Joint Authorities for Rulemaking of Unmanned Systems

Working Group 6 – Safety & Risk Assessment

AMC RPAS.1309

Issue 2

Safety Assessment of Remotely Piloted Aircraft Systems

The views expressed in this document represent the consensus views of the JARUS membership, and may not necessarily represent the views of their associated Authorities.

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

Table of Contents

List of Tables

0. 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, but 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 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 equivalent 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 minimise 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 safety assessment. This document is JARUS's views on how to perform an RPAS 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. INTRODUCTION

(a) Existing guidance material associated with the showing of compliance with system safety assessment requirements used in certification (1309) was not developed with Remotely Piloted Aircraft Systems (RPAS) in mind, and does not fully reflect the unique characteristics of these aircraft. This Acceptable Means of Compliance (AMC) has therefore been produced by JARUS WG-6 to provide additional means, but not the only means, that can be used for showing compliance with the availability and integrity requirements for RPAS systems. It has been developed to be used in conjunction with existing guidance material and to supplement the engineering and operational judgment that should form the basis of any compliance demonstration.

(b) The methodology developed in this AMC is based on the objective that RPAS operations must be as safe as manned aircraft. They should not present a hazard to persons or property on the ground or in the air that is any greater than that attributable to the operation of manned aircraft of equivalent class or category. Furthermore, it is assumed that RPAS will operate in accordance with the rules governing the flight of manned aircraft and must meet equipment requirements applicable to the class of airspace within which they intend to operate.

(c) This document differentiates between two distinct undesirable events:

(1) RPAS surface impact: An analysis of those systems required to ensure continued safe flight and landing (See Section 6), and

(2) RPAS loss of safe separation: An analysis of those systems required to perform Detect and Avoid functions (See Section 8).

(d) 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. It is anticipated that this SC will direct the certification applicant to this AMC. Whilst this AMC details “what” needs to be addressed, the development assurance and the safety assessment process and material providing guidance on “how to” comply with this Special Condition has not been fully completed in this first issue of this document. Sources of “how-to” guidance are published in ARP 4754A/ED-79A and ARP4761. This might form the basis of material to be developed in the future.

2. REFERENCES

(a) ICAO Circular 328: Unmanned Aircraft Systems (UAS)

(b) ICAO Annex 2 Amendment 43

(c) FAA AC 23.1309-1E: System Safety Analysis and Assessment for Part 23 Airplanes http://rgl.faa.gov/Regulatory_and_Guidance_Library/rgAdvisoryCircular.nsf/0/719e41e1d26099108625795d005d5302/$FILE/23.1309-1E.pdf

(d) EASA AMC CS-25.1309 http://easa.europa.eu/document-library/official-publication

(e) UK-CAA CAP 722 (Unmanned Aircraft System Operations in UK Airspace – Guidance) http://www.caa.co.uk/docs/33/CAP722.pdf

(f) UK-CAA CAP 780 (Aviation safety Review 2008) http://www.caa.co.uk/docs/33/CAP780.pdf

(g) CS-LURS: Light Unmanned Rotorcraft Systems http://jarus-rpas.org/index.php/deliverable/documents/file/8-3-deliverables-01-cs-lurs-final-draft-v2-nov2012-b

(h) EUROCAE ED-79A / SAE ARP4754A: Guidelines For Development Of Civil Aircraft And Systems

(i) SAE ARP 4761: Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment

(j) EASA Policy Statement- Airworthiness Certification of Unmanned Aircraft Systems (UAS) E.Y01301. www.easa.europa.eu/.../policy-statements/E.Y013-01_%20UAS_%20Policy.pdf

(k) EUROCAE ED-12C/ RTCA DO-178C: Software Considerations in Airborne Systems and Equipment Certification

(l) EUROCAE ED-80/RTCA DO-254: Design Assurance Guidance For Airborne Electronic Hardware

(m) FAA AC 27.1B, AC 27.1309: Equipment, Systems and Installations http://www.faa.gov/regulations_policies/advisory_circulars/

(n) FAA AC 29.2C, AC 29.1309: Equipment, Systems and Installations http://www.faa.gov/regulations_policies/advisory_circulars/

3. 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').

