ASCOS certification case study: Aircraft system failure management

J.F. Delaigue, J.P. Heckmann, J. Teyssier, S. Bravo Muñoz (all APSYS), G. Temme (Certiflyer), E. van de Sluis, M. Stuip (NLR), S. Bull (Ebeni)

This certification case study proposes an Autonomous Failure Management System installed on RPAs to test a newly proposed ASCOS certification approach (as documented in ASCOS D1.3) in two ways. First: to test how the ASCOS approach can provide a common certification methodology that enables a certification for the Total Aviation System, and secondly to explore how this approach could be used to further develop the common safety standards (e.g. EUROCAE ED78A) already existing.

Coordinator	L.J.P. Speijker (NLR)
Work Package Manager	A.L.C. Roelen (NLR)

Grant Agreement No.	314299
Document Identification	D4.1
Status	Approved
Version	1.1
Date of Issue	5/11/2015
Classification	Restricted

This page is intentionally left blank

Document Change Log

Version	Author(s)	Date	Affected Sections	Description of Change
1.0	J.F. Delaigue et al.	25-02-2015	All	Version for approval by PMT
1.1	J.F. Delaigue et al.	11-05-2015	Executive Summary, Abstract	Minor corrections

Review and Approval of the Document

Organisation Responsible for Review	Name of person reviewing the document	Date
NLR	A.L.C. Roelen	25-02-2015
TATM	H. Neufeldt	25-02-2015
TR6	B. Pauly, F. Orlandi	25-02-2015
APSYS	M. Feuvrier	25-02-2015
CAA UK	A. Eaton	25-02-2015
CertiFlyer	M. Heiligers	25-02-2015
Avanssa	N. Aghdassi	25-02-2015
Ebeni	A. Simpson	25-02-2015
Deep Blue	L. Save	25-02-2015
Organisation Responsible for Approval	Name of person approving the document	Date
NLR	A.L.C. Roelen	25-02-2015
NLR	L.J.P. Speijker	11-05-2015

Document Distribution

Organisation	Names
European Commission	M. Kyriakopoulos
NLR	L. Speijker, A. Rutten, M.A. Piers, P. van der Geest, A. Roelen, J.J Scholte, J. Verstraeten, R. Wever, E. van de Sluis, M. Stuip
Thales Air Systems GmbH	G. Schichtel, J.-M. Kraus, H. Neufeldt
Thales Air Systems SA	B. Pauly, F. Orlandi
Airbus Defence and Space APSYS	S. Bravo Muñoz, J.P. Heckmann, M. Feuvrier
Civil Aviation Authority UK	L. Young, A. Eaton, T. Longhurst, S. Barker, C. Gill
ISDEFE	I. Etxebarria, C. Regidor Gil
CertiFlyer	G. Temme, M. Heiligers
Avanssa	N. Aghdassi
Ebeni	A. Simpson, J. Denness, S. Bull, M. Shuker
Deep Blue	L. Save
JRC	W. Post, R. Menzel
JPM	J. P. Magny
TU Delft	R. Curran, H. Udluft, P.C. Roling
Institute of Aviation	K. Piwek, A. Iwaniuk
CAO	A. Ortyl, R. Zielinski
EASA	E. Isambert
FAA	J. Lapointe, T. Tessitore
SESAR JU	P. Mana
Eurocontrol	E. Perrin
CAA Netherlands	R. van de Boom
JARUS	R. van de Leijgraaf
SRC	J. Wilbrink, J. Nollet
ESASI	K. Conradi
Rockwell Collins	O. Bleeker
Dassault Aviation	B. Stoufflet, C. Champagne
ESA	T. Sgobba, M. Trujillo
EUROCAE	A. n'Diaye
TUV NORD Cert GmbH	H. Schorcht
FAST	R. den Hertog

Acronyms

Acronym	Definition
AFM	Aircraft Flight Manual
ACAS	AirborneCollisionAvoidance System
AIS	Aeronautical Information Service
ALARP	As Low As Reasonably Practicable
AMC	Acceptable Means of Compliance
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
AoC	Area of Change
ATM	Air Traffic Management
ATN	Aeronautical Telecommunications Network
AutoFailMS	Autonomous Failure Management System
CAA	Civil Aviation Authority
CCL	Common Certification Language
CNS	Communication, Navigation and Surveillance
AP	Autopilot
CS	CertificationSpecification
CSM	Continuous Safety Monitoring; Common Safety Method
EASA	European Aviation Safety Agency
EC	European Commission
E-OCVM	European Operational Concept Validation Methodology
EU	European Union
FANS	Future Air Navigation System
FAST	FutureAviation Safety Team
FHA	Functional Hazard Assessment
FMS	Flight Management Systems
FCOM	Flight Crew Operation Manual
EGPWS	Enhanced Ground Proximity Warning System
ICAO	International Civil Aviation Organization
IMA	Integrated Modular Avionics

Acronym	Definition
MET	Meteorological Data
PSSA	Preliminary System Safety Assessment
RNP	Required Navigation Performance
RVSM	Reduced Vertical Separation Minima
RPA	Remote Piloted aircraft (referred only to the aircraft)
RPAS	Remote Piloted Aircraft System (RPA+RPS+C2 link)
RPS	Remote Pilot Station
SESAR	Single European Sky ATM Research
SSA	System Safety Assessment
STCA	Short Term Conflict Alert
TAS	Total Aviation System
UAV	Unmanned Aerial Vehicles
VNAV	Vertical NAVigation

Terminology

Airspace Class A	All operations must be conducted under IFR. All aircraft are subject to ATC clearance. All flights are separated from each other by ATC.
Airspace Class B	Operations may be conducted under IFR, SVFR, or VFR. All aircraft are subject to ATC clearance. All flights are separated from each other by ATC
Airspace Class C	Operations may be conducted under IFR, SVFR, or VFR. All aircraft are subject to ATC clearance (country-specific variations notwithstanding). Aircraft operating under IFR and SVFR are separated from each other and from flights operating under VFR, but VFR flights are not separated from each other. Flights operating under VFR are given traffic information in respect of other VFR flights
Assurance contract	An assurance contract is a documented formal arrangement between two or more modules within argument architecture.[1]
Autonomous mode	Highest automation mode. In the autonomous mode, the RPAS can adapts its speed and execute flight commands received from ATC, it can as well take decisions relative to failure management or/and to an external event. In this mode the remote pilot is considered as a backup. The remote pilot can, at any moment, revert to manned mode.
Collision Avoidance	The capability to take the appropriate avoidance action. Designed to act only if Separation Assurance has been breached. [9]
DAL	All of those planned and systematic actions to substantiate, at an adequate level of confidence, that errors in requirements, design and implementation have been identified and corrected such that the system satisfies the applicable certification basis [9]
Datalink	In this Use Case the term datalink refers to the communication datalink between the ATC and the RPAS.
Detect and Avoid	The capability to see, sense or detect conflicting traffic and take the appropriate action. ('Detect and Avoid' is the combination of 'Separation Assurance' and 'Collision Avoidance') [9] The D&A capability considered here only addresses hazards arising from the vicinity of other airborne aircraft. The definition therefore differs from that of ICAO which considers other hazards such as weather or ground based obstacles.
Intermediary mode	Automation modes between manned and autonomous mode, depending on flight characteristic (weather conditions, type of airspace...) several mode of automation can be envisaged. The characteristics of each potential intermediary mode are not in the scope on this Use Case

Manned mode	Lowest automation mode. The RPAS is totally manned by remote pilot, AutoFailMS deactivated. Note: Certain logics related to recovery actions referred to one single system (e.g. switch to emergency electric bus bar after total loss of normal electric bus bar) might be implemented in the RPAS. This implementation might be active at any autonomy level
Manned on-board aircraft	Current aircraft manned by pilot on board
Pilot in command	Pilot responsible for a flight, either on board or on a remote pilot station
Pilot on board	Pilot in the aircraft
C2 link	The datalink used for the purpose of command and control functions in a RPAS., RPAS C2 functions are usually separated into telecommand and telemetry[8]
Remote back up station	Secondary remote station. A remote back up station provides a backup solution in case of failure of the primary remote station
Remote Pilot	Pilot in a remote pilot station located on ground
Remote Pilot Station	Cockpit located on ground.
Remote primary station	Remote station associated to a specific flight.
Second failure	Second Failure is considered as any failure on RPAS systems that the AutoFailMS, already in failure, is expected to manage.
Telecommand	Telecommand regroups information coming from the remote pilot station (RPS) where the RPIL is located to the RPA (uplink or forward link). [8]
Telemetry	Telemetry regroups information coming from the RPA to the RPS (downlink or return link). [8]
Uncontrolled RPAS	The term "uncontrolled RPAS" is used in this Use Case to refer to an RPAS that cannot be managed by the remote pilot (e.g. loss of C2) nor by the AutoFailMS (loss or erroneous AutoFailMS).

This page is intentionally left blank

Executive Summary

One of the objectives of ASCOS projects is to build a certification methodology that could consider changes where several stakeholders are involved, this certification methodology should not only establish sound safety objectives on a shared change but as well to ensure that the potential new hazards created by that change are actually considered. ASCOS Deliverable D1.3 has defined a high level certification methodology that meets both objectives, this methodology is based on claims and sub-claims decomposition and allows considering current standards as a part of the methodology (safety standards used for product development and standards for safety assurance in operation) This global methodology addresses the interface between stakeholders following the claim and sub-claim structure; in this use Case the interfaces has been managed by analyzing the impact of the stakeholders on each other and proposing standards (or modification in the current standards) that enable to answer to the claims and subclaims.

The chosen system is the Automated Failure Management System (AutoFailMs) installed on an RPAS, that system replaces the pilot in all decision making and surveillance tasks normally performed by a pilot on board, in case of failure, both the AutoFailMs and the ATM need to answer in a coordinated way so the potential safety effects were mitigated.

This Use Case applies the proposed ASCOS D1.3 certification methodology in two different ways:

- First, this Use Case applies the ASCOS D1.3 certification methodology to the AutoFailMs installed in an RPAS in order to test how this approach (as documented in ASCOS D1.3) can provide a common certification methodology that enables a certification for a change to the Total Aviation System.
- Second, this Use Case uses the ASCOS D1.3 methodology to suggest improvements to further develop the common safety standards (e.g. EUROCAE ED_78A) already existing.

This Use Case concludes that

- In general terms, the claim structure proposed originally does not necessarily match the standards. However it is possible to tailor the proposed ASCOS certification methodology (as documented in ASCOS D1.3) in order to adapt it. This process of tailoring and refinement is described in Section 7.1.

- The ASCOS methodology D1.3 can also being used to further develop current standards. It has been found out that the ARP4754A/ED79A could be improved by the introduction of the ATM interface and that the human quality assurance (Human DAL) needs to be developed. The proposed ASCOS methodology D1.3 has also been used to perform a high level revision of a potential adaptation of EUROCAE ED_78A to general operations. It has been found out that the proposed ASCOS D1.3 certification methodology could suggests improvements to the EUROCAE ED_78A.

Content

List of Figures

List of Tables

This page is intentionally left blank

1 Introduction

1.1 Background

As long as the technology advances, new solutions are proposed for old problems. The efficient and fast transports of goods can now be safely achieved by aircraft without pilot on board; therefore, it is possible to envisage dangerous and risky transport routes without facing the risk of losing a human life. However, this type of aircraft might be expected to fly over populated areas, so it needs to be compliant with rules applied in non-segregated areas. The introduction of remote piloted aircraft in non-segregated areas implies several challenges, in case on an emergency, the old procedures might not be safe enough, it is basic then to define a certification approach that enables the RPAS system and the ATM to provide a common acceptable safety level in all situations.

1.2 Objectives

The main objective of this use Case is to test the D1.3 methodology in Autonomous Failure Management Systems installed on a RPAS. The methodology is tested under two approaches:

First approach: the methodology proposed in ASCOS by D1.3 is applied by applicants (meaning partners acting together) to demonstrate that all the requirements (for the TAS as a whole) are met. In this approach, this Use Case develops a common set of safety objectives and safety requirement for the introduction of an RPAS supported by “AUTOnomous FAILure Management System” (AutoFAilMs) in a non-segregated airspace.

Second approach the methodology proposed in ASCOS by D1.3 can be applied by a stakeholder group1 to gather specifications and supporting material which define the requirements for a change. In this approach this Use Case established a comparison between D1.3 and ED_78A. from current scope (datalink applications) to a broader scope to be applied to operation, processes and services in TAS.

1.3 Approach

This Use Case covers two approaches as presented in previous subchapter.

- First approach is developed all along the Use Case following the steps suggested in D1.3 methodology (stage 1, stage 2…), the conclusion of D1.3 application is summarized in chapter 7.1.
- The second approach is developed in 7.2.

Chapter 2 Stage 1 of D1.3 methodology

[1]Stakeholder group: to be understood as a group of industrial and operational partners developing RPAS products and operations (aircraft manufacturers, RPAS operators, ANSPs, maintenance and training organizations, etc)

According to D1.3 methodology [2] stage 1 "*is focused on ensuring that the proposed change*[23] *to the TAS is fully understood*" This chapter presents in first place the general functional architecture of the RPAS proposed (refer to 2.2), in second place the basic concept of the failure management (refer to 2.3), in third place the Autonomous Failure Management System which is the scope of this case study. (Refer to 2.4) and finally the interfaces that are impacted by the introduction of the change (refer to 2.5)

Chapter 3 Stage 2 of D1.3 methodology:

This chapter presents the proposed structure for the argument that the implementation of a failure management system (Autonomous Failure Management System) contributes to an acceptable level of safety for the operation of RPASs, according to the first approach

Chapter 4: Stage 3 of D1.3 methodology

This chapter presents the certification plan; it proposes a certification plan for the Total Aviation System

Chapter 5: Stage 4 and Stage 5 of D1.3 methodology

This chapter defines the safety objectives, requirements and assurance level that is required to meet the requirements defined in stage 2

Chapter6: Stage 6 of D1.3 methodology

This chapter redefines the certification argument in stage 2 by including all the find outs in chapter 4 and chapter 5

Chapter 7. Recommendations for D1.3 and application of D1.3 to ED_78A

Chapter 7 is divided into two subchapters. Subchapter 7.1 that summarizes all the recommendation for D1.3 as a result of the application of D.1.3 to this Use Case, and subchapter 7.2 that presents suggestion of the ED-78A improvement due to the application of D1.3 methodology

2 Stage 1: Define the change

2.1 Introduction

The purpose of this chapter is to describe the change proposed by the Use Case 4.1. The change consists in the Autonomous Failure Management System of a Remote Piloted Aircraft System.

This chapter presents in first place the general functional architecture of the RPAS proposed (refer to 2.2), in second place the basic concepts of the failure management (refer to 2.3), in third place the Autonomous Failure Management System which is the scope of this case study. (Refer to 2.4) and finally the interfaces that are impacted by the introduction of the change (refer to 2.5)

In Appendix A, it has been included a complete list of all additions and/or modifications of the RPAS in comparison with manned aircraft.

2.2 Presentation of the RPAS

The RPAS is conceived as a modification of a civil cargo piloted aircraft similar in size to an A320. RPAS is expected to fly in airspace class A, B and C.

The RPAS presents several modes of autonomy, from autonomous mode to manned mode. In the autonomous mode, the RPAS can adapt its speed and execute flight commands received from ATC, it can as well take decisions relative to failure management or/and to an external events. In this mode the remote pilot is considered as a backup. The remote pilot can, at any moment, revert to manned mode.

In manned mode the remote pilot performs all functions currently allocated to a pilot on board, specific sensors and cameras can be envisaged to replace the physical sensations of a pilot on board. The RPAS is permanently automatically protected by system (flight envelope limitations, protection against stall, overrun…). These protections are already in place in the current aircraft. The level of protection corresponds to the level of the law used by flight controls (normal laws to direct laws).

The “see and avoid” duty performed by the pilot is replaced on the RPAS by a “detect and avoid” function based on specific sensors having capability to detect small, non-cooperative traffic (e.g.: gliders, VLAs), in particular when flying in class B or C airspaces.

The remote pilot communicates with the RPAS thought a C2 link. The C2 is used for transmitting commands from remote pilot station to RPAS (telecommand) and for transmitting data from RPAS to remote pilot station (telemetry). The remote pilot station is similar to current cockpit. For the purpose of Use Case, the performance of the C2 link is sufficient for the continuity and integrity of the function, in the case of erroneous/loss C2 link between the RPAS and the remote pilot station the AutoFailMS will manage the failure.

The RPAS is transparent for the ATC, a priori; the only procedures that are expected to change are relative to a “loss of RPAS control” or “erroneous management of RPAS” situation.

2.3 Approach to Failure Management

On a piloted aircraft, the pilot on board is ultimately responsible for safety during flight, in an RPAS; the remote pilot remains as well responsible for the safety. However, in a RPAS, certain failure such as loss of C2 link or total loss of remote pilot station might lead to a situation on which the RPAS cannot be manned by a pilot. The RPAS needs to be supported by an Autonomous Failure Management System that enables the RPAS to manage the failure modes and provides a level of safety equivalent to manned aircraft. The Autonomous Failure Management System can as well provide flight management and replace the pilot on board in normal conditions, in this situation, the remote pilot remains as a backup.

The role of the remote pilot and the appropriate level of automation for each aircraft function depends on the characteristics of the functions (e.g. the pilot remains responsible or aircraft trajectory, therefore, flight plan modification should be validated by remote pilot) and on the severity and reaction time required after a function failure (e.g. emergency procedures might be totally autonomous at any automation mode).

This chapter presents basic concepts of failure management, it analyses the pilot family procedures and suggests a failure management policy for each family.

To sum up:

- Functions and function failures management without pilot action should be totally autonomous with remote pilot being informed
- Functions and function Failures management leading to pilot action should be automated after pilot validation/confirmation
- At any moment the remote pilot may to revert to manned mode

2.3.1 Failure Management basic concepts

2.3.1.1 Failure detection

In a manned aircraft with on board pilot most of the failures are detected by the aircraft systems and by the pilot through different means of detections (e.g. Flight Warning System, Control Data System …) however some failures modes are only detectable by pilot on board, for example the physical sensation due to aircraft behavior in reaction to controls on attitude or acceleration/deceleration. In this sense, the pilot can be considered as detection means.

For an RPAS Failure Conditions detected by the systems with actual usual means are transferred to the remote pilot. It is considered that all the data available in the cockpit for an on board pilot are also available for the remote pilot

The failure conditions only detectable by on board pilot require unusual means of detection, the RPAS is supposed to be equipped with:

- New sensors (fire, smoke, vibrations, pressure …)
- Video camera for remote pilot information

2.3.1.2 Consideration of concept of isolation of failures and Reconfiguration/ diagnosis

On an onboard piloted aircraft, after failure detection, the system isolates it in order to avoid propagation. Depending on the failure, autonomous isolation can occur or isolatation can be performed by pilot on board applying procedures (e.g. stop engine on fire)

In an RPAS, the isolation of a failure is totally autonomous and does not require the validation of the remote pilot except in the following cases:

- Failures Conditions only detected by Remote Pilot.
- Remote Pilot Request (non application or erroneous application of actions & procedure, detection of a spurious Alert …)

2.3.1.3 Management of the failure

In a normal aircraft, after the failure isolation, the pilot on board decides the proper action: This action can be classified in a family procedure

- EMERGENCY procedure / Warnings requiring immediate action to avoid critical situation or loss of A/C control (e.g. ELEC - EMER CONFIG, SMOKE procedure, Engine FIRE)
- Cautions which are not considered as emergency cases requiring pilot action (not necessary immediate) or leading to pilot workload(degradation in law, speed / performance limitations, degradation of functionalities)
- Cautions for awareness (loss of redundancy, speed/performance limitations)
- Normal procedures: procedures established and recommended by the aircraft manufacturer for particular operations which are considered useful to highlight (e.g. Preflight Checks, Take-Off or Approach procedures ….)

In this Use Case, the RPAS can be managed in several levels of autonomy. In the manned mode, the remote pilot manages all failure conditions; in the total autonomous mode the following approach is proposed:

<u>Emergency and Cautions:</u>

- For emergency procedures, immediate and autonomous application by system of appropriate action / procedure: The failure condition is autonomously managed and remote pilot is considered as a back-up.
- For cautions with actions, autonomous application by system of appropriate action / procedure after validation or confirmation by remote pilot (isolation of failure, automatic reconfiguration) or automatic recovery reconfiguration allowing remote pilot to understand the situation and to take appropriate action if needed
- For cautions without pilot action (only for pilot awareness), autonomous application by system of appropriate action (isolation of failed source, automatic reconfiguration on available source) and

application of the potential speed or performance limitations. The remote pilot has to be informed of the failure and A/C configuration.

Normal procedures

The normal procedures are applied in each flight in normal situation. The normal procedures concern particular operations which are considered during a flight: Preflight checks, TO/ approach procedures, cruise procedures (turbulences) and procedures associated to different A/C systems (Auto flight system, Navigation, Fuel, Ice and Rain protection). Note that basic airmanship can be also considered as a normal procedure. For an RPAS, normal procedures can be managed as following:

- Autonomous management of procedures (specific checks, TO and approach procedures) with validation or confirmation by remote pilot to the correct application of procedure (The remote pilot is responsible for the aircraft trajectory and is informed about the trajectory updates/modifications. In any case the pilot can take the control of the aircraft and responds to trajectory updates/modification. In an autonomous mode the remote pilot validates the trajectory modifications.)
- Basic airmanship and specific procedures will be manually managed (permanent monitoring of data, flight conditions, specific check in TO / approach, …)

Unexpected event

By definition, an unexpected event cannot be anticipated and by consequence cannot be automatically managed. However, it can be considered that such event can lead to erroneous behavior of A/C or can be detected by an A/C system or other means (remote pilot, ATM).

For an RPAS, unexpected event can be managed as following:

- Possible detection of the unexpected event by an A/C system with usual means or unusual means (possibility to introduce in RPAS new means of detection (specific sensors, camera videos..) or possible detection by remote pilot, ATM or others means (traffic control, visual control, erroneous A/C behavior …)
- If detected by an A/C system, unexpected event can be automatically managed and remote pilot will be considered as a back-up: autonomous recovery reconfiguration allowing remote pilot to understand the situation and to take appropriate action if needed.
- If not detected by an A/C system, unexpected event will be manually managed by remote pilot (possibility to command an autonomous recovery reconfiguration allowing remote pilot to take time to understand the situation and to take appropriate action if needed)

2.4 Description of the Autonomous Failure Management System

The Autonomous Failure Management system function is to detect and react to failures of the RPAS and to respond autonomously to these failures as far as possible (using reconfiguration of the systems on the aircraft where appropriate), with the intention to remain on the original intended flight path if possible.

From the point of view of aircraft architecture the AutoFailMS is divided into two sub systems, the Failure Management sub-System (FailMS) and the Failure Reconfiguration sub-System (FailRS). The main difference among them lies in the logic implemented.

The FailMS considers the continuous monitoring of system status and the decision making process (prioritization) usually performed by the pilot during the course of the flight. The FailMS assesses the aircraft system technical status and authorize reconfiguration of aircraft systems in abnormal situation according to prioritization rules implemented on FailMS logics.

The FailRMS is in charge on failures and reconfiguration associated to one single system and it replaces the pilot on board in all those procedures that can be automated internally to one single system (e.g. in an aircraft equipped with several RA, pilot inhibits erroneous RA data and continues flying with remaining RA). The FailRMS, itself, is implemented internally to each system and it can be considered as an evolution of the current failure management already existing in the current systems. The FailRS collects the data of system status and transmits them to the FailMS.

Failure Management System

The failure management systems considers the continuous monitoring and decision making process usually performed by the pilot during the course of the flight: Go Around decision, monitoring of adherence to flight plan / to trajectory constraints, decision to reject take-off, fire procedures, conduct of ditching / crash-landing, etc.

This entails that the system should handle autonomously all the actions that are normally performed by a pilot, as set per the FCOM Normal and Abnormal procedures as example:

- Decision to use the reverse thrust
- Decision of diverting to an emergency site.
- Fuel management/monitoring.
- Flight performance optimization (speed / altitude)
- Prioritization in case of conflict of reconfiguration between different systems.
- Automation level (pilot can chose the automation level delegated to the airborne systems)

Specifically this entails that the FailMS could handle abnormal procedures involving multiple aircraft systems as well as the monitoring of the FailRMS functionality (see below).

Failure reconfiguration System

The management of failures reconfiguration has to be distributed primarily between the different aircraft systems. Each aircraft system shall be capable to handle as planned its own reconfiguration in case of failure. This capacity shall be implemented consistently in each of the aircraft systems under the overall supervision of the FailMS (above) in order to prevent that incompatible or conflicting reconfigurations are applied simultaneously on different systems and to set priorities in case of conflicting reconfigurations. FailRMS will handle:

- Reconfiguration on failure in case failure reconfiguration that does not require a prioritization of the recovery actions amongst the different systems.
- Abnormal procedures applying on one system.

2.5 Interfaces with other TAS stakeholders

In developing the AutoFailMS it becomes apparent that changes are introduced not only to the RPAS, but also to other domains involved in the specification, development, production, operation and maintenance of the AutoFailMS. The changes are investigated by looking at the interfaces the AutoFailMS has with these domains that have been made visible in Figure *1*

The AutoFailMS essentially replaces the pilot in the management of failures on-board the RPA. In the case when one or more failures occur in the aircraft, the pilot has to follow the failure management *instructions*. In manned aircraft the Normal and Abnormal procedures are usually documented by the aircraft manufacturer in the Flight Crew Operation Manual (FCOM) and/or the Aircraft Flight Manual (AFM).

The assumption made in this case study is that the aircraft failure management instructions for the pilot can all be automated for execution by the AutoFailMS.

The AutoFailMS deals with the failures that comes from the RPA systems (box "aircraft" in Figure *1*). These *failures* are detected by the AutoFailMS. In order to handle the failure properly (execute the appropriate procedure) information on the *aircraft status* is a required input for the AutoFailMS. When AutoFailMS executes such a procedure, the AutoFailMS must be able to send commands to systems in the aircraft (e.g. systems that must be reconfigured).

While the AutoFailMS is specified to be able to manage the failures with a great deal of autonomy, it is still important that the RPAS remote pilot is kept aware of the status of failure management in the RPA by the AutoFailMS. The remote pilot must receive *information* on the failures that have been managed. Furthermore, it could be the case the remote pilot still needs to be involved in the failure management process, e.g. in case the AutoFailMS design allows for crew actions for overriding or vetoing of AutoFailMS failure management actions.

The RPAS is interfaced with the operator organisation. It is important that the RPAS operator organisation is kept aware of the *status* of failure management in the RPA by the AutoFailMS.

The RPAS is also interfaced with maintenance by the maintenance organisation. An interface must exist that allows for exchange of data for maintenance purposes. E.g. the maintenance organisation could *request* the

AutoFailMS to report on the *health status* of the RPA systems (this can be considered as a complement to the BITE system)

When the AutoFailMS executes failure management procedures, this may have an impact on the operation of the RPA. Air Traffic Control organisation must be *alerted* on the failure situation of the RPA when this has impact on the execution of the flight plan (e.g. in the case of a lost C2 link when a contingency procedure is executed automatically by the RPA). The RPA is a type of aircraft that is – in some aspects – different from manned aircraft, that it is very likely that it will lead to changes in ATC for handling RPAS traffic.

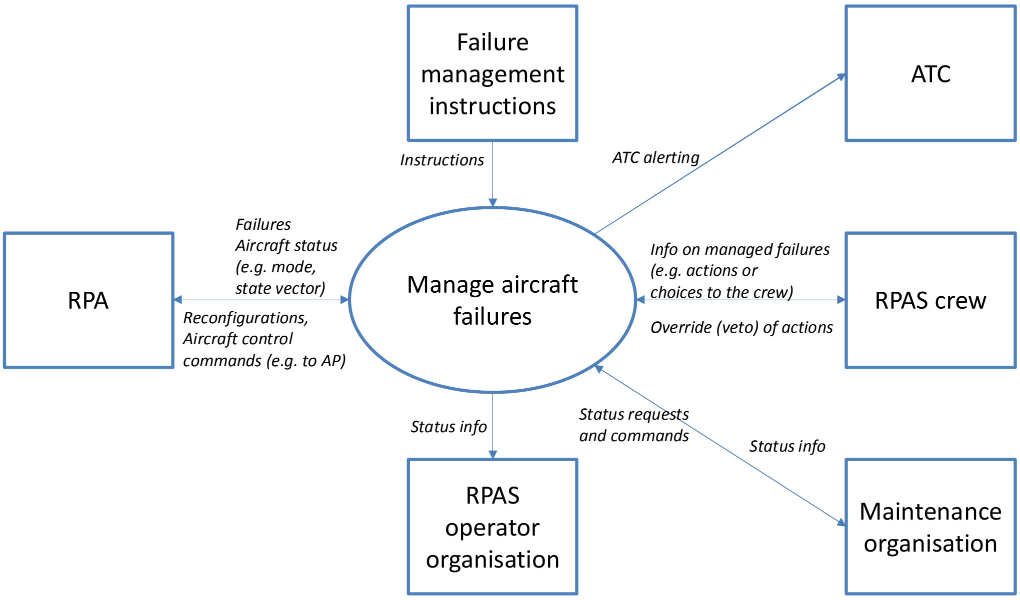


Figure 1 AutoFailMS concept

The main interfaces impacted by the introduction of AutoFailMS are the ATC and the pilot described below,

2.5.1 Air Traffic Control

This section describes the perspective of Air Traffic Control (ATC) in the definition of the change. Air Traffic Control is (ATC) is one of the services provided by an Air Navigation Service Provider (ANSP) as part of the bigger scope of ATM.

The AutoFailMS is a subsystem of the RPAS and (as can be seen in Appendix A) it has a functional interface with ATC. The introduction of the AutoFailMS is part of a larger change, i.e. the change from manned cargo aircraft to unmanned cargo aircraft, which is a situation that does not yet exist today . Therefore we need to make a number of assumptions on the involvement of ATC in this situation, for which we need an analysis on RPAS-ATC level.

For this analysis the main inputs are the considerations from the CANSO report on RPAS [12], which identifies the issues that need to be addressed to safely achieve greater RPAS integration in the future.

Air traffic management integration of RPAS will be safely achieved when routine access by RPAS operations into non-segregated airspace, is transparent to ANSPs. Therefore, the RPAS remote pilot will be required to respond to ATC guidance or requests for information, and comply with any ATC instruction (e.g. fly headings, altitudes, Navaids and Waypoints and comply with standard IFR approach and departure procedures), in the same way and within the same timeframe as the pilot of a manned aircraft.

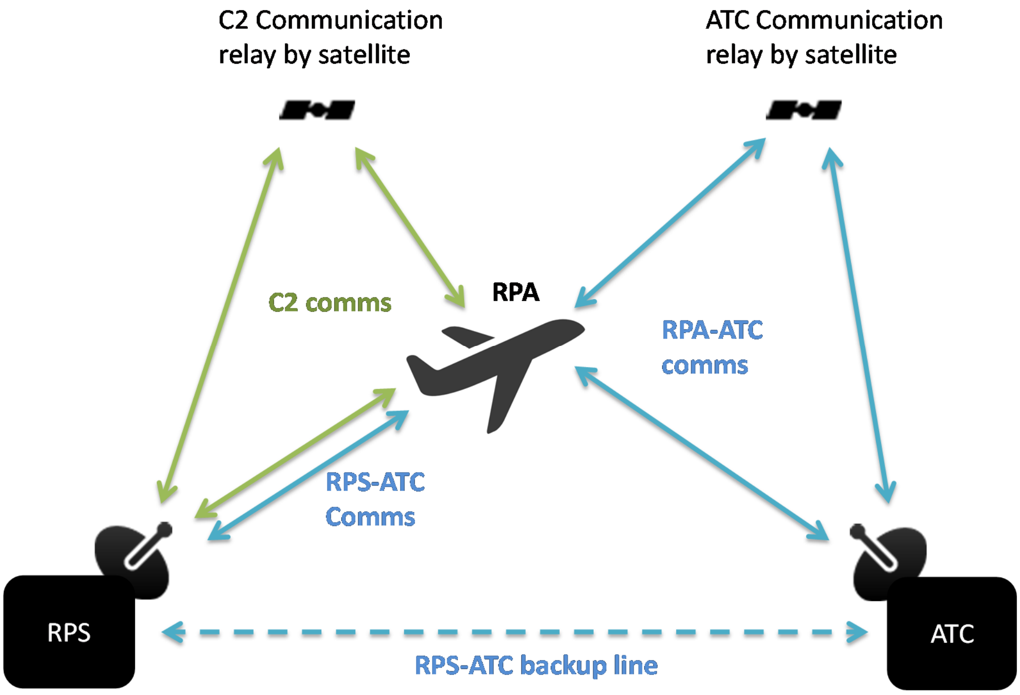


Figure 2 RPAS and ATC communication

Given the RPAS and ATC communication diagram of Figure *2* a number of assumptions on the design of the RPAS system its operation in relation with Air Traffic Control are given below:

- Similarly as with manned traffic Air Traffic Controllers have contact with the RPAS by means of radio communication or by digital data link (VHF terrestrial or via satellite communication).
- The RPA serves as a relay for the voice and data communication between the Air Traffic Controller and the remote pilot.
- In case of loss of communication between RPA and ATC, the ATC could communicate directly with the remote pilot via the backup line.
- As in normal conditions the RPA performs the flight automatically, it is assumed that the RPA is able to perform standard communication with ATC (follow up clearances, respond to requests, etc.). The remote pilot is responsible for the proper execution of the filed flight plan and is monitoring.
- In non-normal conditions the pilot takes over the control of the RPA and communicates with ATC.

Currently, the seamless integration of RPAS into non-segregated airspace has not yet been established. CANSO report [12] lists aspects where special handling of RPAS by ANSPs is required. This list is repeated below, together with any assumptions/effects for this specific case study.

ATC aspects of RPAS	Description [12]	Assumptions for ASCOS study
ATC phraseology	Ideally, RPAS would require no special handling from ATC and therefore would not require any additional ATC phraseology. However, the RPAS programme has not matured enough to be considered as normal ATC operations, especially for contingency operations because of the unique nature of individual RPAS. There is currently no approved, standard RPAS-related ATC phraseology and this will have to be developed and agreed prior to operations.	It is assumed that ATC phraseology has been established, including those for abnormal and emergency situations.
RC2 Datalink	If the RC2 datalink is operating via a satellite, there may be latency in the response to ATCO instructions. If the RPAS C2 datalink is operated by Radio Line of Sight (RLOS), then the RPA may have minimum flight altitudes below which it cannot operate safely.	It is assumed that the RPAS operates both within and beyond RLOS. The latency introduced by the C2 datalink may contribute to potential hazards.
In-Flight Characteristics	The RPAS may also have different in-flight characteristics to manned aircraft, such as a slower than expected airspeed, a slow rate of climb or a preference to spiral climb rather than an en-route climb. The flight profile of an RPAS may also be different to manned aircraft, which normally route from A to B via C, whereas the RPAS may take off and land at the same airport having conducted its mission, that is, from A to A, having orbited at C. Therefore, it will be important for ATC to establish whether the RPAS will be transiting through a sector, or remaining within a sector ‘on task’ either flying a race track or orbit.	It is assumed that RPAS performs cargo flight from A to B, similar to current cargo planes.
Flight Data Processing (FDP) systems	FDP systems may have difficulty processing RPAS flight plans, due to elements such as the flight profile, duration of the flight, inability to specify ‘zero’ persons on board and alerting requirements. For example, the RPA may wish to complete a spiral climb from the aerodrome of departure or may remain airborne for more than 24 hours, both scenarios that would be difficult to define in a standard flight plan.	It is assumed that necessary FDP system modifications have been implemented to allow for RPAS specific flight plans.

ATC aspects of RPAS	Description [12]	Assumptions for ASCOS study
Alerting Services	Alerting Services are provided for all aircraft provided with air traffic control service, or that have filed a flight plan, or are believed to be the subject of unlawful interference. Current ICAO regulations do not differentiate between manned and unmanned aircraft; however some States are reviewing and considering adapting the application of alerting services for RPAS.	It is assumed that necessary alerting services are in place to allow for RPAs that are under air traffic control services.
Utilisation of existing IFR Procedures	Most current RPAS are not fitted with standard, certificated avionics. This means that they cannot utilize existing civil published IFR approach procedures, e.g. ILS, VOR, DME or RNAV, or conduct a standard departure or fly en route procedures, including RVSM.	It is assumed that the RPA is fitted with certificated CNS/ATM equipment that allows for the civil published IFR approach procedures.
Detect and Avoid, Collision Avoidance	In manned aviation it is the pilot-in-command's responsibility to detect and avoid potential collisions and other hazards. Similar requirement exists for RPAS, but there are currently no certified DAA systems available.	It is assumed that the RPAS includes a certificated Detect and Avoid system that allows for flight within non-segregated airspace. As in manned aviation ATC is responsible for separation assurance, while the RPAS remote pilot is responsible to avoid collisions.
Contingency and Emergency Operation Procedures	RPAS emergency procedures should mirror those for manned aircraft as far as practicable. However, because of their unique attributes (mainly, although not exclusively, because the pilot is not on-board), in some cases new procedures will have to be developed by ANSPs to accommodate RPAS, taking into account unique RPAS failure modes such as lost C2 link.	It is assumed that specific Contingency and Emergency Operation Procedures have been established for the RPAS (as part of the operational certification). Basically the RPA behaves in a predictable manner. ATC is fully informed and trained to apply these procedures. E.g. in case of loss of C2, the procedure could involve alerting the ATC and airspace users of the situation (squawk code), the use of a backup line for RPS to ATC communications, predetermined flight or holding patterns and predefined flight completion options (alternate landing sites or in rare cases, terminate the flight by controlled flight into terrain (CFIT) at a pre-determined point That is known to be unpopulated).

