

# **SAFETY ASSESSMENT & CERTIFICATION FOR UAS**

**Andrew R Evans & Dr Mark Nicholson**

**JRA Aerospace Ltd / The University of York**

(andy.evans@jra-aero.com / mark.nicholson@cs.york.ac.uk)

## **ABSTRACT**

As part of the certification process to gain clearance to operate in unsegregated airspace, new UASs will require a robust Safety Assessment process. The authors have looked at the civil manned aircraft safety assessment process defined in ARP 4761 and the safety certification process in ARP4754, as used to demonstrate compliance with EASA / FAA safety target requirements, in order to develop a UAS-applicable process.

The paper looks at the background to UAS safety assessment, in particular why UAS need a structured Safety Assessment process in order to gain access to unsegregated airspace. It then goes on to propose a 'UAS-friendly' safety assessment process, and particularly, UAS hazard identification using a revised Functional Failure Analysis (FFA) method.

## **BIOGRAPHIES**

Andy Evans joined British Aerospace in 1986, with a BSc in Aeronautical Engineering. There (over 7 years) he worked in trials and certification, and cockpit design. Moving to GEC-Marconi, he worked as systems engineer then Technical Procurement Manager on new guided weapon projects. Andy became a consultant in 1996, working on the Jaguar Avionic Upgrade Programme to integrate and clear novel systems, including the first Helmet Mounted Sight in RAF service. Concentrating on system safety and clearance from 1998, he developed Safety Management Systems and safety cases for legacy aircraft platforms, and provided independent assessment of contractor qualification and clearance documentation. Andy joined JRA Aerospace as Director of Safety in 2002, where he is responsible for providing safety management services to defence and civil aerospace clients. Completing a part-time MSc in Safety Critical Systems Engineering at the University of York in 2006, his project looked at the hazards of UAS operation in unsegregated airspace. As a result, Andy is a member of EUROCAE WG73, working to enable the clearance of UASs for operation in unsegregated airspace.

Dr Mark Nicholson is a Research and Teaching Fellow in System Safety Engineering in the High Integrity Systems Engineering Group in the Department of Computer Science at the University of York. He coordinates and teaches on the Masters programs in System Safety Engineering, Safety-Critical System Engineering and Gas Turbine Control in the Department. He has been researching issues in hard real-time and safety-critical systems for more than 15 years. His doctoral research focused upon issues surrounding the selection of architectural structures with appropriate reliability, timing and safety characteristics. He has undertaken extensive research and consultancy collaboration with organisations such as Airbus, BAE SYSTEMS, Rolls Royce, Eurocontrol and the CAA. He has been involved in European framework projects including PAMELA and VICTORIA. He is also a member of EUROCAE WG63 updating the aerospace recommended practices (ARP) 4754 / 4761. This current work comes out of an MSc project and extends his work by looking at how the ARPs can be used / amended to support the use UASs in a civil environment.

## Introduction

As part of the certification process to gain clearance to operate in unsegregated airspace, new UASs will require a robust Safety Assessment process. The authors have looked at the civil manned aircraft safety assessment process (ARP 4761) and the safety certification process (ARP4754), as used to demonstrate compliance with EASA / FAA safety target requirements, in order to develop a UAS-applicable process.

The paper looks at the background to UAS safety assessment:

- Why UAS need a structured Safety Assessment process in order to gain access to unsegregated airspace
- A (very brief) overview of manned aircraft safety assessment requirements and the role of ARPs 4761 and 4754 in showing compliance.
- The differences introduced by UAS that need to be considered, to ensure safety – in particular:
  - Possible safety criteria and for UAS
  - Dealing with system complexity, as the UAS is not neatly bounded by the air vehicle
  - Relating to the 'outside world' System of Systems (including Air Traffic Management)
  - Exotic mission types, environments, flight phases and emergency actions

The paper then proposes a 'UAS-friendly' safety assessment process, and particularly, UAS hazard identification using a revised Functional Failure Analysis (FFA) method:

- The use of airworthiness and traffic separation safety targets to determine 'total safety'
- A 'UAS-level' FFA to assess the complex system boundary, and a Rich Context Diagram to bring in interfaces with the wider System of Systems.
- Particular modifications to the FFA method to take account of UAS environments, emergency conditions, mission types and phases, and (critically) unusual consequences of system 'failures'.

## Why UAS need a structured Safety Assessment process

Indications are that the failure rate for UAS is currently too high. DeGarmo [1] quotes US DoD analyses that show the UAS catastrophic failure rate (in terms of vehicles lost rather than induced fatalities) at around 50 times that of an F16, and around 100 times that of more general aviation. Another statistic compares an accident rate of 0.06 per million flying hours for U.S. commercial aircraft in U.S. airspace to a rate of 1,600 per million flying hours for the Global Hawk. Clearly such figures, if read across to UAS operation in unsegregated airspace and larger UAS fleets, would not seem tenable.

Part of the problem is the data - all of it, currently, is sourced from military UAS which have often been rushed from research into service (e.g. Predator use in Afghanistan); have been employed in fairly high-risk operations; and come from a very small sample, compared to the manned fleet they are being compared with ([1]). Nonetheless, such figures would not currently support integration. If the situation is to improve, we need to understand the causes for the poor safety record. This is not easy: as Williams [2] notes in his review of UAS Human Factors issues, there is a lack of good, reported UAS accident data, even in the military.

DeGarmo [1] picks through what is available to reach indications of the causes. He quotes DoD analyses that around 75-85% of the failures were due to equipment failure – these failures, in turn, break down into:

- 37% propulsion
- 26% flight control
- 11% communications link
- 17% human factors
- 9% miscellaneous

He states that such figures are not unexpected: as we noted above, the current generation of UAS stem from research programmes, and/or have been rapidly put together to satisfy high risk operations at low cost, thus redundancy and reliability have not been high priorities. It is not stated, but we can presume that military programmes have also assumed a higher acceptable risk level, combined with operation over unfriendly territory, so concerns over ground or air collisions have also been pretty low - we are not assessing the record of systems designed for operation in integrated airspace over 'friendly' populated areas!

Schneider [3] concurs, providing a little more detail on the equipment failings:

- Propulsion system unreliability relates to the search for a reliable 'heavy fuel' engine that can cope with the extended endurance requirements, at temperatures and altitudes not generally experienced.
- The flight control failures, on the other hand, relate to the use of Commercial Off The Shelf (COTS) actuators, some drawn from commercial non-aviation sources (hence not intended for this level of criticality) and often being used outside their intended environment.

