Joint Authorities for Rulemaking of Unmanned Systems

Working Group 6 – Safety & Risk Assessment

SCOPING PAPER
to
AMC RPAS.1309
Issue 2

Safety Assessment of Remotely Piloted Aircraft Systems

Amendment Record

Issue	Date	Reason for change
Issue 1	January 2014	Issued for public consultation.
Issue 2	November 2015	Issued with changes incorporated following public consultation

Produced by JARUS WG-6:

Core Group:

Jeff	Bergson	FAA
Alexandra	Florin	EASA
Jonathan	Hughes	UK-CAA
Lorenzo	Murzilli	FOCA
Angela	Rapaccini	ENAC
Wes	Ryan	FAA

With contributions from:

Nick	Brewer	UK-CAA
David	Haddon	EASA
Jose	Ailton	ANAC Brazil
Adrie	Beuk	CAA-NL
Aleš	Böhm	CAA-CZ
Hans	Brants	NLR
Gerry	Corbett	UK-CAA
Riccardo	Delise	ENAC
Keith	Dodson	UK-CAA
Markus	Farner	FOCA
Vladimír	Filip	CAA-CZ
Mike	Gadd	UK-CAA
Jean-Pierre	Heckman	
Thibault	Lang	ONERA
Alistair	Maxwell	UK-CAA
Reto	Senn	FOCA
Jozef	Van Baal	CAA-NL

CONTENTS

LIST OF TABLES

LIST OF FIGURES

FORWARD

(a) Issue 1 of AMC RPAS.1309 together with the accompanying 'Scoping Paper' was published on 28 January 2014 for public consultation. Following closure of the comment period (28 March 2014), over 1000 comments were received in total. The issues raised by these comments ranged from fundamental disagreements with the concept developed, proposals of a technical nature, the need for more clarification, explanation or justification, and comments of an editorial nature.

(b) It was clear that many of the concept related comments were based on a misunderstanding of the applicability of AMC RPAS.1309. It was never the intent that all RPAS would be subject to type-certification and adherence to AMC RPAS.1309 as a means of compliance.

(c) At the time of writing, the EC/EASA/JARUS are currently developing a regulatory concept for RPAS that introduces proportionality by creating RPAS risk categories. The details remain to be defined but can be thought of as follows:

(1) Open Category - Represents very low risk operations. No/limited airworthiness regulations are envisaged and 1309 is not applicable.

(2) Specific Category – Operations that would present a limited risk to people and property. Risk mitigation would be required, mainly through operational restrictions and limitations, which may include 1309, depending on the type of operation and the nature of the risks.

(3) Regulated Category – Follows the traditional approach to aircraft regulation, including type-certification where compliance with 1309 would be mandatory.

(d) AMC RPAS .1309 has been developed as an integral part of a type-certification process (Regulated Category). It is a means of compliance to a 1309 airworthiness requirement, where the requirement will be defined or modified from the equivalent manned CS, as part of the tailoring processes necessary to establish the individual RPAS type-certification basis. The AMC therefore aims to meet a medium/long-term objective of the RPAS industry for full integration with manned aviation. In many cases, including small RPAS or RPAS operating in remote areas, this AMC (or indeed type-certification) may not be the most appropriate nor cost-effective process to gain approval. Alternative procedures that fit into the Open or Specific Categories have been/are being developed specifically for small RPA or those with limited operational capabilities. Applicants must be conversant with these other approaches and select the one appropriate to their specific RPAS and intended operation.

(e) The applicability of AMC RPAS.1309 is unrestricted, and can be used as a means of compliance in the regulated category or voluntarily in any other category, irrespective of size or weight. This was a deliberate act by the JARUS group so as not to restrict the possibility of type-certification to any RPAS, as there may be some types of operations where high airworthiness standards would be expected (e.g. flight over crowds of people, operations in congested airspace, international flights, etc.), or where type-certification may ease the approval process for future variants or facilitate export markets.

(f) The overriding objective which forms the basis of AMC RPAS.1309, is to ensure that the current overall accident rate/category attained by manned aircraft is not increased with the introduction of

civil RPAS. In the absence of actual civil RPAS experience, the WG has had to speculate on the likely reaction from the general and flying public on the acceptance of RPAS. Some knowledge is drawn from freely available censuses specially taken to gauge public reaction to the introduction of RPAS; other information is based on experiences with other industries and other technologies.

(g) Where RPAS have an increased reliance on complex systems to avoid or mitigate potential hazards, compared to manned aircraft of equivalent category, account must be taken of this fact in defining safety targets and development rigour objectives by assigning Development Assurance Levels (DALs). However, in response to comments received, one significant change introduced in Issue 2, is to reduce the number of complexity levels from 4 to 3. This will help in establishing the type-certification basis and was possible following a change to the assigned DALs to provide better coherency with the safety objectives.

(h) Many of the detailed technical and editorial comments received have not been addressed in this Issue 2. JARUS is committed to establishing a forum with industry to try to reach consensus on an RPAS regulatory framework, including airworthiness and the system safety assessment. This document is JARUS's views on how to perform an RPAS System Safety Assessment and as such is an input into this process and a starting point for further debate. Changes of a detailed nature are therefore seen as premature until an overall regulatory concept is established and agreed. The comments received will however be retained and may be used in future developments.

1. EXECUTIVE SUMMARY

(a) This paper outlines a methodology to enable civil RPAS to show compliance with the 1309 safety assessment of the applicable airworthiness code. It will therefore facilitate the applicant in gaining type-certification approval, which is a pre-condition to gaining full integration of RPAS with manned aircraft within unsegregated airspace. Gaining type-certification approval will also minimise the imposition of operational restrictions and reduce barriers to export, thereby maximising the potential market for individual RPAS types.

(b) The overriding safety objective adopted in this paper aims to ensure that the current (manned aircraft) accident rate for the fleet, together with those of each aircraft category, does not increase with the introduction of civil RPAS. Embedding this objective as a foundation within the rationale, and by utilising existing manned aircraft acceptable means of compliance, where practicable, enables RPAS to readily show equivalence with manned aircraft.

(c) In the absence of other criteria, some assumptions have been made regarding the acceptability of RPAS safety targets to both the general and flying public and a cautious approach has been taken to reflect many of the challenges still facing the introduction of civil RPAS. Basing safety targets on existing achieved manned aircraft accident rates may not fully reflect the public's apprehension towards new technologies and automated systems, but is believed to be a balanced approach between the often conflicting needs of safety and commerce and is considered to be a defendable position.

2. DEFINITIONS

(a) ***Collision Avoidance:*** The capability to take the appropriate avoidance action. Designed to act only if Separation Assurance has been breached.

(b) ***Complexity*****:** An attribute of functions, systems or items which makes their operation, failure modes or failure effects difficult to comprehend without the aid of analytical methods. (Ref. ED-79A/ARP4754A).

(c) ***Detect and Avoid (DAA):*** 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').[1]

(d) ***Development Assurance:*** All of those planned and systematic actions used 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 (Ref. ED-79A/ARP4754A).

(e) ***Emergency Recovery Capability***. A means or function that ends the flight following a potentially Catastrophic failure condition, with the intent of reducing the danger to third parties on the ground and in the air. (For example, by use of a ballistic parachute recovery system or through pre-defined emergency recovery procedures).

(f) ***Primary function***: A function installed to comply with applicable regulations for the required function and provides the most pertinent controls or information instantly and directly to the pilot. For example, the Primary Flight Display (PFD) is a single physical unit that always provides the primary display and complies with the requirements of all the following: altitude, airspeed, aircraft heading (direction) and attitude. The PFD is located directly in front of the pilot and used instantly and first by the pilot. A standby or another display intended to be used in the event of failure of the PFD or as a cross reference is an example of a secondary system. For example, a brake control system normally uses the electronic brake system most of the time because of its better performance, but it does not comply with all the requirements. In this case, the mechanical brakes are used as the backup systems; yet, it is consider the primary with regard to meeting the requirements and the electronic brake system is the secondary.

(g) ***Primary system***: A system that provides the primary function.

(h) ***Remote pilot station (RPS)***: The component of the remotely piloted aircraft system containing the equipment used to pilot the remotely piloted aircraft.

[1] The DAA 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.

(i) ***Remotely Piloted Aircraft (RPA)***: An unmanned aircraft which is piloted from a remote pilot station. (Note – this is a subcategory of Unmanned Aircraft).

(j) ***Remotely Piloted Aircraft System (RPAS)*:** A remotely piloted aircraft, its associated remote pilot station(s), the required command and control links and any other components as specified in the type design.

(k) ***Secondary system***: A redundancy system that provides the same function as the primary system.

(l) ***Separation Assurance:*** The capability to maintain safe separation from other aircraft in compliance with the applicable rules of flight.

(m) ***Unmanned Aircraft (UA)***: An aircraft which is intended to operate with no pilot on-board.

(n) ***Unmanned Aircraft System (UAS):*** An aircraft and its associated elements which is operated with no pilot on-board.

