Holistic Safety Analysis for Urban Air Mobility

Contents

1 Introduction

The purpose of this document is to propose an approach that leverages a holistic safety analysis to derive requirements for an Urban Air Mobility (UAM) aircraft. The approach leverages existing and emerging safety analysis techniques, addresses the deficiencies of SC VTOL, modifies probability budgets and Design Assurance Levels (DALs) appropriate for a UAM aircraft and identifies a variety of compensating factors to ensure FAA and EASA safety assurance objectives are exceeded.

2 Background

Traditionally, novel technologies and applications of technologies have been accommodated via special conditions. The intent of requirements such as these can be summarized as the achievement of a societally acceptable level of safety assurance/ risk. However, special conditions are often written independently of the safety analysis introducing inconsistencies.

It is a misconception that Part 23 Amendment 64 is a performance-based requirements framework. In reality many of the performance-based requirements that exist in Amendment 62 do not exist in Amendment 64. Instead, it is an abstraction of Amendment 62 which eliminates a requirements tier. It accommodates a wider variety of system architectures by being less prescriptive. However, it leaves a void because systems engineering and design assurance objectives dictate that there is traceability from safety assurance objectives, through requirements tiers, to the software and complex hardware.

The proposal is that a holistic safety analysis, similar to that advocated by Moak, L. et al. (2020), is leveraged to derive requirements that bridge the gap and that are consistent with safety assurance objectives.

The FAA and EASA have opposing safety assurance objectives for UAM aircraft. The FAA applies a safety continuum that links probability budgets and DALs with aircraft passenger numbers and EASA have released SC VTOL that associates probability budgets and DALs with Basic and Enhanced certification categories, linked to the intended type of operations.

Furthermore, SC VTOL imposes additional requirements for the following reasons:

- It redefines continued safe flight and landing as “continued controlled flight and landing at a vertiport, possibly using emergency procedures, without requiring exceptional piloting skill or strength.” This levies requirements that don’t exist for Part 23, 27, 25 and 29 and doesn’t accommodate a land as soon as possible/ practicable emergency procedure away from a vertiport to prevent a catastrophic failure condition.
- It does not apply the safety continuum. Therefore, the probability budget and DAL objectives for a UAM aircraft are the same as a Part 23 airworthiness level 4 aircraft or a Part 25 aircraft.
- It’s extension of the single failure concept to “also include aircraft structures” ignores the factor of safety approach that is traditionally applied to aircraft structures.
- It increases safety assurance objectives “by one level compared to CS-23 due to a higher dependency on systems that are associated with distributed propulsion.” In reality distributed propulsion is inherently safer than propulsion systems associated with Part 27 and 29 aircraft as a result of fault tolerance and redundancy. UAM aircraft should not be penalized for having distributed propulsion.

Consequently, in order to successfully apply a holistic safety analysis, the safety assurance objectives of the FAA and EASA must be harmonized in a way that is not prohibitive or unreasonably burdensome.

3 Harmonized Safety Assurance Objectives

	aircraft passenger numbers	engine information	category	Catastrophic	Hazardous	Major	Minor
EASA[3]	n/a	n/a	enhanced	FDAL A 1E-9	FDAL B 1E-7	FDAL C 1E-5	FDAL D 1E-3
EASA[1]	0-1	n/a	basic	FDAL C 1E-7	FDAL C 1E-6	FDAL C 1E-5	FDAL D 1E-3
EASA[1]	2-6	n/a	basic	FDAL B 1E-8	FDAL C 1E-7	FDAL C 1E-5	FDAL D 1E-3
EASA[2]	7-9	n/a	basic	FDAL A 1E-9	FDAL B 1E-7	FDAL C 1E-5	FDAL D 1E-3
FAA[3]	0-1	1 reciprocating	n/a	FDAL C/C 1E-6	FDAL C/D 1E-5	FDAL C/D 1E-4	FDAL D 1E-3
FAA[3]	2-6	1 reciprocating	n/a	FDAL C/C 1E-6	FDAL C/D 1E-5	FDAL C/D 1E-4	FDAL D 1E-3
FAA[3]	0-1	1< reciprocating or 0< turbine	n/a	FDAL C/C 1E-7	FDAL C/C 1E-6	FDAL C/D 1E-5	FDAL D 1E-3
FAA[3]	2-6	1< reciprocating or 0< turbine	n/a	FDAL C/C 1E-7	FDAL C/C 1E-6	FDAL C/D 1E-5	FDAL D 1E-3
FAA[3]	7-9	n/a	n/a	FDAL B/C 1E-8	FDAL C/C 1E-7	FDAL C/D 1E-5	FDAL D 1E-3
FAA[3]	10-19	n/a	n/a	FDAL A/B 1E-9	FDAL B/C 1E-7	FDAL C/C 1E-5	FDAL D 1E-3
Harmonized[3]	**0-6**	**n/a**	**n/a**	**FDAL B 1E-8**	**FDAL B 1E-7**	**FDAL C 1E-5**	**FDAL D 1E-3**