Table 1 ASCOS assumptions for RPA related to ATC

The table above indicates that a number of systems are assumed to be in place to enable the RPAS to operate as a cargo aircraft under Air Traffic Control in non-segregated airspace. The AutoFailMS is designed to manage the failures of these systems and to alert ATC on the status of this failure management. Examples are the failures or loss of the C2 link, failures of the Detect and Avoid systems. With this knowledge ATC can then take appropriate actions.

2.5.2 Remote pilot

The RPAS presents several modes of autonomy, in the manned mode the pilot performs all actions as per today, in the autonomous mode the RPAS flights autonomously while remote pilot remains as a backup. However, even in the autonomous mode the trajectory is owned by the remote pilot who knows which are the limits of the aircraft for the current fuel, weight and balance conditions. The remote pilot needs to agree on trajectory or speed modifications requested by the ATC. Then, the aircraft updates the trajectory and the remote pilot informs the ATC. Handling of ATCo instructions of immediate execution (e.g.: Go Around) may require specific arrangement between ATC and RPAS operational organizations

The remote pilot can, at any moment, revert to manned mode. In manned mode the remote pilot performs all functions currently allocated to a pilot on board, specific sensors and cameras can be envisaged to replace the physical sensations of a pilot on board. The cockpit can be enriched with data from aircraft around in a better way than normally

In case of failure if the aircraft is in manned mode the pilot will need to execute action as per today, in the autonomous mode the AutoFailMS systems manage the aircraft, the pilot is informed according to the policy: described in 2.3.1.3 To remind:

- Functions and functions failure without pilot action can be totally autonomous
- Functions and function Failure leading to pilot action can be
    - Automated after pilot validation/confirmation
    - Automated after pilot being informed (pilot can any moment revert to manned mode)

For more details refer to 2.3

2.5.3 Maintenance

Maintenance activities are not expected to be largely impacted. The interface between the RAPS and the maintenance team will be defined under the same principles that current manned aircraft.

2.5.4 RPAS operation organization

This is the company that owns and operates the RPAS; this interface plays a major role on stage 4 and 5 that are not addressed in this analysis.

2.6 Conclusion

Operational description of RPAS operations assisted by AutoFailMS and environmental assumptions:

Item	Description
The overall goal of the change.	The introduction of a civil cargo RPAS in non segregated airspace class A, B and C. The RPAS is supported by an Automatic Failure Management System.

Item	Description
Definition of the change to be made.	The function of the Autonomous Failure Management System (AutoFailMS) is to detect and react to failures of the RPAS and to respond automatically to these failures as far as possible (using reconfiguration of the systems on the aircraft where appropriate), with the intention to remain on the original intended flight path if possible. Where failures make it infeasible to complete the flight with a safe landing at the original intended destination, the Failure Management System will divert the aircraft to the (most appropriate) predefined alternative landing site. In the event of a failure which cannot be handled by the Failure Management System, it will hand control over to the remote pilot supported by sufficient diagnostic information to allow the remote pilot to make an informed decision regarding the continuation of the flight. The Failure Management System also provides full diagnostic information to the remote pilot, including all the information which would normally be available on the aircraft flight deck, supplemented by additional context information which would normally be detectable by the pilot through his presence in the cockpit. The argument presented in this document applies to the Autonomous Failure Management System.
Definition of the time frame for the actual implementation of the change (target year)	The timeframe could be 2025+, as this is roughly in line with integration of RPAS IFR flights in Europe, as defined in the EURoadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System RPAS (European RPAS Steering Group, June 2013).
Areas of Change that have an impact on the modification	Please refer to Appendix C.
Part(s) of the system will be changed	Main stakeholders impacted are remote pilot and ATC, maintenance activities are briefly described. Aircraft operator is considered out of the scope of this Use Case. Refer to 2.5
Organisations are involved in making the change	Aircraft manufacturers (DOA, POA) Maintenance organisations Aviation Authorities (EASA, NAAs) Standardisation groups (Eurocae, RTCA, SAE), Air Navigation Service Providers (national and Eurocontrol), Airports, Airlines, Training organisations
How the external environment may be affected by the change	Introduction of an RPAS should be transparent for the ATC. See 2.4
Initial argument architecture	RPAS operations assisted by AutoFailMS must keep the same level of safety as manned aircraft operators.
Requirements (including safety requirements) the change needs to fulfill	The introduction of the RPAS must achieve a level of safety which is no worse than that achieved in equivalent manned operations

Table 2 ASCOS stage 1 conclusions

Note that the stage 1 has required several updates to provide a description suitable for all stakeholders. Refer to Rec_04

3 Stage 2: Define the certification argument

3.1 Introduction

The argument structure proposed for this case study is developed from the generic argument presented in D1.3 [1] section 3.2. For the purposes of the case study, only claims 1 and 2 of the argument will be developed in detail. The other claims will be developed only in respect of dependencies on and interface to other domains.

We also need to decide **who** should apply the D1.3 approach. We have assumed that the approach is applied in two phases as follows. (This is captured as A0-2 in the argument.)

- **In the first approach,** the approach proposed in ASCOS by D1.3 is applied by applicants (meaning partners acting together) to demonstrate that all the requirements (for the TAS as a whole) are met. This demonstration is supported by the individual demonstrations of each applicant, these individual demonstrations are based on the approach proposed in ASCOS by D1.3 for the ATM and on ARPs/EUROCAE safety standards for the certification of RPAS aircraft and for its operation.(AMC-RPAS.1309_Issue-1 and ARP4754A/ED79A). For more detail of the task of this groups refer to WP 3.5 TESG group. This first approach is developed in sections 2, 3, 4, and 5,.

- **In the second** approach, the approach is applied by a stakeholder group[2] to gather specifications and supporting material which define the requirements for an Autonomous Failure Management System installed on an RPAS. (This may involve developing new specifications where functions and / or interfaces are not covered in existing specifications., refer to paragraphs 3.5.2 and 3.5.3) The overall argument and specifications will be proposed to the Authorities for agreement. The approach will take account of existing specifications, especially for the failure management system itself, while the D1.3 approach will be used to guide development at the TAS level and for interface with ATM.

- This Use Group has identified that the ED 78A/DO 264, follows a similar approach to D1.3. These ED_78A guidelines have been developed by a stakeholder group. This document presents a multi-stakeholder agreement (by prescribing processes such as Operational Environment Definition, Operational Safety and Performance Assessments and Interoperability Assessment) on the inter stakeholder level. However, it was also noted that the ED78A is not sufficient for our WP4.1 case, as proper feedback loops from the different stakeholder domains and the operational phase are not sufficiently included in the ED78A method. This Use Group has established a comparison between D1.3 and ED_78A approach to identify main areas of development of ED78A. .

[2] Stakeholder group: to be understood as a group of industrial and operational partners developing RPAS products and operations (aircraft manufacturers, RPAS operators, ANSPs, maintenance and training organizations, etc)

This split in application of the D1.3 methodology raises the issue of who "owns" the argument – i.e. who is the *argument architect*[3]? Although this is not resolved in the case study, it is a key question for full application of the approach. This Use Case suggests that TESG (TAS Engineering and Safety Group refer to WP 3.5 chapter 7) as a top architect body (TAS Engineering and Safety Group: TESG).

3.2 Claim 0: The failure management system (AutoFailMS) contributes to acceptably safe RPAS operations

Figure 3 shows the adaptation of the top level of the generic argument (see D1.3 [1]section 3.2) to this case study.

The claim is that the Autonomous Failure Management system adequately supports safe RPAS operations. For the purpose of this case study it is decided that it is up to the certification authorities (EASA, CAA, etc) to define the proper level of safety for RPAS operations.

For the purpose of this Safety Case it is agreed that the proper level of safety for RPAS operations means "that introduction of the RPAS must achieve a level of safety which is no worse than that achieved in equivalent manned operations"

Note the following points.

- *The claim covers the lifecycle of the change* – i.e. it covers specification, design and implementation of the AutoFailMS for RPAS; it also covers transition into operation and monitoring while in operation. Each of these elements is covered in a separate subclaim.
- *We do <u>not</u> claim that RPAS operations <u>as a whole</u> are acceptably safe* – we are only considering how the *Autonomous Failure Management System* contributes to the safety of the operation of the RPAS. To make a claim for RPAS operations as a whole, we need to consider significant areas outside the scope of the case study (i.e. the normal operation of an RPAS, including the need for a Detect and Avoid function);
- *We will consider both the positive and negative effects of the Autonomous Failure Management System on the safety of the RPAS* – i.e. we consider how the *Autonomous Failure Management System* benefits the RPAS by "rescuing" it from failures of other systems, as well as how failure of the *Autonomous Failure Management System* itself may threaten the RPAS (and the wider TAS).

[3] See **Error! Reference source not found.** section 2.2.

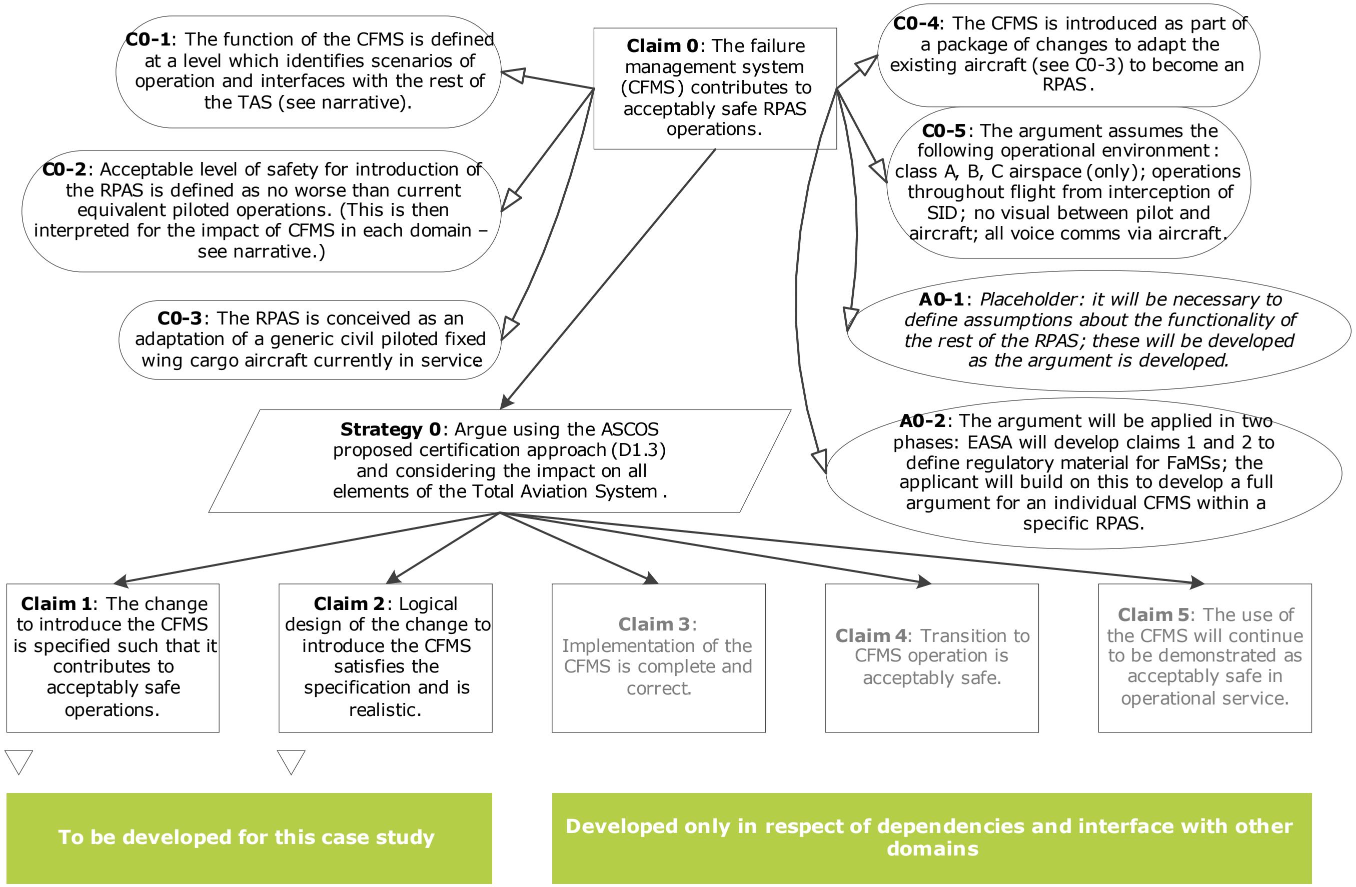


Figure 3 Top Level Argument Structure (Claim 0)

We define items of *context*, to add detail to the claim being made.These items of context are defined further in the following sections.

- **C0-1** provides(a pointer to) the definition, at an abstract functional level, of the operation of the Autonomous Failure Management System
- **C0-2** defines the level of safety which needs to be achieved by the introduction of the Autonomous Failure Management System.
- **C0-3** identifies that the RPAS is conceived as an adaptation of an existing civil piloted fixed wing cargo aircraft.
- **C0-4** identifies that the Autonomous Failure Management System will be introduced as part of a package of changes (to include provision of a Sense and Avoid function) to adapt the existing aircraft (as identified in C0-3) to become an RPAS.
- **C0-5** defines the operational environment to which the safety argument applies.

In addition, we introduce the following assumptions:

- a (placeholder) assumption (**A0-1**) to note that we will need to make a significant number of assumptions about the interface between the Autonomous Failure Management System the other RPAS systems. Refer to 3.2.4, because the proposal is for a change to a hypothetical system (i.e. there is no RPAS of this type currently in operation).
- the assumption (**A0-2**) that the argument is applied in two phases, as discussed in section 3 above.

The top level claim (Claim 0) is then decomposed into subclaims (Claims 1 – 5), each making a "smaller" claim about the Autonomous Failure Management System and its introduction as part of the RPAS system. The premise of the argument is that, when taken together, the subclaims are sufficient to demonstrate that the top level claim has been achieved. **Strategy 0** documents the approach which is taken in subdividing the claim – i.e. the approach proposed in ASCOSD1.3 [1]– which considers specification, design, implementation, transition into operation and operational service. The claims are explained in later sections of this document.

3.2.1 Context C0-1: Definition of operations of the Autonomous Failure Management System

In order to undertake the safety analysis, we need a high level, abstract definition of the operation of the Autonomous Failure Management System and its effect on the other parts of the TAS.

The initial description is made up from:

- a functional description of the operation – see section 2 define the change

- an expansion of this functional description in the form of operational scenarios – see section 3.2.1.1
- the operational environment in which the Autonomous Failure Management System is to operate – see section 3.2.5

3.2.1.1 Operational Scenarios

The analysis within the argument is based on scenarios of operation of the Autonomous Failure Management System and the associated description of the sequence of events in each scenario.

Scenarios describe the operation of the Autonomous Failure Management System, this case the scenarios describe the operation of the Autonomous Failure Management System *as seen from the outside* showing the effect on the rest of the total aviation system (TAS).

Scenarios are divided into three types:

- *normal* scenarios describe the operation of the Autonomous Failure Management System in an "ideal" environment: i.e. in normal conditions of the external system, where the Autonomous Failure Management System itself has not failed in any way.
- *abnormal* scenarios – where the Autonomous Failure Management System is operating outside its usual envelope (e.g. this could be due to (inter alia) incorrect maintenance, incorrect actions by the pilot, severe weather conditions, busy traffic conditions) but the failure management system itself has not failed in any way;
- *(self) failure*[4] scenarios – where the Autonomous Failure Management System itself has failed. Note: at this stage of the analysis we can only consider the consequence of these failures; the causes are considered later.

3.2.1.1.1 Normal scenarios

Analysis of the functional description in "section 2 defines the change reveals the following *normal* operational scenarios:

Ident	Normal Scenarios. AutoFailMS detects a failure and applies recovery action
NS-1	Normal failure-free operation, no intervention required from AutoFailMS (intervention from the AutoFailMS MS would constitute a failure of the AutoFailMS) although it will provide information to the remote pilot

[4]Note, in this context, *(self)failure* refers to failure of the AutoFailMS to function as specified, not to an (aircraft)failure leading to the requirement for an action from the AutoFailMS.

Ident	Normal Scenarios. AutoFailMS detects a failure and applies recovery action
NS-2	Successful reconfiguration of the aircraft systems (by the AutoFailMS MS) following a failure, such that the mission continues according to the flight plan, with no deviation from intended flight path;
NS-3	Successful reconfiguration of the aircraft systems (by the AutoFailMS MS) following a failure before final approach, such that the mission continues according to the flight plan, although with initial deviation (recovered) from intended flight path; *The distinction is made between this scenario and N#2 due to the potential for impact on ATM and other aircraft resulting from the deviation from the intended flight path.*
NS-4	Failure during final approach such that the aircraft must execute a missed approach, followed by successful reconfiguration of the aircraft systems (by the AutoFailMS MS) such that the aircraft can return to land at the intended landing site.
NS-5	Non recoverable failure (but where sufficient control remains to allow successful diversion) before final approach causing diversion (by the AutoFailMS MS) to alternative landing / recovery site;
NS-6	Non recoverable failure (but where sufficient control remains to allow successful diversion) during final approach causing a missed approach followed by diversion (by the AutoFailMS MS) to alternative landing / recovery site;
NS-7	Transfer of control to remote pilot following a failure for which the AutoFailMS is unable to determine / execute a safe recovery action, followed by successful recovery by the remote pilot;
NS-8	Non recoverable failure during landing (by the AutoFailMS)
NS-9	Non recoverable failure (but where sufficient control remains to allow successful diversion) during take off

Table 3 Normal scenarios

3.2.1.1.2 Failure scenarios

Analysis of the functional description in “section 2 define the change” reveals the *failure* operational scenarios. These scenarios present a more detailed level than what is expected according to D1.3 [1]. A compromise has been found between two approaches.

- The aircraft and aircraft systems need to be compliant with current regulation and JARUS [9]. The ARPS 4754A/ED79A [13] is the proper means to support the regulation requirements. Therefore, it seems reasonable to write the scenarios at the level of current SSAs for manned aircraft already based on ARP4754A/ED79A.

- A stated on the stage 1, the RPAS operations are designed in such a way that in normal situation, the RPAS will be transparent for the ATM. Consequently, it is in the failure modes where the impact on the stakeholders is going to be analysed. Therefore it seems reasonable to write the scenarios related to the Autonomous Failure Management System at the level of an aircraft FHA that can be interfaced with the ATM.

The scenario for the failure modes presents therefore a level between the expected level of similar SSAs in current manned aircraft CS-25 and the expected level of an aircraft FHA. Refer to Rec_07 to discussion about the scenario levels

a) **<u>Failure of AutoFailMS without a second failure in the RPAS</u>**

Second failure is defined as any aircraft failure after the failure of the AutoFailMS

Ident	**Failure of AutoFailMS without a second failure in the RPAS**
FS-01.01-A	Loss of the AutoFailMS without second failure
FS-01.01-B	Undetected loss of the AutoFailMS without second failure
FS-01.02-A	Detected erroneous AutoFailMS without second failure
FS-01.02-B	Undetected erroneous AutoFailMS without second failure
FS-01.03-A	Detected intermittent AutoFailMS without second failure
FS-01.03-B	Non-detected intermittent AutoFailMS without second failure

Table 4 Loss of AutoFailMS without a second failure in the RPAS scenarios

b) **<u>Failure of AutoFailMS with a second failure in the RPAS</u>**

i. <u>Loss of AutoFailMS</u>

Ident	Loss of AutoFailMS with a second failure in the RPAS	Flight phase	Recovery of second failure mode.
FS-02.01-A	Detected loss of the AutoFailMS combined with a second failure on board	in cruise	The remote pilot can control the RPAS
FS-.02.01-B	Detected loss of the AutoFailMS combined with a failure on board in cruise	in cruise	The remote pilot cannot control the RPAS
FS-.02.01-C	Undetected loss of the AutoFailMS combined with a failure on board	in cruise	The remote pilot can control the RPAS
FS-02.01-D	Undetected loss of the AutoFailMS combined with a failure on board	in cruise	The remote pilot cannot control the RPAS
FS-02.02-A	Detected loss of the AutoFailMS combined with a failure	Before final approach	The remote pilot can control the RPAS
FS-02.02-B	Detected loss of the AutoFailMS combined with a failure on board	Before final approach	The remote pilot cannot control the RPAS
FS.02.02-C	Undetected loss of the AutoFailMS combined with a failure on board	Before final approach	The remote pilot can control the RPAS

Ident	Loss of AutoFailMS with a second failure in the RPAS	Flight phase	Recovery of second failure mode.
FS-02.02-D	Undetected loss of the AutoFailMS combined with a failure on board	Before final approach	The remote pilot cannot control the RPAS
FS-02.03-A	Detected loss of the AutoFailMS combined with a failure	During final approach	The remote pilot can control the RPAS
FS-02.03-B	Detected loss of the AutoFailMS combined with a failure on board	During final approach	The remote pilot cannot control the RPAS
FS-02.03-C	Undetected loss of the AutoFailMS combined with a failure on board	During final approach	The remote pilot can control the RPAS
FS-02.03-D	Undetected loss of the AutoFailMS combined with a failure on board	During final approach	The remote pilot cannot control the RPAS
FS-.02.04-A	Detected loss of the AutoFailMS combined with a failure	During landing	The remote pilot can control the RPAS
FS-02.04-B	Detected loss of the AutoFailMS combined with a failure on board	During landing	The remote pilot cannot control the RPAS
FS-02.04-C	Undetected loss of the AutoFailMS combined with a failure on board	During landing	The remote pilot can control the RPAS
FS-02.04-D	Undetected loss of the AutoFailMS combined with a failure on board	During landing	The remote pilot cannot control the RPAS

Table 5 Loss of AutoFailMS with a second failure in the RPAS scenarios

ii. Spurious failure detection

Ident	Spurious failure detection	Flight phase	Recovery of second failure mode.
FS-03.01-A	Detection of a non-existing failure	In cruise	The remote pilot can control the RPAS
FS-03,01-B	Detection of a non-existing failure	In cruise	The remote pilot cannot control the RPAS
FS-03.02-A	Detection of a non-existing failure	Before final approach	The remote pilot can control the RPAS
FS-03.02-B	Detection of a non-existing failure	Before final approach	The remote pilot cannot control the RPAS
FS-03.03-A	Detection of a non-existing failure	During final approach	The remote pilot can control the RPAS
FS-03.03-B	Detection of a non-existing failure	During final approach	The remote pilot cannot control the RPAS
FS-03.04-A	Detection of a non-existing failure	Landing	The remote pilot can control the RPAS
FS-03.04-B	Detection of a non-existing failure	Landing	The remote pilot cannot control the RPAS

Table 6 Spurious AutoFailMS scenarios

iii. Erroneous/erratic AutoFailMS

Ident	Erroneous/Erratic AutoFailMS	Flight phase	Recovery of second failure mode.
FS-04.01-A	Detected erroneous/erratic AutoFailMS combined with a second failure on board	In cruise	The remote pilot can control the RPAS
FS-04.01-B	Detected erroneous/erratic AutoFailMS combined with a failure on board in cruise	In cruise	The remote pilot cannot control the RPAS
FS-04.01-C	Undetected erroneous/erratic AutoFailMS combined with a failure on board	In cruise	The remote pilot can control the RPAS
FS-04.01-D	Undetected erroneous/erratic AutoFailMS combined with a failure on board	In cruise	The remote pilot cannot control the RPAS
FS-04.02-A	Detected erroneous/erratic AutoFailMS combined with a second failure on board	Before final approach	The remote pilot can control the RPAS
FS-04.02-B	Detected erroneous/erratic AutoFailMS combined with a failure on board in cruise	Before final approach	The remote pilot cannot control the RPAS
FS-04.02-C	Undetected erroneous/erratic AutoFailMS combined with a failure on board	Before final approach	The remote pilot can control the RPAS
FS-04.02-D	Undetected erroneous/erratic AutoFailMS combined with a failure on board	Before final approach	The remote pilot cannot control the RPAS
FS-04.03-A	Detected erroneous/erratic AutoFailMS combined with a second failure on board	During final approach	The remote pilot can control the RPAS
FS-04.03-B	Detected erroneous/erratic AutoFailMS combined with a failure on board in cruise	During final approach	The remote pilot cannot control the RPAS
FS-04.03-C	Undetected erroneous/erratic AutoFailMS combined with a failure on board	During final approach	The remote pilot can control the RPAS
FS-04.03-D	Undetected erroneous/erratic AutoFailMS combined with a failure on board	During final approach	The remote pilot cannot control the RPAS
FS-04.04-A	Detected erroneous/erratic AutoFailMS combined with a second failure on board	During landing	The remote pilot can control the RPAS
FS-04.04-B	Detected erroneous/erratic AutoFailMS combined with a failure on board in cruise	During landing	The remote pilot cannot control the RPAS
FS-04.04-C	Undetected erroneous/erratic AutoFailMS combined with a failure on board	During landing	The remote pilot can control the RPAS
FS-04.04-D	Undetected erroneous/erratic AutoFailMS combined with a failure on board	During landing	The remote pilot cannot control the RPAS

Table 7 Erroneous AutoFailMS scenarios

iv. Intermittent AutoFailMS connection/disconnection.

Ident	**Intermittent AutoFailMS connection/disconnection**	**Flight phase**
FS-05.01-A	Detected intermittent AutoFailMS connection/disconnection.	In cruise
FS-0501-B	Undetected intermittent AutoFailMS connection/disconnection.	In cruise
FS-05.02-A	Detected intermittent AutoFailMS connection/disconnection.	Before final approach
FS-05.02-B	Undetected intermittent AutoFailMS connection/disconnection.	Before final approach
FS-05.03-A	Detected intermittent AutoFailMS connection/disconnection.	During final approach
FS-05,03-B	Undetected intermittent AutoFailMS connection/disconnection.	During final approach
FS-05.04-B	Detected intermittent AutoFailMS connection/disconnection.	During landing
FS-05.04-B	Undetected intermittent AutoFailMS connection/disconnection.	During landing

Table 8 Intermittent AutoFailMS scenarios

3.2.1.1.3 Abnormal scenarios

Analysis of the functional description in "section 2 defines the change" reveals the *abnormal* operational scenarios. Note that, for an aircraft point of view, the scenarios considered abnormal from an ATM perspective are actually considered by other systems (e.g. loss of datalink is covered by SSA referred to datalink).

Ident	Scenarios
A1	Failure of the C2 link
A2	R/T Failure
A3	Intruder in airspace around RPAS
A4	TCAS alert (related to intruder scenario A#3)
A5	Unexpected instruction from ATC to deviate from planned flight path
A6	Extreme weather conditions
A7	Busy airspace
A8	Incorrect maintenance of aircraft equipment
A9	Incorrect actions by remote pilot

Table 9 Abnormal scenarios

Refer to Rec_04 for discussion about abnormal scenarios.

3.2.2 Context C0-2: Level of safety

This item of context (**C0-2**) defines that introduction of the RPAS must achieve a level of safety which is no worse than that achieved in equivalent manned operations. (Note: this is carefully worded to include the effect on the safety of the whole system, not limited to just the RPAS itself.)

However, we also need to identify how the AutoFailMS element of the RPAS system contributes to achieving this acceptable level of safety. We need to do this for each domain in which we have to assess the impact of the Autonomous failure Management System on safety. As per 2.5 the main domains affected will be the aircraft domain, the ATM domain the remote pilot and the maintenance. The approach is for each domain is outlined below.

For this case study, we interpret the requirements on the AutoFailMS on the aircraft&AutoFailMS domain as follows:

In the aircraft domain, the certification specifications set probability objectives dependent on the severity of the failure. In this regard the objectives set by the JARUS [9] are the same as those set by CS-25. These objectives are therefore reasonable to adopt for this case study.

- the AutoFailMS(when working correctly) must maintain the same level of performance (detection, isolation, reaction) as the pilot which it is replacing; this is an essential requirement to ensure that the RPAS operation are transparent for the ATM. Implicitly it means that the RPAS assisted by Autonomous Failure Management Systems needs to ensure the adherence to flight plan, separation assurance and collision avoidance and landing to emergency site qualitatively and quantitatively as a manned aircraft. The Er-010[16] has performed an analysis of the impact of RPAS operation in ATM.

- The AutoFailMS (under failure conditions) must meet the safety level equivalent to manned aircraft. This is understood the global safety objective for an RPAS equipped with AutoFailMS shall meet the JARUS objectives (as appropriate to the severity of the failure). The allocation of safety objective as from RPAS to each aircraft system should follow the ARP4754A/ED79A [13] rules. Refer to JARUS [9])

For the RPAS equipped with an AutoFailMS, there are two types of objective, performance (driven mainly by ATM needs) and safety (driven by safety effects of failure) both objectives can be justified as per ARP 4754A/ED79A.

For this case study, we interpret the requirements of the AutoFailMS on the ATM as follows:

In the ATM domain, the certification specifications are based on essential requirements (in 216/2008) and “common” requirements (in 1035/2011). The RPAS operations need to be compliant with those. For the purpose of this case study, as stated in § 2.3, the ATM certification specification will be proposed by using the D1.3 methodology. Note that for an ATM certified to provide navigation services to a mixed fleet (RPAS and manned aircraft), the ATM should meet requirements related to the RPAS operation in mixed environment, but not requirements related to the Autonomous Failure Management System itself.

- The ATM (when RPAS assisted by AutoFailMS operation as normal) must maintain the same level of performance (navigation service provision) for a mixture of RPAS and manned aircraft as is achieved today in fully manned operations. For example, the RPAS normal operation might imply as well a diversion to a landing side, in such case the ATM needs to ensure safety (in terms of safe separation) at the same level than today.

- The ATM (when RPAS in failure due to an AutoFailMS failure) must maintain the same level of performance (navigation service provider) for a mixture of RPAS and manned aircraft as is achieved today. For example, after a failure implying loss of C2 and loss of AutoFailMS, the ATM needs to ensure safety (in terms of safe separation) at the same level as today. This might imply the creation of ATC procedures for RPAS in uncontrolled situation.

For this case study, we interpret the requirements of the AutoFailMS on the pilot as follows:

The remote pilot is defined as a backup for the AutoFailMS, at any moment the pilot can reverse to manned mode and take over RPAS operations.

- The pilot (when AutoFailMS operation as normal) validates trajectory changes (as pilot is defined to be the owner of trajectory) and survey aircraft status. Remote pilot needs to perform these functions with an equivalence of performance of a pilot physically on board of the RPAS.

- The pilot, in case of faulty AutoFailMS, needs to replace the AutoFailMS and ensures the safety of the RPAS operations at a level similar to a manned aircraft (CS-25).

For this case study, we interpret the requirements of the AutoFailMS on maintenance as follows:

The maintenance is by definition preventive and corrective activities whose objective is to keep aircraft system at the level of performance expected. Hereafter only preventive aspect is considered.

- The maintenance team (when AutoFailMS operation as normal) needs to periodic checks and maintain activities according to current regulation. See §4.3.1.4

- The maintenance team (when RPAS operation assisted by a faulty AutoFailMS) needs to periodic checks and maintain e activities according to §4.3.1.4

These previous paragraphs have presented the safety level on each impacted domain the overall safety level on RPAS operation assisted by AutoFailMS is a common objective to be achieved by all aviation stakeholders. It is essential to present the safety impact of failures on each domain, this can achieved by a severity matrix. For this Use Case a severity matrix has been created taken as inputs JARUS [9](related to aircraft) ER-010 [16]. See paragraph 5.1

3.2.3 Context C0-3: RPAS as adaptation of existing aircraft

C0-3 identifies that the RPAS is conceived as an adaptation of an existing civil piloted fixed wing cargo aircraft: this provides a significant amount of background information regarding the performance and behavior of the aircraft; it also helps in the decision over the certification basis to use for the assessment. Refer to stage 1 for further details of functions installed on the RPAS.

3.2.4 Context C0-4: Autonomous Failure Management System part of larger change

This case study covers the development of a failure management system (Autonomous Failure Management System) for a Remotely Piloted Aircraft System (RPAS). The RPAS is conceived as an adaptation of a (generic) existing civil fixed wing cargo aircraft with flight crew on board (see C0-3). The scope of the RPAS will include the aircraft, the ground station used to pilot the aircraft and the communications link between aircraft and ground station.

However, introduction of Autonomous Failure Management System is only part of the change needed to convert an existing aircraft to an RPAS. Thus it is assumed that the change considered in this case study is part of a package of changes (to be implemented simultaneously) in order to convert the existing aircraft. (The alternative would be to introduce this extension of the Autonomous Failure Management System after the RPAS entered service – however it is inconceivable in this case, as an RPAS without an adapted Autonomous Failure Management System would not achieve certification to operate. (Refer to Appendix A for detailed delta between RPAS and manned on board aircraft)

For the purpose of this case study we assume that the adaptations will include provision of a Detect and Avoid function.

This context makes it easier to see how the Autonomous Failure Management System contributes to the overall “no less safe than piloted aircraft” argument. In the full application of the D1.3 approach this context significantly affects claim 4 (transition), as it means that the Autonomous Failure Management System is part of the transition into RPAS operations, rather than being a separate transition after RPAS operations commence.

Note The case study has shown that it is very difficult to make a certification argument for only part of a change because (a) of the major assumptions which need to be made about the other parts of the change; (b) the fact that some of the analysis required has to be done at the level of the RPAS system, because (in the end) it is this system which is being shown to be safe. In addition (although not addressed in this case study) claim 4 (migration) would have to be made at the level of the introduction of the RPAS.

3.2.5 Context C0-5: Operational environment

C0-5 defines the operational environment to which the safety argument applies .*Note: this context does not mean that the AutoFailMS will not work outside this environment; it just means that the argument presented here does not cover operations outside these parameters.*

We limit the scope of the argument to consider only class A, B and C airspace. However, it is noted that the inclusion of class C airspace introduces VFR traffic and therefore depends on the RPAS including a Sense and Avoid function (see C0-4).

We do not require visual contact between pilot and aircraft.

We assume that all communications between pilot and other actors is via the aircraft. (I.e. to the other actors, the aircraft appears to be piloted.)

3.3 Claim 1: Introduction of *Autonomous Failure Management System* specified to contribute to safe operations

Methodology proposed in D1.3 [1] the Claim 1(see Figure 4) is that the change to introduce the *Autonomous Failure Management System* is specified such that it contributes adequately to an acceptable level of safety for the RPAS. The acceptable level of the safety for RPAS operation is agreed to be decided by EASA. For the purpose of this safety study it is agreed that safety of RPAS operation is kept as "per today"

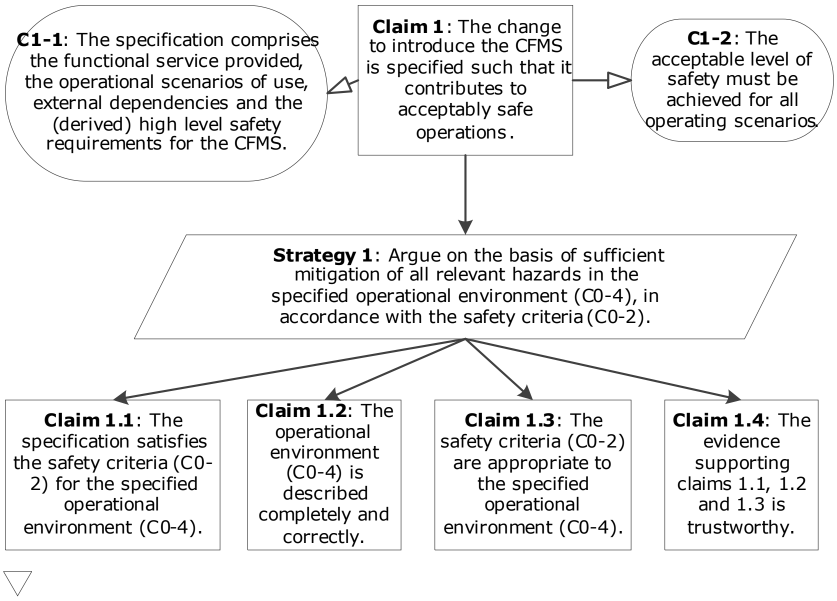


Figure 4 Argument that AutoFailMS is specified to be acceptably safe (Claim 1)

Claim 1 is supported by the following items of context[5]:

Context C1-1: explains that the specification of the AutoFailMS satisfies the safety level (C02) for the operational environment (at the functional level – see section 3.2.4) It comprises the following items.

- a "black box" definition of the function provided by the AutoFailMS;
- a description of the operational scenarios in which it is used, covering normal, abnormal and (self)failure scenarios;

[5]These items of context are in addition to the context already defined for Claim 0: in the GSN notation, context from higher level claims is automatically "inherited" by the lower level claims.

- the high level safety requirements for the AutoFailMS;
- The interactions, at the functional level, between the AutoFailMS and the rest of the TAS.

At this level of claim 1, the methodology D1.3 does not consider how the AutoFailMS is actually implemented[6]; thus there is no consideration of equipment or specific human roles, just what the AutoFailMS will achieve and how it will interact with the rest of the TAS.

Note: the specification referred to here is developed as part of the work to support claim 1, it is not required (or possible) for it to be complete before the stage 4 assessment starts.

- Context **C1-2**: clarifies that the acceptable level of safety (defined in Context 0-2) must be achieved for all the operating scenarios, including normal, abnormal and (self) failure scenarios.

