Loss of functionality	Loss of payload data	-	Minor	1	D	2	Visual or audible warning devices	1	2	2	Operator actions (Performance of proper maintenance on ground)	-


Criticality increase
Table 42 – Mission Payload Sensors Subsystem failure modes criticality matrix
LEVEL A – FREQUENT
LEVEL B – REASONABLY PROBABLE
LEVEL C – OCCASIONAL
LEVEL D – REMOTE
LEVEL E – EXTREMELY UNLIKELY
Photo/video camera failure (MPYSS1)
Other payload sensors failure (MPYSS2)
CATEGORY IV – MINOR
CATEGORY III – MARGINAL
CATEGORY II – CRITICAL
CATEGORY I – CATASTROPHIC

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 43 – Subsystem: On Board Communication Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
On board transmitting antenna	To send telemetry data to the ground segment	CSS1a	The on board transmitting antenna cannot process the control signal	Lack of power supply/ Failure in the electrical system/ Antenna intermitted	1,2,3,4, 5,6,7,8,9	-	-	System loss	Catastrophic	4	D	2	None	5	8	40	Design Solution (Provision of redundant equipment)	-
On board transmitting antenna	To send telemetry data to the ground segment	CSS1b	On board transmitting antenna fade	RPA shape and flight attitude/RPA airframe material	1,2,3,4, 5,6,7,8,9	-	-	System loss	Catastrophic	4	C	3	None	5	12	60	Design Solution (Provision of redundant equipment)	-
On board receiving antenna	To receive the flight command signals from the aerial segment	CSS2a	The on board receiving antenna cannot process the control signals	Lack of power supply/ Failure in the electrical system/ Antenna intermitted	1,2,3,4, 5,6,7,8,9	-	-	System loss	Catastrophic	4	D	2	None	5	8	40	Design Solution (Provision of redundant equipment)	-

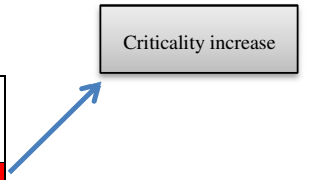
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 43 – Subsystem: On Board Communication Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
On board receiving antenna	To send telemetry data to the ground segment	CSS2b	On board receiving antenna fade	RPA shape and flight attitude/RPA airframe material	1,2,3,4, 5,6,7,8,9	-	-	System loss	Catastrophic	4	C	3	None	5	12	60	Design Solution (Provision of redundant equipment)	-

Table 44 – On Board Communication Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				On board transmitting antenna fade (CSS1b) On board receiving antenna fade (CSS2b)
LEVEL D – REMOTE				The on board transmitting antenna cannot process the control signal (CSS1a) The onboard receiving antenna cannot process the control signal (CSS2a)
LEVEL E – EXTREMELY UNLIKELY				
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 45 – Subsystem: Aerial segment structural frame

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Other structures	Not applicable (N/A)																	
Landing gear	Not applicable (N/A)																	

RPAS definition: Fixed wing RPAS:

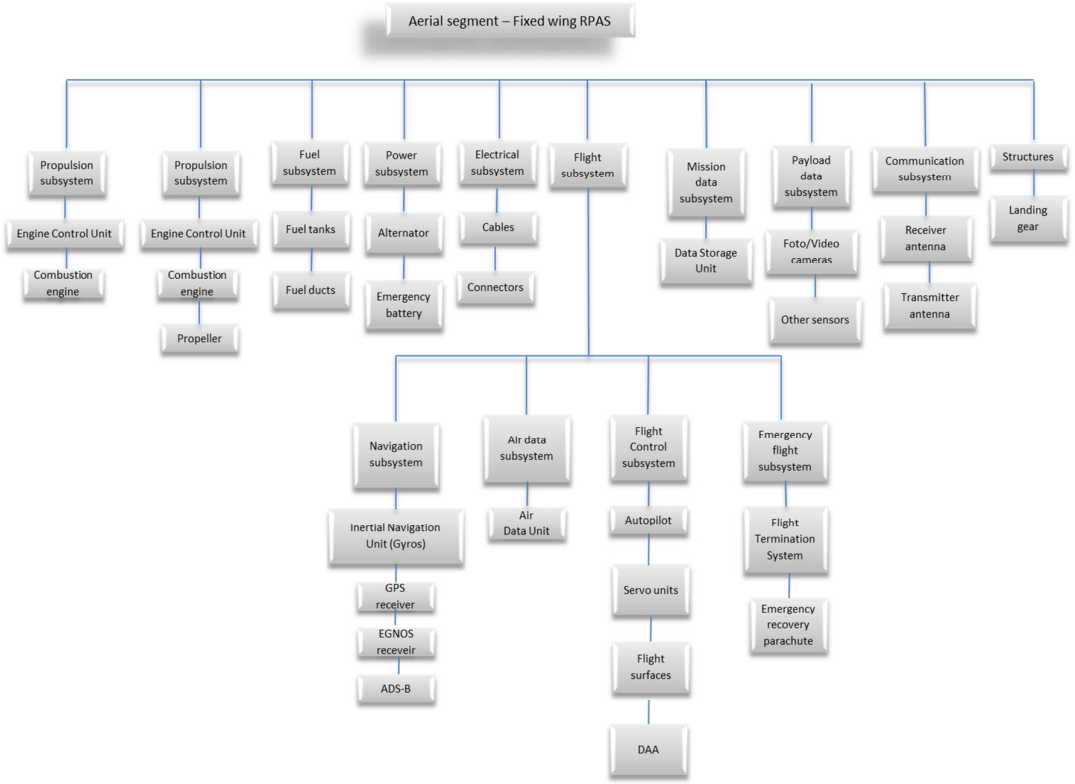


Figure 33 – Fixed wing RPAS

Mission phases: fixed wing RPAS

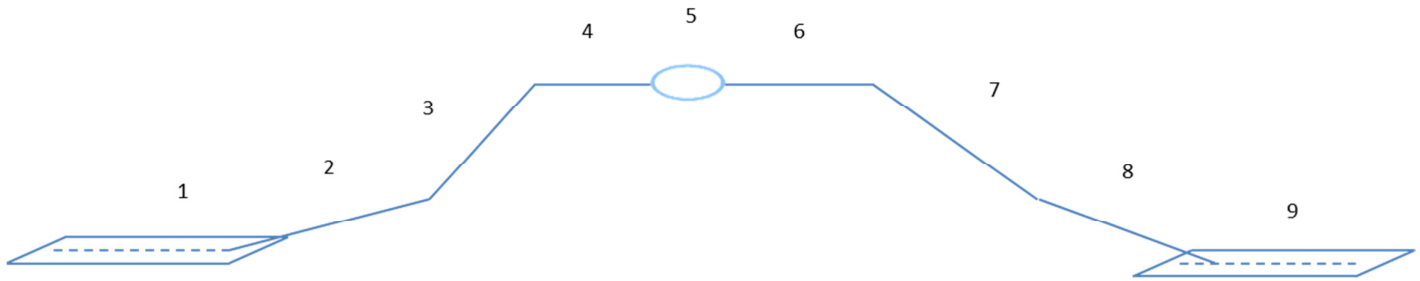


Figure 34 – Fixed wing RPAS mission phases [80]

Table 46 – RPAS mission phases [80]

Item	Mission phase name
1	Taxi – Engines power on
2	Take-off
3	Climb
4	Cruise
5	Loiter – Use of payload in the mission area
6	Cruise
7	Descent
8	Landing
9	Taxi – Engines shutdown

Table 47 – RPAS mission phases [80]

RPAS Flight functionality potentially involved	Mission phases (Fixed wing RPAS)						
	1, 2	3	4	5	6	7	8, 9
Start-up subsystem	X	X	X	X	X	X	X
Structures	X	X	X	X	X	X	X
Landing gear subsystem	X						X
Fuel subsystem	X	X	X	X	X	X	X
Propulsion subsystem	X	X	X	X	X	X	X
Power subsystem	X	X	X	X	X	X	X
Flight Navigation subsystem	-	X	X	X	X	X	-
Flight Information subsystem	-	X	X	X	X	X	-
Flight control subsystem	-	X	X	X	X	X	-
Flight control subsystem	-	X	X	X	X	X	-
Emergency flight subsystem	-	X	X	X	X	X	
Mission data subsystem	X	X	X	X	X	X	X
Payload data subsystem	-	-	-	X	-	-	-
Communication Command and Control subsystem	X	X	X	X	X	X	X
Ground Control Station subsystem	X	X	X	X	X	X	X

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 48 – Subsystem: Propulsion Subsystem (Combustion Engine)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Engine Control Unit	Engine management and control	PSCE1a	Software error	Error during software/firmware upgrade	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss of engine functionality	System Loss	Catastrophic	4	D	2	None	5	8	40	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-
Engine Control Unit	Engine management and control	PSCE1b	Mechanical failure	Controller failure/Actuator failure/Sensor failure/Control cable failure	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss of engine functionality	System Loss	Catastrophic	4	B	4	None	5	16	80	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 48 – Subsystem: Propulsion Subsystem (Combustion Engine) (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Engine Control Unit	Engine management and control	PSCE1c	Loss of on board computer	Loss of power supply	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss of engine functionality	System Loss	Catastrophic	4	E	1	None	5	4	20	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-
Engine Control Unit	Engine management and control	PSCE1d	Carburetor failure	Vibrations/ Human error	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss of engine functionality	System Loss	Catastrophic	4	C	3	None	12	5	60	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	
Engine	Conversion of fuel chemical energy in mechanical energy, thrust generation	PSCE2a	Engine control system failure	Carburetor failure/ Engine control unit failure	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of engine functionality	Loss of thrust	System Loss	Catastrophic	4	A	5	Visual or audible warning devices	1	20	20	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-

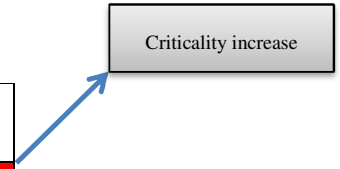
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 48 – Subsystem: Propulsion Subsystem (Combustion Engine) (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Engine	Conversion of fuel chemical energy in mechanical energy, thrust generation	PSCE2b	Mechanical failure	Wear/ Friction/ Lack of lubrication/ Improper lubrication/ Fatigue	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of engine functionality	Loss of thrust	System Loss	Catastrophic	4	C	3	None	5	12	60	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-
Engine	Conversion of fuel chemical energy in mechanical energy, thrust generation	PSCE2c	Engine fire	Loss of fuel/ Fuel tank damage/ Overheating	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of engine functionality	Loss of thrust	System Loss	Catastrophic	4	D	2	Visual or audible warning devices	1	8	8	Design solutions (Provision of redundant equipment)/ Operator actions (Proper maintenance on gro Performance of proper maintenance on ground und)	-
Engine	Conversion of fuel chemical energy in mechanical energy, thrust generation	PSCE2d	Use of improper fuel	Human error	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of engine functionality	Loss of thrust	System Loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (Performance of proper maintenance on ground)	-

Table 49 – Propulsion subsystem (with Combustion Engine) failure modes criticality matrix

LEVEL A – FREQUENT				Engine control system failure (PSCE2a)
LEVEL B – REASONABLY PROBABLE				Mechanical failure (PSCE1b)
LEVEL C – OCCASIONAL				Carburetor failure (PSCE1d) Mechanical failure (PCSE2b)
LEVEL D – REMOTE				Software error (PSCE1a) Engine fire (PSCE2c) Use of improper fuel (PSCE2d)
LEVEL E – EXTREMELY UNLIKELY				Loss of on board computer (PSCE1c)
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 50 – Subsystem: Propulsion Subsystem (Combustion Engine with propeller)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Engine Control Unit	Engine management and control	PSCEP1a	Software error	Error during software/firmware upgrade	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss of engine functionality	System Loss	Catastrophic	4	D	2	None	5	8	40	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-
Engine Control Unit	Engine management and control	PSCEP1b	Mechanical failure	Controller failure/Actuator failure/Sensor failure/Control cable failure	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss of engine functionality	System Loss	Catastrophic	4	B	4	None	5	16	80	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 50 – Subsystem: Propulsion Subsystem (Combustion Engine with propeller) (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Engine Control Unit	Engine management and control	PSCEP1c	Loss of on board computer	Loss of power supply	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss of engine functionality	System Loss	Catastrophic	4	E	1	None	5	4	20	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-
Engine Control Unit	Engine management and control	PSCEP1d	Carburetor failure	Vibrations/ Human error	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss of engine functionality	System Loss	Catastrophic	4	C	3	None	5	12	60	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 50 – Subsystem: Propulsion Subsystem (Combustion Engine with propeller) (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Engine	Conversion of fuel chemical energy in mechanical energy, thrust generation	PSCEP2a	Engine control system failure	Carburetor failure/ Engine control unit failure	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of engine functionality	Loss of thrust	System Loss	Catastrophic	4	A	5	Visual or audible warning devices	1	20	20	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-
Engine	Conversion of fuel chemical energy in mechanical energy, thrust generation	PSCEP2b	Mechanical failure	Wear/ Friction/ Lack of lubrication/ Improper lubrication/ Fatigue	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of engine functionality	Loss of thrust	System Loss	Catastrophic	4	C	3	None	5	12	60	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 50 – Subsystem: Propulsion Subsystem (Combustion Engine with propeller) (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Engine	Conversion of fuel chemical energy in mechanical energy, thrust generation	PSCEP2c	Engine fire	Loss of fuel/ Fuel tank damage/ Overheating	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of engine functionality	Loss of thrust	System Loss	Catastrophic	4	D	2	Visual or audible warning devices	1	8	8	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-
Engine	Conversion of fuel chemical energy in mechanical energy, thrust generation	PSCEP2d	Use of improper fuel	Human error	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of engine functionality	Loss of thrust	System Loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (Performance of proper maintenance on ground)	-

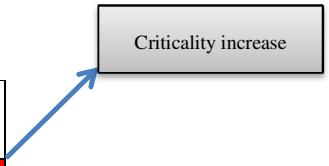
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 50 – Subsystem: Propulsion Subsystem (Combustion Engine with propeller) (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Propeller	Thrust generation	PSCEP3a	Propeller structural failure	Fatigue/ Vibration/ Collision with an obstacle	2, 3, 4, 5, 6, 7, 8	Loss of propeller	Loss of thrust	System loss	Catastrophic	4	E	1	None	5	4	20	Operator actions (Performance of proper maintenance on ground)	-
Propeller	Thrust generation	PSCEP3b	Propeller connection failure	Fatigue/ Vibration	2, 3, 4, 5, 6, 7, 8	Loss of propeller	Loss of thrust	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (Performance of proper maintenance on ground)	-
Propeller	Thrust generation	PSCEP3c	Abrupt stop of the propeller	Friction/ Wear/Lack of lubrication/ Low or improper lubrication	2, 3, 4, 5, 6, 7, 8	Loss of propeller	Loss of thrust	System loss	Catastrophic	4	E	1	None	5	4	20	Operator actions (Performance of proper maintenance on ground)	-

Table 51 – Propulsion Subsystem (Combustion Engine with Propeller) failure modes criticality matrix

LEVEL A – FREQUENT				Engine control system failure (PSCEP2a)
LEVEL B – REASONABLY PROBABLE				Mechanical failure (PSCEP1b)
LEVEL C – OCCASIONAL				Carburetor failure (PSCEP1d) Mechanical failure (PCSEP2b)
LEVEL D – REMOTE				Software error (PSCEP1a) Engine fire (PSCEP2c) Use of improper fuel (PSCEP2d) Propeller connection failure (PSCEP3b)
LEVEL E – EXTREMELY UNLIKELY				Loss of on board computer (PSCEP1c) Propeller structural failure (PSCEP3a) Abrupt stop of the propeller (PSCEP3c)
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 52 – Subsystem: Fuel Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Fuel tank	Fuel containment	FSS1	Structural damage	Shock/ Vibrations	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss of engine functionality	System Loss	Catastrophic	4	D	2	None	5	8	40	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-
Fuel pump	Fuel pressurization	FSS2	Mechanical failure	Fatigue/ Shock/ Vibrations	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss of engine functionality	System Loss	Catastrophic	4	D	2	Visual or audible warning devices	2	8	40	Operator actions (Performance of proper maintenance on ground)	-

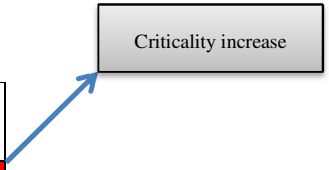
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 52 – Subsystem: Fuel Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Fuel pipelines	Fuel distribution	FSS3	Structural damage	Shock/ Vibrations/ Fatigue/ External stress/ Corrosion	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss of engine functionality	System Loss	Catastrophic	4	E	1	None	5	4	40	Design solutions (provision of anti-vibration devices)/ Operator actions (Performance of proper maintenance on ground)	-

Table 53 – Fuel Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				
LEVEL D – REMOTE				Structural failure (FSS1) Mechanical failure (FSS2)
LEVEL E – EXTREMELY UNLIKELY				Structural failure (FSS3)
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 54 – Subsystem: Power Generation Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Alternator	Alternate current generation	PWGSS1	Mechanical failure	Brushes failure/ Diodes failure	1, 2, 3, 4, 5, 6, 7, 8, 9	-	-	System Loss	Catastrophic	4	C	3	None	5	12	60	Operator actions (Performance of proper maintenance on ground)	-
Rectifier	Conversion of alternate current into direct current	PWGSS2a	Overheating	Excessive alternate current voltage	1, 2, 3, 4, 5, 6, 7, 8, 9	-	-	System Loss	Catastrophic	4	C	3	None	5	12	60	Operator actions (Performance of proper maintenance on ground)	-
Rectifier	Conversion of alternate current into direct current	PWGSS2b	Chemical failure	Corrosion	1, 2, 3, 4, 5, 6, 7, 8, 9	-	-	System Loss	Catastrophic	4	C	3	None	5	12	60	Operator actions (Performance of proper maintenance on ground)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 54 – Subsystem: Power Generation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Emergency battery	Direct current generation	PWGSS3a	Mechanical failure	Vibrations	1, 2, 3, 4, 5, 6, 7, 8, 9	-	-	System Loss	Catastrophic	4	D	2	None	5	8	40	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-
Emergency battery	Direct current generation	PWGSS3b	Thermal failure	Heat	1, 2, 3, 4, 5, 6, 7, 8, 9	-	-	System Loss	Catastrophic	4	D	2	None	5	8	40	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

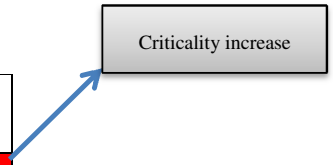
Table 54 – Subsystem: Power Generation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Emergency battery	Direct current generation	PWGSS3c	Chemical failure	Normal chemistry of charge/ discharge cycles	1, 2, 3, 4, 5, 6, 7, 8, 9	-	-	System Loss	Catastrophic	4	D	2	None	5	8	40	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-
Emergency battery	Direct current generation	PWGSS3d	Electrical failure	Short circuit	1, 2, 3, 4, 5, 6, 7, 8, 9	-	-	System Loss	Catastrophic	4	D	2	None	5	8	40	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-

:

Table 55 – Power Generation Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				Mechanical failure (PWGSS1) Electrical failure (PWGSS2a) Chemical failure (PWGSS2b)
LEVEL D – REMOTE				Mechanical failure (PWGSS3a) Thermal failure (PWGSS3b) Chemical failure (PWGSS3c) Electrical failure (PWGSS3d)
LEVEL E – EXTREMELY UNLIKELY				
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	
	EASA Weight class A3	< 25 kg	

Table 56 – Subsystem: Flight Subsystem/Air Data Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Air probe	Measurement of absolute and relative air pressure	ADSS1	Air probe clogging	Ice/Dust	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurements	Incorrect air data reported to computer	System loss	Catastrophic	4	B	4	None	5	16	80	Operator action (Performance of proper maintenance on ground)	
Air Data Unit	Measurement and provision of airspeed and barometric altitude	ADSS2a	Incorrect signal	Reduction of signal level/Impedance mismatch/Analogue to digital conversion failure	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurement	Incorrect air data reported to computer	System loss	Catastrophic	4	A	5	None	5	20	100	Design solutions (Provision of redundant GPS for altitude measurement)/ Operator action (Performance of proper maintenance on ground)	-
Air Data Unit	Measurement and provision of airspeed and barometric altitude	ADSS2b	Loss of signal	Chip failure/ Corrosion	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurement	Incorrect air data reported to computer	System loss	Catastrophic	4	A	5	None	5	20	100	Design solutions (Provision of redundant GPS for altitude measurement)/ Operator action (Performance of proper maintenance on ground)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	
	EASA Weight class A3	< 25 kg	

Table 56 – Subsystem: Flight Subsystem/Air Data Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Air Data Unit	Measurement and provision of airspeed and barometric altitude	ADSS2c	Signal error along the transmission line	Interference on the line	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurement	Incorrect air data reported to computer	System loss	Catastrophic	4	C	3	None	5	12	60	Design solutions (Provision of redundant GPS for altitude measurement)/ Operator action (Performance of proper maintenance on ground)	-
Air Data Unit	Measurement and provision of airspeed and barometric altitude	ADSS2d	Error on output signal	Error in the sensor algorithm	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurement	Incorrect air data reported to computer	System loss	Catastrophic	4	C	3	None	5	12	60	Design solutions (Provision of redundant GPS for altitude measurement)/ Operator action (Performance of proper maintenance on ground)	-

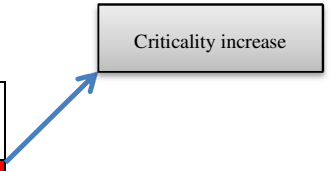
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: rotor wing aircraft	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	
	EASA Weight class A3	< 25 kg	

Table 56 – Subsystem: Flight Subsystem/Air Data Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Air Data Unit	Measurement and provision of airspeed and barometric altitude	ADSS2e	Loss of power supply	Failure in power supply/Mechanical disconnection from power supply	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurement	Incorrect air data reported to computer	System loss	Catastrophic	4	A	5	None	5	20	100	Design solutions (Provision of redundant GPS for altitude measurement)/ Operator action (Performance of proper maintenance on ground)	-
Air Data Unit	Measurement and provision of airspeed and barometric altitude	ADSS2f	Calibration error	Error in the sensor algorithm	2, 3, 4, 5, 6, 7, 8	Inaccurate air data measurement	Incorrect air data reported to computer	System loss	Catastrophic	4	C	3	None	5	12	60	Design solutions (Provision of redundant GPS for altitude measurement)/ Operator action (Performance of proper maintenance on ground)	-

Table 57 – Air Data Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				Incorrect signal (ADSS2a) Loss of signal (ADSS2b) Loss of power supply (ADSS2e)
LEVEL B – REASONABLY PROBABLE				Air probe clogging (ADSS1)
LEVEL C – OCCASIONAL				Signal error along the transmission line (ADSS2c) Error on output signal (ADSS2d) Calibration error (ADSS2f)
LEVEL D – REMOTE				
LEVEL E – EXTREMELY UNLIKELY				
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 58 – Subsystem: Flight Subsystem/Flight Controls Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Servo units	Control surface movement actuation	FCSS1a	Bias	Poor rigging/ Slippage of gears/ Bent linkages [81]	1, 2, 3, 4, 5, 6, 7, 8, 9	Inaccurate servo unit positioning	Low attitude control	Mission loss	Critical	3	C	3	None	5	9	45	Design solutions (provision of controller to compensate bias [81])	-
Servo units	Control surface movement actuation	FCSS1b	Stuck surface	Damaged linkage/ Broken servo driveshaft/ Unbalanced surface [81]	1, 2, 3, 4, 5, 6, 7, 8, 9	Blocked surface	No attitude control	System Loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (Performance of proper maintenance on ground)	-
Servo units	Control surface movement actuation	FCSS1c	Hardover	Broken linkage/ Broken servo driveshaft/ Unbalanced surface [81]	1, 2, 3, 4, 5, 6, 7, 8, 9	Blocked surface	No attitude control	System Loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (Performance of proper maintenance on ground)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 58 – Subsystem: Flight Subsystem/Flight Controls Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Servo units	Control surface movement actuation	FCSS1d	Floating surface	Broken linkage/ Broken servo driveshaft [81]	1, 2, 3, 4, 5, 6, 7, 8, 9	Inaccurate servo unit positioning	Low attitude control	System Loss	Catastrophic	4	C	2	None	5	8	40	Design solutions (provision of redundant equipment)	-
Servo units	Control surface movement actuation	FCSS1e	Oscillatory modes	Software bug/Faulted RxMux [81]	1, 2, 3, 4, 5, 6, 7, 8, 9	Inaccurate servo unit positioning	Low attitude control	System Loss	Catastrophic	4	D	2	None	5	8	40	Design solutions (Design of a control robust against oscillatory modes [81])	-
Servo units	Control surface movement actuation	FCSS1f	Increased dead band/stiction	Slippage of gears/ Damaged servo driveshaft [81]	1, 2, 3, 4, 5, 6, 7, 8, 9	Inaccurate servo unit positioning	Low attitude control	Mission degradation/ System Loss	Catastrophic	4	D	2	None	5	8	40	Design solutions (Design of a control robust against oscillatory modes [81])	-

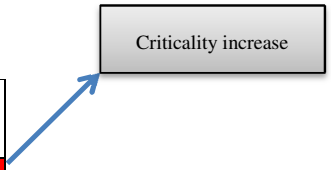
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 58 – Subsystem: Flight Subsystem/Flight Controls Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Servo units	Lift generation	FCSS1g	Structural damage	Lack of preventive maintenance	2, 3, 4, 5, 6, 7, 8	Blocked surface	Complete lack of attitude control	System Loss	Catastrophic	4	E	1	None	5	4	20	Operator actions (Performance of proper maintenance on ground)	-

Table 59 – Flight Control Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				Bias (FCSS1a) Floating surface (FCSS1d)
LEVEL D – REMOTE				Stuck surface (FCSS1b) Hardover (FCSS1c) Oscillatory modes (FCSS1e) Increased dead band/stiction (FCSS1f)
LEVEL E – EXTREMELY UNLIKELY				Structural damage (FCSS2)
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 60 – Subsystem: Flight structures

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Fuselage	Lift generation	Not applicable (N/A)																
Wings	Lift generation	Not applicable (N/A)																
Empennages	Lift generation	Not applicable (N/A)																
Landing gear	Taxi/Take-off/Landing	Not applicable (N/A)																

System definition: Hybrid RPAS (Hydrogen fuel cell + Electrical motor)

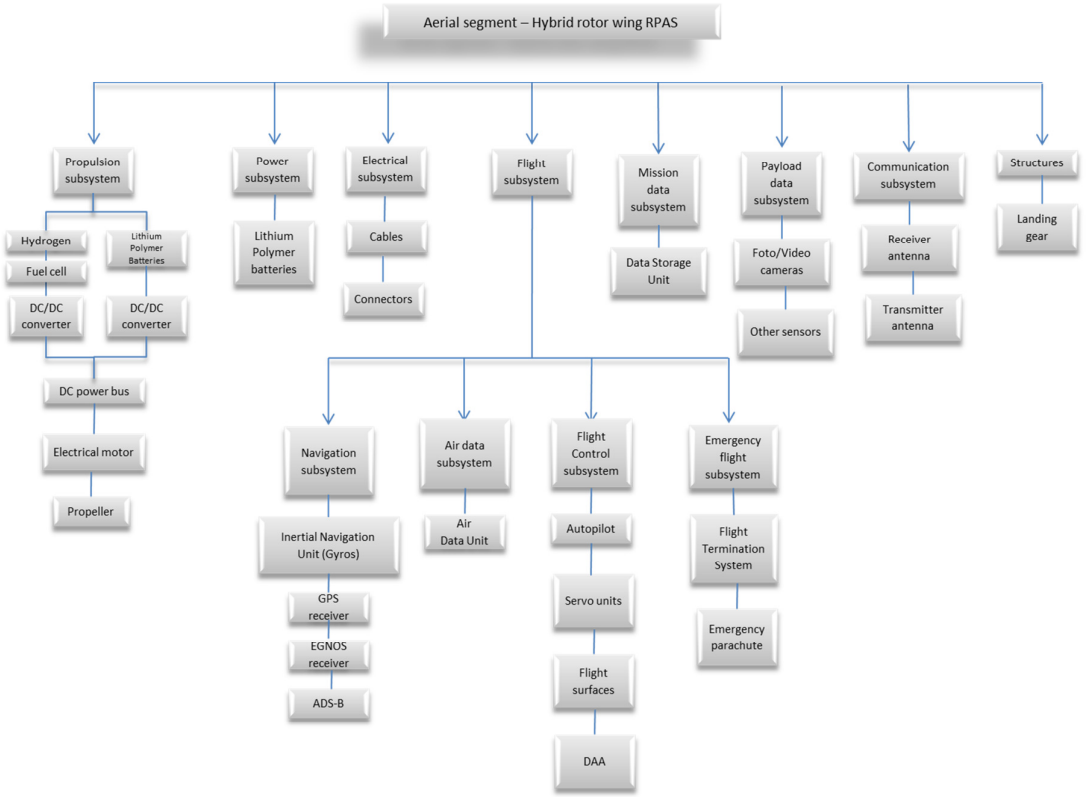


Figure 35 – Hybrid RPAS

Mission phases: hybrid RPAS

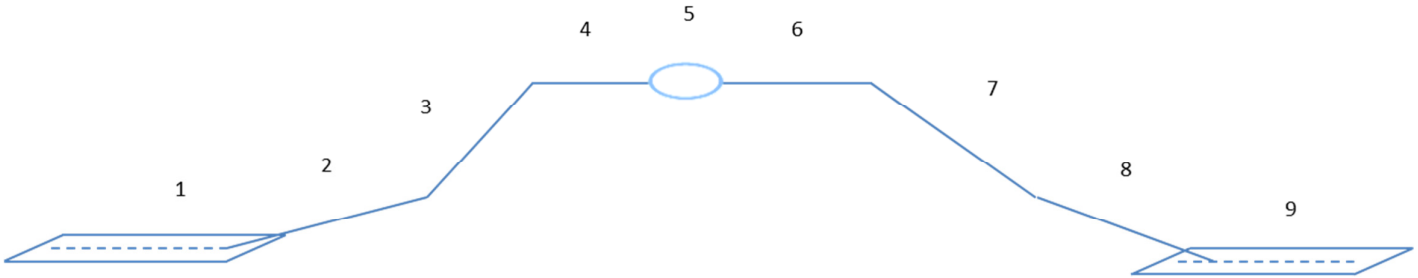


Figure 36 – Hybrid RPAS mission phases [80]

Table 61 – RPAS mission phases [80]

Item	Mission phase name
1	Taxi – Engines power on
2	Take-off
3	Climb
4	Cruise
5	Loiter – Use of payload in the mission area
6	Cruise
7	Descent
8	Landing
9	Taxi – Engines shutdown

Table 62 – Mission phases [80]

RPAS Flight functionality potentially involved	Mission phases (Hybrid RPAS (Electrical motor + Fuel cells)						
	1, 2	3	4	5	6	7	8, 9
Start-up subsystem	X	X	X	X	X	X	X
Structures	X	X	X	X	X	X	X
Landing gear subsystem	X	-	-	-	-	-	X
Hybrid Propulsion subsystem	X	X	X	X	X	X	X
Power subsystem	X	X	X	X	X	X	X
Flight Navigation subsystem	-	X	X	X	X	X	-
Flight Information subsystem	-	X	X	X	X	X	-
Flight control subsystem	-	X	X	X	X	X	-
Emergency flight subsystem	-	X	X	X	X	X	-
Mission data subsystem	X	X	X	X	X	X	X
Payload data subsystem	-	-	-	X	-	-	-
Communication Command and Control subsystem	X	X	X	X	X	X	X
Ground Control Station subsystem	X	X	X	X	X	X	X

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: Hybrid fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 63 – Subsystem: Hybrid Propulsion Subsystem (LiPo batteries + fuel cell)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Hydrogen tank	Hydrogen (fuel) containment	HPSS1a	Structural damage	Shock/ Vibrations/ Wrong seizing	2, 3, 4, 5, 6, 7, 8	Hydrogen leakage	Loss of engine power	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (Performance of proper maintenance on ground like periodical inspection)	-
Hydrogen tank	Hydrogen (fuel) containment	HPSS1b	Leakage	Shock/ Vibrations	2, 3, 4, 5, 6, 7, 8	Hydrogen leakage	Loss of engine power	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (Performance of proper maintenance on ground like periodical inspection)	-
Fuel cell	Electrical current generation	HPSS2a	Membrane drying	Wrong fuel cell thermal management (too high temperatures range)	2, 3, 4, 5, 6, 7, 8	Loss of fuel cell functionality	Loss of engine functionality	System loss	Catastrophic	4	D	2	None	5	8	40	Design solutions (Provision of redundant equipment)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: Hybrid fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 63 – Subsystem: Hybrid Propulsion Subsystem (LiPo batteries + fuel cell) (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Fuel cell	Electrical current generation	HPSS2b	Water condensation inhibition	Wrong fuel cell thermal management (too low temperatures range)	2, 3, 4, 5, 6, 7, 8	Loss of fuel cell functionality	Loss of engine functionality	System loss	Catastrophic	4	D	2	None	5	8	40	Design solutions (Provision of redundant equipment)	-
Hydrogen	Fuel	HPSS3	Fire	Leakage/Accidental contact with oxidizing gas like oxygen or chlorine	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Fire	System loss	Catastrophic	4	C	1	Visual or audible warning devices	1	4	4	Operator actions (Performance of proper maintenance on ground like periodical inspection)	-
LiPo battery	Electrical power generation	HPSS4a	Short circuit	Heat/ External overheating/High rate operation (causing overheat)/ Internal short circuit (hot spot)/ External short circuit/Over charge/Over discharge	2, 3, 4, 5, 6, 7, 8	Loss of battery	Loss or decrease of electrical power/ Loss of thrust	System loss	Catastrophic	4	C	3	Visual or audible warning devices	1	12	12	Design solutions (Provision of redundant equipment)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: Hybrid fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 63 – Subsystem: Hybrid Propulsion Subsystem (LiPo batteries + fuel cell) (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
LiPo battery	Electrical power generation	HPSS4b	Mechanical damage	Crush/Nail Penetration/Drop/ Mechanical Shock/ Vibration /Water Immersion	2, 3, 4, 5, 6, 7, 8	Loss of battery	Loss or decrease of electrical power/Loss of thrust	System loss	Catastrophic	4	C	3	None	5	12	60	Design solutions (Provision of redundant equipment)	-
LiPo battery	Electrical power generation	HPSS4c	Fire	Overheat/ Thermal ramp/Fire	2, 3, 4, 5, 6, 7, 8	Loss of battery	Loss or decrease of electrical power/Loss of thrust	System loss	Catastrophic	4	C	3	Automatic sensing devices	2	12	32	Design solutions (Provision of redundant equipment)	-
DC power bus	Selection of power source	HPSS5	Electrical failure	Over voltage/ under voltage	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss or decrease of electrical power	System loss	Catastrophic	4	C	3	None	2	9	18	Design solutions (Provision of redundant equipment)	-

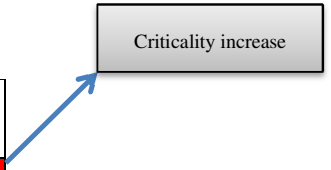
Remotely Piloted Aircraft Systems FMECA			
System name: Aerial segment			
Type of aerial segment: Hybrid fixed wing RPAS	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 63 – Subsystem: Hybrid Propulsion Subsystem (LiPo batteries + fuel cell) (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
DC to DC converter	Voltage regulation	HPSS6	Internal components fault	Capacitors fault/ Transistors fault	1, 2, 3, 4, 5, 6, 7, 8, 9	-	Loss or decrease of electrical power	System loss	Catastrophic	4	C	3	None	2	9	18	Operator actions (Performance of proper maintenance on ground)	-

Table 64 – Hybrid Propulsion Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				Fire (HPSS3) Short circuit (HPSS4a) Mechanical damage (HPSS4b) Fire (HPSS4c) Electrical failure (HPSS5) Internal components fault (HPSS6)
LEVEL D – REMOTE				Structural failure (HPSS1a) Leakage (HPSS1b) Membrane drying (HPSS2a) Water condensation inhibition (HPSS2b)
LEVEL E – EXTREMELY UNLIKELY				
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



System definition: Command and Control (C2) radio link.
Mission phases: all.

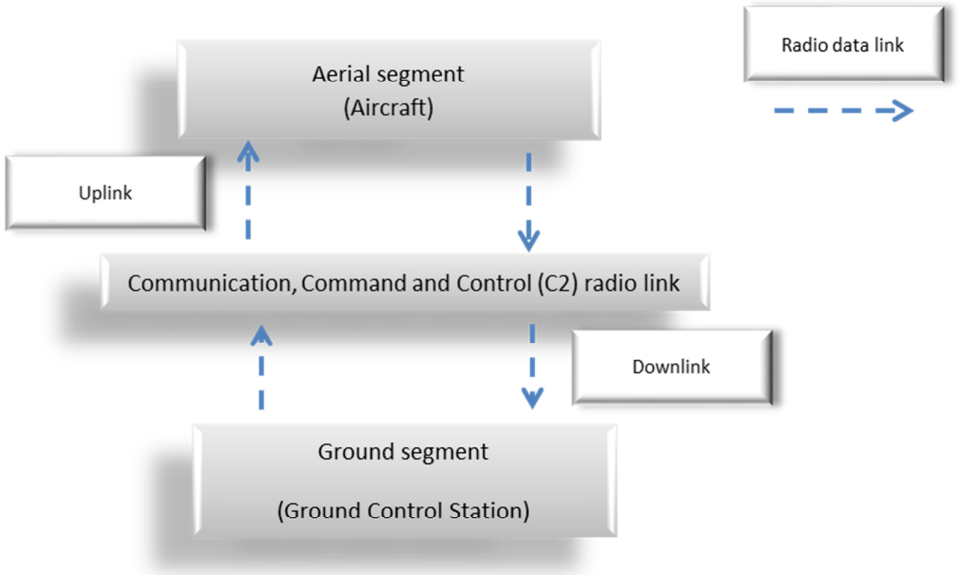


Figure 37 – Command and Control (C2) radio link [80]

Remotely Piloted Aircraft Systems FMECA			
System name: Command and control (C2) link			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 65 – Subsystem: Command and Control Radio Link Subsystem

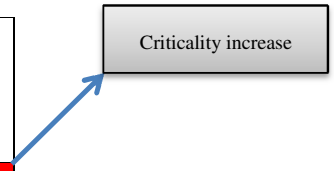
Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Radio link signal	Vehicle operational control (uplink) and monitoring (downlink)	C2LSS1a	Signal degradation	Screening by terrain/ Weather interference/ Man-made unintentional interference (e.g. television broadcast)/ Malicious unlawful interference (jamming, spoofing)/ Vehicle out of range/ Network satellite failures/ Vehicle TX/RX equipment failure/ GCS TX/RX equipment failure/ Human error in the (frequency setting, switches)	1, 2, 3, 4, 5, 6, 7, 8, 9	-	-	System loss	Catastrophic	4	D	2	Visual or audible warning devices	1	8	8	Design solutions (Provision of radio link frequency redundancy)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Command and control (C2) link			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 65 – Subsystem: Command and Control Radio Link Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Radio link signal	Vehicle operational control (uplink) and monitoring (downlink)	C2LSS1b	Signal loss	Screening by terrain/ Weather interference/ Man-made unintentional interference (e.g. television broadcast)/ Malicious unlawful interference (jamming, spoofing)/ Vehicle out of range/ Network satellite failures/ Vehicle TX/RX equipment failure/ GCS TX/RX equipment failure/ Human error in the (frequency setting, switches)	1, 2, 3, 4, 5, 6, 7, 8, 9	-	-	System loss	Catastrophic	4	D	2	Visual or audible warning devices	1	8	8	Design solutions (Provision of radio link frequency redundancy)	-

Table 66 – Command and Control (C2)
Radio Link Subsystem failure modes criticality matrix



LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				
LEVEL D – REMOTE				C2 radio link signal degradation (C2LSS1a) C2 radio link signal loss (C2LSS1b)
LEVEL E – EXTREMELY UNLIKELY				
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC

System definition: Ground Control Station
Mission phases: all

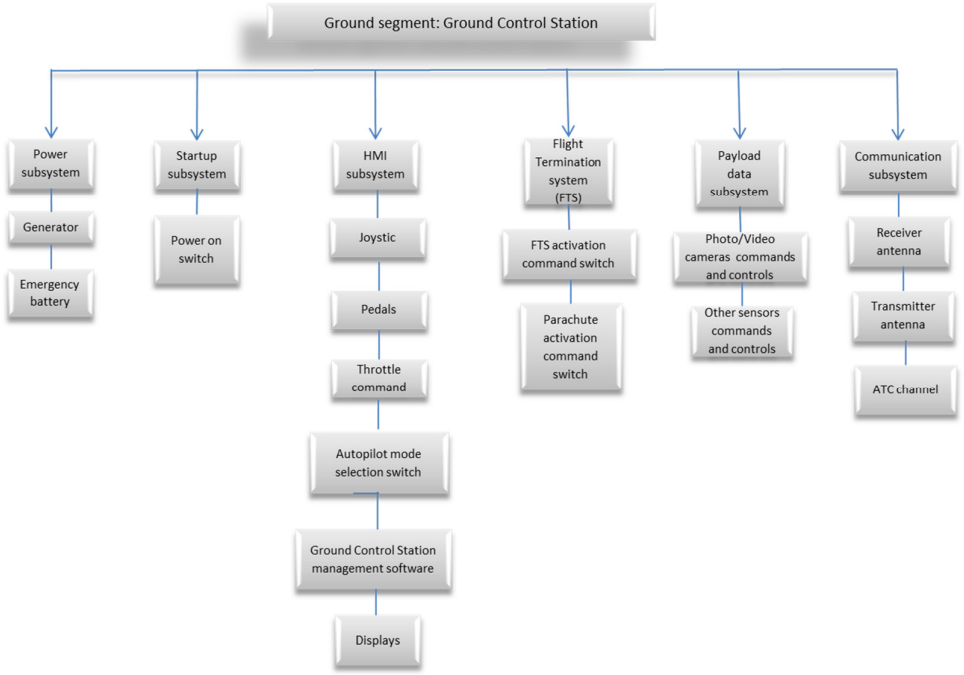


Figure 38 – Ground Control Station [80]

Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 67 – Subsystem: Ground Control Station Power Generation Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Ground generator	Power generation	GCSPWSS 1a	Missed start	Internal electrical/ mechanical failure	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of generator functionality	Loss of Ground Control Station functionality	System loss	Catastrophic	4	D	2	Visual or audible warning devices	1	8	8	Design solutions (provision of an emergency redundant battery)	-
Ground generator	Power generation	GCSPWSS 1b	Sudden stop	Internal electrical/ mechanical failure	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of generator functionality	Loss of Ground Control Station functionality	System loss	Catastrophic	4	D	2	Visual or audible warning devices	1	8	8	Design solutions (provision of an emergency redundant battery)	-
Ground emergency battery	Power generation	GCSPWSS 2a	Low charge	Frequent charge/ discharge cycles/ Corrosion/ Improper maintenance procedures	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of emergency battery functionality	Loss of Ground Control Station functionality	System loss	Catastrophic	4	E	1	Visual or audible warning devices	1	4	20	Operator actions (emergency battery proper maintenance/ handling)	-

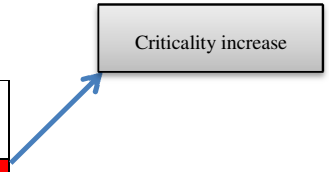
Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 67 – Subsystem: Ground Control Station Power Generation Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Emergency battery	Power generation	GCSPWSS 2b	Lack of charge	Frequent charge/ discharge cycles/ Corrosion/ Improper maintenance procedures	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of emergency battery functionality	Loss of Ground Control Station functionality	System loss	Catastrophic	4	E	1	Visual or audible warning devices	1	4	20	Operator actions (emergency battery proper maintenance/ handling)	-

Table 68 – Ground Control System Power Generation Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				
LEVEL D – REMOTE				Missed start (GCSPWSS1a) Sudden stop (GCSPWSS1b)
LEVEL E – EXTREMELY UNLIKELY				Emergency battery low charge (GCSPWSS2a) Emergency battery lack of charge (GCSPWSS2b)
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



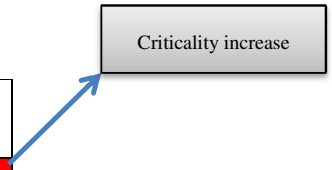
Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 69 – Subsystem: Ground Control Station Start-up Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Power on switch	Ground Control Station power on	GCSSUSS1	Missed start	Open circuit (oxidation non-metallic or corrosive gaseous contamination creates open circuits by forming a surface film or oxidation)/Short circuits caused by mechanical failure/Loss of resilience of spring mechanisms (especially in momentary action switches) contamination or by physical blocks of the movement of mechanical elements)/ Mechanical wear of the switching elements	1, 2, 3, 4, 5, 6, 7, 8, 9	Lack of Ground Control Station functionality	-	Impossibility to start and perform the mission	Minor	1	E	1	None	5	1	5	Design solutions (Provision of redundant equipment)/ Operator actions (Performance of proper maintenance on ground)	-

Table 70 – Ground Control System Start-up Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				
LEVEL D – REMOTE				
LEVEL E – EXTREMELY UNLIKELY	Power on switch missed start (GCSSUSS1)			
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC



Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	
	EASA Weight class A3	< 25 kg	

Table 71 – Subsystem: Ground Control Station Human Machine Interface Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Joystick	Pitch, roll control of the aerial platform	GCSHMISS1a	Lack of calibration	Human error	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of pitch and roll attitude control of the aerial platform	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-
Joystick	Pitch, roll control of the aerial platform	GCSHMISS1b	Software error	Error during firmware/ software update	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of pitch and roll attitude control of the aerial platform	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-
Joystick	Pitch, roll control of the aerial platform	GCSHMISS1c	Missed start	Physical disconnection/ Degradation of electrical power/Loss of electrical power	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of pitch and roll attitude control of the aerial platform	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	
	EASA Weight class A3	< 25 kg	

Table 71 – Subsystem: Ground Control Station Human Machine Interface Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Joystick	Pitch, roll control of the aerial platform	GCSHMISS1d	Sudden stop	Physical disconnection/ Degradation of electrical power/Loss of electrical power	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of pitch and roll attitude control of the aerial platform	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-
Pedals	Lateral control of the aerial platform (fixed wings air segment)	GCSHMISS2a	Lack of calibration	Human error	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of lateral attitude control of the aerial platform	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-
Pedals	Lateral control of the aerial platform (fixed wings air segment)	GCSHMISS2b	Software error	Error during firmware/ software update	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of lateral control of the aerial platform	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	
	EASA Weight class A3	< 25 kg	

Table 71 – Subsystem: Ground Control Station Human Machine Interface Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Pedals	Lateral control of the aerial platform (fixed wings air segment)	GCSHMISS2c	Missed start	Physical disconnection/ Degradation of electrical power/Loss of electrical power	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of lateral control of the aerial platform	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-
Pedals	Lateral control of the aerial platform (fixed wings air segment)	GCSHMISS2d	Sudden stop	Physical disconnection/ Degradation of electrical power/Loss of electrical power	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of lateral control of the aerial platform	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-
Throttle	Thrust control	GCSHMISS3a	Lack of calibration	Human error	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of aerial platform thrust control	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	
	EASA Weight class A3	< 25 kg	

Table 71 – Subsystem: Ground Control Station Human Machine Interface Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Throttle	Thrust control	GCSHMISS3b	Software error	Error during firmware/ software update	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of aerial platform thrust control	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-
Throttle	Thrust control	GCSHMISS3c	Missed start	Physical disconnection/ Degradation of electrical power/Loss of electrical power	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of aerial platform thrust control	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-
Throttle	Thrust control	GCSHMISS3d	Sudden stop	Physical disconnection/ Degradation of electrical power/Loss of electrical power	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of aerial platform thrust control	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	
	EASA Weight class A3	< 25 kg	

Table 71 – Subsystem: Ground Control Station Human Machine Interface Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Autopilot modes selection switch	Selection of the autopilot flight mode	GCSHMISS4a	Mechanical failure	Wear/ Improper installation	1, 2, 3, 4, 5, 6, 7, 8, 9	Wrong or no selection of the proper autopilot flight mode	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-
Autopilot modes selection switch	Selection of the autopilot flight mode	GCSHMISS4b	Electrical failure	Open circuit/ Short circuit	1, 2, 3, 4, 5, 6, 7, 8, 9	Wrong or no selection of the proper autopilot flight mode	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	
	EASA Weight class A3	< 25 kg	

Table 71 – Subsystem: Ground Control Station Human Machine Interface Subsystem (Cont'd)

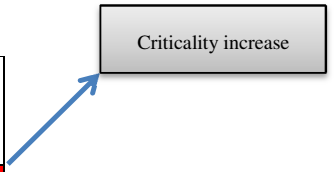
Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Autopilot modes selection switch	Selection of the autopilot flight mode	GCSHMISS4c	Signal error	Wrong signal input	1, 2, 3, 4, 5, 6, 7, 8, 9	Wrong or no selection of the proper autopilot flight mode	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-
Ground Control Station management software	GCS management	GCSHMISS5	Software error	Software error	1, 2, 3, 4, 5, 6, 7, 8, 9	-	-	System loss	Catastrophic	4	E	1	None	5	4	20	Operator actions (use of FTS)	-
Displays	Air segment subsystems and payload sensors monitoring	GCSHMISS6a	Lack of power supply	Loss of electrical power	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of equipment functionality	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	
	EASA Weight class A3	< 25 kg	

Table 71 – Subsystem: Ground Control Station Human Machine Interface Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Displays	Air segment subsystems and payload sensors monitoring	GCSHMISS6b	Software error	Design mechanization error	1, 2, 3, 4, 5, 6, 7, 8, 9	Loss of equipment functionality	-	System loss	Catastrophic	4	D	2	None	5	8	40	Operator actions (use of FTS)	-

Table 72 – Ground Control Station Human Machine Interface Subsystem failure modes criticality matrix



LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				
LEVEL D – REMOTE				Lack of calibration (GCSHMISS1a) Software error (GCSHMISS1b) Joystick missed start (GCSHMISS1c) Joystick sudden stop (GCSHMISS1d) Lack of calibration (GCSHMISS2a) Software error (GCSHMISS2b) Missed start (GCSHMISS2c) Sudden stop (GCSHMISS2d) Lack of calibration (GCSHMISS3a) Software error (GCSHMISS3b) Throttle missed start (GCSHMISS3c) Throttle sudden stop (GCSHMISS3d) Mechanical failure (GCSHMISS4a) Electrical failure (GCSHMISS4b) Software error (GCSHMISS4c) Electrical failure (GCSHMISS6a) Software error (GCSHMISS6b)
LEVEL E – EXTREMELY UNLIKELY				Software error (GCSHMISS5)
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC

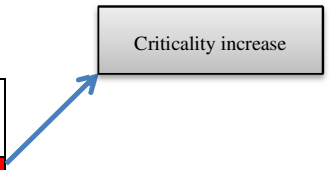
Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 73 – Subsystem: Ground Control Station Emergency Flight Termination HMI Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
FTS command switch	Flight Termination System (FTS) activation	GCSEFTSS1	Mechanical failure	Wear	2, 3, 4, 5, 6, 7, 8	No activation of FTS	-	System loss	Catastrophic	4	E	1	Visual or audible warning devices	1	4	4	Operator actions (Performance of proper maintenance on ground)	-
Parachute deployment command switch	Emergency parachute deployment activation	GCSEFTSS2	Mechanical failure	Wear	2, 3, 4, 5, 6, 7, 8	No deployment of the safety parachute	-	System loss	Catastrophic	4	E	1	Visual or audible warning devices	1	4	4	Operator actions (Performance of proper maintenance on ground)	-

Table 74 – Ground Control Station Emergency Flight Termination HMI Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				
LEVEL D – REMOTE				
LEVEL E – EXTREMELY UNLIKELY				Mechanical failure (GCSEFTSS1) Mechanical failure (GCSEFTSS2)
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC

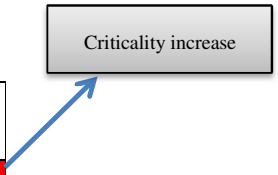


Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 75 – Subsystem: Ground Control Station Payload Sensors HMI Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
Photo/ Video cameras command and control switch	Photo/ Video functionalities management	GCSPYS SS1	Mechanical failure	Wear	2, 3, 4, 5, 6, 7, 8	No photo/ Video camera activation	-	-	Minor	1	D	2	None	5	1	5	Operator actions (Performance of proper maintenance on ground)	-
Other sensors command and control switch	Other sensors functionalities management	GCSPYS SS2	Mechanical failure	Wear	2, 3, 4, 5, 6, 7, 8	No payload other sensors activation	-	-	Minor	1	D	2	None	5	1	5	Operator actions (Performance of proper maintenance on ground)	-

Table 76 – Ground Control Station Payload Sensors HMI Subsystem failure modes criticality matrix



LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				
LEVEL D – REMOTE	Mechanical failure (GCSPYSSS1a) Mechanical failure (GCSPYSSS2a)			
LEVEL E – EXTREMELY UNLIKELY				
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC

Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 77 – Subsystem: Ground Control Station Communication Subsystem

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
GCS transmitting antenna	To send telemetry data to the ground segment	GCSCSS1a	The transmitting antenna cannot process the control signal	Lack of power supply/ Failure in the electrical system/ Antenna intermitted	1,2,3,4, 5,6,7,8,9	-	-	System loss	Catastrophic	4	D	2	None	5	8	40	Design Solution (Provision of redundant equipment)	-
GCS transmitting antenna	To send telemetry data to the ground segment	GCSCSS1b	transmitting antenna fade	RPA shape and flight attitude/RPA airframe material	1,2,3,4, 5,6,7,8,9	-	-	System loss	Catastrophic	4	C	3	None	5	12	60	Design Solution (Provision of redundant equipment)	-
GCS receiving antenna	To receive the flight commands from the aerial segment	GCSCSS2a	The receiving antenna cannot process the control signals	Lack of power supply/ Failure in the electrical system/ Antenna intermitted	1,2,3,4, 5,6,7,8,9	-	-	System loss	Catastrophic	4	D	2	None	5	8	40	Design Solution (Provision of redundant equipment)	-

Remotely Piloted Aircraft Systems FMECA			
System name: Ground Control Station			
Type of aerial segment: Any	EASA Weight class A1	< 250 g and < 80 J or < 900 g	25 kg < Weight < 150 kg
	EASA Weight class A2	< 4 kg	150 kg < Weight < 600 kg
	EASA Weight class A3	< 25 kg	