3. INTRODUCTION

(a) This document has been produced by JARUS WG-6. It complements AMC RPAS.1309 (Ref 1.) by providing the background, development history and justification for the approach adopted in creating a system safety assessment methodology for Remotely Piloted Aircraft Systems (RPAS). Together, both documents provide a general consensus of Authority members on an approach that could be adopted for RPAS System Safety Assessment.

(b) AMC RPAS.1309 is applicable to RPAS of all categories. It does not, however, address autonomous aircraft, as described in ICAO Circular 328 as a UAS that does not allow pilot intervention in the management of the flight. Only RPAS will be able to integrate into the international civil aviation system in the foreseeable future.

(c) The focus of AMC RPAS.1309 is on gaining type-certification, which is a precondition for full integration of RPA with manned aircraft in unsegregated airspace. It establishes an acceptable means of compliance, but not the only means of compliance, to enable a RPAS or component product to show compliance specifically with CS/FAR xx.1309(b)[2] of the applicable airworthiness requirements.

(d) It has been recognised that current technology shortfalls, for example, Detect & Avoid (DAA) systems, may prevent full airspace integration in the short-term. Alternative procedures that allow less capable RPAS to undergo a step-by-step approach to certification have been developed by many authorities, enabling early entry into service, and which can later be upgraded to provide full certification. However, while these alternative procedures can be used to gain limited acceptance, they may be subjected to operational limitations aimed at ensuring safe flight and may limit flight operations to within segregated airspace, in remote areas and/or in line-of-sight of the ground based remote pilot. Applicants should ensure that they are fully conversant with these alternatives before embarking on a type-certification project.

[2] 'xx.1309' refers to paragraph 1309 of the applicable manned airworthiness code (e.g. FAR/CS **23**.1309, or FAR/CS **27**.1309, etc.).

4. BACKGROUND

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

(b) Unmanned aircraft are defined in ICAO (Ref 2) as "*An aircraft which is intended to operate with no pilot on-board*". The implication being that UAS may in the future operate with people on-board, including passengers. The primary intent of AMC RPAS.1309 and this paper, is not to look this far into the future, but to focus on RPAS that are fully unmanned and undertaking an aerial work task for commercial purposes. However, the arguments put forward in this paper will lead to the conclusion that all UAS types could be addressed under the same general system safety assessment principles.

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

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

5. REGULATORY PRINCIPLES & OBJECTIVES

(a) RPAS offer the potential to undertake a wide range of new and existing aerial tasks more efficiently and economically than existing manned aircraft do today. They are seen as the next major evolutionary step in aircraft design. The future market potential of RPAS has been forecast to grow rapidly in this decade, creating jobs and wealth for those in a position to exploit this new technology. However, advanced technologies should not be allowed to impact society by imposing intolerable risks on people and property. It is therefore incumbent on those responsible for creating the hazards (RPAS industry), and those responsible for regulating those hazards (EC/EASA/FAA/NAAs), to take a proactive stance to ensure that adequate controls are put in place to protect people and property from the consequences of those hazards, and in particular those that have no involvement in RPAS activities.

(b) As civil RPAS have developed from a military need, it would be logical to start by understanding how military authorities control the hazards and whether such an approach is transferrable to the civil field. Historically, military/state airworthiness requirements have been developed independently and have focused on different objectives. Approval of aircraft by military authorities is generally through the use of a 'safety case' which takes a total system view of the aircraft and its operation in determining acceptable safety risks and operational limitations, often focussing on a particular mission type. Military/state airworthiness standards were generally considered to offer a lower safety standard than those accepted by civil authorities. This was justified on the grounds that military/state aircraft flying hours are limited and are specifically for the security, safety and emergency medical treatment of the general public, which benefits the whole community. This is not true for civil aircraft whose operation is intended primarily for commercial purposes.

(c) While this approach is well suited to military needs, the civil regulatory framework needs to consider other factors such as commercial competition, adaptability of aircraft to multiple roles and changing customer needs, global acceptance, free movement of products, and a level playing field for all. (For a fuller analysis of the different needs, see Ref 3.).

(d) Military/State[3] aviation safety has increased over the last decade or so, mainly as a result of its lost exemption from health & safety legislation, and now aims to mirror civil safety standards. As it may be difficult for the general public to differentiate between military and civil RPAS, it is likely that any fatal accidents would tarnish the whole industry. Having a single regulatory environment for all RPAS therefore has a certain attraction and may be a worthy goal, but it must be the case that the highest safety standards prevail and accomplishment of this goal should not adversely impact on the operational utility of military/state services.

(e) ICAO, together with FAA, EASA and NAAs, have developed general principles to guide development of the civil RPAS regulatory framework. It is not the intent of this document to re-visit the development of these principles per se, but are discussed in some depth to aid understanding of

[3] In the USA, this is equivalent to 'public aircraft operations' i.e. aircraft operations other than for civil purposes.

the overall approach being proposed. The fact that these principles have received general acceptance is seen as a sound footing and confirmation that industry is generally supportive of the direction taken.

(f) Individual top level principles cited by ICAO, EASA and UK-CAA are as follows:

ICAO Circular 328:

2.8 The principal objective of the aviation regulatory framework is to achieve and maintain the highest possible and uniform level of safety. In the case of UAS, this means ensuring the safety of any other airspace user as well as the safety of persons and property on the ground.

3.1 UAS will operate in accordance with ICAO standards that exist for manned aircraft as well as any special and specific standards that address the operational, legal and safety differences between manned and unmanned aircraft operations…

EASA Airworthiness Policy E.Y01301:

4.1 …A civil UAS must not increase the risk to people or property on the ground compared with manned aircraft of equivalent category.

Airworthiness standards should be set to be no less demanding than those currently applied to comparable manned aircraft nor should they penalise UAS by requiring compliance with higher standards simply because technology permits

CAA CAP 722:

1.1 It is CAA policy that UAS operating in the UK must meet at least the same safety and operational standards as manned aircraft. Thus, UAS operations must be as safe as manned aircraft insofar as they must not present or create a greater hazard to persons, property, vehicles or vessels, whilst in the air or on the ground, than that attributable to the operations of manned aircraft of equivalent class or category.

(g) These statements can be synthesized into the following basic principles for the development of the civil regulatory framework, as follows:

1. The civil framework must set and maintain a high level of safety.

a) It is recognised that in the long-term UAS may contribute to enhancing safety (e.g. reduce/mitigate Human Factors (HF) accident causes, replace "see and avoid" by technology, replace larger manned aircraft in the fleet, etc.). However, in the short-term, a cautious approach is needed since we know that the current safety record of military UAS do not reach civil standards (although it is improving as systems mature – See Figure 1). Furthermore, initial applicants for type-certification may not have the necessary aviation background and

familiarity with civil design and airworthiness standards that define expectations for safety of a civil aircraft.

b) The general public's acceptance of civil RPAS will be subject to many and varying factors including; safety, noise, intrusion/privacy, etc. Here we focus on the design and airworthiness aspects of safety, but as there is little existing experience on which to base a rational judgement, the general and flying public's demands on RPAS safety can only largely be guessed at. The initial reaction to all things automated tends to be one of apprehension and, due to their novelty, RPAS will attract particular media attention. It may only take one high-profile accident (fatal or not) before the public questions their safety. A cautious approach is therefore necessary to avoid any potential public backlash to the introduction of civil RPAS, and robust arguments need to be put in place in order to defend the position taken.

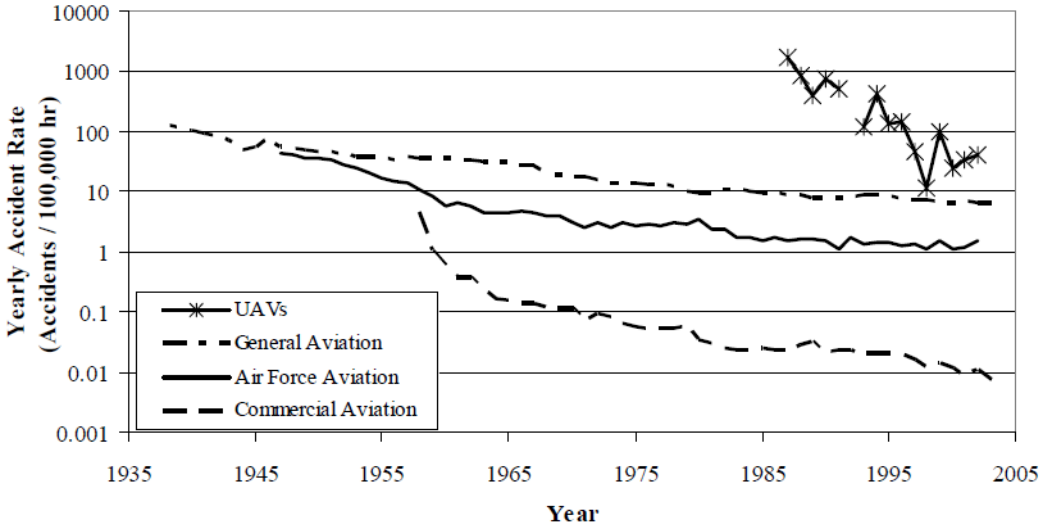


Figure 1: Comparison of Accident Rate Trends between Several Categories of Aircraft (Ref. 4)