This claim (Claim 1) is then decomposed into subclaims (Claims 1.1 – 1.4); together these claims combine to satisfy claim 1, in the same way that claims 1-4 combine to satisfy claim 0. The main claim is Claim 1.1 (that the specification satisfies the safety criteria for the specified operational environment): this is elaborated further below. The other claims may seem obvious, but they are listed to emphasize that we also need to demonstrate that:

- Claim 1.2: the description of the operational environment (C0-4) is complete and correct;
- Claim 1.3: the safety criteria (C0-2) are at the correct level and match the operational environment. (This might be supported by engineering judgment, refer to WP 3.5 task of TESG)I
- Claim 1.4: sufficient backing evidence is in place to show that the direct evidence supporting the claims can be relied upon – i.e. used suitable processes which were correctly applied by competent personnel. (refer to backing evidence 3.6)

3.4 Claim 1.1: The specification of the AutoFailMS) satisfies the safety criteria (C0-2)

Claim 1.1 is that the specification (of the AutoFailMS) satisfies the safety criteria (C0-2) when operating in the specified operational environment (C0-4).The main assessment to support this claim will be a form of functional hazard assessment, using techniques which are well-established in assessing concepts (rather than equipment)..

Strategy 1.1 explains that the strategy for demonstrating Claim 1.1 is to show that all hazards have been identified and that the specification provides sufficient mitigation for those hazards, both for the designed operation of the AutoFailMS (in the absence of (self) failure) and in the event of (self)failure of the AutoFailMS.

[6] It is obviously important that the concept is capable of being implemented: thus achievability is addressed in claim 2.

Each of the sub-claims 1.1.1 to 1.1.3 is described further in the sections below.

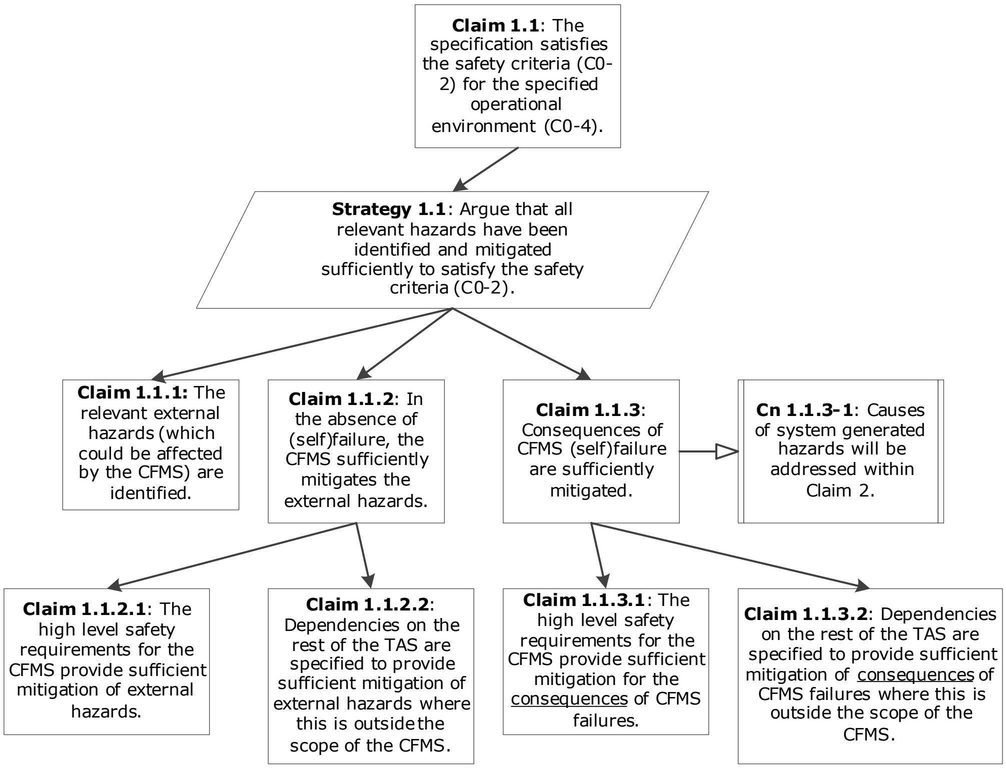


Figure 5 Argument that AutoFailMS specification satisfies the safety criteria (Claim 1.1)

Note that the methodology by D1.3 establishes a clear distinction between the safety level achieved in normal conditions (claim 1.1.2) and the safety level achieved in failure conditions (claim 1.1.3).

3.4.1 Claim 1.1.1: Generic hazards are identified

The methodology proposed by D1.3 presents a distinction between the hazards that the system intend to mitigate (named pre-existing hazards), and the hazard that the system generates (self failure hazards). From an ATM point of view, the hazards are inherent to the aviation, and most of the systems introduced on the aviation industry aim at mitigating these hazards. Although it is possible that the introduction of something new into the environment will introduce a new hazard, it is far more likely that, at the system level, it will affect existing hazards. This reasoning makes sense on the ATM perspective, as most of navigation services are focused on providing safe operations. However from an aircraft perspective, the systems installed on an aircraft aim at providing the capacity of flying. It these systems works as intended the safety is ensured, in case they do not work as intended the safety might be impaired. This different approach to safety presents two main impacts:

From an aircraft perspective the failure of the system impact on the safety, from the point of view of ATM domain, the hazard is anything that could induce an accident. See below the definition to hazard according to ARP4757 attached to the concept of malfunction, errors, etc.

- .EC1035/2011: hazard' means any condition, event, or circumstance which could induce an accident
- ED78A: A situation which has potential to lead harm
- ARP4754-ED79: potentially unsafe condition resulting from failures, malfunctions, external events, errors, or combinations thereof where safety is affected.

In order to avoid any kind of misinterpretation, at the level of the total aviation system, we refer to "generic hazard" as "any potential unsafe situation at TAS level that the system under study (RPAS operation) shall contribute at the level which is acceptable safe as per C0-2". Example of "generic hazards" (refer to Rec_05)

- Loss of control in flight
- Loss of separation
- Increase in ATM workload

In the case of the AutoFailMS, note that the AutoFailMS is expected to manage the failures as a pilot on board. The "external hazards" would be all these failure that the AutoFailMs is intended to manage (e.g. aircraft systems failures). This "external hazard" is actually a self-failure hazard to other system (e.g. loss of bus bar). In the case of the aircraft, the regulation is applied over the aircraft (CS-25) and cascaded to the systems (ARP4754A/ED79A). The hazards, weather external or self-failure are regulated under the same principles, in this Use Case, the term "generic hazard" will be used.

3.4.2 Claim 1.1.2: AutoFailMS provides sufficient mitigation of RPAS operation failures

This claim is about showing that the AutoFailMS, when operating without (self) failure, provides sufficient protection against failures of the other RPAS aircraft systems. Essentially, this answers the question of whether the AutoFailMS is providing the required level of performance at doing the job it is intended for, when it is operating correctly. The AutoFailMS (when working correctly) must maintain the same level of performance (detection, isolation, reaction) as the pilot which it is replacing.

The output of this part of the assessment is still at a high level, considering the AutoFailMS as a "black box" and yielding high level safety requirements for the AutoFailMS function. From an aircraft perspective, these requirements are considered functional requirements.

The high level safety requirements are derived through the identification and assessment of normal and abnormal scenarios. The scenario defines how the AutoFailMS contributes to the safety of RPAS operation in no AutoFailMS failure conditions. The AutoFailMS replaces to the pilot in managing the failure. AutoFailMs contribution to safety in no failure conditions consists in working as intended, the safety requirements are design requirements. The high level safety requirements developed to support this claim form part of the specification of the AutoFailMS, as defined in Context **C1-1**.

Claim 1.1.2 is subdivided into two subclaims to emphasize that, as well as deriving requirements on the AutoFailMS itself (Claim 1.1.2.1), it is necessary to define any interactions (at the "black box" level) with other parts of the system (Claim 1.1.2.2), including: ATM, other aircraft, remote pilot, etc.

Claim 1.1.2.1: The high level of safety requirements for the AutoFailMS provides sufficient mitigation of generic hazards

The claim 1.1.2.1 the high level of safety requirements for the AutoFailMS when working in normal conditions provides sufficient mitigation of generic hazards. The AutoFailMS, when working normally, manages the failure conditions to avoid hazards. This claim is supported by the design.

Claim 1.1.2.2: Dependencies on the rest of the TAS are specified to provide sufficient mitigation of the generic (external) hazard where this is outside the scope of the AutoFailMS

The claim 1.1.2.2 expresses that the interface between stakeholders and AutoFailMS has been designed in such way that the generic hazards (when not related to the AutoFailMS) are mitigated. As stated in 2.5 the interfaces to be considered are, RPAS, ATM, pilot and maintenance.

- Aircraft: Note that the failures originated the aircraft needs to be managed by definition by the AutoFailMS, in this sense, the dependency aircraft-AutoFailMS is in the scope of claim 1.1.2.1 and not claim 1.1.2.2. The allocation of safety objective among aircraft systems (e.g safety objective for electrical system and for AutoFailMs) and the safety requirements (e.g AutofailMs impose a safety requirement of electrical systems) are supported by ARP 4754A/ED79A.

- ATM: In first place, the introduction of an RPAS in the non-segregated airspace is expected to be transparent for the ATC as the AutoFailMS has not been designed to mitigate ATM hazards. However, the AutoFailMS replaces the pilot is all continuous monitoring and surveillance, in this sense, the AutoFailMS needs to identify potential ATM mistakes in the same way that a pilot on board. This is in the scope of AutoFailMS. The dependency aircraft-AutoFailMS is in the scope of claim 1.1.2.1 and not claim 1.1.2.2.

  In second place, the introduction of RPAS in the non-segregated airspace might modify the level of performance (e.g continuity, availability, message corruption rate) that the aircraft requires from of ATM, this might imply an update of the performance requirements in current regulation (ED-85A, ED-89A, ED-160, ED-120-A and ED-122-A).

- Remote pilot (crew): As per stage 1, the pilot is a backup in case of failure of the AutoFailMS (autonomous mode), in this sense, the AutoFailMS is in charge of management of failures. When the AutoFailMs is working in nominal conditions, remote pilot is in back up. Claim 1.1.2.2 N/A to remote pilot dependency.

- Maintenance organization. Any aircraft system installed on an aircraft performs test automatically these test are asked by the Build in Test Equipment system, these tests are performed periodically or after a certain even that triggers them. Potential mistakes of maintenance team over the AutoFailMS would be identified by BITE system. It is not in the scope of AutoFAilMs to identify the mistakes/errors of maintenance team. N/A to maintenance dependency.

As a conclusion, it is shown that claim 1.1.2.2 is not applicable to AutoFailMS dependencies or it is referred to claim 1.1.2.1. This is because the AutoFailMS scope is to mitigate the failure conditions. In this regard the safety level of AutoFailMS is to keep current safety performance, and therefore no mitigation of external hazards is expected.

The requirements related to claim 1.1.2 (see normal and abnormal scenarios) is defined as functional requirement. If AutoFailMS works as intended the current safety level is kept. Claim 1.1.2 can be phrased as AutoFailMS works as intended.

3.4.3 Claim 1.1.3: Sufficient mitigation of AutoFailMS (self) failure

This claim shows that the consequences of failures of the AutoFailMS itself are sufficiently mitigated. As with Claim 1.1.2, the output of this part of the assessment is still at a high level, yielding high level safety requirements for the AutoFailMS function.

The high level safety requirements are derived through the identification and assessment of (self) failure scenarios.

The high level safety requirements developed to support this claim form part of the specification of the AutoFailMS, as defined in Context C1-1.

Claim 1.1.3 is subdivided into two subclaims to emphasize that, as well as deriving requirements on the AutoFailMS itself (Claim 1.1.3.1), it is necessary to define any interactions (at the "black box" level) with other parts of the system (Claim 1.1.3.2), including: ATM, other aircraft, remote pilot.

Claim 1.1.3.1: The high level of safety requirements for the AutoFailMS provide sufficient mitigation for the consequences of the AutoFailMS failures

Claim 1.1.3.1 can be considered supported by the SSAs at system level. The mitigation against self-failures in the scope of the AutoFailMS deals with the system design (e.g. equipment redundancies, etc) and is based on the application of ARP4754A/ED79A. The safety objectives (in terms of probability and performance) are not independent aircraft architecture and system design. The SSA of a system and the FHA at aircraft level are interrelated.

Claim 1.1.3.1 for RPAs and for AutoFailMS system can be expressed as follows: The high level f safety requirement for RPAS operation supported by AutoFailMS is compliant with JARUS [9]

Claim 1.1.3.2: Dependencies on the rest of the TAS are specified to provide sufficient mitigation of the generic consequences of the AutoFailMS failures where this is outside the scope of the AutoFailMS

This claim expresses that the interface between stakeholders and AutoFailMS have been designed in such way that the hazards generated by AutoFailMS (AutoFailMS in failure conditions) are mitigated. As stated in 2.5 the interfaces to be considered are, RPAS, ATM, pilot and maintenance.

- Aircraft: Note that the impact of the AutoFailMS failure in other aircraft systems is actually part of the scope of the aircraft FHA. The aircraft FHA summarizes the results of the aircraft systems SSAs. The SSAs for the Autopilot and the FHA for the RPAS cannot be split, but considered as a one single claim. Refer to Claim 1.1.3.1

- Remote pilot (crew). As per stage 1, the pilot is a backup in case of failure of the AutoFailMS (autonomous mode), in this sense, the pilot is the back up of the AutoFailMS. The AutoFailMS and the pilot are not independent entities, the pilot procedures and the types of AutoFailMS need to be designed in such a way that the remote pilot could take over the RPAS as if he/she was onboard. (E.g. assessment on workload).The claim 1.1.2 will be defined as follows: The dependencies the RPAs operations assisted by an AutoFailMS and the remote pilot shall be assessed in such way that enable RPAS operations to be compliant with JARUS [9]. This implies the update of AFM and FCOM. Refer to 4.3.1.2

- ATM: The dependencies with the ATM must be specified in such way that the hazards created by the introduction of an RPAS equipped with AutoFailMS were mitigated. In the failure scenarios, the interactions between the RPAS equipped with AutoFailMS have been addressed from the point of view of the impact on the ATC (impact on flight adherence, separation and collision avoidance and landing on emergency sites) and the point of view of the impact of the ATC failure on the RPAS operations (loss and/or erroneous datalink) The scenarios have been enriched as well with several failure combination modes. To elaborate these scenarios, the document ER-010 [16] has been used as an input. Claim 1.1.3.2 for the ATM is expressed as follows : The dependencies the RPAs operations assisted by an AutoFailMS and the ATM shall be assessed in such way that enable RPAS operations to keep the same level of safety performance (in tem of adherence to flight plan, separation and collision avoidance and landing in emergency site) are current operation. Note that the claim 1.1.3.2 implies an update of the level of performance of datalink services ATM as well.

- Maintenance organization. The activities related to maintenance are kept as today. The maintenance organization will comply with the maintenance activities and required by Part M. Refer to 4.3.1.4

As a conclusion, it is shown that the safety level in case of failure for AutoFailMS and RPAS operation is stated by current regulation, of the ATM the claim 1.1.3 has been elucidated using D1.3 methodology (as presented in 2.1)

3.5 Claim 2: Realistic logical design satisfies specification

As per defined in D1.3 Claim 2 is that the logical design of the AutoFailMS satisfies the specification (which was defined in support of Claim 1) and is realistically achievable. The logical design includes the architecture of the AutoFailMS (including its impact on the communications link and the remote pilot); it will also consider the other affected elements of the TAS (including primarily ATC and other aircraft). The logical design can largely be developed from the description given in stage 1.

For this Use Case, note that current regulation answers to claim 1. The current regulation ARP4754A/ED79A defines main lines of the logical design refer to Figure 6. When regulation missing (e.g. interface with ATM) it is possible to enlarge the ARP4754A/ED79A scope (Figure 8 and Figure 9) or to develop new regulation (Rec_10).

Note that ARP 4754A/ED79A not only addresses logical design but as well it imposes certain requirements on the equipment (e.g. IDAL) and it develops the safety objectives presented in CS-25. ARP 4754A/ED79A covers not only Claim2 but as well claim 1. This aspect will be further developed in chapter 4

3.5.1 Claim 2.1: the logical design satisfies the specification for the specified operational environment.

Application of ARP4754A/ED79A to the RPAS and to the AutoFailMS

The ARP 4754A/ED79A establishes safety objectives of the RPAS operations for both functional and safety objectives. The ARP 4754A/ED 79A might be modified to support RPAS (See JARUS [9]). As stated in both ARP 4754A/ED79A and JARUS [9] the RPAS and its systems (e.g AutoFAilMS) needs to be compliant with certain safety objectives. These safety objectives are based on the high level requirement that "RPAS must not present a greater risk to persons or property on the ground or in the air than that attributable to manned aircraft of equivalent category". The ARP 4754A/ED79A and JARUS [9] establishes safety objectives that are traceable from claim 1. (refer to appendix E.2)

These safety objectives are cascaded to systems according with rules specified in the ARP 4754A/ ED79A. The application of ARP4754A/ED79A covers both RPAS and AutoFailMS systems for both normal and failure conditions.

Claim 1.1.3.1&claim 1.1.3.2 RPAS and claim 1.1.2.1&claim 1.1.2.2 RPAS are covered by ARP4754A/ED79A.

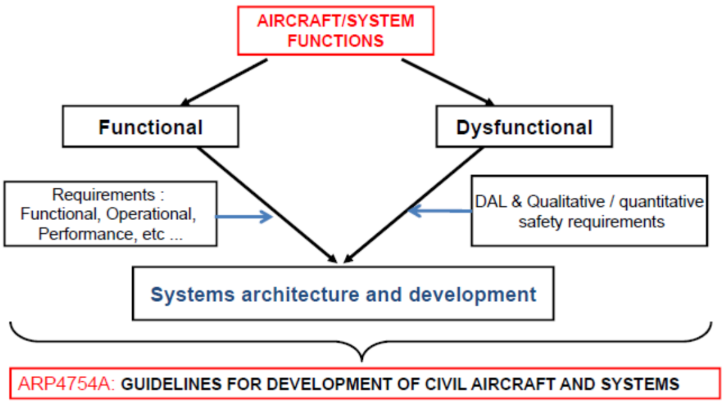


Figure 6 ARP4754A/ED79A Guidelines for development of civil aircraft and systems functional and dysfunctional requirements

The ARP 4754A/ED 79A imposes as well qualitative (e.g DAL) an quantitative objectives in the architecture of the AutoFail MS system. In this sense the application of ARP 4754A/ED 79A is addresses claim 2.1. For this reason standards are used to support claim 1.2

The ARP 4754A/ED 79A establishes as well safety requirements for the interface between the systems in the aircraft (e.g objective of common modes for AutoFailMS and FGCS). To sum up the application of standards is not independent from the design of the aircraft systems, this is driven mainly by DAL..

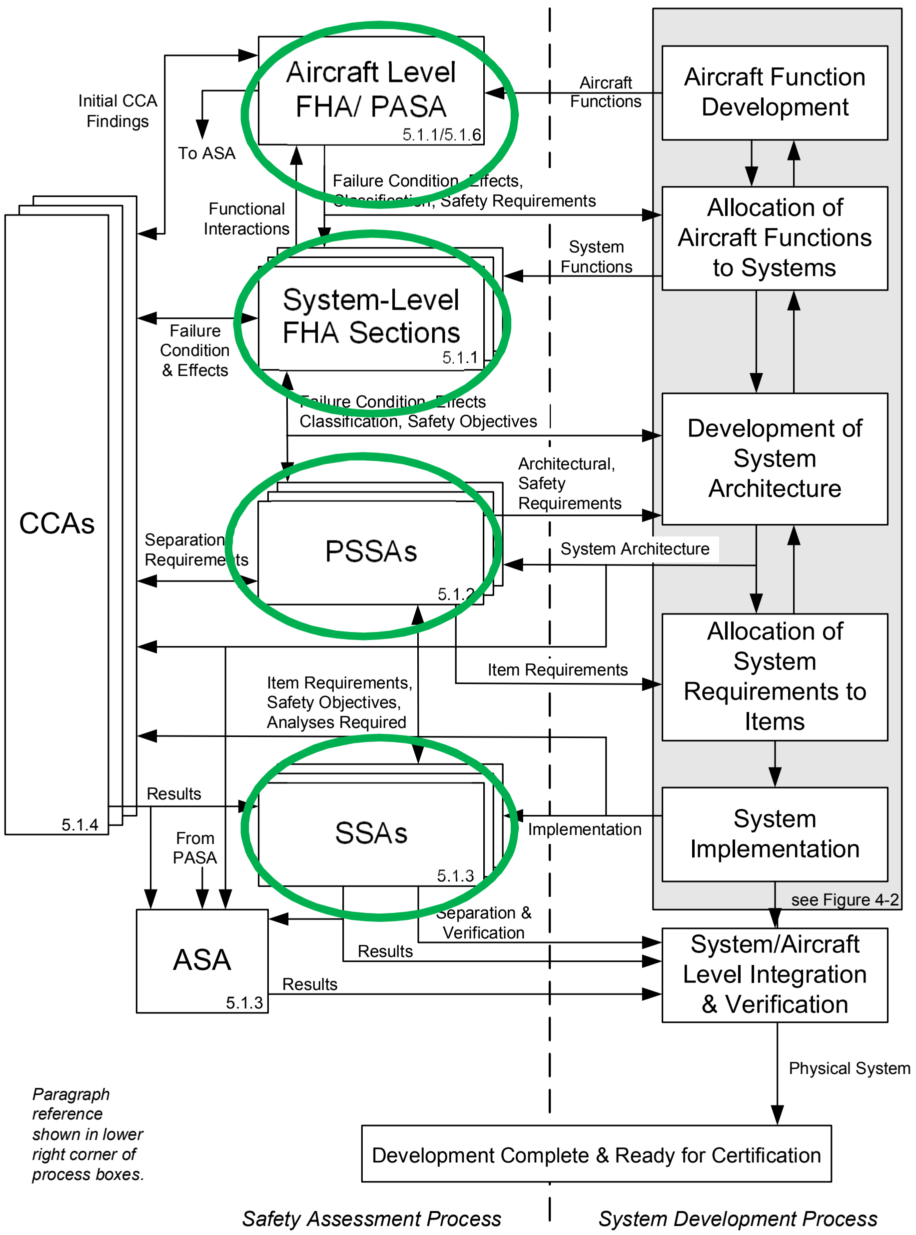


Figure 7 ARP4754A/ED79A Safety requirements at aircraft and system level.

. The DAL is the development assurance level that a certain function need to comply with. This development assurance level ensures that the design is resilient again development errors. The DAL level depends on the severity of the function failure: The DAL assignment depends also on the independencies implemented in architectures development process (from requirement development to hardware and software development). The top level DAL is allocated using the following table from ARP4754A/ED79A

Error severity Classification	DAL of the Develop. process
Catastrophic	A
Hazardous / Severe Major	B
Major	C
Minor	D
No safety effect	E

Table 10 Error severity classification and top DAL

There are two types of DAL: One for function development (FDAL) and one for item development (IDAL). Te IDAL follows the FDAL level.

- FDAL (Function Design Assurance Level) is level of rigor of tasks performed to functions in a development process. It applies to function development (requirement elaboration phase): A/C Functions, Systems functions, Sub-Systems functions, equipment functions.
- IDAL (Item Design Assurance Level) is the level of rigor of tasks performed to items in the development process. IDAL applies to hardware and software items development. These items are addressed ion stage 7 in D1.3 methodology) IDAL is an input for the application of DO-178B/ED-12B (software) and DO-254/ED-80 (Hardware).

Consequently the application of ARP4574A/ED79A covers as well the stage 7 not addressed on this Use Case.

Application of current regulation to the interface with remote pilot

As stated in 2.5.2 the remote pilot and the AutoFailMS are designed together. The design of the remote pilot might ensure that the remote can answer as expected to the failure in the AutoFailMS. The pilot requirements (e.g. limits of workload) are considered in RPAS design. System Safety Assessment developed under ARP4754A/ED79A also consider the inputs to the AFM and FCOM. It is noted that there is no standards for procedures development, it would be reasonable to have a standards process. Refer to Rec_10. Refer to 4.3.1.2

Application of current regulation to the maintenance activities

The maintenance activities are defined as per current regulation from the safety and performance requirements. The objective of maintenance activities is to prevent and to mitigate the failure conditions. The application of ARP457A/ED79A provides inputs to the maintenance activities. Refer to 4.3.1.4

3.5.2 Claim 2.2: the logical designs of RPAS operations assisted by AutoFailMS are compliant with ATM requirements

Until this point, the claims have been answered by current regulation. However, as stated in 3.1 the requirements related to the ATM will be developed by D1.3. Claim 2 needs to answer to Claim 1

Claim 1.1.2.2_ATM: In first place, it has been stated that the RPAS operation must be designed in a way that was transparent for the ATC, therefore the design can be covered by ARP 4754A/ED79A. However there is no actually any clear interface between the aircraft and the ATM. Currently, for example in the case of datalink, there is a methodology called ED-78A that enables to share safety objectives and safety requirement between the ATM and the aircraft. Refer to 7.2

In the frame of this Use Case, we can suggest that the performance requirements of the RPAs operation supported y AutoFailMS were enriched by three main requirements from ATM [16]:

- RPAS shall follows the flight path with the same performance than a manned aircraft
- RPAS shall assures a safe separation and the avoidance of collision with the same performance than a manned aircraft
- The RPAS shall lands in a predefined place or in an emergency place with the same performance than a manned aircraft

Note that the ATM can impose, if necessary, more sever safety objective that those in ARP4754A/ED79A, for example, it is possible that in TMA, the missed approach (assessed as Min or at worst MAJ in current FHAs) would be imposed by ATM to be considered as HAZ (for ATM) and it is possible as well that ATM impose quantitative objective (loss of data link under E-07 rather than E-03 as nowadays) due to ATM reasons. They will depend on the type of airspace

ATM requirements

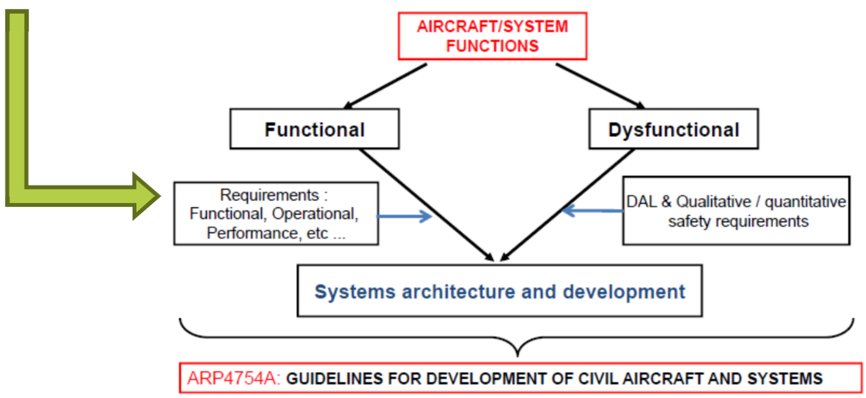


Figure 8ATM requirements and ARP 4754A/ED79A. Functional requirements

The D1.3 enriches the scope of the ARP4754A/ED79A. In this way a larger application of the ARP4754A/ED79A answers to the claim 1.1.2 for the ATM.

In second place, it has been mentioned that the introduction of RPAS into non-segregated environment might imply an increase in the performance level of the datalink services that the aircraft expects from the ATM. Currently loss or erroneous datalink with ATM is assessed MAJ for aircraft, if the performance requirements imposed to the ATM was more strict (see claim 1.1.2.1 and 1.1.2.2) it would be necessary to update the design requirements for ATM. Refer to the Rec_09

Claim 1.1.3 2 for the ATM needs as well an interface with the RPAS. The ATM can ask for certain level safety objective (quantitative and qualitative) to the RPAS operations. This level of safety was later cascaded to the systems (e.g. to the AutoFailMS) and to the items (e.g. to the datalink antennas) to ensure that the aircraft provides with the proper level of safety.

Refer to 4.3.1.3 for coordination among ATM and aircraft standards Refer to the Rec_09 to discussion about safety requirements.

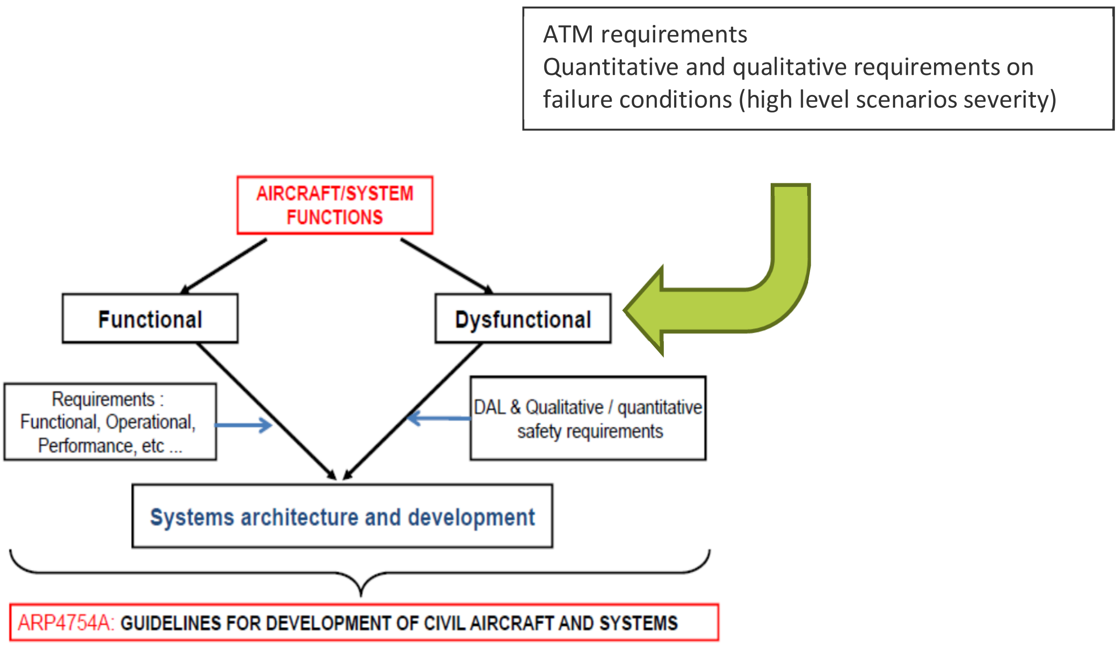


Figure 9 ATM requirements and ARP 4754A/ED79A. Dysfunctional requirements

As a conclusion, the current standards framework allows to answer to claims. These standards needs however a revision.

3.5.3 Claim 2.3: the logical design of the interface pilot in back up and AutoFailMS .is designed is such way that the RPAs operations keeps the same level of safety performance

As stated in 3.4.3 there is no recognized safety standards for the creation of the procedures for the pilot (only manufacturer internal private documentation). The AFM and FCOM consider the inputs of System Safety Assessments and pilot procedures are part of aircraft safety assessment as per ARP4754A/ED79A methodology. But it cannot be considered that the application of ARP4754A/ED79A is enough to support the safety analysis of AutoFailMS safety impact on pilot. It is necessary to address the quality level necessary to mitigate procedure development errors or errors in application by the crew.

The scenarios presented in this Use Case addresses as well some requirements for the pilot in case of failure of AutoFailMS. Refer to Table 17. These requirements will be part of human performance team that will include the requirements in the AFM and FCOM. Refer to 4.3.1.2

3.6 Backing evidence

Direct evidence is the evidence that a particular claim is satisfied – this is evidence relating directly to observable properties of an output or product.

The argument must also be supported by backing evidence, which is the evidence there is sufficient confidence in the direct evidence, i.e. that the processes followed were suitable and that they were undertaken by suitably competent people.

In this Use Case the evidence is ensured by using approved standards.

3.7 Certification Argument

Claim 0- The failure management system (AutoFailMS) contributes to acceptably safe RPAS operations

C0-1 the function AutoFailMS is defined at a level which identifies scenarios of operation and interfaces with the rest of the TAS.

C0-2 Acceptable level of safety for introduction of RPAS is defined as no worse the current equivalent on board piloted (this is then interpreted for the impact of AutoFailMS in each domain). For this Use Case For this Use Case a severity matrix has been created taken as inputs JARUS [9](related to aircraft) ER-010 [16]. See paragraph 5.1

C0-3 The RPAS is conceives as an adaptation of a generic civil on board piloted fixed wing cargo aircraft currently in service

C0-4 the AutoFailMS is introduced as a part of a package of changes to adapts the existing aircraft to become an RPAS

C0-5 the argument assumes that the following operational environment is class A, B and C airspace only, no visual between pilot and aircraft, and all voice comm. via aircraft

Claim 1-the change to introduce the AutoFailMS is specified such that it contributes to acceptably safe opera rations.

Claim 1.1 the specification satisfies the safety criteria (C0-2) for the specified operational environment (C-04)

Claim 1.1.1: Relevant generic hazards are identified. Refer to Rec_06

Claim 1.1.2: In the absence of self-failure the AutoFailMS sufficiently mitigates the external hazards

Claim 1.1.2.1 the high level safety requirements for the AutoFailMS provide sufficient mitigation of external hazards. Supported by design (refer to ARP 4754A/ED79A)

Claim 1.1.2.2 Dependencies on the rest of the TAS are specified to provide sufficient mitigation of external hazards where this is outside the scope of the AutoFailMS

- Aircraft dependency: referred to claim 1.1.2.1
- ATM dependency: dependency: referred to claim 1.1.2.1
- Remote pilot dependency: N/A
- Maintenance dependency: N/A

Claim 1.1.3 Consequences of AutoFailMS self-failure are sufficiently mitigated

Claim 1.1.3.1 the high level safety requirements for the AutoFailMS provide sufficient mitigation for the consequences of the AutoFailMS failures Supported by design (refer to ARP 4754A/ED79A)

Claim 1.13.2 Dependencies on the rest of the TAS are specified to provide sufficient mitigation of consequences of AutoFailMS failure where this is outside the scope of the AutoFailMS

- Aircraft dependency: referred to claim 1.1.3.1
- ATM dependency: dependency: referred to claim 1.1.3.1
- Remote pilot dependency: referred to human interface (Rec_10)
- Maintenance dependency: referred to claim 1.1.3.1

Claim 1.2 the description of the operational environment (C0-4) is complete and correct;(Rec_04)

Claim 1.3: the safety criteria (C0-2) are at the correct level and match the operational environment ;(This might be supported by engineering judgment, refer to WP 3.5 task of TESG refer to Rec_01 and Rec_02)

Claim 1.4- The evidence supporting claim 1.1, 1.2 and 1.3 is trustworthy. Supported by standards

Claim 2 the logical design of the AutoFailMS satisfies the specification is realistically achievable

Claim 2.1 the logical design satisfies the specification for the specified operational environment

Claim .2.2 the logical designs of RPAS operations assisted by AutoFailMS are compliant with ATM requirements

Claim 2.3: the logical design of the interface pilot in back up and AutoFailMS .is designed is such way that the RPAS operations keep the same level of safety performance.

4 Stage 3: Develop and agree a certification plan

4.1 Introduction

This section describes how the approach proposed by ASCOS D1.3 to organize the demonstration of safety can be used to develop and agree the certification plan for an RPAS AutoFailMS function, taking into account the regulatory requirements currently applicable.

The certification plan is the reference for communication between the stakeholder which is seeking for certification of its product and the certification authority, which need to be entirely satisfied of the application by the stakeholder of applicable regulatory requirements before granting the certificate. The Certification Plan needs to contain at least the following elements:

- An overall description of the system, its limits and the way it is interfaced with other systems. This description is primarily intended for experts of the authority. It may highlight relevant aspects as technical novelties, and for changes involving multiple stakeholders, relationship with other products for which a certification is sought by a partnering stakeholder. When more domains are affected the description must mention the relationships between the domains and the relevant assumptions
- Agreement with the authority on a full and consistent set of applicable regulatory requirements and related guidance material. This may require establishing a common agreement between the different authorities involved
- A framework to the authority on how to seek agreement on any further technical issues related to the interpretation of the regulatory requirements that may arise during the design and development of the product
- A comprehensive description of how the evidences will be produced that all the regulatory requirements are complied with
- Agreement with the authority on the organisation of Certification Deliverables. The Certification Deliverables are documents that need either to be approved or agreed or received by the authority prior to granting the certificate. They are to be considered as the core part of the Safety Case
- An overall description of how the "Continuing Safety activities" will be organized in compliance with the reference standards as the response to the mandatory requirements on safety, introducing actors, activities and key documents as output of these activities, including safety activity interface with partnering stakeholders

4.2 General Description of the change

The certification plan needs to include an overall description of the change, the systems involved, their limits and the way they are interfaced with the other, unaffected systems. This description is primarily intended for the experts of the authority who may have to undertake the supervision of the design and development activities performed by the applicant. It may highlight relevant aspects as technical novelties, and for changes involving multiple stakeholders, relationship with changes on their products for which a certification is sought by a partnering stakeholder. Basically, all the aspects of the change as described in section 2 “Stage 1: Define the change” would be covered, focusing on the introduction of the AutoFailMS function in an RPAS. All relations between the affected domains must also be duly described.

4.3 Claims and arguments

It can be seen from the applicable regulations on airborne products that they actually cover through essential requirements, lower level specifications and AMC all the safety aspects an RPAS aircraft product shall comply with: design, manufacture, maintenance, operation & training.

As a consequence, the development of an “argument architecture” for the RPAS product or for the AutoFailMS system is to be constructed as the elaboration of a full and consistent set of applicable regulatory requirements as the “baseline for certification”, focusing primarily on existing acceptable guidance material and standards. The elaboration of the certification baseline is a key element of the certification plan, with the agreement of the plan requiring agreement of the baseline by the authority. This may require establishing an agreement in coordination with the partnering stakeholders and between the authorities involved in the different aviation domains, in order to ensure overall consistency of the different certification baselines proposed by the partners.