Table 77 – Subsystem: Ground Control Station Communication Subsystem (Cont'd)

Equipment	Function	Identification number	Failure modes	Failure causes	Mission phase	Failure effects			Severity classification	Severity number (SN)	Occurrence probability	Probability number (PN)	Failure detection method/ Observable symptoms	Detection ranking (DR)	Criticality number	RPN	Mitigation actions	Remarks
						Local effect	Next higher level	End effects										
GCS receiving antenna	To send telemetry data to the ground segment	GCSCSS2b	Receiving antenna fade	RPA shape and flight attitude/RPA airframe material	1,2,3,4, 5,6,7,8,9	-	-	System loss	Catastrophic	4	C	3	None	5	12	60	Design Solution (Provision of redundant equipment)	-
GCS channel with ATC	To interface with ATC operators during flight sorties	GCS CSS3	Lack of communication with ATC	Lack of power supply/ Failure in the electrical system/ Antenna intermitted	1,2,3,4, 5,6,7,8,9	-	-	Mission degradation/ System loss	Catastrophic	4	C	3	Visual or audible warning devices	1	8	16	Design solutions (Redundant equipment)	-

Table 78 – Ground Control Station Communication Subsystem failure modes criticality matrix

LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				
LEVEL C – OCCASIONAL				Transmitting antenna fade (CSS1b) Receiving antenna fade (CSS2b) Lack of communication with ATC (GCSCSS3)
LEVEL D – REMOTE				The transmitting antenna cannot process the control signal (CSS1a) The receiving antenna cannot process the control signal (CSS2a)
LEVEL E – EXTREMELY UNLIKELY				
	CATEGORY IV – MINOR	CATEGORY III – MARGINAL	CATEGORY II – CRITICAL	CATEGORY I – CATASTROPHIC

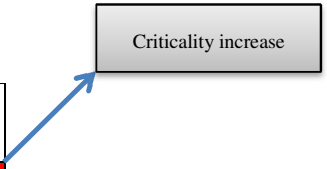


Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
AERIAL SEGMENT													
ROTOR WING RPAS													
PROPULSION SUBSYSTEM													
ESC													
PSS1a	ESC seizing	-	-	-	-	-	-	-	-	-	-	-	C ([57], item B.2a)
PSS1b	ESC degradation	0,120 [53]	-	29,315 [68]	3,518	-	2	0,999	-	7,036E-06	-	0,0281	C
PSS1c	ESC overheating	-	-	-	-	-	-	-	-	-	-	-	C ([57], item B.2a)
PSS1d	ESC burnout	-	-	-	-	1,25E+02 ([58], figure 6)	2	-	0,999	-	2,50E-04	-	C ([57], item B.2a, item B.2d)
	ESC												
BRUSHLESS ELECTRIC MOTOR													
PSS2a	Cranked stator housing	0,001 [53]	-	29,315 [68]	0,029	-	2	0,999	-	5,863E-08	-	0,0014	D
PSS2b	Worn bearings	-	-	-	-	-	-	-	-	-	-	-	C ([57], tem B.3a)
PSS2c1	Windings open circuit	-	-	-	-	-	-	-	-	-	-	-	D ([57], item B.3-c)
PSS2c2	Windings Short circuit	-	-	-	-	-	-	-	-	-	-	-	D ([57], item B.3-c)
PSS2d	Armature shaft structural damage	-	-	-	-	-	-	-	-	-	-	-	D
	Electric brushless motor	-	2,13E+01 [58]	-	-	-	2	0,999	-	-	4,250E-05	-	

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
PROPELLER													
PSS3a	Propeller structural failure	-	-	-	-	-	-	-	-	-	-	-	E [57]
PSS3b	Propeller connection failure	-	-	-	-	-	-	-	-	-	-	-	D[57]
PSS3c	Abrupt stop of the propeller	-	-	-	-	-	-	-	-	-	-	-	E [57]
POWER SUBSYSTEM													
LIPO BATTERIES													
PWSS1a	Short circuit	-	-	-	-	-	-	-	-	-	-	-	C ([57], item B.1a, item B.1b)
PWSS1b	Mechanical failure	-	-	-	-	-	-	-	-	-	-	-	C ([57], item B.1b)
PWSS1c	Fire	-	-	-	-	-	-	-	-	-	-	-	C ([57], item B.1b)
ELECTRICAL SUBSYSTEM													
BALANCE CABLES													
ESS1a	Open circuit	0,03 [64]	-	1	0,03	-	2	0,99999994	-	6E-08	-	0,047846919	C
ESS1b	Short circuit	10 [64]	-	1	10	-	2	0,99998	-	1,99998E-05	-	15,94881383	A
	Balance cable	--	0,627 [52]	1	-	0,627	2	-	0,999998746	-	1,254E-06	-	
DISTRIBUTION CABLES													
ESS2a	Open circuit	0,03 [64]	-	1	0,03	-	2	0,99999994	-	6E-08	-	0,047846919	C
ESS2b	Short circuit	10 [64]	-	1	10	-	2	0,99998	-	1,99998E-05	-	15,94881383	A
	Balance cable	--	0,627 [52]	1	-	0,627	2	-	0,999998746	-	1,254E-06	-	
CONNECTORS ARC													
ESS3	-	-	-	-	-	-	-	-	-	-	-	-	C
NAVIGATION SUBSYSTEM													

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
INERTIAL MEASUREMENT UNIT (IMU)													
NSS1a	Circuitry overload	-	-	-	-	-	-	-	-	-	-	-	D ([57], item D.6-a)
NSS1b	Calibration loss												D ([57], item D.6-b)
NSS1b	Calibration loss	-	-	-	-	-	-	-	-	-	-	-	C ([54], item D.6-b)
GPS													
NSS2a	Failure of GPS receiver	-	-	-	-	-	-	-	1,0E-04 [68]	4,294E-04	-	-	E
NSS2b	GPS signal jamming	-	-	-	-	-	-	-	1,0E-13 [68]	4,294E-13	-	-	E
NSS2c	GPS signal spoofing	-	-	-	-	-	-	-	-	-	-	-	B
	GPS		6000 [69]	22,0952381		132571,4291	2		0,767		0,233		
EGNOS													
NSS2a	EGNOS receiver failure	9,04 [74]	-	22,095 [58]	199,741	-	2	0,999	-	3,994E-04	-	0,361727521	A
NSS2b	Loss of EGNOS signal continuity	9,04E-06 [73]	-	-	-	-	-	4,0E-06	-	-	-	0,00362269	D
NSS2c	Loss of EGNOS signal integrity	1,0E-09 [72]	-	-	-	-	-	1,0E-09	-	-	-	9,05673E-07	E
NSS2d	EGNOS signal delay	3,2E-06 [74]	-	-	-	-	-	3,2E-06	-	-	-	0,002898152	D
	EGNOS		25 [73]	22,095 [58]		552,381	2		0,999		1,1E-03		

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
ADS-B													
NSS4a	Loss of EGNOS position accuracy	-	-	-	-	-	-	-	-	0,05 [68]	-	22,65431955	A
NSS4b	EGNOS receiver unit failure	9,04 [NSS4b]	-	22,0952381	199,7409524	-	2	0,999600598	-	0,000399402	-	0,180963666	B
NSS4c	ADS_B out antenna failure	-	-	-	-	-	-	-	-	0,0001 [68]	-	0,045308639	C
NSS4d	ADS_B out antenna deterioration	-	-	-	-	-	-	-	-	0,0012 [68]	-	0,543703669	B
NSS4e	Signal interruption	-	-	-	-	-	-	-	-	0,01 [68]	-	4,53086391	A
NSS4f	Emitter/ transponder failure	-	-	-	-	-	-	-	-	0,0001 [68]	-	0,045308639	B
NSS4g	Erroneous altitude data	-	-	-	-	-	-	-	-	1E-13 [68]	-	4,53086E-11	E
NSS4h	Data encoding error	-	-	-	-	-	-	-	-	1E-13 [68]	-	4,53086E-11	E
NSS4i	Intentional/ unintentional jamming of ADS-B signal	-	-	-	-	-	-	-	-	1E-13 [68]	-	4,53086E-11	E
NSS4l	Lack of ADS-B service	-	-	-	-	-	-	-	-	1E-13 [68]	-	4,53086E-11	E

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
NSS4m	Inaccurate position datum sent to the ADS-B emitter	-	-	-	-	-	-	-	-	0,05 [68]	-	22,65431955	A
NSS4n	Degradation of accuracy and integrity of data sent by the satellite to the ADS-B	-	-	-	-	-	-	-	-	0,000000001 [72]	-	4,53086E-07	E
NSS4o	Failure of ADS-B transponder/ emitter on the RPA	-	-	-	-	-	-	-	-	0,0001 [68]	-	0,045308639	C
NSS4p	Failure in detection of maneuvering aircraft/RPA	-	-	-	-	-	-	-	-	0,0012 [68]	-	0,543703669	A
NSS4q	Sudden loss of ADS-B data to ATC controllers without any notification	-	-	-	-	-	-	-	-	0,00001 [68]	-	0,004530864	D
NSS4r	ADSB-IN receiving antenna deterioration	-	-	-	-	-	-	-	-	0,0001 [68]	-	0,045308639	D

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
NSS4s	ADS-B ground station failure	-	-	-	-	-	-	-	-	0,00013 [68]	--	0,058901231	D
NSS4t	Performance of wrong pre-flight procedures on ADS-B	-	-	-	-	-	-	-	-	0,0002 [68]	-	0,090617278	C
	ADS_B	-	50 [76]	22,0952381	-	1104,762	-	2	0,998	-	2,2E-03	-	
AIR DATA SUBSYSTEM													
AIR DATA UNIT													
ADSS1a	Incorrect signal	2 [53]	-	22,0952381 [58]	44,19047619	-	2	0,999911623	-	8,8377E-05	-	0,800008838	A
ADSS1b	Loss of signal	2 [53]	-	22,0952381 [58]	44,19047619	-	2	0,999911623	-	8,8377E-05	-	0,8000038	A
ADSS1c	Signal error along the transmission line	0,0416 [54]	-	22,0952381 [58]	0,919161905	-	2	0,999998162	-	1,83832E-06	-	0,016640904	C
ADSS1d	Error on output signal	0,088 [54]	-	22,0952381 [58]	1,944380952	-	2	0,999996111	-	3,88875E-06	-	0,035201876	C
ADSS1e	Loss of power supply	3,9453 [52]	-	29,32432432 [58]	115,6932568	-	2	0,99976864	-	0,00023136	-	2,094320277	A
ADSS1f	Calibration error	0,088 [58]	-	22,0952381 [58]	1,944380952	-	2	0,999996111	-	3,88875E-06	-	0,035201876	C
	Air Data Unit	-	2,5 [77]	22,0952381 [58]	-	55,23809524	2	-	0,99988953	-	0,00011047	-	

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
FLIGHT CONTROL SUBSYSTEM													
AUTOPILOT													
FCSS1a	Failure of weak joint	-	-	-	-	-	-	-	-	-	-	-	D
FCSS1a	Lack of power supply	-	-	-	-	-	-	-	-	-	-	-	D ([57], item D.5-b)
FCSS1a	Software error	-	-	-	-	-	-	-	-	-	-	-	D
DETECT AND AVOID													
FCSS2a	ADS-B IN receiving antenna deterioration	-	-	-	-	-	-	-	-	-	-	-	C (Ref. item NSS4r)
FCSS2b	EGNOS receiver failure	-	-	-	-	-	-	-	-	-	-	-	A (Ref. item NSS3a)
FCSS2c	Erroneous altitude data	-	-	-	-	-	-	-	-	-	-	-	E (Ref. item NSS4g)
EMERGENCY FLIGHT SUBSYSTEM													
FLIGHT TERMINATION SYSTEM													
EFSS1a	Loss of dedicated radio link	-	-	-	-	-	-	-	-	-	-	-	C
EFSS1b	Lack of functionality	-	-	-	-	-	-	-	-	-	-	-	D
EFSS1c	Unlawful interference on dedicated radio link (jamming)	-	-	-	-	-	-	-	-	-	-	-	B

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
EMERGENCY PARACHUTE													
EFSS2a	Loss of dedicated radio link	-	-	-	-	-	-	-	-	-	-	-	C
EFSS2b	Lack of functionality	-	-	-	-	-	-	-	-	-	-	-	D
EFSS2c	Unlawful interference on dedicated radio link (jamming)	-	-	-	-	-	-	-	-	-	-	-	B
MISSION CONTROL SUBSYSTEM													
MISSION DAA STORAGE UNIT													
MC1a	Loss of mission software	-	-	-	-	-	-	-	-	-	-	-	C
MC1b	Physical unit degradation	-	-	-	-	-	-	-	-	-	-	-	C
MISSION PAYLOAD SENSOR SUBSYSTEM													
PHOTO7VIDEO CAMERA SENSORS													
MC1a	Payload Photo/video camera sensors failure	-	-	-	-	-	-	-	-	-	-	-	D (57, item D.13a, D13-b)
MC1b	Other sensors failure	-	-	-	-	-	-	-	-	-	-	-	D

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
COMMUNICATION SUBSYSTEM													
ON BOARD TRANSMITTER ANTENNA													
CSS1a	The transmitter antenna cannot process the control signal	-	-	-	-	-	-	-	-	-	-	-	D
CSS1b	Transmitter antenna fade	-	-	-	-	-	-	-	-	-	-	-	C (57), item D.7-d)
ON BOARD RECEIVING ANTENNA													
CSS2a	The receiver antenna cannot process the control signal	-	-	-	-	-	-	-	-	-	-	-	D
CSS2b	Receiver antenna fade	-	-	-	-	-	-	-	-	-	-	-	C (57), item D.7-d)
STRUCTURES													
-													
FIXED WING RPAS													
PROPULSION SUBSYSTEM (JET TYPE)													
ENGINE CONTROL UNIT													
PSCE1a	Software error	-	-	-	-	-	-	-	-	-	-	-	D [80]
PSCE1b	Mechanical failure	-	-	-	-	-	-	-	-	-	-	-	B [80]

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
PSCE1c	Loss of on board computer	-	-	-	-	-	-	-	-	-	-	-	E [80]
PSCE1d	Carburetor failure	-	-	-	-	-	-	-	-	-	-	-	C [80]
(JET) ENGINE													
PSCE2a	Engine control system failure	-	-	-	-	-	-	-	-	-	-	-	D [80]
PSCE2b	Mechanical failure	-	-	-	-	-	-	-	-	-	-	-	B [80]
PSCE2c	Engine fire	-	-	-	-	-	-	-	-	-	-	-	E [80]
PSCE2d	Human error	-	-	-	-	-	-	-	-	-	-	-	C [80]
PROPELLER													
PSCEP3a	Propeller structural failure	-	-	-	-	-	-	-	-	-	-	-	E [80]
PSCEP3b	Propeller connection failure	-	-	-	-	-	-	-	-	-	-	-	D [80]
PSCEP3c	Abrupt stop of the propeller	-	-	-	-	-	-	-	-	-	-	-	E [80]
FUEL SUBSYSTEM													
FUEL TANK													
FSS1	(Structural damage)	-	-	-	-	-	-	-	-	-	-	-	D
FUEL PUMP													
FSS2	(Mechanical failure)	-	-	-	-	-	-	-	-	-	-	-	D

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
FUEL PIPELINES													
FSS3	(Structural damage)	-	-	-	-	-	-	-	-	-	-	-	E
POWER SUBSYSTEM													
ALTERNATOR													
PWGSS1	Mechanical failure	-	-	-	-	-	-	-	-	-	-	-	C
RECTIFIER													
PWGSS2a	Overheating												C
PWGSS2b	Chemical failure	-	-	-	-	-	-	-	-	-	-	-	C
EMERGENCY BATTERY													
PWGSS3a	Mechanical failure	-	-	-	-	-	-	-	-	-	-	-	D
PWGSS3b	Thermal failure	-	-	-	-	-	-	-	-	-	-	-	D
PWGSS3c	Chemical failure	-	-	-	-	-	-	-	-	-	-	-	D
PWGSS3d	Electrical failure	-	-	-	-	-	-	-	-	-	-	-	D
AIR DATA UNIT													
ADSS1	Air probe clogging	-	-	-	-	-	-	-	-	-	-	-	C ([57], item D.8-a)
ADSS2a	Incorrect signal	2 [53]	-	22,0952381 [58]	44,19047619	-	2	0,999911623	-	8,8377E-05	-	0,800008838	A
ADSS2b	Loss of signal	2 [53]	-	22,0952381 [58]	44,19047619	-	2	0,999911623	-	8,8377E-05	-	0,8000038	A
ADSS2c	Signal error along the transmission line	0,0416 [54]	-	22,0952381 [58]	0,919161905	-	2	0,999998162	-	1,83832E-06	-	0,016640904	C

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
ADSS2d	Error on output signal	0,088 [54]	-	22,0952381 [58]	1,944380952	-	2	0,999996111	-	3,88875E-06	-	0,035201876	C
ADSS2e	Loss of power supply	3,9453 [52]	-	29,32432432 [58]	115,6932568	-	2	0,99976864	-	0,00023136	-	2,094320277	A
DSS1fA	Calibration error	0,088 [58]	-	22,0952381 [58]	1,944380952	-	2	0,999996111	-	3,88875E-06	-	0,035201876	C
	Air Data Unit	-	2,5 [77]	22,0952381 [58]	-	55,23809524	2	-	0,99988953	-	0,00011047	-	
FLIGHT CONTROL SUBSYSTEM													
SERVOUNITS													
FCSS1a	Bias	-	-	-	-	-	-	-	-	-	-	-	C [81]
FCSS1b	Stuck surface	-	-	-	-	-	-	-	-	-	-	-	D [81]
FCSS1c	Hardover	-	-	-	-	-	-	-	-	-	-	-	D [81]
FCSS1d	Floating surfaces	-	-	-	-	-	-	-	-	-	-	-	C [81]
FCSS1e	Oscillatory modes	-	-	-	-	-	-	-	-	-	-	-	D [81]
FCSS1f	Increased dead band/stiction	-	-	-	-	-	-	-	-	-	-	-	D [81]
FCSS1g	Structural damage	-	-	-	-	-	-	-	-	-	-	-	E [81]
STRUCTURES													
-													
HYBRID RPAS													
HYDROGEN TANK													
HPSS1a	Structural damage	-	-	-	-	-	-	-	-	-	-	-	D
HPSS1b	Leakage	-	-	-	-	-	-	-	-	-	-	-	D

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
FUEL CELLS													
HPSS2a	Membrane drying	-	-	-	-	-	-	-	-	-	-	-	D
HPSS2b	Water condensation	-	-	-	-	-	-	-	-	-	-	-	D
HYDROGEN													
HPSS3	Fire												C
BACKUP LIPO BATTERIES													
HPSS4a	Short circuit	-	-	-	-	-	-	-	-	-	-	-	C ([57], item B.1a, item B.1b)
HPSS4b	Mechanical failure	-	-	-	-	-	-	-	-	-	-	-	C ([57], item B.1b)
HPSS4c	Fire	-	-	-	-	-	-	-	-	-	-	-	C ([57], item B.1b)
DC POWER BUS													
HPSS5	Electrical failure	-	-	-	-	-	-	-	-	-	-	-	C
DC TO DC CONVERTER													
HPSS6	Internal components fault	-	-	-	-	-	-	-	-	-	-	-	C
COMMAND AND CONTROL (C2) SUBSYSTEM													
RADIO LINK SIGNAL													
C2LSS1a	Signal degradation	-	-	-	-	-	-	-	-	-	-	-	D
C2LSS1a	Signal loss	-	-	-	-	-	-	-	-	-	-	-	D

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
GROUND SEGMENT													
GCS POWER GENERATION SUBSYSTEM													
POWER GENERATOR													
GCSPWSS1a	Missed start	-	-	-	-	-	-	-	-	-	-	-	D
GCSPWSS1b	Sudden stop	-	-	-	-	-	-	-	-	-	-	-	D
EMERGENCY BATTERY													
GCSPWSS2a	Low charge	-	-	-	-	-	-	-	-	-	-	-	D
GCSPWSS2b	Lack of charge	-	-	-	-	-	-	-	-	-	-	-	D
GCS START-UP SUBSYSTEM													
POWER ON SWITCH													
GCSSUSS1	Missed start	-	-	-	-	-	-	-	-	-	-	-	D
GCS HUMAN MACHINE INTERFACE SUBSYSTEM													
GCS JOYSTICK													
GCSHMI1a	Lack of calibration	-	-	-	-	-	-	-	-	-	-	-	D
GCSHMI1b	Software error	-	-	-	-	-	-	-	-	-	-	-	D
GCSHMI1c	Missed start	-	-	-	-	-	-	-	-	-	-	-	D
GCSHMI1d	Sudden stop	-	-	-	-	-	-	-	-	-	-	-	D
GCS PEDALS													
GCSHMI2a	Lack of calibration												D
GCSHMI2b	Software error	-	-	-	-	-	-	-	-	-	-	-	D
GCSHMI2c	Missed start	-	-	-	-	-	-	-	-	-	-	-	D
GCSHMI2d	Sudden stop	-	-	-	-	-	-	-	-	-	-	-	D

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
GCS THROTTLE													
GCSHMI3a	Lack of calibration	-	-	-	-	-	-	-	-	-	-	-	D
GCSHMI3b	Software error	-	-	-	-	-	-	-	-	-	-	-	D
GCSHMI3c	Missed start	-	-	-	-	-	-	-	-	-	-	-	D
GCSHMI3d	Sudden stop	-	-	-	-	-	-	-	-	-	-	-	D
AUTOPILOT FLIGHT MODES SELECTION SWITCH													
GCSHMI4a	Mechanical failure	-	-	-	-	-	-	-	-	-	-	-	D
GCSHMI4b	Electrical failure	-	-	-	-	-	-	-	-	-	-	-	D
GCSHMI4c	Signal error	-	-	-	-	-	-	-	-	-	-	-	D
GCS MANAGEMENT SOFTWARE													
GCSHMI5	Software error	-	-	-	-	-	-	-	-	-	-	-	E
GCS DISPLAYS													
GCSHMI6a	Lack of power supply	-	-	-	-	-	-	-	-	-	-	-	D
GCSHMI6b	Software error	-	-	-	-	-	-	-	-	-	-	-	D
GCS FLIGHT TERMINATION COMMAND SUBSYSTEM													
GCS EMERGENCY FTS COMMAND SWITCH													
GCSFTSS1	Mechanical failure	-	-	-	-	-	-	-	-	-	-	-	E
GCS EMERGENCY PARACHUTE COMMAND SWITCH													
GCSFTSS2	Mechanical failure	-	-	-	-	-	-	-	-	-	-	-	E

Table 79 – FMECA probability of occurrence determination: data that has been used (when available) and their origin (references) (Cont'd)

Failure mode code	Failure mode definition	Estimated component specific failure mode rate of occurrence (from literature, when available) [failures per million hours]	Estimated overall component basic failure rate (from literature, when available) [failures per million hours]	Corrective factor applicable for RPAS technology level (from [64])	Corrected estimated component specific failure mode rate of occurrence [failures per million hours]	Corrected estimated overall component basic failure rate [failures per million hours]	Expected duration of a standard RPAS flight mission [hours] [64]	Reliability with respect to the specific failure mode	Reliability with respect to the overall component failure mode	Specific failure mode probability of occurrence	Overall component failure probability of occurrence	Failure mode frequency of occurrence as for MIL-STD-1629Rev.A	Estimated component failure mode probability of occurrence level as for MIL-STD-1629Rev.A
GCS PAYLOAD SENSORS COMMAND SUBSYSTEM													
PHOTO/VIDEO CAMERA COMMAND SWITCH													
GCSPYSSS1	Mechanical failure	-	-	-	-	-	-	-	-	-	-	-	E
OTHER SENSORS COMMAND SWITCH													
GCSPYSSS2	Mechanical failure	-	-	-	-	-	-	-	-	-	-	-	E
GCS COMMUNICATION SUBSYSTEM													
GCS TRANSMITTING ANTENNA													
GCSCSS1a	The transmitter antenna cannot process the control signal	-	-	-	-	-	-	-	-	-	-	-	D
GCSCSS1b	Transmitter antenna fade	-	-	-	-	-	-	-	-	-	-	-	C (57, item D.7-d)
GCS RECEIVING ANTENNA													
GCSCSS2a	The receiver antenna cannot process the control signal	-	-	-	-	-	-	-	-	-	-	-	D
GCSCSS2b	Receiver antenna fade	-	-	-	-	-	-	-	-	-	-	-	C (57, item D.7-d)
GCS CHANNEL WITH ATC													
GCSCSS3	Lack of communication with ATC	-	-	-	-	-	-	-	-	-	-	-	C

Table 80 – Summary of FMECA results				
Failure mode	Failure typology	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Criticality level
Aerial segment				
Rotor wing RPAS – Propulsion Subsystem				
ESC seizing (PSS1a)	Mechanical failure	C	5,5E-02	HIGH
ESC degradation PSS1b)	Mechanical failure	C	5,5E-02	HIGH
ESC overheating (PSS1c)	Mechanical failure	C	5,5E-02	HIGH
ESC burn out (PSS1d)	Mechanical failure	C	5,5E-02	HIGH
Worn bearings (PSS2b)	Mechanical failure	C	5,5E-02	HIGH
Windings open circuit (PSS2c1)	Mechanical failure	D	5,5E-03	MEDIUM
Windings short circuit (PSS2c2)	Mechanical failure	D	5,5E-03	MEDIUM
Cranked stator housing (PSS2a)	Mechanical failure	D	5,5E-03	MEDIUM
Armature shaft structural failure (PSS2d)	Mechanical failure	D	5,5E-03	MEDIUM
Propeller connection failure (PSS3b)	Mechanical failure	D	5,5E-03	MEDIUM
Propeller structural failure (PSS3a)	Mechanical failure	E	< 1,0E-03	LOW
Abrupt stop of the propeller (PSS3c)	Mechanical failure	E	< 1,0E-03	LOW
Rotor wing RPAS – Power Subsystem				
Short circuit (PWSS1a)	Electrical failure	C	5,5E-02	HIGH
Mechanical damage(PWSS1b)	Mechanical failure	C	5,5E-02	HIGH
Fire (PWSS1c)	Mechanical failure	C	5,5E-02	HIGH
Rotor wing RPAS - Electrical Subsystem				
Open circuit (ESS1b)	Electrical failure	A	> 2,0E-01	HIGH
Open circuit (ESS2b)	Electrical failure	A	> 2,0E-01	HIGH
Short circuit (ESS1a)	Electrical failure	C	5,5E-02	HIGH
Short circuit (ESS2a)	Electrical failure	C	5,5E-02	HIGH
Electric arc (ESS3)	Electrical failure	C	5,5E-02	HIGH
Rotor wing RPAS – Flight Subsystem/Navigation Subsystem				
EGNOS receiver failure (NSS3a)	Software error	A	> 2,0E-01	HIGH
Loss of EGNOS position accuracy (NSS4a)	Software error	A	> 2,0E-01	HIGH
Inaccurate position datum sent to the ADS-B emitter (NSS4m)	Software error	A	> 2,0E-01	HIGH
Failure in detection of manoeuvring aircraft/RPA (NSS4p)	Software error	A	> 2,0E-01	HIGH
EGNOS receiver unit failure (NSS4b)	Electrical failure	B	1,5E-01	HIGH
ADS-B OUT antenna deterioration (NSS4d)	Mechanical failure/Electrical failure	B	1,5E-01	HIGH
Signal interruption (NSS4e)	Software error	B	1,5E-01	HIGH

Table 80 – Summary of FMECA results (Cont'd)

Failure mode	Failure typology	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Criticality level
Calibration loss (NSS1b)	Software error	D	5,5E-03	MEDIUM
ADS-B OUT antenna failure (NSS4c)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
Emitter/transponder failure (NSS4f)	Electrical failure	D	5,5E-03	MEDIUM
Failure of ADS-B transponder/ emitter on the RPA (NSS4o)	Electrical failure	D	5,5E-03	MEDIUM
ADS-B IN receiving antenna deterioration (NSS4r)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
Circuitry overload (NSS1a)	Electrical failure	E	< 1,0E-03	LOW
GPS antenna failure (NSS2a)	Mechanical failure/ Electrical failure	E	< 1,0E-03	LOW
GPS signal jamming (NSS2b)	Software error	E	< 1,0E-03	LOW
GPS signal spoofing (NSS2c)	Software error	E	< 1,0E-03	LOW
Loss of EGNOS signal integrity (NSS3c)	Software error	E	< 1,0E-03	LOW
Erroneous altitude data (NSS4g)	Software error	E	< 1,0E-03	LOW
Data encoding error (NSS4h)	Software error	E	< 1,0E-03	LOW
Intentional/ unintentional jamming of ADS-B signal (NSS4i)	Software error	E	< 1,0E-03	LOW
Lack of ADS-B service (NSS4l)	Software error	E	< 1,0E-03	LOW
Degradation of accuracy and integrity of data sent by the satellite to the ADS-B (NSS4n)	Software error	E	< 1,0E-03	LOW
Rotor wing RPAS – Flight Subsystem/Air Data Subsystem				
Incorrect signal (ADSS1a)	Software error	A	> 2,0E-01	HIGH
Loss of signal (ADSS1b)	Software error	A	> 2,0E-01	HIGH
Loss of power supply (ADSS1e)	Mechanical failure/ Electrical failure	A	> 2,0E-01	HIGH
Signal error along the transmission line (ADSS1c)	Software error	C	5,5E-02	HIGH
Error on output signal (ADSS1d)	Electrical failure	C	5,5E-02	HIGH
Calibration error (ADSS1f)	Mechanical failure/ Electrical failure	C	5,5E-02	HIGH
Rotor wing RPAS – Flight Subsystem/Flight Control Subsystem				
EGNOS receiver failure (FCSS2b)	Mechanical failure/ Electrical failure	A	> 2,0E-01	HIGH
ADS-B IN receiving antenna deterioration (FCSS2a)	Mechanical failure/ Electrical failure	C	5,5E-02	HIGH
Failure of weak joints (FCSS1a)	Mechanical failure	D	5,5E-03	MEDIUM
Lack of power supply (FCSS1b)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
Software error (FCSS1c)	Software error	D	5,5E-03	MEDIUM

Table 80 – Summary of FMECA results (Cont'd)

Failure mode	Failure typology	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Criticality level
Erroneous altitude data (FCSS2c)	Software error	E	< 1,0E-03	LOW
Rotor wing RPAS – Flight Subsystem/Emergency Flight Termination Subsystem				
Unlawful interference on dedicated radio link (jamming) (EFSS1c)	Software error	B	1,5E-01	HIGH
Unlawful interference on dedicated radio link (jamming) (EFSS2c)	Software error	B	1,5E-01	HIGH
Loss of dedicated radio link (EFSS1a)	Software error	C	5,5E-02	HIGH
Loss of dedicated radio link (EFSS2a)	Software error	C	5,5E-02	HIGH
Lack of functionality (EFSS1b)	Electrical failure	D	5,5E-03	MEDIUM
Lack of functionality (EFSS2b)	Electrical failure	D	5,5E-03	MEDIUM
Rotor wing RPAS – Mission Control Subsystem				
Loss of mission data software (MCSS1a)	Software error	C	5,5E-02	LOW
Physical unit degradation (MCSS1b)	Mechanical failure/ Electrical failure	C	5,5E-02	LOW
Rotor wing RPAS – Mission Payload Sensors Subsystem				
Photo/video camera failure (MPYSS1)	Electrical failure	D	5,5E-03	LOW
Other payload sensors failure (MPYSS2)	Electrical failure	D	5,5E-03	LOW
Rotor wing RPAS – On Board Communication Subsystem				
On board transmitting antenna fade (CSS1b)	Software error	C	5,5E-02	HIGH
On board receiving antenna fade (CSS2b)	Software error	C	5,5E-02	HIGH
The on board transmitting antenna cannot process the control signal (CSS1a)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
The onboard receiving antenna cannot process the control signal (CSS2a)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
Rotor wing RPAS structural airframe				
-				
Fixed wing RPAS – Propulsion Subsystem (Combustion Engine)				
Engine control system failure (PSCE2a)	Mechanical failure	A	> 2,0E-01	HIGH
Mechanical failure (PSCE1b)	Mechanical failure	B	1,5E-01	HIGH
Carburetor failure (PSCE1d)	Mechanical failure	C	5,5E-02	HIGH
Mechanical failure (PCSE2b)	Mechanical failure	C	5,5E-02	MEDIUM
Software error (PSCE1a)	Software error	D	5,5E-03	MEDIUM

Table 80 – Summary of FMECA results (Cont'd)

Failure mode	Failure typology	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Criticality level
Engine fire (PSCE2c)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
Use of improper fuel (PSCE2d)	Human error	D	5,5E-03	MEDIUM
Loss of on board computer (PSCE1c)	Electrical failure	E	< 1,0E-03	LOW
Fixed wing RPAS – Propulsion Subsystem (Combustion Engine with propellers)				
Engine control system failure (PSCEP2a)	Mechanical failure	A	> 2,0E-01	HIGH
Mechanical failure (PSCEP1b)	Mechanical failure	B	1,5E-01	HIGH
Carburetor failure (PSCEP1d)	Mechanical failure	C	5,5E-02	HIGH
Mechanical failure (PCSEP2b)	Mechanical failure	C	5,5E-02	MEDIUM
Software error (PSCEP1a)	Software error	D	5,5E-03	MEDIUM
Engine fire (PSCEP2c)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
Use of improper fuel (PSCEP2d)	Human error	D	5,5E-03	MEDIUM
Propeller connection failure (PSCEP3b)	Mechanical failure	D	5,5E-03	MEDIUM
Loss of on board computer (PSCE1c)	Electrical failure	E	< 1,0E-03	LOW
Propeller structural failure (PSCEP3a)	Mechanical failure	E	< 1,0E-03	LOW
Abrupt stop of the propeller (PSCEP3c)	Mechanical failure	E	< 1,0E-03	LOW
Fixed wing RPAS – Fuel Subsystem				
Structural failure (FSS1)	Mechanical failure	D	5,5E-03	MEDIUM
Mechanical failure (FSS2)	Mechanical failure	D	5,5E-03	MEDIUM
Structural failure (FSS3)	Mechanical failure	E	< 1,0E-03	LOW
Fixed wing RPAS – Power Generation Subsystem				
Mechanical failure (PWGSS1)	Mechanical failure	C	5,5E-02	HIGH
Electrical failure (PWGSS2a)	Mechanical failure	C	5,5E-02	HIGH
Chemical failure (PWGSS2b)	Chemical failure	C	5,5E-02	HIGH
Mechanical failure (PWGSS3a)	Mechanical failure	D	5,5E-03	MEDIUM
Thermal failure (PWGSS3b)	Mechanical failure	D	5,5E-03	MEDIUM
Chemical failure (PWGSS3c)	Mechanical failure	D	5,5E-03	MEDIUM
Electrical failure (PWGSS3d)	Mechanical failure	D	5,5E-03	MEDIUM
Fixed wing RPAS – Flight Subsystem/Air Data Subsystem				
Incorrect signal (ADSS2a)	Software error	A	> 2,0E-01	HIGH
Loss of signal (ADSS2b)	Software error	A	> 2,0E-01	HIGH
Loss of power supply (ADSS2e)	Mechanical failure/ Electrical failure	A	> 2,0E-01	HIGH
Air probe clogging (ADSS1)	Mechanical failure	B	1,5E-01	HIGH

Table 80 – Summary of FMECA results (Cont'd)

Failure mode	Failure typology	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Criticality level
Signal error along the transmission line (ADSS2c)	Software error	C	5,5E-02	HIGH
Error on output signal (ADSS2d)	Electrical failure	C	5,5E-02	HIGH
Calibration error (ADSS2f)	Mechanical failure/ Electrical failure	C	5,5E-02	HIGH
Fixed wing RPAS – Flight subsystem/Flight Control Subsystem				
Bias (FCSS1a)	Mechanical failure	C	5,5E-02	HIGH
Floating surface (FCSS11d)	Mechanical failure	C	5,5E-02	HIGH
Stuck surface (FCSS1b)	Mechanical failure	D	5,5E-03	MEDIUM
Hardover (FCSS1c)	Mechanical failure	D	5,5E-03	MEDIUM
Oscillatory modes (FCSS1e)	Mechanical failure	D	5,5E-03	MEDIUM
Increased dead band/stiction (FCSS1f)	Mechanical failure	D	5,5E-03	MEDIUM
Structural damage (FCSS2)	Mechanical failure	E	< 1,0E-03	LOW
Rotor wing RPAS structural airframe				
-				
Rotor wing hybrid RPAS – Propulsion System				
Fire (HPSS3)	Electrical failure	C	5,5E-02	HIGH
Short circuit (HPSS4a)	Electrical failure	C	5,5E-02	HIGH
Mechanical damage (HPSS4b)	Mechanical failure	C	5,5E-02	HIGH
Fire (HPSS4c)	Electrical failure	C	5,5E-02	HIGH
Electrical failure (HPSS5)	Electrical failure	C	5,5E-02	HIGH
Internal components fault (HPSS6)	Electrical failure	C	5,5E-02	HIGH
Structural failure (HPSS1a)	Mechanical failure	D	5,5E-03	MEDIUM
Leakage (HPSS1b)	Mechanical failure	D	5,5E-03	MEDIUM
Membrane drying (HPSS2a)	Mechanical failure	D	5,5E-03	MEDIUM
Water condensation inhibition (HPSS2b)	Mechanical failure	D	5,5E-03	MEDIUM
Command and Control Radio Link Subsystem				
C2 radio link signal degradation (C2LSS1a)	Software error	D	5,5E-03	MEDIUM
C2 radio link signal loss (C2LSS1b)	Software error	D	5,5E-03	MEDIUM
Ground Segment				
Ground Control Station – Power Generation Subsystem				
Missed start (GCSPWSS1a)	Mechanical failure	D	5,5E-03	MEDIUM
Sudden stop (GCSPWSS1b)	Mechanical failure	D	5,5E-03	MEDIUM
Emergency battery low charge (GCSPWSS2a)	Electrical failure	E	< 1,0E-03	LOW

Table 80 – Summary of FMECA results (Cont'd)

Failure mode	Failure typology	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Criticality level
Emergency battery lack of charge (GCSPWSS2b)	Electrical failure	E	< 1,0E-03	LOW
Ground Control Station – Start Up Subsystem				
Power on switch missed start (GCSSUSS1)	Electrical failure	E	< 1,0E-03	LOW
Ground Control Station – Human Machine Interface Subsystem				
Lack of calibration (GCSHMISS1a)	Electrical failure	D	5,5E-03	MEDIUM
Failure mode	Failure typology	Estimated quantitative probability of occurrence	Estimated qualitative probability of occurrence [MIL-STD-1629A] [47]	Criticality level
Software error (GCSHMISS1b)	Software error	D	5,5E-03	MEDIUM
Joystick missed start (GCSHMISS1c)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
Joystick sudden stop (GCSHMISS1d)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
Lack of calibration (GCSHMISS2a)	Electrical failure	D	5,5E-03	MEDIUM
Software error (GCSHMISS2b)	Software error	D	5,5E-03	MEDIUM
Missed start (GCSHMISS2c)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
Sudden stop (GCSHMISS2d)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
Lack of calibration (GCSHMISS3a)	Electrical failure	D	5,5E-03	MEDIUM
Software error (GCSHMISS3b)	Software error	D	5,5E-03	MEDIUM
Throttle missed start (GCSHMISS3c)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
Throttle sudden stop (GCSHMISS3d)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
Mechanical failure (GCSHMISS4a)	Mechanical failure	D	5,5E-03	MEDIUM
Electrical failure (GCSHMISS4b)	Electrical failure	D	5,5E-03	MEDIUM
Software error (GCSHMISS4c)	Software error	D	5,5E-03	MEDIUM
Electrical failure (GCSHMISS6a)	Electrical failure	D	5,5E-03	MEDIUM
Software error (GCSHMISS6b)	Software error	D	5,5E-03	MEDIUM
Software error (GCSHMISS5)	Software error	E	< 1,0E-03	LOW
Ground Control Station – Emergency Flight Termination HMI Subsystem				
Mechanical failure (GCSEFTSS1)	Mechanical failure	E	< 1,0E-03	LOW
Mechanical failure (GCSEFTSS2)	Mechanical failure	E	< 1,0E-03	LOW
Ground Control Station – Payload Sensors HMI Subsystem				
Mechanical failure (GCSPYSSS1a)	Mechanical failure	D	5,5E-03	LOW
Mechanical failure (GCSPYSSS2a)	Mechanical failure	D	5,5E-03	LOW
Ground Control Station – Communication Subsystem				

Table 80 – Summary of FMECA results (Cont'd)				
Failure mode	Failure typology	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Criticality level
Transmitter antenna fade (CSS1b)	Software error	C	5,5E-02	HIGH
Receiver antenna fade (CSS2b)	Software error	C	5,5E-02	HIGH
Lack of communication with ATC (GCSCSS3)	Mechanical failure/ Electrical failure/ Software error	C	5,5E-02	HIGH
Failure mode	Failure typology	Estimated quantitative probability of occurrence	Estimated qualitative probability of occurrence [MIL-STD-1629A] [47]	Criticality level
The transmitter antenna cannot process the control signal (CSS1a)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM
The receiver antenna cannot process the control signal (CSS2a)	Mechanical failure/ Electrical failure	D	5,5E-03	MEDIUM

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
ESC seizing (PSS1a)	C	5,5E-02	Low RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft
ESC degradation PSS1b)	C	5,5E-02	Low RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft
ESC overheating (PSS1c)	C	5,5E-02	Low RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft
ESC burn out (PSS1d)	C	5,5E-02	Low RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft
Worn bearings (PSS2b)	C	5,5E-02	Low RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft
Short circuit (PWSS1a)	C	5,5E-02	Loss of electrical power Loss of propulsion (rotor wing RPA) Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft
Mechanical damage(PWSS1b)	C	5,5E-02	Loss of electrical power Loss of propulsion (rotor wing RPA) Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft
Fire (PWSS1c)	C	5,5E-02	Loss of electrical power Loss of propulsion (rotor wing RPA) Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft Fire
Open circuit (ESS1b)	A	> 2,0E-01	Loss of electrical power Loss of propulsion (rotor wing RPA) Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft Fire
Open circuit (ESS2b)	A	> 2,0E-01	Loss of electrical power Loss of propulsion (rotor wing RPA) Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft Fire
Short circuit (ESS1a)	C	5,5E-02	Loss of electrical power Loss of propulsion (rotor wing RPA) Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft Fire
Short circuit (ESS2a)	C	5,5E-02	Loss of electrical power Loss of propulsion (rotor wing RPA) Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft Fire
Electric arc (ESS3)	C	5,5E-02	Loss of electrical power Loss of propulsion (rotor wing RPA) Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft Fire

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards (Cont'd)

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
EGNOS receiver failure (NSS3a)	A	> 2,0E-01	Loss of RPA navigation functionality/ Loss of RPA remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Loss of EGNOS position accuracy (NSS4a)	A	> 2,0E-01	Loss of RPA navigation functionality/ Loss of RPA remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Inaccurate position datum sent to the ADS-B emitter (NSS4m)	A	> 2,0E-01	Loss of RPA navigation functionality/ Loss of RPA remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Failure in detection of manoeuvring aircraft/RPA (NSS4p)	A	> 2,0E-01	Loss of RPA navigation functionality/ Loss of RPA remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
EGNOS receiver unit failure (NSS4b)	B	1,5E-01	Loss of RPA navigation functionality/ Loss of RPA remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
ADS-B OUT antenna deterioration (NSS4d)	B	1,5E-01	Loss of RPA navigation functionality/ Loss of RPA remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Signal interruption (NSS4e)	B	1,5E-01	Loss of RPA navigation functionality/ Loss of RPA remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Incorrect signal (ADSS1a)	A	> 2,0E-01	Mid-air collision with other aircraft
Loss of signal (ADSS1b)	A	> 2,0E-01	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Loss of power supply (ADSS1e)	A	> 2,0E-01	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Signal error along the transmission line (ADSS1c)	C	5,5E-02	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Error on output signal (ADSS1d)	C	5,5E-02	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards (Cont'd)

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
Calibration error (ADSS1f)	C	5,5E-02	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
EGNOS receiver failure (FCSS2b)	A	> 2,0E-01	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
ADS-B IN receiving antenna deterioration (FCSS2a)	C	5,5E-02	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Unlawful interference on dedicated radio link (jamming) (EFSS1c)	B	1,5E-01	Hostile takeover of RPAS/ Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Unlawful interference on dedicated radio link (jamming) (EFSS2c)	B	1,5E-01	Hostile takeover of RPAS/ Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Loss of dedicated radio link (EFSS1a)	C	5,5E-02	Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Loss of dedicated radio link (EFSS2a)	C	5,5E-02	Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
On board transmitting antenna fade (CSS1b)	C	5,5E-02	Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
On board receiving antenna fade (CSS2b)	C	5,5E-02	Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Engine control system failure (PSCE2a)	A	> 2,0E-01	Loss of propulsion (rotor wing RPA)/ Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards (Cont'd)

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
Mechanical failure (PSCE1b)	B	1,5E-01	Loss of propulsion (rotor wing RPA)/ Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Carburetor failure (PSCE1d)	C	5,5E-02	Loss of propulsion (rotor wing RPA)/ Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Engine control system failure (PSCEP2a)	A	> 2,0E-01	Loss of propulsion (rotor wing RPA)/ Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Mechanical failure (PSCEP1b)	B	1,5E-01	Loss of propulsion (rotor wing RPA)/ Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Mechanical failure (PWGSS1)	C	5,5E-02	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Electrical failure (PWGSS2a)	C	5,5E-02	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Chemical failure (PWGSS2b)	C	5,5E-02	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Incorrect signal (ADSS2a)	A	> 2,0E-01	Loss of air data/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Loss of signal (ADSS2b)	A	> 2,0E-01	Loss of air data/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Loss of power supply (ADSS2e)	A	> 2,0E-01	Loss of air data/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Air probe clogging (ADSS1)	B	1,5E-01	Loss of air data/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards (Cont'd)

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
Signal error along the transmission line (ADSS2c)	C	5,5E-02	Loss of air data/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Error on output signal (ADSS2d)	C	5,5E-02	Loss of air data/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Calibration error (ADSS2f)	C	5,5E-02	Loss of air data/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Bias (FCSS1a)	C	5,5E-02	Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of RPAS control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Floating surface (FCSS11d)	C	5,5E-02	Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of RPAS control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Fire (HPSS3)	C	5,5E-02	Loss of propulsion (hybrid RPA)/ Loss of RPAS manoeuvrability (hybrid RPA)/ Loss of control (hybrid RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain/ Fire
Short circuit (HPSS4a)	C	5,5E-02	Loss of propulsion (hybrid RPA)/ Loss of RPAS manoeuvrability (hybrid RPA)/ Loss of control (hybrid RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Mechanical damage (HPSS4b)	C	5,5E-02	Loss of propulsion (hybrid RPA)/ Loss of RPAS manoeuvrability (hybrid RPA)/ Loss of control (hybrid RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Fire (HPSS4c)	C	5,5E-02	Loss of propulsion (hybrid RPA)/ Loss of RPAS manoeuvrability (hybrid RPA)/ Loss of control (hybrid RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain/ Fire
Electrical failure (HPSS5)	C	5,5E-02	Loss of propulsion (hybrid RPA)/ Loss of RPAS manoeuvrability (hybrid RPA)/ Loss of control (hybrid RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards (Cont'd)

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
Internal components fault (HPSS6)	C	5,5E-02	Loss of propulsion (hybrid RPA)/ Loss of RPAS manoeuvrability (hybrid RPA)/ Loss of control (hybrid RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Transmitter antenna fade (CSS1b)	C	5,5E-02	Loss link/ Loss of control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Receiver antenna fade (CSS2b)	C	5,5E-02	Loss link/ Loss of control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Lack of communication with ATC (GCSCSS3)	C	5,5E-02	Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Windings open circuit (PSS2c1)	D	5,5E-03	Loss of propulsion (rotor wing RPA)/ Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Windings short circuit (PSS2c2)	D	5,5E-03	Loss of propulsion (rotor wing RPA)/ Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Cranked stator housing (PSS2a)	D	5,5E-03	Loss of propulsion (rotor wing RPA)/ Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Armature shaft structural failure (PSS2d)	D	5,5E-03	Loss of propulsion (rotor wing RPA)/ Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Propeller connection failure (PSS3b)	D	5,5E-03	Loss of propulsion (rotor wing RPA)/ Loss of RPAS manoeuvrability (rotor wing RPA)/ Loss of control (rotor wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Calibration loss (NSS1b)	D	5,5E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
ADS-B OUT antenna failure (NSS4c)	D	5,5E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Emitter/transponder failure (NSS4f)	D	5,5E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards (Cont'd)

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
Failure of ADS-B transponder/ emitter on the RPA (NSS4o)	D	5,5E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
ADS-B IN receiving antenna deterioration (NSS4r)	D	5,5E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Failure of weak joints (FCSS1a)	D	5,5E-03	Loss of RPAS control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Lack of power supply (FCSS1b)	D	5,5E-03	Loss of RPAS control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Software error (FCSS1c)	D	5,5E-03	Loss of RPAS control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
The on board transmitting antenna cannot process the control signal (CSS1a)	D	5,5E-03	Loss link/ Loss of control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
The onboard receiving antenna cannot process the control signal (CSS2a)	D	5,5E-03	Loss link/ Loss of control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Mechanical failure (PCSE2b)	C	5,5E-02	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Software error (PSCE1a)	D	5,5E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Engine fire (PSCE2c)	D	5,5E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Use of improper fuel (PSCE2d)	D	5,5E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Carburetor failure (PSCEP1d)	C	5,5E-02	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards (Cont'd)

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
Mechanical failure (PCSEP2b)	C	5,5E-02	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Software error (PSCEP1a)	D	5,5E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Engine fire (PSCEP2c)	D	5,5E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Use of improper fuel (PSCEP2d)	D	5,5E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Propeller connection failure (PSCEP3b)	D	5,5E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Structural failure (FSS1)	D	5,5E-03	Loss of fuel subsystem/ Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain/ Fire
Mechanical failure (FSS2)	D	5,5E-03	Loss of fuel subsystem/ Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain/ Fire
Mechanical failure (PWGSS3a)	D	5,5E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain/
Thermal failure (PWGSS3b)	D	5,5E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain/
Chemical failure (PWGSS3c)	D	5,5E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain/

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards (Cont'd)

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
Electrical failure (PWGSS3d)	D	5,5E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed wing RPA)/ Loss of control (fixed wing RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain/
Stuck surface (FCSS1b)	D	5,5E-03	Loss of control (fixed wing RPAS)/ Loss of manoeuvrability (fixed wing RPAS)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Hardover (FCSS1c)	D	5,5E-03	Loss of control (fixed wing RPAS)/ Loss of manoeuvrability (fixed wing RPAS)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Oscillatory modes (FCSS1e)	D	5,5E-03	Loss of control (fixed wing RPAS)/ Loss of manoeuvrability (fixed wing RPAS)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Increased dead band/stiction (FCSS1f)	D	5,5E-03	Loss of control (fixed wing RPAS)/ Loss of manoeuvrability (fixed wing RPAS)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Structural failure (HPSS1a)	D	5,5E-03	Loss of propulsion (hybrid RPA)/ Loss of RPAS manoeuvrability (hybrid RPA)/ Loss of control (hybrid RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain/ Fire
Leakage (HPSS1b)	D	5,5E-03	Loss of propulsion (hybrid RPA)/ Loss of RPAS manoeuvrability (hybrid RPA)/ Loss of control (hybrid RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain/ Fire
Membrane drying (HPSS2a)	D	5,5E-03	Loss of propulsion (hybrid RPA)/ Loss of RPAS manoeuvrability (hybrid RPA)/ Loss of control (hybrid RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain/ Fire
Water condensation inhibition (HPSS2b)	D	5,5E-03	Loss of propulsion (hybrid RPA)/ Loss of RPAS manoeuvrability (hybrid RPA)/ Loss of control (hybrid RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain/ Fire
C2 radio link signal degradation (C2LSS1a)	D	5,5E-03	Loss link/ Loss of control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
C2 radio link signal loss (C2LSS1b)	D	5,5E-03	Loss link/ Loss of control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards (Cont'd)

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
Missed start (GCSPWSS1a)	D	5,5E-03	Impossibility to start and perform the flight mission
Sudden stop (GCSPWSS1b)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Lack of calibration (GCSHMISS1a)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Software error (GCSHMISS1b)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Joystick missed start (GCSHMISS1c)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Joystick sudden stop (GCSHMISS1d)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Lack of calibration (GCSHMISS2a)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Software error (GCSHMISS2b)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Missed start (GCSHMISS2c)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Sudden stop (GCSHMISS2d)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Lack of calibration (GCSHMISS3a)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Software error (GCSHMISS3b)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Throttle missed start (GCSHMISS3c)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Throttle sudden stop (GCSHMISS3d)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Mechanical failure (GCSHMISS4a)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards (Cont'd)

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
Electrical failure (GCSHMISS4b)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Software error (GCSHMISS4c)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Electrical failure (GCSHMISS6a)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
Software error (GCSHMISS6b)	D	5,5E-03	Loss of RPAS remote control/ Loss RPAS manoeuvrability/ Mid-air collision with other aircraft/ Mid-air collision with obstacles
The transmitter antenna cannot process the control signal (CSS1a)	D	5,5E-03	Loss link/ Loss of control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
The receiver antenna cannot process the control signal (CSS2a)	D	5,5E-03	Loss link/ Loss of control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Propeller structural failure (PSS3a)	E	< 1,0E-03	Loss of propulsion (rotor wing RPA)/ Loss of RPAS manoeuvrability (hybrid RPA)/ Loss of control (hybrid RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Abrupt stop of the propeller (PSS3c)	E	< 1,0E-03	Loss of propulsion (rotor wing RPA)/ Loss of RPAS manoeuvrability (hybrid RPA)/ Loss of control (hybrid RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Circuitry overload (NSS1a)	E	< 1,0E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
GPS antenna failure (NSS2a)	E	< 1,0E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
GPS signal jamming (NSS2b)	E	< 1,0E-03	Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
GPS signal spoofing (NSS2c)	E	< 1,0E-03	Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Loss of EGNOS signal integrity (NSS3c)	E	< 1,0E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards (Cont'd)