2. <u>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.</u>

a) To understand this statement, an understanding of the existing risk to people in the air and on the ground is essential and how that risk is managed. Some approaches to the RPAS 1309 problem start with defining what an acceptable level of risk is in quantitative terms, focussing directly on the risk to people and property. In the case of ground risk, some previous approaches have focused on defining lethal areas and making assumptions of the population density to be overflown. However, this is not necessary for the following reasons:

b) Today we measure safety in terms of the number of accidents and fatal accidents per flight hour or number of flights.

c) The general public perceive safety as the potential for injury/death and in absolute terms. If the number of UAS crashes where the general public could be at risk was allowed to increase (irrespective of the number of fatalities) there would be a perception of reduced safety; the more crashes there are the more likely you are to be hit at some time in the future!

d) The general public's perception of aviation safety is influenced by a number of factors: the number of people killed or injured; the likelihood of being in that position yourself; and the amount of direct control one has in the aircraft's operation. If you accept that the media reflects public opinion, then this is clearly demonstrated (e.g. an airliner fatal accident will make more headlines than that of a GA aircraft). As safety perception is therefore linked to the category of aircraft and type of operation, it would be inappropriate to treat all aircraft the same. Safety should therefore focus on the risks to persons in the air and on the ground and, in the absence of any better criteria, requiring a level of safety equivalent to manned aircraft of the same category as an objective is a defendable position.

3. The regulatory framework for RPAS should build on existing manned standards.

a) Regulatory Authorities should not stand in the way of progress but be prepared to modify the regulatory framework to allow the RPAS industry to certificate its products and compete on equal terms with manned aircraft. There needs to be fair, consistent and equitable treatment of all stakeholders and all categories of aircraft (manned and unmanned).

b) RPAS development and integration should be considered as an evolutionary step in aviation. The approach being established by many states is built upon existing ICAO standards and recommended practices and aims to insert RPAS into the existing aviation framework rather than to develop a separate or parallel framework. This approach includes the principles around the international recognition of Certificates of Airworthiness (CofA), in that any aircraft having been shown to meet the defined standard and issued with a CofA may be operated, subject to compliance with any applicable limitations (airworthiness or operational) and necessary permissions, in any contracting state's airspace.

c) It should be noted that ICAO has recently adopted changes to Annex 2 'Rules of the air' by creating Appendix 4 specifically addressing UAS. While the Appendix provides specific rules related to RPAS that are not fully aligned with those of manned aircraft, it can perhaps be seen as an enabling step which recognises established procedures (e.g. CofA), but also creates additional safeguards in recognition of the novelty and growing maturity of RPAS.

d) Just how these principles can be applied and demonstrated to be met is the subject of many coordination tasks and working group activities, not least as the end results must withstand scrutiny from both the manned and unmanned communities.

e) This paper describes how the above principles have been embedded into a methodology to support the showing of compliance for type certification of RPAS systems.

6. APPLICABILITY

(a) The methodology outlined in this paper is applicable to all RPAS and addresses all RPAS systems whether located on-board or remote from the RPA.

(b) ICAO as well as many civil authorities are only seriously considering RPAS (as opposed to UAS) for integration into unsegregated airspace due to the need for remote pilot intervention and to be able to respond to ATC instructions in real time. Autonomous UAS are therefore not considered.

(c) A review of 1309 in each of the airworthiness codes concluded that the requirement was sufficiently generic to be applicable to all RPAS. In some codes, the level of detail regarding the scope and depth of a system safety assessment was not specifically defined, but the group concluded that such changes in the requirements were part of the airworthiness tailoring process necessary to turn a manned CS/14 CFR part into an equivalent type-certification basis for a RPAS. The prime focus of WG-6's activities was then to determine how compliance with the 1309 system safety assessment rules should be shown for RPAS.

(d) Two alternate approaches were investigated:

1. Develop a dedicated means of compliance that is limited in scope to specific systems of the RPAS that perform the functions of an on-board pilot, together with supporting systems. Other systems would be required to show compliance using the existing applicable AMC/AC developed for manned aircraft.

2. Develop a dedicated means of compliance that is similar in scope to the base code, but extended to cover the whole RPAS.

(e) The first approach was initially considered a more relevant focus to develop AMC RPAS.1309 with applicability only to RPAS specific systems and their supporting systems. As RPAS specific systems are any system that performs the equivalent role to that of the on-board pilot in a manned aircraft, these systems are unlikely to be found on-board a manned aircraft.

(f) Such a methodology may ease type-certification by allowing an existing aircraft to be developed into a RPAS. For example, an existing manned aircraft will have systems that have been shown to have sufficient robustness for civil certification. AMC RPAS.1309 would then only focus on those specific RPAS systems and any supporting systems that would be fitted to that legacy aircraft in order to make it a RPAS. This would include systems on-board the RPA, the data link and the Remote Pilot Station. Systems that are common to the RPAS and the manned aircraft variant would lie outside the scope of AMC RPAS.1309 and be subject to the existing guidance of AC/AMC xx.1309. It was not envisaged that levels of systems availability and integrity of the RPAS variant be reduced below that of the existing manned aircraft.

(g) The second option took the view that what is currently acceptable for certification of existing manned aircraft systems may not be appropriate for RPAS when considering the interrelationship of systems and equipment, both manned and unmanned, and the lack of an on-board pilot. Certification of manned aircraft systems and equipment often assumes the presence of the pilot can be used as

mitigation in failure scenarios. For example, if an autopilot system in a manned aircraft fails, the pilot is able to disengage the AP and resume manual control. The assumptions used in certificating manned aircraft systems may therefore be invalid if the pilot's actions are now enabled through a datalink, which analysis may show to have insufficient availability, integrity, reliability or unacceptable latency.

(h) A review of aircraft systems and the safety analysis performed concluded that most systems subject to xx.1309 would be impacted in some way in the development of a RPAS. Furthermore, splitting the system safety analysis into two distinct means of compliance, with possibly different safety objectives, would inevitably lead to considerable discussion during the certification programme.

(i) The approach adopted by WG-6 was therefore based on Option 2 and to make AMC RPAS.1309 applicability similar in scope to the base code, but extended to cover the whole RPAS. The certificating Authority may give credit to a legacy system or system element that is identical or functionally similar to that previously designed for manned aircraft and has been shown to be reliable in-service. In this case, the onus on proof would rest with the applicant.

(i) AMC RPAS.1309 does not cover capability requirements for RPAS systems (e.g. Detect and Avoid systems, flight control systems, data link, and Remote Pilot Station systems). These will be established elsewhere e.g. JARUS WG-4 for DAA.

(j) Within Europe, EU regulation 216/2008 specifically states as an objective “to promote cost efficiency in the regulatory and certification process and to avoid duplication at national and European level.” Therefore existing national ‘Health and Safety at work’ legislation will remain applicable to ground equipment and personnel and AMC RPAS.1309 does not address this aspect. However the effects of a Remote Pilot Station failure/malfunction on the ability of the flight crew to perform their duties (e.g. workload and Human Factors), and the effect on the RPA, will need to be assessed as part of the system safety analysis covered by AMC RPAS.1309.

7. COMPLEXITY LEVELS

(a) Certification codes traditionally discriminate between different classes of aircraft based on the type of aircraft, number of passengers, weight and number of engines/engine technology. The underlying assumption in the selection of these discriminators is that they indirectly indicate the complexity of systems installed, the type of use of the aircraft and system reliability. System availability and integrity requirements can then be set accordingly to meet expected safety targets. This concept has been questioned when applied to modern manned aircraft, where higher levels and complexity of installed systems is the norm, irrespective of weight or engine technology. This has been recognised by the Authorities who have already initiated a task aimed at reorganising CS/14 CFR part 23 based on alternative criteria such as aircraft performance and complexity. However, at the time of writing, this initiative has not progressed to the stage where it could be considered for RPAS.

(b) Using the traditional approach, the assumption of simplicity when applied to small RPAS is invalid, as even small RPAS may be equipped with advanced technologies such as fly-by-wire systems, have a data link and ground control station, and may have on-board automated functions. The need to introduce a complexity level criterion for RPAS was therefore considered necessary. Furthermore, prior to adopting the complexity level criterion, the assignment of integrity levels, and in particular DALs, was problematic in balancing the twin objectives of showing equivalence with manned aircraft and reflecting RPAS's increased reliance on systems availability and integrity. Therefore, although the original manned aircraft classification concept can be retained as the means for establishing the base airworthiness code, a new method to classify the RPAS based on three complexity levels has been defined as follows:

1. Complexity level I:

   An RPAS that has some automatic functions with limited authority on the RPA and limited capability of automatic execution of a mission. Independent manual reversion is always provided. The use of software and Airborne Electronic Hardware (AEH) is limited.

   Control by the pilot does not mean that the pilot must be hands-on and have direct manual control at all times. Automatic functions must be of simple design to meet the 10 or fewer catastrophic failure conditions assumed in Table 4. A Complexity Level I RPAS may make use of computer-based interfaces (e.g. point-and-click) for routine remote pilot commands.