Schneider concludes that, while current UASs could have been designed, fabricated and maintained to manned aircraft levels, this had clearly not been the case so far. Marsters [4] states that "It is very important that the overall safety-assurance for UAS operations outside reserved airspace be based upon the design, development and maintenance of highly reliable air vehicles." He presses on that UAS reliability and their contingent catastrophic failure rate must be acceptable by civil aviation standards (discussed briefly, below), and this can only be achieved by adopting *a stringent system-safety design regime for UASs*. What he proposes is to incorporate a 'FAR 1309-type' philosophy in the UAS flight-critical system safety design, and refers to ARP 4761 [5] as a suitable approach for safety analyses.

This requirement for structured safety assessment is being taken up by regulators:

- The Swedish Aviation Safety Authority, [6] looked at JAR 25.1309 and JAR 23.1309 requirements for manned ac, and briefly compared the applicability to UASs. They concluded that targets such as allowable failure rates should be adopted, but that the safety assessment methodology should be amended to suit the differences in UAS.
- The Joint European Task Force, in [7] concluded that the certification of UAS should follow a route similar to that for manned aircraft, against defined standards. However, it was also made clear that a safety objective approach based on EASA CS.25 / CS.23.1309 type requirements should be established, and compliance through structured safety assessment process be followed. This is the approach being taken forward by EASA in their 'Advance Notice of Proposed Amendment 16'.

In summary – UAS developers need to apply a structured safety assessment process because:

- Current catastrophic failure rates (through the results of less-structured design approaches) would be too high to allow flight in unsegregated airspace;
- UAS need to achieve a level of safety 'equivalent' to that for manned aircraft, and the recommended route to this is through applying equivalent safety processes;
- Regulators will demand such safety processes, in order to comply with '1309' equivalent safety objectives.

## Overview of Manned Aircraft Safety Assessment

This section provides a very brief overview of manned aircraft safety assessment, as context for the rest of the discussion. For further information on current requirements, we would recommend the reader to the Certification Standards on the EASA web-site, at [www.easa.eu.int/home/certspecs\\_en.html](http://www.easa.eu.int/home/certspecs_en.html).

Requirements for airworthiness standards have grown steadily, as the capability and number of manned aircraft has increased. While aircraft remained relatively simple, airworthiness and safety certification focussed on 'headline' criteria such as performance and flight handling. With the introduction of more and more supporting systems on the aircraft, regulators realised that safety issues could remain hidden unless a structured means was established for assessing hazards through failures or system interactions.

Hence a section covering equipment, systems and installations (so-called '1309' safety objective requirement, after its section number) is now included in certification specifications such as EASA CS.25 for large aircraft and CS.23 for normal, utility, aerobatic and commuter aircraft (and indeed in the FAA and JAR documents, from which these EASA equivalents are largely drawn). The '1309' requirements themselves are fairly short, primarily requiring identification of any systems and equipments necessary to allow other certification requirements to be met; dictating an acceptable inverse relationship between the probability and severity of failure of such systems and equipments; and requiring the resolution of such hazards through system reliability / redundancy, system monitoring, crew alerting and the capability for corrective action to be taken.

A better appreciation of the safety assessment requirement emerges through looking at the 'guidance' given for these requirements. The Acceptable Means to Compliance provided in Book 2 to each standard or as additional documentation such as the 'Advisory Circulars' published by the FAA (see [8] and [9] for examples) show the types and levels of analysis required to convince the regulators. Functional Hazard Assessments (FHA) are recommended to identify the scope and criticality of functional failures; then analyses such as Fault-Tree Analysis (FTA), Failure Modes and Effects Analyses (FMEA), and Common Cause Analysis (CCA) methods are proposed as suitable analyses for safety certification.

The expectation for robust, structured safety assessments has grown in proportion to the increasing complexity and interaction of aircraft systems. The 'Acceptable Means of Compliance' have spawned their own guidance, in particular that produced by SAE in [10] and [5]. These documents provide additional detail, recommending what analyses to conduct and how to do so in an appropriate manner, as 'one means' of satisfying the high-level '1309' requirements. ARP 4754 discusses the certification aspects of highly-integrated or complex systems installed on aircraft, taking into account the overall aircraft operating environment and functions. It has also been called up as the Means of Compliance on overall aircraft projects, such as the A380. ARP 4761 provides in depth guidance on the techniques used to meet the requirements, and processes, set out in ARP 4754. ARP4761 proposes aircraft-level and sub-system level FHA, flowing down to more detailed Preliminary System Safety Analyses (PSSA) consisting of qualitative FTA and FMEA to help set safety requirements for critical systems; then conduct of System Safety Analyses (SSA) of detailed quantitative FTA and FMEA, backed up with CCA to identify hidden interactions, as the system design is implemented. The whole is accepted as a suitable Safety Assessment means to support certification that safety requirements have been achieved. Figure 1 shows the context of safety assessment within the system development process, with the flow through from FHA into more detailed design analyses, then building through integration into system certification.

Safety assessment requirements and methods have come a long way since manned aircraft first took to the air. Such assessments for UAS will need to be established in far shorter timescales, in order to allow integration into unsegregated airspace.

## **The Differences in UAS that Safety Assessment Must Address**

Having reviewed some of the safety assessment regulation, compliance and guidance material provided for manned aircraft, there are key areas where UASs differ, which are discussed below. These aspects must be addressed for the safety assessment to robustly identify and manage the hazards of UAS operation in unsegregated airspace.

### **Safety criteria**

Safety criteria drawn from EASA CS.25.1309 (and FAR / JAR 25.1309) talk in terms that are focused on manned, large aircraft airworthiness. For example, a Catastrophic consequence is defined as "All failure conditions which prevent continued safe flight and landing". Criteria descriptions for UAS need to reflect air vehicle potential occurrences, such as those proposed by the JAA / EUROCONTROL Joint Task Force in [7]. For example, they suggested modifying the catastrophic definition above, to "UAS's inability to continue controlled flight and reach any predefined landing site".

Perhaps more revolutionary is the need to consider 'total system safety' as required by EASA, rather than just airworthiness. For this, the criteria need to reflect occurrences that compromise safety through the Air Traffic Management (ATM) or operational context. EUROCONTROL have established related (but different!) criteria that they insist are applied where an occurrence could affect the ATM environment, through EUROCONTROL Safety Regulatory Requirement 4 (ESARR 4) [11].