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
Erroneous altitude data (NSS4g)	E	< 1,0E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Data encoding error (NSS4h)	E	< 1,0E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Intentional/unintentional jamming of ADS-B signal (NSS4i)	E	< 1,0E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Lack of ADS-B service (NSS4l)	E	< 1,0E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Degradation of accuracy and integrity of data sent by the satellite to the ADS-B (NSS4n)	E	< 1,0E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Erroneous altitude data (FCSS2c)	E	< 1,0E-03	Loss of RPAS navigation functionality/ Loss of RPAS remote control/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Loss of mission data software (MCSS1a)	C	5,5E-02	Mission degradation/ Loss of mission
Physical unit degradation (MCSS1b)	C	5,5E-02	Mission degradation/ Loss of mission
Photo/video camera failure (MPYSS1)	D	5,5E-03	Loss of payload mission data
Other payload sensors failure (MPYSS2)	D	5,5E-03	Loss of payload mission data
Loss of on board computer (PSCE1c)	E	< 1,0E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed RPA)/ Loss of control (fixed RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain

Table 81 – Failure modes, criticality ranking, probability of occurrence and possible related hazards (Cont'd)

Single failure mode	Estimated qualitative probability of occurrence level [MIL-STD-1629A] [47]	Estimated quantitative value of probability of occurrence level	Possible derived hazards
Loss of on board computer (PSCE1c)	E	< 1,0E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed RPA)/ Loss of control (fixed RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Propeller structural failure (PSCEP3a)	E	< 1,0E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed RPA)/ Loss of control (fixed RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrainLoss
Abrupt stop of the propeller (PSCEP3c)	E	< 1,0E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed RPA)/ Loss of control (fixed RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Structural damage (FCSS2)	E	< 1,0E-03	Loss of propulsion (fixed wing RPA)/ Loss of RPAS manoeuvrability (fixed RPA)/ Loss of control (fixed RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Emergency battery low charge (GCSPWSS2a)	E	< 1,0E-03	Loss of control (fixed RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Emergency battery lack of charge (GCSPWSS2b)	E	< 1,0E-03	Loss of control (fixed RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Power on switch missed start (GCSSUSS1)	E	< 1,0E-03	No possibility to perform the assigned flight mission
Software error (GCSHMISS5)	E	< 1,0E-03	Loss of control (fixed RPA)/ Mid-air collision with other aircraft/ Mid-air collision with obstacles/ Uncontrolled impact into terrain
Mechanical failure (GCSFTSS1)	E	< 1,0E-03	Uncontrolled impact into terrain
Mechanical failure (GCSFTSS2)	E	< 1,0E-03	Uncontrolled impact into terrain
Mechanical failure (GCSPYSSS1a)	D	5,5E-03	Loss of payload data
Mechanical failure (GCSPYSSS2a)	D	5,5E-03	Loss of payload data

Appendix B – Fault Tree Analysis (FTA) – Results

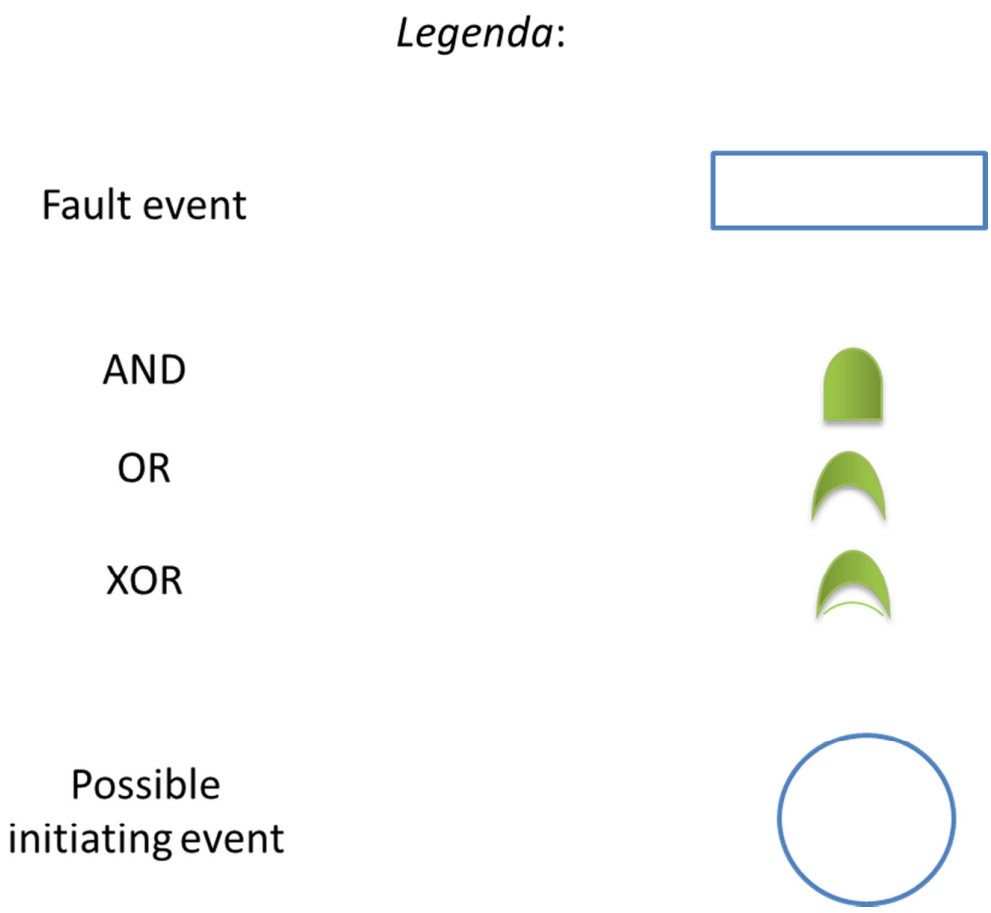


Figure 39 – FTA analysis legend

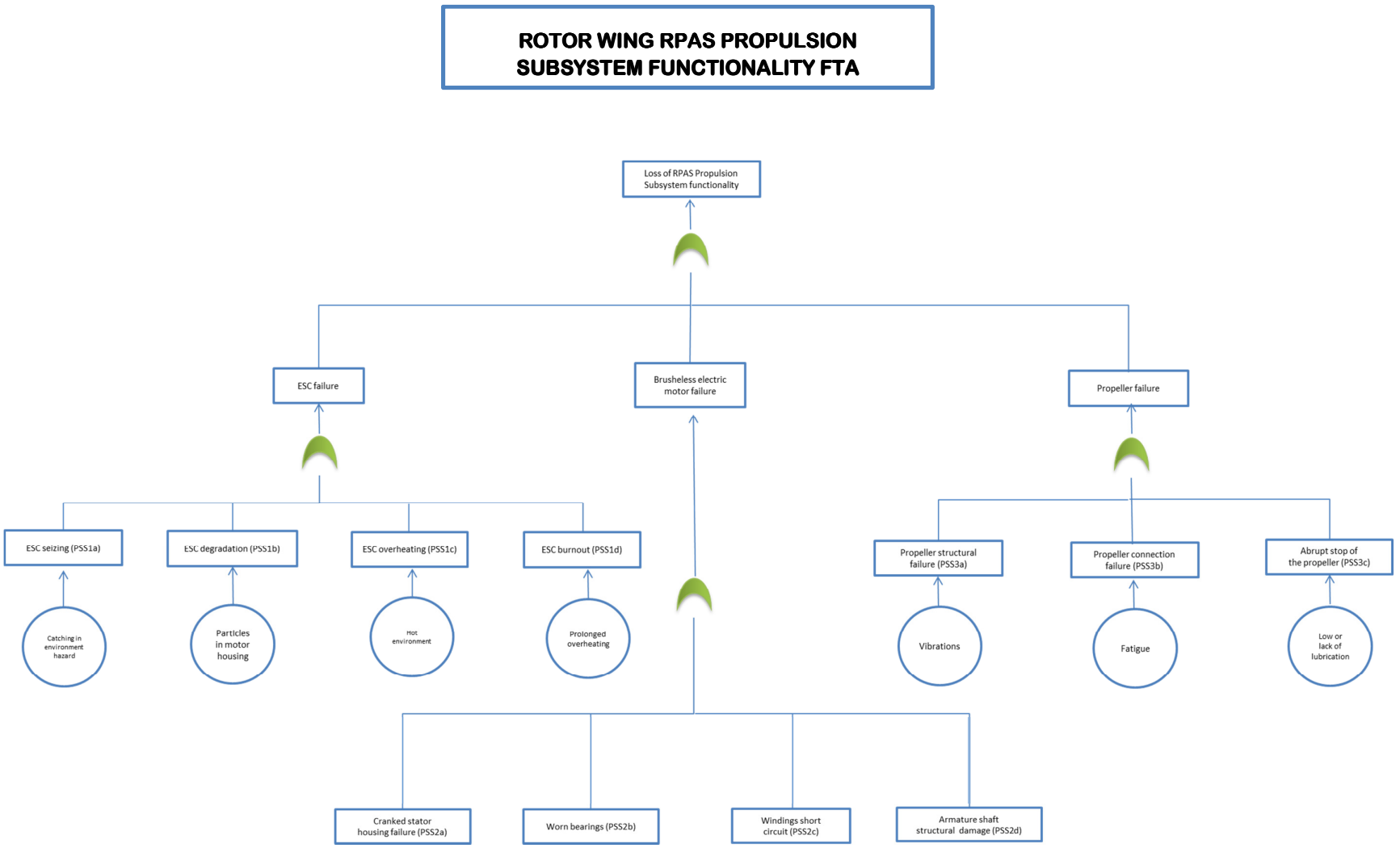


Figure 40 – Rotor wing RPAS Propulsion Subsystem functionality FTA

Table 82 – Rotor wing RPAS – ESC multiple failures

ESC single failure modes					Possible multiple failures	
ESC seizing (PSS1a)	ESC degradation (PSS1b)	ESC overheating (PSS1c)	ESC burnout (PSS1d)	ESC failure		
0	0	0	0	NO	-	-
0	0	0	5,5E-02	YES	-	-
0	0	5,5E-02	0	YES	-	-
0	0	5,5E-02	5,5E-02	YES	ESC overheating/ESC burnout	1,1E-01
0	5,5E-02	0	0	YES	-	
0	5,5E-02	0	5,5E-02	YES	ESC degradation/ESC burnout	1,1E-01
0	5,5E-02	5,5E-02	0	YES	ESC degradation/ESC overheating	1,1E-01
0	5,5E-02	5,5E-02	5,5E-02	YES	ESC degradation/ ESC overheating/ESC burnout	1,65E-01
5,5E-02	0	0	0	YES	-	-
5,5E-02	0	0	5,5E-02	YES	ESC seizing/ESC burnout	1,1E-01
5,5E-02	0	5,5E-02	0	YES	ESC seizing/ESC overheating	1,1E-01
5,5E-02	0	5,5E-02	5,5E-02	YES	ESC seizing/ ESC overheating/ESC burnout	1,65E-01
5,5E-02	5,5E-02	0	0	YES	ESC seizing/ESC degradation	1,1E-01
5,5E-02	5,5E-02	0	5,5E-02	YES	ESC seizing/ ESC degradation/ESC overheating	1,65E-01
5,5E-02	5,5E-02	5,5E-02	0	YES	ESC seizing/ ESC degradation/ESC overheating	1,65E-01
5,5E-02	5,5E-02	5,5E-02	5,5E-02	YES	ESC seizing/ESC degradation/ ESC overheating/ESC burnout	2,2E-01
Estimated probability of occurrence level, average value:						1,4E-01

Table 83 – Rotor wing RPAS – Brushless electric motor multiple failures

Brushless electric motor single failure modes					Possible multiple failures	
Cranked stator housing (PSS2a)	Worn bearings (PSS2b)	Windings open circuit (PSS2c)	Armature shaft structural damage (PSS2d)	Brushless electric motor failure		
0	0	0	0	NO	-	-
0	0	0	5,5E-03	YES	-	-
0	0	5,5E-03	0	YES	-	-
0	0	5,5E-03	5,5E-03	YES	Windings open circuit/ Armature shaft structural damage	1,1E-02
0	5,5E-02	0	0	YES	-	-
0	5,5E-02	0	5,5E-03	YES	Worn bearings/ Armature shaft structural damage	6,05E-02
0	5,5E-02	5,5E-03	0	YES	Worn bearings/ Windings open circuit	6,05E-02
0	5,5E-02	5,5E-03	5,5E-03	YES	Worn bearings/ Windings open circuit/ Armature shaft structural damage	6,6E-02
5,5E-03	0	0	0	YES	-	5,5E-03
5,5E-03	0	0	5,5E-03	YES	Cranked stator housing/ Armature shaft structural damage	1,1E-02
5,5E-03	0	5,5E-03	0	YES	Cranked stator housing/ Windings open circuit	1,1E-02
5,5E-03	0	5,5E-03	5,5E-03	YES	Cranked stator housing/ Windings open circuit/ Armature shaft structural damage	1,65E-02
5,5E-03	5,5E-02	0	0	YES	Cranked stator housing/ Worn bearings	6,05E-02
5,5E-03	5,5E-02	0	5,5E-03	YES	Cranked stator housing/ Worn bearings/ Armature shaft structural damage	6,6E-02
5,5E-03	5,5E-02	5,5E-03	0	YES	Cranked stator housing/ Worn bearings/ Windings open circuit/	6,6E-02
5,5E-03	5,5E-02	5,5E-03	5,5E-03	YES	Cranked stator housing/ Worn bearings/ Windings open circuit/ Armature shaft structural damage	7,15E-02
Estimated probability of occurrence level, average value:						4,22E-02

Table 84 – Rotor wing RPAS – Propeller multiple failures

Propeller single failure modes				Possible multiple failures	
Propeller structural failure (PSS3a)	Propeller connection failure (PSS3b)	Abrupt stop of the propeller (PSS3c)	Propeller failure		
0	0	0	NO	-	-
0	0	< 1,0E-03	YES	-	-
0	5,5E-03	0	YES	-	-
0	5,5E-03	< 1,0E-03	YES	Propeller connection failure/ Abrupt stop of the propeller	6,5E-03
< 1,0E-03	0	0	YES	-	-
< 1,0E-03	0	< 1,0E-03	YES	Propeller structural failure/ Abrupt stop of the propeller	2,0E-03
< 1,0E-03	5,5E-03	0	YES	Propeller structural failure/ Propeller connection failure	6,5E-03
< 1,0E-03	5,5E-03	< 1,0E-03	YES	Propeller structural failure/ Propeller connection failure/ Abrupt stop of the propeller	7,5E-03
Estimated probability of occurrence level, average value:					5,63E-03

Table 85 – Rotor wing RPAS – Loss of Propulsion Subsystem functionality

Loss of RPAS Propulsion Subsystem functionality				Possible multiple failures	Hazards
ESC failure	Brushless electric motor failure	Propeller failure	Loss of RPAS Propulsion Subsystem functionality		
0	0	0	0	-	Degradation or loss of rotor wing RPAS propulsion functionality Degradation or loss of rotor wing RPAS control Degradation or loss of rotor wing RPAS manoeuvrability Uncontrolled projection of propeller debris
0	0	5,63E-03	5,63E-03	-	
0	4,22E-03	0	4,22E-03	-	
0	4,22E-03	5,63E-03	9,85E-03	Electric motor failure/ Propeller failure	
1,4E-01	0	0	1,4E-01	-	
1,4E-01	0	5,63E-03	1,46E-01	ESC failure/ Propeller failure	
1,4E-01	4,22E-03	0	1,44E-01	ESC failure/ Electric motor failure	
1,4E-01	4,22E-03	5,63E-03	1,5E-01	ESC failure/ Electric motor failure/ Propeller failure	
Estimated probability of occurrence level, range:					D → B

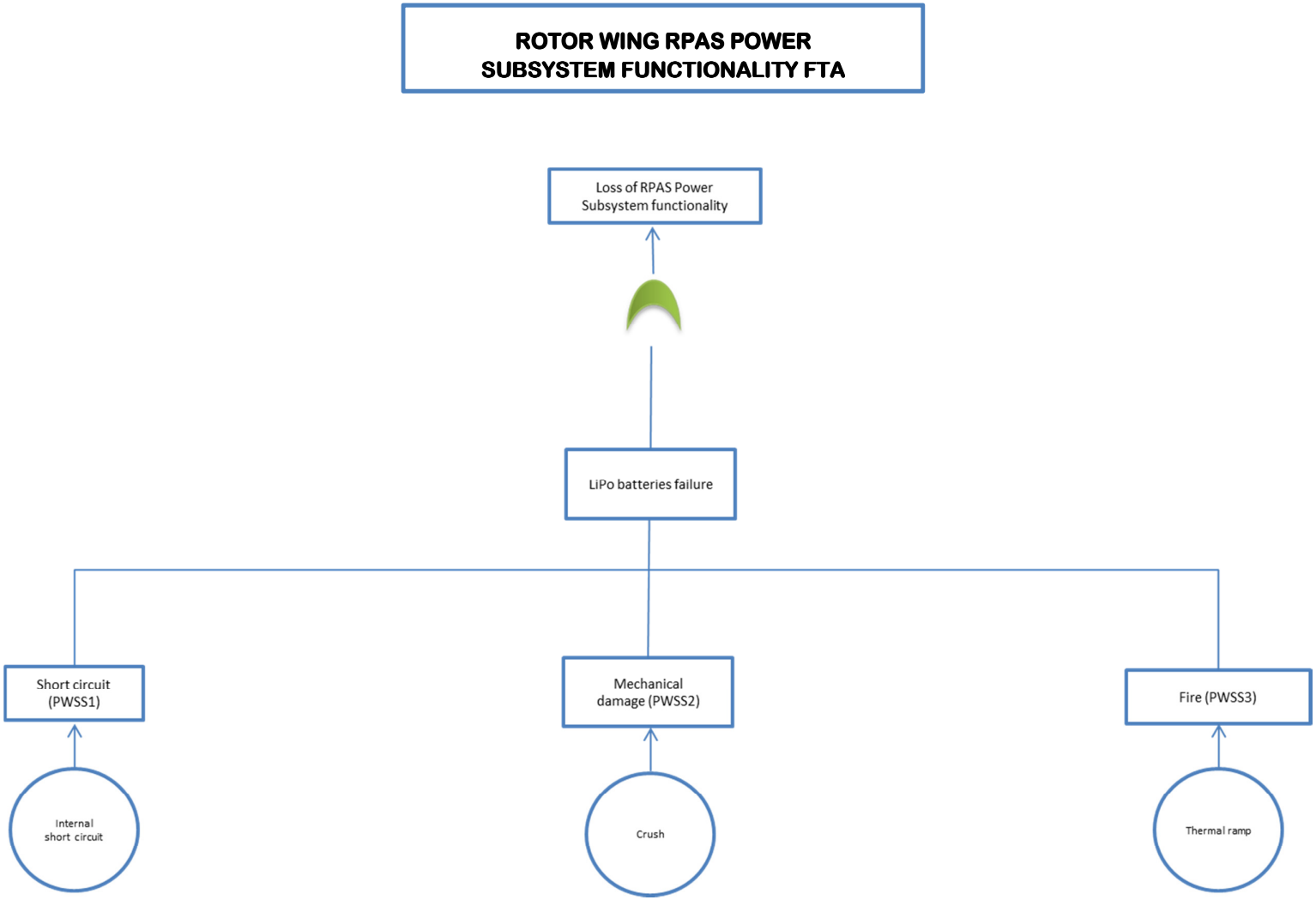


Figure 41 – Rotor wing RPAS Power Subsystem functionality FTA

Table 86 – Rotor wing RPAS – Loss of Power Subsystem functionality

Loss of RPAS Power Subsystem/functionality				Possible multiple failures	Hazards
Short circuit (PWSS1)	Mechanical damage (PWSS2)	Fire (PWSS3)	Loss of RPAS Power Subsystem functionality		
0	0	0	0	-	Degradation or loss of rotor wing RPAS power functionality Fire
0	0	5,5E-02	5,5E-02	-	
0	5,5E-02	0	5,5E-02	-	
0	5,5E-02	5,5E-02	1,1E-01	Mechanical damage/Fire	
5,5E-02	0	0	5,5E-02	-	
5,5E-02	0	5,5E-02	1,1E-01	Short circuit/Fire	
5,5E-02	5,5E-02	0	1,1E-01	Short circuit/ Mechanical damage	
5,5E-02	5,5E-02	5,5E-02	1,65E-01	Short circuit/ Mechanical damage/ Fire	
Estimated probability of occurrence level:					B

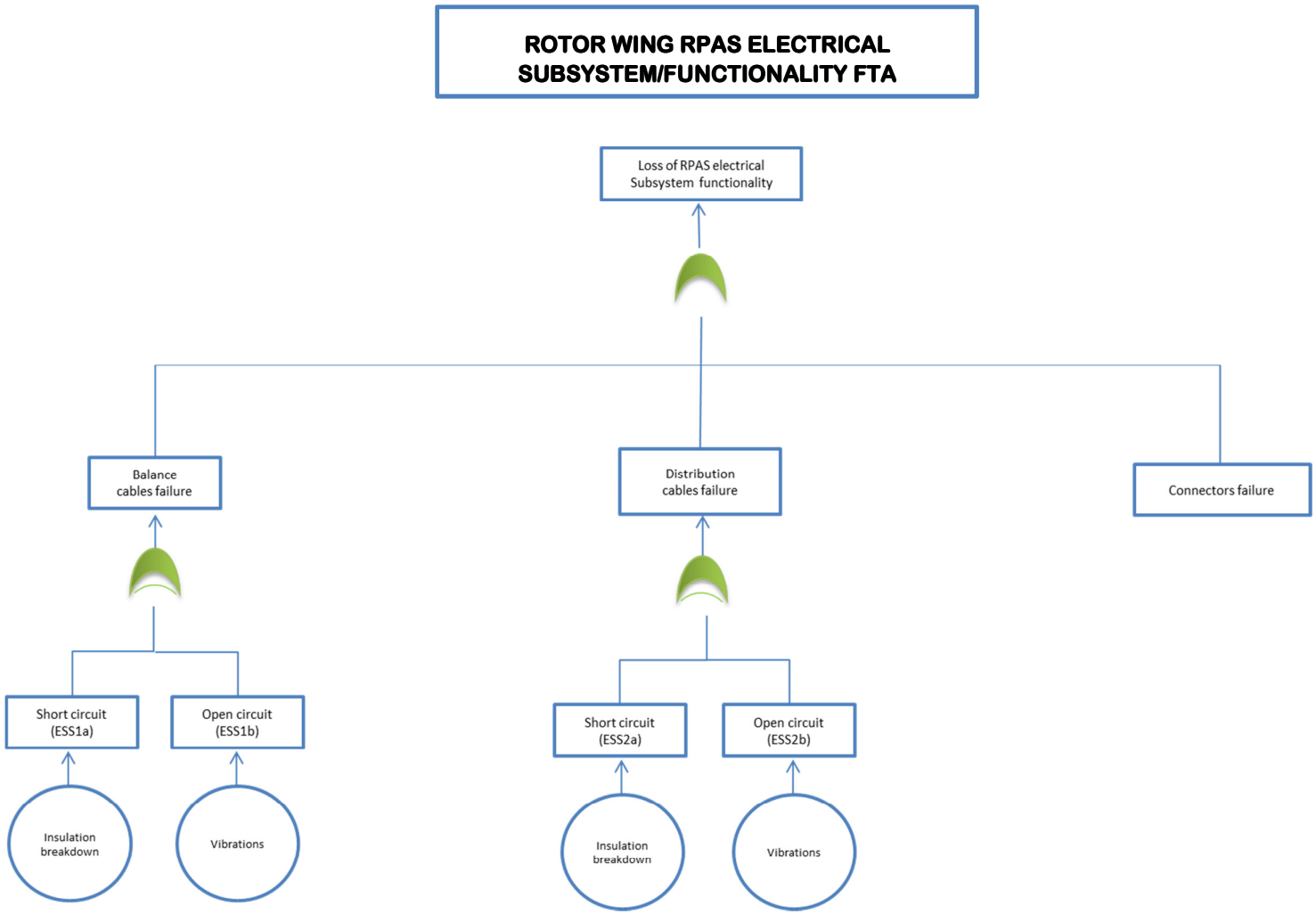


Figure 42 – Rotor wing RPAS Electrical Subsystem functionality FTA

Table 87 – Rotor wing RPAS – Balance cables multiple failures

Balance cables failure modes			Possible multiple failures	
Short circuit (ESS1a)	Open circuit (ESS1b)	Balance cables failure		
0	0	NO	-	-
0	5,5E-02	YES	Short circuit	5,5E-02
2,0E-01	0	YES	Open circuit	2,0E-01
2,0E-01	5,5E-02	YES	-	
Estimated probability of occurrence level, average value:				-

Table 88 – Rotor wing RPAS – Distribution cables multiple failures

Distribution cables failure modes			Possible multiple failures	
Short circuit (ESS2a)	Open circuit (ESS2b)	Balance cables failure		
0	0	NO	-	-
0	5,5E-02	YES	Short circuit	5,5E-02
2,0E-01	0	YES	Open circuit	2,0E-01
2,0E-01	5,5E-02	YES	-	-
Estimated probability of occurrence level, average value:				-

Table 89 – Rotor wing RPAS – Loss of Electrical Subsystem functionality

Loss of RPAS Electrical subsystem functionality				Possible multiple failures	Hazards
Balance wires failure	Distribution cables failure	Electrical connectors failure	Loss of RPAS Electrical Subsystem functionality		
0	0	0	0	-	Degradation or loss of rotor wing RPAS electrical functionality Fire
0	0	5,5E-02	5,5E-02	-	
0	2,0E-01	0	2,0E-01	-	
0	2,0E-01	5,5E-02	2,55E-01	Distribution cables failure/Electrical connectors failure	
2,0E-01	0	0	2,0E-01	-	
2,0E-01	0	5,5E-02	2,55E-01	Balance wires failure/ Electrical connectors failure	
2,0E-01	2,0E-01	0	4,0E-01	Balance wires failure/Distribution cables failure	
2,0E-01	2,0E-01	5,5E-02	4,55E-01	Balance wires failure/Distribution cables failure/Electrical connectors failure	
Estimated probability of occurrence level:					A

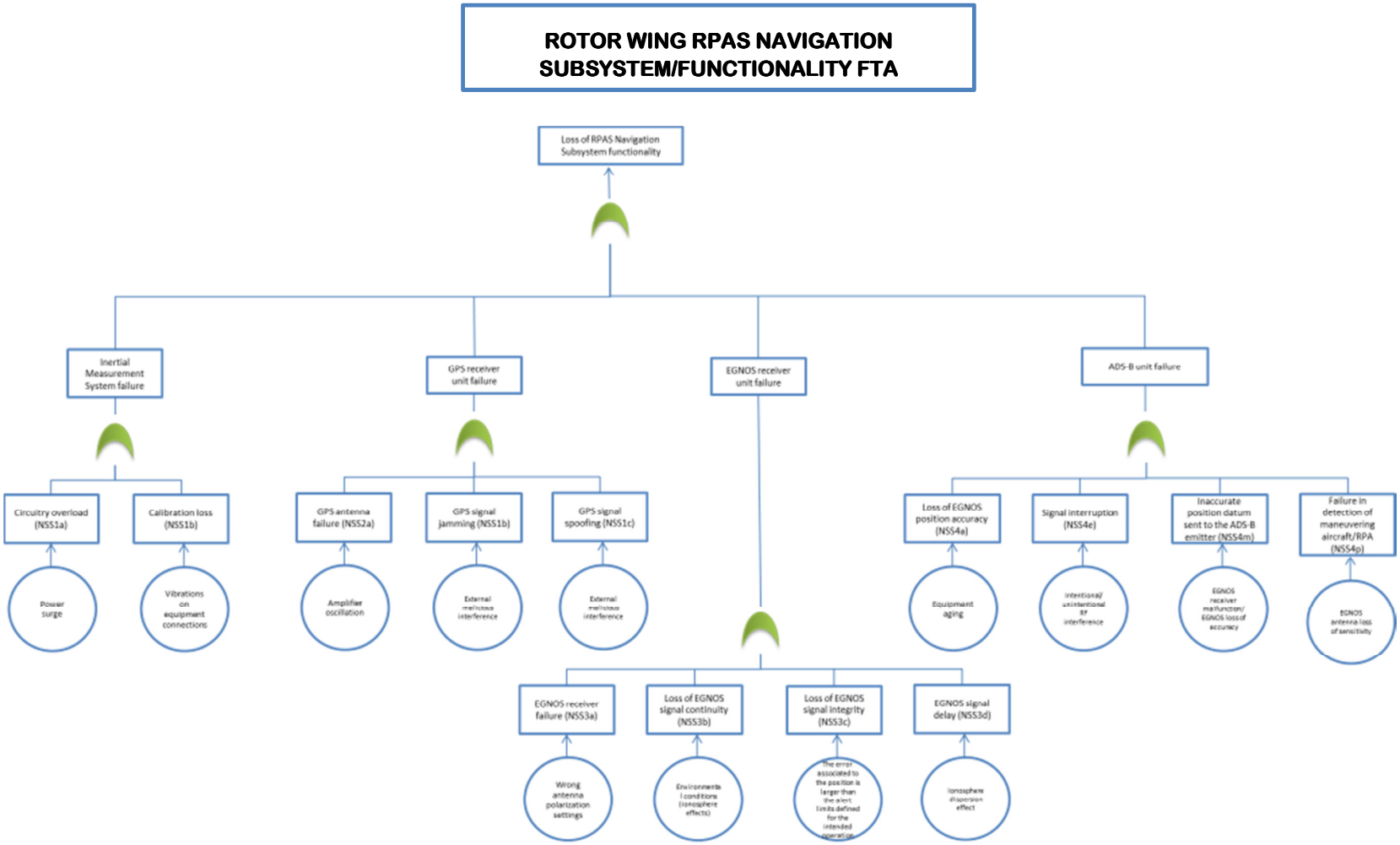


Figure 43 - Rotor wing RPAS Navigation Subsystem functionality FTA

Table 90 – Rotor wing RPAS – Inertial Measurement Unit multiple failures

Inertial Measurement Unit single failure modes			Possible multiple failures	
Circuitry overload (NSS1a)	Calibration loss (NSS1b)	Inertial Measurement Unit failure		
0	0	NO	-	-
0	5,5E-02	YES	-	-
5,5E-03	0	YES	-	-
5,5E-03	5,5E-02	YES	Circuitry overload/Calibration loss	6,05E-02
Estimated probability of occurrence level, average value:				6,05E-02

Table 91 – Rotor wing RPAS – GPS receiver unit multiple failures

GPS receiver unit single failure modes				Possible multiple failures	
GPS antenna failure (NSS2a)	GPS signal jamming (NSS2b)	GPS signal spoofing (NSS2c)	GPS unit receiver failure		
0	0	0	NO	-	-
0	0	1,5E-01	YES	-	-
0	< 1,0E-03	0	YES	-	-
0	< 1,0E-03	1,5E-01	YES	GPS signal jamming/ GPS signal spoofing	1,51E-01
< 1,0E-03	0	0	YES	-	-
< 1,0E-03	0	1,5E-01	YES	GPS antenna failure/ GPS signal spoofing	2,0E-03
< 1,0E-03	< 1,0E-03	0	YES	GPS antenna failure/ GPS signal jamming	1,51E-01
< 1,0E-03	< 1,0E-03	1,5E-01	YES	GPS antenna failure/ GPS signal jamming/ GPS signal spoofing	1,52E-02
Estimated probability of occurrence level, average value:					7,98E-02

Table 92 – Rotor wing RPAS – EGNOS receiver unit multiple failures

EGNOS receiver unit single failure modes					Possible multiple failures	
EGNOS receiver failure (NSS3a)	Loss of EGNOS signal continuity (NSS3b)	Loss of EGNOS signal integrity (NSS3c)	EGNOS signal delay (NSS3d)	EGNOS receiver unit failure		
0	0	0	0	NO	-	-
0	0	0	5,5E-03	YES	-	-
0	0	1,0E-03	0	YES	-	-
0	0	1,0E-03	5,5E-03	YES	Loss of EGNOS signal integrity/ EGNOS signal delay	6,5E-03
0	5,5E-03	0	0	YES	-	-
0	5,5E-03	0	5,5E-03	YES	Loss of EGNOS signal continuity/ EGNOS signal delay	1,1E-02
0	5,5E-03	1,0E-03	0	YES	Loss of EGNOS signal continuity/ EGNOS signal d Loss of EGNOS signal integrity	6,5E-03
0	5,5E-03	1,0E-03	5,5E-03	YES	Loss of EGNOS signal continuity / EGNOS signal d Loss of EGNOS signal integrity/ EGNOS signal delay	1,1E-02
2,0E-01	0	0	0	YES	-	-
2,0E-01	0	0	5,5E-03	YES	EGNOS receiver failure/ EGNOS signal delay	2,055E-01
2,0E-01	0	1,0E-03	0	YES	EGNOS receiver failure/ Loss of EGNOS signal integrity	2,01E-01
2,0E-01	0	1,0E-03	5,5E-03	YES	EGNOS receiver failure/ Loss of EGNOS signal integrity/ EGNOS signal delay	2,065E-01
2,0E-01	5,5E-03	0	0	YES	EGNOS receiver failure/ Loss of EGNOS signal continuity	2,055E-01
2,0E-01	5,5E-03	0	5,5E-03	YES	EGNOS receiver failure/ Loss of EGNOS signal continuity/ EGNOS signal delay	2,11E-01
2,0E-01	5,5E-03	1,0E-03	0	YES	EGNOS receiver failure/ Loss of EGNOS signal continuity/ Loss of EGNOS signal integrity	2,065E-01
2,0E-01	5,5E-03	1,0E-03	5,5E-03	YES	EGNOS receiver failure/ Loss of EGNOS signal continuity/ Loss of EGNOS signal integrity Windings open circuit/ Armature shaft structural damage/ EGNOS signal delay	2,12E-01
Estimated probability of occurrence level, average value:						1,35E-01

Table 93 – Rotor wing RPAS – ADS-B unit multiple failures

ADS-B unit single failure modes					Possible multiple failures	
Loss of EGNOS position accuracy (NSS4a)	Signal interruption (NSS4e)	Inaccurate position datum sent to the ADS-B emitter (NSS4m)	Failure in detection of maneuvering aircraft/RPA (NSS4p)	ADS-B unit failure		
0	0	0	0	NO	-	-
0	0	0	2,0E-01	YES	-	-
0	0	2,12E-01	0	YES	-	-
0	0	2,12E-01	2,0E-01	YES	Inaccurate position datum sent to the ADS-B emitter/ Failure in detection of maneuvering aircraft/RPA	4,0E-01
0	1,51E-01	0	0	YES	-	-
0	1,51E-01	0	2,0E-01	YES	Signal interruption/ Failure in detection of maneuvering aircraft/RPA	4,0E-01
0	1,51E-01	2,12E-01	0	YES	Signal interruption/ Inaccurate position datum sent to the ADS-B emitter	4,0E-01
0	1,51E-01	2,12E-01	2,0E-01	YES	Signal interruption/ Inaccurate position datum sent to the ADS-B emitter/ Failure in detection of maneuvering aircraft/RPA	6,0E-01
2,0E-01	0	0	0	YES	-	-
2,0E-01	0	0	2,0E-01	YES	Loss of EGNOS position accuracy/ Failure in detection of maneuvering aircraft/RPA	4,0E-01
2,0E-01	0	2,12E-01	0	YES	Loss of EGNOS position accuracy/ Inaccurate position datum sent to the ADS-B emitter/	4,0E-01
2,0E-01	0	2,12E-01	2,0E-01	YES	Loss of EGNOS position accuracy/ Inaccurate position datum sent to the ADS-B emitter/ Failure in detection of maneuvering aircraft/RPA	6,0E-01
2,0E-01	1,51E-01	0	0	YES	Loss of EGNOS position accuracy/ Signal interruption/	4,0E-01
2,0E-01	1,51E-01	0	2,0E-01	YES	Loss of EGNOS position accuracy/ Signal interruption/ Failure in detection of maneuvering aircraft/RPA	6,0E-01
2,0E-01	1,51E-01	2,12E-01	0	YES	Loss of EGNOS position accuracy/ Signal interruption/ Inaccurate position datum sent to the ADS-B emitter/	6,0E-01
2,0E-01	1,51E-01	2,12E-01	2,0E-01	YES	Loss of EGNOS position accuracy/ Signal interruption/ Inaccurate position datum sent to the ADS-B emitter/ Failure in detection of maneuvering aircraft/RPA	8,0E-01
Estimated probability of occurrence level, average value:						5,09E-01

Table 94 – Rotor wing RPAS – Loss of Navigation Subsystem functionality

Loss of RPAS Navigation Subsystem functionality					Possible multiple failures	Hazards
Inertial Measurement Unit failure	GPS receiver unit failure	EGNOS receiver unit failure	ADS-B unit failure	Loss of Navigation Subsystem functionality		
0	0	0	0	0	-	Degradation or loss of navigation functionality Degradation or loss of GPS functionality on board the RPAS Degradation or loss of EGNOS functionality on board the RPAS Degradation or loss of ADS-B functionality on board the RPAS
0	0	0	5,09E-01	5,09E-01	-	
0	0	1,35E-01	0	1,35E-01	-	
0	0	1,35E-01	5,09E-01	6,44E-01	EGNOS receiver unit failure/ADS-B unit failure	
0	7,98E-02	0	0	7,98E-02	-	
0	7,98E-02	0	5,09E-01	5,888E-01	GPS receiver unit failure/EGNOS receiver unit failure	
0	7,98E-02	1,35E-01	0	2,148E-01	GPS receiver unit failure/ EGNOS receiver unit failure	
0	7,98E-02	1,35E-01	5,09E-01	7,238E-01	GPS receiver unit failure/ EGNOS receiver unit failure/ADS-B unit failure	
6,05E-02	0	0	0	6,05E-02	-	
6,05E-02	0	0	5,09E-01	5,695E-01	Inertial Measurement Unit failure/ADS-B unit failure	
6,05E-02	0	1,35E-01	0	1,955E-01	Inertial Measurement Unit failure/EGNOS receiver unit failure	
6,05E-02	0	1,35E-01	5,09E-01	7,045E-01	Inertial Measurement Unit failure/EGNOS receiver unit failure/ADS-B unit failure	
6,05E-02	7,98E-02	0	0	1,403E-01	Inertial Measurement Unit failure/GPS receiver unit failure	
6,05E-02	7,98E-02	0	5,09E-01	6,493E-01	Inertial Measurement Unit failure/GPS receiver unit failure/ ADS-B unit failure	
6,05E-02	7,98E-02	1,35E-01	0	2,753E-01	Inertial Measurement Unit failure/GPS receiver unit failure/ EGNOS receiver unit failure	
6,05E-02	7,98E-02	1,35E-01	5,09E-01	7,843E-01	Inertial Measurement Unit failure/GPS receiver unit failure/ EGNOS receiver unit failure/ADS-B unit failure	
Estimated probability of occurrence level:						A

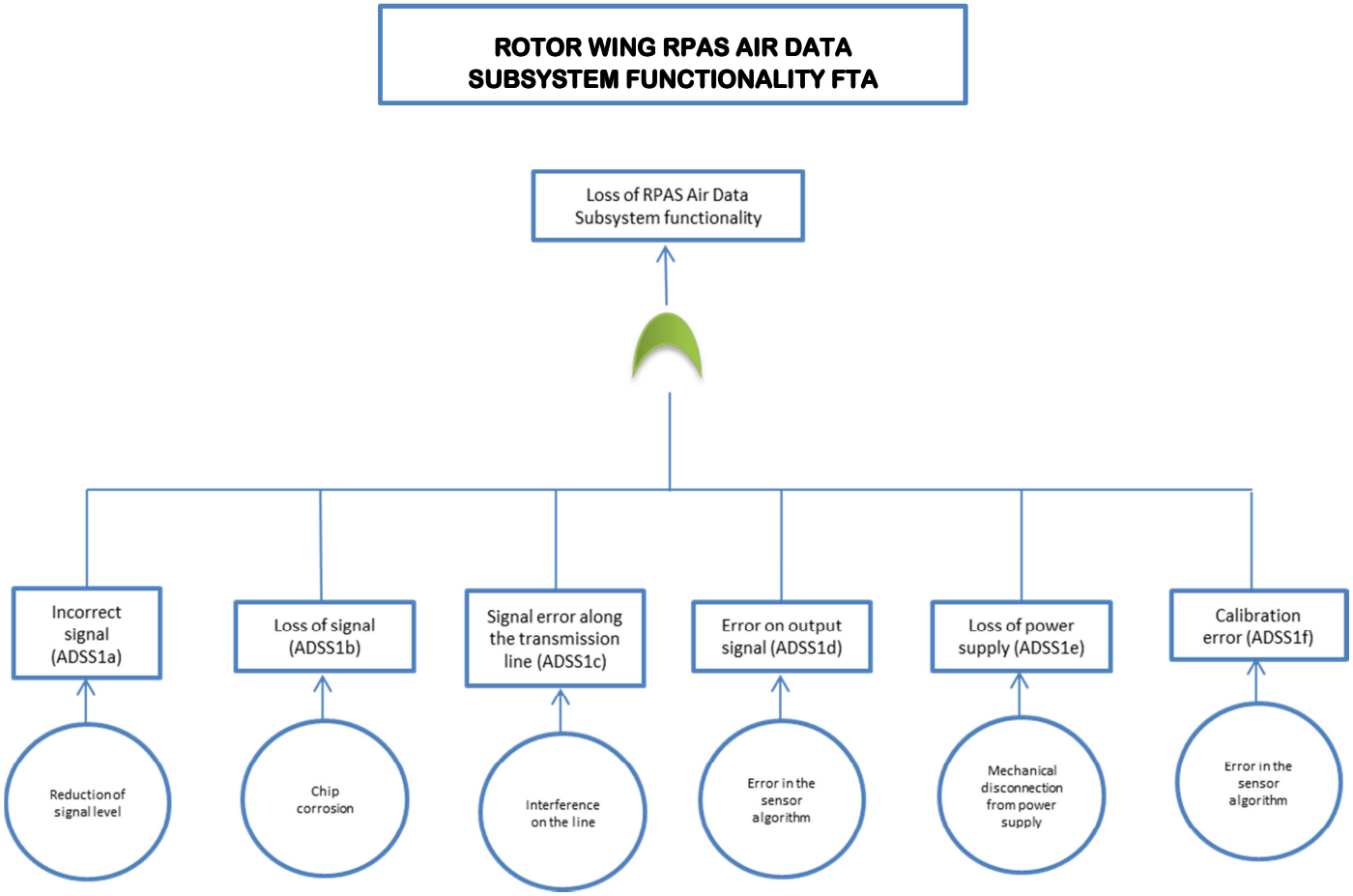


Figure 44 - Rotor wing RPAS Air Data Subsystem functionality FTA

Table 95 – Rotor wing RPAS - Loss of Air Data Subsystem functionality

Loss of RPAS Air Data Subsystem functionality							Possible multiple failures	Hazards
Incorrect signal (ADSS1a)	Loss of signal (ADSS1b)	Signal error along the transmission line (ADSS1c)	Error on output signal (ADSS1d)	Loss of power supply (ADSS1e)	Calibration error (ADSS1f)	Loss of RPAS Air Data Subsystem functionality		
0	0	0	0	0	0	0	-	Pressure sensors failure Misleading altitude indication Misleading airspeed indication Degradation or loss of control of RPAS flight attitude
0	0	0	0	0	5,5E-02	5,5E-02	-	
0	0	0	0	2,0E-01	0	2,0E-01	-	
0	0	0	0	2,0E-01	5,5E-02	2,55E-01	Loss of power supply/Calibration error	
0	0	0	5,5E-02	0	0	5,5E-02	-	
0	0	0	5,5E-02	0	5,5E-02	1,1E-01	Error on output signal/ Calibration error	
0	0	0	5,5E-02	2,0E-01	0	2,55E-01	Error on output signal/Loss of power supply	
0	0	0	5,5E-02	2,0E-01	5,5E-02	3,1E-01	Error on output signal/Loss of power supply/Calibration error	
0	0	5,5E-02	0	0	0	5,5E-02	-	
0	0	5,5E-02	0	0	5,5E-02	1,1E-01	Signal error along the transmission line/ Calibration error	
0	0	5,5E-02	0	2,0E-01	0	2,55E-01	Signal error along the transmission line/Calibration error	
0	0	5,5E-02	0	2,0E-01	5,5E-02	3,1E-01	Signal error along the transmission line/ Loss of power supply/Calibration error	
0	0	5,5E-02	5,5E-02	0	0	1,1E-01	Signal error along the transmission line/Error on output signal	
0	0	5,5E-02	5,5E-02	0	5,5E-02	1,65E-01	Signal error along the transmission line/Error on output signal/Calibration error	
0	0	5,5E-02	5,5E-02	2,0E-01	0	3,1E-01	Signal error along the transmission line/Error on output signal/Loss of power supply	
0	0	5,5E-02	5,5E-02	2,0E-01	5,5E-02	3,65E-01	Signal error along the transmission line/Error on output signal/ Loss of power supply/Calibration error	
0	2,0E-01	0	0	0	0	2,0E-01	-	
0	2,0E-01	0	0	0	5,5E-02	2,55E-01	Loss of signal/ Calibration error	
0	2,0E-01	0	0	2,0E-01	0	4,0E-01	Loss of signal/Loss of power supply	
0	2,0E-01	0	0	2,0E-01	5,5E-02	4,55E-01	Loss of signal/ Loss of power supply/Calibration error	
0	2,0E-01	0	5,5E-02	0	0	2,55E-01	Loss of signal/Error on output signal	
0	2,0E-01	0	5,5E-02	0	5,5E-02	3,1E-01	Loss of signal/Error on output signal/Calibration error	
0	2,0E-01	0	5,5E-02	2,0E-01	0	4,55E-01	Loss of signal/Error on output signal/Loss of power supply	
0	2,0E-01	0	5,5E-02	2,0E-01	5,5E-02	5,1E-01	Loss of signal/Error on output signal/ Loss of power supply/Calibration error	

Table 95 – Rotor wing RPAS - Loss of Air Data Subsystem functionality (Cont'd)

Loss of RPAS Air Data Subsystem functionality							Possible multiple failures	Hazards
Incorrect signal (ADSS1a)	Loss of signal (ADSS1b)	Signal error along the transmission line (ADSS1c)	Error on output signal (ADSS1d)	Loss of power supply (ADSS1e)	Calibration error (ADSS1f)	Loss of RPAS Air Data Subsystem functionality		
0	2,0E-01	5,5E-02	0	0	0	2,55E-01	Loss of signal/Signal error along the transmission line	
0	2,0E-01	5,5E-02	0	0	5,5E-02	3,1E-01	Loss of signal/Signal error along the transmission line/ Calibration error	
0	2,0E-01	5,5E-02	0	2,0E-01	0	4,55E-01	Loss of signal/Signal error along the transmission line/ Loss of power supply	
0	2,0E-01	5,5E-02	0	2,0E-01	5,5E-02	5,1E-01	Loss of signal/Signal error along the transmission line/ Loss of power supply/Calibration error	
0	2,0E-01	5,5E-02	5,5E-02	0	0	3,1E-01	Loss of signal/Signal error along the transmission line/Error on output signal	
0	2,0E-01	5,5E-02	5,5E-02	0	5,5E-02	3,65E-01	Loss of signal/Signal error along the transmission line/ Error on output signal/Calibration error	
0	2,0E-01	5,5E-02	5,5E-02	2,0E-01	0	5,1E-01	Loss of signal/Signal error along the transmission line/Error on output signal/Loss of power supply	
0	2,0E-01	5,5E-02	5,5E-02	2,0E-01	5,5E-02	5,65E-01	Loss of signal/Signal error along the transmission line/Error on output signal/ Loss of power supply/Calibration error	
2,0E-01	0	0	0	0	0	2,0E-01	-	
2,0E-01	0	0	0	0	5,5E-02	2,55E-01	Incorrect signal/ Calibration error	
2,0E-01	0	0	0	2,0E-01	0	4,0E-01	Incorrect signal/ Loss of power supply	
2,0E-01	0	0	0	2,0E-01	5,5E-02	4,55E-01	Incorrect signal/ Loss of power supply/Calibration error	
2,0E-01	0	0	5,5E-02	0	0	2,55E-01	Incorrect signal/Error on output signal	
2,0E-01	0	0	5,5E-02	0	5,5E-02	3,1E-01	Incorrect signal/Error on output signal/Calibration error	
2,0E-01	0	0	5,5E-02	2,0E-01	0	4,55E-01	Incorrect signal/Error on output signal/Loss of power supply	
2,0E-01	0	0	5,5E-02	2,0E-01	5,5E-02	5,1E-01	Incorrect signal/Error on output signal/ Loss of power supply/Calibration error	
2,0E-01	0	5,5E-02	0	0	0	2,55E-01	Incorrect signal/Signal error along the transmission line	
2,0E-01	0	5,5E-02	0	0	5,5E-02	3,1E-01	Incorrect signal/Signal error along the transmission line/ Calibration error	

Table 95 – Rotor wing RPAS - Loss of Air Data Subsystem functionality (Cont'd)

Loss of RPAS Air Data Subsystem functionality							Possible multiple failures	Hazards
Incorrect signal (ADSS1a)	Loss of signal (ADSS1b)	Signal error along the transmission line (ADSS1c)	Error on output signal (ADSS1d)	Loss of power supply (ADSS1e)	Calibration error (ADSS1f)	Loss of RPAS Air Data Subsystem functionality		
2,0E-01	0	5,5E-02	0	2,0E-01	0	4,55E-01	Incorrect signal/Signal error along the transmission line/ Loss of power supply	
2,0E-01	0	5,5E-02	0	2,0E-01	5,5E-02	5,1E-01	Incorrect signal/Signal error along the transmission line/ Loss of power supply/Calibration error	
2,0E-01	0	5,5E-02	5,5E-02	0	0	3,1E-01	Incorrect signal/Signal error along the transmission line/ Calibration error	
2,0E-01	0	5,5E-02	5,5E-02	0	5,5E-02	3,65E-01	Incorrect signal/Signal error along the transmission line/ Error on output signal/Calibration error	
2,0E-01	0	5,5E-02	5,5E-02	2,0E-01	0	5,1E-01	Incorrect signal/Signal error along the transmission line/Error on output signal/Loss of power supply	
2,0E-01	0	5,5E-02	5,5E-02	2,0E-01	5,5E-02	5,65E-01	Incorrect signal/Signal error along the transmission line/ Error on output signal/ Loss of power supply/Calibration error	
2,0E-01	2,0E-01	0	0	0	0	4,0E-01	Incorrect signal/ Loss of signal	
2,0E-01	2,0E-01	0	0	0	5,5E-02	4,55E-01	Incorrect signal/Loss of signal/Calibration error	
2,0E-01	2,0E-01	0	0	2,0E-01	0	6,0E-01	Incorrect signal/Loss of signal/Loss of power supply	
2,0E-01	2,0E-01	0	0	2,0E-01	5,5E-02	6,55E-01	Incorrect signal/Loss of signal/Loss of power supply/Calibration error	
2,0E-01	2,0E-01	0	5,5E-02	0	0	4,55E-01	Incorrect signal/Loss of signal/Error on output signal	
2,0E-01	2,0E-01	0	5,5E-02	0	5,5E-02	5,1E-01	Incorrect signal/Loss of signal/Error on output signal/Calibration error	
2,0E-01	2,0E-01	0	5,5E-02	2,0E-01	0	6,55E-01	Incorrect signal/Loss of signal/Error on output signal/Loss of power supply	
2,0E-01	2,0E-01	0	5,5E-02	2,0E-01	5,5E-02	7,1E-01	Incorrect signal/Loss of signal/Error on output signal/Loss of power supply/Calibration error	
2,0E-01	2,0E-01	5,5E-02	0	0	0	4,55E-01	Incorrect signal/Loss of signal/Signal error along the transmission line	
2,0E-01	2,0E-01	5,5E-02	0	0	5,5E-02	5,1E-01	Incorrect signal/Loss of signal/Signal error along the transmission line/ Calibration error	
2,0E-01	2,0E-01	5,5E-02	0	2,0E-01	0	6,55E-01	Incorrect signal/Loss of signal/Signal error along the transmission line/Loss of power supply	

Table 95 – Rotor wing RPAS - Loss of Air Data Subsystem functionality (Cont'd)

Loss of RPAS Air Data Subsystem functionality							Possible multiple failures	Hazards
Incorrect signal (ADSS1a)	Loss of signal (ADSS1b)	Signal error along the transmission line (ADSS1c)	Error on output signal (ADSS1d)	Loss of power supply (ADSS1e)	Calibration error (ADSS1f)	Loss of RPAS Air Data Subsystem functionality		
2,0E-01	2,0E-01	5,5E-02	0	2,0E-01	5,5E-02	7,1E-01	Incorrect signal/Loss of signal/Signal error along the transmission line/ Loss of power supply/Calibration error	
2,0E-01	2,0E-01	5,5E-02	5,5E-02	0	0	5,1E-01	Incorrect signal/Loss of signal/Signal error along the transmission line/ Error on output signal	
2,0E-01	2,0E-01	5,5E-02	5,5E-02	0	5,5E-02	5,65E-01	Incorrect signal/Loss of signal/Signal error along the transmission line/ Error on output signal/Calibration error	
2,0E-01	2,0E-01	5,5E-02	5,5E-02	2,0E-01	0	7,1E-01	Incorrect signal/Loss of signal/Signal error along the transmission line/Error on output signal/Loss of power supply	
2,0E-01	2,0E-01	5,5E-02	5,5E-02	2,0E-01	5,5E-02	7,65E-01	Incorrect signal/Loss of signal/Signal error along the transmission line/Error on output signal/Loss of power supply/Calibration error	
Estimated probability of occurrence level:								A