4.3.1 High level claim

The applicant of the RPAS airborne segment and designer of the AutoFailMS system has to seek for an agreement with its supervisory authority on a full and consistent set of applicable regulatory requirements and related guidance material. In order to ensure that the authority will be fully satisfied with the demonstration activities and results provided, this agreement needs to be established since the initial step of the RPAS product design.

The certification plan is presented to the relevant authorities and other stakeholders, to gain their agreement that, if the plan is followed and the evidence is presented, they will accept the change into service. Although lack of agreement at this stage does not prevent progress to later stages, the benefit of gaining agreement is to reduce the risk to the certification programme at later stages. This approach can be developed further into requirements. These requirements may all (or mostly) be beneficial, but they introduce significant cost increases if they are introduced progressively through the project.

The ASCOS D1.3 approach proposes to structure the demonstration of safety by building upon the approach of [1] as per Stage 2, suggesting a top-level safety claim (Claim 0) that could be of the form: “*The introduction on an RPAS/several RPAS in the air traffic environment shall keep the same level of safety*”, and then cascading this higher level claim in sub-claims.

Besides, and as part of their overall duty of protecting the public in general and the environment, the authorities of the aviation system continuously develop common safety and environmental rules. These rules are usually formulated as a structured argument of safety requirements. In some domains the argument is more formulated as a performance requirement than as a defined means of compliance (e.g. in the ATM domain).

As consequence, it must be checked whether the current rules and standards are an adequate argument to satisfy the claims it must also be checked whether the assumptions that are used between the domains are adequately addressed.

4.3.1.1 Means of Compliance argument for Claim 0:

4.3.1.1.1 Within the Product Certification Domain

An RPAS considered as an aircraft of CS25 category should without restriction comply with the Essential Requirements for Airworthiness referred to in Article 5 of the Basic Regulation EC216/2008. These Essential Requirements are stated in the Basic Regulation Annex I, which first requirement reads:

1. *Product integrity: product integrity must be assured for all anticipated flight conditions for the operational life of the aircraft. Compliance with all requirements must be shown by assessment or analysis, supported, where necessary, by tests.*

This requirement and all subsequent requirements of Annex I are mandatory to the RPAS. Claim 0 of RPAS could thus be directly inferred from it:

Claim 0 of RPAS: *The integrity of the RPAS product (i.e.: the RPAS system and operation)* ***is*** *assured for all anticipated flight conditions for the operational life of the RPAS system.*

All the subsequent requirements of Annex I applicable to RPAS are then as many points that can be expressed as sub-claims for the RPAS.

Now, developing on the safety requirements that would apply to the AutoFailMS as part of the RPAS system, two requirements of Annex I can be put under focus (amongst many others):

1. C.2. The aircraft, including those systems, equipment and appliances required for type-certification, or by operating rules, must function as intended under any foreseeable operating conditions, throughout, and sufficiently beyond, the operational envelope of the aircraft, taking due account of the system, equipment or appliance operating environment. Other systems, equipment and appliance not required for type-certification, or by operating rules, whether functioning properly or improperly, must not reduce safety and must not adversely affect the proper functioning of any other system, equipment or appliance. Systems, equipment and appliances must be operable without needing exceptional skill or strength.

1. C.3. The aircraft systems, equipment and associated appliances, considered separately and in relation to each other, must be designed such that any catastrophic failure condition does not result from a single failure not shown to be extremely improbable and an inverse relationship must exist between the probability of a failure condition and the severity of its effect on the aircraft and its occupants.

Practically, there is actually no need to cascade claims for AutoFailMS from the RPAS level claims as the Essential Requirements have set up so far the essential requirements applicable to the RPAS constituent systems. Thus, Claim 0 of AutoFailMS could directly mirror ER 1.c.2 & ER 1.c.3:

> **Claim 0 of AutoFailMS:** The AutoFailMS system, **does** function as intended under any foreseeable operating conditions, throughout, and sufficiently beyond, the operational envelope of the RPAS, taking due account of the system operating environment.
>
> The AutoFailMS system considered separately and in relation to the other RPAS constituent systems **is** designed such that any catastrophic failure condition does not result from a single failure not shown to be extremely improbable and an inverse relationship must exist between the probability of a failure condition of AutoFailMS and the severity of its effect on the RPAS operation.

As a consequence, the very high level of safety requirements expressed in Annex I is rarely referred by the designers of aircraft products when more convenient and detailed requirements are expressed in some lower level regulations, like the CS25[7], which are accepted as means of compliance to the higher level requirements of Annex I. For example, article CS 25.1309 "Equipment, systems and installations" reads:

(a) The aeroplane equipment and systems must be designed and installed so that:

(1) Those required for type certification or by operating rules, or whose improper functioning would reduce safety, perform as intended under the aeroplane operating and environmental conditions.

(2) Other equipment and systems are not a source of danger in themselves and do not adversely affect the proper functioning of those covered by sub-paragraph (a) (1) of this paragraph.

(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that -

(1) Any catastrophic failure condition

(i) is extremely improbable; and

(ii) does not result from a single failure; and

(2) Any hazardous failure condition is extremely remote; and

(3) Any major failure condition is remote.

It can be noted that the CS25.1309 details and extends the Essential Requirements on aircraft systems to Hazardous and Major Failure Conditions. So, same as above, the Claim 0 of AutoFailMS could be developed in two sub-claims, by directly mirroring CS25.1309 requirements:

[7] CS (resp. FAR) are maintained by EASA (resp. FAA) and have no official mandatory status. They are established on grounds of previous experience cumulated by authorities, which gives them a "compulsory" status and explain their designation of "soft law".

Sub-claim 1 of AutoFailMS: The AutoFailMS system **is** designed and installed so that it performs as intended under *all anticipated* operating and environmental conditions of the RPAS product.

Sub-claim 2 of AutoFailMS: The AutoFailMS system, considered separately and in relation to the other RPAS constituent systems, **is** designed so that -

(1) Any catastrophic failure condition is extremely improbable; and does not result from a single failure; and

(2) Any hazardous failure condition is extremely remote; and

(3) Any major failure condition is remote.

Where AMC25.1309, supplemented with AMC-RPAS.1309, provides for the agreed definitions and the qualitative and quantitative objectives for all the terms introduced in CS.

The reasoning can be pursued down to the AMC of CS25, with the example of AMC25.1309. Application of the well-known ARP 4754A/ED79A and its related standards is recognized by authority as the backbone of demonstration of compliance to the AMC25.1309.

Finally, as all aspects of certification cannot realistically be completed prior to the starting of design activities, the safety plan should propose to the authority a framework on how to seek agreement on any further technical issues related to the interpretation of the regulatory requirements and the need to consolidate the certification baseline that may arise during the design and development of the product. For EASA or FAA this would be the framework of EASA CRI process (Certification Review Item), or FAA IP process (Issue Paper), which is rather similar framework of discussion and agreement on technical issue in interpretation of the regulatory requirements established by these authorities.

4.3.1.2 Within the Remote Pilot

In a same way than any product intended for sale to the general public must be provided with a “notice of use” leaflet informing the customer of any limitation, precaution and limitation of use, an RPAS product will be required by the supervisory authority of the design to be provided with all necessary documentation for RPAS operation that will define the baseline and specific aspects of the handling of RPAS product for the intended operations. This approach will be very similar to the current approach done for an aircraft product for which operational documentation shall be established as component of the certified product. In addition to the operating manual (the FCOM) which is required by authorities, the AFM (Aircraft Flight Manual) is a document specifically stating all the limitations and particular aspects the operator needs to comply with for safely handling of the product. The authority will have to certify the content of the AFM as part of the aircraft certification.

The RPAS operator will have to demonstrate to its supervisory authority it operates the RPAS system in conformance with the FCOM and AFM established by the RPAS designer. In case an RPAS operator would seek approval for RPAS operations that were not foreseen or anticipated during the design and certification of the RPAS, supplemental demonstration activities are required in order to demonstrate that safe operation is maintained. This demonstration is likely to involve the design authority (i.e.: the design organisation) and its authority, if the change is deemed significant by the operator's authority in terms of operational context or performance (for example, the extension of the maximum distance allowed to an emergency landing site).

4.3.1.3 Within the ATM domain

The demonstration of safe operation of RPAs would probably require specific involvement and handling of the ATCo (e.g.: contingency handling, specific communication channels, etc…) and key assumptions on ATCo working procedures or Air Traffic Services have to be done, entailing a change in ATM operation, it is expected that the description of the change is properly coordinated between the ATM partner(s) and the RPAS design partner(s).Based on this description of the change in ATM operations, each ATM partner will have then to demonstrate to its authority its ability to maintain safe operation of the ATM services following the change and the introduction of RPAS within the controlled traffic.

For those changes requiring coordination between the RPAS system holder and the ATM side, it is important to ensure that the certification process engaged by an RPAS applicant and its ATM stakeholder(s) towards their respective authorities is consistent and coordinated. Noting that for the ATM domain the structure of regulatory requirements is very similar to the airborne domain, with essential requirements (in 216/2008), "common" requirements (in 1035/2011) and future AMC[8], it is expected that the requirement for a risk based approach (i.e.: hazard identification, risk assessment and mitigation approach) would be led commonly by all stakeholders on grounds of a standard previously agreed with the authorities (for example by applying a standard methodology ED78A[9], AMC25.1309, ARP4754/ED79A, ARP 4761/ED135 or a similar approach formerly accepted by the authorities).

4.3.1.4 Within the Maintenance domain

The RPAS product will be required by the supervisory authority of the operator to be maintained in airworthy condition by an approved maintenance organisation complying with regulation EC2042/2003 and addendums ("Part M"). Maintenance shall be carried on in accordance with the maintenance instructions provided by the RPAS designer.

[8] It is worth noting that AMC or agreed industry standards are still to be published.
[9] ED78A methodology has been developed and applied in a number of air-ground applications involving multiple stakeholders, initially for datalink.

The RPAS product will be required by the supervisory authority of the design to be provided with all necessary documentation for maintenance. This approach will be very similar to the current approach done for an aircraft product for which maintenance documentation shall be established as component of the certified product. In addition to the maintenance manuals (the AMM, SRM, etc…) which are required by authorities, the Instructions for Continued Airworthiness (ICA) document all the maintenance aspects that are critical for maintaining safe operation of the product. In the case of an RPAS system it might include the ground station. The authority will have to certify the content of the ICA section as part of the aircraft certification.

4.3.2 Sub claims

Claim 1: The change to introduce the AutoFailMS is specified such that it contributes to acceptably safe operations

Means of compliance argument:

- This considers the AutoFailMS at a conceptual level (as described in Context C0-1, see section 3.2.1.1), without considering how it is actually implemented. At this level there is no consideration of equipment or specific human roles, just what the AutoFailMS will achieve and how it will interact with the rest of the TAS. The assessment is based on scenarios of operation of the AutoFailMS and the associated description of the sequence of events in each scenario (see section 3.2.1.2). Scenarios can be classified as: normal, abnormal and failure scenarios. A set of normal scenarios has been developed in section 3.2.1.2. Further scenarios will be identified and defined as part of developing the argument, but may then need to be fed back into the other work undertaken within the case study. If the operation does not change from current, it is considered that the level of safety is equivalent to the current level of safety
- The main assessment to support this claim will be a form of functional hazard assessment (FHA), using techniques which are well-established in assessing functions (rather than equipment). The form of assessment will be explained in more detail in a later version of this document. Analysis at this level identifies the pre-existing hazards relevant to the function and any system-generated hazards introduced / affected by the function. It also identifies the safety objectives which the function has to meet in order to achieve the level of safety defined in Context C0-2 (see section 3.2.1.1), and any assumptions, at the functional level, about the behavior of the related functions.
- If the operation will be different from the current standard, the applicant will argue the safety level to the Authority by comparison with established operations.

Claim2: Logical design of the change to introduce AutoFailMS satisfies the specification and is realistic

Means of compliance argument:

- The logical design includes the architecture of the AutoFailMS (including its impact on the communications link and the remote pilot);

- The main assessment to support this claim will be a form of preliminary system safety assessment (PSSA) of the logical design, using techniques which are well-established in assessing functions and sub-functions (rather than equipment). The form of assessment will be explained in more detail in a later version of this document.
- The main assessment to support this claim will be an assessment of a logical model of the operations and the establishment of requirements
- This model needs also to take into account all the assumptions that are coming from the other domains (CO-1)
- Initially it will be argued that the operation with AutoFailMS is comparable with the current operation.

Claim 3: Implementation of the AutoFailMS is complete and correct

- The implementation of the AutoFailMS is complete and correct in accordance with its specification and logical design. The assessment of the physical implementation considers the evidence that the specific equipment (hardware and software), procedures and any associated human competence requirements fully and correctly implement the AutoFailMS. This includes an assessment of any emerging properties to ensure that they do not compromise the safety of the system. The development of many systems encounters a major problem at this point, namely the limited ability of test-based V&V to show with sufficient confidence that the required safety integrity properties of the system have been met. This leads to the adoption of an assurance based approach.
- The applicant will show that the actual operation documented and used by the applicant fulfill the requirements as derived in claim 2
- The applicant must show that all the assumptions coming from other domains are still fulfilled

Claim 4: Transition to AutoFailMS operation is acceptably safe

Means of compliance argument:

- The AutoFailMS can be brought into operational service safely and includes confirmation that preparation for operation is complete (procedures have been published, resources procured, personnel trained)
- The arrangements for ongoing safety management are in place
- The switchover process has been fully defined and assessed and any appropriate mitigation are in place.
- This claim would be made as part of a wider claim that the RPAS, within which the AutoFailMS is implemented, can be brought into operational service safely (see section 3.2.4).

Claim 5: The use of the AutoFailMS will continue to be demonstrated as acceptably safe in operational service

Means of compliance argument:

- Continuous safety monitoring will collect appropriate metrics to confirm the results of the safety assessments undertaken under earlier claims;
- Processes are in place to report, investigate and (where appropriate) correct any safety-related incidents
- Processes are in place to assess any interventions (e.g. maintenance) and demonstrate that risks are known and acceptable.
- Processes are in place to produce lessons learned for future developments

4.4 Coordinated approaches between domains

For changes requiring coordination between the RPAS manufacturer and other domains within the TAS, it is important to ensure that the certification process engaged by the applicant and its stakeholders towards their respective authorities is consistent and coordinated. The Assumptions between the domains need to be carefully addressed

4.4 Content of the certification baseline

The certification baseline that can be proposed for agreement in a first step by the applicant of an RPAS constituent system will be:

- EASA Policy Statement airworthiness certification of UAS (EASA-E.Y013-01_ UAS_ Policy)
- Regulation (EC) No 748/2012, “Part 21”, subpart B. (explicitly referred in EASA policy)
- EASA CS 25 (as it can be inferred from the policy for an RPAS the size of a Single Aisle)
- AMC-RPAS.1309_Issue-1 (and AMC-RPAS.1309_Scoping-Paper_Issue-1)
- EASA CS AWO (at least partly)
- JARUS Guidance on RPAS C2 link RCP (for consolidated document)

In addition, for those topics for which it can be known in the first step of the design that a discussion and agreement needs to be conducted with the authority, due to the specifics of the RPAS concept, a list of “Review Items” or “Issues” will be appended to the baseline. For example, the following topics can be presumed to be open in order to agree on interpretation material:

- RPAS tests for Certification (planning and extent of tests to be conducted);
- Human Factors considerations (specific ergonomic and workload aspects of the ground station);
- Compliance with Airworthiness Requirements to isolate RPAS system from security threats;
- Certification of Software and Complex Digital Devices used on ground stations.
- Relationship with Certification Requirements on ATM applications for the handling of RPAS (for example in case the application envisages that the ATCo could take control of the RPAS in some specific circumstances)
- Relationship with Certification Requirements in other domains for the handling of RPAS (e.g.: MET)

4.5 Compliance Demonstration

The certification plan should give a comprehensive description of how the evidences will be produced that all the regulatory requirements are complied with. This can for example take the form of an assembly of plans shown to be consistent in a Means of Compliance Checklist

The certification plan should also propose an organisation of Certification Deliverables together with their certification status. Depending on this status, the Certification Deliverables are documents that need either to be approved or agreed or received by the authority prior to granting the certificate. They can be considered as the core part of the Certification Plan.

A separate document describing the assumptions coming from other domains and how these are being covered must be part of the document deliverables.

A Functional Hazard Assessment (FHA) will be part of the compliance demonstration in order to analyze which hazards need to be considered. The FHA can be the basis for fixing the Design Assurance Levels. The FHA itself must be a certification deliverable.

Any Human Factors considerations and assumptions that are the result of compliance activities must be compiled in a document in order to be useable in the Continuing Safety activities for personnel training requirements.

It may be convenient that the above points are addressed in a safety document called "Safety Master Document SMD". The SMD details and explain how the safety regulation will be interpreted for RPAS project and gives all the data necessary to perform FHA and safety assessments/analyses required to show compliance with the ARP 4754A/ED79A using the methods recommended in the ARP 4761A/ED135A . If used the SMD should be referenced in the certification plan

4.6 Agreement on the Certification Plan

Early agreement on the Certification Plan and the Means of Compliance with the relevant Authorities is important in order to avoid unnecessary "surprises" during the compliance period

4.7 Continuing Safety activities

Understanding and monitoring how the demonstration of safety will be managed and achieved is of utmost importance for the authority. As a consequence a special focus is to be put in the certification plan on how the ARP standards will be implemented, giving sufficient details on:

- the design organisation and the actors in charge;
- the organisation of safety activities, their inputs and outcomes, how they interface;
- the key documents produced as output of these activities

The case occurring, description of safety activities should include safety activities and output documents interfacing with partnering stakeholders.

All these point will be described in the safety plan performed in accordance with ARP4754A/ED79A recommendations. The safety plan will be referenced in the certification plan

4.8 Example outline of a Certification Plan

<u>1. General Description</u>

1.1. Overview of Functional Architecture of the AutoFailMS System

1.2. Interface with other RPAS Systems

1.3. Interface of the AutoFailMS System with other domains

<u>2. Progressive involvement of Authorities (SOI)</u>

2.1. On system development activities

2.2. On Safety Demonstration activities

<u>3. Applicable Requirements, standards and Related Guidance</u>

3.1. Certification Basis (Claims and Argument architecture)

3.2. Special Conditions & Issue Papers & Equivalent Safety Findings

3.3. Interpretative Material

3.4. Listing required tests

3.5. Other requirements and reference documents

3.6. Means of Compliance checklist

3.7Relationship with Certification Requirements in neighboring domains

<u>4. Compliance demonstration</u>

4.1. List of Certification Deliverables

4.2. Summary of the Functional Hazard Assessment

4.3. Determination of the Design Assurance Levels for the change

4.4. Compliance deliverables (including assumptions)

4.5 Test results

4.6. Human Factors considerations

<u>5. Transition requirements</u>

5.1. Transition document

<u>6. Continuing Safety activities</u>

6.1. Scope of the Safety activities

6.2. Main Safety actors and outputs

6.3. Relationship of the AutoFailMS System requirements with the requirements in neighboring domains

6.4. Personnel training requirements

5 Stage 4 Specification and Stage 5 Design

5.1 Safety Objectives

Stage 4 focuses on the behavior of the changed system in the absence of failure and establishes safety objectives on it. This stage identifies the hazards that the system is intended to mitigate (external hazards) and it analyses if the change sufficiently mitigates those hazards. However, as discussed in 3.4.1 this Use Case considers all together the external and the self-failure hazards. The hazards are considered as any potential unsafe situation. Consequently this Use Case addresses together Stage 4 and Stage 5.

The normal, abnormal and failure scenarios have been developed to identify the generic hazards. The proper level of detail to include in the scenarios is a key element to ensure that all the hazards at TAS level have been identified. (Rec_07) In this Use Case:

- The failure scenarios describe as well the impact on the remote pilot (e.g. increase of pilot workload).
- Although the objective of this Use Case is restricted to AutoFailMs, the failure scenarios include explicitly description of combination of AutoFAilMS failure with “C2 failure” or “detect and avoid” failure or “loss of datalink” failure. These combinations of failure can impact on the ATM emergency procedures.

The complete and correct identification of hazards need to be supported by an agreed methodology that common to all TAS stakeholders. In this Use Case the identification of hazards have been performed by analysis the impact of the failures in several domains on several domains.(Rec_06).

Table 13 presents the list of hazards. The hazards have been classified according to three domains:

- Aircraft and AutoFailMS system. (which supports claim 1.1.2.1 and 1.1.3.1 and claim 2.1)
- Remote Pilot. (which supports claim 1.1.3 for remote pilot dependency and claim 2.2)
- ATM (which supports claim 2.3).

Note that the application of current standards implies a close relation between claim 1 and claim 2.

The severity matrix is coherent with to JARUS [9](related to aircraft and on ground) and with ER-010 [16](related to impact of RPAS function on aircraft and on ATM) For this Use Case; the impact on AutoFAilMs is considered as a contributor to the impact on the RPAS. The final severity allocated to the hazards is the worst of the severity considered in aircraft and ATM domain. The final severity has been expressed as CAT, HAZ, MAJ, so on. Note that the ER-010 avoids any kind of equivalence between severity classes and classical CAT, HAZ, etc. Each severity implies a safety objective (qualitative and quantitative).

The final severity has been expressed as CAT, HAZ, MAJ, so on. Note that the ER-010 avoids any kind of equivalence between severity classes and classical CAT, HAZ, etc. Each severity implies a safety objective (qualitative and quantitative):

The quantitative safety objective can be defined by a severity table:

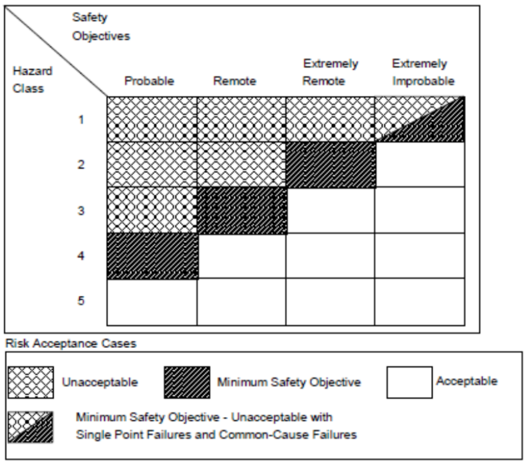


Table 11 Risk acceptance cases [17]

For this use Case, it is suggested that the quantitative safety objective associated to each hazard is:

Severity	Probability
CAT	Extremely improbable
HAZ	Extremely remote
MAJ	Remote
MIN	Probable

Table 12 Safety objectives

The qualitative objective, for this Use Case, is understood in a similar way as per CS25 1309 AMC for Fail Safe requirement for Catastrophic Failure Conditions and as per ARP 4754A/ED79A for DAL assignment. The DAL objective is the level of confidence, that errors in requirements, design and implementation have been considered and mitigated. Refer to Rec_02

The list of hazards, the safety impacts and the severity is summarized in Table 13

.

Ident	name	Effect on RPAS (aircraft level)	Effect on Air Crew (remote pilot)	Effects on Air Traffic Service	Final severity
GEN_HAZ_1	**slight increase of controller workload**	N/A	N/A	Class IV according to ER-010	MIN
GEN_HAZ_2	**significant increase of controller workload**	N/A	N/A	Class III according to ER-010	MAJ
GEN_HAZ_3	**large increase of controller workload**	N/A	N/A	Class III according to ER-010	MAJ
GEN_HAZ_4	**slight increase of pilot workload**	N/A	MIN as per JARUS Class IV according to ER-010	N/A	MIN
GEN_HAZ_5	**significant increase of pilot workload**	N/A	MAJ as per JARUS Class III according to ER-010	N/A	MAJ
GEN_HAZ_6	**large increase of pilot workload**	N/A	HAZ as per JARUS Class III according to ER-010	N/A	HAZ
GEN_HAZ_7	**Loss of RPAS C2 link** **No loss of datalink ATC.** **RPAS controlled by AutoFailMS**	MAJ. Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in functional capabilities.	N/A pilot cannot control the RPAS	AutoFailMS managed the RPAS, detect and avoid function is not lost. FP 1 Class V as per ER-010 However it is expected that situation might increase controller workload. Class IV.	MAJ
GEN_HAZ_8	**loss of RPAS communication** **no loss of C2** **RPAS controlled by AutoFailMS**	MAJ. Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in functional capabilities.	Increase on pilot workload as part of pilot duties. MIN. Pass to voice communication	It is expected that situation might increase controller workload. Class IV.	MAJ

Ident	name	Effect on RPAS (aircraft level)	Effect on Air Crew (remote pilot)	Effects on Air Traffic Service	Final severity
GEN_HAZ_9	**Loss of RPAS communication and C2. RPAS controlled by AutoFailMS**	HAZ Loss of the RPA where it can be reasonably expected that a fatality will not occur The RPAS does no send reports although it is controlled by AutoFailMS and it is reasonable to expect that it follows last flight plan update.	N/A pilot cannot communicate with the RPAS	AutoFailMS managed the RPAS, detect and avoid function is not lost. FP 1 Class V as per ER-010 However it is expected that even if the RPAS cannot report its position (loss of datalink) so the controller will probably need deviate aircraft in the vicinity Class III...	HAZ
GEN_HAZ_10	**Loss of AutoFailMS (pilot revert to manned mode)**	MAJ significant reduction in functional capabilities.	Increase on pilot workload as part of pilot duties. MIN.	Remote pilot manages the RPAS, detect and avoid function is not lost. FP 1	MAJ
GEN_HAZ_11	**Total loss of RPAS control (no AutoFailMS and no pilot)**	CAT Failure conditions that could result in one or more fatalities.	N/A pilot cannot communicate with the RPAS	Total loss of RPAS control. RPAS is not supposed to follow last flight plan update. It is supposed to have detected and avoid function operative. Class II	CAT
GEN_HAZ_12	**loss of adherence to flight plan**	NSE failure conditions that would not affect the operational capability of the RPAS	MIN, slight increase of pilot workload As per JARUS	MIN slight increase in remote crew workload, such as flight plan changes. As per JARUS Class V as per ER-010	MIN
GEN_HAZ_13	**Slight Reduction in separation assurance**	MIN slight reduction separation assurance.	MAJ failure condition has a significant increase in remote crew workload	Class II as per ER-010 (or class III)	MAJ
GEN_HAZ_14	Large reduction of separation	MAJ significant reduction in separation assurance.	MAJ e failure condition has a significant increase in remote crew workload	Class II as per ER-010	MAJ
GEN_HAZ_15	Total loss of separation	HAZ large reduction in safety margins	MAJ e failure condition has a significant increase in remote crew workload	Class II as per ER-010	HAZ

Ident	name	Effect on RPAS (aircraft level)	Effect on Air Crew (remote pilot)	Effects on Air Traffic Service	Final severity
GEN_HAZ_16	**loss of collision avoidance**	HAZ large reduction in safety margins	HAZ large increase of pilot workload. Pilots needs to avoids collision	FP 1 no collision avoidance. Class I	HAZ
GEN_HAZ_17	**missed approach**	NSE failure conditions that would not affect the operational capability of the RPAS	MIN slight increase in remote crew workload	At worst class III, Significant increase of air traffic controller that needs to separate other traffic.	MAJ
GEN_HAZ_18	**landing emergency site**	NSE failure conditions that would not affect the operational capability of the RPAS	MIN slight increase in remote crew workload	At worst class III, Significant increase of air traffic controller that needs to separate other traffic.	MAJ

Table 13 Generic hazard. Safety effects on several domains

The safety objectives (both in terms quantitative and qualitative) need to be cascaded to each of the stakeholder. Once it is agreed which is the safety contribution of each stakeholder to the safety objective, it is possible to properly allocate safety requirements.

For the purpose of this Use case, the following methodology is proposed:

5.1.1 Safety Objectives

Note that in this Use Case, there is not external hazards (refer to 3.4.1) the hazards are related to failure of the RPAS system, the RPAS when working normally is conceived to be transparent for ATM and the remote pilot is not expected to manage failure conditions. For this use Case, it has been suggested that the safety objectives are allocated to the RPAS and to the AutoFailMs, and therefore, they are met by ARP 4754A/ED 79A regulation.

- It is suggested in this Use Case that the quantitative overall safety should not be less demanding than current regulation of aircraft. Refer to JARUS [9] and Table 57
- It is suggested in this Use Case that the qualitative safety objective should not be less demanding than current regulation for aircraft (DAL A/CAT, DAL B/HAZ, so no) Refer to JARUS [9] and Table 59.

As a result, the safety objectives depend on isolation of the RPAS.

Note as well that the ATM requirements have been included in the ARP 4754_A. In normal or failure conditions, the RPAS needs to be compliant with the requirements (safety and performance) from the ATM (Refer 3.5.3). As an example, let us to take the “missed approach”. This hazard is classified MIN in current regulation. , however, using a Total Aviation System severity table, this hazard has been classified MAJ (refer Table 14). The RPAS needs to achieve the MAJ objective in qualitative and quantitative terms.

In case of AutoFAilMS failure, the ATM might perform certain procedures (e.g. emergency procedures). Some of these emergency procedures are associated to a safety net triggering.

It has been mentioned that the current regulation does not totally addresses the allocation of quantitative requirements over human, (e.g. pilot). For the AutoFailMS, the interface of the system with the pilot is managed as currently (inputs of SSA to AFM and FCOM) and involvement of human factor team. The Rec_10 can be plugged in the claim 2.3.

As a result, this Use Case concludes that the safety objectives agreed among all stakeholders could be allocated only by RPAS if the current regulation is developed to include ATM requirements and develops the concept of Human DAL). The ATM emergency procedures are seen as a consequence of a triggering of an ATM or RPAS safety net.

Ident	name	Final severity	comment	Safety objective quantitative	Safety objective qualitative
GEN_HAZ_1	**slight increase of controller workload**	MIN	The increase of workload caused by a failure on the RPAS operation due to an AutoFailMS has only one contributor the RPAS operations.	The contribution of AutoFailMS system to an The RPAS failure modes implying an slightly increase of controller workload shall be compliant in E-03/FH objective	Functions of AutoFailMS whose failure might imply an slight increase on the workload of the controller should be developed at least in DAL D:
GEN_HAZ_2	**significant increase of controller workload**	MAJ	The increase of workload caused by a failure on the RPAS operation due to an AutoFailMS has only one contributor the RPAS operations.	The contribution of AutoFailMS system to The RPAS failure modes implying a significant increase of controller workload shall be complainant the E-05/FH objective.	Functions of AutoFailMS failure modes implying a significant increase of controller workload shall be developed in DAL D
GEN_HAZ_3	**large increase of controller workload**	MAJ		The contribution of AutoFailMS system to an RPAS failure modes implying a large increase of controller workload shall be compliant the E-05/FH objective	Functions of AutoFailMS failure modes implying a large increase of controller workload shall be developed in DAL C
GEN_HAZ_4	**slight increase of pilot workload**	MIN		The contribution of AutoFailMS system to an the RPAS failure modes implying an slightly increase of pilot workload shall be compliant the E-03/FH objective	Functions of AutoFailMS whose failure might imply an slight increase on the workload of the pilot should be developed at least in DAL D:
GEN_HAZ_5	**significant increase of pilot workload**	MAJ		The contribution of AutoFailMS system to a failure modes implying a significant increase of pilot workload shall be compliant the E-05/FH objective.	Functions of AutoFailMS failure modes implying a significant increase of pilot workload shall be developed in DAL C
GEN_HAZ_6	**large increase of pilot workload**	HAZ		The contribution of AutoFailMS system to an RPAS failure modes implying a large increase of pilot workload shall be compliant the E-07/FH objective	Functions of AutoFailMS failure modes implying a large increase of pilot workload shall be developed in DAL B

Ident	name	Final severity	comment	Safety objective quantitative	Safety objective qualitative
GEN_HAZ_7	**Loss of RPAS C2 link No loss of datalink ATC. RPAS controlled by AutoFailMS**	MAJ.		The contribution of AutoFailMS system to and the RPAS failure modes implying a loss of auto C2 shall be compliant the E-05/FH objective.	Functions of AutoFailMS failure modes implying a loss of auto C2 shall be developed in DAL C
GEN_HAZ_8	**loss of RPAS communication no loss of C2 RPAS controlled by AutoFailMS**	MAJ	The loss of datalink communication depends on the ATC and on the RPAS. The allocation of safety objective to each stakeholder might follow the ED-78A. ED-78A is coherent with ARP 4754A/ED79A.	The contribution of AutoFailMS system to and the RPAS failure modes implying a loss of datalink communication shall be compliant the E-05/FH objective.	Functions of AutoFailMS failure modes implying a loss of datalink communication shall be developed in DAL C
GEN_HAZ_9	**Loss of RPAS communication and C2. RPAS controlled by AutoFailMS**	HAZ.	Combination of failure modes, refer to GEN_HAZ_7 and GEN_HAZ_8		
GEN_HAZ_10	**Loss of AutoFailMS (pilot revert to manned mode)**	MAJ		The contribution of AutoFailMS to failure modes implying the loss of AutoFailMS shall be compliant with the E-05/FH objective.	The function of AutoFailMS whose failure mode implies the loss of AutoFailMS shall be developed in DAL C
GEN_HAZ_11	**Total loss of RPAS control (no AutoFailMS and no pilot)**	CAT		The contribution of AutoFailMS to the total loss of RPAS shall be compliant the E-09/FH objective.	Functions of AutoFailMS failure modes implying a total loss of RPAS shall be developed in DAL A
GEN_HAZ_12	**loss of adherence to flight plan**	MAJ		The contribution of AutoFailMS to failure modes implying the loss of adherence to flight plan compliant the E-05/FH objective.	The contribution of AutoFailMS to failure modes implying the loss of adherence to flight plan shall be developed in DAL C

Ident	name	Final severity	comment	Safety objective quantitative	Safety objective qualitative
GEN_HAZ_13	**Slight Reduction in separation assurance**	MAJ		The contribution of AutoFailMS to failure modes implying a slight loss of separation shall be compliant with the E-07/FH objective.	The contribution of AutoFailMS to failure modes implying a slight loss of separation shall be developed in DAL B
GEN_HAZ_14	Large reduction of separation	MAJ		The contribution of AutoFailMS to failure modes implying a large loss of separation shall be compliant with the E-07/FH objective.	The contribution of AutoFailMS to failure modes implying a large loss of separation shall be developed in DAL B
GEN_HAZ_15	Total loss of separation	HAZ		The contribution of AutoFailMS to failure modes implying a total loss of separation shall be compliant with the E-07/FH objective.	The contribution of AutoFailMS to failure modes implying a loss of separation shall be developed in DAL B
GEN_HAZ_16	**loss of collision avoidance**	HAZ		The contribution of AutoFailMS to failure modes implying a loss of collision avoidance shall be compliant with the E-07/FH objective.	The contribution of AutoFailMS to failure modes implying a loss of collision and avoidance shall be developed in DAL B
GEN_HAZ_17	**missed approach**	MAJ		The contribution of AutoFailMS to failure modes implying a missed approach shall be compliant with the E-05/FH objective.	The contribution of AutoFailMS to failure modes implying a missed approach shall be developed in DAL C
GEN_HAZ_18	**landing emergency site**	MAJ		The contribution of AutoFailMS to failure modes implying a landing on emergency site shall be compliant with the E-05/FH objective.	The contribution of AutoFailMS to failure modes implying a landing on emergency site shall be developed in DAL C

Table 14 Generic hazard. Safety objectives

5.1.2 Safety requirements

This Use case has defined some requirements from normal, abnormal and failure scenarios. The process of extracting requirements is not a standardized process. Refer to Rec_08 Note that these safety requirements do not provide complete a correct set of safety requirements

Requirements for AutoFailMS (system level)

Ident	description
Req-1	AutoFailMS shall provide information of aircraft status to remote pilot
Req-2	AutoFailMS shall detect failure conditions
REq-3	AutoFailMS shall manage failure conditions according to autonomy level
Req-4	AutoFailMS shall inform to the remote pilot of a failure condition according to type of failure
REq-7	AutoFailMS shall inform to the ATC of a potential deviation from intended flight plan (depending on autonomy level)
Req-9	AutoFailMS shall guide the RPAS to a landing site
Req-11	AutoFailMS shall execute a missed approach
Req-20	AutoFailMS shall detect the loss of AutoFailMS
Req-27	AutoFailMS shall detect the erroneous AutoFailMS, then AutoFailMS disconnects

Table 15Requirement for AutoFailMS (system level)

Requirement for RPAS

Ident	description
Req-21	Aircraft system shall detect the total loss of AutoFailMS (BITE system)
Req-28	Aircraft system shall detect the erroneous of AutoFailMS (BITE system) then AutoFailMS disconnects
Req-34	Loss of C2 link shall be designed according to DAL A (application of ARP4754A/ED79A)
req-60	RPAS system shall ensure that there is not any single cause implying an spurious failure detection and a faulty C2 (common mode)
Req-61	RPAS system shall ensure that there is not any single cause implying an spurious failure detection and a faulty “detect and avoid” (common mode)
req-70	RPAS system (CDS) shall informs to the remote pilot of the autonomy level
Req-71	RPAS system shall inform to the remote pilot of the modification of autonomy level
req-80	After loss of datalink voice shall be designed as a back up

Table 16Requirement for RPAS

Requirement for the remote pilot

Ident	description
Req-5	Remote pilot shall manage the failure according to autonomy level
Req6	Remote pilot shall inform to the ATC of a potential deviation from intended flight plan (depending on autonomy level)
Req-10	Remote pilot shall guide the RPAS to a landing site
Req-12	Remote pilot shall execute a missed approach
Req-22	Remote pilot shall revert to manned mode after the loss of AutoFailMS

Ident	description
Req-24	The remote pilot shall pilot the RPAS in manned mode for a certain time (maximum time to be decided with human team)
Req-26	Remote pilot shall disengage the AutoFailMS and passes to manned mode after detection of erroneous AutoFailMS
Req-81	Trajectory modifications shall be validated by the remote pilot

Table 17Requirement for the remote pilot

Requirements for ATC

The requirements on the ATC are no necessary to meet the safety objective. Refer to 5.1.1

Ident	description
REq-8	Controller shall check the impact of a potential deviation of RPAS on the ATM
Req-31	ATC shall define procedure for uncontrolled RPAS (e.g. divert traffic around)
Req-32	ATC shall define procedure for disappeared RPAS (e.g. divert traffic around, inform authorities)
Req-33	ATC shall define procedure for RPAS after collision and avoidance loss (e.g. divert traffic around)
Req-40	ATC shall define procedure for uncontrolled RPAS (e.g. divert traffic around) in TMA
Req-41	ATC shall define procedure for disappeared RPAS (e.g. divert traffic around, inform authorities) in TMA
Req-42	ATC shall define procedure for RPAS after collision and avoidance loss (e.g. divert traffic around) in TMA
Req-50	ATC shall define procedure to contact remote pilot in case of abnormal RPAS behaviors
Req-82	ATM shall define a “maximum” level of RPAS allowed in certain airspace.