### **System Complexity – beyond the Air Vehicle**

[5] proposes that Functional Hazard Assessment (FHA) be carried out at what it calls the 'Aircraft-Level', then lower 'System-Level' assessments once the design work starts in earnest. However, for UAS, safety criticality of systems extends beyond the air vehicle. The safety assessment boundary needs to be widened to address this complexity of the system:

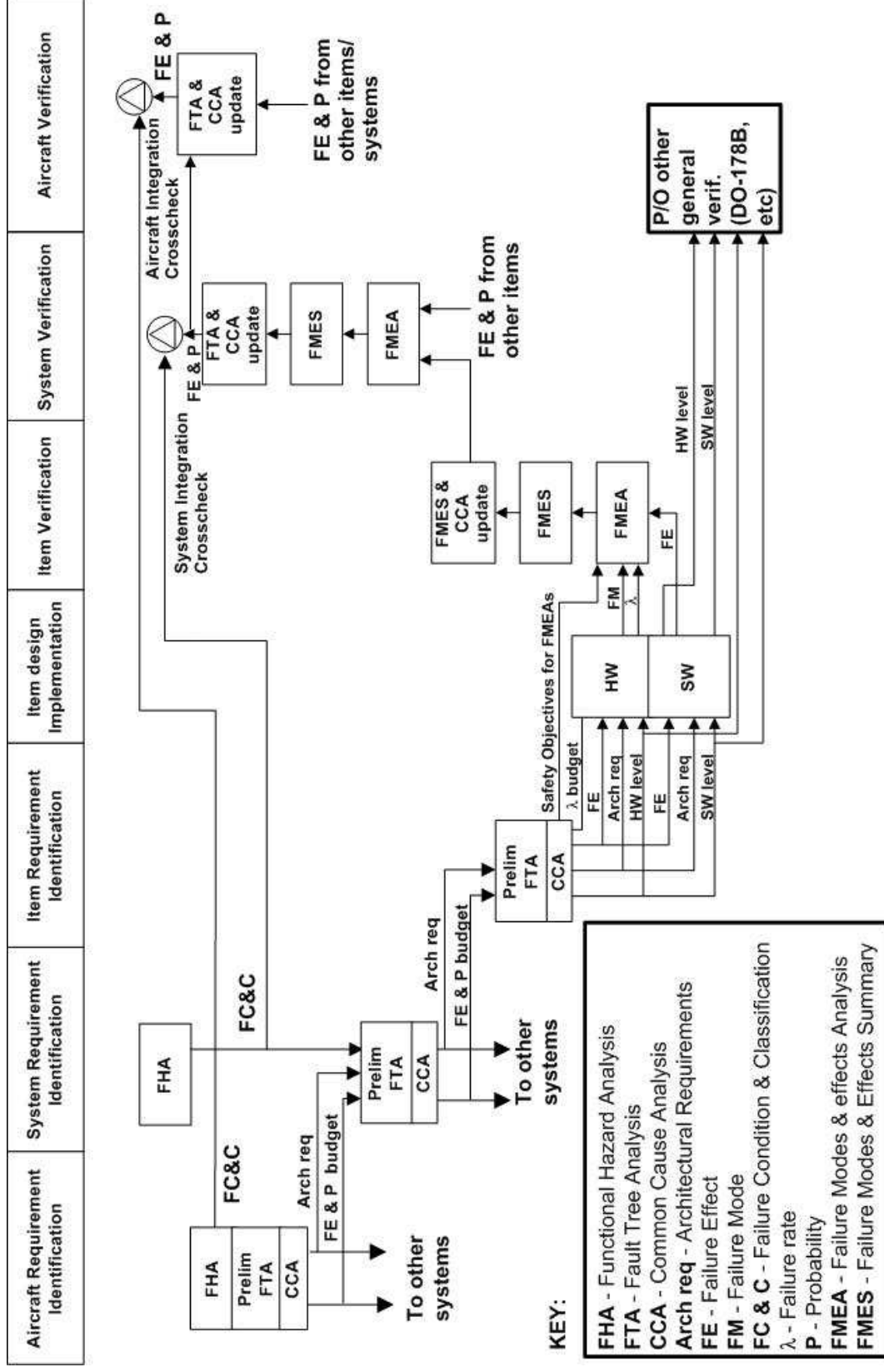


Figure 1 – Overview of safety assessment process, from ARP4761 requirements for manned aircraft systems [5]

- How to identify and assess the extended critical boundary, for 'hard' system elements such as the Datalink and Ground Control System (GCS)
- Identification and assessment of 'softer' elements with safety criticality, such as mission planning
- For 'unmanned' air systems, there may still be critical dependencies on people, their competencies and actions, and procedural elements. These need to be identified and assessed
- Autonomy presents particular challenges for safety assessment. There may well be issues of *technology* and *complexity* over system architecture, but particular concerns over *predictability* of the system. How and where should these aspects be tackled in safety assessment?

### Relating the UAS to the 'Outside World' System of Systems

UAS (generally) have a complex interaction with a wide variety of external systems. This 'system of systems' (where individual systems are linked together in a loose-coupled manner) provides a new challenge for UAS safety assessment.

Some systems, such as Air Traffic Management, while taken for granted in manned aircraft, require different system approaches for UAS. Safety assessment needs to consider what the critical elements are, and how they are managed – elements such as ATC system interoperability, voice commands and communications, interaction with other traffic, recognition of visual signals, and so on.

Other aspects are new, or could become of heightened criticality for UAS. Mission planning is dependent on the gathering, manipulating and communicating of data from many external sources; Weather reporting and analysis may have more significant effects on small craft or datalinks; UAS systems may operate within a larger network of information gathering and communicating systems; UAS may be more dependent on the accuracy and reliability of GPS navigation satellites; etc.

Hence, safety assessment needs to consider not just the UAS, but its *context*, its place within the wider system of systems (to the extent that safety may be affected).