2. Complexity level II:

   Assigned to any other RPAS not classifiable as Level I. The control systems are likely to have full authority on RPAS flight management and are capable of automatic execution of a mission. In the event of a failure, the pilot can intervene if required, unless the failure condition can be shown to be extremely improbable. These RPAS are expected to make extensive use of software and AEH.

3 Complexity level III:

Assigned to those UAS that are autonomous[4]. This category of UAS is not covered by ICAO and is not covered in this document at the present time.

A Complexity Level III UAS is defined as an 'Autonomous aircraft' in ICAO Circular 328.

(c) The complexity levels together with the relative authority of the UAS and remote pilot can be seen pictorially in Figure 2.

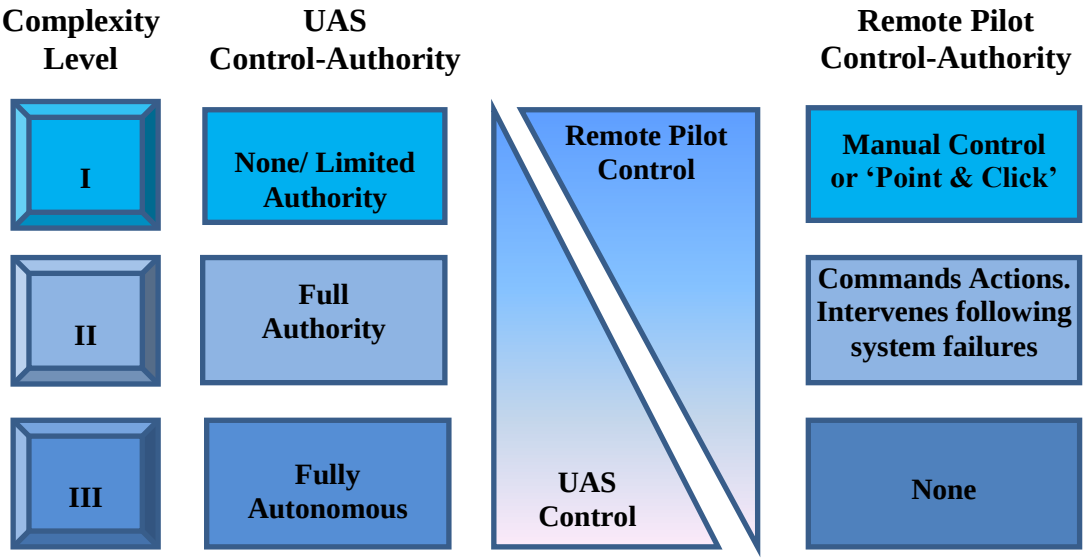


Figure 2: Correlation of UAS Complexity levels with Pilot & UAS Authority

8. FAILURE CONDITION CLASSIFICATION

(a) The familiar failure condition classifications (Catastrophic, Hazardous, Major, Minor and No safety effect) have been retained from manned aviation requirements.

(b) The classification of a failure condition does not depend on whether a system or function is required by specific regulation. Some systems required by regulation, such as position lights and transponders, may have the potential for only minor failure conditions. Conversely, other systems not required by any specific regulation, such as automatic take-off and landing systems may have the potential for Catastrophic failure conditions.

(c) Failure Conditions are classified according to the severity of their effects as follows:

[4] Autonomous aircraft: An unmanned aircraft that does not allow pilot intervention in the management of the flight. (Ref. ICAO Manual on RPAS Doc 10019)

(1) No safety effect

Failure conditions that would have no effect on safety. For example, failure conditions that would not affect the operational capability of the RPAS or increase remote crew workload.

(2) Minor

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.

(3) Major

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.

(4) Hazardous

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 reduction in safety margins or functional capabilities, or

(iii) High workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely.

(5) Catastrophic

Failure conditions that could result in one or more fatalities.

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

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

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

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

(f) For some simple RPAS, a qualitative analysis might be acceptable provided that current commonly accepted industry practices are adopted.

(g) Salient points to note in the definitions and example failure condition classifications are given below.

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

1. No Safety effect

A 'No safety Effect' might be used for a payload system failure condition that has no effect on the airworthiness of the RPAS.

2. Minor

Examples of '*a slight reduction in safety margins or functional capabilities*' might include:

a) Loss of a single redundancy in a multi-redundant system.

3. Major

Possible examples of '*a significant reduction in safety margins or functional capabilities*' might include:

a) Total loss of communications with ATC.

4. Hazardous

Possible examples of '*a large reduction in safety margins or functional capabilities*' might include:

a) Potential loss of safe separation (e.g. loss of DAA, incorrect altitude reporting);
b) Activation of an emergency recovery capability potentially resulting in loss of the RPA where a fatality is not expected to occur.

5. Catastrophic

This refers to one or more fatalities that can occur either in the air (mid-air collision) or on the ground. Where type-certification does not stipulate any limitations on type of airspace to be used and areas to be overflown, the design assumption must be that any failure condition leading to a crash, mid-air collision or forced landing, is potentially fatal.

Examples of potentially Catastrophic failure conditions include:

a) Loss of control over a populated area leading to impact with the surface outside of an approved safe area;
b) Loss of control leading to the inability of a RPA to be contained within a pre-defined segregated area;
c) Malfunction of a DAA system that actively guides the RPA towards neighbouring traffic.

(h) An emergency recovery capability may be used as a means of mitigating Catastrophic failure conditions. Where an emergency recovery function is used as mitigation for what would otherwise be a Catastrophic failure condition, the systems and equipment that supports this functionality would be required to undergo safety analysis to ensure a level of performance acceptable to the certifying authority. The use of emergency crash sites is one option available to applicants to mitigate against high severity failure conditions. The applicant will need to provide evidence to the certifying authority that their use will not result in unacceptable risks to people or property.

9. DEVELOPMENT ASSURANCE PROCESS

(a) This section has been derived from Eurocae ED-79A/ARP4754A. The guidance material presented in DO-178C/ED-12C, DO-254/ED-80 and ARP4754A/ED-79A has been recognised by industry and regulatory authorities as establishing levels of confidence for specific item of software and electronic hardware, and that the aircraft systems as a whole perform to its intended design requirements.

(b) The process includes validating requirements and verifying that requirements are met, together with the necessary configuration management and process assurance activities. As development assurance level assignments are dependent on classification of Failure Conditions, the safety analysis process is used in conjunction with the development assurance process defined within ARP4754A/ED-79A to identify Failure Conditions and severity classifications which are used to derive the level of rigour required for development.

(c) Complex systems and integrated aircraft level functions present greater risk of development error (requirements determination and design errors) and undesirable, unintended effects. At the same time it is generally not practical (and may not even be possible) to develop a finite test suite for highly-integrated and complex systems which conclusively demonstrates that there are no residual development errors. Since these errors are generally not deterministic and suitable numerical methods for characterising them are not available, other qualitative means should be used to establish that the system can satisfy safety objectives. The level of rigour applied to the Development Assurance process is defined by the Development Assurance Level (DAL).

(d) The intent, during the development process is to minimize the number of errors that will remain at the end of the development. This is done through the application of an assurance process (DAL) for review and testing assuring that functional review coverage/test coverage is apportioned to the failure condition severity classification in order to be confident that the malfunctions due to the

manifestation of an error will remain coherent with the safety objectives allocated to the severity classification of the malfunction.

(e) When applying the ARP 4754A DAL process and activities, to remain coherent with the probability requirement associated with failure condition severity classification we can say that:

- DAL A development gives confidence that the manifestation of a possible remaining error is compliant with an Extremely Improbable probability class defined as ≤ 10-9/fh.
- DAL B development gives confidence that the manifestation of a possible remaining error is at least compliant with the Extremely Remote probability class defined as 10-7/fh ≤P >10-9/fh.
- DAL C development gives confidence that the manifestation of a possible remaining error is at least compliant with the Remote probability class defined as 10-5/fh ≤ P > 10-7/fh.
- DAL D development gives confidence that the manifestation of a possible remaining error is at least compliant with the Probable probability class defined as 10-3/fh ≤ P >10-5/fh.

(f) Applying the above considerations leads to the DAL assignments in Table 5.

(g) In summary, development assurance is a process based approach which establishes confidence that system development has been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact aircraft safety, and the measure of rigour applied is defined by the DAL.

10. SYSTEMS AVAILABILITY AND INTEGRITY ASSESSMENT

(a) The safety assessment for RPAS will follow the methodology established for manned aircraft.

(b) Unlike manned aircraft systems which are developed to support the on-board pilot, RPAS systems can be differentiated to address distinct top-level hazards. Guidance regarding availability and integrity of RPAS systems has therefore been split into two parts as follows:

1. Section 11 of this scoping paper addresses systems required to maintain safe flight and landing. The focus here is on system failures that can lead to a forced landing or a crash. In these scenarios, the emphasis is centred on the protection of people and property on the ground.