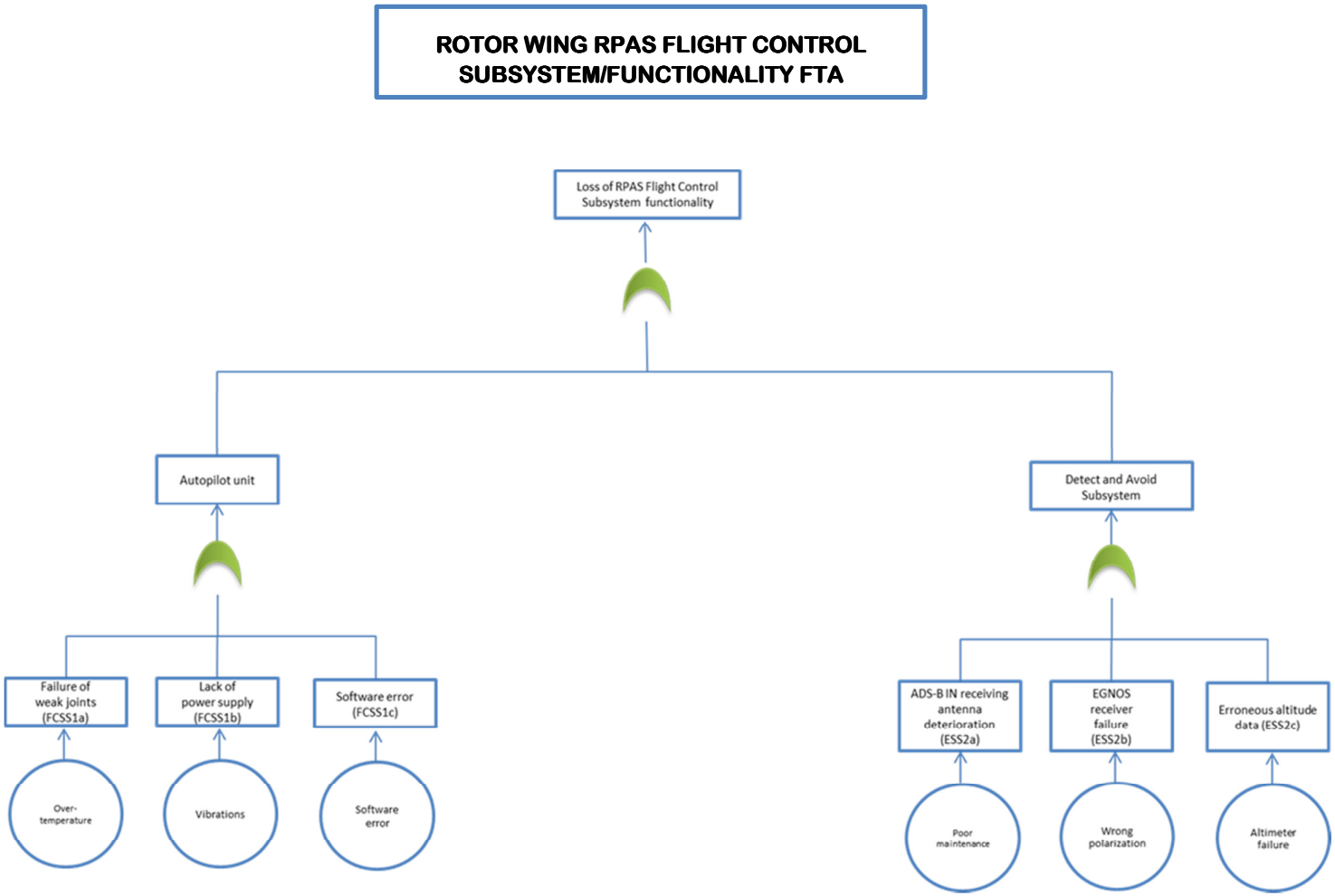


Figure 45 – Rotor wing RPAS Flight Control Subsystem functionality FTA

Table 96 – Rotor wing RPAS – Autopilot Unit multiple failures

Autopilot Unit single failure modes				Possible multiple failures	
Failure of weak joint (FSS1a)	Lack of power supply (FSS1b)	Software error (FSS1c)	Loss of Autopilot Unit functionality		
0	0	0	NO	-	-
0	0	5,5E-03	YES	-	-
0	5,5E-03	0	YES	-	-
0	5,5E-03	5,5E-03	YES	Lack of power supply/ Software error	1,1E-02
5,5E-03	0	0	YES	-	-
5,5E-03	0	5,5E-03	YES	Failure of weak joint/ Software error	1,1E-02
5,5E-03	5,5E-03	0	YES	Failure of weak joint/ Lack of power supply	1,1E-02
5,5E-03	5,5E-03	5,5E-03	YES	Failure of weak joint/ Lack of power supply Software error	1,65E-02
Estimated probability of occurrence level, average value:					1,24E-02

Table 97 – Rotor wing RPAS – Detect and Avoid (DAA) subsystem multiple failures

Detect and Avoid Subsystem single failure modes				Possible multiple failures	
ADS-B IN receiving antenna deterioration (ESS2a)	EGNOS receiver failure (ESS2b)	Erroneous altitude data (ESS2c)	Loss of Detect and Avoid Subsystem functionality		
0	0	0	NO	-	-
0	0	1,0E-03	YES	-	-
0	2,0E-01	0	YES	-	-
0	2,0E-01	1,0E-03	YES	EGNOS receiver failure/ Erroneous altitude data	2,01E-01
5,5E-02	0	0	YES	-	-
5,5E-02	0	1,0E-03	YES	ADS-B IN receiving antenna deterioration/ Erroneous altitude data	5,6E-02
5,5E-02	2,0E-01	0	YES	ADS-B IN receiving antenna deterioration/ EGNOS receiver failure	2,55E-01
5,5E-02	2,0E-01	1,0E-03	YES	ADS-B IN receiving antenna deterioration/ EGNOS receiver failure/ Erroneous altitude data	2,51E-01
Estimated probability of occurrence level, average value:					1,91E-01

Table 98 – Rotor wing RPAS – Loss of Flight Control Subsystem functionality

Loss of RPAS Flight Control subsystem functionality			Possible multiple failures	Hazards
Loss of Autopilot Unit functionality	Loss of Detect and Avoid Subsystem functionality	Loss of RPAS Flight Control Subsystem functionality		
0	0	0	-	Loss or degradation of rotor wing RPAS control Loss or degradation of rotor wing RPAS manoeuvrability
0	1,91E-01	2,55E-01	-	
1,24E-02	0	1,65E-02	-	
1,24E-02	1,91E-01	2,715E-01	Loss of Autopilot Unit functionality/ Loss of Detect and Avoid Subsystem functionality	
Estimated probability of occurrence level, range:				C → A

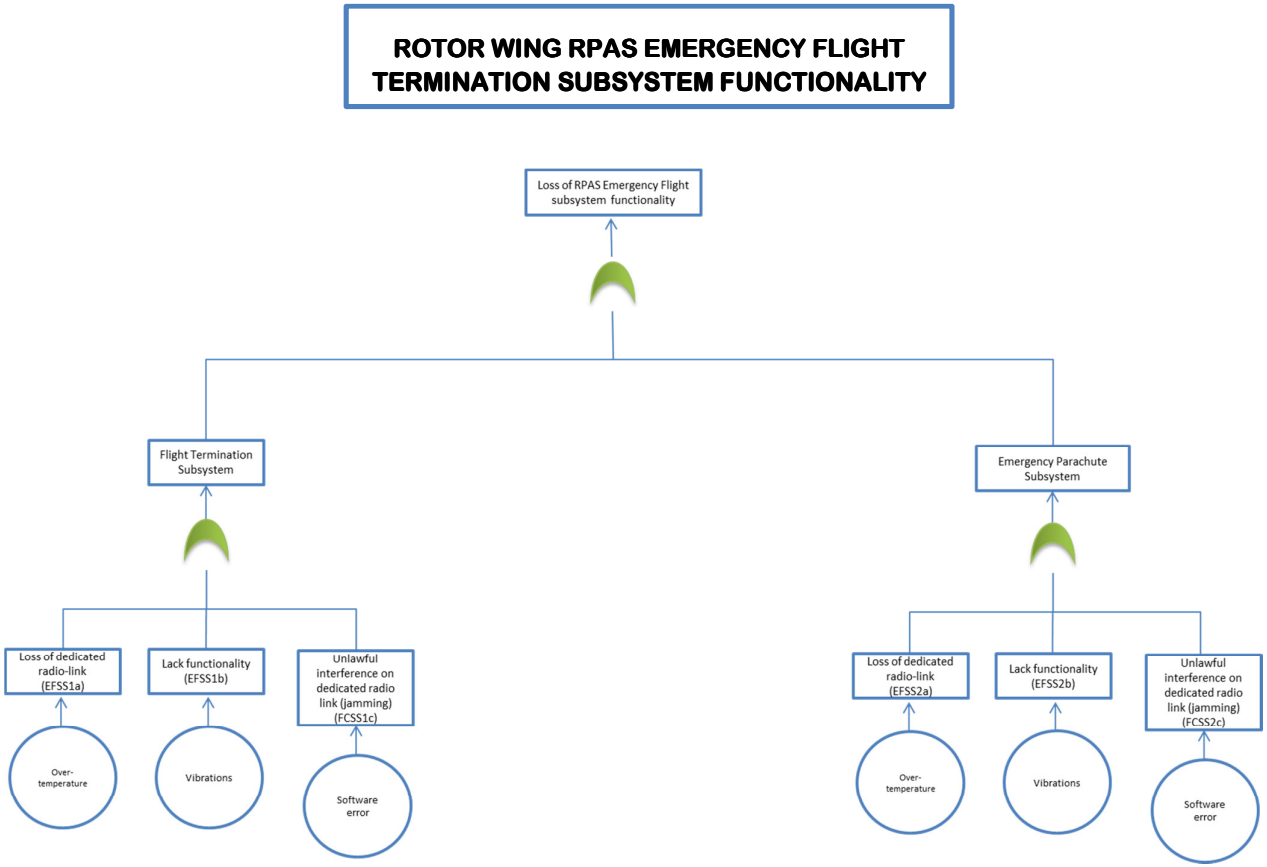


Figure 46 – Rotor wing RPAS Emergency Flight Termination Subsystem functionality FTA

Table 99 – Rotor wing RPAS – Flight Termination System (FTS) multiple failures

Flight Termination System (FTS) single failure modes				Possible multiple failures	
Loss of dedicated radio link (EFSS1a)	Lack of functionality (EFSS1b)	Unlawful interference on dedicated radio link (jamming) (EFSS1c)	Loss of Flight Termination System (FTS) functionality		
0	0	0	NO	-	-
0	0	1,5E-01	YES	-	-
0	5,5E-03	0	YES	-	-
0	5,5E-03	1,5E-01	YES	Lack of functionality/ Unlawful interference on dedicated radio link (jamming)	1,55E-01
5,5E-02	0	0	YES	-	-
5,5E-02	0	1,5E-01	YES	Loss of dedicated radio link/ Unlawful interference on dedicated radio link (jamming)	2,05-01
5,5E-02	5,5E-03	0	YES	Loss of dedicated radio link/ Lack of functionality	6,05E-02
5,5E-02	5,5E-03	1,5E-01	YES	Loss of dedicated radio link/ Lack of functionality/ Unlawful interference on dedicated radio link (jamming)	2,105E-01
Estimated probability of occurrence level, average value:					1,42E-01

Table 100 – Rotor wing RPAS – Emergency parachute multiple failures

Emergency parachute single failure modes				Possible multiple failures	
Loss of dedicated radio link (EFSS2a)	Lack of functionality (EFSS2b)	Unlawful interference on dedicated radio link (jamming) (EFSS2c)	Loss of Emergency Parachute functionality		
0	0	0	NO	-	-
0	0	1,5E-01	YES	-	-
0	5,5E-03	0	YES	-	-
0	5,5E-03	1,5E-01	YES	Lack of functionality/ Unlawful interference on dedicated radio link (jamming)	1,55E-01
5,5E-02	0	0	YES	-	-
5,5E-02	0	1,5E-01	YES	Loss of dedicated radio link/ Unlawful interference on dedicated radio link (jamming)	2,05-01
5,5E-02	5,5E-03	0	YES	Loss of dedicated radio link/ Lack of functionality	6,05E-02
5,5E-02	5,5E-03	1,5E-01	YES	Loss of dedicated radio link/ Lack of functionality/ Unlawful interference on dedicated radio link (jamming)	2,105E-01
Estimated probability of occurrence level, average value:					1,42E-01

Table 101 – Rotor wing RPAS – Loss of Emergency Flight Termination Subsystem functionality

Loss of RPAS Emergency Flight subsystem functionality			Possible multiple failures	Hazards
Loss of Flight Termination System (FTS) functionality	Loss of Emergency Parachute functionality	Loss of RPAS Emergency Flight Termination Subsystem functionality		
0	0	0	-	Degradation or loss of emergency flight termination functionality Degradation or loss of FTS functionality Degradation or loss of Emergency Parachute functionality Uncontrolled impact on ground Uncontrolled projection of debris Uncontrolled impact with third parties
0	1,42E-01	1,42E-01	-	
1,42E-01	0	1,42E-01	-	
1,42E-01	1,42E-01	2,84E-01	Loss of Flight Termination System (FTS) functionality/ Loss of Emergency Parachute functionality	
Estimated probability of occurrence level, range:				B → A

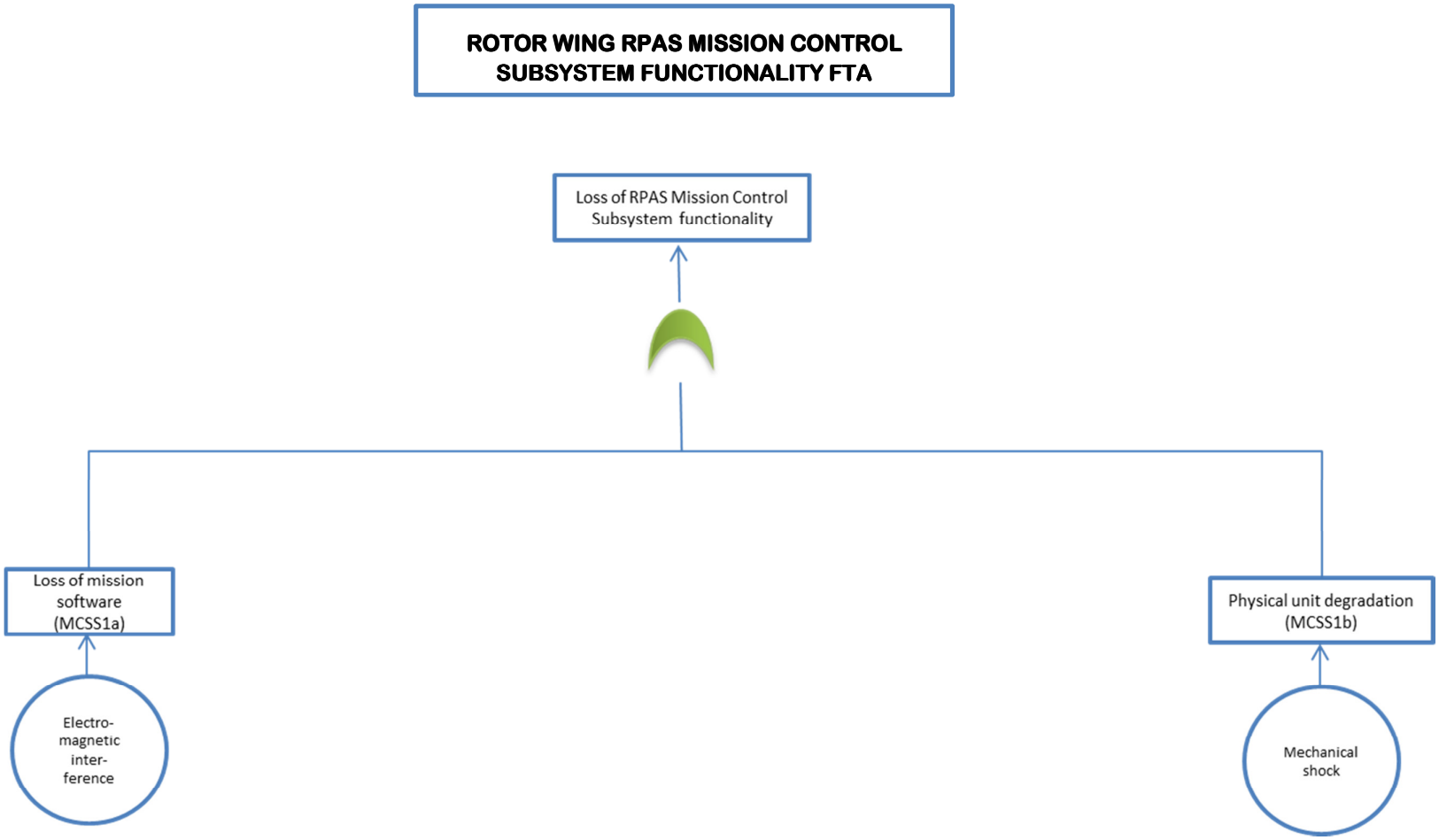


Figure 47 – Rotor wing RPAS Mission Control Subsystem functionality FTA

Table 102 – Rotor wing RPAS – Loss of Mission Control Flight Subsystem functionality

Loss of RPAS Mission Control subsystem functionality			Possible multiple failures	Hazards
Loss of mission software (MCSS1a)	Physical Unit Degradation (MCSS1b)	Loss of RPAS Control Subsystem functionality		
0	0	0	-	Loss of RPAS Mission Control subsystem functionality
0	5,5E-02	5,5E-02	-	
5,5E-02	0	5,5E-02	-	
5,5E-02	5,5E-02	1,1E-01	Loss of mission software/ Physical unit Degradation	
Estimated probability of occurrence level, range:				C → B

ROTOR WING RPAS PAYLOAD SENSORS SUBSYSTEM FUNCTIONALITY FTA

Note: Rotor Wing RPAS Mission Payload Sensors Subsystem FTA: not performed; the effects of mission payload sensor combined failures are negligible for the RPAS specific category operations safety.

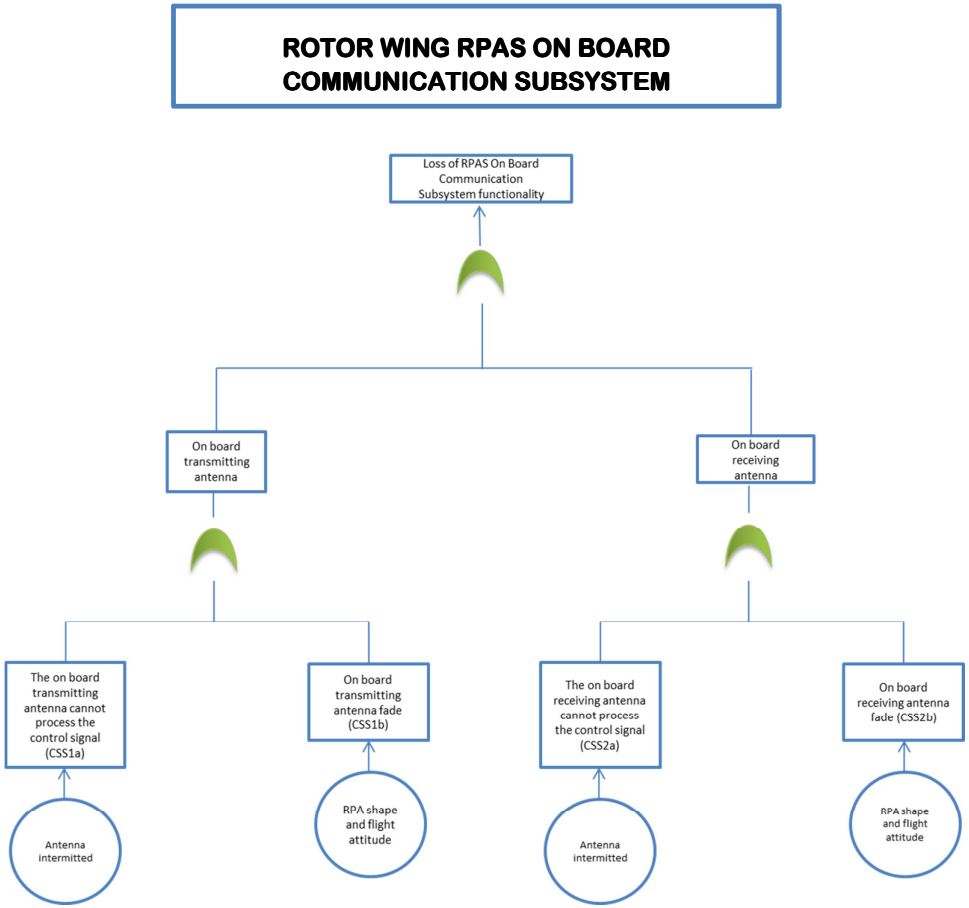


Figure 48 - Rotor Wing RPAS On Board Communication Subsystem functionality FTA

Table 103 – Rotor wing RPAS – On board transmitting antenna multiple failures

On board transmitting single failure modes			Possible multiple failures	
The on board transmitting antenna cannot process the control signal (CSS1a)	On board transmitting antenna fade (CSS1b)	Loss of on board transmitting antenna functionality		
0	0	NO	-	-
0	5,5E-02	YES	-	-
5,5E-03	0	YES	-	-
5,5E-03	5,5E-02	YES	The on board transmitting antenna cannot process the control signal/ On board transmitting antenna fade	6,05E-02
Estimated probability of occurrence level, average value:				6,05E-02

Table 104 – Rotor wing RPAS – On board receiving antenna multiple failures

On board transmitting single failure modes			Possible multiple failures	
The on board receiving antenna cannot process the control signal (CSS2a)	On board receiving antenna fade (CSS2b)	Loss of on board receiving antenna functionality		
0	0	NO	-	-
0	5,5E-02	YES	-	-
5,5E-03	0	YES	-	-
5,5E-03	5,5E-02	YES	The on board receiving antenna cannot process the control signal/ On board receiving antenna fade	6,05E-02
Estimated probability of occurrence level, average value:				6,05E-02

Table 105 – Rotor wing RPAS – Loss of On Board Communication Subsystem functionality

Loss of On Board Communication subsystem functionality			Possible multiple failures	Hazards
Loss of on board transmitting antenna functionality	Loss of on board receiving antenna functionality	Loss of On Board Communication Subsystem functionality		
0	0	0	-	Degradation or loss of rotor wing RPAS control Degradation or loss of telemetry receipt for rotor wing RPAS monitoring
0	6,05E-02	6,05E-02	-	
6,05E-02	0	6,05E-02	-	
6,05E-02	6,05E-02	1,1E-01	Loss of on board transmitting antenna functionality/ Loss of on board receiving antenna functionality	
Estimated probability of occurrence level, range:				C → B

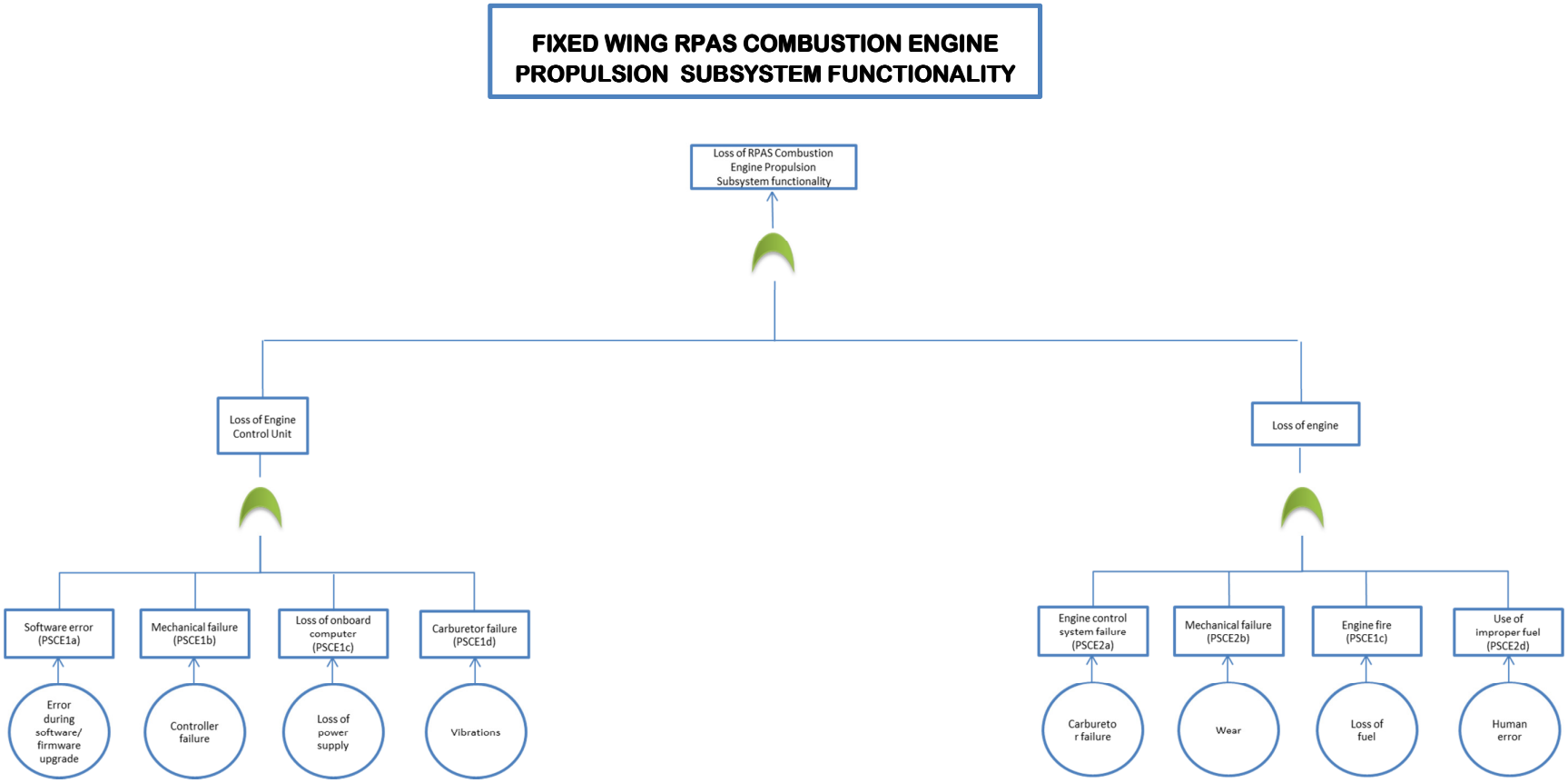


Figure 49 – Fixed Wing RPAS Combustion Engine Propulsion Subsystem functionality FTA

Table 106 – Fixed wing RPAS – Engine Control Unit single failures

Engine Control Unit single failure modes					Possible multiple failures	
Software error (PSCE1a)	Mechanical failure (PSCE1b)	Loss of on board computer (PSCE1c)	Carburetor failure (PSCE1d)	Loss of Engine Control Unit		
0	0	0	0	NO	-	-
0	0	0	5,5E-02	YES	-	-
0	0	1,0E-03	0	YES	-	-
0	0	1,0E-03	5,5E-02	YES	Loss of on board computer/ Carburetor failure	5,6E-02
0	1,5E-01	0	0	YES	-	-
0	1,5E-01	0	5,5E-02	YES	Mechanical failure/ Carburetor failure	2,05E-01
0	1,5E-01	1,0E-03	0	YES	Mechanical failure/ Loss of on board computer	1,51E-01
0	1,5E-01	1,0E-03	5,5E-02	YES	Mechanical failure/ Loss of on board computer/ Carburetor failure	2,06E-01
5,5E-03	0	0	0	YES	-	-
5,5E-03	0	0	5,5E-02	YES	Software error/ Carburetor failure	6,05E-02
5,5E-03	0	1,0E-03	0	YES	Software error/ Loss of on board computer	6,5E-03
5,5E-03	0	1,0E-03	5,5E-02	YES	Software error/ Loss of on board computer/ Carburetor failure	6,15E-02
5,5E-03	1,5E-01	0	0	YES	Software error/ Mechanical failure	1,555E-01
5,5E-03	1,5E-01	0	5,5E-02	YES	Software error/ Mechanical failure/ Carburetor failure	2,105E-01
5,5E-03	1,5E-01	1,0E-03	0	YES	Software error/ Mechanical failure/ Loss of on board computer	1,5E-01
5,5E-03	1,5E-01	1,0E-03	5,5E-02	YES	Software error/ Mechanical failure/ Loss of on board computer/ Carburetor failure	2,115E-01
Estimated probability of occurrence level, average value:						1,42E-01

Table 107 – Fixed wing RPAS – Engine single failures

Engine single failure modes					Possible multiple failures	
Engine control system failure (PSCE2a)	Mechanical failure (PSCE2b)	Engine fire (PSCE3c)	Use of improper fuel (PSCE2d)	Engine failure		
0	0	0	0	NO	-	-
0	0	0	5,5E-03	YES	-	-
0	0	5,5E-03	0	YES	-	-
0	0	5,5E-03	5,5E-03	YES	Engine fire/ Use of improper fuel	1,1E-02
0	5,5E-02	0	0	YES	-	-
0	5,5E-02	0	5,5E-03	YES	Mechanical failure/ Use of improper fuel	6,05E-02
0	5,5E-02	5,5E-03	0	YES	Mechanical failure/ Engine fire	6,05E-02
0	5,5E-02	5,5E-03	5,5E-03	YES	Mechanical failure/ Engine fire/ Use of improper fuel	6,6E-02
2,0E-01	0	0	0	YES	-	-
2,0E-01	0	0	5,5E-03	YES	Engine control system failure/ Use of improper fuel	2,055E-01
2,0E-01	0	5,5E-03	0	YES	Engine control system failure/ Engine fire	2,055E-01
2,0E-01	0	5,5E-03	5,5E-03	YES	Engine control system failure/ Engine fire/ Use of improper fuel	2,11E-01
2,0E-01	5,5E-02	0	0	YES	Engine control system failure/ Mechanical failure/	2,55E-01
2,0E-01	5,5E-02	0	5,5E-03	YES	Engine control system failure/ Mechanical failure/ Use of improper fuel	2,605E-01
2,0E-01	5,5E-02	5,5E-03	0	YES	Engine control system failure/ Mechanical failure/ Engine fire	2,605E-01
2,0E-01	5,5E-02	5,5E-03	5,5E-03	YES	Engine control system failure/ Mechanical failure/ Engine fire/ Use of improper fuel	2,66E-01
Estimated probability of occurrence level, average value:						1,69E-01

Table 108 – Fixed wing RPAS – Loss of Combustion Engine Propulsion Subsystem functionality

Loss of Combustion Engine Propulsion Subsystem functionality			Possible multiple failures	Hazards
Loss of Engine Control Unit	Loss of engine	Loss of Combustion Engine Propulsion Subsystem functionality		
0	0	0	-	Degradation or loss of fixed wing (jet) combustion engine RPAS propulsion functionality Degradation or loss of fixed wing (jet) combustion engine RPAS control Degradation or loss of fixed wing (jet) combustion engine RPAS manoeuvrability
0	1,69E-01	2,66E-01	-	
1,42E-01	0	2,115E-01	-	
1,42E-01	1,69E-01	4,775E-01	Loss of Engine Control Unit/ Loss of engine	
Estimated probability of occurrence level:				A

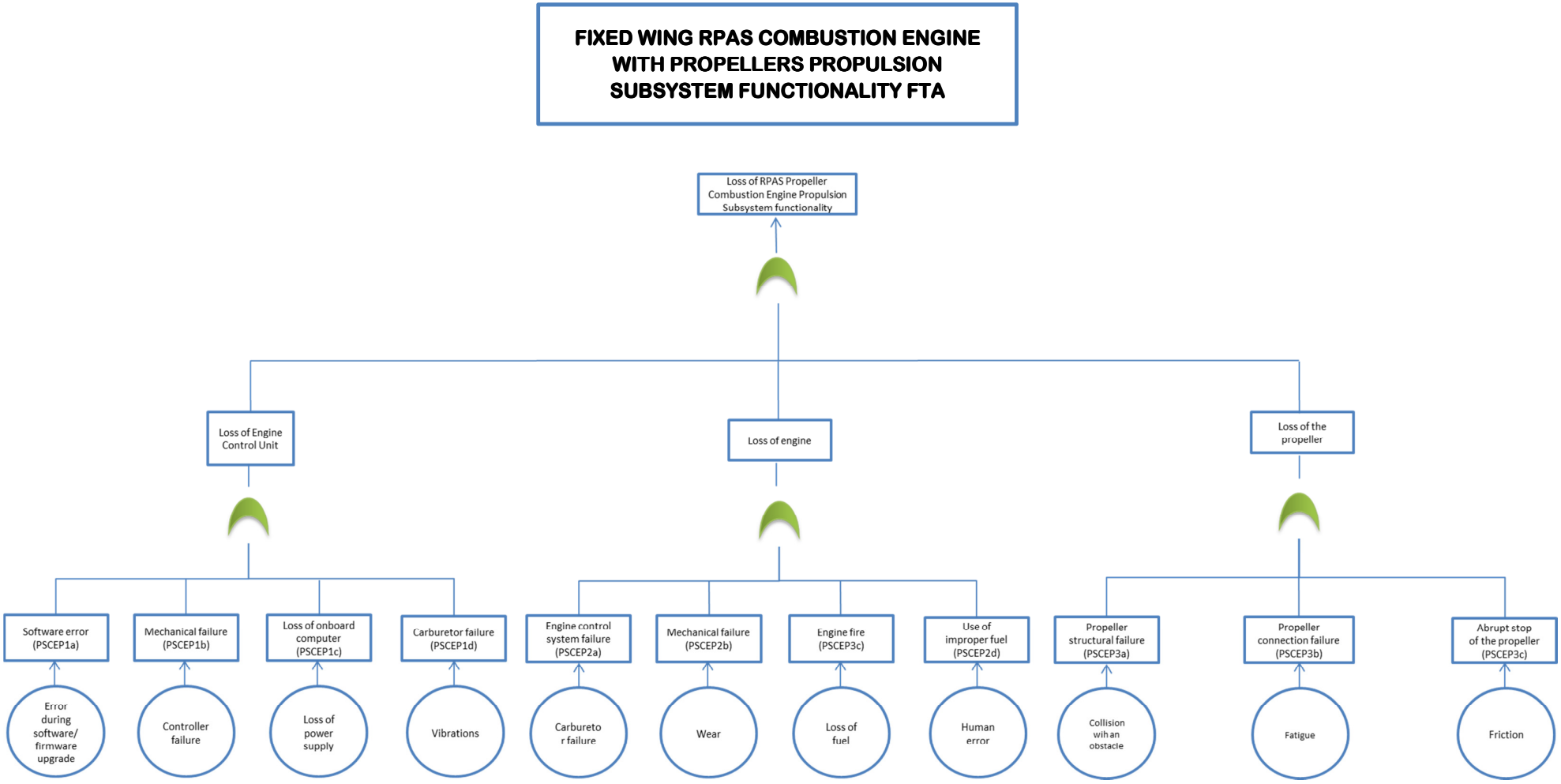


Figure 50 – Fixed wing RPAS Combustion Engine with Propellers Subsystem functionality FTA

Table 109 – Fixed wing RPAS – Engine Control Unit single failures

Engine Control Unit single failure modes					Possible multiple failures	
Software error (PSCEP1a)	Mechanical failure (PSCEP1b)	Loss of on board computer (PSCEP1c)	Carburetor failure (PSCEP1d)	Loss of Engine Control Unit		
0	0	0	0	NO	-	-
0	0	0	5,5E-02	YES	-	-
0	0	1,0E-03	0	YES	-	-
0	0	1,0E-03	5,5E-02	YES	Loss of on board computer/ Carburetor failure	5,6E-02
0	1,5E-01	0	0	YES	-	-
0	1,5E-01	0	5,5E-02	YES	Mechanical failure/ Carburetor failure	2,05E-01
0	1,5E-01	1,0E-03	0	YES	Mechanical failure/ Loss of on board computer	1,51E-01
0	1,5E-01	1,0E-03	5,5E-02	YES	Mechanical failure/ Loss of on board computer/ Carburetor failure	2,06E-01
5,5E-03	0	0	0	YES	-	-
5,5E-03	0	0	5,5E-02	YES	Software error/ Carburetor failure	6,05E-02
5,5E-03	0	1,0E-03	0	YES	Software error/ Loss of on board computer	6,5E-03
5,5E-03	0	1,0E-03	5,5E-02	YES	Software error/ Loss of on board computer/ Carburetor failure	6,15E-02
5,5E-03	1,5E-01	0	0	YES	Software error/ Mechanical failure	1,555E-01
5,5E-03	1,5E-01	0	5,5E-02	YES	Software error/ Mechanical failure/ Carburetor failure	2,105E-01
5,5E-03	1,5E-01	1,0E-03	0	YES	Software error/ Mechanical failure/ Loss of on board computer	1,5E-01
5,5E-03	1,5E-01	1,0E-03	5,5E-02	YES	Software error/ Mechanical failure/ Loss of on board computer/ Carburetor failure	2,115E-01
Estimated probability of occurrence level, average value:						1,42E-01

Table 110 – Fixed wing RPAS – Engine single failures

Engine single failure modes					Possible multiple failures	
Engine control system failure (PSCEP2a)	Mechanical failure (PSCEP2b)	Engine fire (PSCEP3c)	Use of improper fuel (PSCEP2d)	Engine failure		
0	0	0	0	NO	-	-
0	0	0	5,5E-03	YES	-	-
0	0	5,5E-03	0	YES	-	-
0	0	5,5E-03	5,5E-03	YES	Engine fire/ Use of improper fuel	1,1E-02
0	5,5E-02	0	0	YES	-	-
0	5,5E-02	0	5,5E-03	YES	Mechanical failure/ Use of improper fuel	6,05E-02
0	5,5E-02	5,5E-03	0	YES	Mechanical failure/ Engine fire	6,05E-02
0	5,5E-02	5,5E-03	5,5E-03	YES	Mechanical failure/ Engine fire/ Use of improper fuel	6,6E-02
2,0E-01	0	0	0	YES	-	-
2,0E-01	0	0	5,5E-03	YES	Engine control system failure/ Use of improper fuel	2,055E-01
2,0E-01	0	5,5E-03	0	YES	Engine control system failure/ Engine fire	2,055E-01
2,0E-01	0	5,5E-03	5,5E-03	YES	Engine control system failure/ Engine fire/ Use of improper fuel	2,11E-01
2,0E-01	5,5E-02	0	0	YES	Engine control system failure/ Mechanical failure/	2,55E-01
2,0E-01	5,5E-02	0	5,5E-03	YES	Engine control system failure/ Mechanical failure/ Use of improper fuel	2,605E-01
2,0E-01	5,5E-02	5,5E-03	0	YES	Engine control system failure/ Mechanical failure/ Engine fire	2,605E-01
2,0E-01	5,5E-02	5,5E-03	5,5E-03	YES	Engine control system failure/ Mechanical failure/ Engine fire/ Use of improper fuel	2,66E-01
Estimated probability of occurrence level, average value:						1,69E-01

Table 111 – Fixed wing RPAS – Loss of the propeller

Propeller single failure modes				Possible multiple failures	
Propeller structural failure (PSCEP3a)	Propeller connection failure (PSCEP3b)	Abrupt stop of the propeller (PSCEP3c)	Loss of the propeller		
0	0	0	NO	-	-
0	0	1,0E-01	YES	-	-
0	5,5E-03	0	YES	-	-
0	5,5E-03	1,0E-01	YES	Propeller connection failure/ Abrupt stop of the propeller	1,06E-01
1,0E-01	0	0	YES	-	-
1,0E-01	0	1,0E-01	YES	Propeller structural failure/ Abrupt stop of the propeller	2,00E-01
1,0E-01	5,5E-03	0	YES	Propeller structural failure/ Propeller connection failure	1,06E-01
1,0E-01	5,5E-03	1,0E-01	YES	Propeller structural failure/ Propeller connection failure/ Abrupt stop of the propeller	2,06E-01
Estimated probability of occurrence level, average value:					1,55E-01

Table 112 – Fixed wing RPAS – Loss of Combustion Engine with Propellers Propulsion Subsystem functionality

Loss of Propeller Combustion Engine Propulsion Subsystem functionality				Possible multiple failures	Hazards
Loss of Engine Control Unit	Loss of engine	Loss of the propeller	Loss of Combustion Engine Propulsion Subsystem functionality		
0	0	0	0	-	Degradation or loss of fixed wing combustion engine with propeller RPAS propulsion functionality Degradation or loss of fixed wing combustion engine with propeller RPAS control Degradation or loss of fixed wing combustion engine with propeller RPAS manoeuvrability
0	0	1,55E-01	1,55E-01	-	
0	1,69E-01	0	1,69E-01	-	
0	1,69E-01	1,55E-01	3,24E-01	Loss of the engine/ Loss of the propeller	
1,42E-01	0	0	1,42E-01	-	
1,42E-01	0	1,55E-01	2,97E-01	Loss of the Engine Control Unit/Loss of the propeller	
1,42E-01	1,69E-01	0	3,1E-01	Loss of the Engine Control Unit/Loss of the engine	
1,42E-01	1,69E-01	1,55E-01	4,66E-01	Loss of the Engine Control Unit/Loss of the engine/Loss of the propeller	
Estimated probability of occurrence level:					A

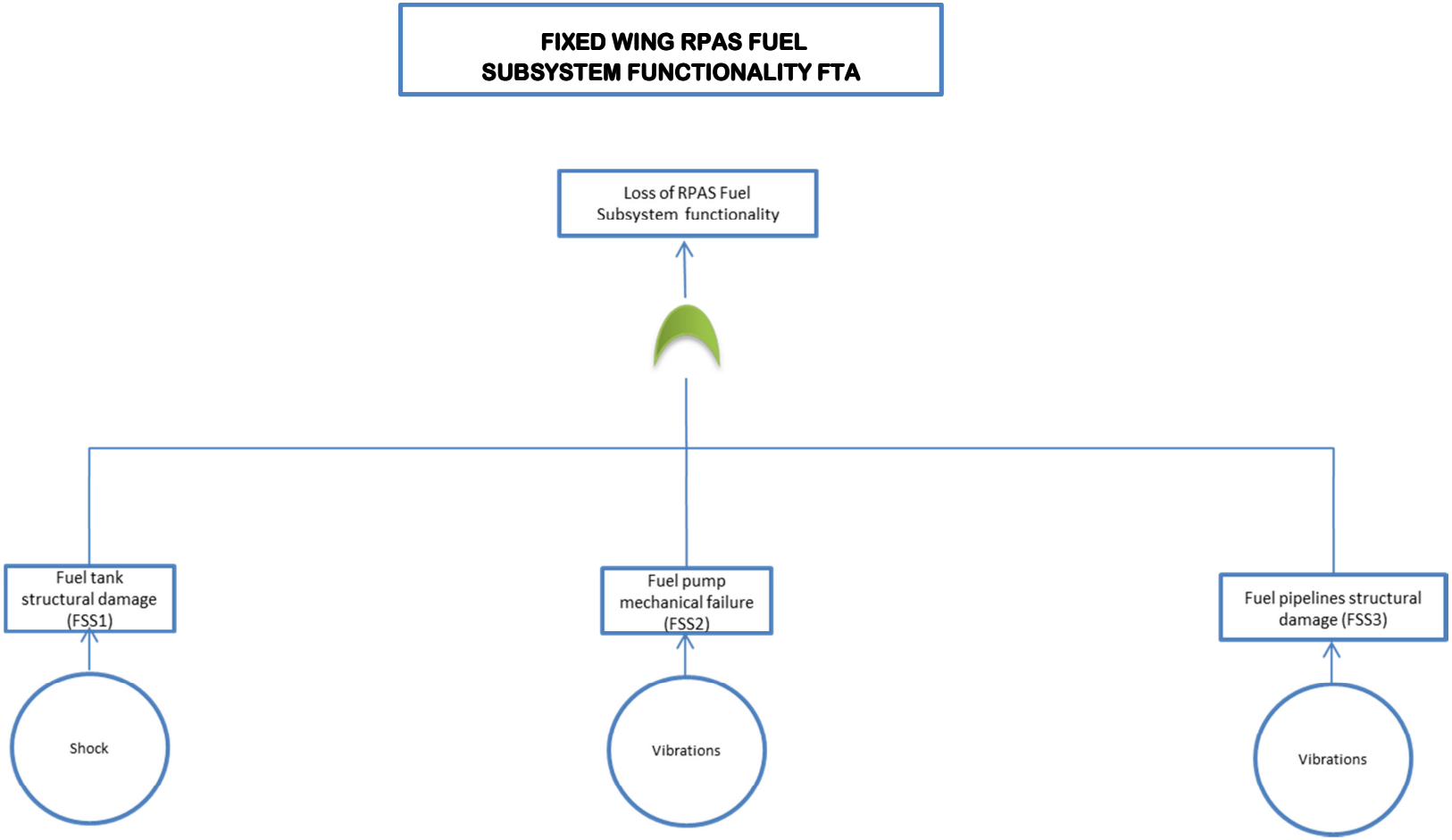


Figure 51 – Fixed wing RPAS Fuel Subsystem functionality FTA

Table 113 – Fixed wing RPAS – Loss of Fuel Subsystem functionality

Loss of RPAS Fuel Subsystem functionality				Possible multiple failures	Hazards
Fuel tank structural damage (FSS1)	Fuel pump mechanical failure (FSS2)	Fuel pipelines structural damage (FSS3)	Loss of RPAS Fuel Subsystem functionality		
0	0	0	0	-	Degradation or loss of fixed wing RPAS fuel subsystem functionality Degradation or loss of fixed wing RPAS propulsion Degradation or loss of fixed wing RPAS control Fire on board fixed wing RPAS
0	0	1,0E-03	1,0E-03	-	
0	5,5E-03	0	5,5E-03	-	
0	5,5E-03	1,0E-03	6,5E-03	Fuel pump mechanical failure/ Fuel pipelines structural damage	
5,5E-03	0	0	5,5E-03	-	
5,5E-03	0	1,0E-03	6,5E-03	Fuel tank structural damage/Fuel pipelines structural damage	
5,5E-03	5,5E-03	0	1,1E-02	Fuel tank structural damage/Fuel pump mechanical failure	
5,5E-03	5,5E-03	1,0E-03	1,2E-02	Fuel tank structural damage/ Fuel pump mechanical failure/Fuel pipelines structural damage	
Estimated probability of occurrence level range					D → B

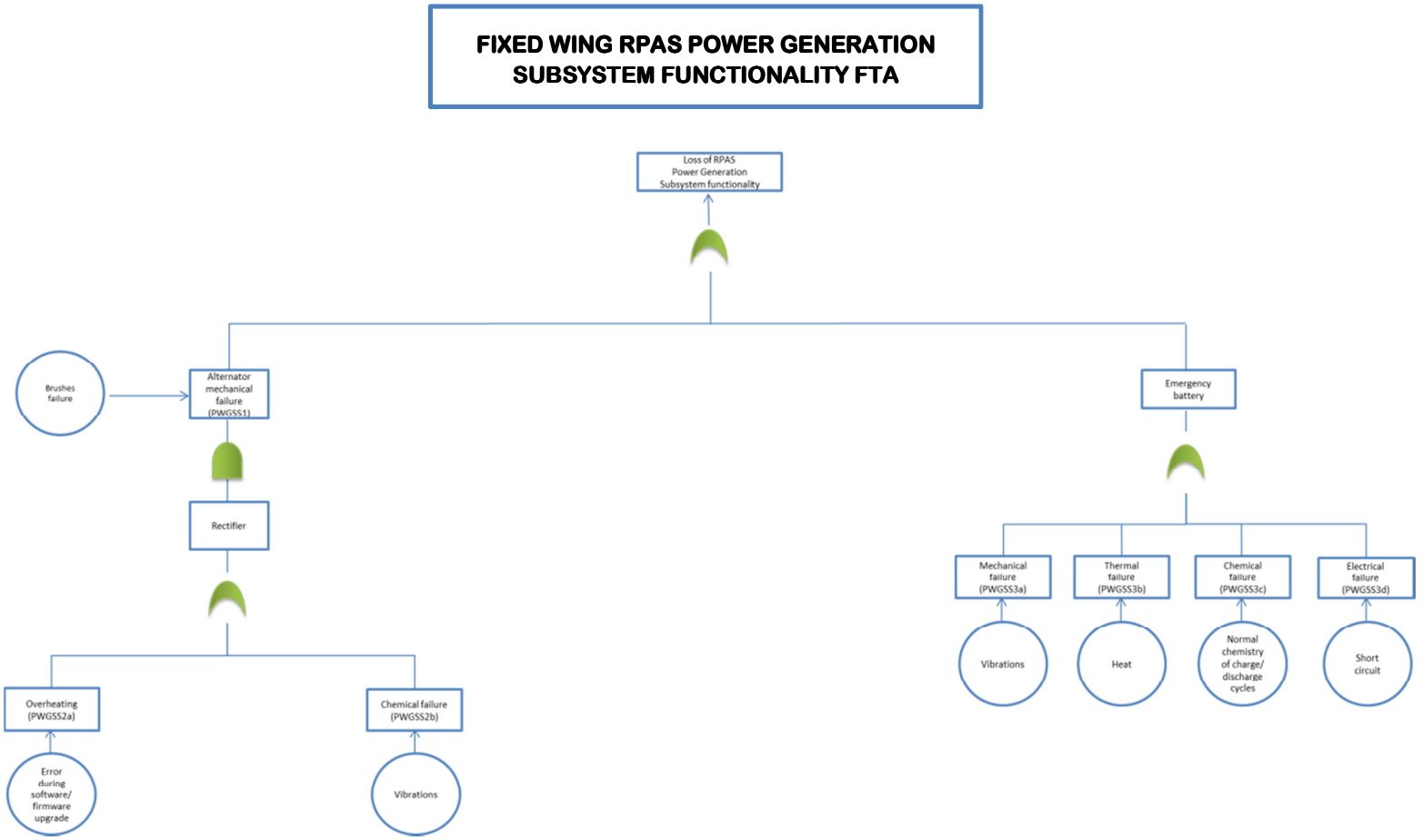


Figure 52 – Power Generation Subsystem functionality FTA

Table 114 – Fixed wing RPAS – Loss of the rectifier

Rectifier single failure modes			Possible multiple failures	
Overheating (PWGSS2a)	Chemical failure (PWGSS2b)	Loss of the rectifier		
0	0	NO	-	-
0	5,5E-03	YES	-	-
5,5E-03	0	YES	-	-
5,5E-03	5,5E-03	YES	Overheating/ Chemical failure	1,1E-02
Estimated probability of occurrence level, average value:				1,1E-02

Table 115 – Fixed wing RPAS – Loss of alternate current generation functionality

Loss of alternate current generation functionality			Possible multiple failures	
Alternator mechanical failure (PWGSS1)	Loss of the rectifier	Loss of alternate current generation functionality		
0	0	NO	-	-
0	1,1E-02	YES	-	-
1,1E-02	0	YES	-	-
1,1E-02	1,1E-02	YES	Alternator mechanical failure/ Loss of the rectifier	2,2E-02
Estimated probability of occurrence level, average value:				2,2E-02

Table 116 – Fixed wing RPAS – Loss of emergency battery

Emergency battery single failure modes					Possible multiple failures	
Mechanical failure (PWGSS3a)	Thermal failure (PWGSS3b)	Chemical failure (PWGSS3c)	Electrical failure (PWGSS3d)	Loss of emergency battery		
0	0	0	0	NO	-	-
0	0	0	5,5E-02	YES	-	-
0	0	5,5E-02	0	YES	-	-
0	0	5,5E-02	5,5E-02	YES	Mechanical failure/ Thermal failure/ Chemical failure/ Electrical failure	1,1E-01
0	5,5E-02	0	0	YES	-	-
0	5,5E-02	0	5,5E-02	YES	Mechanical failure/ Thermal failure/ Chemical failure/ Electrical failure	1,1E-01
0	5,5E-02	5,5E-02	0	YES	Mechanical failure/ Thermal failure/ Chemical failure/ Electrical failure	1,1E-01
0	5,5E-02	5,5E-02	5,5E-02	YES	Mechanical failure/ Thermal failure/ Chemical failure/ Electrical failure	1,65E-01
5,5E-02	0	0	0	YES	-	-
5,5E-02	0	0	5,5E-02	YES	Mechanical failure/ Thermal failure/ Chemical failure/ Electrical failure	1,1E-01
5,5E-02	0	5,5E-02	0	YES	Mechanical failure/ Thermal failure/ Chemical failure/ Electrical failure	1,1E-01
5,5E-02	0	5,5E-02	5,5E-02	YES	Mechanical failure/ Thermal failure/ Chemical failure/ Electrical failure	1,65E-01
5,5E-02	5,5E-02	0	0	YES	Mechanical failure/ Thermal failure/ Chemical failure/ Electrical failure	1,1E-01
5,5E-02	5,5E-02	0	5,5E-02	YES	Mechanical failure/ Thermal failure/ Chemical failure/ Electrical failure	1,65E-01
5,5E-02	5,5E-02	5,5E-02	0	YES	Mechanical failure/ Thermal failure/ Chemical failure/ Electrical failure	1,65E-01
5,5E-02	5,5E-02	5,5E-02	5,5E-02	YES	Mechanical failure/ Thermal failure/ Chemical failure/ Electrical failure Use of improper fuel	2,2E-01
Estimated probability of occurrence level, average value:						1,4E-01

Table 117 – Fixed wing RPAS – Loss of Power Generation Subsystem functionality				
Loss of Power Generation Subsystem functionality			Possible multiple failures	Hazards
Loss of alternate current generation functionality	Loss of emergency battery	Loss of Power Generation Subsystem functionality		
0	0	0	-	Degradation or loss of fixed wing RPAS power functionality
0	1,4E-01	1,40E-01	-	
2,2E-02	0	2,2E-02	-	
2,2E-02	1,4E-01	1,62E-01	Loss of alternate current generation functionality/ Loss of emergency battery	
Estimated probability of occurrence level, range:				B → A