Table 3-1: probability budget and DAL assignments for different compliance methodologies

Table *3-1* summarizes different approaches to the assignment of probability budgets and DALs extracted from ASTM F3061/F3061M-19a, ASTM F3230-17 and SC VTOL. Furthermore, it introduces new harmonized safety assurance objectives that support a holistic safety analysis. Part 23 is the starting point for the following reasons:

[1] no considerations of the system architecture for a DAL reduction are acceptable.
[2] considerations of the system architecture for a DAL reduction are acceptable.
[3] FDAL [primary system]/[secondary system].

- Part 27, 25 and 29 have not been abstracted to accommodates a wider variety of system architectures (unlike Part 23).
- Part 25 and Part 29 are in a different risk category to Part 23 and Part 27.
- The Part 23 and Part 27 safety continuum serve the same purpose and are sufficiently similar to justify focusing on Part 23 and not Part 27 (see PS-ASW-27-15).

TOP-LEVEL FAILURE CONDITION CLASSIFICATION	DEVELOPMENT ASSURANCE LEVEL[4&5]		
	FUNCTIONAL FAILURE SETS WITH A SINGLE MEMBER	FUNCTIONAL FAILURE SETS WITH MULTIPLE MEMBERS	
		OPTION 1[6]	OPTION 2
Column 1	Column 2	Column 3	Column 4
Catastrophic	FDAL A[7]	FDAL A for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level C for the additional Members).	FDAL B for two of the Members leading to top-level Failure Condition. The other Member(s) at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level C for the additional Member(s)).
Hazardous/ Severe Major	FDAL B	FDAL B for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but	FDAL C for two of the Members leading to top-level Failure Condition. The other Members at the level associated with the most severe individual effects of an error in their development process for all applicable

[4] It is necessary to stay in the same row no matter the number of functional decompositions performed (e.g. for a Catastrophic Failure Condition any degree of decomposition from a top FDAL A FFS should include at least one FDAL A or two FDAL B Members).
[5] Some classes of 14CFR Part 23 /CS-23 aircraft have FDALs lower than shown in Table *3-2*. See the current FAA AC23.1309 and equivalent EASA policy for specific guidance.
[6] The assignment of FDAL to each Functional Failure Set Member is independent of their numerical availability. However, if there is a large disparity on the numerical availability of the Members in the Functional Failure Set, it may be beneficial to assign the higher level FDAL to the higher availability Member.
[7] When a FFS has a single Member and the mitigation strategy for systematic errors is to be FDAL A alone, then the applicant may be required to substantiate that the development process for that Member has sufficient independent validation/verification activities, techniques and completion criteria to ensure that potential development error(s) having a catastrophic effect have been removed or mitigated.

TOP-LEVEL FAILURE CONDITION CLASSIFICATION	DEVELOPMENT ASSURANCE LEVEL[4&5]		
	FUNCTIONAL FAILURE SETS WITH A SINGLE MEMBER	FUNCTIONAL FAILURE SETS WITH MULTIPLE MEMBERS	
		OPTION 1[6]	OPTION 2
Column 1	Column 2	Column 3	Column 4
		no lower than level D for the additional Members).	top-level Failure Conditions (but no lower than level D for the additional Members).
Major	FDAL C	FDAL C for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.	FDAL D for two of the Members leading to top-level Failure Condition. The other Members at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.
Minor	FDAL D	FDAL D for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.	
No Safety Effect	FDAL E	FDAL E	

Table 3-2: DAL assignment to members of a functional failure set

Table *3-2* summarizes the ARP4754A prescribed methodology for DAL assignment to members of a functional failure set. Each of the different approaches, as identified by Table *3-1*, either do or do not accept architecture mitigations for a DAL reduction. The harmonized safety assurance objectives accept it.

