A Review of System Safety Failure Probability Objectives for Unmanned Aircraft Systems

Reece A. Clothier [a*] **and Paul Wu** [b]
[a] Australian Research Centre for Aerospace Automation, Queensland University of Technology, Brisbane, Australia
[b] Queensland University of Technology, Brisbane, Australia
* reece.clothier@rmit.edu.au

Abstract: Unmanned Aircraft Systems (UAS) are one of a number of emerging aviation sectors. Such new aviation concepts present a significant challenge to National Aviation Authorities (NAAs) charged with ensuring the safety of their operation within the existing airspace system.

There is significant heritage in the existing body of aviation safety regulations for Conventionally Piloted Aircraft (CPA). It can be argued that the promulgation of these regulations has delivered a level of safety tolerable to society, thus justifying the "default position" of applying these same standards, regulations and regulatory structures to emerging aviation concepts such as UAS. An example of this is the proposed "1309" regulation for UAS, which is based on the 1309 regulation for CPA. However, the absence of a pilot on-board an unmanned aircraft creates a fundamentally different risk paradigm to that of CPA. An appreciation of these differences is essential to the justification of the "default position" and in turn, to ensure the development of effective safety standards and regulations for UAS.

This paper explores the suitability of the proposed "1309" regulation for UAS. A detailed review of the proposed regulation is provided and a number of key assumptions are identified and discussed. A high-level model characterising the expected number of third party fatalities on the ground is then used to determine the impact of these assumptions. The results clearly show that the "one size fits all" approach to the definition of 1309 regulations for UAS, which mandates equipment design and installation requirements independent of where the UAS is to be operated, will not lead to an effective management of the risks.

Keywords: UAS, Unmanned Aircraft Systems, UAS.1309 Regulation, Airworthiness.

1. INTRODUCTION

Unmanned Aircraft Systems (UAS) are one of a number of emerging aviation sectors, which include personal air vehicles, hypersonic aircraft, and reusable sub-orbital aircraft. Like all technologies these emerging aviation sectors have associated risks. The primary safety risks for UAS are associated with the hazards of a collision between the Unmanned Aircraft (UA) and a Conventionally Piloted Aircraft (CPA) situated on the ground or in the air; or a controlled or uncontrolled impact of the UA with terrain or objects on the terrain (*e.g.*, people or structures) [1]. These hazards can have potential consequences in relation to a range of entities of value (*e.g.*, people, property, the environment, or the objectives of the organisation, *etc*.). Of primary concern is the potential harm caused to those people on the ground or on-board other aircraft. National Aviation Authorities (NAAs), would typically manage these risks through the:

a) development and promulgation of a comprehensive framework of safety standards and regulations encompassing the:
    i. design, operation, manufacture, and maintenance of the UAS;
    ii. training and licensing of personnel; and
    iii. supporting organisational structures, accountabilities, policies and practices of the organisation conducting the UAS activity.
b) oversight of the UAS industry.
c) enforcement of safety regulation.

The over-arching safety requirement governing the development of regulations for UAS is referred to as the Equivalent Level of Safety (ELoS) objective. More specifically, the framework of safety regulations should ensure that UAS demonstrate, as a minimum, an ELoS to that currently demonstrated by CPA [2].

A comprehensive framework of regulations has yet to be developed for UAS. In its absence NAAs have managed the risks through the imposition of restrictions on UAS operations. In general, these restrictions can include: limiting UAS operations to segregated airspace and over unpopulated areas or the prohibition of particular UAS operations altogether. The particular restrictions depend on the state or territory where the operation is conducted. The restrictions come at significant cost to the industry and in turn society through the benefits foregone in applications such as search and rescue, law enforcement, bush fire fighting, infrastructure management and agriculture. As awareness of the capability of UAS and of the potential benefits from their application grows, so too does the pressure on the NAAs to relax current restrictions on their operation.

A number of national and international groups are working to develop the framework of standards and regulations for UAS necessary to grant a relaxation in current operational restrictions. Draft working papers and regulatory materials are now beginning to emerge and an example of which is the draft Acceptable Means of Compliance (AMC) for UAS.1309 [3] proposed by the Joint Authorities for Rulemaking on Unmanned Systems (JARUS), UAS Systems Safety Analysis 1309 Group.

This paper provides a critical review of the proposed AMC for UAS.1309 (referred to herein as "UAS.1309"). Following the recommendation made in [2], UAS.1309 was "primarily based" [3] on the existing 1309 regulation for large transport category CPA (*i.e.*, CPA regulation FAR/CS-25.1309 [4, 5] and associated guidance material [6, 7]). It is important to note that the purpose of this paper is not to critique the FAR/CS-25.1309 regulation upon which UAS.1309 is based. Rather, the purpose of this paper is to explore some of the underlying assumptions and in turn suitability of the FAR/CS-25.1309 regulation as a basis for 1309 regulations for UAS.

A review of the major components of the UAS.1309 regulation is provided in Section 2. The objective of the review is to identify and explore some of the key differences and assumptions. In Section 3, a high-level risk model is used to further explore the effectiveness of the draft regulation in terms of the management of the risks to people on the ground. The paper concludes with some brief recommendations.

2. JARUS DRAFT AMC FOR UAS.1309

The Joint Authorities for Rulemaking on Unmanned Systems (JARUS), UAS Systems Safety Analysis 1309 Group released a draft Acceptable Means of Compliance (AMC) for UAS.1309 [3] in August of 2011. UAS.1309 is "primarily based" [3] on the AMC for CS-25.1309 [6]. A briefing on UAS.1309 and the rationale behind it can be found in [8].

2.1. Objective, Scope and Applicability of Regulation

The overall objective of the existing FAR/CS-25.1309 regulation is to ensure an acceptable safety level for equipment and systems designed and installed on an aircraft [6]. For UAS.1309, the overall objective is to ensure UAS demonstrate, at a minimum, an ELoS to that of CPA.

2.1.1 Scope of Regulation

The FAR/CS-25.1309 regulation for large/transport category CPA is a general requirement that is applied to any aircraft equipment or system (there are some exclusions), which is applied in addition to any other prescriptive requirements specific to the design and installation of the particular equipment or system [3, 6]. In contrast, the scope of UAS.1309 is restricted to the Complex Flight Management System (CFMS). The CFMS is defined as "…the collection of automated systems (Synthetic Pilot) that perform the functions usually assigned to an aircraft-located pilot" [3]. All other UAS equipment, systems and installations not considered part of the CFMS would be subject to the "relevant" CS/FAR 1309 code [3]. The safety requirements on the CFMS are then split into those relating to:

a) equipment and systems whose functions are necessary to maintain UAS safe flight and landing, and
b) equipment and systems whose functions are necessary for the provision of separation assurance and collision avoidance.

A similar distinction in safety requirements is not made for CPA, with existing airborne collision avoidance systems being subject to the same requirements as other equipment and systems designed and installed on an aircraft. For the purposes of comparison, the scope of this paper is limited to the review of the requirements relating to equipment and systems whose functions are necessary to maintain safe flight and landing. A separate review of the safety requirements specific to the provision of separation assurance and collision avoidance is needed.