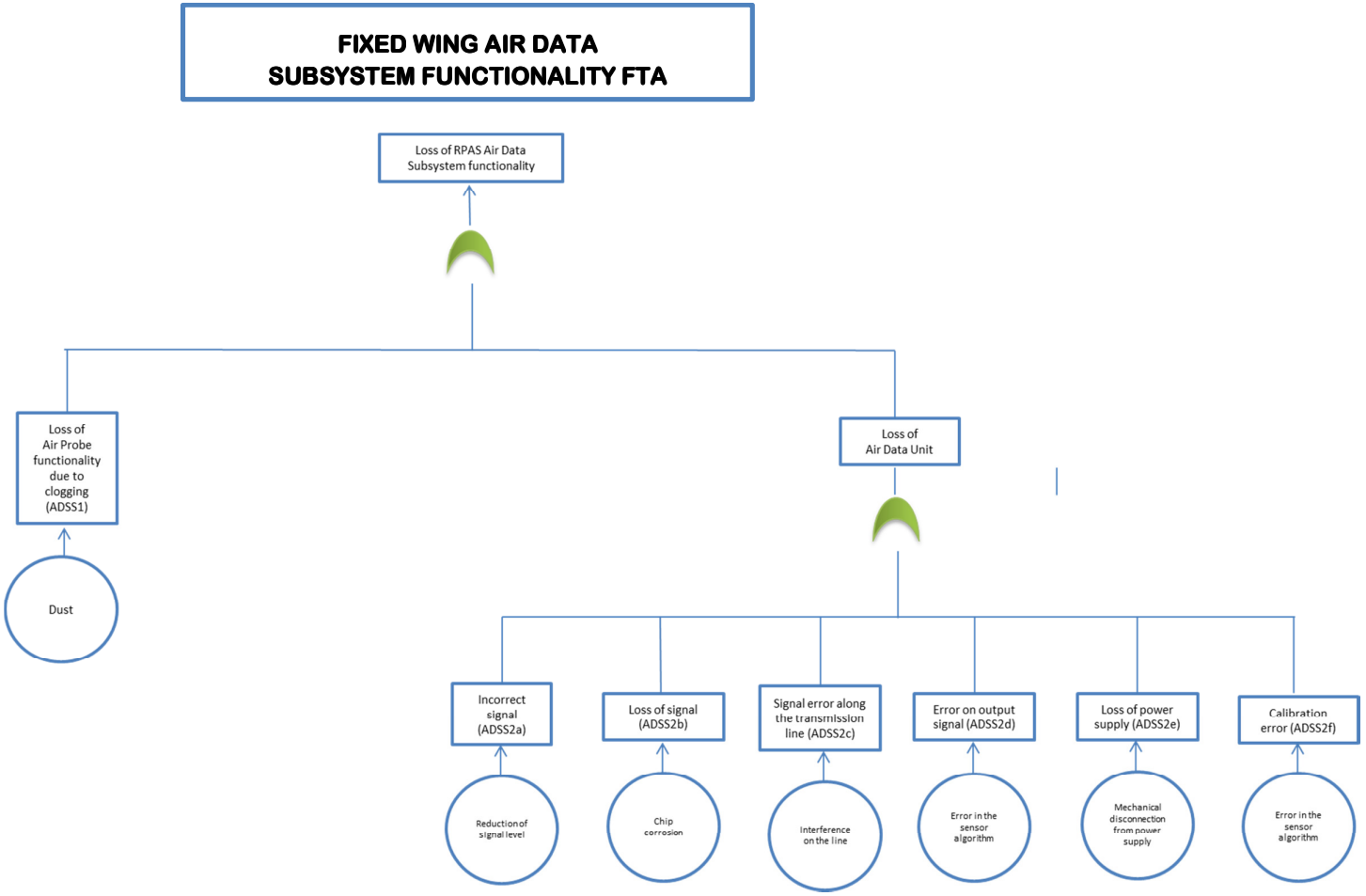


Figure 53 – Fixed wing RPAS Air Data Subsystem functionality FTA

Table 118 – Rotor wing RPAS - Loss of Air Data Unit

Loss of RPAS Air Data Unit							Possible multiple failures	
Incorrect signal (ADSS2a)	Loss of signal (ADSS2b)	Signal error along the transmission line (ADSS2c)	Error on output signal (ADSS2d)	Loss of power supply (ADSS2e)	Calibration error (ADSS2f)	Loss of Air Data Unit		
0	0	0	0	0	0	NO	-	0
0	0	0	0	0	5,5E-02	YES	-	5,5E-02
0	0	0	0	2,0E-01	0	YES	-	2,0E-01
0	0	0	0	2,0E-01	5,5E-02	YES	Loss of power supply/Calibration error	2,55E-01
0	0	0	5,5E-02	0	0	YES	-	5,5E-02
0	0	0	5,5E-02	0	5,5E-02	YES	Error on output signal/ Calibration error	1,1E-01
0	0	0	5,5E-02	2,0E-01	0	YES	Error on output signal/Loss of power supply	2,55E-01
0	0	0	5,5E-02	2,0E-01	5,5E-02	YES	Error on output signal/Loss of power supply/Calibration error	3,1E-01
0	0	5,5E-02	0	0	0	YES	-	5,5E-02
0	0	5,5E-02	0	0	5,5E-02	YES	Signal error along the transmission line/ Calibration error	1,1E-01
0	0	5,5E-02	0	2,0E-01	0	YES	Signal error along the transmission line/Calibration error	2,55E-01
0	0	5,5E-02	0	2,0E-01	5,5E-02	YES	Signal error along the transmission line/ Loss of power supply/Calibration error	3,1E-01
0	0	5,5E-02	5,5E-02	0	0	YES	Signal error along the transmission line/Error on output signal	1,1E-01
0	0	5,5E-02	5,5E-02	0	5,5E-02	YES	Signal error along the transmission line/Error on output signal/Calibration error	1,65E-01
0	0	5,5E-02	5,5E-02	2,0E-01	0	YES	Signal error along the transmission line/Error on output signal/Loss of power supply	3,1E-01
0	0	5,5E-02	5,5E-02	2,0E-01	5,5E-02	YES	Signal error along the transmission line/Error on output signal/ Loss of power supply/Calibration error	3,65E-01
0	2,0E-01	0	0	0	0	YES	-	2,0E-01
0	2,0E-01	0	0	0	5,5E-02	YES	Loss of signal/ Calibration error	2,55E-01
0	2,0E-01	0	0	2,0E-01	0	YES	Loss of signal/Loss of power supply	4,0E-01
0	2,0E-01	0	0	2,0E-01	5,5E-02	YES	Loss of signal/ Loss of power supply/Calibration error	4,55E-01
0	2,0E-01	0	5,5E-02	0	0	YES	Loss of signal/Error on output signal	2,55E-01
0	2,0E-01	0	5,5E-02	0	5,5E-02	YES	Loss of signal/Error on output signal/ Calibration error	3,1E-01
0	2,0E-01	0	5,5E-02	2,0E-01	0	YES	Loss of signal/Error on output signal/Loss of power supply	4,55E-01
0	2,0E-01	0	5,5E-02	2,0E-01	5,5E-02	YES	Loss of signal/Error on output signal/ Loss of power supply/Calibration error	5,1E-01

Table 118 – Rotor wing RPAS - Loss of Air Data Unit (Cont'd)

Loss of RPAS Air Data Unit							Possible multiple failures	
Incorrect signal (ADSS2a)	Loss of signal (ADSS2b)	Signal error along the transmission line (ADSS2c)	Error on output signal (ADSS2d)	Loss of power supply (ADSS2e)	Calibration error (ADSS2f)	Loss of Air Data Unit		
0	2,0E-01	5,5E-02	0	0	0	YES	Loss of signal/Signal error along the transmission line	2,55E-01
0	2,0E-01	5,5E-02	0	0	5,5E-02	YES	Loss of signal/Signal error along the transmission line/ Calibration error	3,1E-01
0	2,0E-01	5,5E-02	0	2,0E-01	0	YES	Loss of signal/Signal error along the transmission line/ Loss of power supply	4,55E-01
0	2,0E-01	5,5E-02	0	2,0E-01	5,5E-02	YES	Loss of signal/Signal error along the transmission line/ Loss of power supply/Calibration error	5,1E-01
0	2,0E-01	5,5E-02	5,5E-02	0	0	YES	Loss of signal/Signal error along the transmission line/Error on output signal	3,1E-01
0	2,0E-01	5,5E-02	5,5E-02	0	5,5E-02	YES	Loss of signal/Signal error along the transmission line/ Error on output signal/Calibration error	3,65E-01
0	2,0E-01	5,5E-02	5,5E-02	2,0E-01	0	YES	Loss of signal/Signal error along the transmission line/Error on output signal/Loss of power supply	5,1E-01
0	2,0E-01	5,5E-02	5,5E-02	2,0E-01	5,5E-02	YES	Loss of signal/Signal error along the transmission line/Error on output signal/ Loss of power supply/Calibration error	5,65E-01
2,0E-01	0	0	0	0	0	YES	-	2,0E-01
2,0E-01	0	0	0	0	5,5E-02	YES	Incorrect signal/ Calibration error	2,55E-01
2,0E-01	0	0	0	2,0E-01	0	YES	Incorrect signal/ Loss of power supply	4,0E-01
2,0E-01	0	0	0	2,0E-01	5,5E-02	YES	Incorrect signal/ Loss of power supply/Calibration error	4,55E-01
2,0E-01	0	0	5,5E-02	0	0	YES	Incorrect signal/Error on output signal	2,55E-01
2,0E-01	0	0	5,5E-02	0	5,5E-02	YES	Incorrect signal/Error on output signal/ Calibration error	3,1E-01
2,0E-01	0	0	5,5E-02	2,0E-01	0	YES	Incorrect signal/Error on output signal/Loss of power supply	4,55E-01
2,0E-01	0	0	5,5E-02	2,0E-01	5,5E-02	YES	Incorrect signal/Error on output signal/ Loss of power supply/Calibration error	5,1E-01
2,0E-01	0	5,5E-02	0	0	0	YES	Incorrect signal/Signal error along the transmission line	2,55E-01
2,0E-01	0	5,5E-02	0	0	5,5E-02	YES	Incorrect signal/Signal error along the transmission line/ Calibration error	3,1E-01

Table 118 – Rotor wing RPAS - Loss of Air Data Unit (Cont'd)

Loss of RPAS Air Data Unit							Possible multiple failures	
Incorrect signal (ADSS2a)	Loss of signal (ADSS2b)	Signal error along the transmission line (ADSS2c)	Error on output signal (ADSS2d)	Loss of power supply (ADSS2e)	Calibration error (ADSS2f)	Loss of Air Data Unit		
2,0E-01	0	5,5E-02	0	2,0E-01	0	YES	Incorrect signal/Signal error along the transmission line/ Loss of power supply	4,55E-01
2,0E-01	0	5,5E-02	0	2,0E-01	5,5E-02	YES	Incorrect signal/Signal error along the transmission line/ Loss of power supply/Calibration error	5,1E-01
2,0E-01	0	5,5E-02	5,5E-02	0	0	YES	Incorrect signal/Signal error along the transmission line/ Calibration error	3,1E-01
2,0E-01	0	5,5E-02	5,5E-02	0	5,5E-02	YES	Incorrect signal/Signal error along the transmission line/Error on output signal/ Calibration error	3,65E-01
2,0E-01	0	5,5E-02	5,5E-02	2,0E-01	0	YES	Incorrect signal/Signal error along the transmission line/Error on output signal/Loss of power supply	5,1E-01
2,0E-01	0	5,5E-02	5,5E-02	2,0E-01	5,5E-02	YES	Incorrect signal/Signal error along the transmission line/Error on output signal/ Loss of power supply/Calibration error	5,65E-01
2,0E-01	2,0E-01	0	0	0	0	YES	Incorrect signal/ Loss of signal	4,0E-01
2,0E-01	2,0E-01	0	0	0	5,5E-02	YES	Incorrect signal/Loss of signal/Calibration error	4,55E-01
2,0E-01	2,0E-01	0	0	2,0E-01	0	YES	Incorrect signal/Loss of signal/Loss of power supply	6,0E-01
2,0E-01	2,0E-01	0	0	2,0E-01	5,5E-02	YES	Incorrect signal/Loss of signal/Loss of power supply/Calibration error	6,55E-01
2,0E-01	2,0E-01	0	5,5E-02	0	0	YES	Incorrect signal/Loss of signal/Error on output signal	4,55E-01
2,0E-01	2,0E-01	0	5,5E-02	0	5,5E-02	YES	Incorrect signal/Loss of signal/Error on output signal/Calibration error	5,1E-01
2,0E-01	2,0E-01	0	5,5E-02	2,0E-01	0	YES	Incorrect signal/Loss of signal/Error on output signal/Loss of power supply	6,55E-01
2,0E-01	2,0E-01	0	5,5E-02	2,0E-01	5,5E-02	YES	Incorrect signal/Loss of signal/Error on output signal/Loss of power supply/Calibration error	7,1E-01
2,0E-01	2,0E-01	5,5E-02	0	0	0	YES	Incorrect signal/Loss of signal/Signal error along the transmission line	4,55E-01
2,0E-01	2,0E-01	5,5E-02	0	0	5,5E-02	YES	Incorrect signal/Loss of signal/Signal error along the transmission line/ Calibration error	5,1E-01
2,0E-01	2,0E-01	5,5E-02	0	2,0E-01	0	YES	Incorrect signal/Loss of signal/Signal error along the transmission line/ Loss of power supply	6,55E-01

Table 118 – Rotor wing RPAS - Loss of Air Data Unit (Cont'd)								
Loss of RPAS Air Data Unit							Possible multiple failures	Hazards
Incorrect signal (ADSS2a)	Loss of signal (ADSS2b)	Signal error along the transmission line (ADSS2c)	Error on output signal (ADSS2d)	Loss of power supply (ADSS2e)	Calibration error (ADSS2f)	Loss of Air Data Unit		
2,0E-01	2,0E-01	5,5E-02	0	2,0E-01	5,5E-02	YES	Incorrect signal/Loss of signal/Signal error along the transmission line/ Loss of power supply/Calibration error	7,1E-01
2,0E-01	2,0E-01	5,5E-02	5,5E-02	0	0	YES	Incorrect signal/Loss of signal/Signal error along the transmission line/Error on output signal	5,1E-01
2,0E-01	2,0E-01	5,5E-02	5,5E-02	0	5,5E-02	YES	Incorrect signal/Loss of signal/Signal error along the transmission line/Error on output signal/Calibration error	5,65E-01
2,0E-01	2,0E-01	5,5E-02	5,5E-02	2,0E-01	0	YES	Incorrect signal/Loss of signal/Signal error along the transmission line/Error on output signal/Loss of power supply	7,1E-01
2,0E-01	2,0E-01	5,5E-02	5,5E-02	2,0E-01	5,5E-02	YES	Incorrect signal/Loss of signal/Signal error along the transmission line/Error on output signal/Loss of power supply/Calibration error	7,65E-01
Estimated probability of occurrence level, average value:								3,83-01

Table 119 – Fixed wing RPAS – Loss of Air Data Subsystem functionality				
Loss of Air Data Subsystem functionality			Possible multiple failures	Hazards
Loss of Air Probe	Loss of Air Data Unit	Loss of Power Generation Subsystem functionality		
0	0	0	-	Fixed wing RPAS pressure sensors failure Fixed wing RPAS misleading altitude indication Fixed wing RPAS misleading airspeed indication Fixed wing RPAS misleading angle of attack indication Fixed wing RPAS misleading stall warning Fixed wing RPAS stall Fixed wing RPAS degradation or loss of flight attitude control
0	1,1E-01	1,1E-01	-	
3,83E-01	0	3,83E-01	-	
3,83E-01	1,1E-01	4,93E-01	Loss of alternate current generation functionality/ Loss of emergency battery	
Estimated probability of occurrence level, range:				B → A

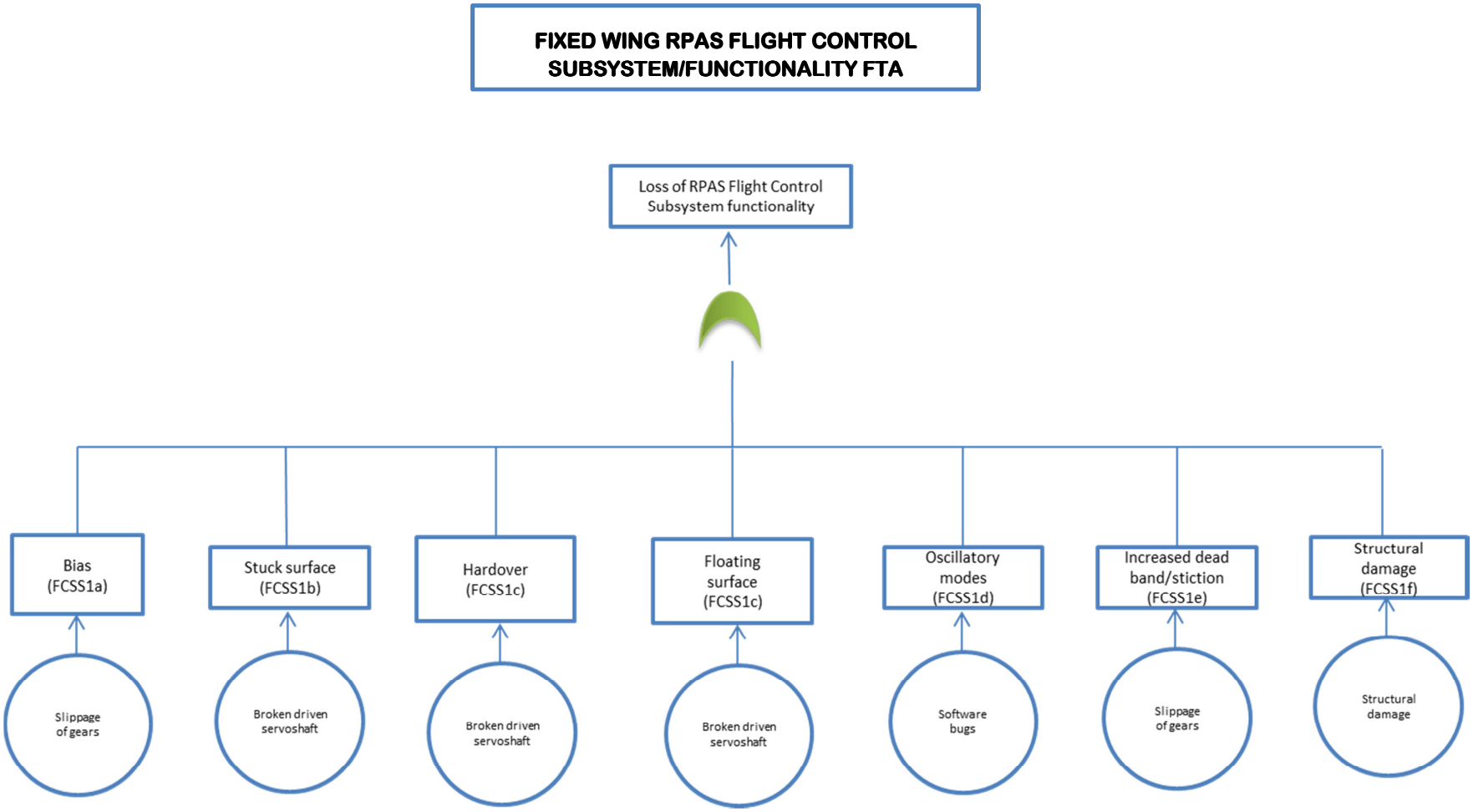


Figure 54 – Flight Control Subsystem/Functionality FTA

Table 120 – Fixed wing RPAS – Loss of Flight Control Subsystem functionality

Loss of RPAS Flight Control Subsystem functionality			Possible multiple failures	Hazards
Bias (FCSS1a)	Floating surface (FCSS1d)	Loss of RPAS Flight Control Subsystem functionality		
0	0	0	-	Degradation or loss of fixed wing RPAS flight control Degradation or loss of fixed wing RPAS manoeuvrability
0	5,5E-02	5,5E-02	-	
5,5E-02	0	5,5E-02	-	
5,5E-02	5,5E-02	1,1E-01	Oscillatory modes/ Increased deadband/stiction	
Estimated probability of occurrence level range				C → B

Note: due to the number of identified failure modes for RPAS Control Subsystem (seven different failure modes), the failure modes with higher criticality (Table 59) have been considered only to avoid the use of more sophisticated techniques to solve truth tables composed of more than four variables (like 'Karnaugh Maps', for example). This choice has been performed considering that more complicated issues do not provide valuable added value to the safety analysis object of this research work.

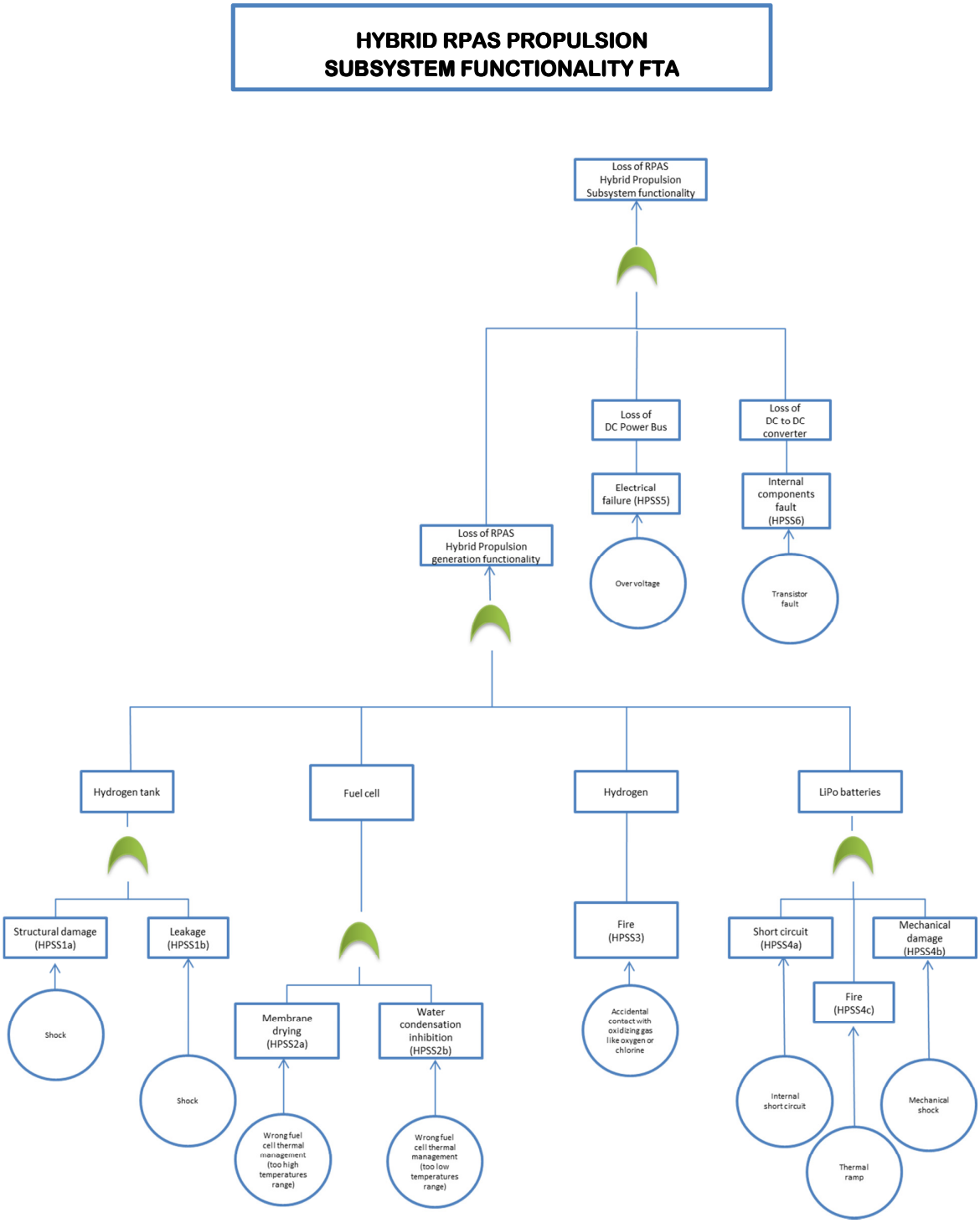


Figure 55 – RPAS Hybrid Propulsion Subsystem functionality FTA

Table 121 – Hybrid RPAS – Hydrogen tank multiple failures				
Hydrogen tank single failure modes			Possible multiple failures	
Structural damage (HPSS1a)	Leakage (HPSS1b)	Loss of hydrogen tank		
0	0	NO	-	-
0	5,5E-03	YES	-	-
5,5E-03	0	YES	-	-
5,5E-03	5,5E-03	YES	Structural damage/Leakage	1,1E-02
Estimated probability of occurrence level, average value:				1,1E-02

Table 122 – Hybrid RPAS – Fuel cell multiple failures				
Ground emergency battery single failure modes			Possible multiple failures	
Membrane drying (HPSS2a)	Water condensation inhibition (HPSS2b)	Loss of Fuel Cells functionality		
0	0	NO	-	-
0	5,5E-03	YES	-	-
5,5E-03	0	YES	-	-
5,5E-03	5,5E-03	YES	Membrane drying/ Water condensation inhibition	2,0E-03
Estimated probability of occurrence level, average value:				2,0E-03

Table 123 – Hybrid RPAS – LiPo batteries multiple failures					
LiPo batteries single failure modes				Possible multiple failures	
Short circuit (PWSS1)	Mechanical damage (PWSS2)	Fire (PWSS3)	Loss of LiPo batteries functionality		
0	0	0	NO	-	0
0	0	5,5E-02	YES	-	5,5E-02
0	5,5E-02	0	YES	-	5,5E-02
0	5,5E-02	5,5E-02	YES	Mechanical damage/Fire	1,1E-01
5,5E-02	0	0	YES	-	5,5E-02
5,5E-02	0	5,5E-02	YES	Short circuit/Fire	1,1E-01
5,5E-02	5,5E-02	0	YES	Short circuit/ Mechanical damage	1,1E-01
5,5E-02	5,5E-02	5,5E-02	YES	Short circuit/ Mechanical damage/ Fire	1,65E-01
Estimated probability of occurrence level, average value:					2,0E-03

Table 124 – Hybrid RPAS – Loss of Hybrid Power Generation functionality

Loss of Hybrid Power Generation functionality					Possible multiple failures	Hazards
Loss of hydrogen tank	Loss of Fuel Cells functionality	Hydrogen fire	Loss of LiPo batteries functionality	Loss of Hybrid Propulsion Generation functionality		
0	0	0	0	NO	-	0
0	0	0	2,0E-03	YES	-	2,0E-03
0	0	5,5E-02	0	YES	-	5,5E-02
0	0	5,5E-02	2,0E-03	YES	Hydrogen fire/ Loss of LiPo batteries functionality	5,7E-02
0	2,0E-03	0	0	YES	-	2,0E-03
0	2,0E-03	0	2,0E-03	YES	Loss of Fuel Cells functionality/ Loss of LiPo batteries functionality	4,0E-03
0	2,0E-03	5,5E-02	0	YES	Loss of Fuel Cells functionality/ Hydrogen fire	5,7E-02
0	2,0E-03	5,5E-02	2,0E-03	YES	Loss of Fuel Cells functionality/ Hydrogen fire/ Loss of LiPo batteries functionality	5,9E-02
1,1E-02	0	0	0	YES	-	1,1E-02
1,1E-02	0	0	2,0E-03	YES	Loss of hydrogen tank/ Loss of LiPo batteries functionality	1,3E-02
1,1E-02	0	5,5E-02	0	YES	Loss of hydrogen tank/ Hydrogen fire	6,6E-02
1,1E-02	0	5,5E-02	2,0E-03	YES	Loss of hydrogen tank/ Loss of LiPo batteries functionality/ Loss of LiPo batteries functionality	6,8E-02
1,1E-02	2,0E-03	0	0	YES	Loss of hydrogen tank/ Loss of Fuel Cells functionality	1,3E-02
1,1E-02	2,0E-03	0	2,0E-03	YES	Loss of hydrogen tank/ Loss of Fuel Cells functionality/ Loss of LiPo batteries functionality	1,5E-02
1,1E-02	2,0E-03	5,5E-02	0	YES	Loss of hydrogen tank/ Loss of Fuel Cells functionality/ Hydrogen fire	6,8E-02
1,1E-02	2,0E-03	5,5E-02	2,0E-03	YES	Loss of hydrogen tank/ Loss of Fuel Cells functionality/ Hydrogen fire/ Loss of LiPo batteries functionality	7,0E-02
Estimated probability of occurrence level, average value:						3,5E-02

Table 125 – Hybrid RPAS – Loss of Hybrid Propulsion Subsystem functionality

Loss of Hybrid Propulsion Subsystem functionality				Possible multiple failures	
Loss of Hybrid Propulsion Generation functionality	Loss of DC Power bus	Loss of DC to DC Converter	Loss of Hybrid Propulsion Subsystem functionality		
0	0	0	0	-	Loss of Hybrid Propulsion Subsystem functionality Loss of Hybrid Power Generation functionality Fire on board hybrid RPAS
0	0	5,5E-02	5,5E-02	-	
0	5,5E-02	0	5,5E-02	-	
0	5,5E-02	5,5E-02	1,1E-01	Loss of DC Power bus/ Loss of DC to DC Converter	
3,5E-02	0	0	3,50E-02	-	
3,5E-02	0	5,5E-02	9,0E-02	Loss of Hybrid Propulsion Generation functionality/ Loss of DC to DC Converter	
3,5E-02	5,5E-02	0	9,0E-02	Loss of Hybrid Propulsion Generation functionality/ Loss of DC Power bus	
3,5E-02	5,5E-02	5,5E-02	1,45E-01	Loss of Hybrid Propulsion Generation functionality/Loss of DC Power bus/Loss of DC to DC Converter	
Estimated probability of occurrence level, range value:					C → B

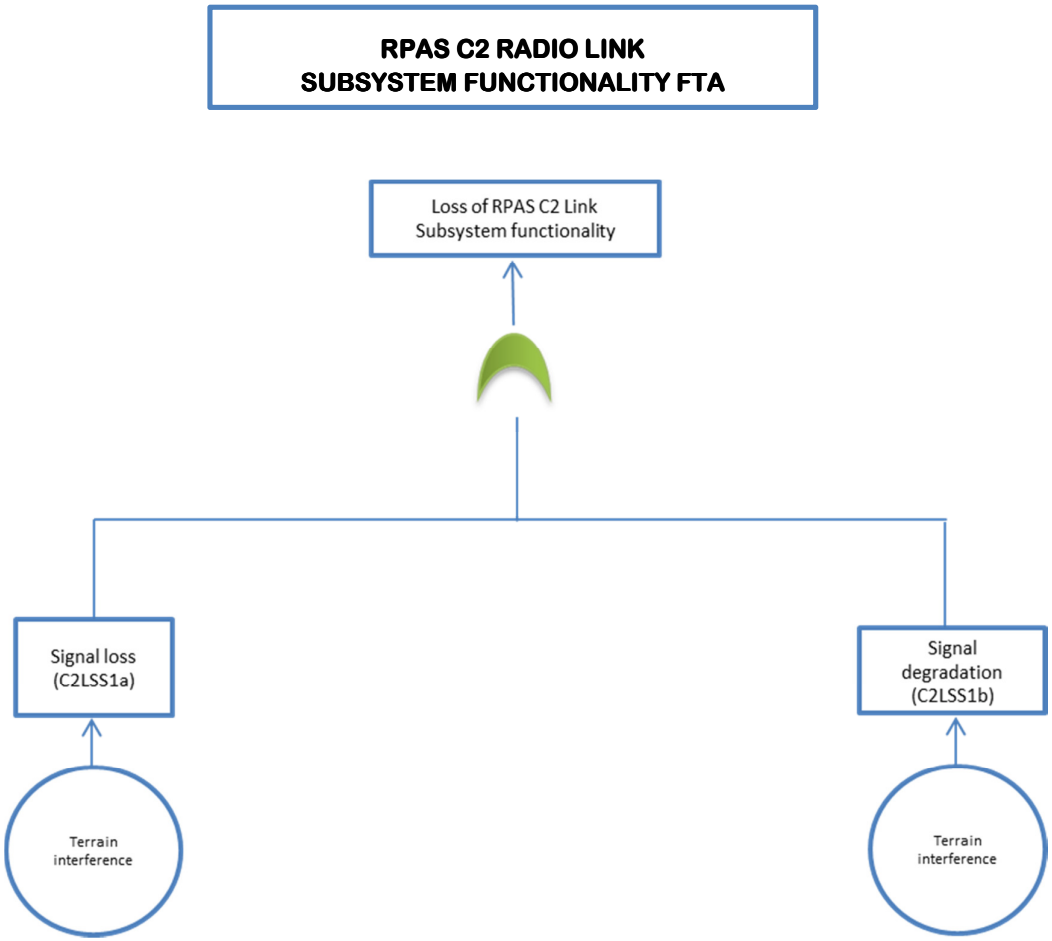


Figure 56 – RPAS C2 Radio link Subsystem functionality FTA

Table 126 – Loss of RPAS C2 Radio Link Subsystem functionality				
Loss of RPAS Fuel subsystem functionality			Possible multiple failures	Hazards
C2link signal degradation (C2LSS1a)	C2link signal loss (C2LSS1b)	Loss of RPAS C2 radio link Subsystem functionality		
0	0	0	-	Degradation or loss of uplink command link with the RPA Degradation or loss of downlink telemetry link from the RPA
0	1,5E-01	1,5E-01	-	
1,5E-01	0	1,5E-01	-	
1,5E-01	1,5E-01	3,0E-01	C2link signal degradation/C2link signal loss	
Estimated probability of occurrence level range				B → A

Note: GCS Start Up Subsystem functionality FTA: not performed due to the identification of a single failure mode in the FMECA analysis (Table 69).

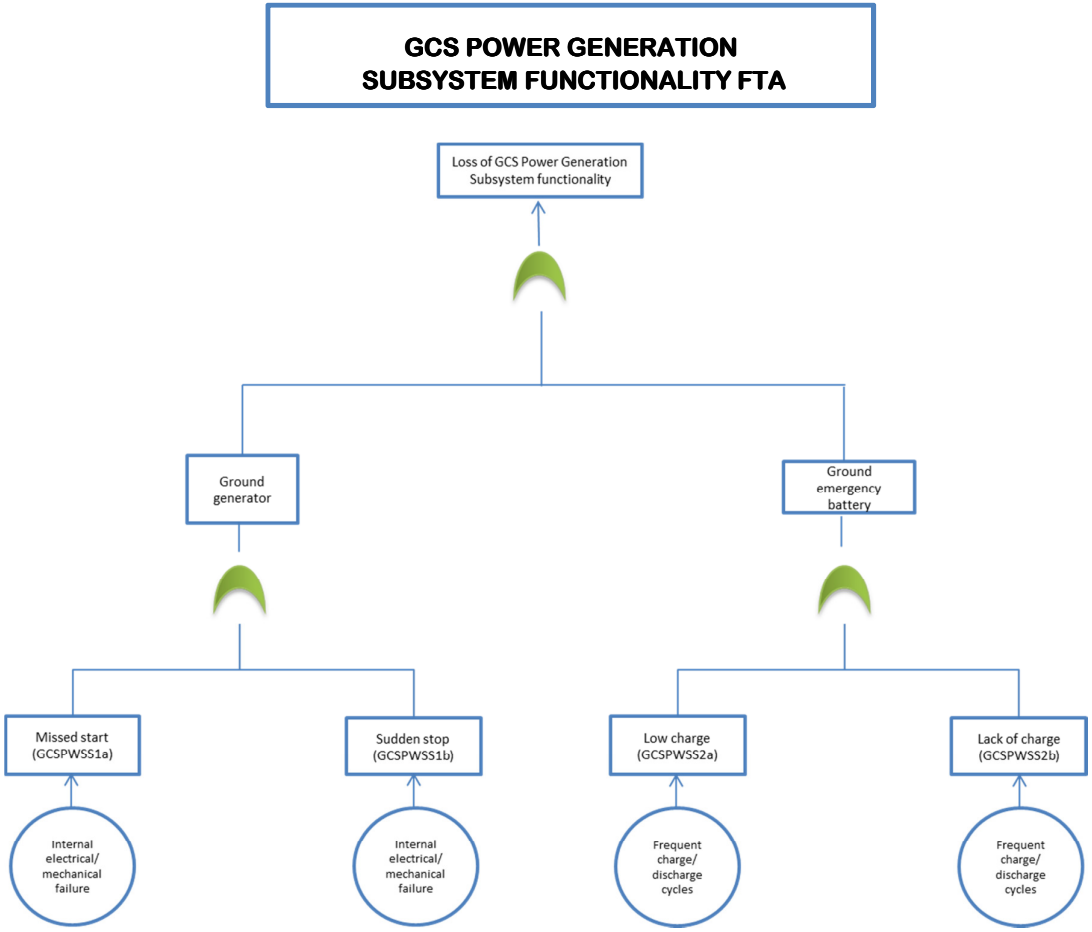


Figure 57 – GCS Power Generation Subsystem functionality FTA

Table 127 – Ground Control Station – Ground generator multiple failures

Ground generator single failure modes			Possible multiple failures	
Missed start (GCSPWSS1a)	Sudden stop (GCSPWSS1b)	Loss of ground generator functionality		
0	0	NO	-	-
0	5,5E-03	YES	-	-
5,5E-03	0	YES	-	-
5,5E-03	5,5E-03	YES	Missed start/Sudden stop	1,1E-02
Estimated probability of occurrence level, average value:				1,1E-02

Table 128 – Ground Control Station – Ground emergency battery multiple failures

Ground emergency battery single failure modes			Possible multiple failures	
Low charge (GCSPWSS2a)	Lack of charge (GCSPWSS2b)	Loss of ground emergency battery functionality		
0	0	NO	-	-
0	1,0E-03	YES	-	-
1,0E-03	0	YES	-	-
1,0E-03	1,0E-03	YES	Low charge/Lack of charge	2,0E-03
Estimated probability of occurrence level, average value:				2,0E-03

Table 129 – Ground Control Station – Loss of GCS Power Generation Subsystem functionality

Loss of GCS Power Generation subsystem functionality			Possible multiple failures	Hazards
Loss of ground generator functionality	Loss of ground emergency battery functionality	Loss of GCS Power Generation Subsystem functionality		
0	0	0	-	Loss of overall GCS functionality Loss of RPAS control due to the loss of overall GCS functionality
0	2,0E-03	2,0E-03	-	
1,1E-02	0	1,1E-02	-	
1,1E-02	2,0E-03	1,3E-02	Loss of ground generator functionality/Loss of ground emergency battery functionality	
Estimated probability of occurrence level:				D

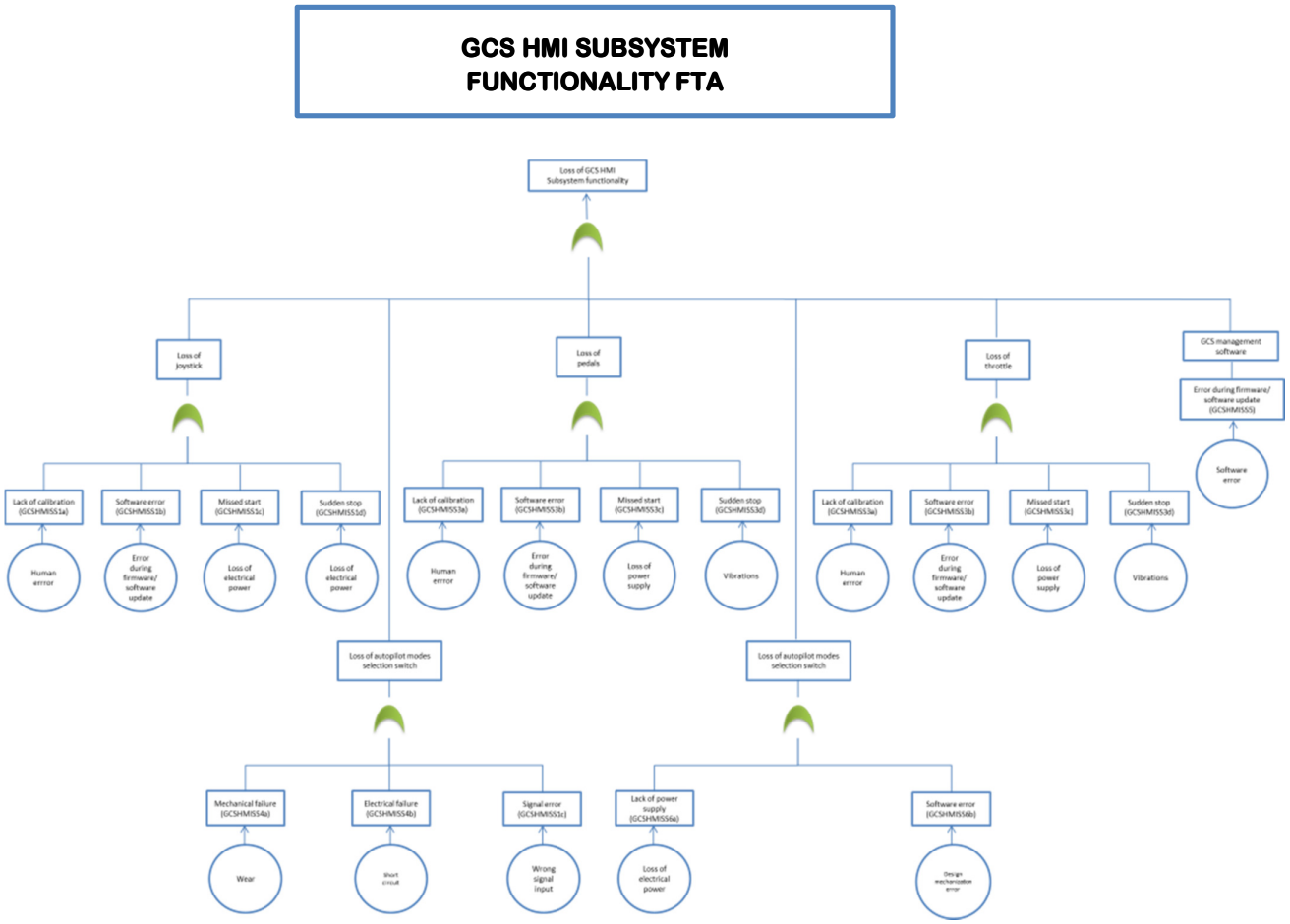


Figure 58 – GCS HMI Subsystem functionality FTA

Table 130 – Ground Control Station – Loss of GCS HMI Joystick functionality

Loss of GCS HMI Joystick functionality					Possible multiple failures	Hazards
Lack of calibration (GCSHMISS1a)	Software error (GCSHMISS1b)	Missed start (GCSHMISS1c)	Sudden stop (GCSHMISS1d)	Loss of GCS HMI Joystick functionality		
0	0	0	0	NO	-	0
0	0	0	5,5E-02	YES	-	5,5E-02
0	0	5,5E-02	0	YES	-	5,5E-02
0	0	5,5E-02	5,5E-02	YES	Missed start/ Sudden stop	1,1E-01
0	5,5E-02	0	0	YES	-	5,5E-02
0	5,5E-02	0	5,5E-02	YES	Software error/ Sudden stop	1,1E-01
0	5,5E-02	5,5E-02	0	YES	Software error/ Missed start	1,1E-01
0	5,5E-02	5,5E-02	5,5E-02	YES	Software error/ Missed start/ Sudden stop	1,65E-01
5,5E-02	0	0	0	YES	-	5,5E-02
5,5E-02	0	0	5,5E-02	YES	Lack of calibration/ Sudden stop	1,1E-01
5,5E-02	0	5,5E-02	0	YES	Lack of calibration/ Missed start	1,1E-01
5,5E-02	0	5,5E-02	5,5E-02	YES	Lack of calibration/ Missed start/ Sudden stop	1,65E-01
5,5E-02	5,5E-02	0	0	YES	Lack of calibration/ Software error	1,1E-01
5,5E-02	5,5E-02	0	5,5E-02	YES	Lack of calibration/ Software error/ Sudden stop	1,65E-01
5,5E-02	5,5E-02	5,5E-02	0	YES	Lack of calibration/ Software error/ Missed start	1,65E-01
5,5E-02	5,5E-02	5,5E-02	5,5E-02	YES	Lack of calibration/ Software error/ Missed start/ Sudden stop	2,2E-01
Estimated probability of occurrence level, average value:						1,1E-01
Main hazard: loss of RPA longitudinal and lateral attitude control; estimated probability of occurrence level:						B

Table 131 – Ground Control Station – Loss of GCS HMI Pedals functionality

Loss of GCS HMI Pedals functionality					Possible multiple failures	Hazards
Lack of calibration (GCSHMISS2a)	Software error (GCSHMISS2b)	Missed start (GCSHMISS2c)	Sudden stop (GCSHMISS2d)	Loss of GCS HMI Pedals functionality		
0	0	0	0	NO	-	0
0	0	0	5,5E-02	YES	-	5,5E-02
0	0	5,5E-02	0	YES	-	5,5E-02
0	0	5,5E-02	5,5E-02	YES	Missed start/ Sudden stop	1,1E-01
0	5,5E-02	0	0	YES	-	5,5E-02
0	5,5E-02	0	5,5E-02	YES	Software error/ Sudden stop	1,1E-01
0	5,5E-02	5,5E-02	0	YES	Software error/ Missed start	1,1E-01
0	5,5E-02	5,5E-02	5,5E-02	YES	Software error/ Missed start/ Sudden stop	1,65E-01
5,5E-02	0	0	0	YES	-	5,5E-02
5,5E-02	0	0	5,5E-02	YES	Lack of calibration/ Sudden stop	1,1E-01
5,5E-02	0	5,5E-02	0	YES	Lack of calibration/ Missed start	1,1E-01
5,5E-02	0	5,5E-02	5,5E-02	YES	Lack of calibration/ Missed start/ Sudden stop	1,65E-01
5,5E-02	5,5E-02	0	0	YES	Lack of calibration/ Software error	1,1E-01
5,5E-02	5,5E-02	0	5,5E-02	YES	Lack of calibration/ Software error/ Sudden stop	1,65E-01
5,5E-02	5,5E-02	5,5E-02	0	YES	Lack of calibration/ Software error/ Missed start	1,65E-01
5,5E-02	5,5E-02	5,5E-02	5,5E-02	YES	Lack of calibration/ Software error/ Missed start/ Sudden stop	2,2E-01
Estimated probability of occurrence level, average value:						1,1E-01
Main hazard: loss of RPA directional attitude control; estimated probability of occurrence level:						B

Table 132 – Ground Control Station – Loss of GCS HMI Throttle functionality

Loss of GCS HMI Throttle functionality					Possible multiple failures	Hazards
Lack of calibration (GCSHMISS3a)	Software error (GCSHMISS3b)	Missed start (GCSHMISS3c)	Sudden stop (GCSHMISS3d)	Loss of GCS HMI Throttle functionality		
0	0	0	0	NO	-	0
0	0	0	5,5E-02	YES	-	5,5E-02
0	0	5,5E-02	0	YES	-	5,5E-02
0	0	5,5E-02	5,5E-02	YES	Missed start/ Sudden stop	1,1E-01
0	5,5E-02	0	0	YES	-	5,5E-02
0	5,5E-02	0	5,5E-02	YES	Software error/ Sudden stop	1,1E-01
0	5,5E-02	5,5E-02	0	YES	Software error/ Missed start	1,1E-01
0	5,5E-02	5,5E-02	5,5E-02	YES	Software error/ Missed start/ Sudden stop	1,65E-01
5,5E-02	0	0	0	YES	-	5,5E-02
5,5E-02	0	0	5,5E-02	YES	Lack of calibration/ Sudden stop	1,1E-01
5,5E-02	0	5,5E-02	0	YES	Lack of calibration/ Missed start	1,1E-01
5,5E-02	0	5,5E-02	5,5E-02	YES	Lack of calibration/ Missed start/ Sudden stop	1,65E-01
5,5E-02	5,5E-02	0	0	YES	Lack of calibration/ Software error	1,1E-01
5,5E-02	5,5E-02	0	5,5E-02	YES	Lack of calibration/ Software error/ Sudden stop	1,65E-01
5,5E-02	5,5E-02	5,5E-02	0	YES	Lack of calibration/ Software error/ Missed start	1,65E-01
5,5E-02	5,5E-02	5,5E-02	5,5E-02	YES	Lack of calibration/ Software error/ Missed start/ Sudden stop	2,2E-01
Estimated probability of occurrence level, average value:						1,1E-01
Main hazard: loss of RPA trust control; estimated probability of occurrence level:						B

Table 133 – Ground Control Station – Loss of GCS HMI Autopilot modes selection switch functionality

Loss of GCS HMI Autopilot modes selection switch				Possible multiple failures	Hazards
Mechanical failure (GCSHMISS4a)	Electrical failure (GCSHMISS4a)	Signal error (GCSHMISS4a)	Loss of GCS HMI Autopilot modes selection switch		
0	0	0	NO	-	0
0	0	5,5E-02	YES	-	5,5E-02
0	5,5E-02	0	YES	-	5,5E-02
0	5,5E-02	5,5E-02	YES	Hydrogen fire/ Loss of LiPo batteries functionality	1,1E-01
5,5E-02	0	0	YES	-	5,5E-02
5,5E-02	0	5,5E-02	YES	Loss of Fuel Cells functionality/ Loss of LiPo batteries functionality	1,1E-01
5,5E-02	5,5E-02	0	YES	Loss of Fuel Cells functionality/ Hydrogen fire	1,1E-01
5,5E-02	5,5E-02	5,5E-02	YES	Loss of Fuel Cells functionality/ Hydrogen fire/ Loss of LiPo batteries functionality	1,65E.01
Estimated probability of occurrence level, average value:					8,25E-02
Main hazard: loss of autopilot modes control and management; estimated probability of occurrence level:					C

Table 134 – Ground Control Station – Loss of GCS HMI displays functionality

Loss of GCS HMI displays functionality			Possible multiple failures	Hazards
Lack of power supply (GCSHMISS4a)	Software error (GCSHMISS4a)	Loss of GCS HMI displays functionality		
0	0	NO	-	0
0	5,5E-02	YES	-	5,5E-02
5,5E-02	0	YES	-	5,5E-02
5,5E-02	5,5E-02	YES	Lack of power supply/ Software error	1,1E-01
Estimated probability of occurrence level:				1,1E-01
Main hazard: loss of RPA on board systems monitoring/telemetry due to GCS displays failure; estimated probability of occurrence level:				B

Note: The resultant of the interaction of the above cases of loss of GCS HMI functionalities has not been considered due to the total physical and functional independence of each one of them with respect to the other ones.

GCS PAYLOAD SENSORS HMI SUBSYSTEM FUNCTIONALITY FTA

Note: GCS Mission Payload HMI Subsystem functionality FTA: not performed; the effects of GCS Mission Payload Sensors HMI Subsystem loss of functionality are deemed negligible for the RPAS operations safety.