2. Section 12 of this scoping paper addresses systems required to maintain safe aircraft separation. Any mid-air collision is likely to result in the loss of both aircraft. The focus here is therefore on the availability and integrity requirements of the Detect and Avoid system and is independent of the class or category of the RPAS.

11. SYSTEM AVAILABILITY & INTEGRITY REQUIRED TO MAINTAIN SAFE FLIGHT & LANDING (GROUND RISK)

11.1 CONCEPT

(a) The risk of suffering harm is an inescapable aspect of living. Nevertheless, there has been tremendous progress in improving many aspects of the quality of people's lives. People now live longer than at any time in history. Although accidents still occur, the trend averaged over the years has been downwards.

(b) This progress in the quality of people's lives is readily acknowledged but, paradoxically, it has been accompanied by an increased expectation for a society free of involuntary risks. The rapid technological developments of recent years have introduced new hazards but also enhanced the scope for controlling existing hazards. Though people accept that we should continue to take advantage of advances in science and technology, such technology should not be allowed to adversely affect this expectation; RPAS should be no different.

(c) In 2012 453[5] people were killed worldwide in large transport aircraft accidents. This is a good record by any standard and far better than other forms of transport, and yet there are still people who are scared of flying and an accident still makes headline news. The public perception of aviation safety cannot therefore be seen as directly linked to the hard facts of accident statistics but to a 'perception of risk' rather than actual danger. As regulators our aim is to manage risk.

(d) We should at this point draw a distinction between risk to persons on the ground and those on-board an aircraft. Other proposed system safety analysis methodologies have started with the premise that only a small proportion of RPAS accidents will actually result in ground fatalities and that a higher RPAS accident rate is therefore acceptable in maintaining the same overall fatality rate. This thinking is flawed due to the 'perception of risk' and by the increased expectation from the general public for a society free of involuntary risk. As aviation still has inherent dangers, persons flying on-board an aircraft consciously or unconsciously accept a higher level of risk. People are less tolerant of risks imposed upon them and over which they have no or little control. This difference in acceptable risk invalidates a simple trade-off between fatalities on-board an aircraft and fatalities on the ground. As third parties on the ground are not engaged in any aviation activity (manned or unmanned), their expectation of risk should be the same and not unduly impacted.

(e) So what is "risk"? Risk is defined as the probability of an occurrence multiplied by the severity of its outcome (Risk = Probability x Severity). The severity of a ground impact is a function of the impact dynamics (e.g. kinetic energies, materials involved, shape, aircraft size, the amount of fuel carried, etc.). The higher the severity, the larger the area of impact likely to be affected and the increased likelihood for a higher number of fatalities and amount of

[5] EASA annual safety review 2012 (Worldwide, commercial air transport, > 2250kg)

property destruction. The probability of a third person on the ground being injured/killed as a result of an aircraft hazard is primarily a function of: accident rate (the more crashes that occur the higher the probability of hitting someone), population density (the more people per given area) and the impact dynamics.

(f) In summary, another way of looking at risk to persons and property on the ground is:
Risk = f(accident rate, population density, impact dynamics, area of impact).

(g) Population density and area of impact cannot be a factor for airworthiness where the intent is for unrestricted operations. In order for a RPAS to be commercially viable in the civil market, it is unlikely that individual types will be constrained to niche market segments but will endeavour to explore a wider market potential through offering multirole capabilities in various environments, including flight over or near to large gatherings of people. The cautious approach is thus to assume that any RPAS failure condition leading to an uncontrolled crash could have fatal consequences. Where the overall risk may be deemed too high, operational rules may be applied in addition to airworthiness requirements, e.g. for single-engine aircraft operating over cities. If a RPA is restricted to fly over remote areas only or a controlled environment, airworthiness alleviations have already been foreseen, but this is an exception rather than the norm and can be dealt with by alternative procedures.

(h) Impact dynamics can be related to aircraft certification category. Due to the low level of energy required to kill and the wide variety of materials, shape and other factors affecting the capability of a RPA to kill and/or penetrate structures, the worst case is to consider contact with an unprotected person as potentially leading to a fatality. Note that this may not appear to be applicable to exceptionally small, light or slow RPA, but again these cases should be considered as exceptions to the basic methodology.

(i) From the above, risk to persons on the ground from airworthiness issues is therefore only a function of accident rate and impact dynamics, or the accident rate per aircraft category.

(j) $Risk_{(airworthiness)}$ = g(accident rate/category)

(k) This leads to the conclusion that it is not necessary to define a specific airworthiness risk to people and property on the ground from a RPA as the current manned aircraft accident based statistics remain valid, and ground based risk should not be a function of whether an aircraft is manned or unmanned. The regulatory objective is then to ensure that ground risk is managed in such a way that the accident rate per aircraft category does not rise with the introduction of RPAS[6]. The existing airworthiness requirements (e.g. CS/part-23, CS/part-25) are airworthiness's contribution to avoiding accidents, so can be used directly as a means of managing risk. Furthermore, this satisfies another underlying principle in that it ensures equivalence with manned aircraft.

[6] There is a long standing ICAO objective that the accident rate should not increase with increased traffic. This would also be applicable for unmanned aircraft.

(l) The approach taken by JARUS in defining required availability and integrity levels for individual system failure conditions is therefore based on establishing accident rates for all RPAS categories, and in proportioning safety targets for individual system failure conditions to reflect the severity and complexity of RPAS systems.

11.2 ACCIDENT STATISTICS

(a) To further support the choice of 'total number of accidents per aircraft category' as the basis for developing a system safety analysis, it is worth analysing aircraft accident statistics and comparing actual safety risks to people on the ground with those of people on-board aircraft.

(b) The difference in level of risk between persons on-board aircraft and those on the ground can be illustrated in aircraft accident statistics. Table 1 illustrates the accident statistics relate to GA accidents (all categories):

	EASA Annual Safety Review 2011 (Ref 6)[7]	**NTSB** (2002-2006) (Ref 7)[8]
Average No. accidents/year (5 year average)	1158	1653
Average No. fatal accidents/year	149 (13% of accidents)	328 (20% of accidents)
Average No. accidents/year with ground fatalities	3 (0.3% of accidents)	3 (0.2% of accidents)

Table 1: Comparison of GA accident statistics

(c) Based on these figures, it can be broadly established that the number of fatal accidents is an order of magnitude lower than the number of accidents. The number of accidents involving ground fatalities is 2 orders of magnitude lower than the number of fatal accidents. Clearly in this example the lower risk and therefore expectation of risk to people on the ground is substantiated. If the RPAS accident rate were permitted to increase in line with the total number of fatalities (both ground and on-board), then ultimately there may be in excess of a 400 fold increase in accidents, which would be unacceptable. Maintaining the same accident rate/category will therefore ensure that one of the defining principles of taking a cautious and defendable approach is met.

[7] EASA MS registered aircraft with MTOM < 2 250 kg
[8] US General Aviation

(d) Performing a similar analysis for Commercial Air Transport reveals the following figures:

	EASA Annual Safety review 2011 (Ref 6)[9]	**NTSB** (2002-2006) (Ref 8)[10]
Average No. accidents/year (5 year average)	30	29
Average No. fatal accidents/year	1 (3% of accidents)	1 (3% of accidents)
Average No. accidents/year with ground fatalities	<1 (<3% of accidents)	<1 (<3% of accidents)

Table 2: Comparison of Commercial Air Transport accident statistics

(e) From Table 2, the number of fatal accidents is of the same order and approaching the absolute number of accidents involving ground fatalities. The argument for a direct trade-off between airborne and ground risk is stronger in this case. However, a more detailed analysis would show that the fatal accidents are more likely to occur during the take-off and landing phase and ground fatalities are in the vicinity of an airport where the risk to the general public is acknowledged to be higher than the average.

11.3 SAFETY OBJECTIVES

(a) When defining RPAS safety objectives, the equivalence with manned aircraft per category principle is applied. The starting point is therefore to establish a range of target levels of safety for manned aircraft. This can be based either on current practice (quantitative target levels of safety are available in AMC 25.1309 and AC-23.1309-1E), or from a knowledge of actual accident rates. For aircraft categories where no target level of safety is defined, actual accident statistics have been established from published data, in this case UK-CAA CAP 780[11] (Ref 9), and is summarised below in Table 3.

[9] EASA MS Operators
[10] U.S. Air Carriers Operating Under 14 CFR 121 Scheduled and Non-scheduled Service (Airlines)
[11] While CAP 780 is based on UK only accident data, it has been assumed that the data will be similar to that of other developed countries.

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

Table 3: Manned aircraft accident rates

(b) A review of the figures shows that the actual accident rates for large public transport aeroplanes and non-public transport aeroplanes are close and of the same magnitude as those values established in AMC 25.1309 and AC 23.1309-1E for Class 1 aircraft, respectively. Setting quantitative safety objectives based on the magnitude of the accident rate per category from all causes, is therefore an appropriate, practical and conservative choice.