4 Compensating factors

The harmonized safety assurance objectives are not a compromise between FAA and EASA requirements. Instead, they enable a more succinct safety analysis without undermining the safety assurance objectives of SC VTOL. This is accomplished by compensating factors.

4.1 Compensating for reduced probability budget

The order of magnitude probability budget reduction for catastrophic failure conditions is compensated for by imposing conservative Failure Mode Effects Analysis (FMEA) and Failure Mode Effect Summary (FMES) assumptions as follows:

- Functional as opposed to piece-part FMEA/ FMES[8].
- Eliminating failure mode distributions and instead using the full failure rate for components and collections of components.

In addition to catastrophic failure conditions, the same order of magnitude probability budget reduction can be applied to hazardous and major failure conditions. However, it should be reserved for failure conditions that satisfy the single failure concept.

4.2 Compensating for reduced design assurance level

By requiring DAL B for systems architectures that have elements that could contribute to a catastrophic failure condition, the use of safety enhancing Commercial Off The Shelf (COTS) equipment is enabled. This is because COTS equipment generally can satisfy the objective of DAL D, but not DAL A, B and C. DAL B can be achieved with a system architecture that has a primary member that is DAL B and a secondary member that is DAL D (see Table *3-2*).

Examples of safety enhancing COTS equipment includes:

- Detect and avoid systems that incorporate neural networks.
- Global navigation satellite system equipment.
- Inertial measurement unit equipment.

5 Consideration of human factors

Historically, safety analysis credit has been taken for flight crew actions documented by the aircraft flight manual and maintenance actions documented by the maintenance manual that can reasonably be expected to be performed correctly. However, ~80 percent of errors can be attributed to human error. Therefore, in accordance with Moak, L. et al. (2020) recommendations, the safety analysis must incorporate the systematic consideration of human error. This is to be accomplished by evaluating human performance in response to nominal and off-nominal conditions and tasks. Also, model-based systems/ safety techniques and control theory must be applied to derive control actions and unsafe control actions. A model-based approach that is recommended is Systems Theoretic Process Analysis (STPA).

6 Continued Airworthiness

Historically, data with sufficient fidelity has not been available to track failures and perform route cause analysis. A mechanism to track this data must be imposed and the safety analysis must be revisited as failure rate

[8] ARP4761 states “an FMEA is a systematic, bottom-up method of identifying the failure modes of a system, item, or function and determining the effects on the next higher level. It may be performed at any level within the system (e.g., piece-part, function, blackbox etc.).”

assumptions change. Maintenance intervals must be updated accordingly. Also, the transition from an open-loop to a closed-loop approach is expected to enable the development of a condition-based maintenance system to minimize unscheduled maintenance actions.

7 Endurance Testing

Critical parts i.e. parts that if they fail are expected to result in a hazardous or catastrophic failure condition are expected to undergo endurance testing. Endurance testing approaches have improved dramatically over recent years. An approach that exploits the interrelationship between Highly Accelerated Life Testing (HALT), Highly Accelerated Stress Screening (HASS), endurance testing and failure rate is required for critical parts.

8 Factors requiring clarification

8.1 ASA/ PASA

ARP4761 introduces the concept of an Aircraft Functional Hazard Analysis (AFHA), a Preliminary Aircraft Safety Assessment (PASA) and an Aircraft Safety Assessment (ASA) to analyze integrated systems. The rationale is that aircraft are becoming highly integrated with fewer federated systems.

Assuming a full transition from federated to integrated systems, the two tiers should be replaced by a single tier of Functional Hazard Analysis (FHA), Preliminary System Safety Assessment (PSSA) and System Safety Assessment (SSA). These items should be linked to each other and should be linked to a single tier of FMEA, FMES and reliability prediction. The links and this flatter structure enable a more iterative safety analysis than traditional approaches such as the V-model. This iterative safety analysis should be repeated regularly throughout the design and development lifecycle of the UAM aircraft.