2.1.2. Applicability of Regulation

Existing CPA regulations define different qualitative safety objectives for each class or category of CPA type. Logically, smaller and inherently less risky CPA (*i.e.*, those having fewer passengers on-board) have less prescriptive safety requirements than those defined for large/transport category aeroplanes (see, for example, the safety requirements contained in sub-part 1309 to airworthiness certification regulations for Very Light Aeroplanes [9], Very Light Rotorcraft [10], and small/normal category rotorcraft [11, 12]). Conversely, UAS.1309 is advocated as a "one size fits all" [8] regulation; defining the same qualitative safety requirements across 10 different classes of UAS types. The justification for the "one size fits all" approach is that all UAS have equally complex CFMS and therefore, should be subject to the same qualitative safety requirements. However, and as acknowledged in UAS.1309, mandating the same qualitative safety requirements across the diverse range of UAS types encounters practical difficulties, particularly for smaller UAS. A recognised disadvantage of the UAS.1309 regulation is that it "mainly applies to the equivalent of manned sized UAS, and cannot be easily read across to small (sub manned sized) UAS…" [8]. Finally, specifying a single prescriptive qualitative safety objective imposes the same compliance effort (*e.g.*, the undertaking of a quantitative system safety assessment) across all UAS types and operations. As will be shown in later sections of this paper, the risks associated with the different UAS types vary significantly and as a result the imposed cost of demonstrating compliance to the prescriptive safety objective is potentially unjustified for some "low risk" UAS operations. As in CPA regulations, the specification of the qualitative safety objective should be tailored to each class of UAS. The tailoring should take into consideration the level of risk associated with the operation of each class of UAS, the costs of demonstrating compliance to the objective, and the complexity of the equipment and systems.

2.2. Overview of the 1309 Regulation

In general, a 1309 regulation requires the:

a) demonstration (through a documented qualitative or quantitative analysis) that equipment and systems perform as intended under foreseeable operating and environmental conditions;
b) adoption of principles drawn from fail-safe design [7]; and
c) demonstration (through a documented qualitative or quantitative analysis) that the likelihood of failure of equipment and systems, considered separately and in relation to other systems, is inversely-related to the severity of its effect on the safe operation of the system.

The focus of this paper is on the specification of the latter of these three general requirements, commonly referred to as the safety objective. The safety objective defines the minimum acceptable safety level for the design and installation of equipment and systems to the UAS. Its specification also comprises three components:

a) a qualitative ordinal scale describing the level of severity of failure conditions;
b) qualitative and quantitative scales describing the likelihood of occurrence of a failure; and

c) Failure Probability Objectives (FPOs) characterising the maximum acceptable likelihood of occurrence of a failure of a given level of severity.

The three regulatory components comprising the specification of the safety objective are briefly described in the following sections.

2.3. Classification of the Severity of Failure Conditions

A failure is defined as "an occurrence, which affects the operation of a component, part, or element such that it can no longer function as intended, (this includes both loss of function and malfunction)." [6] A single failure can give rise to a number of failure conditions, which are defined as "a condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events." [6]

2.3.1. The Failure Condition Classification Scheme

Failure conditions are classified according to the severity of their associated effects. As discussed in [13-15] the primary objective of modern airworthiness regulations for CPA is to provide assurances in the protection of people on-board the aircraft; the primary population at risk due to CPA operations [1]. The risks to people and property on the ground are of secondary concern, being indirectly addressed through the development and promulgation of airworthiness regulations aimed at protecting those on-board the aircraft [15-17]. As such, for CPA the consequence associated with a failure condition is described in relation to the potential damage or degradation of the performance of the aircraft, the effect on the ability of pilots to perform their tasks, and the comfort and wellbeing of the cabin crew and passengers on-board. A *Catastrophic Failure Condition* is therefore defined as one that results in hull loss *or* multiple occupant fatalities.

Recognising that there is no person on-board an UA [18], UAS.1309 classifies failure conditions on the basis of their effect in relation to: people on the ground, the UAS crew, and the capability and safety margins of the UAS (see Table 1). A catastrophic UAS failure condition is thus defined in [3] as "Failure Conditions that could result in multiple fatalities".

Table 1. Classification of the Severity of Failure Conditions [3]

Classification	**Effect of the Failure Condition on:**		
	UAS Capabilities and Safety Margins	**People (on board other aircraft or on the ground)**	**UAS Crew**
No Safety Effect	Negligible effect on safety margins	*No effect defined*	Negligible effect on UAS crew workload
Minor	Slight reduction in safety margins	*No effect defined*	Slight increase in workload
Major	Significant reduction in safety margins	Injuries	Significant increase in workload or conditions that impair UAS crew efficiency
Hazardous	Large reduction in safety margins or functional capabilities	Serious or fatal injury to a relatively small number of people	Physical distress or excessive workload such that the UAS Crew cannot be relied upon to perform their tasks accurately or completely
Catastrophic	*No effect defined* *	Multiple fatalities	*No effect defined*
* The definition of a Catastrophic Failure Condition provided in UAS.1309 [3] does not explicitly describe any effects in relations to the UAS Capabilities and Safety Margins. However, UAS.1309 does use the hull loss rate as a "substitute" effect.			

2.3.2. Classifying the Failure Conditions

The process of classifying failure conditions requires a linkage to be established between a) the incorrect or discontinued functioning of the equipment or system (*i.e.*, a failure) and b) the subsequent realisation of consequential outcomes (*i.e.*, its associated failure conditions, Table 1). For CPA, this linkage needs to be established between a failure in equipment and systems and the consequences, which are specified in relation to the aircraft, passengers, and crew. There is always at least one person on-board a CPA; therefore, it has been assumed that any equipment or system failure that has the potential to cause a hull loss (*i.e.*, any failure that "would prevent the continued safe flight and landing of the aircraft" [4]) also has the potential to cause occupant fatalities, and subsequently can be classified as *Catastrophic*. Due to the nature of this "linkage", this classification can be made independent of where or how the aircraft is being operated. Important to note, a more pragmatic concept of this linkage is adopted in [19], p.11.

The classification of a Catastrophic Failure Condition for UAS relies on the establishment of a similar linkage between: a) the failure or the degradation of equipment or systems comprising the CFMS and b) the realisation of multiple third party fatalities on the ground. The position adopted in UAS.1309 is that the failure/degradation of any CFMS equipment or system whose function is necessary to "continue safe flight and landing" of the Unmanned Aircraft (UA) *will lead to* multiple fatalities on the ground, and as such should be classified as *Catastrophic* (this assumption is herein referred to as "*Assumption One*"). Based on *Assumption One*, the classification of Catastrophic Failure Conditions for UAS is considered independent of the nature or location of the operation. Thus, the position adopted in UAS.1309 is that all failures of CFMS equipment or systems whose function is necessary to maintain safe flight and landing will have the same outcome (in terms of the level of consequence to people and property overflown), irrespective of the level of their exposure to the hazard of a crashing UA or the ability of the UA to inflict harm to a person. This position places UAS.1309 in conflict with discussion and recommendations made in [2], specifically: "UAV System failure conditions leading to a controlled crash over unpopulated areas should obviously be considered less severe than those leading to an uncontrolled crash over populated areas." [2]. Quantitative risk studies [20-25] illustrate the significant variability in the level of risk to third parties on the ground due to the operation of an aircraft, be it manned or unmanned. This variability arises due to the distribution of the population overflown relative to the aircraft flight path; the total energy and frangibility of the crashing aircraft; the area over which the energy is distributed; and the types of sheltering available to people on the ground. Further, given an UA impacts a person, there is no guarantee of a fatal outcome. As shown in [26, 27], some classes of UAS are incapable of causing fatal injury to a person, let alone multiple fatalities. For such classes of UAS, and in accordance with the definitions provided in Table 1, the failure conditions should only be classified as *Major*, or at worst, *Hazardous*.

It could be argued that *Assumption One* is a conservative position to adopt. However, due to the variability in the level of the risks presented to third party people overflown, the adoption of this "conservative" assumption does not necessarily result in a "conservative" management of the risks. This point is further illustrated in §3. The above examples objectively question the validity of *Assumption One*. It is advocated here, that the classification of the failure condition needs to be based on an established linkage between the occurrence of the failure and *its effects* specified in terms of the potential harm to people over-flown. This linkage should take into consideration the nature of the exposure and the potential for harm.