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

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

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

(f) In the late 1990s, FAA AC 23-1309-1 was amended to introduce different system target levels of safety. The changes were made following a study of GA accident causes, which indicated that pilot error, including 'loss of situational awareness' and 'inadvertent weather penetration' was by far the single largest causal factor. Enhancing cockpit avionics was seen as an effective means to increase pilot situational awareness and to reduce those fatal accident causes. However, the integrity requirements of 14 CFR part-25 prohibited manufacturers from developing cost-effective avionics for GA installations. AC 23-1309-1 was therefore amended by creating 4 aircraft classes and establishing safety objectives for each class based on the actual accident rates for each class. To reflect the non-complex nature of GA systems, only 10 catastrophic failure conditions at aircraft level was assumed. While the reliability of the avionics was not as high as CS/part-25 standards, the reduced reliability in the systems was more than offset by enhanced operational safety, leading to a net safety gain. In time, it was found that the AC became appropriate for any equipment.

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

(h) The DAL has been assigned to different RPAS categories and complexity levels in accordance with the principles set out in Section 7 of this scoping paper.

(i) Table 4 is a development of the rationale presented in AC 23-1309-1E to illustrate the approach adopted for a range of manned aircraft and the equivalent RPAS. Note the column titled 'Number of Potential Failure Conditions' (shown in grey), which is key in differentiating between manned aircraft and RPAS.

Note on Rotorcraft Safety Objectives

System safety assessment methodology and target levels of safety for manned rotorcraft have been adopted from that developed for large fixed wing aeroplanes. Accepted target levels for CS/part-27 and CS/part-29 both directly align with CS/part-25 ($1x10^{-6}$/fh for all causes). Current certification practice however is to assign safety objectives for CS/part-27 depending on the complexity of systems fitted and the intended type of operations of the rotorcraft (VFR or IFR).

Prior to 2000, the FAA and JAA initiated a review of AC 27/29.1309 to rationalise the guidance material, but this was subsequently withdrawn at a late stage in its development and prior to publication, in order for a part-23 type approach to be considered. The supporting regulatory activity has yet to start.

Until such time as safety objectives are agreed for manned rotorcraft, the approach adopted in this concept for RPAS was therefore to retain existing certification practice. Large rotorcraft will therefore retain the $1x10^{-6}$/fh target level of safety (all causes) commensurate with CS/part-25, but values for CS/part-27 will be considered on a case-by-case basis.

Aircraft Type	RPAS Complexity Level	Accident Rate (pfh) All Causes *(Note 1&4)*	% Due to Systems (10%) *(Note 2)*	Number of Potential Catastrophic Failure Conditions	Probability of a Catastrophic Failure Condition (pfh)
Manned CS-25		$1x10^{-6}$	$1x10^{-1}$	100 (10^{-2})	$1x10^{-9}$
RPAS CS-25	N/A *(Note 3)*	$1x10^{-6}$	$1x10^{-1}$	100 (10^{-2})	$1x10^{-9}$
Manned CS-29		$1x10^{-6}$	$1x10^{-1}$	100 (10^{-2})	$1x10^{-9}$
RPAS CS-29	N/A *(Note 3)*	$1x10^{-6}$	$1x10^{-1}$	100 (10^{-2})	$1x10^{-9}$
Manned CS-23 Class I		$1x10^{-4}$	$1x10^{-1}$	10 (10^{-1})	$1x10^{-6}$
RPAS CS-23 Class I	I	$1x10^{-4}$	$1x10^{-1}$	10 (10^{-1}) *(Note 5)*	$1x10^{-6}$
	II	$1x10^{-4}$	$1x10^{-1}$	100 (10^{-2}) *(Note 6)*	$1x10^{-7}$ *(Note 7)*
Manned CS-23 Class II		$1x10^{-5}$	$1x10^{-1}$	10 (10^{-1})	$1x10^{-7}$
RPAS CS-23 Class II	I	$1x10^{-5}$	$1x10^{-1}$	10 (10^{-1}) *(Note 5)*	$1x10^{-7}$
	II	$1x10^{-5}$	$1x10^{-1}$	100 (10^{-2}) *(Note 6)*	$1x10^{-8}$ *(Note 7)*
Manned CS-23 Class III		$1x10^{-6}$	$1x10^{-1}$	10 (10^{-1})	$1x10^{-8}$
RPAS CS-23 Class III	I	$1x10^{-6}$	$1x10^{-1}$	10 (10^{-1}) *(Note 5)*	$1x10^{-8}$
	II	$1x10^{-6}$	$1x10^{-1}$	100 (10^{-2}) *(Note 6)*	$1x10^{-9}$ *(Note 7)*
Manned CS-23 Class IV		$1x10^{-6}$	$1x10^{-1}$	100 (10^{-2})	$1x10^{-9}$
RPAS CS-23 Class IV	N/A *(Note 3)*	$1x10^{-6}$	$1x10^{-1}$	10 (10^{-2})	$1x10^{-9}$
Manned CS-27		$1x10^{-4}$	No quantitative criteria defined		
RPAS CS-27	I	$1x10^{-4}$	No quantitative criteria defined *(See Note following paragraph 11.3(i) above)*		
	II	$1x10^{-4}$			
Manned CS-VLA		No data	No quantitative criteria defined *(Note 8)*		
RPAS CS-LUAS *(Note 9)*	I	$1x10^{-4}$	$1x10^{-1}$	10 (10^{-1})	$1x10^{-6}$
	II	$1x10^{-4}$	$1x10^{-1}$	100 (10^{-2}) *(Note 6)*	$1x10^{-7}$ *(Note 7)*
Manned CS-VLR		No data	No quantitative criteria defined *(Note 8)*		
RPAS CS-LURS *(Note 9)*	I	$1x10^{-4}$	$1x10^{-1}$	10 (10^{-1})	$1x10^{-6}$
	II	$1x10^{-4}$	$1x10^{-1}$	100 (10^{-2}) *(Note 6)*	$1x10^{-7}$

Table 4: Derived quantitative systems availability and integrity required to maintain safe flight and landing (excluding loss of safe separation)

Notes to Table 4

1. Where an Emergency Recovery Capability has been utilised following an emergency condition and results in flight termination of a RPA in a pre-defined safe area, this occurrence may be excluded from the accident data, provided effective controls are in place to ensure that there is no risk to people and property.
2. Due to a RPAS's increased reliance on systems and higher levels of systems complexity and integration, it is recognise that the 10% attributed to RPAS systems may be underestimated. However, this value can never be 100% as other failure modes (e.g. structure, engines, HF, operations) will still be present. Furthermore, if the same accident rate per category is to be maintained, then an increase in systems related failures must be compensated for by a reduction in failures from other causes. In the medium term, this is expected to be achieved through a reduction in pilot error and HF causes, but as of today, there is no evidence that failures due to these causes is diminishing. Therefore, the airworthiness objective to limit system related failures to 10% is maintained.
3. Large RPAS systems are deemed to be complex (i.e. Equivalent to CL II).
4. The overall safety objective is to maintain the same accident rate for RPAS as for manned aircraft of equivalent category.
5. RPAS with Complexity Level I systems are assumed to have limited capability and are comparable with manned aircraft complexity levels.
6. For RPAS with systems Complexity Level II, the number of potentially catastrophic failure conditions is raised from 10 to 100.
7. For RPAS of system Complexity level II, the integrity level for individual Catastrophic failure conditions is raised by one order of magnitude to maintain the same accident rate as a manned aircraft of equivalent category.
8. These areas relate to small, relatively simple, manned aircraft where the 1309 criteria does not rely on a quantitative analysis and these categories of aircraft may not have demonstrated a level of system integrity in the same way as for other aircraft categories. However, for equivalent RPAS, the methodology follows that developed for other RPAS.
9. CS-LURS & CS-LUAS represent the minimum standard for type-certification.

11.4 CERTIFICATION TARGETS

(a) The full classification of failure conditions, including DALs and probability targets to maintain safe flight and landing for each RPAS class and complexity level, is presented in Table 5.

Table 5 - Relationship Among Aircraft Classes, Probabilities, Severity of Failure Conditions and Software and Complex hardware DALs required to maintain safe flight and landing to that of equivalent manned aircraft (excluding loss of safe separation).