Table 18Requirement for Requirements for ATC

Requirement for maintenance

Ident	description
Req-25	Maintenance Activities shall address the MTBF for the hidden failure “undetected loss of AutoFailMS”
Req-30	Maintenance Activities shall address the MTBF for the hidden failure “loss of automation mode”

Table 19Requirement for Requirements maintenance

5.2 Safety objectives and safety requirements using WP 3 techniques

The allocation of safety objectives only to the RPAS stakeholder simplifies the justification of claim 1 and claim 2 . However, the objective of ASCOS is to create a common certification approach. It is possible to “share” the safety objective among several stakeholders. The D1.3 should include a task to cascade quantitatively and qualitatively safety objectives to the TAS stakeholders refer to Rec_03.

Let us take the case of “**total loss of separation**”. It has been assessed HAZ and therefore the probability is “extremely remote”. The TAS stakeholders need to agree with authorities what “extremely remote” means for this specific case. Currently “Extremely Remote” means E-07/FH (see ARP4754A/ED79A)., This objective is cascaded to the stakeholders:

5.2.1 The cascading of quantitative safety objectives to several stakeholders is coherent with the design.

The safety objective E-07/FH is achieved by RPAS E-06/FH AND E-01 ATM. In this case, stakeholders needs to analyze interface to ensure that the "AND" tree is coherent with the design. If there is a single failure that causes a total loss of separation in the RPAS and as well loss of separation assurance in the ATM, then the design needs to be updated or the "AND" tree is not correct. As an example, the Flight Management system of the RPAS is erroneous ant it can no longer manage the flight plan. The AutoFailMs (no failure) detects it and communicates it to remote pilot who passes to manned mode. But the remote pilot cannot assure the separation because the trajectory calculated by the Flight Management System is incorrect. The remote pilot cannot ensure the adherence to flight plan nor the separation, the ATM does not know the flight plan then ATM cannot ensure the separation

The interface between the ATM and the RPAS has created a common mode failure. The RPAS, the remote pilot and the ATM shares the same trajectory updates. In case of erroneous trajectory updates the remote pilot cannot be the backup of the RPAS, nor the ATM can divert the traffic.

In the previous approach (refer to 5.1) the hazards are mitigated only one RPAS (e.g. independent trajectory calculators), and the ATM is seen as a safety net. In this approach, however, the stakeholders needs to ensure that there is no common mode failure in the design that might impair the safety objective allocation

This level of analysis is performed on stage 7 of D1.3 [1] and it is out of the scope of this safety Case. However, let us see how the methodology proposed by WP 3.2 [18] can provide relevant safety inputs to the safety practitioners.

The ESDs proposed by WP 3.2 [18] consider contribution of several stakeholders to the same end state by the use of ESD, the ESD represents the architecture of a system and the interfaces among stakeholders. ESDs are a graphical representation of stage 1 of D1.3 and they are composed by initiating event, pivotal events and the end element. An initiating event represents the start of the accident scenario, the pivotal element represent safety barriers that can avoid the accident and the end event stats the final outcome. The safety practitioner can impose a failure rate (safety objective) to the end state. The safety objectives need to be coherent with context--C02.

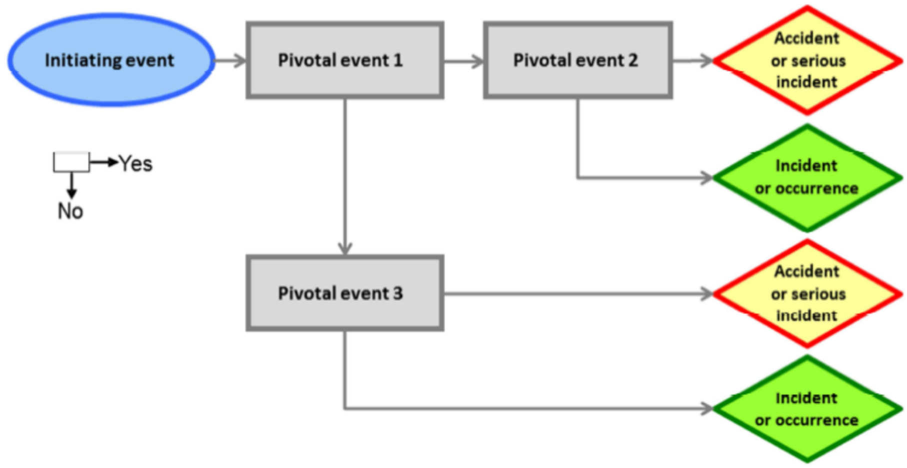


Figure 10 ESD as per WP 3.2

Each element is fed by a fault tree that represents the design. The fault trees can be quite complex and they include contributors referred to different stakeholders. It is possible them to find a common contributor to the initiating event and to the pivotal events.

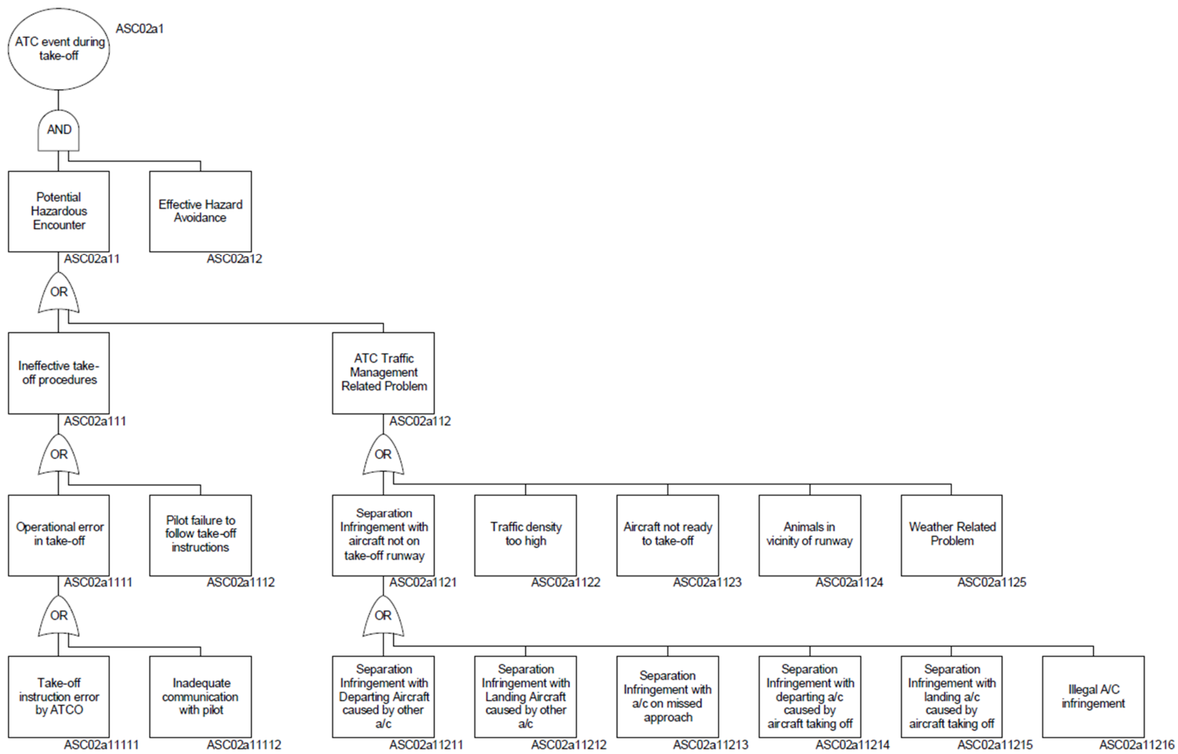


Figure 11 Fault tree

The safety objective allocated to the end element can be cascaded to the fault tress and allocated to the stakeholders coherently with the design structure.

5.2.2 The cascading of qualitative safety objectives to several stakeholders is coherent with the design

The allocation of safety requirements only to the RPAS as proposed in approach proposed in 5.1 allows to ensure the qualitative objective by means of DAL (refer to 3.5.1) However if the safety objectives are supported by several stakeholders, it is necessary to agree the same or coherent level of quality development. The ARP4754A/ED79A methodology addresses the concept of develop assurance level depending on the design.

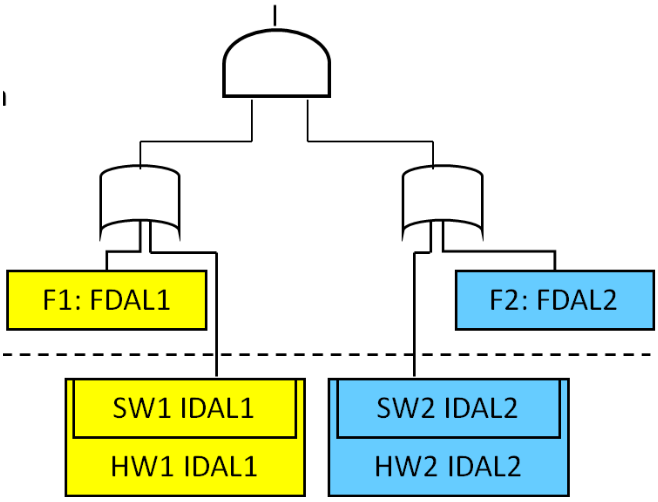


Figure 12 DAL cascading in independent systems

The ESD proposed in WP 3.2 might be tailored to allocate quality development in a similar way than the process followed on aircraft.

5.3 Conclusion

The safety impact of each hazard has been analyzed for the Total Aviation System and associated to a severity; the worst severity has been retained. The safety objective has been expressed in qualitative and quantitative terms depending on the severity, it has been decided that the RPAS meets in isolation the safety objective and the ATC provides safety net in case of failure.

This stage presents a list of safety objectives, safety requirements and degree of assurance (DAL) for the RPAS operations assisted by AutoFailMS.

6 Stage 6 : Update of argument

The study of the impact on AutoFailMS in the RPAS operations imply the following modification on the certification argument as presented on stage 2

C0-2 Level of safety defined as per severity matrix

This use Case has defined a common severity matrix that classifies the severity of the hazards. The TAS stakeholders are supposed to agree on both the severities and the safety objectives (in term of qualitative a quantitative).

The C0-2 is achieved by imposing safety objectives to the RPAS in isolation. These safety objectives are coherent with current draft regulation on UAV (JARUS and ER_010). This approach, to impose the safety objectives to one single stakeholder (the RPAS) allows that the safety argument can be justified by current regulation and practices.

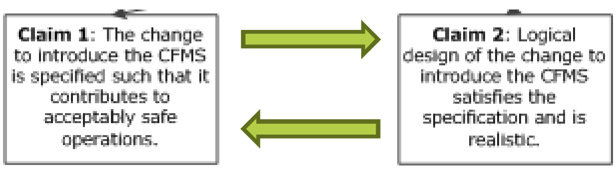
This Use Case has highlighted the necessity of improving the interface of current regulation with ATM and human performance See. Figure 6 and Figure 7

Claim 1 and Claim 2 interrelation

The D1.3 methodology presents five level highlevel claims. This Use Cases addresses only the two firsts claims

Claim 1 express that the change is specified in such way that it complains with the safety objective. Claim 1 does not consider how the AutoFailMS is actually implemented, thus there is no consideration of equipment of human roles (refer to 3.3). Claim 2 express that the logical design satisfies the specification defined in claim 1, claim 2 adresses the architecture of the AutoFailMS.

In the D1.3 methodology claim 1 and claim 2 are presented as independent claims, however note that the introduction of current standards (ARP4754A/ED79A) as means to support the claims, implies that the specification (claim 1) and the logical design (claim 2) are not independent, claim 1 and claim 2 are interrelated.



Claim 1.1.2 can be referred to claim 1.1.1

The analysis of the dependencies of the AutofailMS has shown that claim 1.1.2.2 is not applicable to AutoFailMS dependencies or it is referred to claim 1.1.2.1. This is because the AutoFailMS scope is to mitigate the failure conditions.

AutoFailMs is not expected to mitigate "external hazards" except those hazards related to the scope of the AutoFailMS (and covered in claim 1.1.2.1). Refer to 3.4.2.

The Claim 1.1.2.2 is either non applicable either considered as part of claim 1.1.2.1.Refer to 3.4.2

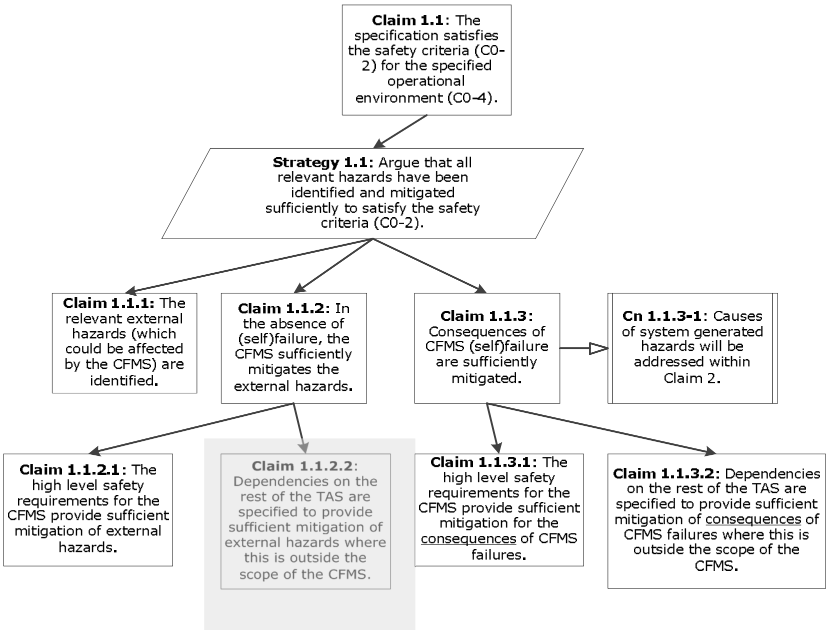


Figure 13 Update of certification argument

7 Conclusions

7.1 Conclusion Use of D1.3 on RPAS operations supported by AutoFailMS. First Approach

The application of D1.3 methodology to a system installed on an aircraft has identified some recommendations to D1.3.

Ident	Recommendation
Rec_01	D1.3 should propose that Context C0-2 can be expressed by a severity matrix at the level of the Total Aviation System level
Rec_02	D1.3 should set a task for TAS stakeholders agree on the safety objectives imposed for each severity at TAS level
Rec_03	D 1.3 should set a task for Context C0-2 to be completed by a guideline to cascade Safety Objective from TAS to stakeholder level
Rec_04	D1.3 should complete stage 1 by a guideline on production operational, and functional description of the change.
Rec_05	D1.3 should set up a clear activity for the stakeholder to agree on the safety terminology (hazards, safety objective, safety requirements, etc.)
Rec_06	D1.3 should set a task for the TAS stakeholders to agree on a guideline to identify hazards
Rec_07	D1.3 should set an activity for TAS to agree on the proper level of scenarios at TAS level, these scenarios need being updated as long as the design in being detailed.
Rec_08	D1.3 should set a task for the TAS stakeholder to agree on guideline to identify requirements from scenarios.
Rec_09	D1.3 should set a task for the TAS stakeholder to agree on guideline to share requirements from scenarios.
Rec_10	D1.3 should set a task for the stakeholder to agree on a guideline to allocate qualitative requirements to human errors.
Rec_11	D1.3 should define a process to produce lessons learned for future developments
Rec_12	D1.3 should improve the description of the certification argument to address changes at different levels.

Table 20 Conclusion. First approach

7.1.1 Rec_01: D1.3 should propose that Context C0-2 can be expressed by a severity matrix at the level of the Total Aviation System level

Rec_01. D1.3 should propose that Context C0-2 can be expressed by a severity matrix at the level of the Total Aviation System level.

In a Total Aviation System, the safety is no longer understood as a performance achieved in isolation by each stakeholder, the safety has become into an overall objective. Therefore, the level of safety needs to be defined at inter-stakeholders level and cascaded to each stakeholder (see chapter 6 WP 3.5 [19]).

This Use Case proposes to define the "acceptable safety level" by a severity matrix. This is coherent with current regulation for ATM and aircraft domain. The severity matrix needs to consider the safety impact of the change in all aviation domains.

- The severity allocated to each hazard is the worst of all severities identified for each of the domains.
- If current standards are used to support claim 2, then, the severity matrix at the level of the TAS needs to be aligned with current regulation.

7.1.2 Rec_02: D1.3 should set a task for TAS stakeholders agree on the safety objectives imposed for each severity at TAS

Rec_02 D1.3 should set a task for TAS stakeholders agree on the safety objectives imposed for each severity at TAS level

The severity associated to each hazard implies a safety objective. See for example the Table *21*. TAS stakeholders (see task WP 3.5) needs to agree about the safety objective accepted to each hazard. (see chapter 6 WP 3.5 [19]).

Severity	Probability
CAT	Extremely improbable
HAZ	Extremely remote
MAJ	Remote
MIN	Probable

Table 21 Safety objectives TAS level

7.1.3 Rec_03: D1.3 should set a task for Context C0-2 to be completed by a guideline to cascade Safety Objective from TAS to stakeholder level

Rec_03: D1.3 should set a task for Context C0-2 to be completed by a guideline to cascade Safety Objective from TAS to stakeholder level

The agreed safety objectives at the TAS level needs to be met by the aviation stakeholders as a whole. The stakeholder needs to agree (task WP 3.5) in a methodology to share the safety objectives.

- In the case that several stakeholder supports the same safety objective the D1.3 methodology should impose a common mode analysis, in order to ensure the independency of the design of each stakeholder level and at interstakeholder level (e.g. to refine the chapter 2.2.3 in D1.3)
- In the case that stakeholder share a same safety objective the stakeholders design need to be developed under similar levels of quality.

7.1.4 Rec_04 D1.3 should complete stage 1 by a guideline on production operational, and functional description of the change..

Rec_04 D1.3 should complete stage 1 by a guideline on production operational, and functional description of the change.

Stage 1 should be completed with guidelines that enable to each stakeholder to present a complete and correct list of operations, services and function impacted by the change. The operations are achieved by means of functions and services.

Stage 1 should propose the list of scenarios (normal, abnormal and failure) according to the complete list of operation, services and function impacted by the change .

The complete list of operations, services and function should include a clear traceability of stakeholders involved in them. If an operation, service and functions is performed by several stakeholders (e.g datalink) the D1.3 should allow capture the contribution of each stakeholder to the overall objective of the scenario associated to that operation, service and function.

7.1.5 Rec_05 D1.3 should propose TAS stakeholder needs to agree about terminology.

Rec_05 D1.3 should set up a clear activity for the stakeholder to agree on the safety terminology (hazards, safety objective, safety requirements, etc.)

As stated in 3.4.1, this Use Case has identified that the definition of hazards might be different on the aviation domains and other stakeholder domains. D1.3 should set up an activity for the TAS to agree on the terminology.

This is as well the case of the abnormal scenarios, as stated in 3.2.1.1.3 the definition of an abnormal scenario might be not the same for all stakeholders. The definition of the operational concept should clearly identify what a normal and abnormal scenario is (Rec_04). If current standards are used to support claim 2, the definition of normal and abnormal should be traceable with current standards (see Rec_05).

If claim 2 is supported by current standards, then, the agreed terminology at the TAS level need to be coherent with the terminology used in the standards.

7.1.6 Rec_06 D1.3 should set a task for the TAS stakeholder to agree on a guideline to identify hazards.

Rec_06 D1.3 should set a task for the TAS stakeholders to agree on a guideline to identify hazards

The guideline D1.3 should be completed by a guidelines to define hazards. The hazards need to be referenced to the Operational concept defined in stage1. The TAS stakeholder needs to agree in the guidelines about identifying hazards. (see chapter 6 WP 3.5 [19]).

If claim 2 is supported by current standards, then the guidelines defined for identifying hazards needs to be coherent with those standards.

A complete and correct list of hazards depends on a complete and correct operation concept in stage 1 (rec-4), an agreed definition of hazards (see rec-5) and guidelines to identify hazard tailored to that hazard definition.

7.1.7 Rec_07 D1.3 should define the level of the scenarios

Rec_07 D1.3 should set an activity for TAS to agree on the proper level of scenarios at TAS level, these scenarios need being updated as long as the design in being detailed.

As stated in 3.2.1.1.2 this Use Case has identified that the required level of the scenarios might differ depending on the stakeholders. In the case that the aircraft used the ARP4754A/ED79A the level of the scenario will probably lower than required by an ATM partners (note that ARP 4754A/ED79A imposes requirements to design).

It is recommended that the level of the scenarios was agreed by TAS according to stage 1, but updated as long as the standards are applied.

Scenarios description should be considered as an iterative activity until the total application of the D1.3 methodology.

7.1.8 Rec_08 D1.3 should set a task for the stakeholder to agree on a guideline to identify requirements

Rec_08 D1.3 should set a task for the TAS stakeholder to agree on guideline to identify requirements from scenarios.

The D1.3 should be completed by guidelines to define requirements. The requirements need to be referenced to the Hazards. (see chapter 6 WP 3.5 [19]).

If claim 2 is supported by current standards, then the guidelines defined for identifying requirements needs to be coherent with those standards.

7.1.9 Rec_09 D1.3 should set a task for the stakeholder to agree on a guideline to share requirements

Rec_09 D1.3 should set a task for the TAS stakeholder to agree on guideline to share requirements from scenarios.

When a safety objective is supported by several stakeholders, the safety requirements need to be share by stakeholders as well. D1.3 should set a task for the stakeholder share requirements. (see chapter 6 WP 3.5 [19]).

If current standards are used to support claim 2, the requirements in interface (req imposed from one stakeholder to other) need to be coherent with the standards of the stakeholders in interface.

As an example see how ATM requirements (performance and safety) can be allocated over aircraft. Figure 8 and Figure 9) and how the aircraft might impose requirements to the ATM.

7.1.10 Rec_10 D1.3 should set a task for the stakeholder to agree on a guideline to allocate requirements to humans

It has been noted that there is a gap in current regulation regarding the human in the system. The D1.3 should define a task for stakeholder to agree a common guideline to create requirements on the human (remote pilot, controller).

7.1.11 Rec_11 D1.3 should define a process to produce lessons learned for future developments

The methodology proposed does not define any process to improve the claim structure D1.3 should define. a feedback loop to improve the claim argument using a continuous improvement process from lessons learned from operation. (see chapter 6 WP 3.5 [19])

7.1.12 Rec_12: D1.3 should improve the description of the certification argument at different levels.

The methodology D1.3 has not fully addressed the safety issues of the implementation of an AutoFailMs in the TAS. In part, this is because the introduction of AutoFailMS is only part of the change (which is to introduce an RPAS). As stated in 3.2.1.1.2 the level of the change (change in one single stakeholder) has driven a too low level of scenarios to support claim2. The methodology D1.3 might not be necessary for a change restricted to one single stakeholder; the critical question to answer is whether the impact of the change extends beyond a single domain on the TAS. If the D1.3 methodology is used to address low level changes for a single stakeholder, then D 1.3 should provide a clear traceability between stage 7 and stage 9 and higher stages.

Note that a big change (RPAS operations) might be enabled by lower level changes (AutoFailMs implementation), the certification plan at a high level (e.g certification argument for TAS) can be supported by certification plans at smaller level (AutoFail Ms compliance with ARP 4754/ED-79).

7.2 Conclusion. D1.3 used to develop ED-78A.Second Approach

As presented in 1.2 the approach D 1.3 [1] is applied by a stakeholder group10 to gather specifications and supporting material. This may involve developing new specifications where functions and / or interfaces are not covered in existing specifications The application of the D1.3 to the RPAS operations has pointed out that connection between ATM and aircraft standards needs to be reinforced. (refer to 3.5.2 and 3.5.3).

In this subchapter, the D1.3 is used as a guide to develop the ED-78A, (currently restricted to data link application) to apply to any kind of change in the TAS.

The D1.3 presents the main ideas to develop a logical argument that can be applied to address to operation, processes and services in the TAS. On the contrary, the ED-78A is focused in a much more restricted scope, ED-78A presents a guideline to establish operational, safety, performance, and interoperability requirements on data link applications"[17]. However, the ED-78A presents a methodology to share safety and performance requirement among several stakeholders and it has been already used to develop regulations, for example FANS application in ED-120 and ED122 based on ED-78A.

In the first subchapter, we compare the stages proposed by D1.3 with the steps proposed by ED-78A. The objective is to analyze if the overall structure of ED -78A would allow it to be updated to cover as well operation, processes and services. This comparison is performed at high level. Refer to 7.2.1

The application of D1.3 to the RPAS operation supported by the AutoFailMS has produced a certain quantity of recommendations (refer to 7.1). Mainly the recommendations addresses the fact that the introduction of standards in the certification argument structure induce some issues (REC_01, Rec_02, REC_05, REC_06) and the necessity of D1.3 to detail inter stakeholders activates (REC_03, Rec_04 rec_07, rec_08 and rec_09) Some of these recommendation can be as well applicable to ED-78A. The second subchapter analysis on one hand, how the ED-78A interface with the current standards and secondly how the ED-78A manages safety activities inter-stakeholder.

7.2.1 High level comparison between ED-78A and D1.3

The Table *22* shows the main activities of D1.3 and establishes a parallelism with main section in ED-78A.

[10] Stakeholder group: to be understood as a group of industrial and operational partners developing RPAS products and operations (aircraft manufacturers, RPAS operators, ANSPs, maintenance and training organizations, etc)

Aspects covered in D1.3[1]	Link with covered in ED-78A[17]	Comparison D1.3 vs. ED-78A
Stage 1: Description of the change This step is focused in describing the changes and the main impact in safety, as well as the applicable regulation This steps identifies as well involved stakeholders and its role in the change . [1]	The description of the change is mainly addressed in the OSED (The evidence for coordinated requirements determination is a description of operational services and their intended operating environments in an operational services and environment description (OSED). The ED-78A proposes a process to capture elements related to all stakeholders, this process is called OSEIC. The impact on the applicable regulation is addresses in section "for approval planning"	The OSED description of ED-78A supported by the guideline OSEIC matches the step 1 "description of the change". The guideline proposed to develop the OSED (OSEIC) is tailored to datalink applications. At high level, the ED_78A addresses the activities proposed on stage 1 of D1.3 Stage 1 identifies as well applicable regulation. Refer to Stage 3 of this table.
Stage 2 :Certification argument This stage is focused on developing the initial certification argument which will be made for the change. At this stage the argument should identify any potential impact either on or from existing assurance contracts or modules outside the initial scope of the change. […]The architecture will follow existing established certification approaches where these remain appropriate while ensuring that any consequences of using this approach are fully understood and managed [1]	The ED-78A does no present a certification argument per se. Ed-78A establishes a process to follow that covers from the design to operations and that is addressed to several stakeholders. The assurance contracts are managed by allocation of safety objectives and requirements to partners (OSEIC, OSA, OPA, IA activities.) and by ensuring that the requirements responds to the certification. The assurance contracts are updated when required.	At a high level comparison, the ED-78A presents an argument which is comparable to the argument structure of D1.3 presented in §3.4.1 3 "Change between performance-based and compliance-based or vice versa" The ED-78A covers both performance and safety requirements together and it cannot be considered as a "pure-compliance based approach" Rec_ED_78_A.1: ED_78A should clearly expose the interfaces among stakeholders and the allocation of safety requirements
Stage 3 Develop and agree certification plan The role of the certification plan is to show	Stage 3 of D1.3 is similar to Section 3 of ED-78A. "Approval planning" The evidence for approval planning is the approval plan and the acceptance of the plan by the	ED-78A bases the approval planning on the existing regulation, in case that there is not regulation, the ED-78A suggests that: "*In cases where there is no regulatory*

Aspects covered in D1.3[1]	Link with covered in ED-78A[17]	Comparison D1.3 vs. ED-78A
how the certification argument architecture will be developed and substantiated with evidence to the point where it can be presented for acceptance by the relevant authorities[1]	approval authority [17]	*basis for a particular element of the CNS/ATM system, the regulatory requirements refer to those requirements established by the stakeholder responsible for development and qualification of the element*." [17] The ED-78A does not foresee any procedure to develop in common regulatory requirements at the level of the TAS when missing. This is coherent with the scope of the ED-78A. Rec_ED_78_A.2: ED_78A should define an activity to stakeholders develop new specifications where functions and / or interfaces are not covered in existing specifications.
Stage 4 Specification This stage is focused on demonstrating that […] the change is specified to achieve an acceptable level of safety. [1] Safety assessment in this stage is used to identify the pre-existing hazards relevant to the system and assesses the consequences of these hazards on the safety of the TAS. [1] **Stage 5:Design** This stage is focused on demonstrating […] that the logical design for the change satisfies the specification derived within Claim 1 of stage 2.	ED-78A includes the process of identification of safety objectives and requirements in the section 4 called "coordinated requirements demonstration". This section establishes requirements that require coordination among organizations involved in the development, qualification, operation, and approval of the CNS/ATM system. It consists of the OSEIC (refer to stage 1 of this table) , OSA, OPA, and the IA. [17] The OSA, OPA, and IA identify, coordinate, allocate, and validate the operational, safety, performance and	The Ed-78A is focused on datalink communication, the objective of the datalink is to support communication and not to mitigate a pre-existing hazards. (see 3.4.1) consequently, stage 4 is not applicable directly in ED-78A. Stage 4 can be comparable however to the OPA "The OPA provides methods to derive or validate required communication performance type (RCP type) from the OSED, based on the RCP concept." Note as well that ED-78A addresses the performance and the safety requirement as part of the same process similarly to ARP 4754A/ED79A (refer to Figure 6). The

Aspects covered in D1.3[1]	Link with covered in ED-78A[17]	Comparison D1.3 vs. ED-78A
This stage identifies hazards resulting from failures of the system and produces a set of Design Safety Requirements (DSRs) which define what each element of the design has to do, in terms of functionality and performance, in order to mitigate these hazards[1]	interoperability requirements, and update the OSED, as necessary. The operational, safety, and performance requirements provide the operational basis for the operational implementation and are captured in the SPR standard. [17] The interoperability requirements provide the technological and functional basis for the operational implementation and are captured in the INTEROP standard. The requirements in the standards are allocated to each of the stakeholders in control of or responsible for an element of the CNS/ATM system[17] The section 4 of the ED_78A covers the stage 4, 5 and 7 for the datalink application.	ED-78A considers that the implementation of the change might impact on the OSA, OPA and IA, this is line with Figure 7
Stage 7 Implementation This stage is focused on demonstrating [...] that the physical implementation of the logical design for the change is complete and correct. The principle aim of safety assessment at this stage is to demonstrate by a combination of analysis and testing, that the (as-built) system meets the safety requirements . [1]		
Stage 6 Refinement of Argument Following the detailed assessment undertaken in stage 4 and stage 5 the detail of the safety argument is updated to correspond to the safety requirements derived and the more detailed understanding of the system architecture which has been developed. [1]	The Ed-78A considers updating the requirements and the interface among stakeholders.	Refer to comments on stage 2 of this table
Stage 8 Transfer into operation assessment	ED-78A addresses as the" bullet a" of stage 8 D1.3 in section 6 "entry into service". Section 6:	The Ed-78A does not clearly addresses the impact of the introduction of datalink applications

Aspects covered in D1.3[1]	**Link with covered in ED-78A**[17]	**Comparison D1.3 vs. ED-78A**
This stage is focused on demonstrating […]that the transition to introduce the change is acceptably safe. This consists: a) the fully proven change is ready to be brought into operational use b) that the introduction of the change can be achieved without affecting the overall safety of the system while the change is being introduced. [1]	• Accepts the development and qualification data produced by the stakeholders • Ensures that the elements of the CNS/ATM system have been implemented in accordance with approved plans. ED-78A addresses bullet b as a part of Section 5.1.1.j: Transition criteria are defined, including procedures, airspace requirements, and NOTAM;	Rec_ED_78_A.3: The ED78A should address the transition to introduce the change
Stage 9 Define arrangements for continuous safety monitoring This stage is focused on demonstrating that 5 […] that arrangements are in place to ensure that the change is demonstrated to be acceptably safe in operational service. . [1]	Stage 9 is addressed on section 7 “operations”. Section 7 provides objectives and guidance on evidence required for operations. The operations process ensures that system operations continue to satisfy operational, safety, performance, and interoperability requirements while in service. For each applicant, this process consists of continued operations, including system monitoring and iterative operational safety, performance, and interoperability assessments as internal or external changes are made for adjustments and problem resolution; and the development and qualification of follow-on modifications.	ED_78A addresses the continuous safety monitoring similar to D1.3
Stage 10: Obtain initial operational certification At this stage, the evidence generated in earlier	Compliance with ED-78A can be shown by a compliance matrix	Not relevant

Aspects covered in D1.3[1]	Link with covered in ED-78A[17]	Comparison D1.3 vs. ED-78A
stages is presented by the applicant to the relevant authorities in order to obtain permission to introduce the change into service.		
Stage 11: Ongoing monitoring and maintenance of certification Following introduction into service, the monitoring arrangements defined in stage 9 must be implemented. The certification argument must be updated at regular intervals to confirm that the changed system continues to achieve the relevant requirements. The intervals for update and recertification should be specified by the certifying authority	ED-78A consider the update of regulation basis as part of section 3 "approval planning" Schedule. The schedule for operational implementation is identified and indicates the interaction between the applicant and the approval authority, including milestones for reviews, evaluations, and data submittals.	Rec_ED_78_A.4 ED_78A section 3 "approval planning" should clearly be addressed to all stakeholders.

Table 22 High level comparison between ED-78A and D1.3

As a conclusion ED-78A steps are totally covered in D1.3, the delta found between the ED_78A and D1.3 are mainly due to fact that ED_78A scope is restricted to datalink operations. It has been found four recommendations for ED_78A.

Ident	recommendation
Rec_ED_78_A.1	ED_78A should clearly expose the interfaces among stakeholders and the allocation of safety requirements
Rec_ED_78_A.2	ED_78A should define an activity to stakeholders to develop new standards where functions and / or interfaces are not covered in existing standards. This new standards will be proposed to the Authorities for agreement.
Rec_ED_78_A.3	ED_78A should address the transition to introduce the change
Rec_ED_78_A.4	ED_78A section 3 “approval planning” should clearly be addressed to all stakeholders.

Table 23 Recommendation ED_78A

7.2.2 Comparison between recommendation of WP 4.1 to D1.3 and ED-78A guidelines

The D1.3 is a high-level methodology that needs being refined; the process of applying the D1.3 to the introduction of an RPAS in a non-segregated airspace has generated number of recommendation. In this subchapter we analyze if that recommendation are as well applicable to the ED_78A.

Rec_01 Context **C0-2 can be expressed by a severity matrix at the level of the Total Aviation System level**

The level of safety need to be agreed among stakeholder, the ED_78A has proposed a severity matrix/

Hazard Class	**1 (most severe)**	**2**	**3**	**4**	**5 (least severe)**
Effect on Operations	Normally with hull loss. Total loss of flight control, mid-air collision, flight into terrain or high speed surface movement collision.	Large reduction in safety margins or aircraft functional capabilities.	Significant reduction in safety margins or aircraft functional capabilities.	Slight reduction in safety margins or aircraft functional capabilities.	No effect on operational capabilities or safety
Effect on Occupants	Multiple fatalities.	Serious or fatal injury to a small number of passengers or cabin crew.	Physical distress, possibly including injuries.	Physical discomfort.	Inconvenience.
Effect on Air crew	Fatalities or incapacitation.	Physical distress or excessive workload impairs ability to perform tasks.	Physical discomfort, possibly including injuries or significant increase in workload.	Slight increase in workload.	No effect on flight crew.
Effect on Air Traffic Service	Total loss of separation.	Large reduction in separation or a total loss of air traffic control for a significant period of time.	Significant reduction in separation or significant reduction in air traffic control capability.	Slight reduction in separation or slight reduction in air traffic control capability. Significant increase in air traffic controller workload.	Slight increase in air traffic controller workload.