2.4. Classification of the Probability of Failure Terms

UAS.1309 proposes the same qualitative and quantitative scale of probability terms as used in existing CPA 1309 regulations [6, 7] (Table 2), with the only difference being the substitution of the term "aircraft" in place of "aeroplane". The scale is described in relation to the expected frequency of occurrence of a failure relative to the operational lifetime of an individual aircraft of the relevant class, or relative to the operational lifetime of the entire fleet of aircraft of the relevant class of UAS types. Quantitative limits are associated with each of the qualitative likelihood terms. The limits are characterised by a measure of the Average Probability of Failure (APF) per flight hour, defined as "… a representation of the number of times the subject Failure Condition is predicted to occur during the entire operating life of all aeroplanes of the type divided by the anticipated total operating hours of all aeroplanes of that type (Note: The Average Probability

Per Flight Hour is normally calculated as the probability of a Failure Condition occurring during a typical flight of mean duration divided by that mean duration)." [6] The quantified limits associated with each of the probability classifications for individual failure conditions (*APF_{IND}*) are summarised in Table 2. The APF is determined for a particular Failure Condition through the use a variety of assessment techniques (*e.g.*, see [6, 7, 28]).

Table 2. Classification of Probability Terms [3]

Classification	**Qualitative Description**	**Quantified Limits** **(average probability per flight hour)**
Probable	those anticipated to occur one or more times during the entire operational life of each aircraft.	$APF_{IND} > 10^{-5}$
Remote	those unlikely to occur to each aircraft during its total life, but which may occur several times when considering the total operational life of a number of aircraft of the type.	$10^{-7} < APF_{IND} \leq 10^{-5}$
Extremely Remote	those not anticipated to occur to each aeroplane during its total life but which may occur a few times when considering the total operational life of all aircraft of the type.	$10^{-9} < APF_{IND} \leq 10^{-7}$
Extremely Improbable	those so unlikely that they are not anticipated to occur during the entire operational life of all aircraft of one type.	$APF_{IND} \leq 10^{-9}$

2.5. Failure Probability Objectives

The safety objective states that an inverse-relationship must exist between the APF of equipment and systems and the severity of their effects. This safety objective can be expressed qualitatively or quantitatively. UAS.1309 specifies the same qualitative safety objective across all type/classes of UAS as that described in AMC CS-25.1309 [6]. Specifically:

> *(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****.*
>
> p.5, [3]

As above, each classification of a failure condition severity has an associated maximum acceptable likelihood of occurrence, referred to as a Failure Probability Objective (FPO). The collection of FPOs partitions the two-dimensional design space into "acceptable" and "unacceptable" sub-spaces as illustrated in Table 3. The quantitative FPOs for a "catastrophic failure condition" are summarised in Table 4 for each of the 10 UAS "classes" described UAS.1309.

It is important to note an inconsistency arising from the "one size fits all" UAS.1309 approach. According to the qualitative expression of the safety objective (*i.e.*, the qualitative FPOs stated above), a Catastrophic Failure Condition must be *Extremely Improbable*. As per Table 2, Extremely Improbable is defined as: $APF_{IND} \leq 10^{-9}$. With the exception of UAS classified as belong to the UAS-25 or UAS-23 Class III, all other UAS classes have quantitative FPOs for Catastrophic Failure Conditions with $APF_{IND} > 10^{-9}$ (see Table 4). Thus the quantitative FPOs defined in UAS.1309 are in conflict with the qualitative FPOs defined in UAS.1309. Assuming that the quantitative FPOs remain the same, either the quantified limits for the probability terms need to be redefined (*e.g.*, those in Table 2, §2.4) or the qualitative FPOs need to be redefined (*e.g.*, a *Catastrophic Failure Condition* only needs to be *Extremely Remote* or *Remote*) for each class of UAS.

2.5.1. Derivation of the Failure Probability Objectives

The derivation of the FPOs for UAS is described in §9, p.7-10 of [3] and is illustrated in Fig. 1. The approach is based on that used for CPA 1309 regulations (described in AMC to CS-25.1309 [6] and AC 23.1309 [19]).

Step One - Establishing the Safety Performance Baseline

Referring to Fig.1, the starting premise for the derivation of the quantified FPOs for UAS is that UAS should be at least as safe as a CPA of "equivalent" type. In accordance with the definition of a Catastrophic Failure Condition (Table 1), the safety baseline should be expressed in terms of the risk of fatal injury to more than one person on the ground. However, the approach used in UAS.1309 (Fig.1) characterises the baseline safety performance of CPA through measures of the accident rate. These measures are then assumed equivalent to measures of the hull loss rate (see note to Table 3, p.9 of [3]). The justification for using the CPA hull loss rate in place of measures of the third party fatality rate (or other measures characterising the risk of fatal injury to people on the ground) is not made explicit, however comments are made in relation to the:

a) need to use hull loss rate measures so as to be consistent with the relationship between probability and failure conditions as used in AMC CS-25.1309 (see note to Table 3, p.9 of [3]);
b) danger to third parties (in terms of the rate of CPA accidents resulting in ground fatalities) is "very small", approximately two orders of magnitude less than the total aircraft accident (§8, p.6-7 [3]).

The latter of the above comments implies that there is a requirement for UAS to demonstrate an equivalent rate of accident/hull loss to that of CPA, and that an equivalent hull loss rate will ensure UAS demonstrate an ELoS to that of CPA (herein referred to as *Assumption Two*). *Assumption Two* is confirmed in the statement "…it would be reasonable to assume that in order to maintain equivalence with manned aircraft safety, UAS could adopt the figures derived in Table 2…" p.8 [3]. Where, Table 2, p.8 of [3] contains measures of the "probability of an accident due to operational and airframe-related causes per flight hour" for a number of different CPA types.

The hull loss rate does not adequately characterise the risk to people on the ground due to aircraft operations. As will be shown in §3, a UAS operation can have a comparable accident/crash rate to an "equivalent" CPA but pose a different level of risk. These differences arise through, for example, differences in the (a) nature of the typical areas over-flown by a class of UAS compared to the nature of the areas over-flown by the "equivalent" type/class of CPA and (b) the ability of a class of UAS to cause harm to people on the ground compared to the "equivalent" type/class of CPA (*e.g.*, due to the use of frangible materials or lower energy profiles)[*]. As a result, the proposed FPOs developed on the basis of *Assumption Two* may not result in an effective management of the risks to people on the ground. This critical point is illustrated through the use of a high-level quantitative model in §3.