		Classification of failure Conditions				
		No Safety Effect	**Minor**	**Major**	**Hazardous**	**Catastrophic**
		Allowable Qualitative Probability				
		No Probability Requirement	**Probable**	**Remote**	**Extremely Remote**	**Extremely Improbable**
Classes of RPAS	**Complexity Levels (CL)**	**Allowable Quantitative Probabilities and DAL (Note 2)**				
RPAS-25	**N/A**	See AMC 25.1309				
RPAS-29	**N/A**	See AC 29-2C, AC 29.1309				
RPAS-23 Class I (SRE under 6,000lbs)	**I**	No probability/DAL Requirement	**<10^{-3}** P=D, S=D (Notes 1 & 4)	**<10^{-4}** P=C, S=D (Notes 1 & 4)	**<10^{-5}** P=C, S=C (Note 4)	**<10^{-6}** P=C, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**<10^{-3}** DAL=D (Note 1)	**<10^{-5}** DAL=C (Note 1)	**<10^{-6}** DAL=C	**<10^{-7}** DAL=B (Note 3)
RPAS-23 Class II (MRE, STE or MTE under 6000lbs)	**I**	No probability/DAL Requirement	**<10^{-3}** P=D, S=D (Notes 1 & 4)	**<10^{-5}** P=C, S=D (Notes 1 & 4)	**<10^{-6}** P=C, S=C (Notes 4)	**<10^{-7}** P=B, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**<10^{-3}** DAL=D (Note 1)	**<10^{-5}** DAL=C (Note 1)	**<10^{-7}** DAL=B	**<10^{-8}** DAL=B (Note 3)
RPAS-23 Class III (SRE, MRE, STE or MTE > 6000lbs)	**I**	No probability/DAL Requirement	**<10^{-3}** P=D, S=D (Notes 1 & 4)	**<10^{-5}** P=C, S=D (Notes 1 & 4)	**<10^{-7}** P=C, S=C (Notes 4)	**<10^{-8}** P=B, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**<10^{-3}** DAL=D (Note 1)	**<10^{-5}** DAL=C (Note 1)	**<10^{-7}** DAL=B	**<10^{-9}** DAL=A (Note 3)
RPAS-23 Class IV	**N/A**	See AC 23.1309-1E				
CS-LUAS, or **CS-LURS**	**I** (Note 6)	No probability/DAL Requirement	**<10^{-3}** P=D, S=D (Notes 1 & 4)	**<10^{-4}** P=C, S=D (Notes 1 & 4)	**<10^{-5}** P=C, S=C (Note 4)	**<10^{-6}** P=C, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**<10^{-3}** DAL=D (Note 1)	**<10^{-5}** DAL=C (Note 1)	**<10^{-6}** DAL= B	**<10^{-7}** DAL=A (Note 3)
RPAS-27 (Note 5)	**I**	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, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**<10^{-3}** DAL=D (Note 1)	**<10^{-5}** DAL=C (Note 1)	**<10^{-6}** DAL=B	**<10^{-7}** DAL=A (Note 3)

Notes to Table 5

1. Numerical values indicate an order of probability range and are provided here as a reference. The applicant is usually not required to perform a quantitative analysis for minor and major failure conditions.

2. The symbology denotes typical DALs for primary systems (P) and secondary systems (S). For example, DAL Level A on primary system is noted by P=A.

3. At RPAS functional level, no single failure will result in a catastrophic failure condition.

4. Secondary system (S) may not be required to meet probability goals. If installed, S should meet stated requirements.

5. These values are not currently aligned with AC 27-1B. Current certification practice applied to manned rotorcraft may change these values depending on the intended type of operation (e.g. VFR/IFR) and the type certification basis of the rotorcraft.

6. Irrespective of the probability and DAL levels assigned, a CL I RPAS that requires real-time communication with the remote pilot station to maintain basic vehicle stability and control is unlikely to be granted type-certification.

(b) Development Assurance Process

(1) This AMC recognises the Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A / EUROCAE ED-79A, "Guidelines for Development of Civil Aircraft and Systems", ED-12C/ DO-178C and ED-80/DO-254 as acceptable methods for establishing a development assurance process for aircraft, system software and airborne electronic hardware for all classes of RPAS.

(2) The extent of application of ARP 4754A/ED-79A to substantiate the aircraft development process would be related to the complexity of the systems used and their level of interaction with other systems. It is anticipated that for CL II RPAS application of ARP 4754A/ED-79A methodologies would be required. However, for CL I RPAS a reduced extent might be appropriate. In this case, early concurrence with the Certification Authority is essential.

(3) For those cases where the Certification Authority has agreed that functional development assurance activities need not to be performed (e.g. RPAS typically in CL I), Table 3 should be used to assign DALs at software and airborne electronic hardware levels. In particular the DAL assignment method proposed in ARP4754A/ED-79A section 5.2 should not be used to assign DALs lower than those proposed in Table 3.

(4) The DAL assignments in other AC/AMCs, when applicable, should take precedence over the application of ARP 4754A/ED-79A, Section 5.2. If the applicant decides to use DAL assignments in other AC/AMCs, no further reduction of DAL is allowed.

12. SYSTEM AVAILABILITY & INTEGRITY REQUIRED TO MAINTAIN SAFE AIRCRAFT SEPARATION (MID-AIR COLLISION RISK)

(a) This section discusses that part of the system that would have been the pilot in a manned aircraft and the functions necessary to observe and separate from other aircraft. These systems do not have direct correlation with traditional manned aircraft systems but the functions performed by these systems are intended to maintain separation assurance and to provide collision avoidance. The regulatory requirement to observe and separate from other aircraft is required for both manned and unmanned aircraft operating in all unsegregated airspace.

(b) It should be noted that the definition of Detect and Avoid contained in this paper and AMC RPAS.1309 differs slightly from that produced by ICAO. The reason for this is that this section deals with detection and avoidance of other aircraft in the air and not other hazards such as weather and ground based obstacles. As such it may be possible that systems within the DAA that perform differing functions i.e. avoidance of other aircraft or avoidance of weather or ground obstacles may have differing levels of availability and integrity dependant on the function of the DAA system. Therefore functions that directly contribute to the avoidance of airborne aircraft would come under this chapter and functions that contribute to the avoidance of weather and ground obstacles may use the guidance set out in the previous chapter dealing with safe flight to landing.

(c) The ability to safely separate and avoid mid-air collisions are essential RPAS capabilities before being granted access into non-segregated airspace. A mid-air collision is generally considered as having catastrophic consequences for all aircraft types, irrespective of size or weight. Even impacts with small, low weight, RPA can result in damage that can compromise the safety of both aircraft. This could be disputed for very small RPA within the bird-strike capability of the aircraft/engine, but the impact dynamics would be very different and have yet to be tested.

(d) Procedures for the avoidance of collisions are built up through multiple safety barriers. These include airspace classifications, rules of the air, flight planning and ATC. In addition, certain aircraft may be fitted with an approved Airborne Collision Avoidance System (ACAS) to advise the pilot of the presence of conflicting traffic and any action to be taken to avoid a collision occurring. The final safety barrier for collision avoidance rests with the pilots of both conflicting aircraft to ‘see-and-avoid’. In the case of smaller aircraft not fitted with ACAS or operating in uncontrolled airspace, greater reliance is placed on the pilots’ see-and-avoid capability.

(e) For RPAS to integrate with manned aviation, they must show no lesser capability than that of manned aircraft to avoid collisions. Systems will therefore be required to have a sufficient level of availability and integrity regardless of their size and type. Systems that aim to provide this capability are generically termed ‘Detect and Avoid’ systems. They may comprise separate sub-systems to perform the functions of separation assurance and collision avoidance, and will be integrated with other RPAS systems (e.g. Flight Control System).

(f) To allow flight in unsegregated airspace, some regulatory authorities have allowed acceptable alternative approaches, such as the use of chase aircraft, observers, compulsory ATC surveillance, etc., to avoid the need for a Detect and Avoid system. These approaches must be considered as short-term exemptions and may not be acceptable in a fully type-certificated design.

(g) JARUS WG-6 adopted the approach contained in EUROCAE ED-79A / SAE ARP 4754A (Ref 10) for Functional DAL (FDAL) assignment taking credit for external events. Under this approach, the Detect and Avoid function can be seen as a protection function against an event external to the RPAS design; this event is two aircraft on a conflicting trajectory and the other aircraft failing to separate from the UA[12]. The analysis of such a function should consider, in addition to failure conditions related to erroneous operation or activation of the protection function, at least the two failure conditions as follows:

1. Loss of Detect & Avoid combined with the external event;
2. Loss of Detect & Avoid alone.

(h) The external event, if uncorrected, could lead to a mid-air collision that is classified as Catastrophic. Without quantitative data to the contrary, basic intuition would lead to the assumption that, without the intervention of one or both flight crews or ATC, the probability of two aircraft being on a conflicting course is not an uncommon event (greater than 10^{-5}/fh). Therefore, from Figure 3 the assignment of FDAL Level A to the Detect & Avoid system is appropriate. This may be revised once better data is available.