### Exotic Characteristics

UAS introduce a range of different characteristics from their manned counterparts: Safety assessment methods (brought up on fairly steady assumptions of aircraft behaving in certain ways and operating in 'usual' environments) will need to be alert and able to assess these differences for hazards. Some areas of difference are touched on, below:

- Unusual mission types – a UAS may undertake a range of mission types, each quite different from the fairly benign world of transport aircraft. These may introduce new terrain types, flight profiles and performance considerations. They may also introduce different phases of flight to be considered within a given mission.
- Environments – the exotic performance capabilities of some UAS expose the system to very different environments. Altitude, speed, endurance capabilities of the system may expose the vehicle in turn to a broad range of climatic, weather, electrical, overflowed terrain and air traffic environments.
- Emergency / abnormal flight conditions – regulators will require new Particular Emergency Conditions to be assessed, such as datalink failure response and effect of Flight Termination (or Emergency Recovery) procedures, with or without the UAS ground pilot in the loop. Other critical aspects to be assessed will stem from the UAS system architecture under consideration. It is likely that the number and range of such conditions will be greater than for manned equivalents.

UAS are at the same time similar and different to manned aircraft. The system safety assessment, while drawing on manned equivalents, will need to be able to identify and analyses these differences robustly.

### Proposing a 'UAS-Friendly' Safety Assessment Process

The safety assessment process defined in [5] is a well-known approach among developers of manned aircraft systems, and an acceptable means of compliance for regulators. From our investigations, it is proposed that, with modification to capture hazards from 'differences', it provides a good basis for UAS developers also. Some of these proposed modifications are discussed below, focussing on the up-front hazard identification aspects of the Functional Hazard

Assessment. In showing how this can be made more 'UAS-friendly', to ensure UAS specific hazards will be identified, provides the spring-board to a robust safety process for the whole UAS development.

The following discussion assumes some awareness of Functional Hazard Analysis, "...a systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity" [5]. The reader is referred to the descriptive material in [5] if necessary to provide further context to this paper.

### Safety Criteria

We need to define suitable safety criteria in order to assess the effects and consequences of potential UAS hazards. The first consideration is "who is likely to be affected by the UAS". A quick review of existing airworthiness criteria such as in [9] leads us to the following traditional parties:

- Passengers of the vehicle? NO, this should not be an issue for a UAV.
- Flight crew - NO (but possibly indirect effects on UAS operators?).
- The air vehicle itself

ARP 4761 [5], looking to support ARP 4754 [10] (and hence EASA CS.25.1309) focuses on these parties, to give a set of airworthiness criteria. It can be argued that, if the aircraft is kept safely in the air, then the safety of the 3rd parties on the ground is necessarily protected. The Joint UAV Task Force [7] suggested modifications to these criteria to make them more UAS applicable and from these a modified set of airworthiness criteria has been drawn together as shown in Table (i) below.

Looking at a wider requirement for overall safety (and not just airworthiness) leads us to the following affected parties, additionally:

- 3rd parties on the ground - the overflown public.
- 3rd parties in other aircraft - in the air or on the ground at airfields.
- ATM personnel

It could be argued that, in providing criteria aimed at keeping the aircraft reliably in the air, the requirements of the overflown public are met (especially as the criteria in [7] include consideration of whether the vehicle can reach an unpopulated site) - this is consistent with the view that UAS must meet an Equivalent Level of Safety

to that for manned aircraft, and the criteria above are set for manned aircraft. What then should be done about the second two parties, other aircraft occupants and ATM personnel, where the criteria currently say little? EUROCONTROL are insistent that their criteria must be applied in all instances where the ATM environment may be affected. Although the criteria are focussed on applications for ATM system developments, it can be seen that they would be applicable for a UAS and particular concerns over manned aerospace integration. These criteria are shown in Table (ii) below.

First thought was to try and combine these criteria with those previously, e.g. to add the 'Severity 1' criteria to those for 'Catastrophic'. However, on further consideration, this was rejected:

- The criteria are specifically separation and collision focussed, and do not map well onto airworthiness criteria.
- The criteria introduce issues which may have no airworthiness causes - particularly in the way they consider effects on ATM personnel and 'flight crew' (or UAS operators in our case).
- The associated probability targets required by EUROCONTROL under the ESARR 4 regulation do not line up directly with those for airworthiness under CS.23.1309 or CS.25.1309; hence the requirements for a merged category would be out of step.

Overall, it was felt clearer to maintain the different severity titles in order to dissuade readers' instinctive attempts to merge the safety objectives.

What is arrived at is a *dual-criteria system*, to satisfy different hazard types and regulatory bodies. This might seem unwieldy, but should be fairly simple to apply in practice:

For hazards and potential accidents where the UAV comes to ground - affecting the overflown population and / or the UAV itself: apply the Airworthiness safety criteria. These will be predominantly due to airworthiness and reliability causes, and the effect will vary with the system size and speed (see Safety Objectives below). They will also fit within the airworthiness occurrence reporting regime.

Safety Assessment & Certification for UAS

<b>Failure Severity Classification</b>	<b>Condition</b>	<b>FAA Minor</b>	<b>Major</b>	<b>Severe Major</b>	<b>Catastrophic</b>
		<b>JAA Minor</b>	<b>Major</b>	<b>Hazardous</b>	<b>Catastrophic</b>
<b>Existing Condition Effect criteria</b> ( FAA & JAA / EASA manned aircraft assessments)		<ul style="list-style-type: none"> <li>- Slight reduction in safety margins</li> <li>- Slight increase in crew workload</li> <li>- Some inconvenience to occupants</li> </ul>	<ul style="list-style-type: none"> <li>- Significant reduction in safety margins or functional capabilities</li> <li>- Significant increase in crew workload or in conditions impairing crew efficiency</li> <li>- Some discomfort to occupants</li> </ul>	<ul style="list-style-type: none"> <li>- Large reduction in safety margins or functional capabilities</li> <li>- Higher workload or physical distress such that the crew could not be relied on to perform tasks accurately or completely</li> <li>- Adverse effects upon occupants</li> </ul>	<ul style="list-style-type: none"> <li>- All failure conditions which prevent continued safe flight and landing</li> </ul>
<b>Proposed UAS criteria</b> (taken from UAV Task Force [UTF04])		<ul style="list-style-type: none"> <li>- Slight reduction in safety margins (e.g. loss of redundancy)</li> </ul>	<ul style="list-style-type: none"> <li>- Significant reduction in safety margins (e.g., total loss of communication with autonomous flight and landing on a predefined emergency site)</li> </ul>	<ul style="list-style-type: none"> <li>- Controlled loss of the UAV over an unpopulated emergency site, using Emergency Recovery procedures where required.</li> </ul>	<ul style="list-style-type: none"> <li>- UAV's inability to continue controlled flight and reach any predefined landing site</li> </ul>