Table 3. Illustration of the UAS.1309 Safety Objective

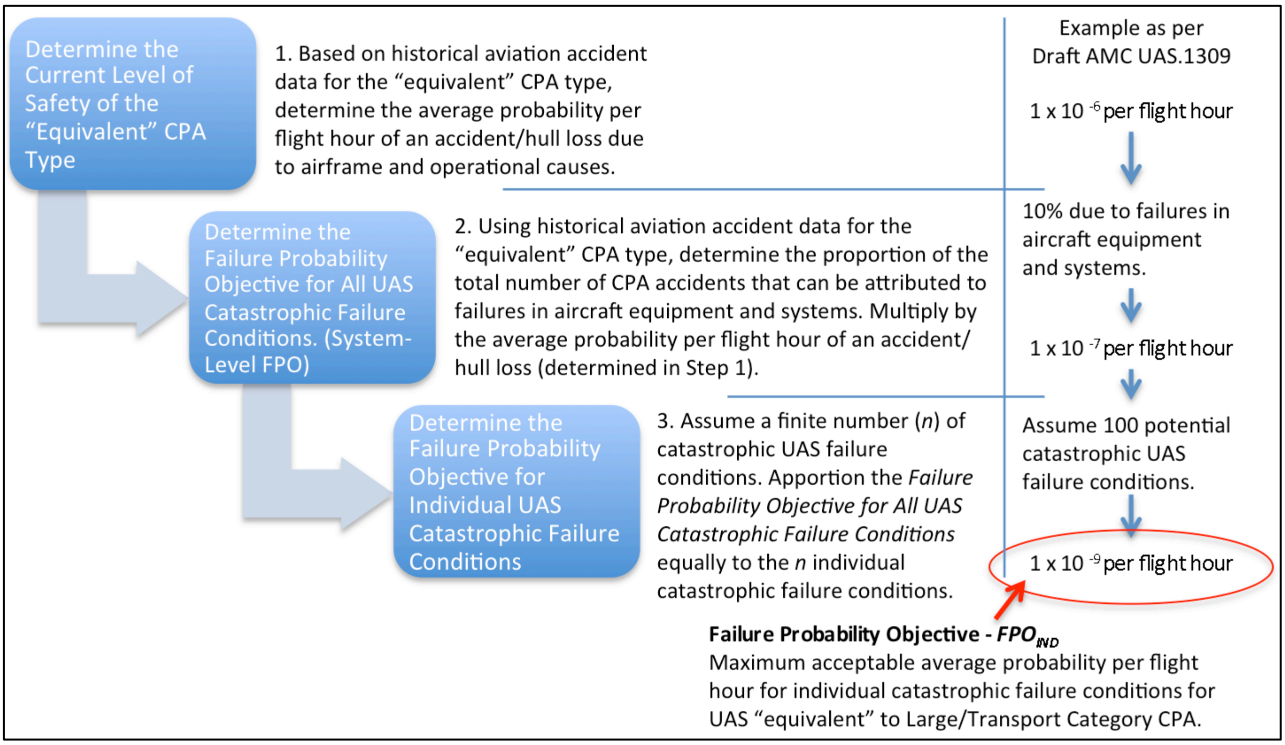
	No Safety Effect	**Minor**	**Major**	**Hazardous**	**Catastrophic**
Probable $APF_{IND} > 10^{-5}$	-	🟩	🟥	🟥	🟥
Remote $10^{-7} < APF_{IND} \leq 10^{-5}$	-	🟩	🟩	🟥	🟥
Extremely Remote $10^{-9} < APF_{IND} \leq 10^{-7}$	-	🟩	🟩	🟩	🟥
Extremely Improbable $APF_{IND} \leq 10^{-9}$	-	🟩	🟩	🟩	🟩

KEY:		
	🟩	Acceptable
	🟥	Not acceptable
	-	No probability requirement prescribed

[*] Differences in the potential harm caused given a crash primarily relate to small UAS where frangibility and energy considerations become more significant, or if the UAS has a hazardous payload (*e.g.*, hydrogen powered UAS, ordinance, chemicals, *etc*.).

Table 4. Summary of Catastrophic Failure Condition FPOs for Different Classes of UAS [3]

UAS Class	**FPO for All UAS Catastrophic Failure Conditions (FPO_{SYS})**	**FPO for Individual Catastrophic Failure Conditions (FPO_{IND})**
UAS-25 Large Transport Aircraft	$APF_{SYS} \leq 10^{-7}$	$APF_{IND} \leq 10^{-9}$
UAS-23 Class I	$APF_{SYS} \leq 10^{-5}$	$APF_{IND} \leq 10^{-7}$
UAS-23 Class II	$APF_{SYS} \leq 10^{-6}$	$APF_{IND} \leq 10^{-8}$
UAS-23 Class III	$APF_{SYS} \leq 10^{-7}$	$APF_{IND} \leq 10^{-9}$
UAS-27 Small Rotorcraft	$APF_{SYS} \leq 10^{-5}$	$APF_{IND} \leq 10^{-7}$
UAS-29 Large Rotorcraft	$APF_{SYS} \leq 10^{-6}$	$APF_{IND} \leq 10^{-8}$
UAS-VLA Very Light Aircraft	$APF_{SYS} \leq 10^{-5}$	$APF_{IND} \leq 10^{-7}$
UAS-VLR Very Light Rotorcraft	$APF_{SYS} \leq 10^{-5}$	$APF_{IND} \leq 10^{-7}$
UAS below that of CPA weights operating beyond visual line of sight (UAS-BVLOS)	$APF_{SYS} \leq 10^{-4}$	$APF_{IND} \leq 10^{-6}$
UAS below that of CPA weights operating within visual line of sight (UAS-WVLOS)	$APF_{SYS} \leq 10^{-4}$	$APF_{IND} \leq 10^{-5}$


Determine the Current Level of Safety of the "Equivalent" CPA Type
Determine the Failure Probability Objective for All UAS Catastrophic Failure Conditions. (System-Level FPO)
Determine the Failure Probability Objective for Individual UAS Catastrophic Failure Conditions
Example as per Draft AMC UAS.1309
1 x 10 $^{-6}$ per flight hour
10% due to failures in aircraft equipment and systems.
1 x 10 $^{-7}$ per flight hour
Assume 100 potential catastrophic UAS failure conditions.
1 x 10 $^{-9}$ per flight hour

1. Based on historical aviation accident data for the "equivalent" CPA type, determine the average probability per flight hour of an accident/hull loss due to airframe and operational causes.

2. Using historical aviation accident data for the "equivalent" CPA type, determine the proportion of the total number of CPA accidents that can be attributed to failures in aircraft equipment and systems. Multiply by the average probability per flight hour of an accident/hull loss (determined in Step 1).

3. Assume a finite number (n) of catastrophic UAS failure conditions. Apportion the *Failure Probability Objective for All UAS Catastrophic Failure Conditions* equally to the n individual catastrophic failure conditions.

Failure Probability Objective - *FPO$_{IND}$*
Maximum acceptable average probability per flight hour for individual catastrophic failure conditions for UAS "equivalent" to Large/Transport Category CPA.

Figure 1. Derivation of Safety Objectives for Catastrophic Failure Conditions for UAS [3]

Step Two – Calculating the FPO for All UAS Catastrophic Failure Conditions

The second step in the derivation of quantified FPOs for UAS is to determine the proportion of all accidents that can be attributed to failures of the relevant equipment and systems (Fig.1). For CPA, it is estimated that 10% of CPA accidents can be attributed "to failure conditions caused by the aeroplane's systems." [6] UAS.1309 directly adopts the same proportion of 10% and uses it to determine the FPOs for *All UAS Catastrophic Failure Conditions* (Fig.1). The direct adoption of the same proportion fails to consider the difference in the respective scope of each regulation. As described in §2.1.1, the scope of the CPA 1309 regulation is all equipment and systems, whereas UAS.1309 is restricted to the CFMS (*i.e.*, "the collection of automated systems (Synthetic Pilot) that perform the functions usually assigned to an aircraft-located pilot"). Subsequently, the proportion figure used in UAS.1309 should be based on the proportion of CPA accidents caused by pilots and not those caused by CPA equipment and systems. As pilot decision making causes most CPA accidents [29], it is likely that the quantitative FPOs derived within UAS.1309 are overly conservative.

Step Three - Calculating the FPO for Individual UAS Catastrophic Failure Conditions

The final step in the derivation of quantified FPOs is to apportion the FPO for All UAS Catastrophic Failure Conditions (the FPO defined at the system-level) to the individual failure conditions. With the exception of those UAS classified as UAS-WVLOS, UAS.1309 assumes that there are 100 potential catastrophic failure conditions attributable to equipment and systems within the UAS CFMS. An apportioning of the system-level FPO to individual Failure Conditions is ultimately required. An appropriate apportioning should take into consideration the Failure Conditions associated with the "system" and not just a single UA. Take for example the not unrealistic case of UAS where there are multiple simultaneously operating UA supported by a single Ground Control System (GCS). The CFMS can comprise of elements on-board the individual UA, belonging to the GCS and/or the communications link between them. If CFMS equipment and systems essential to the operation of both UA fail (*e.g.*, the GCS), then multiple UA accidents could then result. Such a scenario is not captured by the equal apportioning of the system-level FPO to individual systems and equipment.