(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) ***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.

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

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

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

(i) ***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.

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

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

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

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

4. APPLICABILITY

(a) This document is applicable to all RPAS irrespective of class or category[1] for which 1309 is part of the type-certification basis. The RPAS includes the aircraft, data link, control station and any other element required for operation. Approval of the complete RPAS or individual products forming a RPAS is envisaged.

(b) For RPAS to be certificated under Part/CS-25, Part/CS-29 or Part/CS-23 Class IV, existing means of compliance (e.g. AMC 25.1309, AC 29-2C and AC 23-1309-1E Class IV) are deemed appropriate for these products. However, the failure classification definitions within Section 7 of this AMC RPAS.1309 and the availability and integrity requirements to maintain safe aircraft separation within Section 8 of this AMC RPAS.1309 will still apply.

(c) AMC RPAS.1309 does not apply to the performance, flight characteristics requirements of CS/FAR Subpart B, and structural loads and strength requirements of CS/FAR Subparts C and D. The flight structure such as wing, empennage, control surfaces; the fuselage, engine mounting, and landing gear and their related primary attachments are also excluded, as are rotorcraft rotors and transmissions.

5. COMPLEXITY LEVELS OF UAS

(a) To facilitate the assignment of system safety objectives, a classification scheme is introduced to differentiate between UAS based on system complexity.

(b) The existing manned initial airworthiness requirements currently use parameters such as weight, number of passengers, type/number of engines and performance to differentiate between aircraft classes, e.g. per AC-23.1309-1E Figure 2. For UAS to be certificated in ‘Large Aeroplane’, ‘Large Rotorcraft’ or ‘Commuter’ categories, the equivalent manned aircraft is already deemed to be highly complex, containing a high proportion of integrated systems. The change to UAS will therefore have little consequences in terms of the UAS overall level of complexity. However, this is not so for RPAS that are comparable to the other classes of aircraft.

(c) FAA AC 23.1309-1E defines four certification classes of aeroplanes in order to establish the acceptability of an aircraft design. The AC states that “*These classes were defined based on the way accident and safety statistics are currently collected. Generally, the classes deal with airplanes of historical equivalent levels of system complexity, type of use, system reliability and historical divisions of airplanes according to*

[1] The class or category of an RPAS will be established in the type-certification basis.

these characteristics. However, these classes could change because of new technology". The underlying assumption that traditional criteria would indirectly indicate the *"complexity, type of use and system reliability"* no longer holds true for UAS and is no longer adequate to categorise the complexity of a UAS that can utilise advanced technologies, even in relatively small RPA. The rigour and objectives of a safety assessment of RPAS cannot therefore fully rely only on the existing classification of small aircraft.

(d) The Complexity Levels (CL) classifications below apply to any UAS and should be applied in addition to the normal aircraft categorisation (e.g. AC-23.1309-1E Class I, CS-LURS, etc.).

(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.

(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[2]. This category of UAS is not covered by ICAO and is not covered in this document at the present time.

Note 1: Early in the certification programme, the applicant should seek the concurrence of the appropriate certificating authority on the selection of the Complexity Level.

Note 2: RPAS to be certificated under Part/CS-25, Part/CS-29 or Part/CS-23 Class IV are not affected by this classification.

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

6. SYSTEMS AVAILABILITY AND INTEGRITY REQUIRED TO MAINTAIN SAFE FLIGHT AND LANDING

(a) This section addresses the regulatory objective of ensuring that the accident rate per aircraft category does not rise with the introduction of RPAS.