**Table (i) - Airworthiness Failure Condition Severities (after [5], with additions from [7] as noted)**

Safety Assessment & Certification for UAS

Failure Condition Severity Classification	Severity 5 - No Severity Immediate Effect Incidents on Safety	4 - Minor	Severity 3 - Significant Incidents	Severity 2 - Major Incidents	Severity 1 - Accidents
Failure Condition Effect	<ul style="list-style-type: none"> <li>No hazardous condition i.e. no immediate direct or indirect impact on the operations</li> </ul>	<ul style="list-style-type: none"> <li>Increasing workload of the air traffic controller or [UAS] crew, or slightly degrading the functional capability of the enabling CNS System.</li> <li>Minor reduction (e.g., a separation of more than half the separation minima) in separation with [UAS] crew or ATC controlling the situation and fully able to recover from the situation.</li> </ul>	<ul style="list-style-type: none"> <li>Large reduction (e.g., a separation of less than half the separation minima) in separation with [UAS] crew or ATC controlling the situation and able to recover from the situation.</li> <li>Minor reduction (e.g., a separation of more than half the separation minima) in separation without [UAS] crew or ATC fully controlling the situation, hence jeopardising the ability to recover from the situation (without the use of collision or terrain avoidance manoeuvres).</li> </ul>	<ul style="list-style-type: none"> <li>Large reduction in separation (e.g., a separation of less than half the separation minima), without [UAS] crew or ATC fully controlling the situation or able to recover from the situation.</li> <li>One or more aircraft deviating from their intended clearance, so that abrupt manoeuvre is required to avoid collision with another aircraft or with terrain (or when an avoidance action would be appropriate).</li> </ul>	<ul style="list-style-type: none"> <li>One or more catastrophic accidents</li> <li>One or more mid-air collisions</li> <li>One or more collisions on the ground between two aircraft</li> <li>One or more Controlled Flight Into Terrain</li> <li>Total loss of flight control.</li> <li>No independent source of recovery mechanism, such as surveillance or ATC and/or [UAS] crew procedures can reasonably be expected to prevent the accident(s).</li> </ul>

Note: our substitution of [UAS] for flight crew references.

Table (ii) - EUROCONTROL ATM-Focused Separation / Collision Safety Criteria (from [11])

If a situation arises with potential overlap, i.e. it could cause both an airworthiness and collision risk, what then? It is not easy to 'pick the highest severity' as the different criteria have different safety targets. A different view is that such situations will need the different criteria at different times (e.g. a failure in control causes a UAV to wander off through controlled airspace first, before ultimately crashing to the ground). Hence our proposal is to split the potential hazard into its airworthiness and collision components, and apply each criterion to the applicable component.

### **The Complex System Boundary**

#### Dealing with the UAS System boundary & complexity

As noted earlier, there were concerns over the 'airworthiness' boundary for the UAS. It is clear that the critical elements extend beyond just the air vehicle itself, and probably include elements such as the GCS, the Datalink, the Flight Termination System (FTS) (if used), but does it include wider aspects such as mission planning systems and so on? The boundary is unclear.

However, if we consider that the aim of the Aircraft Level FHA in [5] is to explore the critical functions that lie within the designer's control, then the boundary does not really matter at this stage. The bulk of functionality within the planned UAS is to replace those taken for granted in manned systems. Thus, by extending the Aircraft Level FHA to be a **UAS Level FHA**, looking at all functions of the UAS within the designer's control, then the outcome is an identification of all the functions that are critical to the safe behaviour of the system and the consequences of their breakdown.

These can then be flowed down into the System level FHA, et al, as described in [5], to be analysed as functional sub-systems within the UAS.

#### Dealing with the System of Systems around the UAS

As was discussed earlier, UAS operate within a wide System of Systems (SoS), and traditional manned aircraft analyses are not strong in analysing these relationships.

One consideration was to introduce a 'Super-system' level FHA to the process, to assess the functions of the wider SoS. However, this was not felt to be practical for the UAS designer to attempt: while he wishes to understand the SoS to the extent that it affects his system, he can control only a (relatively) small element of it and a full

analysis would take excessive resources. On reflection, this level of analysis might be useful for a wider SoS player such as EUROCONTROL or EASA to conduct, and provide resulting information to inform system designers.

The UAS designer's interest is to achieve a better understanding of the interactions between the UAS and the wider SoS. This suggests parallels with Requirements Engineers, trying to understand the 'problem domain' and how the World and their potential Machine interface. From a review of their methodologies, it is proposed that a *Rich Context Diagram* provides a suitable visual model to help draw out complexities and interactions.

An example of a Rich Context Diagram, drawn up for a generic Tactical UAS, is shown in Figure 2. While it can take a while to achieve a suitable representation, this is usually due to the complexity of interactions, rather than the method itself. The resulting diagram can prove very useful, directly through ensuring that the designer / safety assessor has a sound understanding of the system context, and also indirectly, by providing a starting point for discussions with other stakeholders over functions and hazards.

### **Modifying Functional Failure Analysis to take account of UAS Differences**

#### Function Identification

Our analysis method needs a robust identification of functions, as these are the building blocks for the hazard identification. We do not want to miss out vital functions (and thus areas of hazard analysis and design requirement) due to assumption or error, which will later be found to have critical safety implications for the system in-service. ARP 4761 [5] provides a little guidance on function identification aimed at Aircraft Level FHA, but what is there is aimed at a primarily unitary overall system. This guidance needs to be built upon, to ensure a more structured approach for a UAS made up of several system elements and working within a wider SoS.

#### *UAS-Level FHA Source Data Input Requirements*

From our investigation, there are additions to the list of source documents described in [5], in order to carry out the UAS-Level assessment. The proposed list would now read:



1. List of generic UAS functions (when available).
2. The UAS objectives and customer requirements - ideally from a User Requirement Document or similar specification.
3. Initial design decisions or constraints (e.g. size and type of UAV, scope of GCS, scope of Datalink) - perhaps a simple design representation, such as Yourdon or Functional Block Diagram; or an initial architectural representation of the system elements (such as an 'internal' Context Diagram).
4. A representation (such as a Rich Context Diagram) showing the interactions of the UAS with the outside world (the SoS) and any critical interactions between those external elements (such as between ATM and other, manned aircraft).
5. Initial mission types or constraints – perhaps from a simple ConOps for the system.