2.6. Summary

To summarise, this section has provided a brief review of the components of UAS.1309 relating to the derivation of system safety objectives for the design and installation of CFMS equipment and systems for UAS. The review identifies a number of issues, of particular concern are the two critical assumptions that:

a) the failure/degradation of any CFMS equipment or system whose function is necessary to "continue safe flight and landing" of the UA will lead to multiple fatalities on the ground, and as such should be classified as catastrophic; and
b) an equivalent hull loss rate will ensure UAS demonstrate an ELoS to that of CPA.

As a consequence of these assumptions, the FPOs proposed in UAS.1309 may not result in a suitable management of the level of the risk to third party people on the ground due to UAS operations. This outcome is further explored in the following section.

3. QUANTITATIVE ANALYSIS OF UAS.1309

This section explores the effectiveness of the safety objective proposed in UAS.1309 regulation in terms of its management of the level of risk to people on the ground.

3.1. Third Party Ground Fatality Expectation Model

[21] describe a model for estimating the expected number of third party ground fatalities per flight hour due to UA operations:

$$FE = APF_{SYS} \times P_{Kill\,|\,Strike} \times P_{Strike\,|\,Impact} \times P_{Impact} \tag{1}$$

where, FE is the expected number of fatalities per flight hour, APF_{SYS} is equal to the FPO for All UAS Catastrophic Failure Conditions, $P_{Kill\,|\,Strike}$ is the probability that a person is killed given they are struck by a UA, $P_{Strike\,|\,Impact}$ is the probability that a person is struck in a given impact location, and P_{Impact} is the probability of impacting a particular location. P_{Impact} is assumed equal to one (*i.e.*, given the Catastrophic Failure, the UA will crash in the particular region of interest on the ground). The model assumes people are uniformly distributed within the area of interest and that they are all equally likely to become a fatality given an impact. Based on these assumptions, $P_{Strike\,|\,Impact}$ is taken to be the expected number of people N within the lethal impact area:

$$N = L_A \times \rho \tag{2}$$

where, L_A is the maximum lethal area in square metres and ρ is the population density of the region overflown in people per square metre. L_A is determined as the projected area on the ground for an UA following a gliding descent from the height of a person:

$$L_A = (W + 2\times R)\times(L + G_L + 2\times R) \tag{3}$$

where, W is the wingspan of the UA in metres, R is the average radius of a person (0.3048m), L is the length of the UA in metres, and G_L is the distance in metres the UA can glide from the maximum height of a person (assumed as 2.0m). The conservative assumption is made that all of the N people struck are killed (*i.e.*, $P_{Kill\,|\,Strike} = 1$). As discussed in [26, 27], this assumption is only significant for small UAS, typically with a maximum kinetic energy value of less than 42 Joules [26].

3.1.1. Limitations of the Model

The focus of this analysis is not on the fidelity of the existing model used but the general nature of the relationship between the FPOs and the degree of risk to people on the ground. It must be noted that a comprehensive representation of the risks to people on the ground should consider measures of the individual risk and societal risk in addition to the measure of the fatality expectation (a measure of collective risk). Other limitations are discussed in [21].

3.2. Case Study Unmanned Aircraft Systems

The fatality expectation model is evaluated for a range of case study UAS (Table 5). The classification criteria necessary to assign UAS to one of the 10 classes are not specified in UAS.1309 [3]. Therefore, it is assumed that UAS are assigned to a class based on the Maximum Take-Off Weight (MTOW) of the UA.

Table 5. Case Study UAS (Data From [30])

UAS Type	Maximum Take-Off Weight *(kg)*	Length *(ft)*	Wingspan *(ft)*	Assumed Class (as per [3])	FPO for All UAS Catastrophic Failure Conditions (*FPO_{SYS}*, from Table 4)
Global Hawk	11,611	44.4	130.9	UAS-25	$APF_{SYS} \leq 10^{-7}$
Predator B	4,762	35.6	66.0	UAS-23	$APF_{SYS} \leq 10^{-5}$
Shadow 200	154.2	11.2	12.75	UAS-VLA	$APF_{SYS} \leq 10^{-5}$
ScanEagle	15.4	3.9	10.2	UAS-BVLOS	$APF_{SYS} \leq 10^{-4}$

3.3. The Equivalent Level of Safety Criteria

The over-arching objective for UAS regulations is to ensure that UAS demonstrate, at a minimum, an ELoS to that of an equivalent type or class of CPA. The specification of the ELoS objective in terms of the expected number of third party ground fatalities per flight hour is summarised in Table 6. Note that the ELoS criterion determined for CPA General Aviation operations is used for those classes of UAS for which no ELoS criterion has previously been defined (*i.e.*, for UAS-VLA and UAS-BVLOS classes). The analysis in §3.4 is for UAS operations over continental Australia. The ELoS criteria in Table 6 are determined based on CPA operations in the USA. The results of the analysis in §3.4 would be improved if ELoS criteria for Australian CPA operations were available, which would account for any potential differences in the risk to third parties on the ground between the two countries (*e.g.*, potential differences in the exposure of the population due to different CPA accident rates by type, and number and distribution of flights relative to population centres, *etc*.).

Table 6. Equivalent Level of Safety (ELoS) Criteria

UAS Class	ELoS Criteria *(Third Party Ground Fatalities per Flight Hour)*	Notes
UAS-25	0.0313×10^{-06}	From [17]. Based on historical accident data for CPA operating as Air Carriers in the USA.
UAS-23	0.084×10^{-06}	From [17]. Based on historical accident data for CPA operating as General Aviation in the USA.
UAS-VLA		
UAS-BVLOS		

3.4. Analysis of Third Party Ground Fatality Risk

UAS.1309 [3] proposes quantitative FPOs independent of consideration of the areas over-flown. This subsection uses the third party fatality expectation model (§3.1) as a measure of the risk to people on the ground due to UAS operations over continental Australia. Land area and population data are obtained from the Australian Bureau of Statistics 2006 Census [31] and are summarised in Fig.2. The expected number of fatalities per flight hour is calculated for each of the case study UAS using the FPOs proposed in UAS.1309 across the range of population densities in Australia. The fatality expectation curves can then be compared against the ELoS criteria determined for the equivalent CPA type (Table 6), as shown in Fig.3.

The minimum system-level FPO necessary to satisfy the ELoS criterion (FPO_{MIN}) is also determined by rearranging Eq.1 and solving for APF_{SYS}. The results are presented in Fig.4. For comparison, the FPOs defined in the UAS.1309 (Table 5) are also plotted in Fig.4. Note, the FPOs defined in UAS.1309 appear as horizontal lines as they are derived independent of where the UAS is operated (*i.e.*, independent of ρ).