Table 24 Qualitative Safety impacts Eurocae ED78A

<u>Rec_02 D1.3 should set a task for TAS stakeholders agree on the safety objectives imposed for each severity at TAS level</u>

The ED_78A has addressed this issue by proposing the following table. This table should be reviewed to assure coherency with a similar table used for aircraft stakeholder:

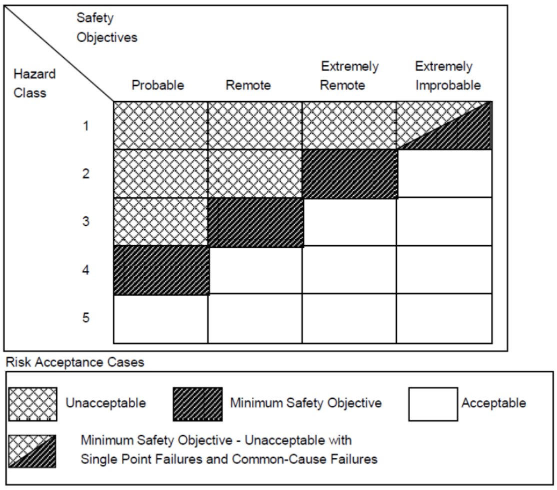


Table 25 Hazard classification and safety objectives relationship

<u>Rec_03: D1.3 should set a task for Context C0-2 to be completed by a guideline to cascade Safety Objective from TAS to stakeholder level</u>

In the Use Case WP 4.1, the safety objectives have allocated to the aircraft (as ATM is seen as a safety net) however, in the case that the safety objective was shared by different stakeholder, it would be necessary to decide how the safety objectives are supported by the stakeholder acting as a whole. The Use Case WP 4.1 proposed that to cascade safety objective it is necessary first to ensure the independency of the systems among stakeholders, and that the quality level need to be coherent among stakeholder. See discussion in 5.2.2

ED_78A establishes a process ASOR that allocates safety objectives among stakeholders. This process consider the common failures and review the implementation of system. The safety qualitative objective are covered.

The ED_78A, does not consider the qualitative safety objective and it does not address the concept of quality (e.g. DAL).

Rec_03 is partially applicable to ED_78A

Rec_04 D1.3 should complete stage 1 by a guideline on production operational, and functional description of the change.

The ED_78A presents an OSED and a guideline OSEIC. A close reading of the ED_78A OSEIC process makes it clear that the OSEIC is focused on datalink application, it would be necessary to update this process to cover all type of operations and services.

Rec_04 is applicable to ED_78A

Rec_05 D1.3 should set up a clear activity for the stakeholder to agree on the safety terminology (hazards, safety objective, safety requirements, etc)

The Use Case WP 4.1 that there is a difference between the meaning of certain safety terms (refer to 3.4.1) The ED_78A propose definition but it does not explain how to manage the potential divergences among stakeholders.

Rec_05 is applicable to ED_78A

Rec_06 D1.3 should set a task for the TAS stakeholders to agree on a guideline to identify hazards

The hazard identification in ED_78A is briefly described "*The operational hazards are identified as the loss or malfunction of the service, including misleading or delayed information [17]*". This description is not detailed enough. ED878A should describe a clear methodology to identify hazards from the OSED.

Rec 06 is applicable to ED_78A

Rec_07 D1.3 should set an activity for TAS to agree on the proper level of scenarios at TAS level, these scenarios need being updated as long as the design in being detailed

The Use Case WP 4.1 has found out that the proper level of the scenario highly depends on the safety methodology that the stakeholder uses. Given the fact that the D1.3 is expected to be supported by current standards when possible, the definition of the proposer level of scenarios requires stakeholder agreement.

The ED_78A does not address this issue. Note that ED_78A is only focused on the datalink applications.

Rec_07 is applicable to ED_78A

Rec_08 D1.3 should set a task for the TAS stakeholder to agree on guideline to identify requirements from scenarios

The identification of safety requirements are performed in ED_78A in terms of safety and in terms of performance. ED_78A addresses as well the requirement of interoperatibility. However there is not nay guideline that explains how to define these requirements. Rec_08 is applicable to ED_78A

Rec_09 D1.3 should set a task for the TAS stakeholder to agree on guideline to share requirements from scenarios

ED_78A establish a process to define requirements in interface. ED_78A presents a guideline INTEROPS applicable to datalink. This guideline need to be enlarged to cover all type of the operation, processes and services and to consider. Rec_09 is applicable to ED_78A

Rec_10 D1.3 should set a task for the stakeholder to agree on a guideline to allocate requirements to humans

ED_78A does not establish clear principles on humans. Rec_10 is applicable to ED_78A

Rec_11 D1.3 should define a process to produce lessons learned for future developments

ED_78A established does not include process to clearly modify the standards. A process o fstandards improvement s(lesson learned)should be developed. Rec_11 is applicable to ED_78A

Rec_12: D1.3 should improve the description of the certification argument to address changes in one single stakeholder.

ED_78A established a clear traceability between changes to a low level (e.g equipment) and high level safety objectives. Rec_12 is not applicable to ED_78A

7.3 Final conclusion

This Use Case presented two approaches., for each one of them the main conclusion are:

- First approach: the approach proposed in ASCOS by D1.3 is applied by applicants to demonstrate that all the requirements are met.

In general terms, it has been found out that the claim structure proposed originally does not necessarily match the standards. However it is possible to tailor D1.3 in order to adapt it. This process of tailoring and refinement is described in 7.1

- Second approach the approach is applied by a stakeholder group to gather specifications and develop standards which define the requirements for the change

The methodology D1.3 can also being used to develop current standards. It has been found out that the ARP4754A/ED79A could be improved by the introduction of the ATM interface and that the human quality (Human DAL) need to be developed. This methodology D1.3 has also been used to perform a high level revision of a potential adaptation of ED_78A to general operations. It has been found out that the D1.3 methodology could suggests improvements to the ED_78A. Refer to 7.2

References

#	Authors(s), Title, Year
[1]	ASCOS D1.3:Outline proposed certification approach, A. Simpson, S. Bull, T. Longhurst, v1.2, 18-12-2013.
[2]	List of Areas of Change, In: Ongoing and Future Phenomena and Hazards Affecting Aviation compiled by Brian Smith, NASA Ames Research Center November 15, 2013,http://www.nlr-atsi.nl/fast/FAST_AoCs_20131115.pdf
[3]	EU 1178/2011
[4]	EC 2096/2005
[5]	Annex to ED Decision 2011/016/R
[6]	EASA CS-25 Amendment 14 (19 December 2013)
[7]	EASA Unmanned Aircraft Systems (UAS) E.Y013-01 25/08/2009
[8]	JARUS: Guidance on RPAS C2 link Required Communication Performance (C2 link RCP) (Issue 21 Nov 2013)
[9]	JARUS: SCOPING PAPER to AMC RPAS.1309, Remotely Piloted Aircraft Systems Systems Safety Assessment Issue 1 – January 2014
[10]	ICAO Unmanned Aircraft Systems (UAS) Cir 328 AN/190
[11]	CAP 393 (12th May 2014)
[12]	CANSO publication “ANSP Considerations for RPAS Operations”, 2014
[13]	ED-79A / SAE ARP 4754A GUIDELINES FOR DEVELOPMENT OF CIVIL AIRCRAFT AND SYSTEMS, December 2010
[16]	EUROCAE UAS/RPAS AIRWORTHINESS CERTIFICATION “1309” System Safety Objectives and Assessment Criteria, ER-010, July 2013.
[17]	ED-78A: GUIDELINES FOR APPROVAL OF THE PROVISION AND USE OF AIR TRAFFIC SERVICES SUPPORTED BY DATA COMMUNICATIONS, December 2000
[18]	ASCOS. WP 3.2 Risk models and accident scenarios
[19]	ASCOS WP 3.5 Total Aviation System Safety Standards

Table 26 References

Appendix A Modified functions. RPAS vs. manned aircraft

The following table details additions and/or modifications of the RPAS in comparison to the manned aircraft systems

RPAS high level function	Sub functions description	Additions and/or modifications of the RPAS in comparison to the manned aircraft systems
1. Accommodate payload	It includes the proper accommodation of cargo in terms of ventilation, temperature, pressure, humidity	A priori no modification is expected. In case of failure the current detection and actuation means (sensors, valves) are installed.
2. Fly		
2.1 Aircraft configuration	It considers aircraft configuration controls (control drag, control lift, LGERS extension…) required to adapt aircraft shape/performance to the required flight phase.	Aircraft configuration needs to be automated. Some sub-functions require design modifications. **Gear Extension / Retraction** In case of failed gear extension, the pilot can recycle the maneuver, extend in emergency mode (gravity extension) and confirm actual position of the gears with help of TWR ATCo. For these reasons specific sensors and procedures have to be considered for RPAS. **Slats /flaps configuration** In case of dissymmetric slat or flap configuration the detection by the pilot of aircraft abnormal behavior and his recovery action are immediate. For these reasons a specific multi-sensors detection function has to be considered for RPAS.

RPAS high level function	Sub functions description	Additions and/or modifications of the RPAS in comparison to the manned aircraft systems
2.2 Speed control	On ground. It includes retardation means on ground (spoilers, reverses) and parking brakes	**Deceleration on landing** Auto brake function remains the only means to control speed on ground with the brakes during rollout. Spoilers and/or reverses extension need to be automated. Acceleration/deceleration sensed by the pilot is considered as detection means. Specific sensors need to be implemented on RPAS. **Wheel rotation** During taxi phase on ground the pilot detects abnormal rolling behavior due to erroneous wheel rotation (i.e.: wheel blocked). Automatic monitoring of speed and steering on ground needs to be implemented.
	At take-off	**Decision speed.** Aircraft behavior –acceleration rate, aircraft performance, and noises- are directly sensed by the pilot and contribute to his decision at V1. As the remote pilot will not be in position to monitor and react effectively, some alternative to the decision speed needs to be implemented for automatic take-off. The physical sensation associated to the loss of acceleration/deceleration is considered as detection means. Specific sensors need to be implemented on RPAS.
	In flight	RPAS adapts speed in flight to trajectory and aircraft characteristics. Trajectory is owned by the remote pilot who knows which are the limits of the aircraft for the current weight and balance conditions. The remote pilot needs to agree on trajectory or speed modifications requested by the ATCo. The physical sensation by the pilot of the aircraft behavior in reaction to controls on attitude or acceleration/deceleration is considered as detection means. Specific sensors need to be implemented on the RPAS (e.g.: flutter, buffeting).
2.3 Attitude Control	On ground (lateral control)	Lateral control on ground by means of surfaces control (in high speed) and steering (in low speed) needs to be automated.

RPAS high level function	Sub functions description	Additions and/or modifications of the RPAS in comparison to the manned aircraft systems
	In flight (lateral and vertical control)	Lateral and vertical control in flight is achieved by surfaces control. Depending of the number and role of failed control surfaces (e.g.: jamming) different control laws are implemented in the flight control system, some of them requiring pilot in the loop. Alternative automated control laws would have to be implemented on RPAS in order to maintain minimum flight control for landing on a diversion airfield or for crash landing. In addition, the RPAS flight control laws would implement an automatic de-crabbing function for flare phase.
3. Guidance and navigation		
3.1 Provide navigation and control data.	This function implies the collecting and treatment of the data required for navigation purposes (position data, heading data, time references data)	No modification in the function. Loss or erroneous behavior of main navigation functions will have the same consequences as for a manned aircraft. If the navigation of RPAS has to be reverted in dead reckoning, guidance of the RPAS towards a diversion airfield or a crash landing site might request the help of the ATC resources, as for manned traffic.
3.2 Management of flight plan	On ground (pre departure)	No modification. Remote pilot performs the same functions as with a manned aircraft.
	In flight	The flight plan is managed by the remote pilot In the same way as today. The instructions or clearances are received from the controller by datalink or voice (RT). Trajectory is owned by the remote pilot who knows which are the limits of the aircraft for the current fuel, weight and balance conditions. The remote pilot needs to agree on trajectory or speed modifications requested by the ATC. Then the aircraft updates the trajectory and the remote pilot informs the ATC. Handling of ATCo instructions of immediate execution (e.g.: Go Around) may require specific arrangement between ATC and RPAS operational organizations.
3.3 Support flight optimization		No modification, aircraft made prediction about fuel computation, arrival time … as per today.

RPAS high level function	Sub functions description	Additions and/or modifications of the RPAS in comparison to the manned aircraft systems
3.4 Guidance	on ground	The primary means to control aircraft on ground is the pilot view. Pilot guides the aircraft following the instructions of the ATC. In order to deal with any unpredictable obstacle that may interfere with aircraft trajectory on ground, the RPAS pilot needs to have the same view (i.e.: video transmission)
	at T/O or Go-Around	Trajectory of RPAS during the take-off and in case of go-around needs to be automated. It encompasses situations of OEI, HERTO or balked landing.
	on cruise	Guidance in cruise will be fully autonomous. Back-up by the remote pilot may be limited, in particular over remote/oceanic areas where the C2 link capability could be reduced or delayed.
	for approach and landing	RPAS needs to be able to land automatically. The remote pilot will have direct control of the RPAS for the landing clearance or go-around instruction. This may require specific arrangement between ATC and RPAS operational organizations. Some ILS type guidance means at the destination airfield may be required to be permanently available with a zero-zero landing capability (i.e.: an ATOLS- level capability or equivalent system of CAT III performance)
4. Provision of resources	Provision of fuel and Power (electric, hydraulic, propulsive, pneumatic, thermal)	No modification of systems envisaged for the RPAS in case of failure of propulsion, hydraulic or pneumatic systems. The electric system in manned aircraft has a panel of circuit-breakers accessible to pilots, which constitute a specific "HMI" used by pilots in a variety of abnormal procedures and contingency situations (e.g.: fire, reset). An automatic management of the electrical distribution / protection function will have to be implemented for RPAS.
5. Human machine interface		
5.1 Information to remote pilot (downlink)	Information	The remote pilot will have all the information usually displayed in the manned cockpit. However, all abnormal procedures in case of failure an aircraft system shall be automated, as latency of communications could prevent the remote pilot to react efficiently in most of the cases. Though, the information displayed "for information" on the remote pilot position is more comprehensive than in a piloted aircraft and allows a more efficient monitoring of aircraft system status, better prognosis in case of failure and improved decision making for recovery.

RPAS high level function	Sub functions description	Additions and/or modifications of the RPAS in comparison to the manned aircraft systems
5.2 Downlink / status. Telemetry	Warning/Cautions	The RPAS implements an automated decision making process in case of warnings or cautions, able to execute the related abnormal procedures. In case of failure of the communication with the pilot station, the RPAS will initiate an alternative communication link with a backup pilot station through an available sub-network on reach. The other pilot will take over the aircraft control (backup remote station).
5.3 Uplink-command. Telecommand		The remote pilot shall have capability to take full control of the RPAS. However, this capability may be limited to situations where the performance of the C2 link is sufficient for the continuity and integrity of the function. This could be required for departure or arrival phases and overflying of crowded areas. In case of failure of the remote station or sub-network during these phases, a handover might be automatically initiated by the RPAS to connect to a backup remote station through an alternative sub-network.
5.4 Provide communication with ATC		When ATC communication (RT or datalink) is relayed through the C2 link, the latter shall have at minimum the same level of performance of continuity and integrity and shall maintain the overall latency of transactions within the prescribed limits. In situations when this might not be practically achievable (e.g.: remote / oceanic areas) some specific arrangement for direct communication could take place between ATC and RPAS operational organizations. The remote pilot is provided with a continuous indication of the link signal quality (strength, range limit, masking, etc.). Planning of the available network and links to be used during the different phases of is part of the flight preparation. RPAS shall be able to monitor autonomously that the communication between the remote pilot and the ATCo is active. In case of loss of communication with the ATC, the aircraft shall inform either the pilot or the ATCo of the situation (i.e.: squawk code 7600). When the remote pilot is informed that the uplink is lost, he may contact directly the ATC. This may require specific arrangement between ATC and RPAS operational organizations. In the meantime the aircraft follows the planned trajectory.

RPAS high level function	Sub functions description	Additions and/or modifications of the RPAS in comparison to the manned aircraft systems
6. Support maintenance	This function includes the recording of RPAS status / events and failures.	The information transmitted the remote control position is more comprehensive than in a piloted aircraft and encompasses all aircraft systems. It allows a more efficient monitoring of aircraft systems status, better prognosis in case of failure and improved decision making for maintenance. In any case, a flight recorder function might be required on board the aircraft in case of incident or accident in circumstances of loss of the C2 link.
7. Ensure safety/security of operations		
7.1 Protection against environment	Protection against hail, ice accretion	On manned aircraft a visual indication of icing condition is provided to the pilot. Specific sensors and procedures would be implemented in RPAS for situations of potential ice accretion in case of undetected failure of the anti-ice system.
	Weather conditions, storms, strong turbulences, wake vortices	The remote pilot should be provided with accurate, real time map of significant thunderstorms along the planned trajectory, in order to avoid excessive turbulences to the RPAS. This information might be greatly improved by airborne dedicated sensors of the weather conditions around and in front of the RPAS (e.g.: lidar)
	wind shear	A predictive windshear protection system might be necessary in order to reproduce the reaction of a skilled pilot, based on dedicated sensors (e.g.: lidar)
	Electromagnetic protection, HIRF, lightning	RPAS might need to be more robust against HIRF, due to potential negative impact on the continuity of the C2 link communication
	Bird strikes	Specific shielding of RPAS nose should be designed.
7.2 Protection against external event	anti-collision protection, in flight	EGPWS and TCAS coupled to autopilot shall be envisaged. The “see and avoid” duty performed by the pilot shall be replaced on the RPAS by a “detect and avoid” function based on specific sensors having capability to detect small, non-cooperative traffic (e.g.: gliders, VLAs), in particular when flying in class B or C airspaces. This may be extended as well to “see and recognize” capabilities if autonomous taxiing capacity is sought for. For example recognize and understand aerodrome signs, markings and lighting (as per ICAO circular 328). However the remote pilot will still be involved in complying with the ground controller instructions and execute the taxi clearance.

RPAS high level function	Sub functions description	Additions and/or modifications of the RPAS in comparison to the manned aircraft systems
	anti-collision protection, on ground	Due to the diversity of potential obstacles on ground, most of them unpredictable, the primary means for collision prevention on ground would be video and remote control, or direct visual control by the pilot
	Corruption of data	The C2 link communication needs to be highly robust against data corruption. However, protective devices or features shall not degrade significantly the expected performance of the C2 link for continuity. Scenarios of unlawful interference should be considered too.
7.3 Protection against intrinsic events	Protection against fire/overheat smoke	In case of smoke / overheat / fire early detection is essential. In manned aircraft, the crew is often the first step of smoke / fire detection. Specific sensors need to be implemented in critical areas of the RPAS.
	Protection against detachment of the structure part	No modifications
	Induced vibration protection	As there is no pilot on board who would be prevented to perform his duties in case of excessive vibrations, the protection is only required for the continued functioning of the sensors and equipment on board.
7.4 Protection flight envelope an s structure protection	Lateral control/vertical control/ flight envelope	Autonomous control. No modification, protection is autonomous The aircraft is no longer protected against over speed
	Loads in flight/touch down	In case of too much load for landing/in flight, RPAS will inform to the remote pilot and it will automatically alleviate load (fuel) if necessary
8. Failure management system		

RPAS high level function	Sub functions description	Additions and/or modifications of the RPAS in comparison to the manned aircraft systems
	FailMS Failure Management System	The autonomous failure management considers the continuous monitoring and decision making process usually performed by the pilot during the course of the flight: Go Around decision, monitoring of adherence to flight plan / to trajectory constraints, decision to reject take-off, fire procedures, conduct of ditching / crash-landing, etc. This entails that the system should handle autonomously all the actions that are normally performed by a pilot, as set per the FCOM Normal and Abnormal procedures : • Decision to use the reverse thrust • Decision of diverting to an emergency site. • Fuel management. • Flight performance optimization (speed / altitude) • Prioritization in case of conflict of reconfiguration between different systems. • Automation level (pilot can chose the automation level delegated to the airborne systems) Specifically this entails that the AFMS could handle abnormal procedures involving multiple aircraft systems as well as the monitoring of the FailRMS functionality (see below).
	FailRMS	The management of failures has to be distributed primarily between the different aircraft systems. Each aircraft system shall be capable to handle as planned its own reconfiguration in case of failure. This capacity shall be implemented consistently on each of the aircraft systems under the overall supervision of the AFMS (function A above) in order to prevent that incompatible or conflicting reconfigurations are applied simultaneously on different systems and to set priorities in case of conflicting reconfigurations. FailRMS will handle: • Reconfiguration on failure in case failure reconfiguration does not require a prioritization of the recovery actions amongst the different systems. • Abnormal procedures applying on one system.

Table 27Addition and/or modifications of the RPAS in comparison to the manned aircraft systems

Appendix B RPAS assumptions

	Operational environment
OP_1	Scope of the argument limited to consider only class B and C airspace. However, it is noted that the inclusion of class C airspace introduces VFR traffic and therefore depends on the RPAS including a Sense and Avoid function
OP_2	No require visual contact between pilot and aircraft.
OP_3	The scope of the RPAS will include the aircraft, the ground station used to pilot the aircraft and the communications link between aircraft and ground station.
OP_4	RPAS operates both within and beyond RLOS. The latency introduced by the C2 datalink may contribute to potential hazards.
OP_5	RPAS performs cargo flight from A to B, similar to current cargo planes.

Table 28 Assumption Operational Environment

	Communication
COM_1	Similarly as with manned traffic Air Traffic Controllers have contact with the RPAS by means of radio communication or by digital data link (VHF terrestrial or via satellite communication).
COM_2	The RPA serves as a relay for the voice and data communication between the Air Traffic Controller and the remote pilot.
COM_3	In case of loss of communication between RPA and ATC, the ATC could communicate directly with the remote pilot via the backup line.
COM_4	As in normal conditions the RPA performs the flight automatically, it is assumed that the RPA is able to perform standard communication with ATC (follow up clearances, respond to requests, etc.). The remote pilot is responsible for the proper execution of the filed flight plan and is monitoring.
COM_5	In non-normal conditions the pilot takes over the control of the RPA and communicates with ATC.
COM_6	Similarly as with manned traffic Air Traffic Controllers have contact with the RPAS by means of radio communication or by digital data link (VHF terrestrial or via satellite communication).

Table 29 Assumption Communication

	ATC
ATC_1	ATC phraseology has been established, including those for abnormal and emergency situations.
ATC_2	Necessary FDP system modifications have been implemented to allow for RPAS specific flight plans.
ATC_3	Necessary alerting services are in place to allow for RPAs that are under air traffic control services.

	ATC
ATC_4	Specific Contingency and Emergency Operation Procedures have been established for the RPAS (as part of the operational certification). Basically the RPA behaves in a predictable manner. ATC is fully informed and trained to apply these procedures. E.g. in case of loss of C2, the procedure could involve alerting the ATC and airspace users of the situation (squawk code), the use of a backup line for RPS to ATC communications, predetermined flight or holding patterns and predefined flight completion options (alternate landing sites or in rare cases, terminate the flight by controlled flight into terrain (CFIT) at a pre-determined point that is known to be unpopulated).

Table 30 Assumption ATC

	RPAS and aircraft itself
RPAS_1	RPAS is conceived as an adaptation of an existing civil piloted fixed wing cargo aircraft:
RPAS_2	The adaptations will include provision of a Detect and Avoid function.
RPAS_3	The scope of the RPAS will include the aircraft, the ground station used to pilot the aircraft and the communications link between aircraft and ground station.
RPAS_4	It is assumed that the RPA is fitted with certificated CNS/ATM equipment that allows for the civil published IFR approach procedures.
RPAS_5	It is assumed that the RPAS includes a certificated Detect and Avoid system that allows for flight within non-segregated airspace. As in manned aviation ATC is responsible for separation assurance, while the RPAS remote pilot is responsible to avoid collisions.
RPAS_6	The RPAS is transparent for the ATC

Table 31 Assumption RPAS

Appendix C Areas of Change

The impact that the RPAS might cause in the AoC are classified in four groups

- N/A: not applicable
- No: No impact identified
- I: Indirect: There is an impact that the Aoc might cause to the RPAS, but this impact is common to other aircraft and it is not related to the fact that the aircraft is piloted from ground.
- Yes; there is a clear impact on the RPAS operations.

#	Area of Change		Relevance for RPAS.
1.	Introduction of new aircraft aerodynamic and propulsion configurations	I	Indirect. Unless RPAS counts itself with new aerodynamic and propulsion configurations, but even in this case, the fact that the pilot was on ground is independent from the aerodynamic and propulsion system.
3.	Changes in design roles and responsibilities among manufacturing organizations	I	Indirect, the RPAS can be impacted by a new definition in roles in the aircraft manufactures, in case the RPAS is manufactured by traditional large aircraft companies (e.g. Boeing).
5.	Introduction of new runway-independent aircraft concepts	N	RPAS is based on a traditional manned cargo aircraft, which requires certain types of runways
6.	New supersonic and hypersonic transport aircraft	I	Indirect, The interaction between RPAS and other aircraft is transparent and does not rely on pilot on board. In case of loss of separation RPAS reacts faster than piloted aircraft (do not wait for pilot decision.
9.	Accelerating scientific and technological advances enabling improved performance, decreased fuel burn, and reduced noise	I	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft.
11.	Air traffic composed of a mix of aircraft and capabilities	Y	RPAS integration is more difficult in mixed zones, as additional safety measures may need to be taken.
13.	Reliance on automation supporting a complex air transportation system	I	Indirect The automation of the RPAS might not impact specifically to the RPAS, RAPS is transparent form an ATC point of view.
14.	Advanced vehicle health management systems	Y	RPAS may benefit from this change
18.	New cockpit and cabin surveillance and recording systems	N	No, RPAS has its proper cockpit (on ground) and surveillance system.
19.	Emergence of high-energy propulsion, power, and control systems	I	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft.

21.	Advanced supplementary weather information systems	I	Indirect, our cargo RPAS might benefit from this advance like other non-RPAS aircraft
...	New cockpit warning and alert systems	I	Indirect, our cargo RPAS failure management might benefit from this advance,
27	Next-generation in-flight entertainment and business systems	N	No passengers
31	New glass-cockpit designs in general aviation aircraft	N	No, RPAS cargo does not include glass-cockpit.
33	Entry into service of Very Light Jets	N	No, this Use Case proposed an RPAS supported by detect and avoid system that is expected to detect Very Light Jets.
36	Increasing implementation of Electronic Flight Bag (EFB) for efficient and safe operations	N	No, no people on board.
39	Increasing use of composite structural materials	I	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft.
41	Ongoing electronic component miniaturization	I	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft.
43	Highly-integrated, interdependent aircraft systems	I	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft.
47	Changing human factors assumptions for implementing technology	Y	RPAS ground station might benefit from better HMI
51	Delegation of responsibility from the regulating authority to the manufacturing, operating or maintaining organization	Y	Y, the RPAS operation and the behavior of RPAS after a failure require a close collaboration of stakeholder's ant the involvement of authorities.
53	Trend toward privatization of government ATC systems and airports	I	I, RPAS trusts on ground services
58	Shift toward performance-based solutions and regulations	Y	Yes, this may help the acceptance of RPAS
64	Remote Virtual Tower (RVT) operational concepts	I	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft.
66	Societal pressure to find individuals and organizations criminally liable for errors in design and operations	I	Indirect. The design and the definition of requirements are expected to trace the liability of stakeholders.
67	Economic incentives to form partnerships and outsource organizational activities	I	Indirect, our cargo RPAS might benefit from this advance like other non-RPAS aircraft.
68	Global organizational models	I	Indirect. In the same way that for manned aircraft.

69	Evolution in lines of authority, command and responsibilities within the air transport system	Y	This may accelerate or delay the acceptance of RPAS
73	Increasing complexities within future air transportation systems	I	Indirect, our cargo RPAS might benefit from this advance like other non-RPAS aircraft.
78	Increasing size of maintenance, ATM, and operations databases	I	Indirect, our cargo RPAS might benefit from this advance like other non-RPAS aircraft.
80	Reduction in numbers of aviation personnel familiar with previous generation technology and practices	N	No, RPAS are a new technology.
82	Technologies and procedures enabling reduced separation	I	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft.
86	Evolution in the type and quantity of information used by ATM personnel	I	Indirect, our cargo RPAS might benefit from this advance like other non-RPAS aircraft.
87	Changing design, operational, and maintenance expertise involving air navigation system (ANS) equipment	I	Indirect, our cargo RPAS might benefit from this advance like other non-RPAS aircraft.
89	Increasing heterogeneity of hardware and software within the ANS system	Y	Y, RPAS requires compatibility in performance and quality with ANS systems.
93	Increasing reliance on satellite-based systems for Communications, Navigations, and Surveillance (CNS) Air Traffic Management functions	I	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft.
95	Changing approaches to ATM warning and alert systems	I	Indirect, our cargo RPAS might benefit from this advance like other non-RPAS aircraft.
96	Increasing interactions between highly-automated ground-based and aircraft-based systems	Y	RPAS is very reliant on A-G interactions and may benefit
97	Introduction of artificial intelligence in ATM systems	I	Indirect, our cargo RPAS might benefit from this advance like other non-RPAS aircraft.
99.	Increasing dependence on in-flight electronic databases	Y	RPAS is very reliant on onboard databases.
100.	Increasing operations of military and civilian unmanned aerial systems in shared military, civilian, and special use airspace	I	Indirect, our cargo RPAS might benefit from this advance like other non-RPAS aircraft.
101.	Redesigned or dynamically reconfigured airspace	Y	Airspace redesign may consider RPAS operational aspects.

109.	Increasing utilization of RNAV/RNP departures and approaches by smaller aircraft	I	Indirect, our cargo RPAS might benefit from this advance like other non-RPAS aircraft.
114	Increasing operations of cargo aircraft	Y	Y, RPAS is a cargo aircraft.
117.	Very long-range operations, polar operations, and ETOPS flights.	I	Indirect, cargo RPAS might benefit from this advance like other non-RPAS aircraft.
118.	. Emerging alternate operational models in addition to hub-and-spoke concepts	I	Indirect, cargo RPAS might benefit from this advance like other non-RPAS aircraft.
119.	Increasing numbers of Light Sport Aircraft	I	Indirect, our cargo RPAS may have to deal with more Light Sport Aircraft just like other non-RPAS aircraft.
122.	Accelerated transition of pilots from simple to complex aircraft	I	RPAS pilot training could benefit from new training developments.
125.	Operation of low-cost airlines	N	No, in the same way that for manned aircraft
129	Growth in aviation system throughput	N	No, in the same way that for manned aircraft
133.	Assessment of user fees within the aviation system to recover costs of operation	N	No, in the same way that for manned aircraft
136.	Increasing use of Commercial Off The Shelf (COTS) products in aviation	N	no , in the same way that for manned aircraft
138.	Increased need to monitor incident and accident precursor trends	I	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft. RAPS records not only on the aircraft but as well on the cabin on ground.
139	Increasingly stringent noise and emissions constraints on aviation operations	N	No, in the same way that for manned aircraft
141.	Changes in aviation fuel composition	I	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft
142.	Language barriers in aviation	N/A	N/A the RPAS uses voice communication only in emergence procedures. This is common with non-RPAS aircraft.
144	Changing management and labor relationships in aviation	N	No, in the same way that for manned aircraft
148.	Increasing frequency of hostile acts against the aviation system	I	I, this RPAS is a cargo aircraft with no passengers on board.
161	. Increasing numbers of (migratory) birds near airports	I	Indirect. RPAS does not include glass on the cockpit; it is more robust against bird collision.

170	. Increasing manufacturer sales price incentives due to expanding competitive environment	I	I, This cargo RPAS might benefit from this advance like other non-RPAS aircraft.
174	New surface traffic flow management technologies	I	I, RPAS might adapt to the new surface traffic flow management
184.	Increasing amount of information available to flight crew	I	I, Flight crew, located on ground.
185.	Introduction of Non-Deterministic Approaches (NDA) and artificial intelligence (self learning) in aviation systems	Y	Y, the RPAS might improve the AFMS system.
187.	Shift in responsibility for separation assurance from ATC to flight crew	I	I, This cargo RPAS might benefit from this advance like other non-RPAS aircraft.
188	. Introduction of new training methodologies for operation of advanced aircraft	I	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft
189.	Shifting demographics from military to civilian trained pilots	N	No, in the same way that for manned aircraft. Remote pilot is expected to be a manned trained pilot.
200	Increased dependence on synthetic training in lieu of full-realism simulators	N	no , in the same way that for manned aircraft
202.	Shortened and compressed type rating training for self-sponsored pilot candidates	N	no , in the same way that for manned aircraft
205.	Operational tempo and economic considerations affecting flight crew alertness	N/A	Remote pilot is not under the same consideration that an on board pilot
218	. Supplementary passenger protection and restraint systems	N	N/A no passenger on board
220.	Increasing functionality and use of personal electronic devices by passengers and flight crew	N	N/A no passenger on board. Remote pilot
221.	Introduction of sub-orbital commercial vehicles	N	no , in the same way that for manned aircraft
222	Standards and certification requirements for sub-orbital vehicles	N	No, in the same way that for manned aircraft. Remote pilot is expected to be a manned trained pilot.
223.	Increasing frequency of commercial and government space vehicle traffic	N	No, in the same way that for manned aircraft. Remote pilot is expected to be a manned trained pilot.

225.	Entry into service of commercial, space-tourism passenger vehicles	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
226.	. Changes in the qualifications of maintenance personnel	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
230.	Paradigm shift from paper based to electronic based maintenance records and databases	N/A	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
236	Increasing use of virtual mock-ups for maintenance training and for evaluation of requirements	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
241	Operational tempo and economic considerations affecting fatigue among maintenance personnel	I	The RPAS might require higher maintenance tasks.
242	Increasing single-engine taxi operations or taxi on only inboard engines of 4-engine aircraft	I	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft
243.	Novel technologies to move aircraft from gate-to-runway and runway-to-gate	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
244	High-density passenger cabin configurations	N/A	N/A no passenger on board
245.	Worldwide implementation of SMS	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
246	World wide climate change trending towards warmer temperatures	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft. Increase of warmer temperatures implies fastest formation of winds.
247.	New aircraft recovery systems in general aviation and commercial aircraft	N/A	Indirect, RPAS might benefit from this advance like other non-RPAS aircraft
249	Increasing demands for limited radio frequency bandwidth	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
250.	Shortage of rare-earth elements	N	No, in the same way that for manned aircraft. Remote pilot is expected to be a manned trained pilot.
251.	Introduction of new training methodologies for maintenance staff	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
252.	Smaller organizations and owners operating aging aircraft	I	Indirect, a priori the RPAS will not be an again aircraft (for certain time). The interaction on flight or on ground of RPAS and old aircraft should not be different from the interaction with a current aircraft and aging aircraft.

254.	Aging maintenance workforce	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
255	New pilot licensing standards	Y	Yes, remote pilot licensing might be impacted
256	Decreasing availability of qualified maintenance staff at stations other than home base of operation	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
257.	Reluctance among operators to implement voluntary proactive safety mitigations	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
259.	Shift in the demographics of newly-hired air traffic controllers compared with retiree skills and interests	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
260.	. Increasing use of Controller Pilot Data Link Communication (CPDLC) for weather information and advisories/clearances	I	Indirect, communication with ATC is not considered, datalink do not change...
261.	Operational tempo and economic considerations affecting air traffic controller alertness	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
262.	Potential pilot shortages	Y	RPAS is piloted remotely, pilot shortage impacts as well in RPAS
263.	Shift from clearance-based to trajectory-based air traffic control	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
265.	Socio-economic and political crises affecting aviation	N	No
266.	Single-pilot cockpits for large commercial transports	N	N/A
267.	Increasing adoption of software defined radio systems in commercial aviation	N	Indirect, adoption of radio system might be used for remote pilot and ATC communication.
268.	Decrease in turboprop fleets and operations	I	Indirect, RPAS might be impacted by this change like other non-RPAS aircraft
269.	Proliferation of voluntarily-submitted safety information	N	No, the voluntary safety information , provided by ATC, pilot or maintenance
270.	Initiation of collaborative air traffic management	N	No, the RPAS is transparent in from the point of view of the ATC.
271.	Improved surface operations technologies and procedures	N	No, in the same way that for manned aircraft. Remote pilot is expected to be a manned trained pilot.

272.	Increased traffic flows involving closely-spaced parallel, converging, and intersecting runway operations	N	No, the RPAS is transparent in from the point of view of the ATC. In the case of loss of separation, potential collision, the RPAS does not wait for pilot instruction, the reaction time of an RPAS are shorter.
273.	Increased throughput utilizing improved vertical flight profiles and aids to low-visibility operations	N	No, in the same way that for manned aircraft. Remote pilot is expected to be a manned trained pilot.
274.	Widespread deployment of System Wide Information Management (SWIM) on-demand NAS information services	N	No, the RPAS is transparent in from the point of view of the ATC.

Table 32 Areas of Changes impacted by the RPAS operations

Appendix D Scenarios

D.1 Normal Scenarios

This list of scenario presents the operational scenarios for an AutoFailMS working normally.