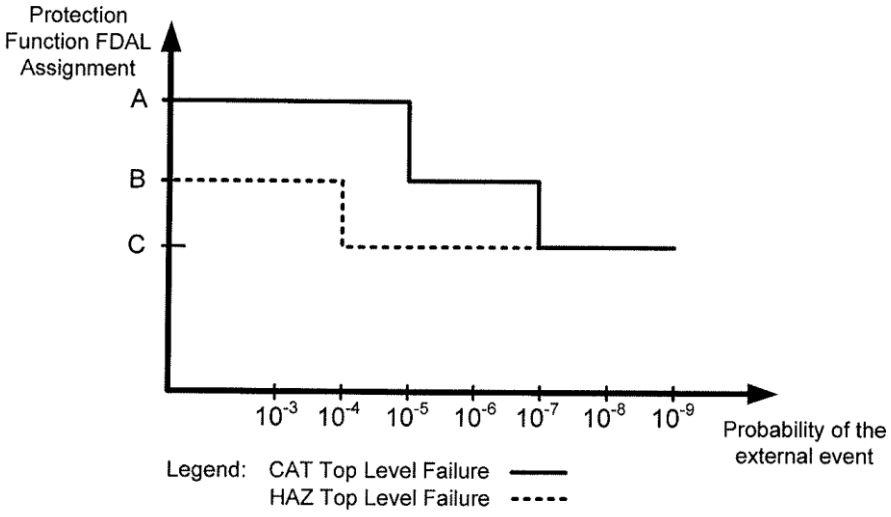


Figure 3: Protection Function FDAL Assignment as a Function of Probability of an External Event

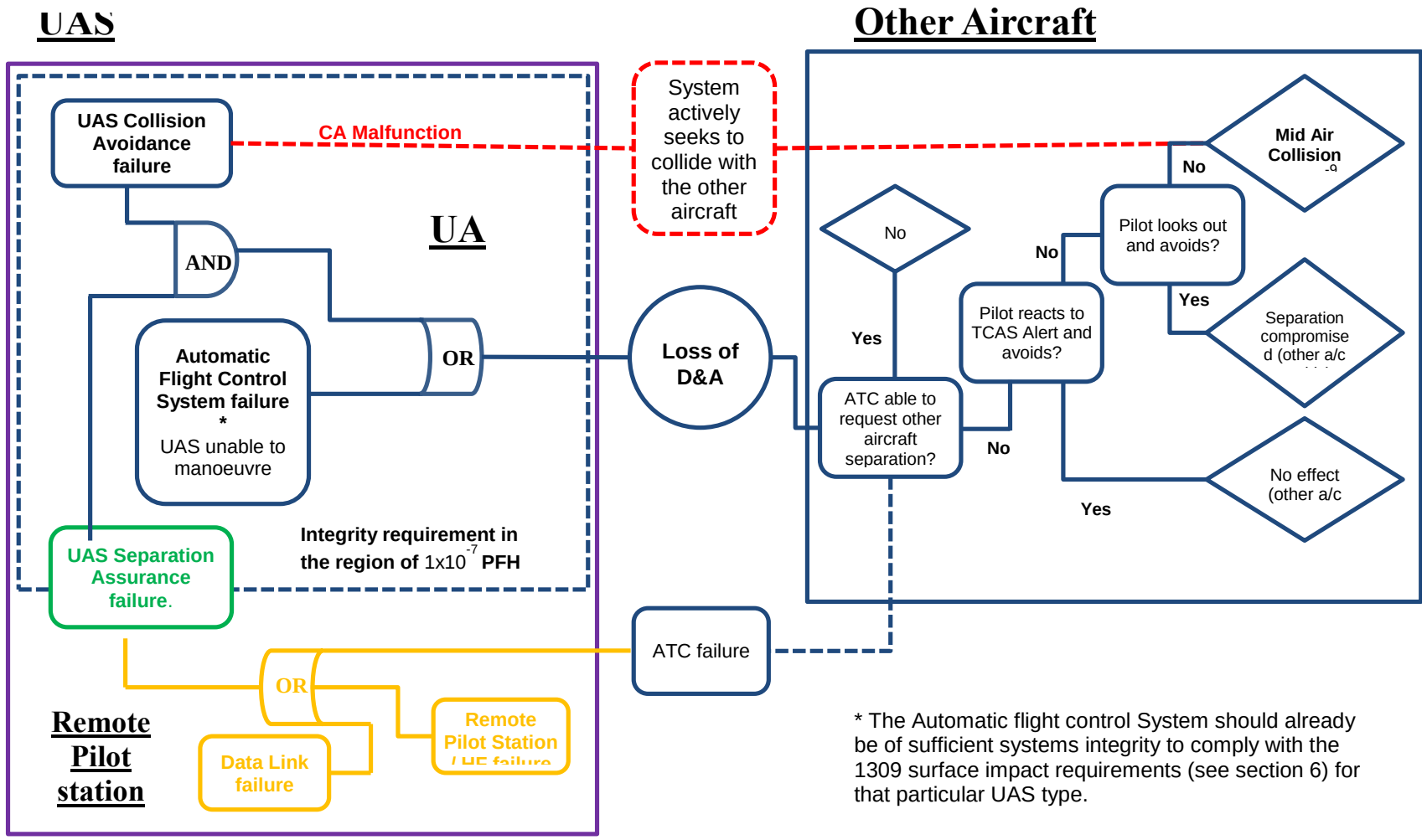
[12] It is acknowledged that the literal interpretation of the concept of "protection function" cannot be applied to the separation assurance portion of DAA due to the fact that while seeking separation the RPAS is actively involved in the avoidance of the external event. However, JARUS WG-6 came to the conclusion that the benefits of analysing the DAA as a protection function are by far greater than the drawbacks that could arise due to the highlighted discrepancy.

(i) In assigning a safety objective for the loss of the Detect & Avoid system alone, ARP4754A/ED-79A states that the classification should reflect the reduction in safety margins. A Catastrophic mid-air collision cannot be a direct consequence of a Detect & Avoid system failure condition alone, as the consequence of a system failure should be no worse than loss of adequate separation. There must be at least another aircraft on a conflicting trajectory that fails to separate, and possibly ATC failures. However, the loss of Detect and Avoid would result in a large reduction in safety margins and is therefore classified Hazardous. Furthermore, as type-certification would permit operations in all classes of airspace, the possibility of a mid-air collision with a large transport aircraft cannot be ruled out. Thus a classification of Hazardous would require a quantitative probability requirement commensurate with that of a large transport aircraft (CS/part-25/29), giving a probability value of 1 x 10^{-7}/fh for the Detect & Avoid system and supporting systems.

(j) As a note of caution, there may be malfunctions of a Detect & Avoid system that could lead directly to a mid-air collision, i.e. the system malfunctions in such a way that it actively guides the RPAS towards other traffic rather than acting to avoid a collision. These malfunctions are of such significance that it must be considered to result in a Catastrophic event and thus be assigned 1 x 10^{-9} /fh, DAL A.

(k) The example in Figure 4 demonstrates a possible concept of how the RPAS failure conditions (on the left hand side) culminate in a top event in the middle (loss of Detect and Avoid), which may result in a mid-air collision depending on the effectiveness of the human and system safety barriers associated with the conflicting aircraft and possibly ATC (on the right hand side).

FIGURE 4: EXAMPLE FAILURES THAT COULD CAUSE A MID-AIR COLLISION
Two aircraft on a conflicting trajectory



(a)

* The Automatic flight control System should already be of sufficient systems integrity to comply with the 1309 surface impact requirements (see section 6) for that particular UAS type.

13. REFERENCES

1. JARUS AMC RPAS.1309 Issue 1.
2. ICAO Circular 328: Unmanned Aircraft Systems (UAS)
3. Advance -Notice Of Proposed Amendment (NPA) No 16/2005. Policy for Unmanned Aerial Vehicle (UAV) certification.
   http://easa.europa.eu/rulemaking/docs/npa/2005/NPA_16_2005.pdf
4. Safety Considerations For Operation Of Unmanned Aerial Vehicles In The National Airspace System
   Roland E. Weibel and R. John Hansman, MIT
   Report No. ICAT-2005-1, March 2005
5. ICAO Circular 328
6. EASA Annual Safety Review 2011
   http://easa.europa.eu/communications/docs/annual-safety-review/2011/EASA-Annual-Safety-Review-2011.pdf
7. NTSB Annual Review of Accident Data (ARG) (2002-2006)
   http://library.erau.edu/find/online-full-text/ntsb/aircraft-accident-data.html#ARG
8. NTSB Annual Aviation Statistics
   http://www.ntsb.gov/data/table5_2012.html
9. UK-CAA CAP 780 (Aviation safety Review 2008)
   http://www.caa.co.uk/docs/33/CAP780.pdf
10. EUROCAE ED-79A / SAE ARP 4754A: Guidelines For Development Of Civil Aircraft And Systems
11. EASA Policy Statement - Airworthiness certification of Unmanned Aircraft Systems (UAS). Doc # **E.Y01301**
    www.easa.europa.eu/.../policy-statements/E.Y013-01_%20UAS_%20Policy.pdf
12. JAA/Eurocontrol UAV Task-force, final report
    http://easa.europa.eu/rulemaking/docs/npa/2005/NPA_16_2005_Appendix.pdf
13. CAP 722: Unmanned Aircraft System Operations in UK Airspace - Guidance
    http://www.caa.co.uk/docs/33/CAP722.pdf
14. EUROCAE ED-12C/ RTCA DO-178C: Software Considerations in Airborne Systems and Equipment Certification
15. EUROCAE ED-80/RTCA DO-254: Design Assurance Guidance For Airborne Electronic Hardware
16. FAA AC 27.1B, AC 27.1309: Equipment, Systems and Installations
    http://www.faa.gov/regulations_policies/advisory_circulars/
17. FAA AC 29.2C, AC 29.1309: Equipment, Systems and Installations
    http://www.faa.gov/regulations_policies/advisory_circulars/