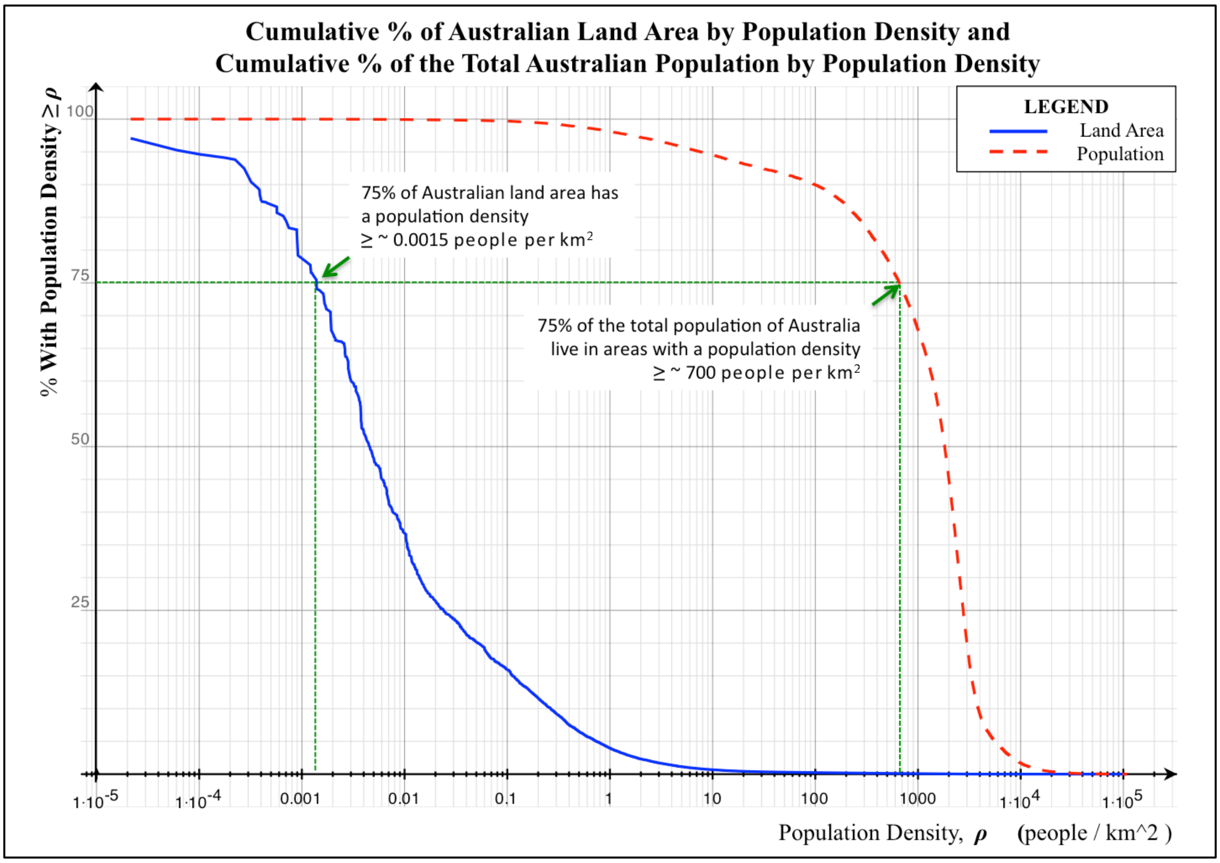


Figure 2. Summary of Australian Operational Environment

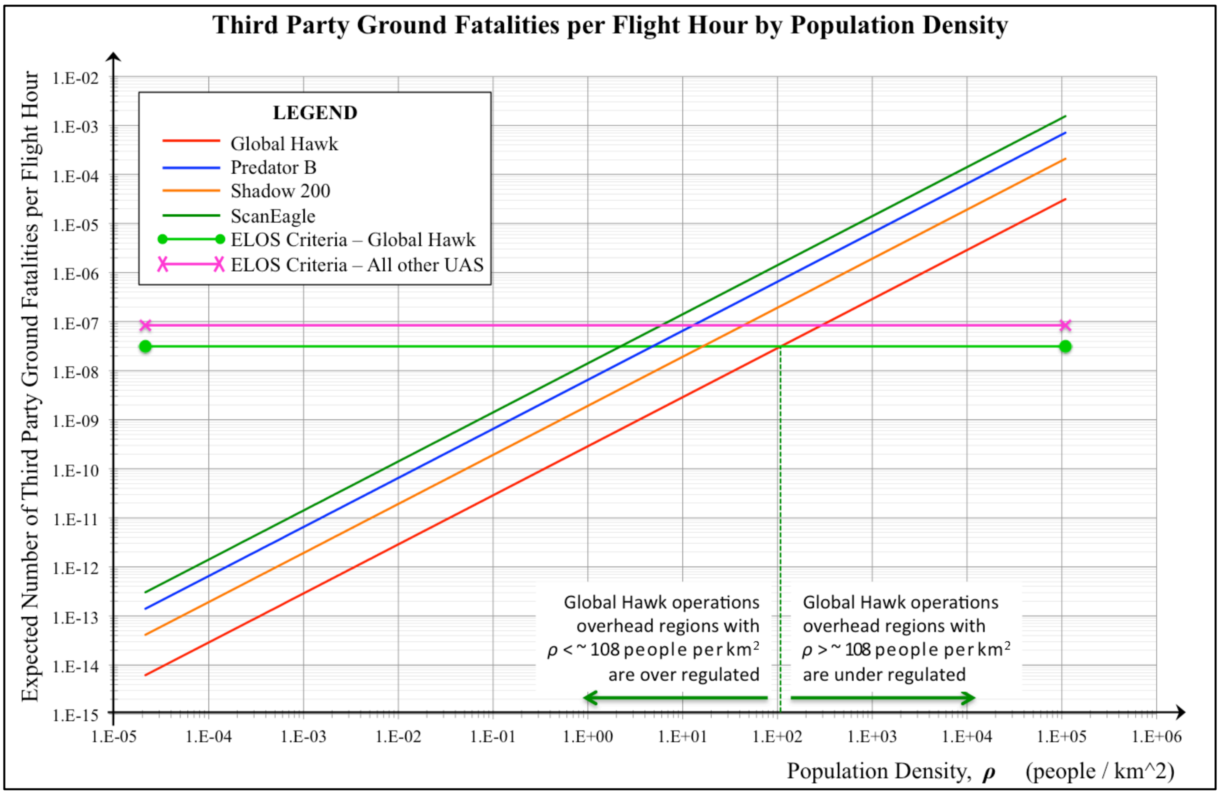


Figure 3. Third Party Ground Fatality Expectation for Different UAS Types

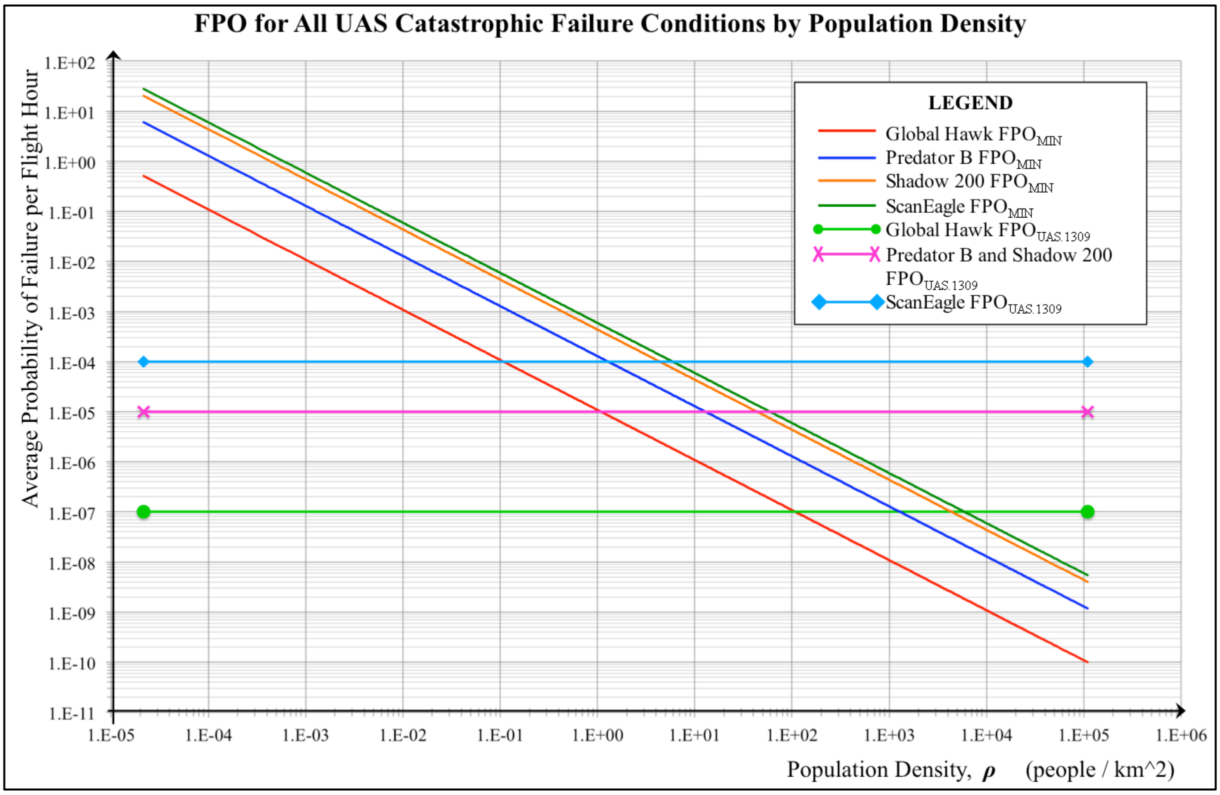


Figure 4. Minimum Failure Probability Objective Necessary to Satisfy the ELoS Objective

3.5. Discussion

Referring to Fig.3, it can be seen that the expected number of third party fatalities on the ground per flight hour varies significantly with the density of the population overflown. Logically, the fatality expectation approaches zero for UAS operations over lower population densities. Interestingly enough, the Shadow 200 UA has a lower theoretical third party fatality rate than that of the larger Predator B UA. Both UAS have the same system-level FPO (APF_{SYS} = $1x10^{-05}$, Table 4) however, the Shadow 200 UA has a lower fatality expectation due to its smaller lethal area.

The results presented in Fig.3 bring into question the validity of *Assumption One* and *Assumption Two*. It can be clearly seen that the risk (in this case characterised by the measure of the expected number of fatalities) of a UA accident/hull loss depends on the region it is over-flying. The fatality expectation rapidly approaches zero as population density, $\boldsymbol{\rho}$, decreases. Although the risk is not zero and in practice never will be [1, 32], it can be argued that the level of risk associated with UAS operations at the left end of the population spectrum are tending towards a *de minimis* level of risk (see [1] and associated references). The fatality expectation increases with population density and eventually a transition point is reached whereby the risks associated with the operation of the UAS fail to satisfy the criteria describing the minimum level of safety (*i.e.*, the ELoS criteria). The threshold population density at which this "transition" occurs can be determined for each UAS type by finding the intersection between its fatality expectation curve and the appropriate ELoS criteria line (example shown for Global Hawk in Fig.3). The threshold densities for the case study UAS types are summarised in Table 7. UAS operations over regions with population densities greater than the type's threshold population density present an unacceptable level or risk to the people overflown (*i.e.*, a level of risk greater than the risk posed by an "equivalent" CPA operation). This directly challenges the validity of *Assumption Two*; as shown in Fig.3, it cannot be assumed that an equivalent hull loss rate will result in an ELoS. Referring to Table 7, UAS can safely operate above 99% of the Australian continent (by aggregate land area), however, independent of the type of UAS operated, at least 89% of the Australian population would be exposed to an unacceptable level of risk.

Table 7. Management of Third Party Fatality Expectation by % of Australian Land Area and % of Total Australian Population

UAS Type	Threshold Population Density *(People per km²)*	% of Total Australian Land Area Exposed to an Unacceptable Level of Risk	% of Total Australian Population Exposed to an Unacceptable Level of Risk
Global Hawk	1.085×10^{02}	0.23%	89.7%
Predator B	0.129×10^{02}	0.56%	94.0%
Shadow 200	0.437×10^{02}	0.31%	91.7%
ScanEagle	0.060×10^{02}	0.98%	95.4%