(b) AC-23.1309 1E states that: *In assessing the acceptability of a design, it is recognised the need to establish rational probability values. Historical evidence indicates that the probability of a fatal accident in restricted visibility due to operational and airframe-related causes is approximately one per ten thousand flight hours or 1 x 10^{-4} per flight hour for single-engine airplanes under 6,000 pounds. Furthermore, from accident data bases, it appears that about 10 percent of the total was attributed to failure conditions caused by the airplane's systems. It is reasonable to expect that the probability of a fatal accident from all such failure conditions would not be greater than one per one hundred thousand flight hours or 1 x 10^{-5} per flight hour for a newly designed airplane. From past service history, it is also assumed, that there are about ten potential failure conditions in an airplane that could be catastrophic. The allowable target average probability per flight hour of 1 x 10^{-5} was thus apportioned equally among these failure conditions, which resulted in an allocation of not greater than 1 x 10^{-6} to each. The upper limit for the average probability per flight hour for catastrophic failure conditions would be 1 x 10^{-6}, which establishes an approximate probability value for the term 'extremely improbable'. Failure conditions having less severe effects could be relatively more likely to occur. Similarly, airplanes over 6,000 pounds have a lower fatal accident rate; therefore, they have a lower probability value for catastrophic failure conditions.*

(c) At the time of writing no manned Part-23 aircraft has been certificated with complex fly-by-wire flight control systems. If such an application were to be made it would be reasonable for the authorities to raise the number of potential catastrophic failure conditions by 1 order of magnitude. While it is accepted that Complexity Level I RPAS will have less complex systems, this cannot be said for Complexity Level II RPAS. It is therefore reasonable to assume that Complexity Level II RPAS containing complex airborne electronic hardware and software may have an order of magnitude of one hundred potential failure conditions regardless of the category of RPAS. This figure is shown as $1x10^{-2}$ pfh (see Table 2).

(d) In the past, accident statistics have been collected and used as the basis for deriving the quantitative probability figures established in AMC 25.1309 and AC 23.1309-1E. For aircraft types for which no quantitative figures are available in 1309, the latest actual accident statistics have been used, in this case UK-CAA CAP 780. It is acknowledged that other statistics are also available. The data set out in Table 1 illustrates the real accident rates and assumed safety targets.

Table 1 - Manned aircraft accident statistics.

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

(e) Where a direct comparison can be made, it can be seen that the assumed target level of safety for large transport aeroplanes in CS-25 (1x10^{-6} pfh) is of the same order of magnitude as the true accident rate (4.8x10^{-6} pfh), and provides a conservative margin. Similarly, for CS-23 Class I aeroplanes the safety target (1x10^{-4} pfh) is close to the non-public transport accident rate of (1.79 x 10^{-4} pfh).

(f) The same approach for defining safety objectives has been retained in this AMC using actual accident statistics for a wide range of aircraft types. It can be concluded, based on the data shown in Table 1, that the accident rate for GA (non-public transport aircraft) is approximately 1x10^{-4} pfh.

(g) To maintain equivalence with manned aircraft safety, RPAS accident rate should not be allowed to increase above that of an equivalent manned aircraft. Furthermore, a value of 1x10^{-4} pfh should be established as a minimum target accident rate for those RPAS for which no equivalent manned aircraft exists. The rationale is based on the need to maintain the overall fleet accident rate close to that of manned aircraft.

(h) For operations where the overall risk may be deemed too high, operational restrictions may be applied in addition to airworthiness requirements.

(i) Table 2 provides an example of how the methodology is applied.

Table 2 - Derived safety objectives to maintain safe flight and landing

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

(j) Note the difference between manned vs. RPAS number of potential catastrophic failure conditions shown in grey.

(k) It is acknowledged that RPAS may have a greater proportion of systems related failures than the arbitrary 10% given to manned aircraft systems. However, a 100% figure would be equally unrepresentative and therefore this figure is retained as an airworthiness objective.

7. FAILURE CONDITION CLASSIFICATIONS AND PROBABILITY TARGETS

(a) The classification of a failure conditions 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.