Ident	Presentation of the Scenario	Description of scenarios	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HaZ
NS-1	Normal failure-free operation, no intervention required from AutoFailMS (intervention from the AutoFailMS would constitute a failure of the AutoFailMS) although it will provide information to the remote pilot.	AutoFailMS works normally. AutoFailMS provides system status information to remote pilot to allow remote pilot to monitor AutoFailMS function.	NSE	None	NSE
NS-2	successful reconfiguration of the aircraft systems (by the AutoFailMS) following a failure, such that the mission continues according to the flight plan, with no deviation from intended flight path;	Failure occurs to aircraft system before final approach AutoFailMS detects failure. Depending on the type of failure and (emergency, caution with action pilot, caution without action, normal procedure) the AutoFailMS informs to the remote pilot and waits for validation, informs to the remote and applies the action, or applies the action automatically. In case actions required a validation by remote pilot, remote pilot validates. AutoFailMS instructs RPAS. Note: there is no need to provide any information to ATM or other aircraft because the aircraft is able to continue the flight without deviation.	The AutoFailMS informs to the remote pilot who validates (if required) the action. The severity of the scenario depends on the failure. From MIN (slight increase in pilot workload such a routine flight changes)	None)	GEN_HAZ_1 GEN_HAZ_4

Ident	Presentation of the Scenario	Description of scenarios	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HaZ
NS-3	successful reconfiguration of the aircraft systems (by the AutoFailMS) following a failure before final approach, such that the mission continues according to the flight plan, although with initial deviation (recovered) from intended flight path; The distinction is made between this scenario and NS-2 due to the potential for impact on ATM and other aircraft resulting from the deviation from the intended flight path.	Failure occurs to aircraft system before final approach AutoFailMS detects failure. Depending on the type of failure (emergency, caution with action pilot, caution without action, normal procedure) the AutoFailMS either (1) informs to the remote pilot and waits for validation, or (2) informs to the remote pilot and applies the action, or (3) applies the action automatically. In case actions required a validation by remote pilot, remote pilot validates. In case action requires ATC agreement, remote pilot request ATC permission for temporary diversion from the flight plan. If necessary ATC and remote pilot negotiate on possible diversion from the flight plan. ATC accepts the temporary diversion. Remote pilot checks (using information provided by RPS) that reconfiguration has been successfully applied. Remote pilot informs ATC that RPA is able to return to the intended flight path. . ATC accepts return to intended flight path. . RPA returns to the intended flight path	The AutoFailMS informs to the remote pilot who validates (if required) the action. The severity of the scenario depends on the failure. **MIN** (slight increase in pilot workload such a routine flight changes)	For the Air controller slight increase on workload. The potential deviation of the intended flight plan is classified as worst **severity IV,** potential slight reduction of separation during final approach.	GEN_HAZ_1 GEN_HAZ_2 GEN_HAZ_4 GEN_HAZ_12

Ident	Presentation of the Scenario	Description of scenarios	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HaZ
NS-4	Failure during final approach such that the aircraft must execute a missed approach, followed by successful reconfiguration of the aircraft systems (by the AutoFailMS) such that the aircraft can return to land at the intended landing site.	Failure occurs to RPAS during final approach which prevents landing at normal landing site (example: failure of landing gear during final approach). AutoFailMS detects failure and determines that it is not possible to continue with the landing. AutoFailMS informs to the remote pilot about the issue and the intention of executing a missed approach. Remote pilot validates Remote pilot informs the ATC about the missed approach If necessary ATC and remote pilot negotiate. ATC accepts AutoFailMS instructs RPAS to execute missed approach. AutoFailMS reconfigurates RPA Remote pilot checks (using information provided by RPAS) that reconfiguration has been applied. Remote pilot informs ATC that RPA is ready for a new approach at intended landing site. ATC accepts. RPA lands at intended landing site.	The AutoFailMS informs to the remote pilot who validates (if required) the action. The severity of the scenario depends on the failure. The go-around itself is assessed MIN of MAJ depending on the slope at the moment of engine thrust.	The effect on ATS depends on the situation of traffic around. The missed approach should not be worst than IV (slight increase on controller workload) Slight impact on adherence to flight plan	GEN_HAZ_1 GEN_HAZ_2 GEN_HAZ_4 GEN_HAZ_5 GEN_HAZ_12 GEN_HAZ_18 GEN_HAZ_17

Ident	Presentation of the Scenario	Description of scenarios	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HaZ
NS-5	non recoverable failure (but where sufficient control remains to allow successful diversion) before final approach causing diversion (by the AutoFailMS) to alternative landing / recovery site;	Failure occurs to RPAS before final approach which prevents landing at normal landing site AutoFailMS detects failure and determines that it is not possible to start the landing AutoFailMS informs to the remote pilot of the issue and the intention of executing a missed approach followed by a diversion to an alternative landing. Remote pilot validates AutoFailMS informs to the ATM ATM accepts If necessary ATM and remote pilot negotiate AutoFailMS instructs RPAS to divert to alternative landing site. . If necessary ATM manages traffic as usual.	The AutoFailMS informs to the remote pilot who validates (if required) the action. The severity of the scenario depends on the failure. The go-around itself is assessed MIN of MAJ depending on the slope at the moment of engine thrust.	The effect on ATS depends on the situation of traffic around. The missed approach should not be worst than Class IV (slight increase on controller workload) Impact on adherence to flight plan and landing in emergency site	GEN_HAZ_1 GEN_HAZ_2 GEN_HAZ_4 GEN_HAZ_5 GEN_HAZ_12 GEN_HAZ_17 GEN_HAZ_18

Ident	Presentation of the Scenario	Description of scenarios	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HaZ
NS-6	non recoverable failure (but where sufficient control remains to allow successful diversion) during final approach causing a missed approach followed by diversion (by the AutoFailMS) to alternative landing / recovery site;	Failure occurs to aircraft system during final approach which prevents landing at normal landing site (example: failure of landing gear during final approach). AutoFailMS detects failure and determines that it is not possible to continue with the landing. AutoFailMS informs to the remote pilot of the issue and the intention of executing a missed approach followed by a diversion to an alternative landing. Remote pilots validates AutoFailMS informs to the ATM ATM accepts If necessary ATM and remote pilot negotiate. AutoFailMS instructs FMS to execute missed approach. AutoFailMS instructs FMS to divert to alternative landing site.	The AutoFailMS informs to the remote pilot who validates (if required) the action. The severity of the scenario depends on the failure. The go-around itself is assessed MIN of MAJ depending on the slope at the moment of engine thrust.	The effect on ATS depends on the situation of traffic around. The missed approach should not be worst than 5 Class IV (slight increase on controller workload). Impact on adherence to flight plan and landing in emergency site	GEN_HAZ_1 GEN_HAZ_2 GEN_HAZ_4 GEN_HAZ_5 GEN_HAZ_12 GEN_HAZ_17 GEN_HAZ_18
NS-7	transfer of control to remote pilot following a failure for which the AutoFailMS is unable to determine / execute a safe recovery action, followed by successful recovery by the remote pilot;	Failure occurs to aircraft system. AutoFailMS detects failure and determines that it is not possible for the AutoFailMS to manage it AutoFailMS MS informs to the remote pilot of the issue and the impossibility of managing the issue. Remote pilots passes from "autonomous mode" to "manned mode" Remote pilot executes a successful recovery.	The severity of the scenario depends on the failure. At least this scenario is considered MAJ (significant increase of pilot workload) to HAZ	None. Severity 5	GEN_HAZ_1 GEN_HAZ_5 GEN_HAZ_6 GEN_HAZ_12

Ident	Presentation of the Scenario	Description of scenarios	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HaZ
NS-8	non recoverable failure during landing (by the AutoFailMS)	Failure occurs to aircraft system during landing which prevents landing at normal landing site (example: failure of landing gear during final approach). AutoFailMS detects failure and determines that it is not possible to continue with the landing is safe conditions. AutoFailMS informs to the remote pilot of the issue. 4. Remote pilots validated a missed approach or continue landing. AutoFailMS informs to the ATM ATM accepts If necessary ATM and remote pilot negotiate. AutoFailMS instructs FMS to execute missed approach. AutoFailMS instructs FMS to divert to alternative landing site. AutoFailMS instruct continue landing in unsafe situation	The AutoFailMS informs to the remote pilot who validates (if required) the action. The severity of the scenario depends on the failure. From MAJ (go around with negative slope) to CAT (condition that could result in one of more fatalities)	At worst crashing at landing at the airport severity from II to I. Impact on adherence to flight plan, impact on separation assurance.	GEN_HAZ_2 GEN_HAZ_3 GEN_HAZ_4 GEN_HAZ_12 GEN_HAZ_17 GEN_HAZ_18
NS-9	non recoverable failure (but where sufficient control remains to allow successful diversion) during take off	Failure occurs to aircraft system during takeoff that prevents aircraft from continuous taking off AutoFailMS detects failure and determines that it is not possible to continue the take off AutoFailMS informs to the remote pilot of the issue. Remote pilot validates the procedure (continue take off and lands, or stop taking off) AutoFailMS informs to the ATM . ATM accepts If necessary ATM and remote pilot negotiate. AutoFailMS instructs FMS to apply procedure	The severity of the scenario depends on the failure. This scenario is considered MAJ	Increase in controller workload Impact on adherence to flight plan, severity from III	GEN_HAZ_1 GEN_HAZ_2 GEN_HAZ_5 GEN_HAZ_12 GEN_HAZ_18

Table 33 Normal Scenarios

D.1.1 Requirements: Normal Scenarios

	req	Allocated to	Related to Scenarios								
			N1	N2	N3	N4	N5	N6	N7	N8	N9
Req-1	AutoFailMS shall provide information of aircraft status to remote pilot	AutoFailMS	X	x	x	x	x	x	x	x	x
Req-2	AutoFailMS shall detect failure conditions	AutoFailMS		X	X	X	X	X	X	X	X
REq-3	AutoFailMS shall manage failure conditions according to autonomy level	AutoFailMS		X	X	X	X	X	X	X	X
Req-4	AutoFailMS shall inform to the remote pilot of a failure condition according to type of failure	AutoFailMS		X	X	X	X	X	X	X	X
Req-5	Remote pilot shall manage the failure according to autonomy level	Remote pilot		x	X	X	X	X	X	X	X
Req6	Remote pilot shall inform to the ATC of a potential deviation from intended flight plan (depending on autonomy level)	Remote pilot			X	x	x	x		x	x
REq-7	AutoFailMS shall inform to the ATC of a potential deviation from intended flight plan (depending on autonomy level)	AutoFailMS			X	X	X	X		X	X
REq-8	Controller shall check the impact of a potential deviation of RPAS on the ATM	ATC			X	X	X	X		X	X
Req-9	AutoFailMS shall guide the RPAS to a landing site	AutoFailMS				X	X	X		X	
Req-10	Remote pilot shall guide the RPAS to a landing site	Remote pilot				X	X	X		X	
Req-11	AutoFailMS shall execute a missed approach	AutoFailMS				X	X	X		X	
Req-12	Remote pilot shall execute a missed approach	Remote pilot				X	X	X		X	
REq-13	ATC shall manage traffic to ensure a safe diversion of an RPAS to a landing site.	ATC				X	X	X		X	

Table 34 Requirements from Normal Scenarios

D.2 Failure Scenarios

D.2.1 Failure of AutoFailMS without a second failure in the RPAS

idem	title	Description of scenarios	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HaZ
FC-01.01-A	loss of the AutoFailMS without second failure	The loss of AutoFailMS is detected. The pilot receives the alert relative to the loss of AutoFailMS S. The pilot revert to manned mode for failure management After the loss of the AutoFailMS a) The RPAS sends information relative to aircraft status. And the remote pilot in manned mode can detect the failures on board, so the remote pilot can monitor the RPAS. b) The remote pilot continues flying, if the pilot cannot be piloting for a long time, then go to emergency landing site.	Increase on pilot workload, MIN/MAJ:	Increase on pilot workload, severity IV	GEN_HAZ_4
FC-01.01-B	undetected loss of the AutoFailMS without second failure	The loss of AutoFailMS is not detected No second failure. NSE In case of second failure, then at worst CAT. Refer to scenario FC-02.01 Hidden failure. Impact on maintenance.	reduction in safety margins or functional capabilities, as no second failure then NSE	reduction in safety margins or functional capabilities, as no second failure then severity 4	N/A
FC-01.02-A	detected erroneous AutoFailMS without second failure	An erroneous AutoFailMS is detected AutoFailMS informs to the pilot of "malfunctioning AutoFailMS Remote pilot reverts to manned mode. Go to FS-01.01-A	Increase on pilot workload, MIN/MAJ:	Increase on pilot workload, severity IV	GEN_HAZ_5 GEN_HAZ_4
FC-01.02-B	undetected erroneous AutoFailMS without second failure	AutoFailMS is erroneous but the erroneous behavior is not detected. At worst spurious detection. Refer to "spurious failure detection" scenarios. Go to FS-03.03-B	refer to spurious scenarios	refer to spurious scenarios	refer to spurious scenarios

idem	title	Description of scenarios	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HaZ
FC-01.03-A	detected intermittent AutoFailMS without second failure	AutoFailMS connects and disconnects intermittently. The FWS informs to the remote pilot after each modification of autonomous level The remote pilot disengages the AutoFailMS and passes to manned failure mode . At worst intermittently functioning continues. . Increase of pilot workload . AutoFailMS does not take erroneous decisions. to be decided with the human factor team the level of workload (MIN/MAJ) for the pilot	Increase on pilot workload, MIN/MAJ:	Increase on pilot workload, severity IV	GEN_HAZ_5 GEN_HAZ_4
FC-01.03-B	non-detected intermittent AutoFailMS without second failure	AutoFailMS connects and disconnects intermittently. At worst the pilot is not aware of the continuous modification of autonomy level. (in case of combination AutoFailMS and FWS failure) no second failure	reduction in safety margins or functional capabilities, as no second failure then NSE	No physical hit, as no second failure then severity IV	N/A

Table 35 Failure of AutoFailMS without a second failure in the RPAS scenarios

D.2.2 Safety Requirements from scenarios Failure of AutoFailMS without a second failure in the RPAS

Note all requirements from normal scenarios are applicable to failure scenarios as well.

	req	Allocated to	Related to Scenarios					
			FC-01.01-A	FC-01.01-B	FC-01.02-A	FC-01.02-B	FC-01.03-A	FC-01.03-B
Req-20	AutoFailMS shall detect the loss of AutoFailMS	AutoFailMS	X					
Req-21	Aircraft system shall detect the total loss of AutoFailMS (BITE system)	RPAS system	X					
Req-22	Remote pilot shall revert to manned mode after the loss of AutoFailMS	Remote pilot	X		X			
Req-24	The remote pilot shall pilot the RPAS in manned mode for a certain time (maximum time to be decided with human team)	Remote pilot	X		X		x	
Req-25	Maintenance Activities shall address the MTBF for the hidden failure “undetected loss of AutoFailMS”	Maintenance	x	x				x
Req-26	Remote pilot shall disengage the AutoFailMS and passes to manned mode after detection of erroneous AutoFailMS	Remote pilot			X		x	
Req-27	AutoFailMS shall detect the erroneous AutoFailMS, then AutoFailMS disconnects	AutoFailMS			X			
Req-28	Aircraft system shall detect the erroneous of AutoFailMS (BITE system) then AutoFailMS disconnects	RPAS system			x			

Table 36 Safety Requirements from scenarios Failure of AutoFailMS without a second failure in the RPAS

D.2.3 Loss of AutoFailMS followed of a second failure on RPAS

D.2.3.1 Loss of AutoFailMS followed of a second failure on RPAS in cruise

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-02.01-A	Detected loss of the AutoFailMS combined with a second failure on board. In cruise	The remote pilot can control the RPAS	AutoFailMS detects the loss of the AutoFailMS <u>Second failure</u> The RPAS passes to manned mode and RPAS continue sending information relative to aircraft status, this information enables the pilot to continue managing the potential failures in manned mode. The remote pilot identifies that there is a second failure on the RPAS The remote pilot executes the required action to control the RPAS If the action requires any modification of the trajectory the pilot informs the ATC <u>Second failure: Loss of C2 (N/A in this scenario)</u> After the loss of AutoFailMS, there is a second failure (total loss of C2; refer to scenario FS-02.01-B <u>Second failure: loss of datalink</u> After the loss of AutoFailMS, the RPAS loss the datalink. ATC cannot contact with the RPAS. Passes to voice comm. Increase pilot workload <u>Second failure: loss of detection and avoid</u> After the loss of AutoFailMS, the RPAS losses the "detect and avoid" capability. The AutoFailMS informs to the remote pilot. The remote pilot informs to the ATM that the RPAS can no longer assure the collision avoidance. Pilot needs to ensure the collision avoidance.	At worst loss of AutoFailMS combined to loss of detect and avoid: Pilot needs to ensure the collision avoidance. Loss of AutoFailMS and loss of "detect and avoid". HAZ)	At worst loss of AutoFailMS combined with loss of C2, then ATC divert traffic around. Increase of workload. Severity IV	GEN_HAZ_5 GEN_HAZ_2 GEN_HAZ_10 GEN_HAZ_12 GEN_HAZ_14 GEN_HAZ_16

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-.02.01-B	Detected loss of the AutoFailMS combined with a failure on board in cruise	The remote pilot cannot control the RPAS	AutoFailMS detects the loss of the AutoFailMS After the detection of loss of AutoFailMS, the pilot tries to pass to manned mode. But, in this case, the pilot cannot pass to manned mode. For the purposes of this scenario, it is considered that the "loss of automation change" is a hidden failure, the remote pilot finds out that he cannot pass to manned mode when he tries to change the automation level. This is the worst case scenario The AutoFailMS continues sending information relative to RPAS status. In this case, the remote pilot knows the intended trajectory of the RPAS The pilot informs to the ATC of an "uncontrolled RPAS". ATC triggers the procedure for "uncontrolled RPAS". The RPAS continues sending trajectory updates by datalink. ATC diverts traffic around Second failure Then, the remote pilot identifies a second failure on board The AutoFailMS cannot manage the failure nor the remote pilot. CAT. Second failure: Loss of C2 This scenario already considers the loss of control of RPAS by remote pilot. Second failure: Loss of datalink After the loss of AutoFailMS, there is a second failure (total loss of datalink) ."Disappeared RPAS" ATC diverts traffic around according to last intended trajectory of the RPAS. Second failure: loss of detection and avoid After the loss of AutoFailMS, there is a second failure (loss of detection and avoid) The pilot cannot assures the avoid and collision function. The remote pilot informs to the ATC of the situation. RPAS continue sending trajectory intend by datalink. ATC divert the traffic around	AT worst CAT Failure conditions that could result in one or more fatalities.	AT worst RPAS disappeared. No communication with RPAS. Total loss of flight control. Severity I Total loss of separation. Severity I	GEN_HAZ_2 GEN_HAZ_10 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_15 GEN_HAZ_12 GEN_HAZ_11 GEN_HAZ_6

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-.02.01-C	undetected loss of the AutoFailMS combined with a failure on board In cruise	The remote pilot can control the RPAS	The AutoFailMS is loss but the loss is not detected. .Second failure. The second failure is not detected (loss of AutoFailMS) The pilot does not pass to manned mode. The RPAS continues flying with a failure, at worst then CAT. Second failure: Loss of C2 After the undetected loss of AutoFailMS the pilot losses the C2. AT worst CAT Second failure: Loss of datalink After a certain time ATC and/or realizes there is not more information from the RPAS. The remote pilot deduces that the AutoFailMS must have been lost or erroneous, pilot passes to manned mode, but there is a total loss of AutoFailMS. Go to SC-F02.01.A Second failure: Loss of detection and avoid. Pilot is not informed of the loss of detection and avoid function (Loss of AutoFailMS is not detected) Large reduction of safety margins. HAZ Note: undetected loss of AutoFailMS will be eventually detected by remote pilot due to loss of aircraft status messages. Go to SC-F02.01.A	AT worst CAT Failure conditions that could result in one or more fatalities.	Total loss of flight control. Severity I Total loss of separation. Severity I	GEN_HAZ_2 GEN_HAZ_10 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_15 GEN_HAZ_12 GEN_HAZ_11
FS-02.01-D	undetected loss of the AutoFailMS combined with a failure on board In cruise	The remote pilot cannot control the RPAS	The pilot cannot detect the loss of AutoFailMS so he does not pass to manned mode. Same consequences than previous scenario	AT worst CAT Failure conditions that could result in one or more fatalities.	Total loss of flight control. Severity I Total loss of separation. Severity I	GEN_HAZ_3 GEN_HAZ_10 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_15 GEN_HAZ_12 GEN_HAZ_11

Table 37 Loss of AutoFailMS followed of a second failure on RPAS in cruise Scenarios

D.2.3.2 Safety Requirements from scenarios Failure of AutoFailMS without a second failure in the RPAS in cruise

	req	Allocated to	Related to Scenarios			
			FS-02.01-A	FS-02.01-B	FS-02.01-C	FS-02.01-D
Req-30	Maintenance Activities shall address the MTBF for the hidden failure “loss of automation mode”	Maintenance		x		
Req-31	ATC shall define procedure for uncontrolled RPAS (e.g. divert traffic around)	ATC		x		
Req-32	ATC shall define procedure for disappeared RPAS (e.g. divert traffic around, inform authorities)	ATC		x		
Req-33	ATC shall define procedure for RPAS after collision and avoidance loss (e.g. divert traffic around)	ATC	X	x		x
Req-34	Loss of C2 link shall be designed according to DAL A (TBC) (application of ARP4754A/ED79A)	RPAS systems	x	x	x	x

Table 38 Requirements from Loss of AutoFailMS followed of a second failure on RPAS in cruise Scenarios

D.2.3.3 Loss of AutoFailMS followed of a second failure on RPAS before final approach

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-02.02-A	Detected loss of the AutoFailMS combined with a failure: Before final approach	The remote pilot can control the RPAS	AutoFailMS detects the loss of the AutoFailMS before final approach. The remote pilot needs to perform the approach in manned mode or to decide missed approach. <u>Second failure</u> The RPAS passes to manned mode and RPAS continue sending information relative to aircraft status, this information enables the pilot to continue managing the potential failures in manned mode. The remote pilot identifies that there is a second failure on the RPAS The remote pilot executes the required action to control the RPAS If the action requires any modification of the trajectory or missed approach the pilot informs the ATC <u>Second failure: Loss of C2 (N/A in this scenario)</u> After the loss of AutoFailMS, there is a second failure (total loss of C2; refer to scenario FS-02.02-B <u>Second failure: loss of datalink</u> After the loss of AutoFailMS, the RPAS loss the datalink. ATC cannot contact with the RPAS. Passes to voice comm. Increase pilot workload <u>Second failure: loss of detection and avoid</u> After the loss of AutoFailMS, the RPAS losses the “detect and avoid” capability. The AutoFailMS informs to the remote pilot. The remote pilot informs to the ATM that the RPAS can no longer assure the collision avoidance. RPAS is in approach. Pilot needs to ensure the collision avoidance.	At worst loss of AutoFailMS combined to loss of detect and avoid: Pilot needs to ensure the collision avoidance. Increase of pilot workload before final approach MAJ/HAZ Loss of AutoFailMS and loss of “detect and avoid “in missed approach (or landing) at worst HAZ)	At worst loss of AutoFailMS combined with loss of C2, then ATC divert traffic around. Increase of workload. Severity III.	GEN_HAZ_5 GEN_HAZ_2 GEN_HAZ_10 GEN_HAZ_12 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_17

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-02.02-B	Detected loss of the AutoFailMS combined with a failure on board. Before final approach	The remote pilot cannot control the RPAS	AutoFailMS detects the loss of the AutoFailMS before final approach After the detection of loss of AutoFailMS, the pilot tries to pass to manned mode. But, in this case, the pilot cannot pass to manned mode. "Loss of automation change" is a hidden failure). The AutoFailMS continues sending information relative to RPAS status. In this case, the remote pilot knows the intended trajectory of the RPAS The pilot informs to the ATC of an "uncontrolled RPAS". ATC triggers the procedure for "uncontrolled RPAS". The RPAS continues sending trajectory updates by datalink. ATC diverts traffic around in TMA. RPAS is supposed to continue with the landing. <u>Second failure</u> Then, the remote pilot identifies a second failure on board The AutoFailMS cannot manage the failure nor the remote pilot. CAT. <u>Second failure: Loss of C2</u> This scenario already considers the loss of control of RPAS by remote pilot. <u>Second failure: Loss of datalink</u> After the loss of AutoFailMS, there is a second failure (total loss of datalink) ."Disappeared RPAS" ATC diverts traffic around according to last intended trajectory of the RPAS. RPAS is in an TMA <u>Second failure: loss of detection and avoid</u> After the loss of AutoFailMS, there is a second failure (loss of detection and avoid) The pilot cannot assures the avoid and collision function. The remote pilot informs to the ATC of the situation. RPAS continue sending trajectory intend by datalink. ATC divert the traffic around RPAS is in TMA	AT worst CAT Failure conditions that could result in one or more fatalities.	AT worst RPAS disappeared. No communication with RPAS. Total loss of flight control. Severity I Total loss of separation. Severity I	GEN_HAZ_3 GEN_HAZ_10 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_15 GEN_HAZ_12 GEN_HAZ_11 GEN_HAZ_6

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-.02.02-C	undetected loss of the AutoFailMS combined with a failure on board before final approach	The remote pilot can control the RPAS	The AutoFailMS is loss but the loss is not detected. .<u>Second failure.</u> The second failure is not detected (loss of AutoFailMS) The pilot does not pass to manned mode. The RPAS continues flying with a failure, at worst then CAT. Maybe RPAS crash in TMA. <u>Second failure: Loss of C2</u> After the undetected loss of AutoFailMS the pilot losses the C2. AT worst CAT. <u>Second failure: Loss of datalink</u> After a certain time ATC and/or realizes there is not more information from the RPAS. The remote pilot deduces that the AutoFailMS must have been lost or erroneous, pilot passes to manned mode, but there is a total loss of AutoFailMS. Go to SC-F02.02.A <u>Second failure: Loss of detection and avoid.</u> Pilot is not informed of the loss of detection and avoid function (Loss of AutoFailMS is not detected) Large reduction of safety margins in TMA. HAZ Note: undetected loss of AutoFailMS will be eventually detected by remote pilot due to loss of aircraft status messages. Go to SC-F02.02.A	AT worst CAT Failure conditions that could result in one or more fatalities.	Total loss of flight control. Severity I Total loss of separation. Severity I	GEN_HAZ_2 GEN_HAZ_10 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_15 GEN_HAZ_12 GEN_HAZ_11
FS-02.02-D	Undetected loss of the AutoFailMS combined with a failure on board. Before final approach	The remote pilot cannot control the RPAS	The pilot cannot detect the loss of AutoFailMS so he does not pass to manned mode. Same consequences than previous scenario	AT worst CAT Failure conditions that could result in one or more fatalities.	Total loss of flight control. Severity I Total loss of separation. Severity I	GEN_HAZ_3 GEN_HAZ_10 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_15 GEN_HAZ_12 GEN_HAZ_11

Table 39 Loss of AutoFailMS followed of a second failure on RPAS before final approach scenarios

D.2.3.4 Safety Requirements from scenarios Loss of AutoFailMS followed of a second failure on RPAS before final approach

	req	Allocated to	Related to Scenarios			
			FS-02.02-A	FS-02.02-B	FS-02.02-C	FS-02.02-D
Req-40	ATC shall define procedure for uncontrolled RPAS (e.g. divert traffic around) in TMA	ATC		x	X	
Req-41	ATC shall define procedure for disappeared RPAS (e.g. divert traffic around, inform authorities) in TMA	ATC		x	X	
Req-42	ATC shall define procedure for RPAS after collision and avoidance loss (e.g. divert traffic around) in TMA	ATC	X	x	x	x

Table 40 Requirements from Loss of AutoFailMS followed of a second failure on RPAS before final approach scenarios

D.2.3.5 Loss of AutoFailMS followed of a second failure on RPAS during final approach

Ident	title	Pilot control	Description of the scenario
FS-02.03-A	Detected loss of the AutoFailMS combined with a failure: during final approach	The remote pilot can control the RPAS	No relevant difference with FS-02.02-A. To be confirmed after stage 7
FS-02.03-B	Detected loss of the AutoFailMS combined with a failure on board During final approach	The remote pilot cannot control the RPAS	No relevant difference with FS-02.02-A. To be confirmed after stage 7
FS-.02.03-C	Undetected loss of the AutoFailMS combined with a failure on board During final approach	The remote pilot can control the RPAS	No relevant difference with FS-02.02-A. To be confirmed after stage 7
FS-02.03-D	Undetected loss of the AutoFailMS combined with a failure on board. During final approach	The remote pilot cannot control the RPAS	No relevant difference with FS-02.02-A. To be confirmed after stage 7

Table 41 of AutoFailMS followed of a second failure on RPAS during final approach scenarios

D.2.3.6 Loss of AutoFailMS followed of a second failure on RPAS during landing

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-02.04-A	Detected loss of the AutoFailMS combined with a failure: during landing	The remote pilot can control the RPAS	AutoFailMS detects the loss of the AutoFailMS during landing. The remote pilot needs to perform the landing in manned mode. Pilot is supported by ATOLS <u>Second failure</u> The RPAS passes to manned mode and RPAS continue sending information relative to aircraft status, this information enables the pilot to continue managing the potential failures in manned mode. The remote pilot identifies that there is a second failure on the RPAS The remote pilot executes the required action to control the RPAS If the action requires any modification of the trajectory or missed approach the pilot informs the ATC <u>Second failure: Loss of C2 (N/A in this scenario)</u> After the loss of AutoFailMS, there is a second failure (total loss of C2; refer to scenario FS-02.04-B <u>Second failure: loss of datalink</u> After the loss of AutoFailMS, the RPAS loss the datalink. ATC cannot contact with the RPAS. Passes to voice comm. Increase pilot workload <u>Second failure: loss of detection and avoid</u> After the loss of AutoFailMS, the RPAS losses the "detect and avoid" capability. The AutoFailMS informs to the remote pilot. The remote pilot informs to the ATM that the RPAS can no longer assure the collision avoidance. RPAS is in landing. Pilot needs to ensure the collision avoidance.	At worst loss of AutoFailMS combined to loss of detect and avoid: Pilot needs to ensure the collision avoidance. Increase of pilot workload before final approach MAJ/HAZ Loss of AutoFailMS and loss of "detect and avoid "in missed approach (or landing) at worst HAZ)	At worst loss of AutoFailMS combined with loss of C2, then ATC divert traffic around. Increase of workload. Severity III	GEN_HAZ_5 GEN_HAZ_2 GEN_HAZ_10 GEN_HAZ_12 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_17

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-02.02-B	Detected loss of the AutoFailMS combined with a failure on board. Before final approach	The remote pilot cannot control the RPAS	AutoFailMS detects the loss of the AutoFailMS during landing After the detection of loss of AutoFailMS, the pilot tries to pass to manned mode. But, in this case, the pilot cannot pass to manned mode. ("Loss of automation change" is a hidden failure). The AutoFailMS continues sending information relative to RPAS status. In this case, the remote pilot knows the intended trajectory of the RPAS. The RPAS cannot lands (loss of AutoFailMS) and it cannot be controlled by the remote pilot. Then CAT. The pilot informs to the ATC of an "uncontrolled RPAS". ATC triggers the procedure for “uncontrolled RPAS”. The RPAS continues sending trajectory updates by datalink. ATC diverts traffic around in TMA. RPAS is supposed to continue with the landing. <u>Second failure</u> Then, the remote pilot identifies a second failure on board The AutoFailMS cannot manage the failure nor the remote pilot. CAT. <u>Second failure: Loss of C2</u> This scenario already considers the loss of control of RPAS by remote pilot. <u>Second failure: Loss of datalink</u> After the loss of AutoFailMS, there is a second failure (total loss of datalink) ."Disappeared RPAS" ATC diverts traffic around according to last intended trajectory of the RPAS. RPAS is in an TMA <u>Second failure: loss of detection and avoid</u> After the loss of AutoFailMS, there is a second failure (loss of detection and avoid) The pilot cannot assures the avoid and collision function. The remote pilot informs to the ATC of the situation. RPAS continue sending trajectory intend by datalink. ATC divert the traffic around RPAS is in TMA	AT worst CAT Failure conditions that could result in one or more fatalities.	AT worst RPAS disappeared. No communication with RPAS. Total loss of flight control. Severity I Total loss of separation. Severity I	GEN_HAZ_10 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_15 GEN_HAZ_12 GEN_HAZ_11 GEN_HAZ_6 GEN_HAZ_3

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-.02.02-C	Undetected loss of the AutoFailMS combined with a failure on board before final approach	The remote pilot can control the RPAS	The AutoFailMS is loss but the loss is not detected. AutoFailMS does not properly configure the RPAS of landing, so RPAS out of the landing path. ATC detects the failure and contact the pilot. Pilot passes to manned mode. At worst the ATC detects lately the RPAS deviation. Potential loss of separation .<u>Second failure.</u> The second failure is not detected (loss of AutoFailMS) The pilot does not pass to manned mode. RPAS uncontrolled AT worst CAT. <u>Second failure: Loss of C2</u> After the undetected loss of AutoFailMS the pilot losses the C2. AT worst CAT. <u>Second failure: Loss of datalink</u> After a certain time ATC and/or realizes there is not more information from the RPAS. The remote pilots deduce that the AutoFailMS must have been lost or erroneous, pilot passes to manned mode, but there is a total loss of AutoFailMS. Go to SC-F02.02.A <u>Second failure: Loss of detection and avoid.</u> Pilot is not informed of the loss of detection and avoid function (Loss of AutoFailMS is not detected) Large reduction of safety margins in TMA. HAZ Note: undetected loss of AutoFailMS will be eventually detected by remote pilot due to loss of aircraft status messages. Go to SC-F02.02.A	AT worst CAT Failure conditions that could result in one or more fatalities.	Total loss of flight control. Severity I Total loss of separation. Severity I	GEN_HAZ_10 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_15 GEN_HAZ_12 GEN_HAZ_11 GEN_HAZ_2
FS-02.02-D	Undetected loss of the AutoFailMS Combined with a failure on board. Before final approach	The remote pilot cannot control the RPAS	The pilot cannot detect the loss of AutoFailMS so he does not pass to manned mode. Same consequences than previous scenario	AT worst CAT Failure conditions that could result in one or more fatalities.	Total loss of flight control. Severity 1 Total loss of separation. Severity 1	GEN_HAZ_10 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_15 GEN_HAZ_12 GEN_HAZ_11 GEN_HAZ_2 GEN_HAZ_3

Table 42 Requirements of AutoFailMS followed of a second failure on RPAS during landing scenarios

D.2.3.7 Safety Requirements from scenarios Loss of AutoFailMS followed of a second failure on RPAS during landing

	req	Allocated to	Related to Scenarios			
			FS-02.04-A	FS-02.04-B	FS-02.04-C	FS-02.04-D
Req-50	ATC shall define procedure to contact remote pilot in case of abnormal RPAS behaviors	ATC			x	

Table 43 requirements from Loss of AutoFailMS followed of a second failure on RPAS during landing scenarios

D.2.4 Spurious detection of a non-existing failure by AutoFailMS

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-03.01-A	Detection of a non-existing failure in cruise	The remote pilot can control the RPAS	The AutoFailMS erroneously detect a spurious failure. Spurious Failure If the remote pilot realizes that there is spurious detection, then remote pilot considers AutoFailMS is erroneous, disconnects the AutoFailMS and passes to manned mode. Then go to scenarios "detected loss of AutoFailMS" If the remote pilot does not realizes then: The AutoFailMS execute an erroneous reconfiguration of the aircraft. At worst this reconfiguration implies A. Deviation of trajectory. AutoFailMS informs to the remote pilot of the intention of modifying the trajectory. Negotiation with ATC, b. Landing in an emergency site. AutoFailMS informs to the remote pilot of the intention of modifying the trajectory. Negotiation with ATC Spurious failure: Loss or erroneous 2RC AutoFailMS informs that the C2 is lost or non reliable. Remote pilot thinks that it is no possible to manage the RPAS. RPAS manages autonomously by AutoFailMS without remote pilot. However AutoFailMS is erroneous. Non foreseeable consequences. At worst CAT. Spurious failure is:"total loss or erroneous datalink" The remote pilot continues receiving the data from the aircraft. This is incoherent with the alarm "loss of data-link". The remote pilot is confused, he/she does not know where the RPAS is, nor where it is going. The remote pilot informs the ATC of "disappeared RPAS" ATC diverts traffic around according to last intended trajectory Spurious failure is :"loss/erroneous detect and avoid" The AutoFailMS informs that the "detect and avoid "system is faulty. Remote Pilot assures the collision avoidance. Increase pilot workload.	At worst erroneous detection of a non-existing failure, landing in emergency site or disconnection of manned mode. RPAS uncontrolled. AT worst CAT	At worst erroneous AutoFailMS, severity I diversion, landing in emergency site, increase of controller workload at worst severity III	GEN_HAZ_18 GEN_HAZ_16 GEN_HAZ_15 GEN_HAZ_14 GEN_HAZ_13 GEN_HAZ_12 GEN_HAZ_10 GEN_HAZ_9 GEN_HAZ_6 GEN_HAZ_3

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-03.01-B	Detection of a non-existing failure	The remote pilot cannot control the RPAS	The AutoFailMS erroneously detect a spurious failure. Spurious Failure If the remote pilot realizes that there is spurious detection, then remote pilot considers AutoFailMS is erroneous, disconnects the AutoFailMS and tries to pass to manned mode. But the pilot cannot manage the RPAS. Pilot informs to the ATC that there is an uncontrolled RPAS. ATC diverts traffic around. If the remote pilot does not realize then: The AutoFailMS executes an erroneous reconfiguration of the aircraft. At worst this reconfiguration implies A. Unnecessary deviation of trajectory. AutoFailMS informs to the remote pilot of the intention of modifying the trajectory. b. Unnecessary landing in an emergency site. AutoFailMS informs to the remote pilot of the intention of modifying the trajectory. Spurious failure: Loss or erroneous 2RC AutoFailMS informs that the C2 is lost or non reliable. Remote pilot thinks that it is no possible to manage the RPAS. RPAS manages autonomously by AutoFailMS without remote pilot. However AutoFailMS is erroneous. Non foreseeable consequences. At worst CAT. Spurious failure is:"total loss or erroneous datalink" The remote pilot continues receiving the data from the aircraft. This is incoherent with the alarm "loss of data-link". The remote pilot is confused, he/she does not know where the RPAS is, nor where it is going. The remote pilot informs the ATC of "disappeared RPAS" ATC diverts traffic around according to last intended trajectory of the RPAS. Spurious failure is :"loss/erroneous detect and avoid" The AutoFailMS informs that the "detect and avoid "system is faulty. Remote Pilot tries to manage the RPAS but it is not possible. The pilot cannot assure the "detect and avoid". Pilot informs to the ATC that there is an uncontrolled RPAS. ATC diverts traffic around	At worst erroneous detection of a non-existing failure, landing in emergency site or disconnection of manned mode. RPAS uncontrolled. Total loss of detect and avoid CAT	At worst erroneous AutoFailMS, severity I diversion, landing in emergency site, increase of controller workload at worst severity III	GEN_HAZ_3 GEN_HAZ_7 GEN_HAZ_10 GEN_HAZ_11 GEN_HAZ_12 GEN_HAZ_13 GEN_HAZ_14 GEN_HAZ_15 GEN_HAZ_16 GEN_HAZ_18 GEN_HAZ_6