The deficiency of the proposed FPOs is further illustrated in Fig.4. The FPOs proposed in UAS.1309 represent straight lines as they are mandated independent of $\boldsymbol{\rho}$. The downward sloping lines correspond to the minimum FPO necessary to satisfy the ELoS criteria for each of the case study UAS. For those UAS operations at extreme values of $\boldsymbol{\rho}$, it can be seen that the FPOs proposed in UAS.1309 are at least three orders of magnitude beneath the minimum FPOs required to satisfied the ELoS Criteria (Fig.4). Clearly more stringent FPOs are required for operations over these areas. Conversely, the FPOs proposed in UAS.1309 can exceed the minimum FPOs by up to six orders of magnitude for operations at low values of $\boldsymbol{\rho}$. It could be argued that this is an unjustifiable cost to impose on such "low risk" UAS operations. More stringent FPOs translate to higher cost through, for example, increases in the:

a) cost of components, equipment and systems (*e.g.*, the use of higher-end avionics over industrial or commercial-off-the-shelf componentry);
b) non-recurring engineering expense in the design and compliance (*e.g.*, increasing complexity in design, more detailed analysis and testing);

c) cost of continuing airworthiness (*e.g.*, higher cost of replacement parts, specialist tools, and personnel training and licensing needed to provide ongoing support for high-end equipment and systems);
d) overall weight, volume and power consumption of the installed equipment and systems (*e.g.*, additional equipment and systems required to implement redundant architectures, to eliminate single point or common-mode failures, *etc*.);
e) system performance cost (*e.g.*, reduction in system range, endurance or aerodynamic performance due to additional weight);
f) mission cost (*e.g.*, reduced capacity to support payloads or to meet mission performance requirements);
g) market cost (*e.g.*, reduction in the number of commercially-viable services/applications).

In practice few commercial business cases would support the high loss rate of UAS that would be permissible as the population density approaches zero (Fig.4). For operations over low population densities where the minimum safety criteria has been satisfied (*e.g.*, the ELoS criteria has been met), more stringent FPOs should be determined through a systematic trade-off between the costs and benefits associated with the further reduction in the risk. Such an approach is consistent with the ICAO recommendation that the policy and rulemaking activities undertaken by NAAs should be guided by a safety risk management process [32], which includes consideration of the costs and benefits associated with regulations (*i.e.*, the application of the ALARP risk management principle) [1, 32].

3.6. Summary

A high-level fatality expectation model has been used to explore key assumptions under-pinning the FPOs proposed in UAS.1309. The analysis brought into question the validity of the assumptions that (1) all UAS accidents/hull losses constitute a Catastrophic Failure Condition, and (2) an equivalency in UAS accident or hull loss rates to those exhibited by CPA will ensure an ELoS.

The model clearly showed that the "one size fits all" FPOs, which are derived from accident/hull loss rate metrics, do not provide an effective management of the risks across the spectrum of possible classes of UAS AND their operations. The proposed UAS.1309 requirements can impose unjustified costs on some UAS operations, and worse, permit some UAS operations to pose unacceptable levels of risk to the third party people overflown. A more effective management of the risks requires a shift from the "aircraft" based certification mentality as adopted for CPA, to an "aircraft and operation" based certification mentality. Such an approach is described in Clothier *et al.* [14], who propose the top-down definition of FPOs for UAS airworthiness categories (defined by the combination of a class of UAS and an operational area). The outcome is a systematic tailoring of the FPOs in line with the risks presented to third party people on the ground.