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

(1) No safety effect

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

(c) National 'Health and Safety at work' legislation will be applicable to ground equipment and personnel. However the effects of a Remote Pilot Station failure or event 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 Safety Analysis covered by AMC RPAS.1309.

(d) When establishing the Aircraft and Systems Functional Hazard Assessment, the applicant will have to substantiate the effects of failure conditions with consideration to operational conditions and events. Therefore, it is expected that a failure condition leading to a ground impact of the RPA within its approved area of operation might be classified as Hazardous if the RPAS is certified to operate over remote areas only.

Table 3 - 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=D, S=D (Notes 1 & 4)	**$<10^{-5}$** P=C, S=D (Note 4)	**$<10^{-6}$** P=C, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**$<10^{-3}$** DAL=D (Note 1)	**$<10^{-5}$** DAL=C (Note 1)	**$<10^{-6}$** DAL=C	**$<10^{-7}$** DAL=B (Note 3)
RPAS-23 Class II (MRE, STE or MTE under 6000lbs)	**I**	No probability/DAL Requirement	**$<10^{-3}$** P=D, S=D (Notes 1 & 4)	**$<10^{-5}$** P=C, S=D (Notes 1 & 4)	**$<10^{-6}$** P=C, S=C (Notes 4)	**$<10^{-7}$** P=B, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**$<10^{-3}$** DAL=D (Note 1)	**$<10^{-5}$** DAL=C (Note 1)	**$<10^{-7}$** DAL=B	**$<10^{-8}$** DAL=B (Note 3)
RPAS-23 Class III (SRE, MRE, STE or MTE > 6000lbs)	**I**	No probability/DAL Requirement	**$<10^{-3}$** P=D, S=D (Notes 1 & 4)	**$<10^{-5}$** P=C, S=D (Notes 1 & 4)	**$<10^{-7}$** P=B, S=C (Notes 4)	**$<10^{-8}$** P=B, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**$<10^{-3}$** DAL=D (Note 1)	**$<10^{-5}$** DAL=C (Note 1)	**$<10^{-7}$** DAL=B	**$<10^{-9}$** DAL=A (Note 3)
RPAS-23 Class IV	**N/A**	See AC 23.1309-1E				
CS-LUAS, or **CS-LURS**	**I** (Note 6)	No probability/DAL Requirement	**$<10^{-3}$** P=D, S=D (Notes 1 & 4)	**$<10^{-4}$** P=D, S=D (Notes 1 & 4)	**$<10^{-5}$** P=C, S=D (Note 4)	**$<10^{-6}$** P=C, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**$<10^{-3}$** DAL=D (Note 1)	**$<10^{-5}$** DAL=C (Note 1)	**$<10^{-6}$** DAL= C	**$<10^{-7}$** DAL=B (Note 3)
RPAS-27 (Note 5)	**I**	No probability/DAL Requirement	**$<10^{-3}$** P=D, S=D (Notes 1 & 4)	**$<10^{-4}$** P=D, S=D (Notes 1 & 4)	**$<10^{-5}$** P=C, S=C (Note 4)	**$<10^{-6}$** P=C, S=C (Notes 3&4)
	II	No probability/DAL Requirement	**$<10^{-3}$** DAL=D (Note 1)	**$<10^{-5}$** DAL=C (Note 1)	**$<10^{-6}$** DAL=C	**$<10^{-7}$** DAL=B (Note 3)

Notes pertaining to Table 3

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

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

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

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

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

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

(e) 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, systems, software and airborne electronic hardware for all classes of RPAS.

(2) The extent of application of ARP 4754A/ED-79A to substantiate functional development assurance activities 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 and 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 the DAL assignment method proposed in 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.

8. AVAILABILITY AND INTEGRITY REQUIREMENTS FOR SYSTEMS TO MAINTAIN SAFE AIRCRAFT SEPARATION

(a) This paragraph deals with Detect and Avoid (DAA) functions that are intended to maintain Separation Assurance and to provide Collision Avoidance.