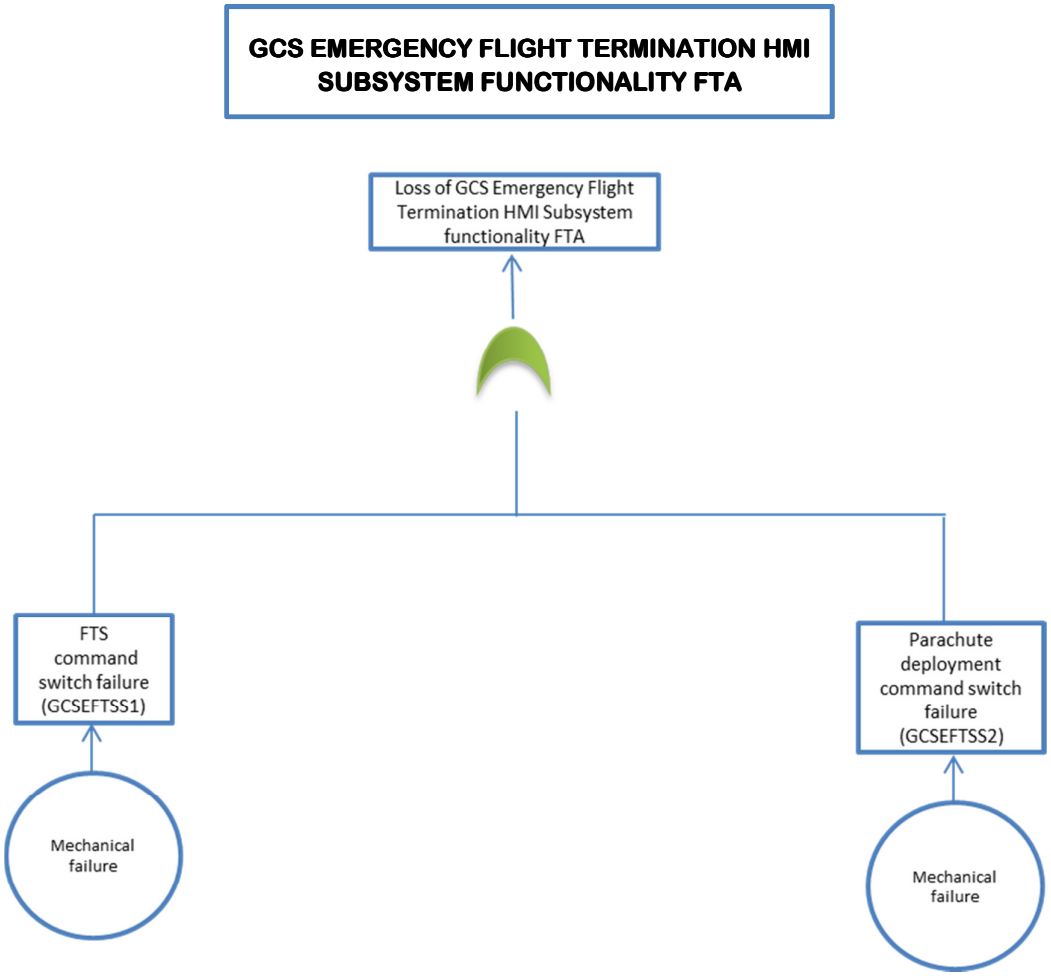


Figure 59 – GCS Emergency Flight Termination HMI Subsystem functionality FTA

Table 135 – Ground Control Station - Loss of GCS Emergency Flight Termination HMI Subsystem functionality

Loss of GCS Emergency Flight Termination HMI Subsystem functionality			Possible multiple failures	Hazards
FTS command switch failure (GCSEFTSS1)	Parachute deployment command switch failure (GCSEFTSS2)	Loss of GCS Emergency Flight Termination HMI subsystem functionality		
0	0	0	-	Loss of GCS Emergency Flight Termination HMI Subsystem functionality Uncontrolled impact of the RPA on ground Uncontrolled projection of debris on ground
0	1,5E-01	1,5E-01	-	
1,5E-01	0	1,5E-01	-	
1,5E-01	1,5E-01	3,0E-01	FTS command switch failure/ Parachute deployment command switch failure	
Estimated probability of occurrence level, range:				B → A

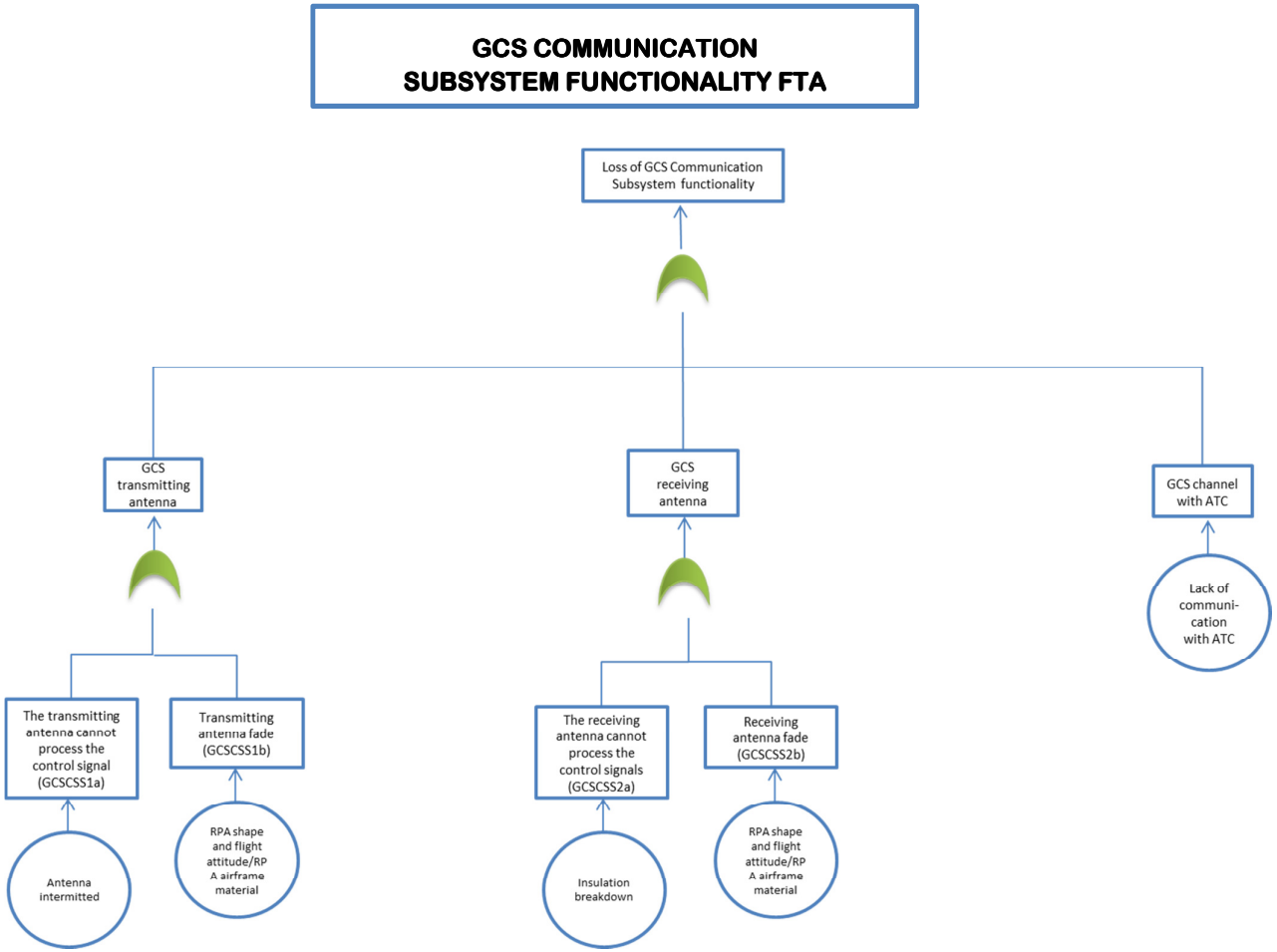


Figure 60 – GCS Communication Subsystem functionality FTA

Table 136 – Ground Control Station – Transmitting antenna multiple failures

Transmitting antenna single failure modes			Possible multiple failures	
The transmitting antenna cannot process the control signal (GCSCSS1a)	Transmitting antenna fade (GCSCSS1b)	Loss of transmitting antenna functionality		
0	0	NO	-	-
0	5,5E-02	YES	-	-
5,5E-03	0	YES	-	-
5,5E-03	5,5E-02	YES	The transmitter antenna cannot process the control signal/ Transmitting antenna fade	6,05E-02
Estimated probability of occurrence level, average value:				6,05E-02

Table 137 – Ground Control Station – Receiving antenna multiple failures

Receiving antenna failure modes			Possible multiple failures	
The receiving antenna cannot process the control signal (GCSCSS1a)	Receiving antenna fade (GCSCSS1b)	Loss of receiving antenna functionality		
0	0	NO	-	-
0	5,5E-02	YES	-	-
5,5E-03	0	YES	-	-
5,5E-03	5,5E-02	YES	The receiving antenna cannot process the control signal/Receiving antenna fade	6,05E-02
Estimated probability of occurrence level, average value:				6,05E-02

Table 138 – Ground Control Station – Loss of Communication Subsystem functionality

Loss of GCS Communication subsystem functionality			Possible multiple failures	Hazards
Loss of transmitting antenna functionality	Loss of receiving antenna functionality	Loss of GCS Communication Subsystem functionality		
0	0	0	-	Degradation or loss of link with the RPA Degradation or loss of RPAS control Degradation or loss of aerial segment monitoring through downlink telemetry
0	6,05E-02	6,05E-02	-	
6,05E-02	0	6,05E-02	-	
6,05E-02	6,05E-02	1,1E-01	Loss of transmitting antenna functionality/ Loss of receiving antenna functionality	
Estimated probability of occurrence level:				C

Table 139 - Selection of hazards derived from FTA analysis

Hazard	Estimated probability of occurrence level
Degradation or loss of rotor wing RPAS propulsion functionality	D → B
Degradation or loss of rotor wing RPAS control	D → B
Degradation or loss of rotor wing RPAS manoeuvrability	D → B
Uncontrolled projection of propeller debris	D → B
Degradation or loss of rotor wing RPAS power functionality	B
Fire on board rotor wing RPA	B
Degradation or loss of rotor wing RPAS electrical functionality	A
Fire on board rotor wing RPA	A
Degradation or loss of navigation functionality	A
Degradation or loss of GPS functionality on board the RPAS	A
Degradation or loss of EGNOS functionality on board the RPAS	A
Degradation or loss of ADS-B functionality on board the RPAS	A
Pressure sensors failure	A
Misleading altitude indication	A
Misleading airspeed indication	A
Degradation or loss of control of RPAS flight attitude	A
Loss or degradation of rotor wing RPAS manoeuvrability	A
Degradation or loss of emergency flight termination functionality	B → A
Degradation or loss of FTS functionality	B → A
Degradation or loss of Emergency Parachute functionality	B → A
Uncontrolled impact on ground	B → A
Uncontrolled projection of debris	B → A
Uncontrolled impact with third parties	B → A
Loss of RPAS Mission Control subsystem functionality	C → B
Degradation or loss of telemetry receipt for rotor wing RPAS monitoring	C → B
Degradation or loss of fixed wing (jet) combustion engine RPAS propulsion functionality	A
Degradation or loss of fixed wing (jet) combustion engine RPAS control	A
Degradation or loss of fixed wing (jet) combustion engine RPAS manoeuvrability	A
Degradation or loss of fixed wing combustion engine with propeller RPAS propulsion functionality	A
Degradation or loss of fixed wing combustion engine with propeller RPAS control	A
Degradation or loss of fixed wing combustion engine with propeller RPAS manoeuvrability	A
Degradation or loss of fixed wing RPAS fuel subsystem functionality	D → B
Degradation or loss of fixed wing RPAS propulsion	D → B
Degradation or loss of fixed wing RPAS control	D → B
Fire on board fixed wing RPAS	D → B
Degradation or loss of fixed wing RPAS power functionality	B → A
Fixed wing RPAS pressure sensors failure	B → A
Fixed wing RPAS misleading altitude indication	B → A
Fixed wing RPAS misleading airspeed indication	B → A
Fixed wing RPAS misleading angle of attack indication	B → A
Fixed wing RPAS misleading stall warning	B → A
Fixed wing RPAS stall	B → A
Fixed wing RPAS degradation or loss of flight attitude control	B → A
Degradation or loss of fixed wing RPAS flight control	C → B
Degradation or loss of fixed wing RPAS manoeuvrability	C → B
Loss of Hybrid Propulsion Subsystem functionality	Fuel
Loss of Hybrid Power Generation functionality	C → B
Fire on board hybrid RPAS	C → B
Degradation or loss of uplink command link with the RPA	B → A
Degradation or loss of downlink telemetry link from the RPA	B → A
Loss of overall GCS functionality	D
Loss of RPAS control due to the loss of overall GCS functionality	D
Loss of RPA longitudinal and lateral attitude control	B
Loss of RPA directional attitude control	B
Loss of RPA trust control	B
Loss of autopilot modes control and management	C
Loss of RPA on board systems monitoring/telemetry due to GCS displays failure	B
Loss of GCS Emergency Flight Termination HMI Subsystem functionality	B → A
Uncontrolled impact of the RPA on ground	B → A
Uncontrolled projection of debris on ground	B → A

Appendix C – Human factor analysis – Results

The following mismatches are conceived with reference to an operative context involving RPAS and manned aircraft performing flight operations in the civil not segregated airspace.

Table 140 – Application of the SHELL model and derived hazards

Interface	Relationship typology	Mismatches between interfaces from the remote pilot perspective	Mismatches between interfaces from the manned aircraft pilot perspective	Mismatches between interfaces from the ATC operator perspective	Hazards
L – H (Liveware – Hardware)	Human/Physical attributes of equipment, machines and facilities	Erroneous use of a human machine interface due to misleading workplace layout (RP1) Unintentional use of a human machine interface due to misleading workplace layout (RP1) Lack of awareness/monitoring of an alarm due to inconsistent implementation (not well visible for its position on the console; not well visible among other ones; not audible because without any sound associated, not audible because its sound is produced among many others) (RP3) Failure of warning system during abnormal situation (RP4) Erroneous use of a human machine interface due to low training or lack of training (RP5) Lack of manned intruder detection (RP6)	Insufficient HMI to detect RPAS (MAP1) Failure of warning system during abnormal situation (MAP2)	Insufficient HMI to identify RPAS (ATC1) Lack of separation provision instruction (ATC2) Lack of separation provision monitoring (ATC2) Incorrect separation provision monitoring (ATC4)	Misleading workplace layout Lack of remote pilot training Inconsistent or wrong implementation of warning/cautions Failure of warning/ caution system Loss of RPAS control Lack of RPAS detection Lack of manned aircraft detection Lack of separation provision from ATC Incorrect separation monitoring from ATC

Table 140 – Application of the SHELL model and derived hazards (Cont'd)					
Interface	Relationship typology	Mismatches between interfaces from the remote pilot perspective	Mismatches between interfaces from the manned aircraft pilot perspective with respect to RPAS intrusion on the track	Mismatches between interfaces from the ATC operator perspective with respect to RPAS intrusion on the track	Hazards
L – H (Liveware – Software)	Human/Supporting systems (regulations, manuals, checklists, publications, standard operating procedures, computer software)	Lack of use of checklists from the remote pilot (RP7) Misleading indication to the remote pilot generated by computer software error (RP8) Insufficient or inappropriate operational procedures (RP9) Misinterpretation of confusing procedures and/or checklists (RP10) Confusing, misleading or cluttered documents, maps or charts (RP11) Irrational indexing of an operations manual (RP12) Intentional violation of standard operating procedures (RP13) Intentional violation of separation (RP14)	Insufficient/inappropriate operating procedures to avoid RPAS intrusion (MAP3) Intentional deviation from ATC separation (MAP4)	Communication errors with the manned aircraft pilot (ATC5) Communication errors with the with the RPAS remote pilot (ATC6)	Lack of checklists Low remote pilot training in using checklist Insufficient or inappropriate operational procedures Confusing, misleading or cluttered documents, maps or charts Intentional violation of standard procedures Intentional violation of separations Intentional deviation from ATC separation ATC communication errors
L – H (Liveware – Liveware)	Persons/Persons (Flight crews, air traffic controllers, RPAS maintenance personnel, operational personnel)	Communication errors with ATC (RP15)	Low crew cooperation (MAP5) Communication errors due to misleading, ambiguous, inappropriate or poorly constructed communication within the crew (MAP6) Reduced performance and error from an imbalanced authority relationship within the crew (MAP7)	Communication errors with the manned aircraft pilot or with the RPAS remote pilot (ATC7) Communication errors with the manned aircraft pilot or with the RPAS remote pilot (ATC8) Reduced physical performance to lack of rest, unhealthy crew physical conditions, high workload (ATC9)	Remote pilot communication errors with ATC Communication errors from ATC Low manned aircraft crew resource management

Table 140 – Application of the SHELL model and derived hazards (Cont'd)

Interface	Relationship tipology	Mismatches between interfaces from the remote pilot perspective	Mismatches between interfaces from the manned aircraft pilot perspective with respect to RPAS intrusion on the track	Mismatches between interfaces from the ATC operator perspective with respect to RPAS intrusion on the track	Hazards
L – H (Liveware – Environment)	Humans/Internal & external environment (temperature, ambient light, noise, vibration, air quality & weather factors, aviation infrastructure and terrain)	Reduced physical performance to lack of rest, unhealthy crew physical conditions, high workload (RP16) Reduced performance and errors caused by stress/high workload (RP17) Remote pilot perceptual errors (RP18)	Reduced performance and errors due to lack of rest, unhealthy crew physical conditions, high workload (MAP8) Crew perceptual errors induced by environmental conditions (MAP9)	Reduced performance and errors due to lack of rest, unhealthy crew physical conditions, high workload (ATC10) Crew perceptual errors induced by environmental conditions (ATC11)	Remote pilot/crew/ATC operator reduced physical performance Remote pilot/manned aircraft crew perceptual errors

Table 141 – Application of the HFACS model and derived hazards

Classification according to HFACS methodology	Details	RPAS remote pilot	Manned aircraft pilot with respect to RPAS intrusion on the track	ATC operator with respect to RPAS intrusion on the track	Hazards
Unsafe acts					
Decision errors					Mid-air collision with other aircraft Collision with natural/man made obstacles when the RPAS is flying in manual mode Violation of separations Violation of operational procedures Lack of RPAS detection Mid-air collision with the RPAS Error to assign separations Error to manage separations RPAS flight in adverse conditions Loss of situational awareness
	Rule-based decisions	x	x	x	
	Choice decisions	x	x	x	
	Structured decisions	x	x	x	
Skill-based errors					
	Attention failures	x	x	x	
	Memory failures	x	x	x	
	Technique errors	x	x	x	
Perceptual errors					
	Misperceptions	x	x	x	
	Misjudgments	x	x	x	
Routine violations					
	Violation of training rules	x	x	x	
	Failed to comply with departmental manuals	x	x	x	
	Violations of orders, regulations and/or SOPs	x	x	x	
Exceptional violations					
	Performed unauthorized operations	x	x	x	
	Accepted unauthorized hazards	x	x	x	
	Not current/qualified	x	x	x	

Table 141 – Application of the HFACS model and derived hazards (Cont'd)

Classification according to HFACS methodology	Details	RPAS remote pilot	Manned aircraft pilot with respect to RPAS intrusion on the track	ATC operator with respect to RPAS intrusion on the track	Hazards
Preconditions for unsafe acts					RPAS flight in adverse conditions Mid-air collision with other aircraft RPAS automation failure RPAS remote pilot missing of checklist performance Collision with natural/man made obstacles when the RPAS is flying in manual mode
Environmental factors					
	Physical environment:				
	Weather	x	x	-	
	Lighting	x	x	-	
	Noise	x	x	x	
	Heat	x	x	-	
	Vibration	-	x	-	
	Technological environment:				
	Equipment and controls	x	x	x	
	Automation reliability/complexity	x	x	x	
	Task and procedure design	x	x	x	
	Manuals and checklist design	x	x	x	
	Interfaces and displays	x	x	x	

Table 141 – Application of the HFACS model and derived hazards (Cont'd)

Classification according to HFACS methodology	Details	RPAS remote pilot	Manned aircraft pilot with respect to RPAS intrusion on the track	ATC operator with respect to RPAS intrusion on the track	Hazards
Condition of employees					Mid-air collision with other aircraft Collision with natural/man made obstacles when the RPAS is flying in manual mode Loss of situational awareness
	Adverse mental states:				
	Complacency	x	x	x	
	Stress	x	x	x	
	Overconfidence	x	x	x	
	Mental fatigue	x	x	x	
	Distraction	x	x	x	
	Confusion	x	x	x	
	Adverse psychological states:				
	Physical fatigue	x	x	x	
	Visual illusions	x	x	x	
	Hypoxia	-	x	-	
	Medical illness	x	x	x	
	Physical/Mental limitations:				
	Visual limitations	x	x	x	
	Hearing limitations	x	x	x	
	Not current/qualified	x	x	x	
	Incompatible physical capability	-	-	-	
	Incompatible intelligence/aptitude	-	-	-	

Table 141 – Application of the HFACS model and derived hazards (Cont'd)

Classification according to HFACS methodology	Details	RPAS remote pilot	Manned aircraft pilot with respect to RPAS intrusion on the track	ATC operator with respect to RPAS intrusion on the track	Hazards
Personal/interpersonal factors					Mid-air collision with other aircraft Collision with natural/man made obstacles when the RPAS is flying in manual mode Violation of separations Violation of operational procedures Lack of RPAS detection Mid-air collision with the RPAS Error to assign separations Error to manage separations RPAS flight in adverse conditions
	Communication, coordination and planning:				
	Failed to conduct adequate brief	x	x	x	
	Lack of teamwork	x	x	x	
	Poor communication/coordination	x	x	x	
	Failure of leadership	x	x	x	
	Fitness for duty:				
	Crew rest requirements	x	x	x	
	Bottle to brief rules	x	x	x	
	Self-medicating	x	x	x	
	Poor dietary practice	x	x	x	
	Overexertion while off duty	x	x	x	
	Inadequate preparation skill	x	x	x	

Table 141 – Application of the HFACS model and derived hazards (Cont'd)

Classification according to HFACS methodology	Details	RPAS remote pilot	Manned aircraft pilot with respect to RPAS intrusion on the track	ATC operator with respect to RPAS intrusion on the track	Hazards
Unsafe supervision					Mid-air collision with other aircraft Collision with natural/man made obstacles when the RPAS is flying in manual mode Violation of separations Violation of operational procedures Lack of RPAS detection Mid-air collision with the RPAS Error to assign separations Error to manage separations RPAS flight in adverse condition
Inadequate supervision					
	Failure to administer proper training	x	x	x	
	Lack of professional guidance	x	x	x	
	Failure to provide oversight	x	x	x	
Planned inappropriate operations					
	Risk outweighs benefits	X	X	X	
	Excessive tasking/workload	X	X	X	
	Poor crew pairing	x	x	x	
Failed to correct problems					
	Failure to correct inappropriate behavior	x	x	x	
	Failure to correct a safety hazard	x	x	x	
Supervisory violations					
	Failed to enforce the rules	x	x	x	
	Authorized unnecessary hazard	x	x	x	
	Authorized unqualified crew for flight	x	x	x	

Table 141 – Application of the HFACS model and derived hazards (Cont'd)

Classification according to HFACS methodology	Details	RPAS remote pilot	Manned aircraft pilot with respect to RPAS intrusion on the track	ATC operator with respect to RPAS intrusion on the track	Hazards
Organizational influences					-
Resource management					
	Human	x	x	x	
	Monetary	x	x	x	
	Equipment/Facility	x	x	x	
Organizational climate					
	Structure	x	x	x	
	Policy	x	x	x	
	Culture	x	x	x	
Operational process					
	Operations	x	x	x	
	Procedures	x	x	x	
	Oversight	x	x	x	

Table 142 – Hazard derived from human factor (SHELL and HFACS models)

Possible hazards	Estimated probability of occurrence level
ATC communication errors	Improbable - 2 [85]
Collision with natural/man made obstacles when the RPAS is flying in manual mode	Occasional - 4
Confusing, misleading or cluttered operational documents, and checklists	Frequent - 5
Error to manage separations	Occasional - 4
Human senses limitation	Frequent - 5
Loss of remote pilot situational awareness	Frequent - 5
Insufficient or inappropriate operational procedures	Occasional - 4
Intentional violation of standard procedures	Remote - 3
Lack of specific checklists, operational procedures	Frequent - 5
Low manned aircraft crew resource management	Occasional - 4
Low remote pilot training	Occasional - 4
Performance of non-compliant operational procedure	Occasional - 4
Excessive workload	Occasional - 4
Remote pilot reduced physical performance	Remote - 3
Remote pilot perceptual errors	Frequent - 5
RPAS flight in adverse weather conditions	Occasional - 4
Unintentional violation of operational procedures	Remote - 3
Intentional violation of operational procedures	Occasional - 4
Unintentional violation of separations	Remote - 3
Intentional violation of separations	Occasional - 4

Appendix D - Safety risk assessment matrices - Results

Table 143 – U-Space Safety Risk Matrix

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
RPAS Aviate functionality related hazards											
H01	Loss of abort launch capability	Impossibility to abort the RPA launch if less than optimal conditions of launch occur	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/Use of recovery parachute system	3D	Moderate risk Acceptable based on risk mitigation
H02	Loss of flight controls	Loss of ESC for rotor wing RPA; loss of the possibility to command the moving surfaces of fixed wing RPAS; degradation of RPAS maneuverability and dynamic control in flight; loss of the possibility to change altitude or heading	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/Use of recovery parachute system	4D	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H03	Loss of propulsion	Loss of one or more electrical engine for rotor RPAS; loss of combustion engine for fixed wing RPAS; impossibility to change airspeed	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/Use of recovery parachute system	4D	Moderate risk Acceptable based on risk mitigation
H04	Loss of GCS HMI	Loss of the HMI functionality in the Ground Control Station	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/Use of recovery parachute system	3D	Moderate risk Acceptable based on risk mitigation
H05	Deviation from steady-state (not- accelerating) flight condition	Impossibility for the aircraft to perform the cruise phase of a flight mission	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/Use of recovery parachute system	3D	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H06	Loss of Emergency Flight Termination System	Loss of Flight Termination System functionality	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Set autopilot on landing flight mode	2A	Moderate risk Acceptable based on risk mitigation
H07	Loss of "Return to home function"	Loss of the possibility to use the predefined procedure '"Return to home function" to safely recover the RPAS	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Use of Flight Termination system (FTS)/ Use of parachute recovery system	2E	Low risk Acceptable
RPAS Navigate functionality related hazards											
H08	Loss of mission plan	Loss of mission plan functionality	Remote - 3	Minor – D	3D	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Use the "Return to home" function	2E	Low risk Acceptable

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H09	Loss of GPS signal	Abrupt loss of GPS signal	Occasional - 4	Minor – D	4D	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Switch to EGNOS service/Switch to inertial navigation/ Use the "Return to home" function	4E	Low risk Acceptable
H10	Loss of EGNOS signal	Abrupt loss of EGNOS signal	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch to GPS service/Switch to inertial navigation/ Use the "Return to home" function	3D	Moderate risk Acceptable based on risk mitigation
H11	Drift from the mission plan	The RPAS does not copy the predefined mission profile	Remote - 3	Hazardous - B	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Use of 'Return to home' function/ Use of Flight Termination system (FTS)/Use of recovery parachute system	3E	Low risk Acceptable

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
RPAS Communicate functionality related hazards											
H12	Loss of uplink channel of the RPAS radio link	Loss of command link to send command signals and controls to the RPAS	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of a redundant radio link/Use of 'Return to home' function/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	4E	Moderate risk Acceptable based on risk mitigation
H13	Loss of downlink channel of the RPAS radio link	Loss of command link to send command signals and controls to the RPAS	Occasional - 4	Hazardous - B	4B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of a redundant radio link/Use of 'Return to home' function/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	4E	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H14	Loss of ADS_B	Failure of the ADS-B or degradation of its signal	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/ Use of parachute recovery system	4D	Moderate risk Acceptable based on risk mitigation
RPAS Hazards avoidance functionality related hazards											
H15	Presence of natural obstacles	Flight operations performed in close proximity to hills, mountains or terrain	Frequent - 5	Catastrophic - A	5A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of on board collision avoidance systems based on the use of downward LIDAR or SONAR sensor/Provision of terrain profile data from mapping services (Like Google Map) to be implemented into the RPAS mission planner	5E	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H16	Presence of man-made manufactures	Flight operations in presence of man-made manufactures like buildings or other civil infrastructures (bridges, electrical lines, etc.)	Frequent - 5	Catastrophic - A	5A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of on board collision avoidance systems based on the use of downward LIDAR or SONAR sensor/Provision of terrain profile data from mapping services (Like Google Map) to be implemented into the RPAS mission planner/ Provision of geofence software functionality	5E	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H17	Mid-air collision with other aircraft	Mid-air collision with other manned or unmanned aircraft	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of onboard DAA subsystem in case of mid-air collision with cooperative traffic/Provision of on board collision avoidance systems based on the use of downward LIDAR/SONAR sensors in case of mid-air collision with not cooperative traffic	4E	Moderate risk Acceptable based on risk mitigation
H18	Loss of DAA functionality	Loss of Detection and Avoid capability	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/ Use of parachute recovery system	3D	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H19	No detectability from other airspace users	Low or no detectability of flying RPAS from manned aircraft or from other unmanned aircraft	Frequent - 5	Catastrophic - A	5A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of on board ADS_B	5D	Moderate risk Acceptable based on risk mitigation
H20	Cooperative traffic intrusion	Abrupt intrusion of cooperative manned or unmanned traffic	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of ADS_B equipment and DAA subsystem on board the RPAS	4D	Moderate risk Acceptable based on risk mitigation
H21	Not cooperative traffic intrusion	Abrupt intrusion of not cooperative manned or unmanned traffic	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of secondary (with respect to DAA subsystem) LIDAR /SONAR sensors as collision avoidance system against not cooperative traffic	4D	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H22	Missed cooperative traffic tracking	Missed surveillance and tracking of cooperative traffic	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of ADS_B equipment and DAA subsystem on board the RPAS	3D	Moderate risk Acceptable based on risk mitigation
H23	Missed not cooperative traffic tracking	Missed surveillance and tracking of not cooperative traffic	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of secondary (with respect to DAA subsystem) LIDAR /SONAR on board the RPA	3D	Moderate risk Acceptable based on risk mitigation
H24	Collision with cooperative traffic	Mid-air collision with other cooperative manned or unmanned aircraft	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of onboard DAA subsystem	4E	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H25	Collision with not cooperative traffic	Mid-air collision with other not cooperative manned or unmanned aircraft	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of secondary (with respect to DAA subsystem) LIDAR /SONAR on board the RPA	4E	Moderate risk Acceptable based on risk mitigation
H26	Missed performance of avoidance collision maneuver	Missed performance of collision avoidance maneuver: for example due to primary collision avoidance system DAA failure or degraded functionality	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of secondary (with respect to DAA subsystem) LIDAR /SONAR on board the RPA	3D	Moderate risk Acceptable based on risk mitigation
H27	Missed monitoring of performance of avoidance collision maneuver	Missed monitoring of performance of avoidance collision maneuver example due to human error	Occasional - 4	Hazardous - B	4B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Increase remote pilot training	3B	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H28	Missed weather awareness capability	Missed access to weather information for the remote pilot causing decrease in his/her awareness of weather conditions	Remote - 3	Hazardous - B	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Use of Flight Termination system (FTS)/ Use of parachute recovery system	3E	Low risk Acceptable
H29	Missed gathering of contingent weather information	The human machine interface cannot enable the remote pilot to request weather specific to a current or future flight mission or cannot convey weather information to the remote pilot	Remote - 3	Hazardous - B	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Increase on ground routine maintenance/ checks for weather information gathering HMI	2B	Low risk Acceptable
H30	Missed avoidance of adverse weather	The pilot shall remotely enable the RPAS to avoid adverse weather performing the correct avoidance maneuver	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provide support to the remote pilot with an onboard miniaturized weather Doppler RADAR	4E	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
Cross cutting functionalities related hazards											
H31	Loss of RPAS subsystems health and status monitoring	The RPAS health and status signals are not sent to ground	Occasional - 4	Hazardous - B	4B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of 'Return to home' function/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	4E	Moderate risk Acceptable based on risk mitigation
H32	Loss of communication while transiting from LOS to BRLOS and vice versa	Loss of communication while transiting from LOS to BRLOS and vice versa due to physical obstacles (natural or man-made)	Frequent - 5	Catastrophic - A	5A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Performance of an accurate pre-flight mission planning in accordance with the RPAS radio link range capability	4E	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H33	Unintentional radio link interference	Unintentional radio frequency interference of RPAS radio link due to other civil sources of electromagnetic signals (telecommunication, airport surveillance systems, etc.)	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant radio link band	2A	Moderate risk Acceptable based on risk mitigation
H34	Malicious radio link jamming	Intentional unlawful RF interference of RPAS radio - link	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant radio link using another radio frequency band /Use of Flight Termination system (FTS)/ Use of parachute recovery system	3D	Moderate risk Acceptable based on risk mitigation
H35	Malicious radio link spoofing	Intentional unlawful RF interference of RPAS radio - link	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant radio link using another radio frequency band /Use of Flight Termination system (FTS)/ Use of parachute recovery system	3D	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
Contingencies → Failures related hazards											
H36	Fire	Fire on board the RPAS	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Immediate flight termination using the Flight Termination system (FTS)	4D	Moderate risk Acceptable based on risk mitigation
H37	Loss of RPAS autopilot	Loss of autopilot functionality	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant autopilot/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	2E	Low risk Acceptable
H38	Loss of electrical power	Loss electrical power generation	Frequent - 5	Catastrophic - A	5A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/ Use of parachute recovery system	4D	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H39	Loss of inertial platform	Loss of all inertial references for navigation	Occasional - 4	Hazardous - B	4B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant inertial platform/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	3D	Moderate risk Acceptable based on risk mitigation
H40	Loss of heading indication	Loss of heading indication for example caused by loss of inertial platform	Improbable - 2	Hazardous - B	2B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant inertial platform/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	1E	Moderate risk Acceptable based on risk mitigation
H41	Loss of altitude indication	Loss of altitude indication; for example caused by altimeter failure	Improbable - 2	Catastrophic - A	2B	Unacceptable	Moderate risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant altimeter/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	1D	Low risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H42	Pressure sensors failure	Loss of absolute or differential pressure sensor	Frequent - 5	Catastrophic - A	5A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant pressure sensor/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	4D	Moderate risk Acceptable based on risk mitigation
H43	Misleading altitude indication	Misleading altitude indication due to pressure sensor failure	Frequent - 5	Catastrophic - A	5A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant altimeter/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	4D	Moderate risk Acceptable based on risk mitigation
H44	Misleading airspeed indication	Misleading airspeed indication due to pressure sensor failure	Frequent - 5	Catastrophic - A	5A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on pressure sensor/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	4D	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 ft, RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H45	Misleading indication of the angle of incidence	Misleading angle of incidence indication due to pressure sensor failure	Frequent - 5	Catastrophic - A	5A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant pressure sensor/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	4D	Moderate risk Acceptable based on risk mitigation
H46	Stall	Fixed wing RPAS stall caused by misleading instrumental indications or by remote pilot error	Frequent - 5	Catastrophic - A	5A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Performance of diving maneuver/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	5D	Moderate risk Acceptable based on risk mitigation
H47	Loss of fuel cell	Loss of fuel cell in an hybrid RPAS leading to degradation or loss of propulsion functionality and aircraft maneuverability and control during the flight	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on LiPo batteries as redundant source of electrical power	3D	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
Contingencies → Human factor related hazards											
H48	Remote pilot low training	Lack or not appropriate remote pilot training	Occasional - 4	Hazardous - B	4B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Increase/ improve remote pilot training	3D	Moderate risk Acceptable based on risk mitigation
H49	Non-compliant operational procedures	Lack of compliant operational procedures, check-lists, etc.	Frequent - 5	Hazardous - B	5B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of proper operational procedures, check-lists, etc.	3D	Moderate risk Acceptable based on risk mitigation
H50	Remote pilot loss of situational awareness	Loss of remote pilot situational awareness	Frequent - 5	Hazardous - B	5B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Increase remote pilot training	3D	Moderate risk Acceptable based on risk mitigation

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H51	Human senses limitations	Limitations of human senses due to the fact that the remote pilot is on ground and not on board the aircraft and he/she has to use sensors and not his/her 'senses'	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Increase remote pilot training	3D	Moderate risk Acceptable based on risk mitigation
H52	Remote pilot excessive workload	Excessive remote pilot workload	Occasional - 4	Major - C	4C	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Increase remote pilot training	3E	Low risk Acceptable
Contingencies → Weather related hazards											
H53	Cloud cover	Weather hazard	Frequent - 5	Major - C	5C	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Flight mission interruption and application of the "Return to Home" function	5D	Moderate risk Acceptable based on risk mitigation
H54	Fog	Weather hazard	Occasional - 4	Major - C	4C	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Flight mission interruption and application of the "Return to Home" function	3E	Low risk Acceptable

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H55	Freezing rain	Weather hazard	Remote - 3	Hazardous - B	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Flight mission interruption and application of the "Return to Home" function	3E	Low risk Acceptable
H56	Glare	Weather hazard	Occasional - 4	None - E	4E	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	-	-	- -
H57	Haze	Weather hazard	Occasional - 4	Major - C	4C	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Flight mission interruption and application of the "Return to Home" function	4E	Low risk Acceptable
H58	Humidity	Weather hazard	Frequent - 5	Hazardous - B	5B	Acceptable	High risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Mission not to be performed due to less than optimal operational conditions	5E	Moderate risk Acceptable
H59	Ice	Weather hazard	Occasional - 4	Hazardous - B	4B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	4E	Moderate risk Acceptable

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H60	Rain	Weather hazard	Frequent - 5	Hazardous - B	5B	Unacceptable	High risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Provision of an on board miniaturized weather Doppler RADAR to identify the weather hazard and application of the "Return to Home" function	5E	Moderate risk Acceptable
H61	Snow	Weather hazard	Occasional - 4	Hazardous - B	4B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of an on board miniaturized weather Doppler RADAR to identify the weather hazard and application of the "Return to Home" function	5E	Moderate risk Acceptable
H62	Solar storms	Weather hazard	Remote - 3	Hazardous - B	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Use 'Return to Home" function	3E	Low risk Acceptable

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H63	Temperature	Weather hazard	Frequent - 5	Hazardous - B	5B	Acceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	5E	Moderate risk Acceptable
H64	Turbulence	Weather hazard	Occasional - 4	Hazardous - B	4B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	4E	Moderate risk Acceptable
H65	Wind	Weather hazard	Frequent - 5	Hazardous - B	5B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	5E	Moderate risk Acceptable

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H66	Lightening strike	Weather hazard	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	4E	Moderate risk Acceptable
H67	Hail	Weather hazard	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	4E	Moderate risk Acceptable
H68	Hurricanes	Weather hazard	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	3E	Low risk Acceptable

Table 143 – U-Space Safety Risk Matrix (Cont'd)

Safety risk assessment
Airspace service: U-Space
RPAS specific category operations
[Flight limitations: Max height: 500 Ft., RLOS, MTOW: 25 kg < MTOW < 150 kg]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H69	Volcanic ash	Volcanic hazard	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	3E	Low risk Acceptable

Table 144 – ATM safety risk matrix

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
RPAS Aviate functionality related hazards											
H01	Impossibility to perform maneuvers on ground	Degradation or loss of functionalities to maneuver the aircraft on ground using flight controls, steering controls and propulsion controls	Remote - 3	Hazardous - B	3B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Increase RPA maintenance	2B	Moderate risk Acceptable based on risk mitigation
H02	Loss of abort launch capability	Impossibility to abort the RPA launch if less than optimal conditions of launch occur	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/Use of recovery parachute system	3D	Moderate risk Acceptable based on risk mitigation

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H03	Loss of flight controls	Loss of ESC for rotor wing RPA; loss of the possibility to command the moving surfaces of fixed wing RPAS; degradation of RPAS maneuverability and dynamic control in flight; loss of the possibility to change altitude or heading	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/Use of recovery parachute system	3D	Moderate risk Acceptable based on risk mitigation
H04	Loss of propulsion	Loss of one or more electrical engine for rotor RPAS; loss of combustion engine for fixed wing RPAS; impossibility to change airspeed	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/Use of recovery parachute system	3D	Moderate risk Acceptable based on risk mitigation
H05	Loss of GCS HMI	Loss of the HMI functionality in the Ground Control Station	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Use of Flight Termination system (FTS)/Use of recovery parachute system	2D	Low risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H06	Loss of GCS monitoring displays	Loss of the HMI in the Ground Control Station	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/Use of recovery parachute system	3D	Moderate risk Acceptable based on risk mitigation
H07	Deviation from steady-state (not- accelerating) flight condition	Impossibility for the aircraft to perform the cruise phase of a flight mission	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Use of Flight Termination system (FTS)/Use of recovery parachute system	2D	Low risk Acceptable
H08	Loss of Emergency Flight Termination System	Loss of Flight Termination System functionality	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Set autopilot on landing flight mode	2D	Low risk Acceptable
H09	Loss of 'Return to home function'	Loss of the possibility to use a predefined procedure to safely recover the RPAS	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Use of Flight Termination System (FTS)	2E	Low risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment
Airspace service: ATM
RPAS certified category operations
[Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H10	Impossibility to perform a go-around maneuver	Impossibility to perform a go-around maneuver during approach	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Flight termination using emergency recovery parachute	4D	Moderate risk Acceptable based on risk mitigation
RPAS Navigate functionality related hazards											
H11	Loss of mission plan	Loss of mission plan functionality	Improbable - 2	Minor – D	2D	Acceptable	Low risk	Acceptable	-	-	- -
H12	Loss of GPS signal	Abrupt loss of GPS signal	Occasional - 4	Minor – D	4D	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Switch to EGNOS service/ Switch to inertial navigation/ Use the "Return to home" function	4E	Low risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H13	Loss of EGNOS signal	Abrupt loss of EGNOS signal	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch to GPS service/ Switch to inertial navigation/ Use the "Return to home" function	3D	Moderate risk Acceptable based on risk mitigation
H14	Drift from the mission plan	The RPAS does not copy the predefined mission profile	Improbable - 2	Hazardous - B	2B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Use of 'Return to home' function/ Use of Flight Termination system (FTS)/Use of recovery parachute system	2D	Low risk Acceptable
H15	Loss of mission plan updating software functionality	Loss of mission plan updating software functionality (for RPAS capable of mission lasting several days or weeks)	Remote - 3	Hazardous - B	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Use of 'Return to home' function/ Use of Flight Termination system (FTS)/Use of recovery parachute system	3E	Low risk Acceptable
H16	Lack of communication of mission plan updating to ATC	Lack of communication of mission plan updating to ATC	Remote - 3	Hazardous - B	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Increase remote pilot training	2E	Low risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment
Airspace service: ATM
RPAS certified category operations
[Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
RPAS Communicate functionality related hazards											
H17	Loss of uplink channel of the RPAS radio link	Loss of command link to send command signals and controls to the RPAS	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of a redundant radio link/Use of 'Return to home' function/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	3D	Moderate risk Acceptable based on risk mitigation
H18	Loss of downlink channel of the RPAS radio link	Loss of command link to send command signals and controls to the RPAS	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of a redundant radio link/Use of 'Return to home' function/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	3D	Moderate risk Acceptable based on risk mitigation

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H19	Loss of ADS_B	Failure of the ADS-B or degradation of its signal	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Provision of a redundant ADS-B	1A	Moderate risk Acceptable based on risk mitigation
H20	Loss of communication with ATC	Loss of communication radio link with ATC	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Rely on controller-pilot data link communication channel	2A	Moderate risk Acceptable based on risk mitigation

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H21	Presence of natural obstacles	Flight operations performed in close proximity to hills, mountains or terrain	Frequent - 5	Catastrophic - A	5A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of on board collision avoidance systems based on the use of downward LIDAR or SONAR sensor/Provision of terrain profile data from mapping services (Like Google Map) to be implemented into the RPAS mission planner	5E	Moderate risk Acceptable based on risk mitigation

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H22	Presence of man-made manufactures	Flight operations in presence of man-made manufactures like buildings or other civil infrastructures (bridges, electrical lines, etc.)	Frequent - 5	Catastrophic - A	5A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of on board collision avoidance systems based on the use of downward LIDAR or SONAR sensor/Provision of terrain profile data from mapping services (Like Google Map) to be implemented into the RPAS mission planner/ Provision of geofence software functionality	5E	Moderate risk Acceptable based on risk mitigation

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H23	Mid-air collision with other aircraft	Mid-air collision with other manned or unmanned aircraft	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of onboard DAA subsystem in case of mid-air collision with cooperative traffic/Provision of on board collision avoidance systems based on the use of downward LIDAR/SONAR sensors in case of mid-air collision with not cooperative traffic	4E	Moderate risk Acceptable based on risk mitigation
H24	Loss of DAA functionality	Loss of Detection and Avoid capability	Improbable	Catastrophic - A	2A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant DAA	1A	Moderate risk Acceptable based on risk mitigation

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H25	No detectability from other airspace users	Low or no detectability of flying RPAS from manned aircraft or from other unmanned aircraft	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of on board ADS_B	3D	Moderate risk Acceptable based on risk mitigation
H26	Cooperative traffic intrusion	Abrupt intrusion of cooperative manned or unmanned traffic	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of ADS_B equipment and DAA subsystem on board the RPAS	3D	Moderate risk Acceptable based on risk mitigation
H27	Not cooperative traffic intrusion	Abrupt intrusion of not cooperative manned or unmanned traffic	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of secondary (with respect to DAA subsystem) LIDAR /SONAR sensors as collision avoidance system against not cooperative traffic	4D	Moderate risk Acceptable based on risk mitigation

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H28	Missed cooperative traffic tracking	Missed surveillance and tracking of cooperative traffic	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Provision of ADS_B equipment and DAA subsystem on board the RPAS	2D	Low risk Acceptable
H29	Missed not cooperative traffic tracking	Missed surveillance and tracking of not cooperative traffic	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Provision of ADS_B equipment and DAA subsystem on board the RPAS	2D	Low risk Acceptable
H30	Collision with cooperative traffic	Mid-air collision with other cooperative manned or unmanned aircraft	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Provision of onboard DAA subsystem	2D	Low risk Acceptable
H31	Collision with not cooperative traffic	Mid-air collision with other not cooperative manned or unmanned aircraft	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Provision of a secondary (redundant) LIDAR or infrared or SONAR sensors equipped collision avoidance system	2D	Low risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H32	Missed performance of avoidance collision maneuver	Missed performance of collision avoidance maneuver: for example due to primary collision avoidance system DAA failure or degraded functionality	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of secondary (with respect to DAA subsystem) LIDAR /SONAR on board the RPA	3D	Moderate risk Acceptable based on risk mitigation
H33	Missed monitoring of performance of avoidance collision maneuver	Missed monitoring of performance of avoidance collision maneuver example due to human error	Remote - 3	Hazardous - B	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Increase remote pilot training	1B	Low risk Acceptable
H34	Missed weather awareness capability	Missed access to weather information for the remote pilot causing decrease in his/her awareness of weather conditions	Improbable - 2	Hazardous - B	2B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Use of Flight Termination system (FTS)/ Use of parachute recovery system	2D	Low risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H35	Missed contingent weather information gathering	The human machine interface cannot enable the remote pilot to request weather specific to a current or future flight mission or cannot convey weather information to the remote pilot	Improbable - 2	Hazardous - B	2B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Increase on ground routine maintenance/ checks for weather information gathering HMI	1B	Low risk Acceptable
H36	Missed adverse weather avoidance	The pilot shall remotely enable the RPAS to avoid adverse weather performing the correct avoidance maneuver	Improbable - 2	Catastrophic - A	2A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provide support to the remote pilot with an onboard miniaturized weather Doppler RADAR	1B	Low risk Acceptable
Cross cutting functionalities related hazards											
H40	Loss of RPAS subsystems health and status monitoring	The RPAS health and status signals are not sent to ground	Improbable - 2	Hazardous - B	2B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Increase maintenance on ground	1B	Low risk Acceptable based on risk mitigation

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment
Airspace service: ATM
RPAS certified category operations
[Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H41	Loss of communication while transiting from LOS to BRLOS and vice versa	Loss of communication while transiting from LOS to BRLOS and vice versa due to physical obstacles (natural or man-made)	Extremely improbable - 1	Catastrophic - A	1A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	-	-	-
											-
H42	Unintentional radio link interference	Unintentional radio frequency interference of RPAS radio link due to other civil sources of electromagnetic signals (telecommunication, airport surveillance systems, etc.)	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Switch on redundant radio link band	1D	Low risk
											Acceptable
H43	Malicious radio link jamming	Intentional unlawful RF interference of RPAS radio - link	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant radio link using another radio frequency band /Use of Flight Termination system (FTS)/ Use of parachute recovery system	2D	Moderate risk
											Acceptable based on risk mitigation

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment
Airspace service: ATM
RPAS certified category operations
[Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H44	Malicious radio link spoofing	Intentional unlawful RF interference of RPAS radio - link	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant radio link using another radio frequency band /Use of Flight Termination system (FTS)/ Use of parachute recovery system	2D	Moderate risk Acceptable based on risk mitigation
Contingent hazards											
H42	Fire	Fire on board the RPAS	Extremely improbable - 1	Catastrophic - A	1A	Acceptable	Moderae risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Immediate flight termination using the Flight Termination system (FTS)	1E	Low risk Acceptable
H43	Loss of RPAS autopilot	Loss of autopilot functionality	Extremely improbable - 1	Catastrophic - A	1A	Acceptable	Moderae risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Switch on redundant autopilot/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	1E	Low risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment
Airspace service: ATM
RPAS certified category operations
[Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H44	Loss of electrical power	Loss electrical power generation	Extremely improbable - 1	Catastrophic - A	1A	Acceptable	Moderae risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Use of Flight Termination system (FTS)/ Use of parachute recovery system	1E	Low risk Acceptable
H45	Loss of inertial platform	Loss of all inertial references for navigation	Extremely improbable - 1	Hazardous - B	1B	Acceptable	Low risk	Acceptable	-	-	- -
H46	Loss of heading indication	Loss of heading indication for example caused by loss of inertial platform	Extremely improbable - 1	Hazardous - B	1B	Acceptable	Low risk	Acceptable	-	-	- -
H47	Loss of altitude indication	Loss of altitude indication; for example caused by altimeter failure	Extremely improbable - 1	Catastrophic - A	1A	Acceptable	Moderae risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Switch on redundant altimeter	1E	Low risk Acceptable
H48	Loss of airspeed indication	Loss of airspeed indication	Extremely improbable - 1	Hazardous - B	1B	Acceptable	Low risk	Acceptable	-	-	- -

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H49	Pressure sensors failure	Loss of absolute or differential pressure sensor	Extremely improbable - 1	Catastrophic - A	1A	Acceptable	Moderae risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Switch on redundant pressure sensor	4D	Low risk Acceptable
H50	Misleading altitude indication	Misleading altitude indication due to pressure sensor failure	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant altimeter	3D	Moderate risk Acceptable based on risk mitigation
H51	Misleading airspeed indication	Misleading airspeed indication due to pressure sensor failure	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Switch on redundant pressure sensors	3D	Moderate risk Acceptable based on risk mitigation

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H52	Misleading indication of the angle of incidence	Misleading angle of incidence indication due to pressure sensor failure	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Switch on redundant pressure sensor/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	2D	Low risk Acceptable
H53	Stall	Fixed wing RPAS stall caused by misleading instrumental indications or by remote pilot error	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Performance of diving maneuver/ Use of Flight Termination system (FTS)/ Use of parachute recovery system	3D	Moderate risk Acceptable based on risk mitigation
H54	Loss of fuel cell	Loss of fuel cell in an hybrid RPAS leading to degradation or loss of propulsion functionality and aircraft maneuverability and control during the flight	Improbable - 2	Catastrophic - A	2A	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Switch on LiPo batteries as redundant source of electrical power	2D	Low risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H55	Loss of fuel	Loss of fuel due to failure to fuel tank or pipelines	Remote - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination System (FTS)	4D	Moderate risk Acceptable based on risk mitigation
Human factor related hazards											
H56	Remote pilot low training	Lack or not appropriate remote pilot training	Remote - 3	Hazardous - B	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Increase/ improve remote pilot training	2D	Low risk Acceptable
H57	Non-compliant operational procedures	Lack of compliant operational procedures, check-lists, etc.	Remote - 3	Hazardous - B	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Provision of operational procedures, check-lists, etc.	2D	Low risk Acceptable
H58	Remote pilot loss of situational awareness	Loss of remote pilot situational awareness	Remote - 3	Hazardous - B	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.	Increase remote pilot training	2D	Low risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment
Airspace service: ATM
RPAS certified category operations
[Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H59	Human senses limitations	Limitations of human senses due to the fact that the remote pilot is on ground and not on board the aircraft and he/she has to use sensors and not his/her 'senses'	Occasional - 4	Catastrophic - A	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Increase remote pilot training	3D	Moderate risk Acceptable based on risk mitigation
H60	Remote pilot excessive workload	Excessive remote pilot workload	Occasional - 4	Major - C	4C	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Increase remote pilot training	3E	Low risk Acceptable
H61	Loss of separation provision from the ATC	The separation provision instructions are no longer being provided from ATC, specifically to the Pilot. It is not loss of air traffic control to all air traffic. It is assumed that in this scenario the remote pilot will follow standard procedures in the event of loss of communications	Remote - 3	Hazardous - B	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Provision of DAA/LIDAR sensor on board the RPA against mid-air conflict/collision risks	3E	Low risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment
Airspace service: ATM
RPAS certified category operations
[Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]

Hazard	Definition	Description	Safety risk probability	Safety risk severity	Safety risk assessment	Tolerance	Risk range description	Recommended action	Mitigation factors	Residual risk	
H62	Loss of separation provision from the remote pilot	Loss of separation provision from the remote pilot	Occasional - 4	Hazardous - B	4B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of DAA/LIDAR sensor on board the RPA against mid-air conflict/collision risks	4D	Moderate risk Acceptable based on risk mitigation
H63	Erroneous separation provision instruction from ATC	Provision of erroneous separation instruction from ATC	Exremely improbable - 1	Hazardous - B	1B	Acceptable	Low risk	Acceptable	-	-	- -
H64	Erroneous execution of the separation provision instruction from the remote pilot	The remote pilot does not follow correctly the ATC instruction provision	Occasional - 4	Hazardous - B	4B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Provision of DAA/LIDAR sensor on board the RPA against mid-air conflict/collision risks /Increase remote pilot training	4E	Low risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H65	The RPAS does not comply or incorrectly responds to separation provision instruction issued by ATC	RPAS response to ATC instructions is not as expected	Remote - 3	Catastrophic - A	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Use of Flight Termination system (FTS)/ Use of parachute recovery system	3D	Moderate risk Acceptable based on risk mitigation
H66	Remote pilot delayed response to separation instruction provision from ATC	Remote pilot delayed response to separation provision instruction from ATC causing ATC workload increase	Occasional - 4	Major - C	4C	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Increase remote pilot training	3E	Low risk Acceptable
H67	Excessive number of intentional deviations from separation provision instruction	Excessive number of intentional deviations from separation provision instruction (for genuine reasons like weather and similar and not for malicious intentions)	Frequent - 5	Major - C	5C	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Increase remote pilot training	3C	Moderate risk Acceptable based on risk mitigation

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H68	Missed submission of flight plan to ATC	Missed submission of flight plan to ATC from the remote pilot	Occasional - 4	Hazardous - B	4B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Increase remote pilot training	3B	Moderate risk Acceptable based on risk mitigation
Weather related hazards											
H69	Cloud cover	Weather hazard	Frequent - 5	Negligible – E *(IFR flights)*	5E	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Flight mission interruption and application of the "Return to Home" function	5E	Moderate risk Acceptable based on risk mitigation
				Minor – D *(VFR flights)*	5D	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Flight mission interruption and application of the "Return to Home" function	5E	Moderate risk Acceptable based on risk mitigation

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H70	Fog	Weather hazard	Occasional - 4	Negligible – E *(IFR flights)*	4E	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Flight mission interruption and application of the "Return to Home" function	4E	Moderate risk Acceptable based on risk mitigation
				Minor – D *(VFR flights)*	4D	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Flight mission interruption and application of the "Return to Home" function	4E	Moderate risk Acceptable based on risk mitigation
H71	Freezing rain	Weather hazard	Remote - 3	Catastrophic – A (IFR/VFR flights)	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Flight mission interruption and application of the "Return to Home" function	3E	Low risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H72	Glare	Weather hazard	Occasional - 4	Negligible – E (IFR/VFR flights)	4E	Acceptable	Moderate risk	-	-	-	-
H73	Haze	Weather hazard	Occasional - 4	Negligible – E (IFR flights)	4E	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Flight mission interruption and application of the "Return to Home" function	4E	Moderate risk
											Acceptable based on risk mitigation
				Minor – D *(VFR flights)*	4D	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Flight mission interruption and application of the "Return to Home" function	4E	Moderate risk
											Acceptable based on risk mitigation
H74	Humidity	Weather hazard	Frequent - 5	Negligible – E (IFR/VFR flights)	5E	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	-	-	-
											-

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H75	Ice	Weather hazard	Occasional - 4	Catastrophic - A (IFR/VFR flights)	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	4E	Moderate risk Acceptable
H76	Rain	Weather hazard	Frequent - 5	Hazardous – B (IFR/VFR flights)	5B	Unacceptable	High risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Provision of an on board miniaturized weather Doppler RADAR to identify the weather hazard and application of the "Return to Home" function	5E	Moderate risk Acceptable
H77	Snow	Weather hazard	Frequent - 5	Hazardous – B (IFR/VFR flights)	5B	Unacceptable	High risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Provision of an on board miniaturized weather Doppler RADAR to identify the weather hazard and application of the "Return to Home" function	5E	Moderate risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H78	Solar storms	Weather hazard	Remote - 3	Hazardous – B (IFR/VFR flights)	3B	Acceptable	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable	Use 'Return to Home" function	3E	Low risk Acceptable
H79	Temperature	Weather hazard	Frequent - 5	Negligible – D (IFR/VFR flights)	5E	Acceptable	Moderate risk	-	-	-	- -
H80	Turbulence	Weather hazard	Occasional - 4	Hazardous – B (IFR/VFR flights)	4B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	4E	Moderate risk Acceptable
H81	Wind	Weather hazard	Frequent - 5	Hazardous – B (IFR/VFR flights)	5B	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	5E	Moderate risk Acceptable
H82	Lightening strike	Weather hazard	Occasional - 4	Catastrophic – A (IFR/VFR flights)	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	4E	Moderate risk Acceptable

Table 144 – ATM safety risk matrix (Cont'd)