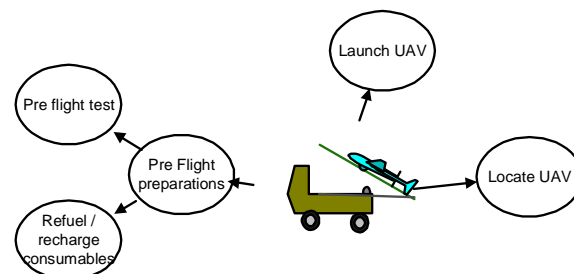
From the above input data, it should prove feasible to draw up a suitably robust Function List or Function Tree, and hence get the FHA off on a sound basis.

#### Internal Functions

The ARP [SAE96] suggests that, for the Aircraft Level "...these are main functions of the aircraft and functions exchanged between the internal systems of the aircraft." Our concern here is to ensure that the identification adequately explores the complexity of the UAS, both in its overall capabilities and in its internal interactions. To achieve this, the following structured approach has been developed, to identify the Functions List (or Functions Tree as preferred):

1. Consider UAS functions overall:
  - a. Ideally, there will be an established User Requirement Document or similar specification to draw upon.
2. Consider functions determined by the UAS internal structure:
  - a. Is there a simple representation of the initial design concept? These could be as formal as Yourdon diagrams or Functional Block Diagrams, or could be a simple architectural model (like an internal Context Diagram) showing interactions between the UAV, the GCS, use of the datalink etc.
  - b. Consider each major element of the structure and identify any additional internal functions - it may help to

consider each as a transform mechanism (such as in Figure 3), that is to consider the inputs and the resultant modified set of outputs, in order to determine what functions that element needs to perform the transformation:



**Figure 3 - Assessing an element of the system**

- (i) Does the element have particular *behaviour* functions - e.g. does it react physically to inputs?
  - (ii) Does it have *control* functions - does it monitor and/or control the behaviour of other elements?
  - (iii) Does it have *information* functions - does it generate information or process data, to be used elsewhere?
  - (iv) Does it have *utility* functions - such as power generation, needed to provide support elsewhere in the system?
- c. Care will be needed to balance what is sensible to achieve at the UAS level analysis, and what can be left to the more in-depth System-Level analyses. The balance may be self-imposed by the limited design information available at the early stages of the project.
3. Consider the effect of flight phases, as UAS usually have a broader mission profile than the transport aircraft that [5] was intended for originally:
    - a. See 'Flight Phases' below for discussion on identifying flight phases.
    - b. Review the function list (so far) for each proposed flight phase and mission variation, to identify any additional functions or sub-functions.

### *Exchanged Functions*

[5] suggests that, for the Aircraft Level "...these are functions that interface with other aircraft or with ground systems." As discussed earlier, more guidance is needed for UAS, to ensure that the interactions with the wider SoS are identified, hence the following additional advice is proposed:

1. Using the Rich Context Diagram discussed above (with the example at Figure 2):
  - a. Consider each element in turn that the UAS will interact with.
  - b. Consider each Rich Context Diagram interaction for implied functions on the UAS. Again it may help to consider the UAS as a transform mechanism, for: behaviour functions; control functions; information functions; utility functions.

### *Flight Phases*

The phases of flight for the vehicle can indicate further UAS functions to be assessed for hazards. However, UAS flight phases can be somewhat more exotic than the transport aircraft originally considered by ARP 4761. It is important that all phases are identified, for the main mission and also any variations (e.g. a UAV might act as a sensor gathering target information, but might also be able to act as a datalink relay for another UAV). For this reason, the following modification is proposed to supplement the HazID method:

1. Mission types and parameters should be reviewed to identify the various flight phases possible, for main and alternate mission types. This could be gleaned from the User Requirement Document (URD), or maybe there is a simple Concept of Operation (ConOps) that can be used

### Identification and Description of Failure Conditions

[5] proposes that identification and description of failure conditions for a particular function begins with definition of an Environment and Emergency Configuration list (in order to understand 'normal' and 'degraded' aspects of operation), before going on to consider failure conditions in depth. Each of these aspects is discussed below.

#### *Environment List*

[5] starts with suggestions of weather, High Intensity Radio Frequency (HIRF) and volcanic ash as examples pertinent to transport aircraft. For UAS, the list of possible environments to consider needs to grow. As noted earlier, UAS may

operate in a very different environment from manned aircraft, due to a combination of their performance and role / mission differences.

1. The Environment List should be defined from a review of appropriate domains:
  - a. Weather aspects - e.g. temperature, icing, precipitation, winds, visibility...
  - b. Overflown terrain aspects - this may raise additional 'weather' aspects, such as wind-shear, sand and dust storms. It may also indicate other aspects such as for landing and take-off, or communications masking.
  - c. Electrical environment - in particular, man-made or natural RF fields such as High Intensity Radio Transmission Areas (HIRTAs), and perhaps aspects of limited or overlapping spectrum, where problems can be foreseen.
  - d. Mission environment - such as personnel shift-changeovers (for long endurance missions), or action of hostile forces for military uses, or use in day or night.
  - e. Air traffic environment - such as the classes of airspace that may be flown through or nearby, and the levels and types of traffic.

2. Some of these aspects might already have come to light from creation of the Rich Context Diagram. However, in order to define this list adequately, it may prove necessary to extend the assessment through use of a series of simple scenarios or vignettes, to define typical situations.

#### *Emergency Configuration List*

The FHA needs to consider any specific emergency or 'expected' abnormal flight conditions that may occur. Some will be defined in regulation, others might be necessary due to design choices. A preliminary listing of aspects of regulation and guidance has been identified below, though it is not proposed as being complete in all respects:

1. Single failure of the UAV communication link, and/or control link (uplink and/or downlink, depending on implementation)
2. Operation of Flight Termination System (if fitted)
3. Else, conduct of other Emergency Recovery procedures due to loss of critical

system(s) – both with and without UAV-p control (i.e. autonomous)

4. Emergency landing due to loss of thrust
5. Collision avoidance with co-operative and non-cooperative aircraft - including evasive manoeuvre
6. Terrain avoidance
7. Interception by military aircraft
8. Failure of onboard Sense and Avoid equipment
9. Operation with degraded systems
10. Degradation of weather conditions
11. Security threats to upload data, commands and transmissions

Items 1-8 are drawn from [7]; items 1, 3, 6, 7, 9 - 11 from [12]. Clearly the intent of these sources is to try and mitigate what are seen as the inherent hazards of UAS. However, consideration of this list (during a trial of the FHA process) quickly highlighted a need to consider what the UAS intended behaviour would be in event of such emergencies, especially for system failures. Hence, a useful source document is an initial definition of emergency procedures, as part of the 'initial design considerations'. These considerations spawn additional functions (to be added to the tree), to be assessed for further functional failures.