(b) DAA functions may be separated into two sub functions as follows:

(1) Separation Assurance: Functions that are required to maintain safe separation from other aircraft in compliance with the applicable rules of the air. This may include any input from ATC or from remain-well-clear function on-board the RPA and may involve the remote crew.

(2) Collision Avoidance: Functions with the capability to see, sense or detect conflicting traffic and to take the appropriate avoidance action. Collision Avoidance should be seen as an automated function that interacts with the RPAS control system and is designed to act if safe separation has been compromised.

(c) The combination of RPAS Separation Assurance and Collision Avoidance functions should provide an acceptable level of safety in maintaining safe separation with any aircraft the RPA may encounter. The avoidance of a mid-air collision is achieved by a combination of the RPAS Separation Assurance and Collision Avoidance functions, the conflicting aircraft's pilot(s) and/or systems, and ATC when available.

(d) A mid-air collision cannot solely be a direct consequence of the loss of the Detect and Avoid function alone. For this to happen there must be at least another aircraft on a conflicting trajectory that fails to separate.

(e) The Detect and Avoid function can be seen as a protection function against an event external to the RPAS design; this event being the two aircraft on a conflicting trajectory and the other aircraft failing to separate from the RPA. 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 and Avoid combined with the external event (leading to a mid-air collision)

(2) Loss of Detect and Avoid alone.

(f) The first failure condition defined above is classified as Catastrophic. However, 'Loss of Detect and Avoid' alone has no direct safety effect although it results in a reduction in safety margin that is proportional to the probability of being in a conflicting trajectory with another aircraft that fails to separate.

(g) Several different studies are on-going at the time of writing of this AMC to better characterise the external event, i.e. an RPA being in a conflicting trajectory with another aircraft. It is possible that the external event probability may change with different operational scenarios (e.g. IFR vs. VFR) or due to other factors not yet fully understood. Therefore, without quantitative data to the contrary, this AMC conservatively stipulates that the external event is Probable. This assumption may need to be revised as more data becomes available to better characterise the external event.

(h) In accordance with the guidelines provided in ED-79A/ARP 4754A paragraph 5.2.4, the reduction of safety margins resulting from the 'Loss of Detect and Avoid' alone is Large and a Hazardous failure condition classification for this failure condition is therefore appropriate.

(i) As operations in all classes of airspace would be eligible with type approval, the possibility of a mid-air collision with a large transport aircraft cannot be ruled out. Thus a failure condition classification of Hazardous would require a quantitative probability requirement commensurate with that of a large transport aircraft (CS-25/29). Therefore the probability value of 1 x 10^{-7} per flight hour is deemed appropriate for the 'Loss of Detect and Avoid' alone.

(j) Details on the development of protection functions can be found in the ED-79A/ARP 4754A paragraph 5.2.4. and is considered appropriate for the development of the safety objectives for the Detect and Avoid function of a RPAS

(k) Application of ED-79A/ARP 4754A paragraph 5.2.4 Figure 11 results in a top-level FDAL A assigned to the DAA aircraft level function.

(l) A malfunction of the Detect and Avoid function that could directly cause a mid-air collision, i.e. the RPA is directed into rather than away from the path of another aircraft, shall be shown to be no greater than 1x10-9 per flight hour, functional development assurance level A and not result from a single failure.

9. SYSTEM SAFETY ASSESSMENT PROCESS

(a) The extent to which the more structured methods and guidelines contained in this AMC should be applied is a function of systems complexity and systems failure consequence. In general, the extent and structure of the analyses required to show compliance with 1309 will be greater when the system is more complex and the effects of the failure conditions are more severe. This AMC is not intended to require that the more structured techniques be applied where traditional techniques have been shown to be acceptable.

(b) This section has not been fully developed at this time, and more guidance on methods of showing compliance is anticipated. One source of 'how-to' guidance is published in ARP 4754A/ED-79A and ARP4761. The ARP4761 is currently under review by SAE S-18 committee and EUROCAE WG-63. This might form the basis of useful material to be presented herein.