8.2 Continued Safe Flight and Landing

The redefinition of catastrophic failure condition from “continued safe flight and landing” to “continued safe flight and landing at a vertiport, possibly using emergency procedures, without requiring exceptional piloting” (SC VTOL) should not occur. This redefinition would have a profound effect on the safety analysis and result in is a decrease as opposed to an increase in safety for the following reasons:

- No safety analysis credit for the development of systems that enable a landing as soon as possible/ practicable emergency procedure that is not at a vertiport.
- Prohibiting a UAM aircraft that is in a degraded state from landing as soon as possible/ practicable exposes passengers and/ or third parties to an increased level of risk.
- The direct relationship between the safety analysis and societally acceptable safety assurance/ risk would be undermined.
- Catastrophic failure conditions would be assessed with respect to the ability of the UAM aircraft to complete a landing at a vertiport as opposed to risk to passengers and/ or third parties.
- It would introduce unprecedented regulatory requirements for UAM aircraft that don’t exist for Part 23, 25, 27 and 29 aircraft when flying over congested areas.

8.3 Multiple Instances of a COTS device

EASA via SWCEH-001 impose architectural mitigation wherever multiple instances of a COTS device incurring a common failure mode could cause a catastrophic failure condition. The FAA do not explicitly impose this requirement. However, obtaining the information necessary to satisfy design assurance objectives can be difficult for a COTS device. This is changing with an increase in automation across other industries and the more widespread use of standards such as ISO 26262 and IEC 61580 with similarities to DO-178C and DO-254. Therefore, instead of requiring architectural mitigation, the option should exist to utilize information generated for a COTS device as a result of a functional safety process completed by a manufacturer. This information, which is a

combination of quality assurance, configuration management and other lifecycle data, should be used carefully because it is generated out of context with assumptions that may not be applicable. Also, ISO 26262 and IEC 61580 are goal based[9] and DO-178C and DO-254 are objective based[10], the goals that have been met should be examined with respect to DO-178C and DO-254 design assurance objectives.

8.4 Failure Condition Classification

Classification of Failure Conditions	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal injury or incapacitation
Effect on maintenance crew	No effect on maintenance crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal injury or incapacitation

Table 8-1: failure condition classification

Table *8-1* is used to classify failure conditions. To facilitate a holistic safety analysis that considers the effect on persons interacting with the UAM aircraft, effect on maintenance crew is added to Table *8-1*.

As a result of an accident, compared to passengers there is a decreased level of risk to third parties[11]. Therefore, effect on third parties is implicitly accounted for and is not added to Table *8-1*.

SC EVTOL attempts to consider the effect on third parties by assigning safety assurance objectives regardless of aircraft passenger numbers. This isn't appropriate for the following reasons:

[9] Not requiring that all goals are met

[10] Requiring that all goals are met.

[11] Of all the accidents that resulted in fatalities involving Part 27 and 29 aircraft between 2010 and 2020, five were over congested areas. Of these five, two resulted in third party fatalities (29th November 2013 EC135-T2+ incident and 16th January 2013 AW109 G-CRST). Therefore, indicating that, compared to passengers there is a decreased level of risk to third parties.

- Part 27 aircraft and even Part 23 aircraft operate in and out of and over densely populated areas such as cities regularly without any additional requirements.
- UAM aircraft will operate to and from cities. However, with ranges of ~100km it is expected that the majority of the flight path will not be over densely populated areas. Also, the flight path can be selected so that it mitigates risk to third parties.
- There are more effective ways of mitigating risk to third parties near densely populated areas such as automated takeoff and landing aids.

When assigning effect on flight crew, the impact of automation including the effect of loss of automation and vigilance decrement[12] must be considered. The effect on flight crew could be the effect on pilot or a remote pilot depending on the UAM aircraft. Also, if there is a many-to-many relationship between UAM aircraft and a team of pilots, the most severe effect on any individual pilot must be considered. If automation can mitigate the effect of a degraded state on flight crew, airplane and occupants, the effect on safety margins may be the delineator between minor, major and hazardous failure conditions. In this case, a determination of whether a failure condition results in a slight, significant or large reduction in safety margins is the difference. Therefore, if a UAM aircraft can reduce its exposure time[13] to a second catastrophic failure by landing as soon as possible/ practicable after a first failure, a case can be made for the first failure condition being minor as opposed to major or hazardous (see Table *8-2*).

Probability of second catastrophic failure condition after first failure condition has occurred	**Classification of first failure condition**
<1e-5	Minor
From 1e-5 to <1e-3	Major
From 1e-3 to <1e-1	Hazardous

Table 8-2: classification of first failure condition

To calculate the probability of the second failure condition after the first failure condition has occurred, each cut set contributing to the first failure condition, consecutively, is set a probability of 1. The result with the highest probability is used to set the classification of the first failure condition.