#### *Failure Condition Determination*

While not UAS specific, it is suggested that Functional Failure Analysis guidance helps to structure the determination of failure conditions. This proposes three categories of failures to assess:

1. *Function not provided* – this is fairly easy to interpret for responsive functions, but care is required with continuous or periodic functions, to ensure that variations are assessed: single failure; periodic failure; complete loss.
2. *Function provided when not required* – obviously, this is not applicable to continuous functions.
3. *Incorrect operation of function* – this can be a tricky catch-all, which needs care to ensure completeness. Examples include: asymmetry; substitution; partial; timing.

To identify multiple failures, [5] suggests that "...this process is aided by an understanding of the aircraft and system architecture. Multiple failures have to be considered, especially when the effect of

a certain failure depends on the availability of another system". To apply some structure to this, we should consider multiple failure conditions:

1. Through assessment of the initial design architecture. In particular consider any elements that could suffer some common cause for failure (such as EMI affecting both navigation and communications functions).
2. Where mitigation for a critical function failure is expected by the successful operation of another function. Here, we should reconsider the criticality of that function, and review 'what if' that function failed also, to give us a more rounded assessment overall.

In part, some of this multiple failure analysis will occur through application of the Emergency Condition list, where regulation and guidance has already highlighted some expected areas of criticality such as datalink and propulsion functions.

#### Identification and Classification of failure condition effects

For UAS, it is not the effect of a failure on the UAS that matters, it is the end effect on other stakeholders, such as airspace users or the overflowed public, so our method needs to ensure that the mission / environmental / ATM *context* is adequately understood. There is already some foundation in the methodology proposed so far, with definition of the Rich Context diagram, Flight Phases and Environment and Emergency Condition list. This is supplemented further, through the following:

1. For the majority of failure conditions assessed, it is proposed that the existing contextual information (as noted above) will be sufficient. However, as mentioned in the discussion over environmental conditions, there may be some cases where this is not sufficient. Our existing contextual information is trying to cover the broad scope of variations and generally applicable parameters, in essence defining the outer envelope of how the system will be used.
2. For more complex failure conditions, use of *scenarios* is recommended. A scenario provides a more detailed representation of a situation within the broader envelope defined in our other contextual representations. We could not hope to cover the whole envelope of environments and usage with scenarios, but used selectively as supplements, they help draw out some of the complexities of key situations and (in particular) how conditions and events might come together to affect the UAS. Drawing parallels from Human

Factors Engineering, scenarios could be selected for specific situations of interest, such as:

- a. (Initially) 'routine' mission stages - all was going well, just like every other day, until...
- b. Exceptional circumstances - perhaps extremes of climate, weather or unusual terrain, or variations of mission type...
- c. Disadvantaged or extraordinary users - e.g. operation at the end of a shift (fatigue) or after shift change (unfamiliarity); under extreme workload (such as busy airspace)...
- d. Accident or failure - e.g. specific instances of system failure (e.g. multiple failure conditions); or expected crisis procedures such as Emergency Recovery, weather diversion...

Rather than text based scenarios (as initially tried), a better alternative is *graphical scenarios*. This approach is to plan actual missions over typical terrain, on air maps. Using this, the user gets a better idea of the type and range of challenges – terrain, airspace, obstructions, HIRTAs etc. It is vital to actually plan the route out, not just look at the maps, in order to think into actual mission-type situations. For example, identifying where to place a GCS to achieve datalink coverage along the full length of the planned route. The map can be annotated with other conditions of interest, such as the possible range of weather. Graphical scenarios also work well when looking at emergency situations. For instance: what if the satellite datalink becomes unavailable 'here' when Ground Control System range is marginal. They allow 'what ifs' to be raised and assessed quickly, and the user's creativity is fostered by the map terrain and airspace content.

## Conclusions

It is recommended that UAS developers will need to incorporate a safety assessment process, similar to those used in the development and certification of manned aircraft. This is an essential step, in order to improve UAS safety and reliability, and to meet regulatory requirements to allow flight in unsegregated airspace.

In order to make manned safety assessments more UAS applicable, the paper recommends modification to the hazard identification process. Considering the ARP 4761 [5] FHA process, the proposed changes are summarised thus:

1. A dual set of safety criteria is proposed, to satisfy both airworthiness requirements (where the UAV may come to ground and affect the overflowed population) and ATM separation / collision requirements (where the UAV might affect other airspace users).
2. It has been proposed that the complexities of the extended system could be addressed by carrying out 'Aircraft Level' FHA as a 'UAS-Level FHA'. To bring in consideration of the wider System of Systems, the use of a Rich Context Diagram is proposed.
3. The paper goes on to consider the conduct of the UAS-Level FHA. These activities are summarised in Figure 4, below. This figure is based heavily (in style) on the original 'Aircraft Level FHA' Figure A1 in ARP 4761 [5], in order to ensure recognition by experienced users and regulators.