4. Conclusion

The draft AMC for UAS.1309 endeavours to adapt an existing CPA regulatory structure and apply it to UAS. Key assumptions made in this process fail to account for differences in the nature of the risk associated with the operation of the two different technologies. The result is a regulation that does not provide an effective management of the risks. It is contended here that the "default position" of adopting existing regulatory structures and standards should be guided by a safety risk management process (a position consistent with recommendations made by ICAO [32]). The safety risk management process includes a structured assessment of the relevant risks and decision-making that takes into account the risks, costs, and benefits associated the development and promulgation of a proposed regulation.

References

[1] Clothier, R A and Walker, R A. The Safety Risk Management of Unmanned Aircraft Systems. To appear in The Handbook of Unmanned Aerial Vehicles, K. P. Valavanis and G. J. Vachtsevanos, Eds., Springer Science + Business Media B.V., Dordrecht, Netherlands, 2012 (In Press).

[2] JAA/EUROCONTROL. A Concept For European Regulations For Civil Unmanned Aerial Vehicles (UAVs). The Joint JAA/EUROCONTROL Initiative on UAVs, 11 May 2004.

[3] JARUS. JARUS II: AMC UAS.1309, Draft, Issue B. UAS Systems Safety Analysis 1309 Group, Joint Authorities for Rulemaking of Unmanned Systems (JARUS), August 2011.

[4] EASA. Annex to ED Decision 2011/004/R, Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes (CS-25), Ammendment 11. European Aviation Safety Authority (EASA), 4 July 2011.

[5] FAA. FAR Part 25, Airworthiness Standards: Transport Category Airplanes, Federal Aviation Regulation (FAR), Title 14, Code of Federal Regulations (CFR). Accessed on 10 January 2012.

[6] EASA. AMC 25.1309, System Design and Analysis, Annex to ED Decision 2011/004/R, Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes (CS-25), Ammendment 11. European Aviation Safety Authority (EASA), 4 July 2011.

[7] FAA. AC-25.1309-1A, System Design and Analysis. Federal Aviation Administration (FAA), U.S. Department of Transportation, 21 June 1988.

[8] Brewer, N. A Brief Explanation of the JARUS AMC UAS.1309 Concept. Presented at the Unmanned Aircraft Systems Operational and Technology Readiness Conference, Royal Aeronautical Society (RAeS), London, 2011. Available: http://aerosociety.com/Assets/Docs/Events/672/672_Nick_Brewer.pdf (Accessed: 5 April 2012)

[9] EASA. Annex to ED Decision 2009/003/R, Certification Specifications for Very Light Aeroplanes (CS-VLA), Ammendment 1. European Aviation Safety Agency (EASA), 5 March 2009.

[10] EASA. Annex to ED Decision 2008/011/R, Certification Specifications for Very Light Rotorcraft (CS-VLR), Ammendment 1. European Aviation Safety Agency (EASA), 17 November 2009.

[11] FAA. FAR Part 27, Airworthiness Standards: Normal Category Rotorcraft, Federal Aviation Regulation (FAR), Title 14, Code of Federal Regulations (CFR). Accessed on 10 January 2012.

[12] EASA. Annex to ED Decision 2008/009/R, Certification Specifications for Small Rotorcraft (CS-27), Ammendment 2. European Aviation Safety Agency (EASA), 17 November 2008.

[13] Hayhurst, K J, Maddalon, J M, Miner, P S, DeWalt, M P, and McCormick, F G. IEEE/AIAA Unmanned Aircraft Hazards and their Implications for Regulation. In 25th Digital Avionics Systems Conference (DASC), Portland, USA, 2006, pp. 1-12.

[14] Clothier, R A, Palmer, J L, Walker, R A, and Fulton, N L. Definition of an Airworthiness Certification Framework for Civil Unmanned Aircraft Systems. Safety Science*,* vol. 49, pp. 871-885, 2011.

[15] De Florio, F. Airworthiness - an Introduction to Aircraft Certification. Butterworth-Heinemann, Burlington, MA, 2006.

[16] Haddon, D and Whittaker, C. Aircraft Airworthiness Certification Standards for Civil UAVs. UK Civil Aviation Authority (CAA), Department for Transport (DfT), London, August 2002.

[17] Clothier, R A and Walker, R A. Determination and Evaluation of UAV Safety Objectives. Presented at the 21st International Unmanned Air Vehicle Systems Conference, Bristol, United Kingdom, 2006.

[18] NATO. STANAG 4671 (Edition 1) - Unmanned Aerial Vehicles Systems Airworthiness Requirements (USAR). NATO Standardization Agency (NSA), North Atlantic Treaty Organization (NATO), Brussels, Belgium, 3 September 2009.

[19] FAA. AC 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes. Federal Aviation Administration (FAA), U.S. Department of Transportation, 17 Nov 2011.

[20] Weibel, R and Hansman, R. Safety Considerations for Operation of Different Classes of UAVs in the NAS. In American Institute of Aeronautics and Astronautics, 3rd "Unmanned Unlimited" Technical Conference, Workshop and Exhibit, Chicago, Illinois, 2004.

[21] Clothier, R A, Walker, R A, Fulton, N L, and Campbell, D A. A Casualty Risk Analysis For Unmanned Aerial System (UAS) Operations Over Inhabited Areas. Presented at the Twelfth

Australian International Aerospace Congress (AIAC-12), 2nd Australasian Unmanned Air Vehicles Conference, Melbourne, Australia, 2007.

[22] Dalamagkidis, K, Valavanis, K P, and Piegl, L A. Evaluating the Risk of Unmanned Aircraft Ground Impacts. Presented at the 16th Mediterranean Conference on Control and Automation, Ajaccio, France, 2008.

[23] Thompson, K M. Variability and Uncertainty Meet Risk Management and Risk Communication. Risk Analysis, vol. 22, pp. 647-654, 2002.

[24] Thompson, K M, Rabouw, R F, and Cooke, R M. The Risk of Groundling Fatalities from Unintentional Airplane Crashes. Risk Analysis, vol. 21, pp. 1025-1037, 2001.

[25] Goldstein, B L, Demak, M, Northridge, M, and Wartenberg, D. Risk to Groundlings of Death Due to Airplane Accidents: A Risk Communication Tool. Risk Analysis, vol. 12, pp. 339-341, 1992.

[26] Clothier, R A, Palmer, J L, Walker, R A, and Fulton, N L. Definition of Airworthiness Categories for Civil Unmanned Aircraft Systems (UAS). Presented at the 27th International Congress of the Aeronautical Sciences, Nice, France, 2010.

[27] Fraser, C and Donnithorne-Tait, D. An Approach to the Classification of Unmanned Aircraft. In Bristol International Unmanned Aerial Vehicle Systems (UAVS) Conference, Bristol, UK, 2011, pp. 157-211.

[28] SAE. ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. Aircraft And Systems Development And Safety Assessment Committee, Society Automotive Engineers (SAE), December 1996.

[29] FAA. FAR Part 23, Airworthiness Standards: Normal, Utility, Acrobatic and Commuter Airplanes, Federal Aviation Regulation (FAR), Title 14, Code of Federal Regulations (CFR). Accessed on 10 January 2012.

[30] RTCA. DO-320, Operational Services and Environmental Definition (OSED) for Unmanned Aircraft Systems (UAS). RTCA, Washington, DC., 10 June 2010.

[31] ABS. (2012, 28 January). *2006 Census Data*. Available: http://www.abs.gov.au/websitedbs/censushome.nsf/home/Census (Accessed: 5 April 2012)

[32] ICAO. Safety Management Manual (SMM), Doc 9859. International Civil Aviation Organization (ICAO), Montréal, Quebec, Canada, 2009.