Safety risk assessment Airspace service: ATM RPAS certified category operations [Flight limitations: 0 Ft. < h < 500 Ft.; 500 Ft. < h < FL600, h > FL 600; VFR/IFR; Weight: 150 kg < MTOW < 600 kg (MALE class)]											
Hazard	**Definition**	**Description**	**Safety risk probability**	**Safety risk severity**	**Safety risk assessment**	**Tolerance**	**Risk range description**	**Recommended action**	**Mitigation factors**	**Residual risk**	
H83	Hail	Weather hazard	Occasional - 4	Catastrophic – A (IFR/VFR flights)	4A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	4E	Moderate risk Acceptable
H84	Hurricanes	Weather hazard	Remote - 3	Catastrophic – A (IFR/VFR flights)	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	3E	Low risk Acceptable
H85	Volcanic ash	Remote - 3	Remote - 3	Catastrophic – A (IFR/VFR flights)	3A	Unacceptable	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.	Mission not to be performed due to less than optimal operational conditions	3E	Low risk Acceptable

Appendix E - Barriers and mitigation factors - The Bow Tie analysis – Results

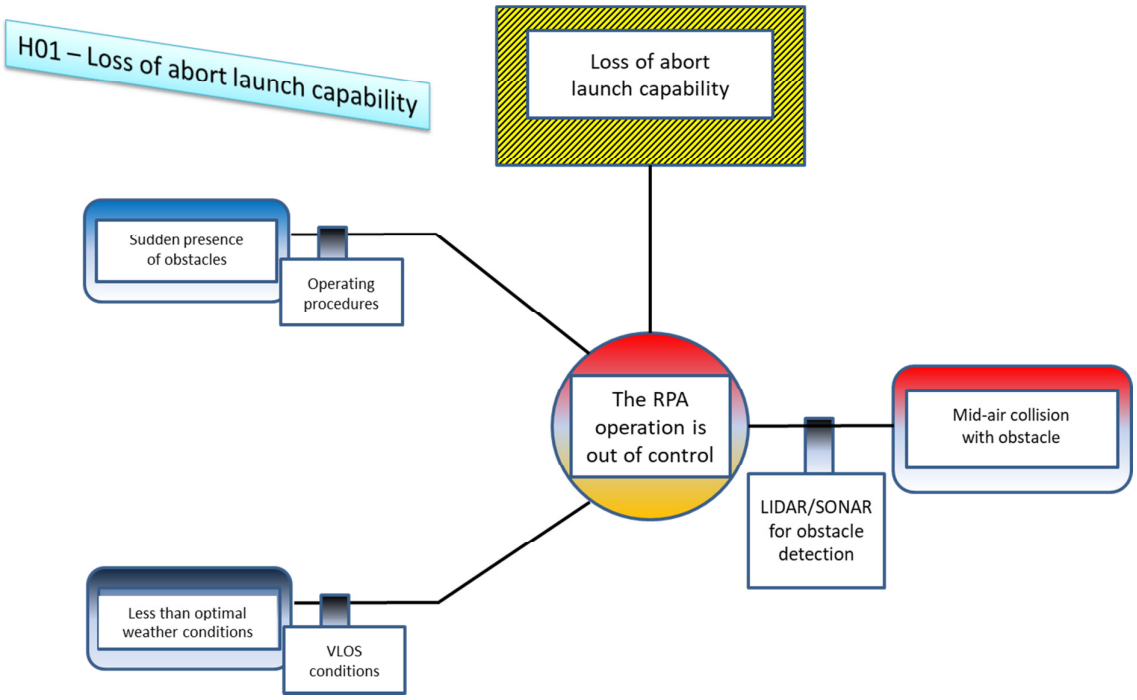


Figure 61 – Bow Tie depiction of hazard H01

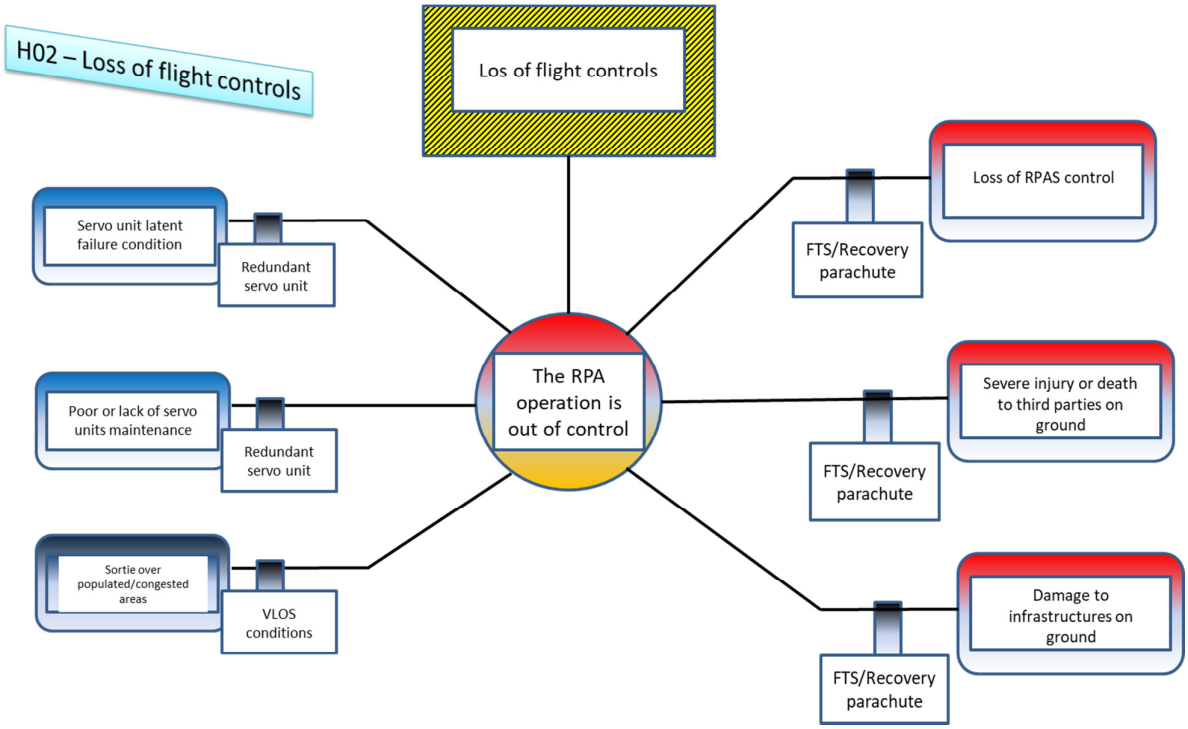


Figure 62 – Bow Tie depiction of hazard H02

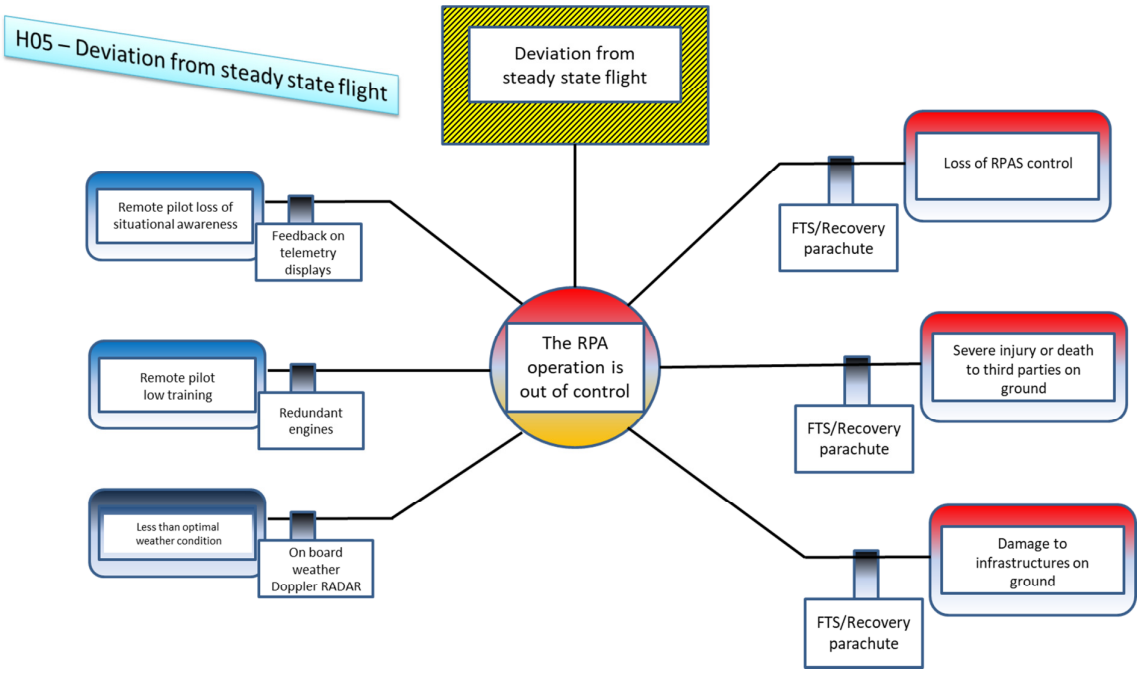


Figure 63 - Bow Tie depiction of hazard H05

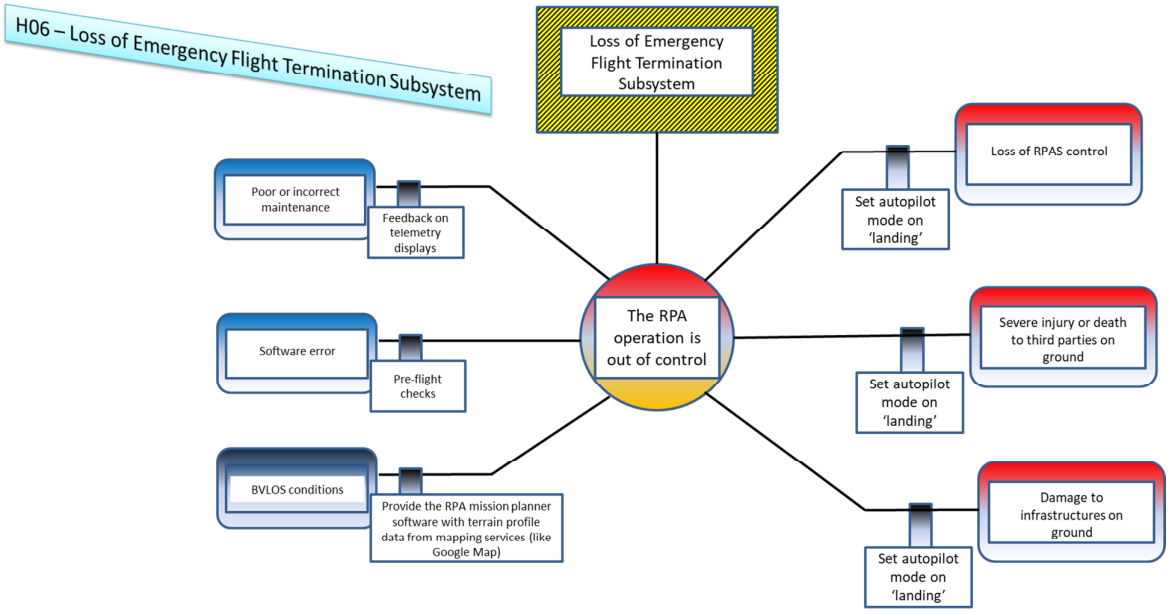


Figure 64 - Bow Tie depiction of hazard H06

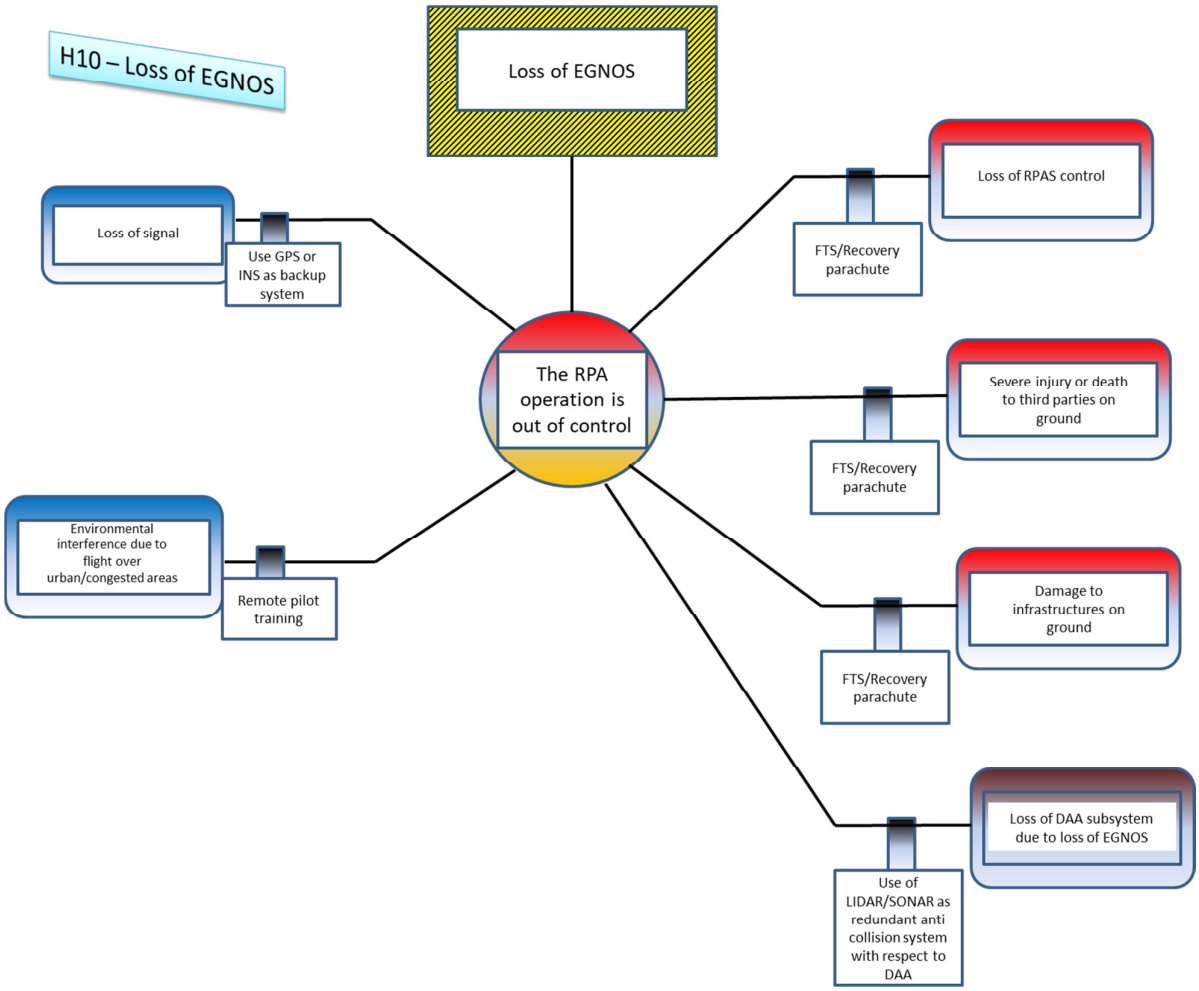


Figure 65 - Bow Tie depiction of hazard H10

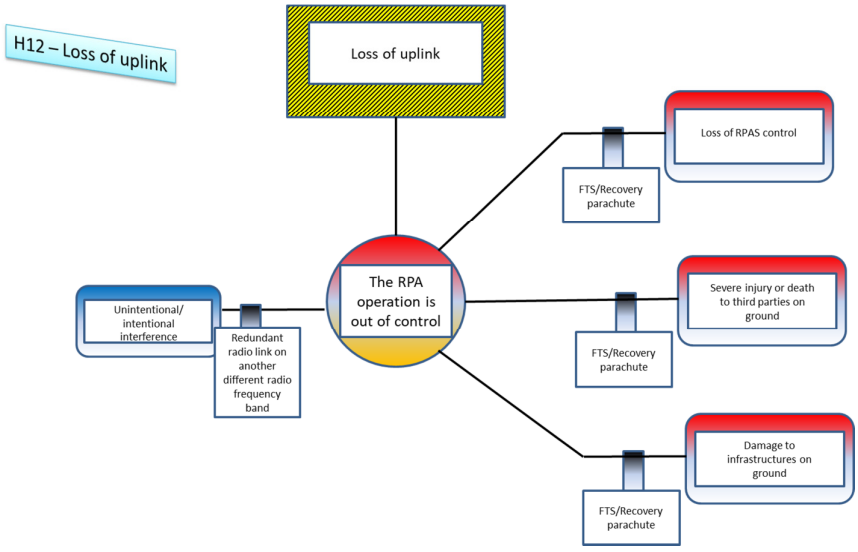


Figure 66 - Bow Tie depiction of hazard H12

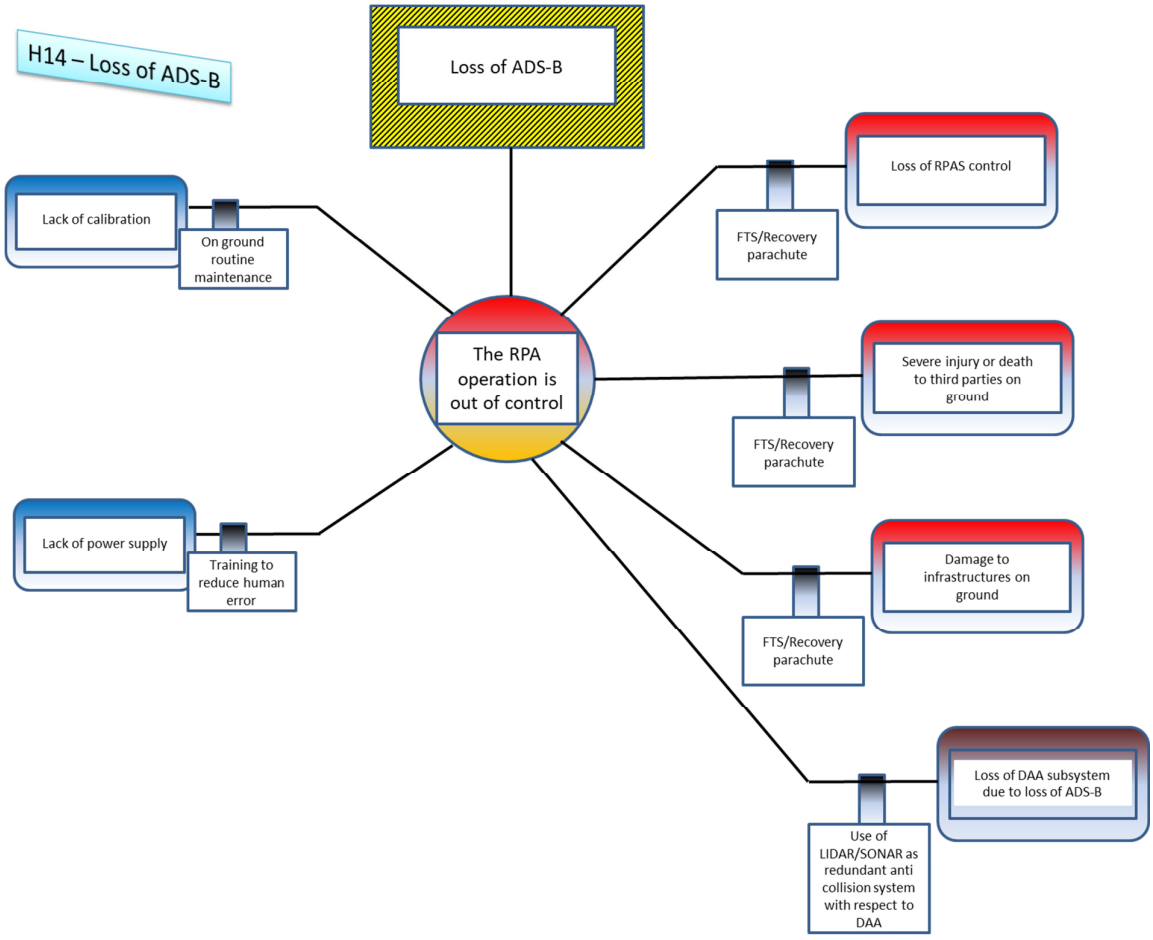


Figure 67 - Bow Tie depiction of hazard H14

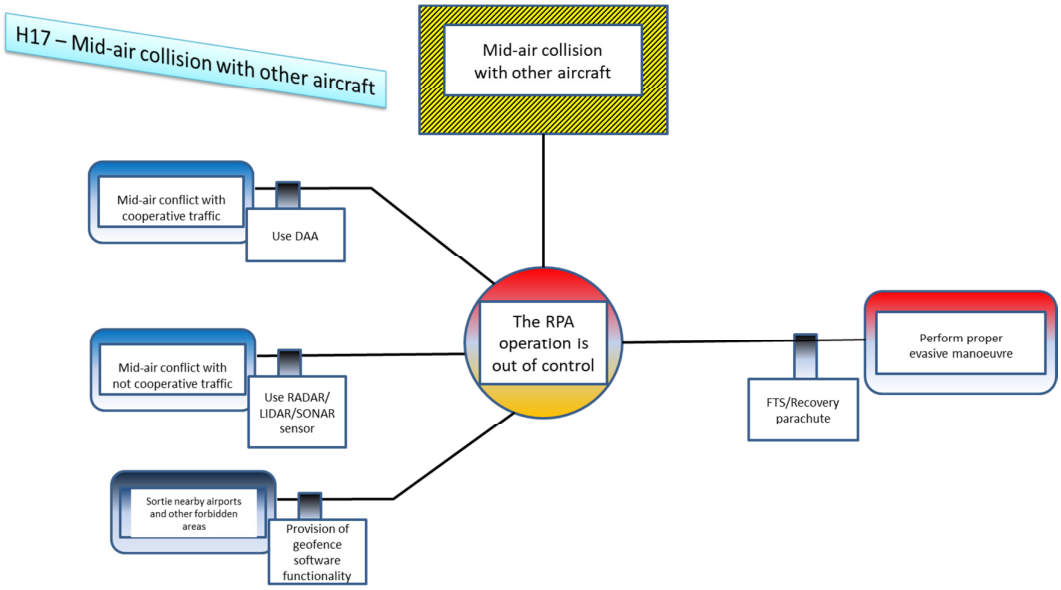


Figure 68 - Bow Tie depiction of hazard H17

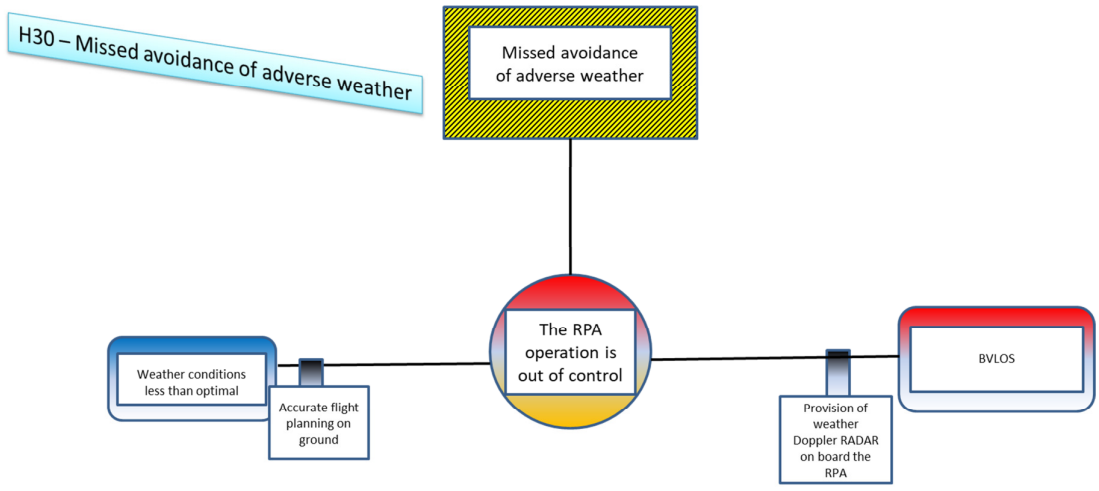


Figure 69 - Bow Tie depiction of hazard H30

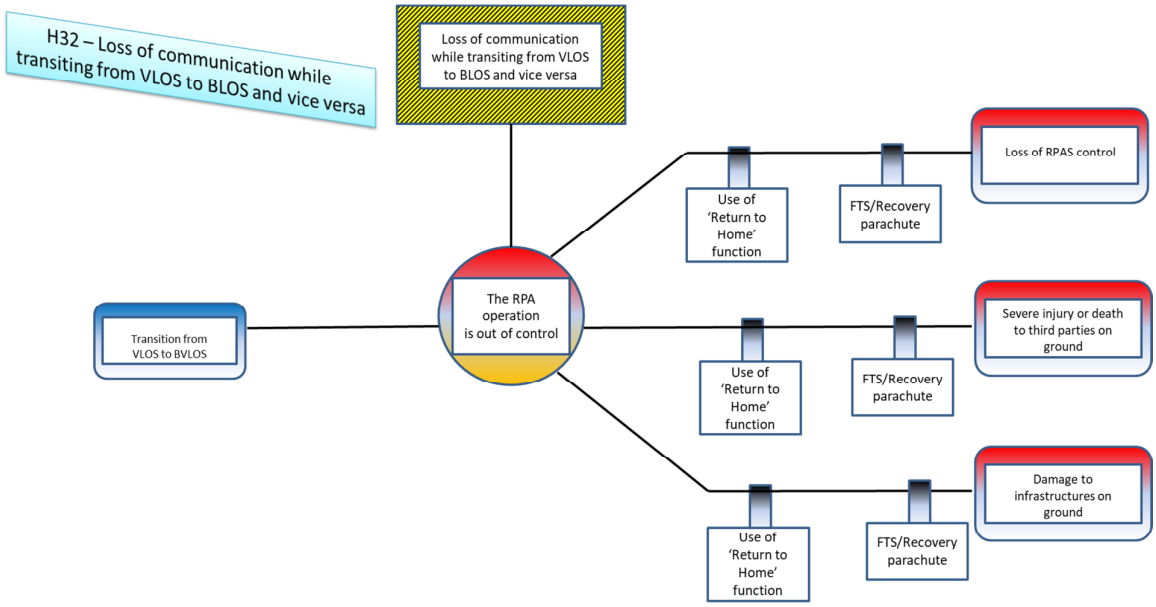


Figure 70 - Bow Tie depiction of hazard H32

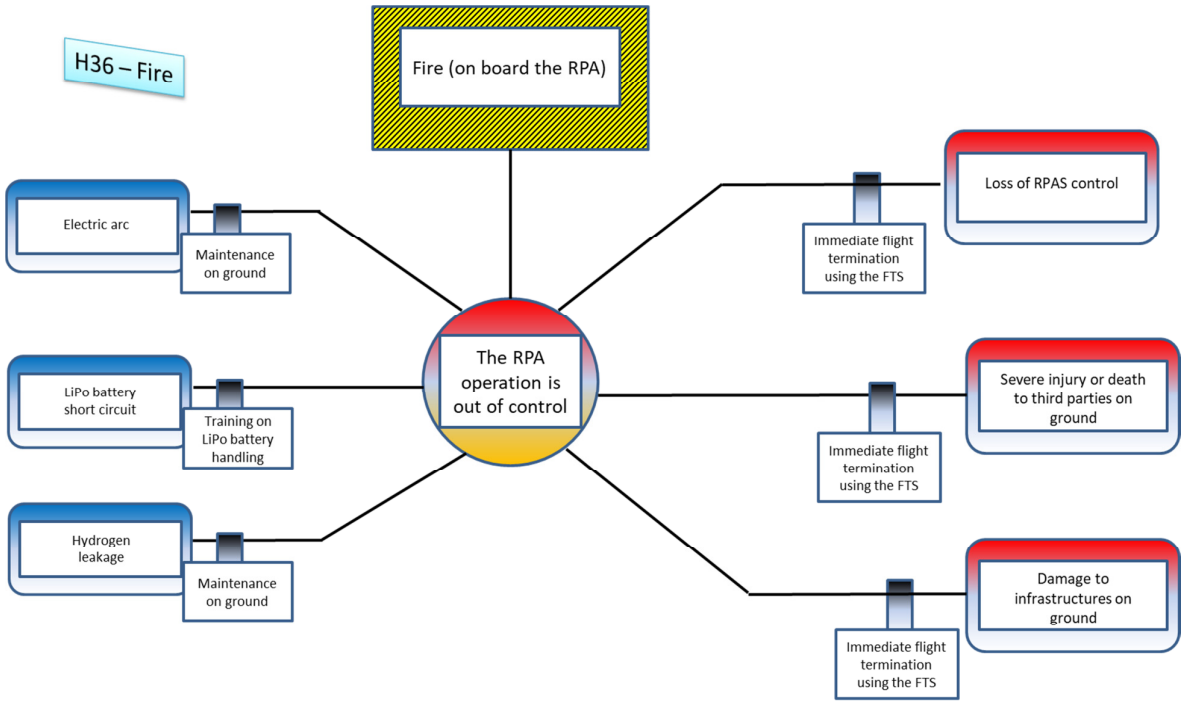


Figure 71 - Bow Tie depiction of hazard H36

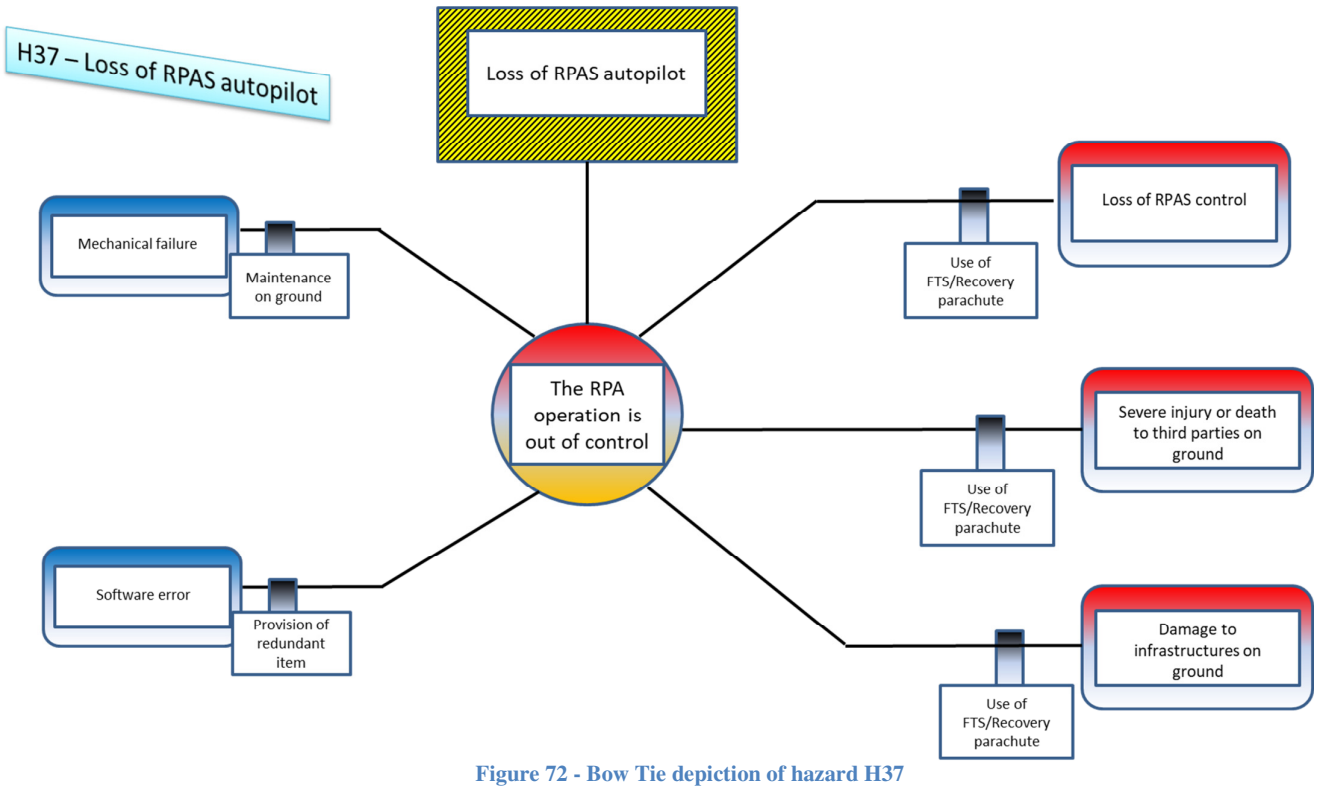


Figure 72 - Bow Tie depiction of hazard H37

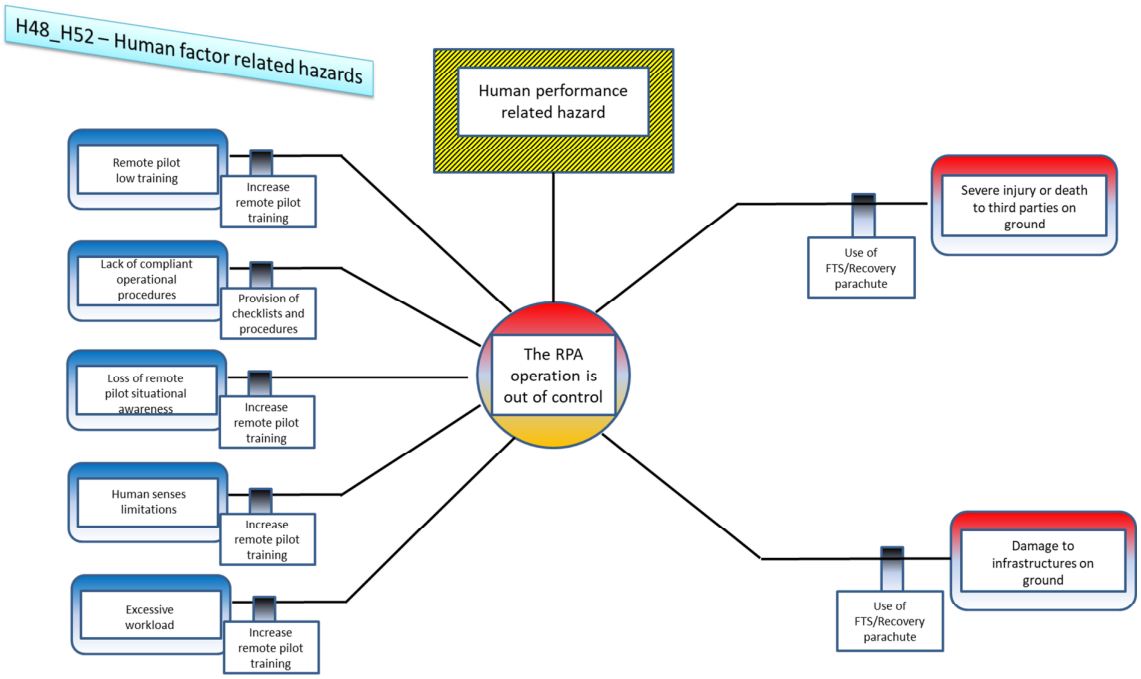


Figure 73 - Bow Tie depiction of an example of human factor/performance related hazard

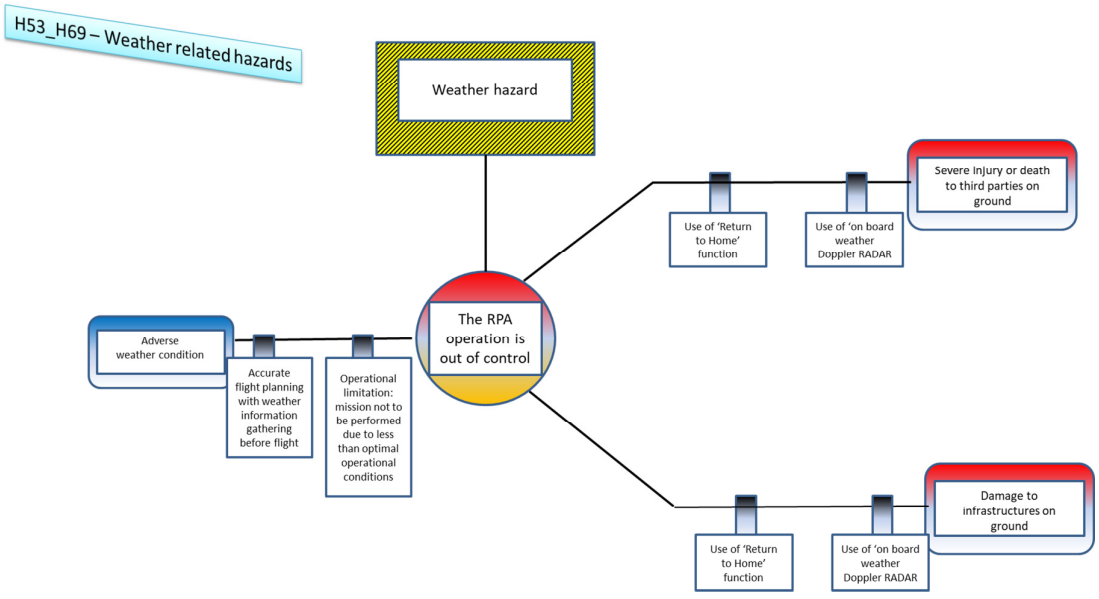


Figure 74 - Bow Tie depiction of an example of weather related hazard

Appendix F - The expert system logical - Results

Expert System: RPAS U-space Risk Matrix

Hypotheses:
- Light RPAS: 25 kg < MTOW < 150 kg
- Propulsion subsystem: Hybrid powered electric rotor engines

List of variables and definition:

IRGRC = INTRINSIC RPAS GROUND RISK CLASS:
- IRGRC = 1 → LOW GROUND RISK
- IRGRC > 1 → HIGH GROUND RISK

INTRINSIC RPAS GROUND RISK CLASS:

Table 145 - Intrinsic Ground Risk Class (FROM JARUS SORA) → IRGRC [68]				
RPAS Max characteristic dimension	1 m (~ 3 feet)	3 m (~ 10 feet)	8 m (~ 25 feet)	> 8 m (~ 25 feet)
Typical expected kinetic energy	< 700 J	< 34000 J	< 1084 kJ	> 1084 kJ
Operational scenario				
RLOS over controlled area, located inside a sparsely populated environment	1	2	3	5
BRLOS over sparsely populated environment (over-flown areas uniformly inhabited)	2	3	4	6
RLOS over controlled area, located inside a populated environment	3	4	6	8
RLOS over populated environment	4	5	7	9
BRLOS over controlled area, located inside a populated environment	5	6	8	10
BRLOS over populated environment	6	7	9	11
RLOS over gathering of people	7			
BRLOS over gathering of people	8			

Table 146 - ‘Expert System’ knowledge basis rules variables
RPAS_ALT = RPAS Altitude, measured in ‘feet’ by the altimeter
RPAS_ENGINE_OMEGA = RPAS electric engine angular speed measured in radians per second
RPAS_RATE_OF_CLIMB = RPAS vertical rate of climb, measured in ‘feet per second’
RPAS_LIDAR_SENSOR_OUTPUT = RPAS LIDAR anti-collision RADAR sensor output
RPAS_AUTOPILOT_ABORT_LAUNCH_MODE = RPAS autopilot abort take-off/launch mode
RPAS_RECOVERY_PARACHUTE_CMD = Command signal to activate the RPAS recovery parachute
PITCH_CMD = Pitch command sent from ground to the RPA
RPAS_PITCH_ANGLE = RPAS attitude pitch angle, measured in degrees
ROLL_CMD = Roll command sent from ground to the RPA
RPAS_ROLL_ANGLE = RPAS attitude roll angle, measured in degrees
YAW_CMD = Yaw command sent from ground to the RPA
RPAS_YAW_ANGLE = RPAS attitude yaw angle, measured in degrees
RPAS_LIPO_BATTERY_CURRENT = Current from a LiPo battery to feed all the other electric loads (engines included)
RPAS_FTS_CMD = Command signal to activate the RPAS ‘Flight Termination System’
RPAS_ESC_FAILURE_SENSOR = Electronic Speed Control failure sensor
PITCH_CMD_LONGITUDINAL_SHIFT = Longitudinal shift of pitch stick
PITCH_CMD_ELECTRICAL_SIGNAL = Electrical signal generated by the pitch stick as soon as a shift of the stick is performed by the remote pilot on ground
ROLL_CMD_LONGITUDINAL_SHIFT = Lateral shift of pitch stick
ROLL_CMD_ELECTRICAL_SIGNAL = Electrical signal generated by the pitch stick as soon as a lateral shift of the stick is performed by the remote pilot on ground
IF YAW_CMD_DIRECTIONAL_SHIFT = Directional shift of the yaw command (pedals/lever switch)
YAW_CMD_ELECTRICAL_SIGNAL = electrical signal generated by the pedal as soon as a shift of the stick is performed by the remote pilot on ground (pedals/lever switch)
WP_ALT = Altitude of a given RPAS route waypoint, measured in meters
RPAS_IAS = RPAS indicated airspeed
RPAS_FTS_BIT = The ‘Built in Test’ functionality embedded in the RPAS ‘Flight Termination System’
RPAS_AUTOPILOT_LANDING_MODE = RPAS autopilot landing mode
RPAS_RECOVERY_PARACHUTE_BIT = The ‘Built in Test’ functionality embedded in the RPAS ‘Recovery Parachute System’
RPAS_AUTOPILOT_RETURN_TO_HOME_MODE = RPAS autopilot return to home mode to safely recover the RPAS following a predefined procedure
RPAS_MISSION_PLAN = RPAS mission plan management software functionality
GPS_LAT = The spatial position latitude coordinate provided by the Global Positioning Service for civilian applications
GPS_LONG = The spatial position longitude coordinate provided by the Global Positioning Service for civilian applications
GPS_ALT = The spatial position altitude coordinate provided by the Global Positioning Service for civilian applications
EGNOS_LAT = The spatial position latitude coordinate provided by GALILEO EGNOS service for civilian aerospace applications

Table 147 - 'Expert System' knowledge basis rules variables (Cont'd)
EGNOS_LONG = The spatial position longitude coordinate provided by GALILEO EGNOS service for civilian aerospace applications
EGNOS_LONG = The spatial position altitude coordinate provided by GALILEO EGNOS service for civilian aerospace applications
DOWNLINK_RPAS_LAT = The RPA current latitude spatial coordinate measured on board and sent to the ground telemetry monitoring displays via the downlink channel
DOWNLINK_RPAS_LONG = The RPA current longitude spatial coordinate measured on board and sent to the ground telemetry monitoring displays via the downlink channel
DOWNLINK_RPAS_ALT = The RPA current altitude spatial coordinate measured on board and sent to the ground telemetry monitoring displays via the downlink channel
PLANNED_WP_LAT = The expected RPA latitude spatial coordinate value according to the given flight mission plan
PLANNED_WP_LONG = The expected RPA longitude spatial coordinate value according to the given flight mission plan
PLANNED_WP_ALT = The expected RPA altitude spatial coordinate value according to the given flight mission plan
RPAS_UPLINK_PATH_LOSS = Loss of the signal path sent from ground on the uplink channel to manage the aircraft
RPAS_ADS-B_BIT = The 'Built in Test' functionality embedded in the ADS-B
RPAS_DISTANCE_FROM_OBSTACLE = RPAS distance from the detected fixed (natural or man-made)or moving obstacle (cooperative or not cooperative aerial traffic)
THRESHOLD_DISTANCE = It is the distance from the obstacle less than which the evasive manoeuver is recommended
MINIMAL_DISTANCE = = It is the distance from the obstacle beyond which the evasive manoeuver shall be commanded
RPAS_LIDAR_SENSOR_OUTPUT = LIDAR sensor indication of the detected obstacle (nature or man-made obstacle or not cooperative air traffic)
DAA_OUTPUT = DAA indication of the detected obstacle cooperative air traffic
RPAS_ADS-B_BIT = It is the 'Built in Test' functionality embedded in the ADS-B transponder
EGNOS_BIT = The 'Built in Test' functionality embedded in the EGNOS spatial position service provider
RPAS_ALTIMETER_BIT = The 'Built in Test' functionality embedded in the altimeter WEATHER_DOPPLER_RADAR_BIT = It is the 'Built in Test' functionality embedded in the weather Doppler RADAR installed on the RPAS for contingent weather awareness
HEALTH_AND_STATUS_MONITORING_BIT = It is the 'Built in Test' functionality embedded in the Health and Status monitoring subsystem installed on the RPAS
RPAS_RANGE = It is the distance between the flying RPAS and the GCS/Hand held portable device covered by the radio link
RPAS_RANGE_RLOS = It is the RPAS range under 'Visual Line of sight condition'
RPAS_FIRE_WARNING = It is the signal to warn the remote pilot that a fire is occurring on board the RPA
RPAS_AUTOPILOT_FAILURE_WARNING = It is the signal to warn the remote pilot the RPA autopilot is in failure
RPAS_IMU_BIT = It is the 'built in test' functionality of the Inertial Measurement Unit installed on board the RPAS

Table 147 - 'Expert System' knowledge basis rules variables (Cont'd)
RPAS_HDG1 and RPAS_HDG2 = The two different heading indications that feed flight instruments on ground to warn the remote pilot if the flight parameter is correct or not
RPAS_ALT1 and RPAS_ALT2 = The two different altitude indications that feed flight instruments on ground to warn the remote pilot if the flight parameter is correct or not
RPAS_PSR1 and RPAS_PSR2 = The two different pressure sensor indications that feed two ground flight instruments on ground to warn the remote pilot if the flight parameter is correct or not
RPAS_IAS1 and RPAS_IAS2 = The different indicated airspeed indications that feed two ground flight instruments on ground to warn the remote pilot if the flight parameter is correct or not
RPAS_FUEL_CELL_CURRENT = It is the intensity of the electric current generated by the fuel cell installed on board the hybrid RPAS
WEATHER_DOPPLER_RADAR_IMAGE = It is the meteorological condition recorded by the Weather Doppler RADAR and indicated on board the RPAS

KNOWLEDGES BASIS RULES

H01 – Loss of abort launch capability

Definition: the contingent loss of abort launch capability when conditions for take-off are recognised to be less than optimal

Rule number 1
IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO radians/sec
AND IF RPAS_RATE_OF_CLIMB IS GREATER TO ZERO m/s
AND IF RPAS_LIDAR_SENSOR_OUTPUT IS OBSTACLE
AND IF RPAS_AUTOPILOT_ABORT_LAUNCH_MODE = FAILED
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF ABORT LAUNCH CAPABILITY HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF ABORT LAUNCH CAPABILITY MODERATE RISK'

Rule number 2
IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO radians/sec
AND IF RPAS_RATE_OF_CLIMB IS GREATER TO ZERO m/s
AND IF RPAS_LIDAR_SENSOR_OUTPUT IS OBSTACLE
AND IF RPAS_AUTOPILOT_ABORT_LAUNCH_MODE = FAILED
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF ABORT LAUNCH CAPABILITY HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE

Printout ‘LOSS OF ABORT LAUNCH CAPABILITY MODERATE RISK’
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout ‘MODERATE RISK’

H02 – Loss of flight controls

Definition: the contingent partial or complete loss of flight control functionality during flight

Rule number 1
IF PITCH_CMD IS DIFFERENT FROM ZERO
AND IF $RPAS\_PITCH\_ANGLE_{t+1}$ – $RPAS\_PITCH\_ANGLE_{t}$ IS EQUAL TO ZERO degree
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO radians/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout ‘LOSS OF FLIGHT CONTROLS HIGH RISK’
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout ‘LOSS OF FLIGHT CONTROLS MODERATE RISK’

Rule number 2
IF PITCH_CMD IS DIFFERENT FROM ZERO
AND IF $RPAS\_PITCH\_ANGLE_{t+1}$ – $RPAS\_PITCH\_ANGLE_{t}$ IS EQUAL TO ZERO degree
AND IF $RPAS\_ENGINE\_OMEGA_{n}$ IS GREATER THAN ZERO radians/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS EQUAL TO ONE
Printout ‘LOSS OF FLIGHT CONTROLS HIGH RISK’
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout ‘LOSS OF FLIGHT CONTROLS MODERATE RISK’

Rule number 3
IF ROLL_CMD IS DIFFERENT FROM ZERO
AND IF $RPAS\_ROLL\_ANGLE_{t+1}$ – $RPAS\_ROLL\_ANGLE_{t}$ IS EQUAL TO ZERO degree
AND IF $RPAS\_ENGINE\_OMEGA_{n}$ IS GREATER THAN ZERO radians/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout ‘LOSS OF FLIGHT CONTROLS HIGH RISK’
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout ‘LOSS OF FLIGHT CONTROLS MODERATE RISK’

Rule number 4
IF ROLL_CMD IS DIFFERENT FROM ZERO
AND IF $RPAS\_ROLL\_ANGLE_{t+1}$ – $RPAS\_ROLL\_ANGLE_{t}$ IS EQUAL TO ZERO degree
AND IF $RPAS\_ENGINE\_OMEGA_{n}$ IS GREATER THAN ZERO radians/sec

AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF FLIGHT CONTROLS HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF FLIGHT CONTROLS MODERATE RISK'

Rule number 5
IF YAW_CMD IS DIFFERENT FROM ZERO
AND IF $RPAS\_YAW\_ANGLE_{t+1}$ – $RPAS\_YAW\_ANGLE_{t}$ IS EQUAL TO ZERO degree
AND IF $RPAS\_ENGINE\_OMEGA_{n}$ IS GREATER THAN ZERO radians/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF FLIGHT CONTROLS HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF FLIGHT CONTROLS MODERATE RISK'

Rule number 6
IF YAW_CMD IS DIFFERENT FROM ZERO
AND IF $RPAS\_YAW\_ANGLE_{t+1}$ – $RPAS\_YAW\_ANGLE_{t}$ IS EQUAL TO ZERO degree
AND IF $RPAS\_ENGINE\_OMEGA_{n}$ IS GREATER THAN ZERO radians/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF FLIGHT CONTROLS HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF FLIGHT CONTROLS MODERATE RISK'

Note:
Where 't' is time measured in seconds
Where 'n' is each electric rotor engine

H03 – Loss of propulsion
Definition: the contingent partial or complete loss of propulsion functionality during flight

Rule number 1
IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF $RPAS\_ENGINE\_OMEGA_{t+1}$ – $RPAS\_ENGINE\_OMEGA_{t}$ IS SMALLER THAN ZERO radians/sec
AND IF $RPAS\_LIPO\_BATTERY\_CURRENT_{i}$ IS EQUAL TO ZERO Ampere
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF PROPULSION HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF PROPULSION MODERATE RISK'

Rule number 2
IF RPAS_ALT IS GREATER THAN ZERO feet

AND IF $RPAS\_ENGINE\_OMEGA_{t+1}$ - $RPAS\_ENGINE\_OMEGA_{t}$ IS SMALLER THAN ZERO radians/sec
AND IF $RPAS\_LIPO\_BATTERY\_CURRENT_{i}$ IS EQUAL TO ZERO Ampere
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF PROPULSION HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF PROPULSION MODERATE RISK'

Rule number 3
IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF $RPAS\_LIPO\_BATTERY\_CURRENT_{i}$ IS GREATER THAN ZERO Ampere
AND IF RPAS_ESC_FAILURE_SENSOR IS EQUAL TO FAILED
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF PROPULSION HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF PROPULSION MODERATE RISK'

Rule number 4
IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF $RPAS\_LIPO\_BATTERY\_CURRENT_{i}$ IS GREATER THAN ZERO Ampere
AND IF RPAS_ESC_FAILURE_SENSOR IS EQUAL TO FAILED
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF PROPULSION HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF PROPULSION MODERATE RISK'

Where 't' is time measured in seconds
Where 'n' is each electric rotor engine
Where 'i' is each LiPo battery

H04 – Loss of GCS Human Machine Interface

Definition: the contingent loss of human machine interface to generate flight command signals on ground (in the Ground Control Station or on a hand held portable device)

Rule number 1
IF PITCH_CMD_LONGITUDINAL_SHIFT IS DIFFERENT FROM ZERO
AND PITCH_CMD_ELECTRICAL_SIGNAL IS EQUAL TO ZERO
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF $RPAS\_ENGINE\_OMEGA_{n}$ IS GREATER THAN ZERO radians/sec
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF GCS HMI HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF GCS HMI MODERATE RISK'

Rule number 2

IF PITCH_CMD_LONGITUDINAL_SHIFT IS DIFFERENT FROM ZERO
AND PITCH_CMD_ELECTRICAL_SIGNAL IS EQUAL TO ZERO
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF RPAS_ENGINE_OMEGA$_n$ IS GREATER THAN ZERO radians/sec
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF GCS HMI HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF GCS HMI MODERATE RISK'

Rule number 3
IF ROLL_CMD_LATERAL_SHIFT IS DIFFERENT FROM ZERO
AND ROLL_CMD_ELECTRICAL_SIGNAL IS EQUAL TO ZERO
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF RPAS_ENGINE_OMEGA$_n$ IS GREATER THAN ZERO radians/sec
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF GCS HMI HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF GCS HMI MODERATE RISK'

Rule number 4
IF ROLL_CMD_LATERAL_SHIFT IS DIFFERENT FROM ZERO
AND ROLL_CMD_ELECTRICAL_SIGNAL IS EQUAL TO ZERO
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF RPAS_ENGINE_OMEGA$_n$ IS GREATER THAN ZERO radians/sec
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF GCS HMI HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF GCS HMI MODERATE RISK'

Rule number 5
IF YAW_CMD_DIRECTIONAL_SHIFT IS DIFFERENT FROM ZERO
AND YAW_CMD_ELECTRICAL_SIGNAL IS EQUAL TO ZERO
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF RPAS_ENGINE_OMEGA$_n$ IS GREATER THAN ZERO radians/sec
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF GCS HMI HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF GCS HMI MODERATE RISK'

Rule number 6
IF YAW_CMD_DIRECTIONAL_SHIFT IS DIFFERENT FROM ZERO
AND YAW_CMD_ELECTRICAL_SIGNAL IS EQUAL TO ZERO
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF RPAS_ENGINE_OMEGA$_n$ IS GREATER THAN ZERO radians/sec
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF GCS HMI HIGH RISK'
=>

THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout ‘LOSS OF GCS HMI MODERATE RISK’

Note:
Where ‘t’ is time measured in seconds

H05 – Deviation from steady-state (not-accelerating) flight condition
Definition: the contingent loss of RPAS capability to maintain constant indicated airspeed and altitude flight conditions

Rule number 1
IF WP_ALT_{t+1} – WP_ALT_{t} IS EQUAL TO ZERO meters
AND IF $RPAS\_IAS_{t+1}$ – $RPAS\_IAS_{t}$ IS SMALLER THAN ZERO kts
AND IF IRGRC IS GREATER THAN ONE
Printout ‘DEVIATION FROM STEADY-STATE CONDITION HIGH RISK’
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout ‘DEVIATION FROM STEADY-STATE CONDITION MODERATE RISK’

Rule number 2
IF WP_ALT_{t+1} – WP_ALT_{t} IS EQUAL TO ZERO meters
AND IF $RPAS\_IAS_{t+1}$ – $RPAS\_IAS_{t}$ IS GREATER THAN ZERO kts
AND IF IRGRC IS EQUAL TO ONE
Printout ‘DEVIATION FROM STEADY-STATE CONDITION HIGH RISK’
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout ‘DEVIATION FROM STEADY-STATE CONDITION MODERATE RISK’

Rule number 3
IF WP_ALT_{t+1} – WP_ALT_{t} IS EQUAL TO ZERO meters
AND IF $RPAS\_IAS_{t+1}$ – $RPAS\_IAS_{t}$ IS GREATER THAN ZERO kts
AND IF IRGRC IS GREATER THAN ONE
Printout ‘DEVIATION FROM STEADY-STATE CONDITION HIGH RISK’
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout ‘DEVIATION FROM STEADY-STATE CONDITION MODERATE RISK’

Rule number 4
IF WP_ALT_{t+1} – WP_ALT_{t} IS EQUAL TO ZERO meters
AND IF $RPAS\_IAS_{t+1}$ – $RPAS\_IAS_{t}$ IS GREATER THAN ZERO kts
AND IF IRGRC IS EQUAL TO ONE
Printout ‘DEVIATION FROM STEADY-STATE CONDITION HIGH RISK’
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout ‘DEVIATION FROM STEADY-STATE CONDITION MODERATE RISK’

Rule number 5
IF $RPAS\_IAS_{t+1}$ – $RPAS\_IAS_{t}$ IS EQUAL TO ZERO kts
AND IF $RPAS\_ALT_{t+1}$ – $RPAS\_ALT_{t}$ IS SMALLER THAN ZERO meters

AND IF IRGRC IS GREATER THAN ONE
Printout 'DEVIATION FROM STEADY-STATE CONDITION HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'DEVIATION FROM STEADY-STATE CONDITION MODERATE RISK'

Rule number 6
IF $RPAS\_IAS_{t+1}$ – $RPAS\_IAS_t$ IS EQUAL TO ZERO kts
AND IF $RPAS\_ALT_{t+1}$ – $RPAS\_ALT_t$ IS SMALLER THAN ZERO meters
AND IF IRGRC IS EQUAL TO ONE
Printout 'DEVIATION FROM STEADY-STATE CONDITION HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'DEVIATION FROM STEADY-STATE CONDITION MODERATE RISK'

Rule number 5
IF $RPAS\_IAS_{t+1}$ – $RPAS\_IAS_t$ IS EQUAL TO ZERO kts
AND IF $RPAS\_ALT_{t+1}$ – $RPAS\_ALT_t$ IS GREATER THAN ZERO meters
AND IF IRGRC IS GREATER THAN ONE
Printout 'DEVIATION FROM STEADY-STATE CONDITION HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'DEVIATION FROM STEADY-STATE CONDITION MODERATE RISK'

Rule number 6
IF $RPAS\_IAS_{t+1}$ – $RPAS\_IAS_t$ IS EQUAL TO ZERO kts
AND IF $RPAS\_ALT_{t+1}$ – $RPAS\_ALT_t$ IS SMALLER THAN ZERO meters
AND IF IRGRC IS EQUAL TO ONE
Printout 'DEVIATION FROM STEADY-STATE CONDITION HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'DEVIATION FROM STEADY-STATE CONDITION MODERATE RISK'

Note:
Where 't' is time measured in seconds

H06 – Loss of Emergency Flight Termination System

Definition: the contingent failure of the Emergency Flight Termination System intended both as the loss of the 'Flight Termination System' capable of cutting off the electrical power supply to rotor engines and as the loss of 'Recovery Parachute' functionality.