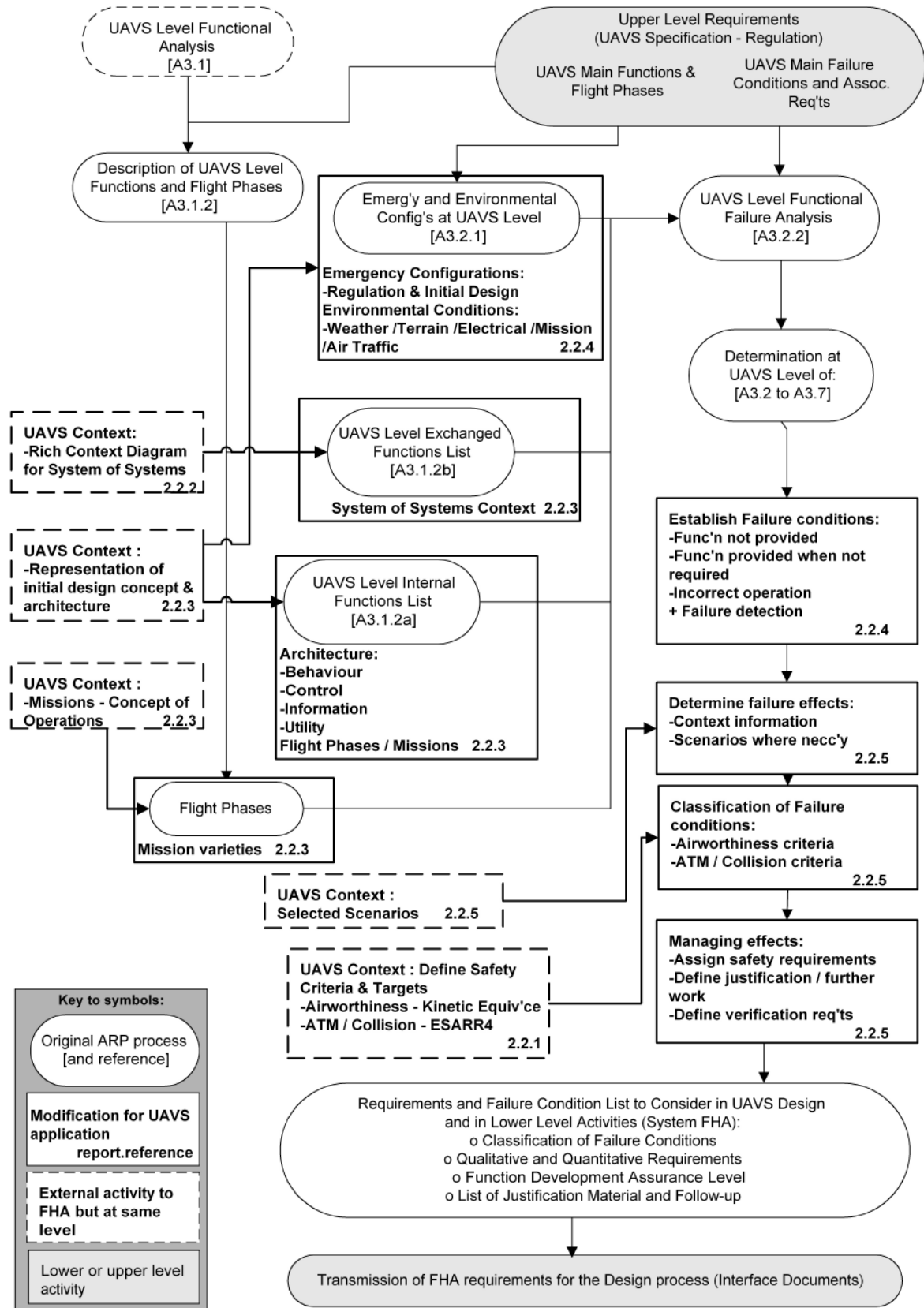


Figure 4 – Overview of ARP 4761 FHA Process, with modifications overlaid for UAS applicability

## References

1. “Issues Concerning Integration of Unmanned Aerial Vehicles in Civil Airspace”, MP 04W0000323, DeGarmo MT, Nov 2004, Mitre Corporation - Center for Advanced Aviation System Development
2. “A Summary of Unmanned Aircraft Accident/Incident Data: Human Factors Implications”, DOT/FAA/AM-04/24, Williams K, 2004, Federal Aviation Authority
3. “Defense Science Board Study on UAS andUCAVs”, Schneider W (Chairman), Feb 2004, DSB for Secretary of Defense
4. “Suggested Flight Approval Process for Unmanned Air Vehicles (UAVS)”, Marsters GF & Sinclair M, 2003, AeroVations Associates
5. “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment”, ARP 4761, 1996, SAE
6. “Flying with Unmanned Aircraft (UAVs) In Airspace Involving Civil Aviation Activity - Air Safety and the Approvals Procedure”, Wiklund E, March 2003, Swedish Aviation Safety Authority
7. “UAV Task Force Final Report”, JAA / EUROCONTROL, May 2004, EASA
8. “Advisory Circular: Transport Category Airplanes, Federal Aviation Regulations - System Design and Analysis”, AC 25.1309-1A, Jun 88, Federal Aviation Authority
9. “Advisory Circular: Normal, Utility, Aerobatic and Commuter Category Aeroplanes - Equipment, Systems, and Installations In Part 23 Airplanes”, AC 23.1309-1C, Mar 1999, Federal Aviation Authority
10. “Certification Considerations for Highly-Integrated Or Complex Aircraft Systems”, ARP 4754, 1996, SAE
11. “EUROCONTROL Safety Regulatory Requirement 4 - Risk Assessment and Mitigation in ATM”, ESARR 4, Apr 2001, EUROCONTROL
12. “Unmanned Aerial Vehicle Operations in UK Airspace – Guidance”, CAP722 (2nd Edition), Nov 2004, Civil Aviation Authority - Directorate of Airspace Policy

## Glossary of Acronyms

CCA	Common Cause Analysis - Generic term encompassing Zonal Analysis, Particular Risks Analysis and Common Mode Analysis. In these methods, analysis is made of common modes of failure, which could affect a number of elements otherwise considered to be independent.
ConOps	Concept of Operations
ESARR	Eurocontrol Safety Regulatory Requirements
EUROCAE	EUROpean Organisation for Civil Aviation Electronics
FFA	Functional Failure Analysis - A technique which is part of FHA. Applies a systematic review of system functions to determine the ways in which failure may occur; then analyses these failures for potential accident consequences.
FHA	Functional Hazard Assessment - A systematic, comprehensive examination of functions to identify and classify Failure Conditions of those functions according to their severity. The intent is to be predictive of system failure conditions, to allow safety targets to be set for system component reliabilities, in order to achieve an acceptable overall platform safety level once the design is realised.
FMEA	Failure Modes & Effects Analysis - Safety analysis to determine hazard effects of lower level system and component failures
FTA	Fault Tree Analysis - Safety analysis subsequent to FHA, to determine contributory causes for potential hazards
HIRF	High Intensity Radio Frequency
UAVp	UAV Pilot
URD	User Requirement Document
WG73	Working Group 73 (part of EUROCAE looking at UAS)