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-03.02-A	Detection of a non-existing failure before final approach	The remote pilot can control the RPAS	The AutoFailMS erroneously detect a spurious failure. Before finale approach Spurious Failure If the remote pilot realizes that there is spurious detection, then remote pilot considers AutoFailMS is erroneous, disconnects the AutoFailMS and passes to manned mode. Then go to scenarios "detected loss of AutoFailMS before final approach" If the remote pilot does not realizes then: The AutoFailMS execute an erroneous reconfiguration of the aircraft. At worst this reconfiguration implies A. Deviation of trajectory. AutoFailMS informs to the remote pilot of the intention of modifying the trajectory. Negotiation with ATC, (maybe missed approach) b. Landing in an emergency site. AutoFailMS informs to the remote pilot of the intention of modifying the trajectory. Negotiation with ATC Spurious failure: Loss or erroneous 2RC AutoFailMS informs that the C2 is lost or non reliable. Remote pilot thinks that it is no possible to manage the RPAS. RPAS manages autonomously by AutoFailMS without remote pilot. However AutoFailMS is erroneous. Non foreseeable consequences. At worst CAT. Spurious failure is:"total loss or erroneous datalink" The remote pilot continues receiving the data from the aircraft. This is incoherent with the alarm "loss of data-link". The remote pilot is confused, he/she does not know where the RPAS is, nor where it is going. The remote pilot informs the ATC of "disappeared RPAS". Voice communication. ATC diverts traffic around according to last intended trajectory of the RPAS. Increase of workload controller Spurious failure is :"loss/erroneous detect and avoid" The AutoFailMS informs that the "detect and avoid "system is faulty. Remote Pilot assures the collision avoidance. Increase pilot workload Act manages the traffic around, RPAS in or close to a TMA.	At worst erroneous detection of a non-existing failure, landing in emergency site or disconnection of manned mode. RPAS uncontrolled. AT worst CAT	At worst erroneous AutoFailMS, severity I diversion, landing in emergency site or missed approach, increase of controller workload at worst severity III	GEN_HAZ_3 GEN_HAZ_6 GEN_HAZ_9 GEN_HAZ_10 GEN_HAZ_11 GEN_HAZ_12 GEN_HAZ_13 GEN_HAZ_14 GEN_HAZ_15 GEN_HAZ_16 GEN_HAZ_17

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
c	Detection of a non-existing failure before final approach	The remote pilot cannot control the RPAS	The AutoFailMS erroneously detect a spurious failure. Spurious Failure If the remote pilot realizes that there is spurious detection, then remote pilot considers AutoFailMS is erroneous, disconnects the AutoFailMS and tries to pass to manned mode. But the pilot cannot manage the RPAS. Pilot informs to the ATC that there is an uncontrolled RPAS. ATC diverts traffic around. RPAS in or close to a TMA If the remote pilot does not realize then: The AutoFailMS executes an erroneous reconfiguration of the aircraft. At worst this reconfiguration implies A. Unnecessary deviation of trajectory. AutoFailMS informs to the remote pilot of the intention of modifying the trajectory. b. Unnecessary landing in an emergency site. AutoFailMS informs to the remote pilot of the intention of modifying the trajectory. Spurious failure: Loss or erroneous 2RC AutoFailMS informs that the C2 is lost or non reliable. RPAS manages autonomously by AutoFailMS without remote pilot. However AutoFailMS is erroneous. Non foreseeable consequences. At worst CAT. Spurious failure is:"total loss or erroneous datalink" The remote pilot continues receiving the data from the RPAS. This is incoherent with the alarm "loss of data-link". The remote pilot is confused, he/she does not know where the RPAS is, nor where it is going. The remote pilot informs the ATC of "disappeared RPAS" ATC diverts traffic around according to last intended trajectory of the RPAS. RPAS in or close to TMA. Spurious failure is :"loss/erroneous detect and avoid" The AutoFailMS informs that the "detect and avoid "system is faulty. Remote Pilot tries to manage the RPAS but it is not possible. The pilot cannot assure the "detect and avoid". Pilot informs to the ATC that there is an uncontrolled RPAS. ATC diverts traffic around	At worst erroneous detection of a non-existing failure, landing in emergency site or disconnection of manned mode. RPAS uncontrolled. Total loss of detect and avoid CAT	At worst erroneous AutoFailMS, severity I diversion, landing in emergency site, increase of controller workload at worst severity III	GEN_HAZ_3 GEN_HAZ_7 GEN_HAZ_10 GEN_HAZ_11 GEN_HAZ_12 GEN_HAZ_13 GEN_HAZ_14 GEN_HAZ_15 GEN_HAZ_16 GEN_HAZ_18 GEN_HAZ_6

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-03.03-A	Detection of a non-existing failure during final approach	The remote pilot can control the RPAS	No relevant difference with FS-03.02-A. To be confirmed after stage 7	Refer to FS-03.02-A	Refer to FS-03.02-A	Refer to FS-03.02-A
FS-03.03-B	Detection of a non-existing failure during final approach	The remote pilot cannot control the RPAS	No relevant difference with FS-03.02-B. To be confirmed after stage 7	Refer to FS-03.02-B	Refer to FS-03.02-B	Refer to FS-03.02-B
FS-03.04-A	Detection of a non-existing failure during landing	The remote pilot can control the RPAS	No relevant difference with FS-03.02-A. To be confirmed after stage 7	Refer to FS-03.02-A	Refer to FS-03.02-A	Refer to FS-03.02-A
FS-03.04-B	Detection of a non-existing failure during landing	The remote pilot cannot control the RPAS	No relevant difference with FS-03.02-B. To be confirmed after stage 7	Refer to FS-03.02-B	Refer to FS-03.02-B	Refer to FS-03.02-B

Table 44 Spurious detection of a non-existing failure by AutoFailMS scenarios

D.2.4.1 Safety Requirements from scenarios Spurious detection of an non-existing failure by AutoFailMS

	req	Allocated to	Related to Scenarios							
			FS-03.01-A	FS-03.01-B	FS-03.02-A	FS-03.02-B	FS-03.03-A	FS-03.03-B	FS-03.04-A	FS-03.04-B
req-60	RPAS system needs to ensure that there is not any single cause implying an spurious failure detection and a faulty C2 (common mode)	RPAS systems	X		X		X		x	
Req-61	RPAS system needs to ensure that there is not any single cause implying an spurious failure detection and a faulty “detect and avoid” (common mode)	RPAS systems		X		X		X		X

Table 45 Requirements from spurious detection of a non-existing failure by AutoFailMS scenarios

D.2.5 Erroneous AutoFailMS

D.2.5.1 Erroneous/Erratic AutoFailMS combined with a second failure on board in cruise

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-04.01-A	detected erroneous/erratic AutoFailMS combined with a second failure on board	The remote pilot can control the RPAS	AutoFailMS detects the erroneous AutoFailMS Then the AutoFailMS reconfigurates itself. If it is no possible to reconfigurate then inform to the remote pilot. AT worst Remote pilot consider loss of AutoFailMS. Go to loss of AutoFailMS scenarios FS-02.01-A	FS-02.01-A	FS-02.01-A	FS-02.01-A
FS-04.01-B	detected erroneous/erratic AutoFailMS combined with a failure on board in cruise	The remote pilot cannot control the RPAS	AutoFailMS detects the erroneous AutoFailMS Then the AutoFailMS reconfigurates itself. If it is no possible to reconfigurate then inform to the remote pilot. Remote pilot consider loss of AutoFailMS. Go to loss of AutoFailMS scenarios FS-02.01-B	FS-02.01-A	FS-02.01-A	FS-02.01-A

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-04.01-C	undetected erroneous/erratic AutoFailMS combined with a failure on board	The remote pilot can control the RPAS	The AutoFailMS identifies correctly the failure but the decision or execution is erroneously applied. Second failure. The AutoFailMS executes an erroneous recovery action (refer to scenario spurious detection of an erroneous failure) and at the same time, the AutoFailMS does not manage a real failure (refer to loss of AutoFailMS scenarios FS.02.01-A). Second failure. Loss or erroneous 2RC The AutoFailMS correctly identifies the loss of 2RC, but it applies an erroneous reconfiguration action. Remote pilot does not pass to manned mode. At worst undetected loss of control. Loss of RPAS. CAT Second failure is :"total loss or erroneous datalink" AutoFailMS correctly identifies the loss of datalink but it applies an erroneous reconfiguration action. After certain time ATC and/or remote pilot realizes of the loss/erroneous of datalink, Voice communication. Pilot passes to made mode. HAZ/MAJ Second failure is :"loss/erroneous detect and avoid" AutoFailMS correctly identifies the loss/erroneous detect and avoid but it applies an erroneous reconfiguration action. Remote pilot is not informed of the loss/erroneous detect and avoid. Remote pilot does not assure the collision and avoid	At worst undetected loss of "detect and avoid" function. No control of RPAS. CAT	No control of RPAS. Severity I. Large reduction in safety margins.	GEN_HAZ_5 GEN_HAZ_2 GEN_HAZ_10 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_3 GEN_HAZ_6 GEN_HAZ_9 GEN_HAZ_11 GEN_HAZ_13 GEN_HAZ_15 GEN_HAZ_18

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-04.01-D	undetected erroneous/erratic AutoFailMS combined with a failure on board in cruise	The remote pilot cannot control the RPAS	The AutoFailMS identifies correctly the failure but the decision or execution is erroneously applied. Second failure. The AutoFailMS executes an erroneous recovery action (refer to scenario spurious detection of an erroneous failure) and at the same time, the AutoFailMS does not manage a real failure (refer to loss of AutoFailMS scenarios FS.02.01-B). Second failure. Loss or erroneous 2RC The AutoFailMS correctly identifies the loss of 2RC, but it applies an erroneous reconfiguration action. Remote pilot does not pass to manned mode. At worst undetected loss of control. Loss of RPAS. CAT Second failure is :"total loss or erroneous datalink" AutoFailMS correctly identifies the loss of datalink but it applies an erroneous reconfiguration action. After certain time ATC and/or remote pilot realizes of the loss/erroneous of datalink, Voice communication. Pilot ties to pass to manned mode, but it s not possible. Loss of control. HAZ/CAT. Second failure is :"loss/erroneous detect and avoid" AutoFailMS correctly identifies the loss/erroneous detect and avoid but it applies an erroneous reconfiguration action. Remote pilot is not informed of the loss/erroneous detect and avoid. Remote pilot does not assure the collision and avoid	At worst undetected loss of "detect and avoid" function. No control of RPAS. CAT	No control of RPAS. Severity I. Large reduction in safety margins.	GEN_HAZ_2 GEN_HAZ_10 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_15 GEN_HAZ_12 GEN_HAZ_11 GEN_HAZ_3 GEN_HAZ_7 GEN_HAZ_13 GEN_HAZ_15 GEN_HAZ_18

Table 46 Erroneous/Erratic AutoFailMS combined with a second failure on board in cruise scenarios

D.2.5.2 Erroneous/Erratic AutoFailMS combined with a second failure on board before final approach

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-04.02-A	detected erroneous/erratic AutoFailMS combined with a second failure on board before final approach	The remote pilot can control the RPAS	AutoFailMS detects the erroneous AutoFailMS Then the AutoFailMS reconfigurates itself. If it is no possible to reconfigurate then inform to the remote pilot. AT worst Remote pilot consider loss of AutoFailMS. Go to loss of AutoFailMS scenarios FS-02.02-A	FS-02.02-A	FS-02.02-A	FS-02.02-A
FS-04.02-B	detected erroneous/erratic AutoFailMS combined with a failure on board before final approach	The remote pilot cannot control the RPAS	AutoFailMS detects the erroneous AutoFailMS Then the AutoFailMS reconfigurates itself. If it is no possible to reconfigurate then inform to the remote pilot. Remote pilot consider loss of AutoFailMS. Go to loss of AutoFailMS scenarios FS-02.02-B	FS-02.02-B	FS-02.02-B	FS-02.02-B

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-04.02-C	undetected erroneous/erratic AutoFailMS combined with a failure on board	The remote pilot can control the RPAS	The AutoFailMS identifies correctly the failure but the decision or execution is erroneously applied. <u>Second failure.</u> The AutoFailMS executes an erroneous recovery action (refer to scenario spurious detection of an erroneous failure FS-03.02-A) and at the same time, the AutoFailMS does not manage a real failure (refer to loss of AutoFailMS scenarios FS.02.02-A). <u>Second failure. Loss or erroneous 2RC</u> The AutoFailMS correctly identifies the loss of 2RC, but it applies an erroneous reconfiguration action. Remote pilot does not pass to manned mode. At worst undetected loss of control. Loss of RPAS. CAT <u>Second failure is :"total loss or erroneous datalink"</u> AutoFailMS correctly identifies the loss of datalink but it applies an erroneous reconfiguration action. After certain time ATC and/or remote pilot realizes of the loss/erroneous of datalink, Voice communication. Pilot passes to made mode. HAZ/MAJ potential missed approach <u>Second failure is :"loss/erroneous detect and avoid"</u> AutoFailMS correctly identifies the loss/erroneous detect and avoid but it applies an erroneous reconfiguration action. Remote pilot is not informed of the loss/erroneous detect and avoid. Remote pilot does not assure the collision and avoid RPAS in or close to a TMA.	At worst erroneous detection of a non-existing failure, landing in emergency site or disconnection of manned mode. RPAS uncontrolled. AT worst CAT	At worst erroneous AutoFailMS, severity I Diversion, landing in emergency site or missed approach, increase of controller workload at worst severity III.	GEN_HAZ_3 GEN_HAZ_5 GEN_HAZ_6 GEN_HAZ_9 GEN_HAZ_10 GEN_HAZ_12 GEN_HAZ_11 GEN_HAZ_13 GEN_HAZ_14 GEN_HAZ_15 GEN_HAZ_16 GEN_HAZ_18 GEN_HAZ_17

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-04.02-D	undetected erroneous/erratic AutoFailMS combined with a failure on board in cruise	The remote pilot cannot control the RPAS	The AutoFailMS identifies correctly the failure but the decision or execution is erroneously applied. Second failure. The AutoFailMS executes an erroneous recovery action (refer to scenario spurious detection of an erroneous failure) and at the same time, the AutoFailMS does not manage a real failure (refer to loss of AutoFailMS scenarios FS.02.02-B). Second failure. Loss or erroneous 2RC The AutoFailMS correctly identifies the loss of 2RC, but it applies an erroneous reconfiguration action. Remote pilot does not pass to manned mode. At worst undetected loss of control. Loss of RPAS in TMA or close to it. CAT Second failure is :"total loss or erroneous datalink" AutoFailMS correctly identifies the loss of datalink but it applies an erroneous reconfiguration action. After certain time ATC and/or remote pilot realizes of the loss/erroneous of datalink, Voice communication. Pilot tries to pass to manned mode, but it s not possible. Loss of control. HAZ/CAT. Uncontrolled RPAS procedure Second failure is :"loss/erroneous detect and avoid" AutoFailMS correctly identifies the loss/erroneous detect and avoid but it applies an erroneous reconfiguration action. Remote pilot is not informed of the loss/erroneous detect and avoid. Remote pilot does not assure the collision and avoid RPAS in or close to a TMA.	AT worst CAT Failure conditions that could result in one or more fatalities.	AT worst RPAS disappeared. No communication with RPAS. Total loss of flight control. Severity I Total loss of separation. Severity I	GEN_HAZ_10 GEN_HAZ_14 GEN_HAZ_16 GEN_HAZ_15 GEN_HAZ_12 GEN_HAZ_11 GEN_HAZ_3

Table 47 Erroneous/Erratic AutoFailMS combined with a second failure on board before final approach scenarios

D.2.5.3 Erroneous/Erratic AutoFailMS combined with a second failure on board during final approach

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-04.03-A	detected erroneous/erratic AutoFailMS combined with a second failure on board before final approach	The remote pilot can control the RPAS	No relevant difference with FS-04.02-A. To be confirmed after stage 7	Refer to FS-04.02-A	Refer to FS-04.02-A	Refer to FS-04.02-A
FS-04.03-B	detected erroneous/erratic AutoFailMS combined with a failure on board before final approach	The remote pilot cannot control the RPAS	No relevant difference with FS-04.02-B. To be confirmed after stage 7	Refer to FS-04.02-B	Refer to FS-04.02-B	Refer to FS-04.02-B
FS-04.03-C	undetected erroneous/erratic AutoFailMS combined with a failure on board	The remote pilot can control the RPAS	No relevant difference with FS-04.02-C. To be confirmed after stage 7	Refer to FS-04.02-C	Refer to FS-04.02-C	Refer to FS-04.02-C
FS-04.03-D	Undetected erroneous/erratic AutoFailMS combined with a failure on board in cruise	The remote pilot cannot control the RPAS	No relevant difference with FS-04.02-D. To be confirmed after stage 7	Refer to FS-04.02-D	Refer to FS-04.02-D	Refer to FS-04.02-D

Table 48 Erroneous/Erratic AutoFailMS combined with a second failure on board during final approach scenarios

D.2.5.4 Erroneous/Erratic AutoFailMS combined with a second failure on board during landing

Ident	title	Pilot control	Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-04.03-A	detected erroneous/erratic AutoFailMS combined with a second failure on board before final approach	The remote pilot can control the RPAS	No relevant difference with FS-04.02-A. To be confirmed after stage 7	Refer to FS-04.02-A	Refer to FS-04.02-A	Refer to FS-04.02-A
FS-04.03-B	detected erroneous/erratic AutoFailMS combined with a failure on board before final approach	The remote pilot cannot control the RPAS	No relevant difference with FS-04.02-B. To be confirmed after stage 7	Refer to FS-04.02-B	Refer to FS-04.02-B	Refer to FS-04.02-B
FS-04.03-C	undetected erroneous/erratic AutoFailMS combined with a failure on board	The remote pilot can control the RPAS	No relevant difference with FS-04.02-C. To be confirmed after stage 7	Refer to FS-04.02-C	Refer to FS-04.02-C	Refer to FS-04.02-C
FS-04.03-D	Undetected erroneous/erratic AutoFailMS combined with a failure on board in cruise	The remote pilot cannot control the RPAS	No relevant difference with FS-04.02-D. To be confirmed after stage 7	Refer to FS-04.02-D	Refer to FS-04.02-D	Refer to FS-04.02-D

Table 49 Erroneous/Erratic AutoFailMS combined with a second failure on board during landing scenarios

D.2.6 Inadvertent/uncommanded AutoFailMS connection/disconnection all flight phases

D.2.6.1 Safety Requirements from Inadvertent/uncommanded AutoFailMS connection/disconnection all flight phases Scenarios

Ident	title		Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-05.01-A	Detected intermittent AutoFailMS connection/disconnection.	in cruise	The pilot is aware of the connection disconnection difficulty. The pilot knows when the RPAS is in manned on in autonomous mode The pilot manages the failure in manned mode .(refer to scenarios detected loss of AutoFailMS) and monitor the aircraft in autonomous mode.(refer to normal scenarios) Increase of pilot workload	Refer to FS-02.01-A	Refer to FS-02.01-A	Refer to FS-02.01-A
FS-0501-B	Undetected intermittent AutoFailMS connection/disconnection.	in cruise	At worst the pilot is not aware of the continuous modification of autonomy level. If pilot considers to be in autonomous mode, then the remote pilot will not control the aircraft after failure at worst CAT (refer to undetected loss of AutoFailMS) If pilot considers to be in manned mode, then control actions decided by remote pilot will be superseded by the AutoFailMS. NSE (in this case, during autonomous mode, the AutoFailMS needs the pilot to confirm control actions, the pilot eventually will detect the failure)	Refer to FS-02.01-D	Refer to FS-02.01-D	Refer to FS-02.01-D
FS-05.02-A	Detected intermittent AutoFailMS connection/disconnection.	Before final approach	The pilot is aware of the connection disconnection difficulty. The pilot knows when the RPAS is in manned on in autonomous mode The pilot manages the failure in manned mode .(refer to scenarios detected loss of AutoFailMS) and monitor the aircraft in autonomous mode.(refer to normal scenarios) Increase of pilot workload	Refer to FS-02.02-A	Refer to FS-02.02-A	Refer to FS-02.02-A

Ident	title		Description of the scenario	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
FS-05.02-B	Undetected intermittent AutoFailMS connection/disconnection.	Before final approach	At worst the pilot is not aware of the continuous modification of autonomy level. If pilot considers to be in autonomous mode, then the remote pilot will not control the aircraft after failure at worst CAT (refer to undetected loss of AutoFailMS) Total loss of RPAS in TMA or close to TMA If pilot considers to be in manned mode, then control actions decided by remote pilot will be superseded by the AutoFailMS. NSE (in this case, during autonomous mode, the AutoFailMS needs the pilot to confirm control actions, the pilot eventually will detect the failure)	Refer to FS-02.02-D	Refer to FS-02.02-D	Refer to FS-02.02-D
FS-05.03-A	Detected intermittent AutoFailMS connection/disconnection.	During final approach	No relevant difference with FS-05.02-A. To be confirmed after stage 7	Refer to FS-02.03-A	Refer to FS-02.03-A	Refer to FS-02.03-A
FS-05,03-B	Undetected intermittent AutoFailMS connection/disconnection.	During final approach	No relevant difference with FS-05.02-B. To be confirmed after stage 7	Refer to FS-02.03-D	Refer to FS-02.03-D	Refer to FS-02.03-D
FS-05.04-B	Detected intermittent AutoFailMS connection/disconnection.	During landing	No relevant difference with FS-05.02-A. To be confirmed after stage 7	Refer to FS-02.04-A	Refer to FS-02.04-A	Refer to FS-02.04-A
FS-05.04-B	Undetected intermittent AutoFailMS connection/disconnection.	During landing	No relevant difference with FS-05.02-A. To be confirmed after stage 7	Refer to FS-02.04-D	Refer to FS-02.04-D	Refer to FS-02.04-D

Table 50 Erroneous/Erratic AutoFailMS combined with a second failure on board during landing scenarios

D.2.6.2 Safety Requirements from Inadvertent/uncommanded AutoFailMS connection/disconnection all flight phases

	req	Allocated to	Related to Scenarios							
			FS-05.01-A	FS-05.01-B	FS-05.02-A	FS-05.02-B	FS-05.03-A	FS-05.03-B	FS-05.04-A	FS-05.04-B
req-70	RPAS system (CDS) informs to the remote pilot of the autonomy level	RPAS systems	X	X	X	X	X	X	X	X
Req-71	RPAS system informs to the remote pilot of the modification of autonomy level	RPAS systems	X	X	X	X	X	X	X	X

Table 51 Safety Requirements from Inadvertent/uncommanded AutoFailMS connection/disconnection all flight phases

D.3 Abnormal Scenarios

D.3.1 Abnormal Scenarios

Ident	title	Description	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
A1	Loss/erroneousC2 datalink.	If the RC2 link fails then the RPAS will be unable to provide situational information to the remote pilot and will be unable to transfer control to the remote pilot. At aircraft level loss of C2 implies RPAS uncontrolled managed by AutoFailMS This scenario will be addressed in the SSA of C2 (guidelines ARP4754A/ED79A). The combination of this failure mode with loss/erroneous have been slightly described in previous scenarios. The application of ARP 4754A/ED79A requires a common mode analyses	HAZ Loss of the RPA where it can be reasonably expected that a fatality will not occur	III significant reduction in air traffic control capability	GEN_HAZ_2 GEN_HAZ_7
A2	datalink Failure	If the datalink (RPAS to ATC) fails then the remote pilot will be unable to communicate with ATC via the RPAS... As per current procedure voice as a backup.	Loss of datalink, voice as a backup. Increase on pilot workload MAJ	IV increase in air traffic controller workload	GEN_HAZ_8 GEN_HAZ_4
A3	Intruder in airspace around RPAS	This intruder would be detected by the “detect and avoid” system, which would take action to avoid the intruder. At aircraft level loss of “detect and avoid” implies RPAS cannot assures the collision avoidance. It is up to the remote pilot to ensure the collision avoidance function. This scenario will be addressed in the SSA of “detect and avoid” (guidelines ARP4754A/ED79A). The combination of this failure mode with loss/erroneous have been slightly described in previous scenarios. The application of ARP 4754A/ED79A requires a common mode analysis The failure mode is the loss of Detect and avoid	MAJ failure condition has a significant increase in remote crew workload	IV slight increase in air traffic controller workload	GEN_HAZ_13
A5	Unexpected instruction from ATC to deviate from planned flight path	ATC instruct erroneously to the RPAS. The AutoFailMS has not been designed to mitigate ATM hazards. Trajectory modifications needs to be validated by the emote pilot (design)	N/A	IV slight increase in air traffic controller workload	GEN_HAZ_12

Ident	title	Description	Safety impact in Aircraft and pilot	Safety impact in ATC and controller	HAZ
A6	Extreme weather conditions	In case of extreme weather condition, RPAS is expected to deviate. As per current practices. A loss/erroneous weather radar will be treated in the related SSA.	-	-	Out of scope
A7	Busy airspace	In case of RPAS operation in busy airspace. RPAS is expected to be transparent to ATC, in case of failure of RPAS certain procedures are expected from ATC (uncontrolled, disappeared RPAS, etc) ATM needs to assure the capacity to apply these procedure. ATC can define a "maximum" level of PAS allowed in certain airspace.	-	At worst I Total loss of separation	GEN_HAZ_15
A8	Incorrect maintenance of aircraft equipment	The AutoFailMS has not been designed to detect maintenance failure. In case of erroneous AutoFailMS the information is stored in the BITE system, the BITE information is used by maintenance team.	-	-	Out of scope
A9	Incorrect actions by remote pilot	AutoFailMS has not been designed to manage the pilot failures.	-	-	Out of scope

Table 52 Abnormal scenarios

D.3.2 Requirements from Abnormal Scenarios

	req	Allocated to	Related to Scenarios								
			A1	A2	A3	A4	A5	A6	A7	A8	A9
req-80	After loss of datalink voice shall be designed as a back up	RPAS systems		x							
Req-81	Trajectory modifications shall be validated by the remote pilot	Remote pilot					x				
Req-82	ATM shall define a "maximum" level of RPAS allowed in certain airspace.	ATC							x		

Table 53 Requirements from abnormal scenarios

Appendix E RPAS Operation Hazards Classification

E.1 Eurocae UAV Severity matrix

This ER-010 [16] identifies the risk scenarios for unmanned aircraft and their outcomes. According to ER-010 [16] RPAS performs the following functions from immediately after take-off:

- The following of a flight path
- The assurance of safe separation and the avoidance of collision
- Landing

The failure scenarios for the high-level functions failure for an UAV are:

- After occurrence of the failure, the unmanned aircraft is still able to continue its flight according to its intended and planned flight plan FP 1
- After occurrence of the failure, the UAV is not able to continue the flight […] leading to
  - The UAV follows an unplanned but predictable and safe flight plan in accordance with Emergency Procedures FP 2.1
  - The UAV does not follow its intended and planned flight with the required accuracy while its attitude is still under control, which could lead UAV to fly out of the assigned airspace or even CFIT. FP 2.2
  - The UAV enters an uncontrolled flight o taxiing FP 2.3
- After occurrence of the failure, the UAV is still able to land on the normally planned landing site L1
- After occurrence of the failure the UAV is not able to land in the normally planned landing site leading to:
  - The UAV can land or crash at a pre-planned uninhabited emergency site: L2.1
  - The UAV cannot land or crash at a pre-planned u uninhabited emergency site but the remote pilot has still means to select an unplanned uninhabited d emergency site where to land o to crash the UAV L2.2
  - The UAV has neither option L2.1 not L 2.2 and crashes on an uncontrolled manner to at a location totally unpredictable L2.3

Each of these may also have an effect on Separation Avoidance (SA) and Collision Avoidance (CA):

These scenarios are classified according to five levels of severity

Severity	Definition
Class I:	Failure condition that is expected to directly or indirectly hit of third parties in the air or on the ground.
Class II:	Failure condition that is not expected to lead to physical hit of third parties in the air or on the ground but it is expected to lead to stress to third parties in the air or on the ground as a result of nearby collision or crash nearby third parties
Class III	Failure condition that is not expected to lead to physical hit of third parties in the air or on the ground nor to stress to third partied in the air or on the ground but it is expected to lead to a significant increase in workload to RPAS crew, to ATC, …

Severity	Definition
Class IV:	Failure Condition that is not expected to lead to physical hit of third parties in the air or on the ground nor to stress to third parties in the air or on the ground but is expected to lead to a slight increase in workload to RPAS crew or ATC
Class V:	Failure Condition that is not expected to lead to physical hit nor stress to third parties in the air or on the ground and will not increase the workload to RPAS or ATC

Table 54 Severity matrix as per ER-010 [16]

The scenarios are classified as follows:

		High Level End effect of UAS failure				Potential Effect to people		Proposed Class (see A4.4)
		FP	L	SA	CA	Ground	Air	
1	1.1	FP1 (per flight path)	L1 (Normal)	OK	OK	None	None	V
2	1.2	FP1 (per flight path)	L1 (Normal)	NOK	OK	None	Stress	II
3	1.3	FP1 (per flight path)	L1 (Normal)	OK	NOK	None	None	IV
4	1.4	FP1 (per flight path)	L1 (Normal)	NOK	NOK	Physical	Physical	I
5	2.1	FP2.1 (Emergency)	L1 (Normal) or L2.1 (Predefined)	OK	OK	None	None	IV
6	2.2	FP2.1 (Emergency)	L1 (Normal) or L2.1 (Predefined)	NOK	OK	None	Stress	II
7	2.3	FP2.1 (Emergency)	L1 (Normal) or L2.1 (Predefined)	OK	NOK	None	None	III
8	2.4	FP2.1 (Emergency)	L1 (Normal) or L2.1 (Predefined)	NOK	NOK	Physical	Physical	I
9	3.1	FP2.1 (Emergency)	L2.2 (Unplanned selected)	OK	OK	None	None	III
10	3.2	FP2.1 (Emergency)	L2.2 (Unplanned selected)	NOK	OK	None	Stress	II
11	3.3	FP2.1 (Emergency)	L2.2 (Unplanned selected)	OK	NOK	None	None	III
12	3.4	FP2.1 (Emergency)	L2.2 (Unplanned selected)	NOK	NOK	Physical	Physical	I
13	4.1	FP2.2 (inaccurate navigation)	-	-	-	-	-	I (Worst case)
14	7.1	FP2.3 (Uncontrolled flight)	L2.3 (Unplanned unselected)	-	-	Physical	Physical	I

Table 55 Severity allocation to failure scenarios for UAV operations in ER-010 [16]

E.2 JARUS RPAS Severity matrix

JARUS presents an update on the definition of CAT, HAZ, MAH, MIN and NSE currently on the ARPS 4754ª. These definitions are updated to include the RPAS operations.

Severity	Definition
NSE	Failure conditions that would have no effect on safety. For example, failure conditions that would not affect the operational capability of the RPAS or increase the remote crew workload.
MIN	Failure conditions that would not significantly reduce RPAS safety and that involve remote crew actions that are within their capabilities. Minor failure conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in remote crew workload, such as flight plan changes.
MAJ	Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins, functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote crew efficiency. (E.g. Total loss of communications with ATC.)
HAZ	Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be the following: (i) Loss of the RPA where it can be reasonably expected that a fatality will not occur, or (ii) A large decrease on safety margins or (iii) High workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely. Possible examples of 'a large reduction in safety margins or functional capabilities' might include: • Unintended deviations from the flight path if operating in the open airspace; • Potential loss of safe separation (e.g. loss of D&A, incorrect altitude reporting); • Activation of an emergency recovery capability potentially resulting in loss of the RPA where a fatality is not expected to occur.
CAT	Failure conditions that could result in one or more fatalities. This refers to one or more fatalities that can occur either in the air (mid-air collision) or on the ground. Where type-certification does not stipulate any limitations on type of airspace to be used and areas to be overflow, the design assumption must be that any failure condition leading to a crash, mid-air collision or forced landing, is potentially fatal. Examples of potentially Catastrophic failure conditions include: • Loss of control leading to impact with the surface outside of a pre-defined safe area; • Loss of the command & control datalink (Complexity Level I & II) outside of a pre-defined safe area; • Loss of control leading to the inability of a RPA to be contained within a pre-defined segregated area; • Malfunction of a D&A system that actively guides the RPA towards neighboring traffic.

Table 56 Severity matrix as per JARUS [9]

JARUS suggests as well quantitative (pro/FH) and qualitative (DAL) objective for theses failure conditions.

- For quantitative objective:

Aircraft type	Complexity Level	Accident rate (pfh) All Causes *(Note 1&4)*	% due to Systems (10%) *(Note 2)*	Number of Potential Failure Conditions	Probability of a single Catastrophic failure condition
Manned CS-25		$1x10^{-6}$	$1x10^{-1}$	100 (10^{-2})	$1x10^{-9}$
RPAS CS-25	N/A *(Note 3)*	$1x10^{-6}$	$1x10^{-1}$	100 (10^{-2})	$1x10^{-9}$

Table 57 Quantitative safety objective for CAT as per JARUS [9]

Safety objective for non catastrophic condition might be derived as in ARP4754A/ED79A (10E-7 for HAZ, 10E-05 for MAJ, 10E-03 for MIN, etc…)

Classification of failure Conditions	No Safety Effect	<....Minor….>	<..Major...>	<Hazardous.>	<Catastrophic>
Allowable Quantitative Probability	No Probability Requirement	Probable	Remote	Extremely Remote	Extremely Improbable
Effect on the Aircraft	No Effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Flight into terrain (Normally with hull loss)

Table 58 Safety objective for NSE, MIN, MAJ, HAZ and CAT as per JARUS [9]

- For qualitative objective:

DAL allocation under revision

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

Table 59 Qualitative Safety objective for NSE, MIN, MAJ, HAZ and CAT as per JARUS [9]

Appendix F ED-78A Guidelines for Approval of the provision and use of Air Traffic services supported by data communications.

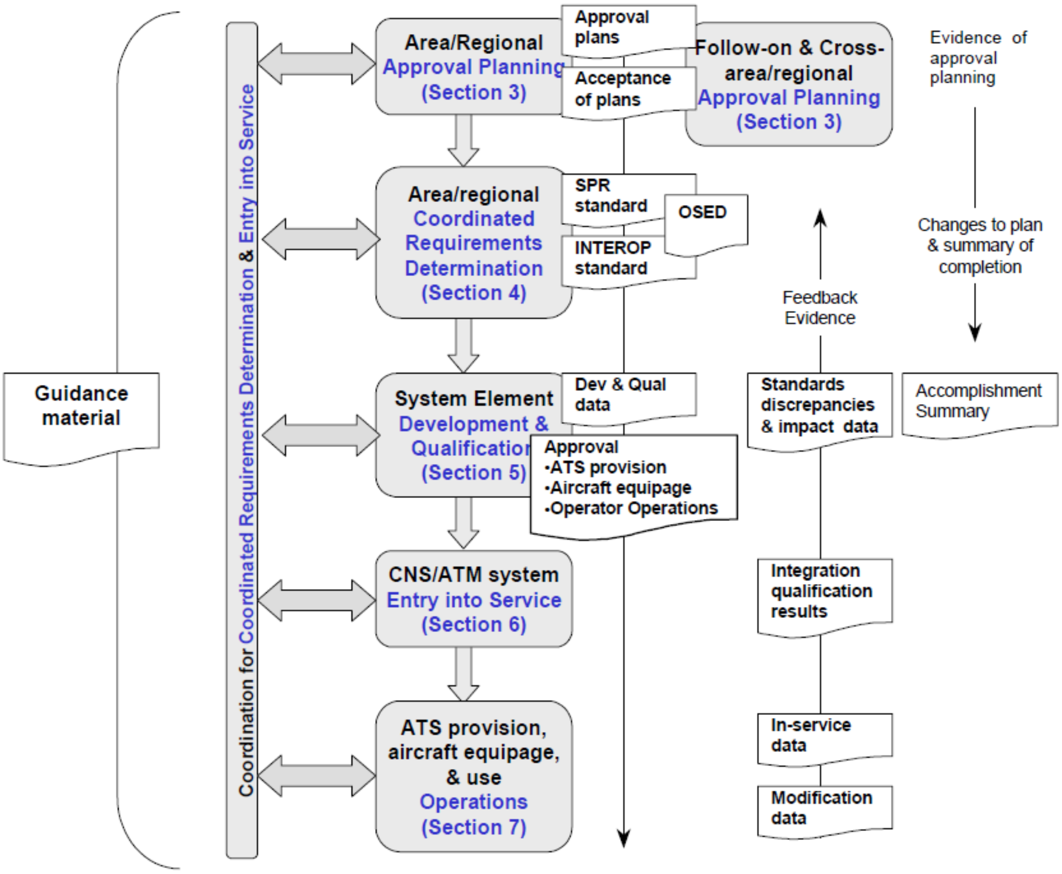


Figure 14 Process for ATS supported by DATA communication *[17]*