Note:
It is supposed that both these subsystems have a BITE ('Built In Test Equipment') capable of performing a 'Built In Test' of the Emergency Temination Subsystem main devices (FTS and Recovery parachute devices respectively) (BIT).

Rule number 1

IF RPAS_FTS_BIT IS EQUAL TO FAILED
Printout ‘LOSS OF FTS HIGH RISK’
=>
THEN SET RPAS_AUTOPILOT_LANDING_MODE EQUAL TO ONE
Printout ‘LOSS OF FTS MODERATE RISK’

Rule number 2
IF RPAS_RECOVERY_PARACHUTE_BIT IS EQUAL TO FAILED
Printout ‘LOSS OF FTS HIGH RISK’
=>
THEN SET RPAS_AUTOPILOT_LANDING_MODE EQUAL TO ONE
Printout ‘LOSS OF FTS MODERATE RISK’

H07 – Loss of ‘Retun to Home’ (RTH) mode

Definition: the contingent loss of the autopilot flight mode that allows to use a predefined autopilot mode to safely recover the RPAS

Rule number 1
IF RPAS_AUTOPILOT_RETURN_TO_HOME_MODE IS EQUAL TO FAILED
AND IF IRGRC IS GREATER THAN ONE
Printout ‘LOSS OF RTH MODE MODERATE RISK’
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout ‘LOSS OF RTH MODE LOW RISK’

Rule number 2
IF RPAS_AUTOPILOT_RETURN_TO_HOME_MODE IS EQUAL TO FAIL
AND IF IRGRC IS EQUAL TO ONE
Printout ‘LOSS OF RTH MODE MODERATE RISK’
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout ‘LOSS OF RTH MODE LOW RISK’

H08 – Loss of mission plan

Rule number 1
IF RPAS_MISSION_PLAN IS EQUAL TO FAILED
AND IF IRGRC IS GREATER THAN ONE
Printout ‘LOSS OF MISSION PLAN MODERATE RISK’
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout ‘LOSS OF MISSION PLAN LOW RISK’

Rule number 2
IF RPAS_MISSION_PLAN IS EQUAL TO FAILED
AND IF IRGRC IS EQUAL TO ONE
Printout ‘LOSS OF MISSION PLAN MODERATE RISK’
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE

Printout ‘LOSS OF MISSION PLAN LOW RISK’

H09 – Loss of GPS signal

Definition: the contingent loss of the GPS spatial position signal identified with frozen GPS data

Rule number 1
IF GPS_LAT_{t+1} IS EQUAL TO GPS_LAT_{t}
AND IF GPS_LONG_{t+1} IS EQUAL TO GPS_LONG_{t}
AND IF GPS_ALT_{t+1} IS EQUAL TO GPS_ALT_{t}
Printout ‘LOSS OF GPS MODERATE RISK’
=>
THEN SWITCH TO EGNOS SERVICE
Printout ‘LOSS OF GPS LOW RISK’

Rule number 2
IF GPS_LAT_{t+1} IS EQUAL TO GPS_LAT_{t}
AND IF GPS_LONG_{t+1} IS EQUAL TO GPS_LONG_{t}
AND IF GPS_ALT_{t+1} IS EQUAL TO GPS_ALT_{t}
Printout ‘LOSS OF GPS MODERATE RISK’
=>
THEN SWITCH TO IMU SIGNAL
Printout ‘LOSS OF GPS LOW RISK’

Rule number 3
IF GPS_LAT_{t+1} IS EQUAL TO GPS_LAT_{t}
AND IF GPS_LONG_{t+1} IS EQUAL TO GPS_LONG_{t}
AND IF GPS_ALT_{t+1} IS EQUAL TO GPS_ALT_{t}
Printout ‘LOSS OF GPS MODERATE RISK’
=>
THEN SET RPAS_AUTOPILOT_RETURN TO HOME_MODE EQUAL TO ONE
Printout ‘LOSS OF GPS LOW RISK’

Note:
Where ‘t’ is time measured in seconds

H10 – Loss of EGNOS

Definition: the contingent loss of the EGNOS spatial position signal identified with frozen EGNOS data

Rule number 1
IF $EGNOS\_LAT_{t+1}$ IS EQUAL TO $EGNOS\_LAT_{t}$
AND IF $EGNOS\_LONG_{t+1}$ IS EQUAL TO $EGNOS\_LONG_{t}$
AND IF $EGNOS\_ALT_{t+1}$ IS EQUAL TO $EGNOS\_ALT_{t}$
Printout ‘LOSS OF EGNOS HIGH RISK’
=>
THEN SWITCH TO GPS SERVICE
Printout ‘LOSS OF EGNOS MODERATE RISK’

Rule number 2
IF $EGNOS\_LAT_{t+1}$ IS EQUAL TO $EGNOS\_LAT_{t}$
AND IF $EGNOS\_LONG_{t+1}$ IS EQUAL TO $EGNOS\_LONG_{t}$
AND IF $EGNOS\_ALT_{t+1}$ IS EQUAL TO $EGNOS\_ALT_{t}$
Printout 'LOSS OF EGNOS HIGH RISK'
=>
THEN SWITCH TO IMU SIGNAL
Printout 'LOSS OF EGNOS MODERATE RISK'

Rule number 3
IF $EGNOS\_LAT_{t+1}$ IS EQUAL TO $EGNOS\_LAT_{t}$
AND IF $EGNOS\_LONG_{t+1}$ IS EQUAL TO $EGNOS\_LONG_{t}$
AND IF $EGNOS\_ALT_{t+1}$ IS EQUAL TO $EGNOS\_ALT_{t}$
Printout 'LOSS OF EGNOS HIGH RISK'
=>
THEN SET RPAS_AUTOPILOT_RETURN TO HOME_MODE EQUAL TO ONE
Printout 'LOSS OF EGNOS MODERATE RISK'

Note:
Where 't' is time measured in seconds

H11 – Drift from mission plan
Definition: the contingent drift of the RPA from the planned mission route

Rule number 1
IF DOWNLINK_RPAS_LAT IS NOT EQUAL TO PLANNED_WP_LAT
AND IF DOWNLINK_RPAS_LONG IS NOT EQUAL TO PLANNED_WP_LONG
AND IF DOWNLINK_RPAS_ALT IS NOT EQUAL TO PLANNED_WP_ALT
AND IF IRGRC IS GREATER THAN ONE
Printout 'DRIFT FROM MISSION PLAN HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'DRIFT FROM MISSION MODERATE RISK'

Rule number 2
IF RPAS_LAT IS NOT EQUAL TO PLANNED_WP_LAT
AND IF RPAS_LONG IS NOT EQUAL TO PLANNED_WP_LONG
AND IF RPAS_ALT IS NOT EQUAL TO PLANNED_WP_ALT
AND IF IRGRC IS GREATER THAN ONE
Printout 'DRIFT FROM MISSION HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'DRIFT FROM MISSION MODERATE RISK'

H12 – Loss of the uplink channel of the RPAS radio link
Definition: the contingent loss of the command radio link on the uplink channel to manage the RPAS aerial segment from ground

Rule number 1
IF RPAS_UPLINK_PATH_LOSS IS EQUAL TO ONE
Printout 'LOSS OF UPLINK HIGH RISK'
=>
THEN SET RPAS_RETURN_TO_HOME_FUNCTION EQUAL TO ONE
Printout 'LOSS OF UPLINK MODERATE RISK'

H13 – Loss of the downlink channel of the RPAS radio link

Definition: the contingent loss of the telemetry radio link on the downlink channel to monitor the RPAS on ground

Rule number 1
IF RPAS_DOWN_LINK_PATH_LOSS IS EQUAL TO ONE
Printout 'LOSS OF UPLINK HIGH RISK'
=>
THEN SET RPAS_RETURN_TO_HOME_FUNCTION EQUAL TO ONE
Printout 'LOSS OF DOWNLINK MODERATE RISK'

H14 – Loss of ADS-B

Definition: the contingent failure of the ADS-B equipment.

Note:
It is supposed that the ADS-B has a BITE ('Built In Test Equipment') capable of performing a 'Built In Test' of the device (BIT).

Rule number 1
IF RPAS_ADS-B_BIT IS EQUAL TO FAILED
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF ADS-B HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF ADS-B MODERATE RISK'

Rule number 2
IF RPAS_ADS-B_BIT IS EQUAL TO FAILED
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF ADS-B HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF ADS-B MODERATE RISK'

Hazards H15 ÷ H25

Note:
The 'Expert System' rules deriving from hazards from H15 to H25 are referred to the following scheme (Figure 75):

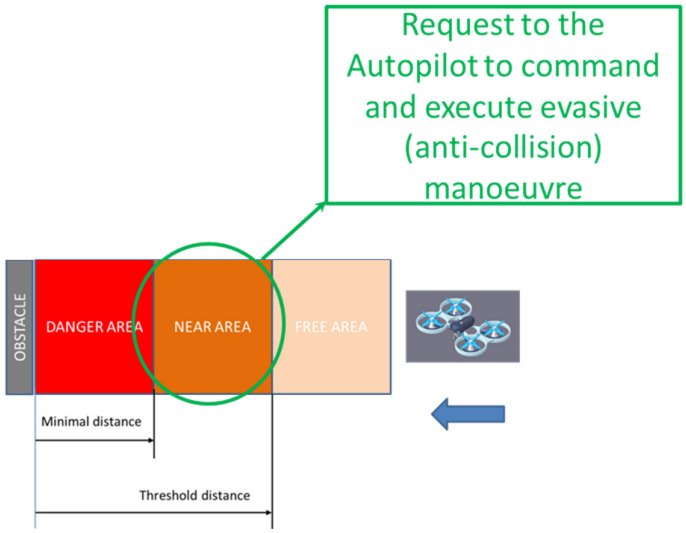


Figure 75 – Collision avoidance distances

Note:
In case of mid-air collision with cooperative aircraft(that is equipped with switched-on and working ADS-B equipment), the RPA shall use the DAA subsystem to avoid mid-air collision; otherwise, if the traffic is not cooperative (that is equipped with not switched-on and/or not working ADS-B equipment) or in case of risk of mid-air collision with a natural or a man-made obstacle, the RPAS shall use LIDAR/SONAR sensors to avoid the collision

Note:
The detectability follow the same above mentioned criteria

H15 – Presence of natural obstacle

Definition: an hazard related to the eventual missed avoidance of a natural obstacle

Rule number 1
IF RPAS_LIDAR_SENSOR_OUTPUT IS 'OBSTACLE'
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN THRESHOLD_DISTANCE
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS GREATER THAN MINIMAL_DISTANCE
Printout 'OBSTACLE HIGH RISK'
=>
THEN SET AUTOPILOT TO PERFORM EVASIVE MANOUVER
Printout 'OBSTACLE MODERATE RISK'

H16 – Presence of man-made manufactures

Definition: an hazard related to the eventual missed avoidance of man-made manufactures

Rule number 1
IF RPAS_LIDAR_SENSOR_OUTPUT IS 'OBSTACLE'
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN THRESHOLD_DISTANCE
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS GREATER THAN MINIMAL_DISTANCE
Printout 'OBSTACLE HIGH RISK'
=>
THEN SET AUTOPILOT TO PERFORM EVASIVE MANOUVER
Printout 'OBSTACLE MODERATE RISK'

H17 – Mid-air collision with other aircraft

Note:
Case of mid-air collision risk with cooperative traffic

Rule number 1
IF RPAS_DAA_OUTPUT IS 'TRAFFIC'
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN THRESHOLD_DISTANCE
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS GREATER THAN MINIMAL_DISTANCE
Printout 'TRAFFIC HIGH RISK'
=>
THEN SET AUTOPILOT TO PERFORM EVASIVE MANOUVER
Printout 'TRAFFIC MODERATE RISK'

Note:
Case of mid-air collision risk with not cooperative traffic

Rule number 2
IF RPAS_LIDAR_SENSOR_OUTPUT IS 'OBSTACLE'
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN THRESHOLD_DISTANCE
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS GREATER THAN MINIMAL_DISTANCE
Printout 'TRAFFIC HIGH RISK'
=>
THEN SET AUTOPILOT TO PERFORM EVASIVE MANOUVER
Printout 'TRAFFIC MODERATE RISK'

H18 – Loss of DAA capability

Definition: the contingent loss of DAA subsystem/functionality

Note:
The RPAS 'Detect and Avoid' (DAA) functionality is compromised if each single equipment composing DAA subsystem fails (Table 35 items FCSS2a, FCSS2b and FCSS2c) or if any of their combined failures listed in Table 98 occurs during a flight sortie.

In order to write simpler rules for Hazard H18, the possible occurrence of single failures of each DAA equipment have been considered only, because the combined failures of those equipment implies their single failure occurrence by definition.
It is supposed that DAA subsystem has a BITE ('Built In Test Equipment') capable of performing a 'Built In Test' of the device (BIT).
Further, even if the use of proper checklists on DAA is foreseen among mitigation actions, the most severe case of sudden loss of DAA equipment functionality during the flight mission is hereinafter considered; therefore, in this case, the following rules will apply:

```
Rule number 1
IF RPAS_ADS-B_BIT IS EQUAL TO FAILED
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF DAA HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF DAA MODERATE RISK'

Rule number 2
IF RPAS_ADS-B_BIT IS EQUAL TO FAILED
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF DAA HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF DAA MODERATE RISK'

Rule number 3
IF RPAS_ALTIMETER_BIT IS EQUAL TO FAILED
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF DAA HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF DAA MODERATE RISK'

Rule number 4
IF RPAS_ALTIMETER_BIT IS EQUAL TO FAILED
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF DAA HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF DAA MODERATE RISK'

Rule number 5
IF EGNOS_BIT IS EQUAL TO FAILED
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF DAA HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
```

Printout ‘LOSS OF DAA MODERATE RISK’

Rule number 6
IF EGNOS_BIT IS EQUAL TO FAILED
AND IF IRGRC IS EQUAL TO ONE
Printout ‘LOSS OF DAA HIGH RISK’
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout ‘LOSS OF DAA MODERATE RISK’

H19 – No detectability from other airspace users

Definition: the hazard deriving from the impossibility for other airspace users to detect an operating RPAS; the idea to manage this hazards is to move from the other airspace users to the RPA: if other users do not detect the RPA, the RPA shall avoid the cooperative/not cooperative obstacle as above described in previous rules

Rule number 1
IF DAA_OUTPUT IS ‘TRAFFIC’
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN THRESHOLD_DISTANCE
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS GREATER THAN MINIMAL_DISTANCE
Printout ‘LOSS OF DAA HIGH RISK’
=>
THEN SET AUTOPILOT TO PERFORM EVASIVE MANOUVER
Printout ‘LOSS OF DAA MODERATE RISK’

Rule number 2
IF LIDAR_OUTPUT IS ‘OBSTACLE’
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN THRESHOLD_DISTANCE
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS GREATER THAN MINIMAL_DISTANCE
Printout ‘LOSS OF DAA HIGH RISK’
=>
THEN SET AUTOPILOT TO PERFORM EVASIVE MANOUVER
Printout ‘LOSS OF DAA MODERATE RISK’

H20 – Cooperative traffic intrusion

Definition: the contingent intrusion of traffic equipped with switched on and working ADS-B equipment

Rule number 1
IF DAA_OUTPUT IS ‘TRAFFIC’
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN THRESHOLD_DISTANCE

AND IF RPAS_DISTANCE_FROM_OBSTACLE IS GREATER THAN MINIMAL_DISTANCE
Printout ‘COOPERATIVE TRAFFIC INTRUSION HIGH RISK’
=>
THEN SET AUTOPILOT TO PERFORM EVASIVE MANOUVER
Printout ‘COOPERATIVE TRAFFIC INTRUSION MODERATE RISK’

H21 – Not cooperative traffic intrusion

Definition: the contingent intrusion of traffic not equipped with switched on and working ADS-B equipment

Rule number 1
IF LIDAR_OUTPUT IS ‘OBSTACLE’
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN THRESHOLD_DISTANCE
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS GREATER THAN MINIMAL_DISTANCE
Printout ‘NOT COOPERATIVE TRAFFIC INTRUSION HIGH RISK’
=>
THEN SET AUTOPILOT TO PERFORM EVASIVE MANOUVER
Printout ‘NOT COOPERATIVE TRAFFIC INTRUSION MODERATE RISK’

H22 – Missed cooperative traffic tracking

Definition: the RPA misses to track cooperative traffic that enters the danger area represented in Figure 75; immediate evasive manoeuvre shall be commanded and executed

Rule number 1
IF DAA_OUTPUT IS ‘TRAFFIC’
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN MINIMAL_DISTANCE
Printout ‘MISSED COOPERATIVE TRAFFIC TRACKING HIGH RISK’
=>
THEN SET AUTOPILOT TO PERFORM EVASIVE MANOUVER
Printout ‘MISSED COOPERATIVE TRAFFIC TRACKING MODERATE RISK’

H23 – Missed not cooperative traffic tracking

Definition: the RPA misses to track cooperative traffic that enters the danger area represented in Figure 75; immediate evasive manoeuvre shall be commanded and executed

Rule number 1
IF LIDAR_OUTPUT IS ‘TRAFFIC’
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN MINIMAL_DISTANCE
Printout ‘MISSED NOT COOPERATIVE TRAFFIC TRACKING HIGH RISK’
=>
THEN SET AUTOPILOT TO PERFORM EVASIVE MANOUVER

Printout ‘MISSED NOT COOPERATIVE TRAFFIC TRACKING MODERATE RISK’

H24 – Cooperative traffic collision avoidance
Definition: collision avoidance with cooperative traffic

Rule number 1
IF DAA_OUTPUT IS ‘TRAFFIC’
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN THRESHOLD_DISTANCE
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS GREATER THAN MINIMAL_DISTANCE
Printout ‘COOPERATIVE TRAFFIC COLLISION HIGH RISK’
=>
THEN SET AUTOPILOT TO PERFORM EVASIVE MANOUVER
Printout ‘COOPERATIVE TRAFFIC COLLISION MODERATE RISK’

H25 – Not cooperative traffic collision avoidance
Definition: collision avoidance with not cooperative traffic

Rule number 1
IF LIDAR_OUTPUT IS ‘OBSTACLE’
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN THRESHOLD_DISTANCE
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS GREATER THAN MINIMAL_DISTANCE
Printout ‘NOT COOPERATIVE TRAFFIC COLLISION HIGH RISK’
=>
THEN SET AUTOPILOT TO PERFORM EVASIVE MANOUVER
Printout ‘NOT COOPERATIVE TRAFFIC COLLISION MODERATE RISK’

H26 – Missed avoidance collision maneuver performance
Definition: the missed performance of avoidance collision manoeuvre with cooperative or not cooperative traffic

Rule number 1
IF DAA_OUTPUT IS ‘TRAFFIC’
AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN MINIMAL_DISTANCE
Printout ‘MISSED AVOIDANCE COLLISION MANOUVRE PERFORMANCE HIGH RISK’
=>
THEN SET FTS_CMD EQUAL TO ONE
Printout ‘MISSED AVOIDANCE COLLISION MANOUVRE PERFORMANCE MODERATE RISK’

Rule number 1
IF LIDAR_OUTPUT IS ‘OBSTACLE’

AND IF RPAS_DISTANCE_FROM_OBSTACLE IS SMALLER THAN MINIMAL_DISTANCE
Printout 'MISSED AVOIDANCE COLLISION MANOUVRE PERFORMANCE HIGH RISK'
=>
THEN SET FTS_CMD EQUAL TO ONE
Printout 'MISSED AVOIDANCE COLLISION MANOUVRE PERFORMANCE MODERATE RISK'

H27 – Missed collision avoidance manoeuvring performance monitoring

Note:
This is an hazard condition related to human factor performance; no Expert System rules are deemed applicable in this case

H28 – Missed weather awareness capability

Definition: the contingent miss of weather awareness capability; the following cases for which weather Doppler RADAR is applicable are considered: rain, snow and similar adverse weather conditions.

Note:
It is supposed that the Weather Doppler RADAR has a BITE ('Built In Test Equipment')capable to perform a 'Built In Test' of the device (BIT).

Rule number 1
IF WEATHER_DOPPLER_RADAR_BIT IS FAILED
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout 'MISSED WEATHER AWARENESS CAPABILITY MODERATE RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'MISSED WEATHER AWARENESS CAPABILITY LOW RISK'

Rule number 2
IF WEATHER_DOPPLER_RADAR_BIT IS FAILED
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout 'MISSED WEATHER AWARENESS CAPABILITY MODERATE RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'MISSED WEATHER AWARENESS CAPABILITY LOW RISK'

H29 – Missed contingent weather information gathering

Definition: the miss of contingent weather information gathering

Note:
This is an hazard condition that can be verified on ground performing pre-flight briefing, checklists, etc.; no 'Expert System' rules are deemed to be applicable in this case

H30 – Missed avoidance of adverse weather

Definition: the missed avoidance of adverse weather due to weather Doppler RADAR failure.

Note:
It is supposed that the Weather Doppler RADAR has a BITE ('Built In Test Equipment') capable of performing a 'Built In Test' of the device (BIT).

Rule number 1
IF WEATHER_RADAR_DOPPLER_BIT IS FAILED
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout 'MISSED AVOIDANCE OF ADVERSE WEATHER HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'MISSED AVOIDANCE OF ADVERSE WEATHER LOW RISK'

Rule number 2
IF WEATHER_RADAR_DOPPLER_BIT IS FAILED
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS EQUAL TO ONE
Printout 'MISSED AVOIDANCE OF ADVERSE WEATHER HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'MISSED AVOIDANCE OF ADVERSE WEATHER MODERATE RISK'

H31 – Loss of Health and Status Monitoring subystem

Definition: loss of the RPAS Health and Status Monitoring on the aerial platform due to a failure occurrence

Note:
It is supposed that the RPAS Health and Status Monitoring subsystem has a BITE ('Built In Test Equipment') capable of performing a 'Built In Test' of the device (BIT).

Rule number 1
IF HEALTH_AND_STATUS_MONITORING_BIT IS FAILED
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE

Printout 'HEALTH AND STATUS MONITORING SUBSYSTEM FAILURE HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'HEALTH AND STATUS MONITORING SUBSYSTEM FAILURE MODERATE RISK'

Rule number 2
IF HEALTH_AND_STATUS_MONITORING_BIT IS FAILED
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS EQUAL TO ONE
Printout 'HEALTH AND STATUS MONITORING SUBSYSTEM FAILURE HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'HEALTH AND STATUS MONITORING SUBSYSTEM FAILURE MODERATE RISK'

H32 – Loss of communication while transiting from LOS to BRLOS and vice versa

Definition: the contingent loss of communication signal path passing from 'Line of Sight' to 'Beyond line of sight' distance between the remote pilot and the aerial platform

Rule number 1
IF $RPAS\_RANGE_t$ IS SMALLER THAN RPAS_RANGE_RLOS
AND IF $RPAS\_RANGE_{t+1}$ IS GREATER THAN RPAS_RANGE_RLOS
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF RPAS_UPLINK_PATH_LOSS IS EQUAL TO ONE
AND IF RPAS_DOWNLINK_PATH_LOSS IS EQUAL TO ONE
Printout 'LOSS OF LINK WHILE TRANSITING FROM RLOS TO BRLOS HIGH RISK'
=>
THEN SET RPAS_AUTOPILOT_RETURN TO HOME_MODE EQUAL TO ONE
Printout 'LOSS OF LINK WHILE TRANSITING FROM RLOS TO BRLOS MODERATE RISK'

Rule number 2
IF $RPAS\_RANGE_t$ IS GREATER THAN RPAS_RANGE_RLOS
AND IF $RPAS\_RANGE_{t+1}$ IS SMALLER THAN RPAS_RANGE_RLOS
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF RPAS_UPLINK_PATH_LOSS IS EQUAL TO ONE
AND IF RPAS_DOWNLINK_PATH_LOSS IS EQUAL TO ONE
Printout 'LOSS OF LINK WHILE TRANSITING FROM BRLOS TO RLOS HIGH RISK'
=>
THEN SET RPAS_AUTOPILOT_RETURN TO HOME_MODE EQUAL TO ONE

Printout 'LOSS OF LINK WHILE TRANSITING FROM BRLOS TO RLOS MODERATE RISK'
Where 't' is time

H33 – Unintentional radio link interference
Definition: unintentional radio link interference due to the survey of telecommunication transmitting antennas, airport areas etc.

This is an hazard condition that can be solved using operational procedures; no 'Expert System' rules are deemed to be applicable in this case

H34 – Malicious radio link jamming
Definition: malicious intentional cyber threat against RPAS radio link

This is an hazard condition that can be solved using operational procedures: switching on secondary redundant radio frequency band or immediately terminate the flight; no 'Expert System' rules are deemed to be applicable in this case

H35 – Malicious radio link spoofing
Definition: malicious intentional cyber threat against RPAS radio link

This is an hazard condition that can be solved using operational procedures: switching on secondary redundant radio frequency band or immediately terminate the flight; no 'Expert System' rules are deemed to be applicable in this case

H36 – Fire
Definition: the contingent fire outbreak on board the RPA

Rule number 1
IF RPAS_FIRE_WARNING IS EQUAL TO ONE
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
Printout 'FIRE HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'FIRE MODERATE RISK'

H37 – Loss of RPAS autopilot
Definition: the contingent loss of the RPAS autopilot during a flight operation

Rule number 1
IF RPAS_AUTOPILOT_FAILURE_WARNING IS EQUAL TO ONE
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout 'AUTOPILOT FAILURE HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'AUTOPILOT FAILURE LOW RISK'

Rule number 2
IF RPAS_AUTOPILOT_FAILURE_WARNING IS EQUAL TO ONE
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS EQUAL TO ONE
Printout 'AUTOPILOT FAILURE HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'AUTOPILOT FAILURE LOW RISK'

H38 – Loss of RPAS electrical power

Definition: the contingent loss of the RPAS electrical power during a flight operation

Rule number 1
IF $\sum$LIPO_BATTERY_CURRENT$_i$ IS EQUAL TO 0 Ampere
AND IF RPAS_ENGINE_OMEGA$_{t+1}$ – RPAS_ENGINE_OMEGA$_t$ IS SMALLER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF ELECTRICAL POWER HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'RPAS_ENGINE_OMEGAt+1 MODERATE RISK'

Rule number 2
IF $\sum$LIPO_BATTERY_CURRENT$_i$ IS EQUAL TO 0 Ampere
AND IF RPAS_ENGINE_OMEGA$_{t+1}$ – RPAS_ENGINE_OMEGA$_t$ IS SMALLER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF ELECTRICAL POWER HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF ELECTRICAL POWER MODERATE RISK'

Note:
Where 'i' is each LiPo battery

H39 – Loss of inertial platform

Definition: the contingent loss of the RPAS electrical power during a flight operation

Note:
It is supposed that the IMU has a BITE ('Built In Test Equipment') capable of performing a 'Built In Test' of the device (BIT).

Rule number 1
IF RPAS_IMU_BIT IS EQUAL TO FAILED
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF INERTIAL PLATFORM HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF INERTIAL MODERATE RISK'

Rule number 2
IF RPAS_IMU_BIT IS EQUAL TO FAILED
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF INERTIAL PLATFORM HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF INERTIAL MODERATE RISK'

Hazards H40 ÷ H44

Note:
With reference to Hazards 40 ÷ 44, , the comparison between two contingent indications for heading, altitude, pressure is supposed to be performed to determine if the given air sensor is measuring the correct parameter for the flight control system

H40 – Loss of heading indication

Definition: the contingent loss of the RPAS heading indication

Rule number 1
IF (RPAS_HDG1 – RPAS_HDG2) IS DIFFERENT FROM ZERO
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF HEADING INDICATION HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF HEADING INDICATION MODERATE RISK'

```
Rule number 2
IF (RPAS_HDG1 – RPAS_HDG2) IS DIFFERENT FROM ZERO
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF HEADING INDICATION HIGH RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF HEADING INDICATION MODERATE RISK'
```

H41 – Loss of altitude indication

Definition: the contingent loss of the RPAS heading indication

```
Rule number 1
IF (RPAS_ALT1 – RPAS_ALT2) IS DIFFERENT FROM ZERO
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF ALTITUDE INDICATION HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF ALTITUDE MODERATE RISK'

Rule number 2
IF (RPAS_ALT1 – RPAS_ALT2) IS DIFFERENT FROM ZERO
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS EQUAL TO ONE
Printout 'LOSS OF ALTITUDE MODERATE RISK'
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF ALTITUDE MODERATE RISK'
```

H42 – Pressure sensor failure

Definition: the contingent loss of the RPAS pressure sensor failure

```
Rule number 1
IF (RPAS_PSR1 – RPAS_PSR2) IS DIFFERENT FROM ZERO
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout 'LOSS OF PRESSURE SENSOR HIGH RISK'
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout 'LOSS OF PRESSURE SENSOR MODERATE RISK'

Rule number 2
IF (RPAS_PSR1 – RPAS_PSR2) IS DIFFERENT FROM ZERO
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
```

```
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS EQUAL TO ONE
Printout ‘LOSS OF PRESSURE SENSOR HIGH RISK’
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout ‘LOSS OF PRESSURE SENSOR MODERATE RISK’
```

H43 – Misleading altitude indication

Definition: the contingent misleading RPAS altitude indication

```
Rule number 1
IF (RPAS_ALT1 – RPAS_ALT2) IS DIFFERENT FROM ZERO
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout ‘LOSS OF ALTITUDE INDICATION HIGH RISK’
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout ‘LOSS OF ALTITUDE INDICATION MODERATE RISK’

Rule number 2
IF (RPAS_ALT1 – RPAS_ALT2) IS DIFFERENT FROM ZERO
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS EQUAL TO ONE
Printout ‘LOSS OF ALTITUDE INDICATION HIGH RISK’
=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout ‘LOSS OF ALTITUDE INDICATION MODERATE RISK’
```

H44 – Misleading airspeed indication

Definition: the contingent misleading RPAS airspeed indication

```
Rule number 1
IF (RPAS_IAS1 – RPAS_IAS2) IS DIFFERENT FROM ZERO
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS GREATER THAN ONE
Printout ‘LOSS OF AIRSPEED INDICATION HIGH RISK’
=>
THEN SET RPAS_RECOVERY_PARACHUTE_CMD EQUAL TO ONE
Printout ‘LOSS OF AIRSPEED MODERATE RISK’

Rule number 2
IF (RPAS_IAS1 – RPAS_IAS2) IS DIFFERENT FROM ZERO
AND IF RPAS_ENGINE_OMEGA IS GREATER THAN ZERO rad/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
AND IF IRGRC IS EQUAL TO ONE
Printout ‘LOSS OF AIRSPEED HIGH RISK’
```

=>
THEN SET RPAS_FTS_CMD EQUAL TO ONE
Printout 'LOSS OF AIRSPEED MODERATE RISK'

H45 – Misleading angle of attack indication

Definition: the contingent misleading RPAS angle of attack indication

Note:

Applicable to fixed wing RPAS only; not valid for the RPAS model object of the 'Expert System' knowledge basis in object

H46 – Stall

Definition: aerial segment aerodynamic stall condition

Note:

Applicable to fixed wing RPAS only; not valid for the RPAS model object of the 'Expert System' knowledge basis in object

H47 – Loss of fuel cell

Definition: the contingent loss of on board fuel cell

Rule number 1
IF RPAS_FUEL_CELL_CURRENT IS EQUAL TO ZERO Ampere
AND IF $RPAS\_ENGINE\_OMEGA_{t+1}$ - $RPAS\_ENGINE\_OMEGA_{t}$ IS SMALLER THAN ZERO radians/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
Printout 'LOSS OF FUEL CELL HIGH RISK'
=>
THEN SWITCH TO RPAS_LIPO_BATTERY_CURRENT
Printout 'LOSS OF FUEL CELL MODERATE RISK'

H48 – Remote pilot low training

Definition: hazard deriving from lack of or low remote pilot training

Note:

This is an hazard condition due to human factor issues: 'Expert System' rules are deemed not applicable

H51 – Non compliant operational procedures

Definition: hazard deriving from the application during flight of not compliant operational procedures

Note:

This is an hazard condition due to human factor issues: 'Expert System' rules are deemed not applicable

H52 – Loss of remote pilot situational awareness

Definition: hazard deriving from the loss of the remote pilot situational awareness during the flight

Note:
This is an hazard condition due to human factor issues: 'Expert System' rules are deemed not applicable

H53 – Human senses limitation

Definition: hazard deriving from the physiological limits of human senses (for example during night flight operations or under low visibility/low light operational conditions)

Note:
This is an hazard condition due to human factor issues: 'Expert System' rules are deemed not applicable

H54 – Remote pilot excessive workload

Definition: hazard deriving from the excessive crew workload during flight operations

Note:
This is an hazard condition due to human factor issues: 'Expert System' rules are deemed not applicable

WEATHER HAZARDS: H55 ÷ H69 (HAZARDS EXCLUDED: H56, H60, H61, H62)

Note:
They are hazards due to daily contingent weather conditions that can be managed with on ground operational procedures foreseeing that the flight operations cannot be performed if weather conditions are less than optimal or they shall be interrupted if less than optimal conditions occur during the flight mission

H56 – GLARE

Definition: weather hazard deemed to cause moderate acceptable risk due to the fact that the remote pilot is not on board the RPA

H60 – RAIN

Definition: rain adverse weather hazard

Note:
A weather Doppler RADAR is foreseen to be installed on board the RPAS to identify rain during an operational mission

Rule number 1
IF WEATHER_DOPPLER_RADAR_IMAGE is equal to 'RAIN'

AND IF RPAS_ENGINE IS GREATER THAN ZERO radians/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
Printout 'RAIN HIGH RISK'
=>
THEN SET RPAS_AUTOPILOT_RETURN TO HOME_MODE EQUAL TO ONE
Printout 'RAIN MODERATE RISK'

H61 – SNOW

Definition: rain adverse weather hazard

Note:
A weather Doppler RADAR is foreseen to be installed on board the RPAS to identify rain during an operational mission

Rule number 1
IF WEATHER_DOPPLER_RADAR_IMAGE is equal to 'SNOW'
AND IF RPAS_ENGINE IS GREATER THAN ZERO radians/sec
AND IF RPAS_ALT IS GREATER THAN ZERO feet
Printout 'SNOW HIGH RISK'
=>
THEN SET RPAS_AUTOPILOT_RETURN TO HOME_MODE EQUAL TO ONE
Printout 'SNOW MODERATE RISK'

H62 – SOLAR STORM

Definition: hazard deriving from the contingent solar storm occurrence during flight operations

Note:
Solar storms mainly appears as a degradation of navigation satellite signals that leads to all signal loss. For this reason, this hazard can be expressed according to these rules:

Rule number 1
IF GPS_LAT_{t+1} IS EQUAL TO GPS_LAT_{t}
AND IF GPS_LONG_{t+1} IS EQUAL TO GPS_LONG_{t}
AND IF GPS_ALT_{t+1} IS EQUAL TO GPS_ALT_{t}
AND IF $EGNOS\_LAT_{t+1}$ IS EQUAL TO $EGNOS\_LAT_{t}$
AND IF $EGNOS\_LONG_{t+1}$ IS EQUAL TO $EGNOS\_LONG_{t}$
AND IF $EGNOS\_ALT_{t+1}$ IS EQUAL TO $EGNOS\_ALT_{t}$
Printout 'SOLAR STORM MODERATE RISK'
=>
THEN SET RPAS_AUTOPILOT_RETURN TO HOME_MODE EQUAL TO ONE
Printout 'SOLAR STORM LOW RISK'

Note:
Where 't' is time measured in seconds

Appendix G - System-Theoretic Accident Model and Processes - (STPA) safety analysis - Results

Table 147 – STPA methodology applied to light RPAS: unsafe control action identification (STPA step 1) ([42], [102], [103])

Investigated scenario: mid-air collision of an RPAS in the VLL with a cooperative manned aircraft		
Hazardous or unsafe control actions (UCA)		
Control action (CA)	**Not capable of providing hazards**	**Capable of providing hazards**
[CA1] Climb	[UCA1] The RPA climbs to avoid the intruder when the DAA indicates climb evasive manoeuvre	[UCA2] The RPA does not climb when the DAA indicates climb evasive manoeuvre [H02, H03]
		[UCA3] The remote pilot does not command the RPA to climb when the DAA indicates climb evasive manoeuvre [H01]
[CA2] Descend	[UCA4] The RPA descends to avoid the intruder when the DAA indicates descend evasive manoeuvre	[UCA5] The RPA does not descend when the DAA indicates descend evasive manoeuvre [H02, H03]
		[UCA6] The remote pilot does not command the RPA to descend when the DAA indicates descend evasive manoeuvre [H01]
[CA3] Turn	[UCA7] The RPA turns right to avoid the intruder when the DAA indicates right turn evasive manoeuvre	[UCA8] The RPA turns left to avoid the intruder when the DAA indicate right turn evasive manoeuvre [H02, H03]
		[UCA9] The remote pilot does not command the RPA to turn right when the DAA indicates right turn evasive manoeuvre [H01]
	[UCA10] The RPA turns left to avoid the intruder when the DAA indicates left turn evasive manoeuvre	[UCA11] The RPA turns right to avoid the intruder when the DAA indicates left turn evasive manoeuvre [H02, H03]
		[UCA12] The remote pilot does not command the RPA to turn left when the DAA indicates left turn evasive manoeuvre [H01]
[CA4] Move forward	[UCA13] The remote pilot does not command the RPA to move forward when the RPA is in track and closer to the intruder less than the collision avoidance threshold distance	[UCA14] The remote pilot commands the RPA to move forward when the RPA is in track and closer to the intruder less than the collision avoidance threshold distance [H02, H03]
[CA5] Move backward	[UCA15] The remote pilot commands the RPA to move backward when the RPA is in track and closer to the intruder less than the collision avoidance threshold distance	[UCA16] The remote pilot does not command the RPA to move backward when the RPA is in track and closer to the intruder less than the collision avoidance threshold distance [H01]
[CA6] Increase airspeed	[UCA17] The remote pilot does not command the RPA to increase speed when the RPA is in track and closer to the intruder less than the collision avoidance threshold distance	[UCA18] The remote pilot commands the RPA to increase speed when the RPA is in track and closer to the intruder less than the collision avoidance threshold distance [H02, H03]
[CA7] Decrease airspeed	[UCA19] The remote pilot does not command the RPA to decrease speed when the RPA is in track and closer to the intruder less than the collision avoidance threshold distance	[UCA20] The remote pilot does not command the RPA to decrease when the RPA is in track and closer to the intruder less than the collision avoidance threshold distance [H01]
[CA8] Deactivate		[UCA21] The remote pilot deactivates the RPA when it is in flight [H02]
[CA9] Reactivate	[UCA22] The remote pilot does not reactivate the RPA when it is deactivated ad still in flight	

Table 148 – Causal factors for light RPAS
Identified unsafe control actions (STPA step 2) ([42], [102], [103])

Investigated scenario: Mid-air collision of an RPAS in the VLL with a cooperative manned aircraft			
Generic causal factor	**Detailed causal factor**	**Causing action**	
		Ineffective control action (CA)	**Unsafe control action (UCA)**
Inadequate flight commands and controls operation	Inherent technical flow:	1-7, 9	
	1. Remote control		-
	2. Display		-
	3. RPA		2, 6, 8, 11,
Inadequate communication	Signal disruption because of electromagnetic interference in the communication between:	1-7, 9	
	1. Remote controller and RPA		2, 3, 5, 6, 8, 9, 11, 12, 14, 16, 18, 20, 21
	2. RPA and displays		2, 3, 5, 6, 8, 9, 11, 12, 14, 16, 18, 20, 21
Inadequate remote pilot operation	Inadequate knowledge or skills (where applicable) in:	-	
	1. Authority regulation		-
	2. RPA operation		3, 6, 9, 12, 16, 20, 21
	3. Terrain		-
	4. Weather forecast		-
-	Inadequate (incomplete, unclear, written in unfamiliar language to the operator):		
-	1. Authority regulation	-	-
-	2. RPA operations procedures	-	3, 6, 9, 12, 16, 20, 21
-	Exceedance of cognitive capacity	-	1 - 21
-	Effects on emotional state	-	1 - 21
-	Inadequate information about RPA density in the operational area	-	3, 6, 9, 12, 16, 20, 21
Insufficient energy level	Chronic known physiological problems	-	
	Unanticipated physiology limitations	-	-
	Display battery depleted	-	-
	Remote controller battery depleted	-	3, 6, 9, 12, 16, 20, 21
	RPA battery depleted	-	3, 6, 9, 12, 16, 20, 21

Appendix H - RPAS endurance and range performance improvement - A proposal solution: hybrid RPAS

A consistent increase in light RPAS range and endurance performances is necessary to integrate them into the civil airspace for specific category commercial flight operations. A model architecture for an hybrid RPAS is hereinafter proposed (Figure 76 [106], [107]): it shows an RPAS electric propulsion subsystem fed by hydrogen fuel cells as primary source of energy and LiPo battery as redundant one.

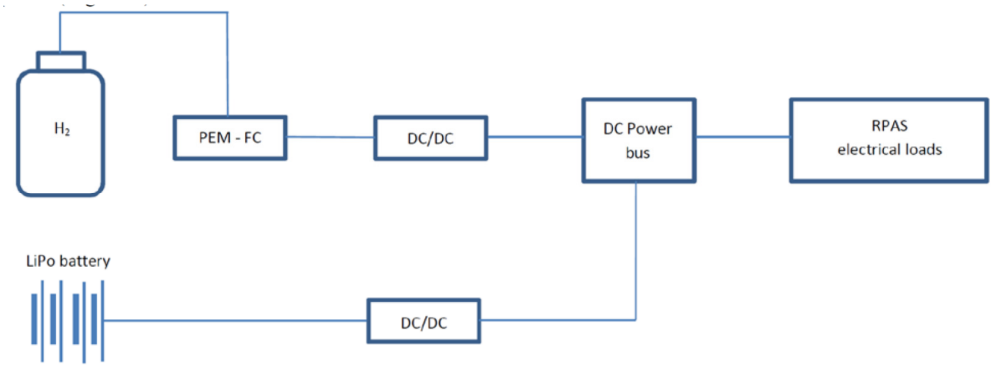


Figure 76 – Hybrid RPAS propulsion system architecture ([106], [107])

The fuel cells are electrochemical devices capable of converting the energy of a fuel (hydrogen in the present case) directly into electricity. The fuel cells are characterized by the same principle of operation of other cells, but they are particularly of interest because of their high efficient performance. The fuel cells are composed of an electrolyte layer in contact with an anode on one side and with a cathode on the either side. The fuel cell converts the chemical energy embedded in the hydrogen fuel by mean of an electrolysis reaction (Figure 77 [108]) (oxidation on the anode side of the fuel cell and reduction on the cathode side). Among the variety of fuel cells available on the market the attention is focused on Polymer Electrolyte Membrane or Proton Exchange Membrane Fuel Cell (PEM FC) technology. Currently, this kind of fuel cell are mostly of interest for the low working temperature (between -25°C and 75°C) and for the particular properties of the polymer the cell membrane is made of [109].

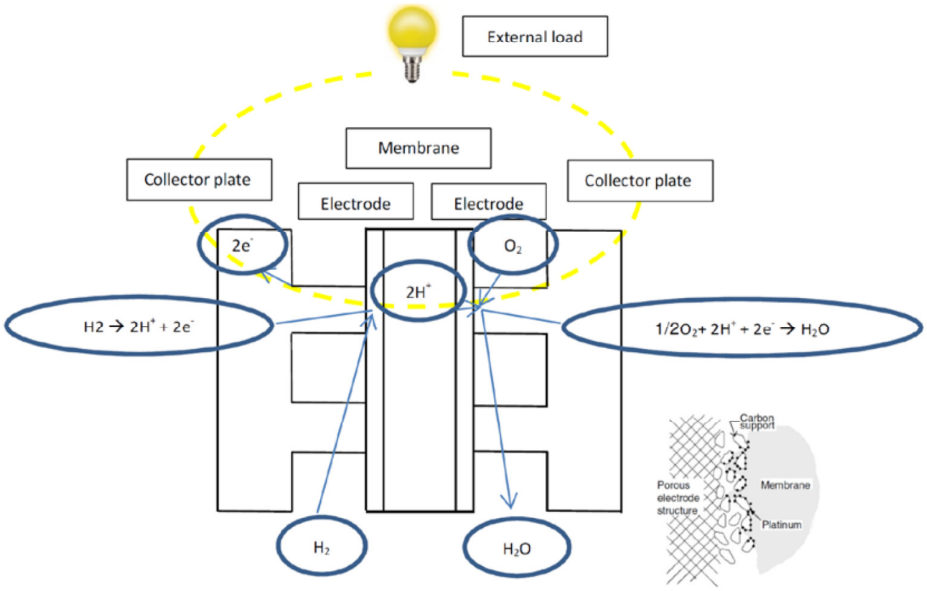


Figure 77 – PEM fuel cell principle of operation [108]

With reference to the RPAS integration into the civil airspace, the main focus is on the parametric model associated to the proposed technical solution (Figure 78 [107]):

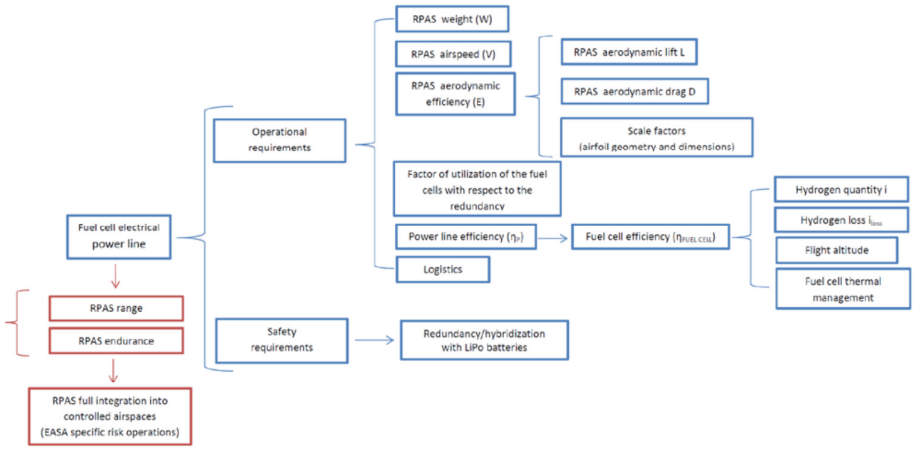


Figure 78 – Hybrid RPAS systems: safety and operational requirements model [107]

The model identifies two groups of parameters hereinafter described and discussed [107]:

- Operational parameters: RPAS weight, RPAS airspeed, RPAS airframe (scaling factors and aerodynamic efficiency shall be considered as well); the factor of utilization of the fuel cells with respect to its redundancy; the power line efficiency which depends on

the fuel cell efficiency and on altitude, pressure, temperature flight conditions; the necessary logistics for hydrogen supply

- Safety parameters: in the power line they mainly deal with the LiPo battery package that becomes a redundant source of energy with respect to the fuel cell intended to be used as the primary one

As a first estimation, the power requested to the fuel cell can be assumed to be directly proportional to the RPA weight for a given set of required design performances. A heavier RPA requests more power to the propulsion system to reach the same performances. As said, PEM fuel cells are highly efficient (52% [106]) in converting chemical into electrical energy and, as known, the hydrogen energy content is very high. Nevertheless, due to the low density of hydrogen, (the lowest among chemical elements), large volumes of it can be requested to be stored on ground and properly loaded on board the RPA. The weight of the tank necessary to embody such large volumes of hydrogen can make the fuel power system total weight affect the RPA flight performances. This issue suggests that the best compromise shall be found among the necessary quantity of hydrogen, the power system weight with respect to the RPA weight and the RPA flight performances. Hence, the hydrogen tank sizing is crucial for hydrogen fed hybrid RPAS design. As a general requirement, the best combination of pressure and volume of the hydrogen tank shall be determined after an accurate global evaluation of the RPA flight performance.

The RPA airspeed and aerodynamic impact on the request of energy to the power line during the cruise flight phase performance (that is during most of flight time). Smart aerodynamic design solutions assuring high values of efficiency and scale factors can positively influence the RPA hydrogen consumptions and consequently the power line sizing.

The power line shall be designed to be efficient both as a whole and with reference to each single component. The fuel cell efficiency is the ratio between the developed electrical power and the consumed hydrogen. The fuel consumption depends on the hydrogen fuel cells utilization factor with respect to the LiPo battery set as redundant equipment. In fact, the fuel cell will be sized to work as primary source of energy thus serving the RPA for the whole mission length; the LiPo battery will be mainly requested to satisfy peaks of energy during or in case of sudden highly demanding phases of flight or manoeuvers. The LiPo battery will be used as primary source of energy only in case of fuel cells system failure.

The flight altitude, pressure and temperature conditions heavily impact on the fuel cells performances making them decrease with altitude [110]. In particular wrong hydrogen fuel cell thermal management makes them get dramatically worse: too high fuel cell temperatures cause water evaporation and membranes drying; too low fuel cell temperatures hinder water condensation inside the stack. In the first case, no hydrogen ion conduction though the membranes occurs while in the second one the gas diffusion and the transport of the reactants to the membranes are prevented to occur [111].

The use of hydrogen fuel cells on board RPA will request strategically organised logistic chain for refurbishment [107] to allow hybrid RPAS daily specific category operations in the civil airspaces. The hydrogen fuel cells installed on board the RPA are the final element of a future integrated logistic infrastructure able to produce, transport and store hydrogen to make it available in airports or other proper sites used by RPAS as basis for flight operations as it currently occurs with kerosene. The main concerns related to hydrogen transportation are closely related its natural physical properties. The hydrogen can be transported under the liquid or the gaseous state. The liquid state option ensures minor losses during transport and a higher volumetric storage density with less frequent refill of stationery tanks; on the other side, more energy is requested to liquefy hydrogen at temperatures of 21 K and at pressures of 1.3 MPa. The gaseous state option for transportation causes major energy expenditures due to the hydrogen density that is the lowest one among all chemical elements.

The hydrogen fuel cells have demonstrated a better reliability with respect to, for example, small internal combustion engines (higher MTBF, up to five times according to some Authors [112]). In addition, the same redundancy of the LiPo battery working in parallel to the fuel cell system strongly extends the PEM fuel cell operating life and enhances the overall power line safety. Thanks to its high power density, the LiPo battery easily provides the excess of power requested during more demanding phases of flight preserving the PEM fuel cell reliability and durability and avoiding PEM fuel cell oversizing. As a final consideration, a good flexibility results from the proposed power line architecture

Among the possible disadvantages related to the use of fuel cells the membrane damage caused by fuel or oxygen starvation can be mentioned also as a critical issue to be considered during design.

With reference to ground and flight operational safety, the presence of hydrogen on board the RPA introduces the potential hazard of formation of explosive mixtures. The hydrogen is naturally flammable being an energy carrier. The pure hydrogen is not explosive or reactive, but it can be in presence of precursors oxidizing gas like oxygen or chlorine [113].

In conclusion, the proposed use of Proton Electron Membrane Fuel Cells (PEM FC) can be considered as a realistic technical option to increase RPAS range and endurance performances with relatively low economic investments.