9 Further considerations

9.1 Aircraft parachute system

An aircraft parachute can be used to mitigate certain UAM aircraft failure conditions. The Cirrus SR20/SR22 was certified with an aircraft parachute system.

The disadvantage of an aircraft parachute system for a UAM aircraft are:

- Additional mass.
- A minimum deployment altitude of ~500ft therefore it does not mitigate loss of vertical thrust during the critical takeoff and landing phase of flight.
- The pyrotechnics can fail latently and require scheduled maintenance actions.

The advantages are:

- If detected, it could mitigate loss of vertical thrust during the cruise phase of flight.

[12] Vigilance decrement is defined as "deterioration in the ability to remain vigilant for critical signals with time, as indicated by a decline in the rate of the correct detection of signals" (see Parasuraman R. 1997 and Mackworth N. H. 1948).

[13] Probability is a function of exposure time and failure rate. Therefore, reducing exposure time or failure rate reduces probability.

- It can be operated with no electrical power.

9.2 Dispatch Relief

The dispatchability of a UAM aircraft warrants consideration as the takeoff and landing locations are likely to be austere with few replacement parts. Additional fault tolerance and redundancy can be added so that the UAM aircraft can be dispatched with a failure. However, it cannot be dispatched if it cannot satisfy the single failure concept. Also, to determine an acceptable dispatch relief interval, all failures that are latent are set an exposure time equal to the dispatch relief time in the Master Minimum Equipment List (MMEL). The failure is set a probability of 1. With these conditions set, it must be possible to satisfy probability budgets.

9.3 Neural Networks

There has been much deliberation about an approach to certify safety enhancing neural networks. The biggest challenge is the structural coverage and low-level requirements objectives of DO-178C that apply to DAL A, B and C. However, there are no structural coverage objectives or low-level requirements objectives for DAL D. Also, in accordance with Table *3-2* a primary DAL B member and a secondary DAL D member or two independent DAL D members can satisfy FDAL C objectives. Therefore, with architecture mitigation an approach to certify safety enhancing neural networks already exists.

9.4 Operating and Environmental Limitations

The safety analysis is valid assuming the UAM aircraft remains within its operating and environmental limits. The majority of regulatory requirements including SC VTOL are to ensure that the operating and environmental limitations are set for a particular aircraft type. They should be developed in conjunction with the safety analysis.

10 Definitions

Single failure concept:	The objective of this design concept is to permit the airplane to continue safe flight and landing after any single failure. Protection from multiple malfunctions or failures should be provided when the first malfunction or failure would not be detected during normal operations of the airplane, which includes preflight checks, or if the first malfunction or failure would inevitably cause other malfunctions or failures (AC 23.1309).
Land as soon as possible:	A landing as a result of a hazardous failure condition at a landing site that exposes persons or property to the least possible level of risk.
Land as soon as practicable:	A landing as a result of a major or minor failure condition at the nearest vertiport or at a landing site that is known to be clear of persons or property. If nearest vertiport, it is expected the UAM aircraft will be prioritized.
Continued safe flight and landing:	This phrase means that the airplane is capable of continued controlled flight and landing, possibly using emergency procedures, without requiring exceptional pilot skill or strength. Upon landing, some airplane damage may occur as a result of a failure condition (AC 23.1309).

11 Comparison of ARP4761 and ARP4761A

Figure *11-1* is a copy of the ARP4761 safety framework and Figure *11-2* is a copy of the ARP4761A safety framework. Fundamentally, they are different representations of a very similar process. The notable similarities are as follows:

- Each has two tiers of FHA,
- Both are represented as a V-model,

The notable differences are as follows:

- Figure *11-1* shows 3 levels of FTA/ CCA and Figure *11-2* shows 2 tiers (a PASA and a PSSA) on the left side of the V-model.
- Figure *11-1* shows 3 levels of FTA/ CCA and Figure *11-2* shows 2 tiers (an SSA and a ASA) on the right side of the V-model.
- Figure *11-1* identifies FMEA and FMES items specifically (these can be assumed to be part of the SSA and ASA of Figure *11-2*).

The main difference which is the difference in the number of tiers does not represent a fundamental change in approach. In practice, the number of tiers is selected based on the type of system or systems being developed.

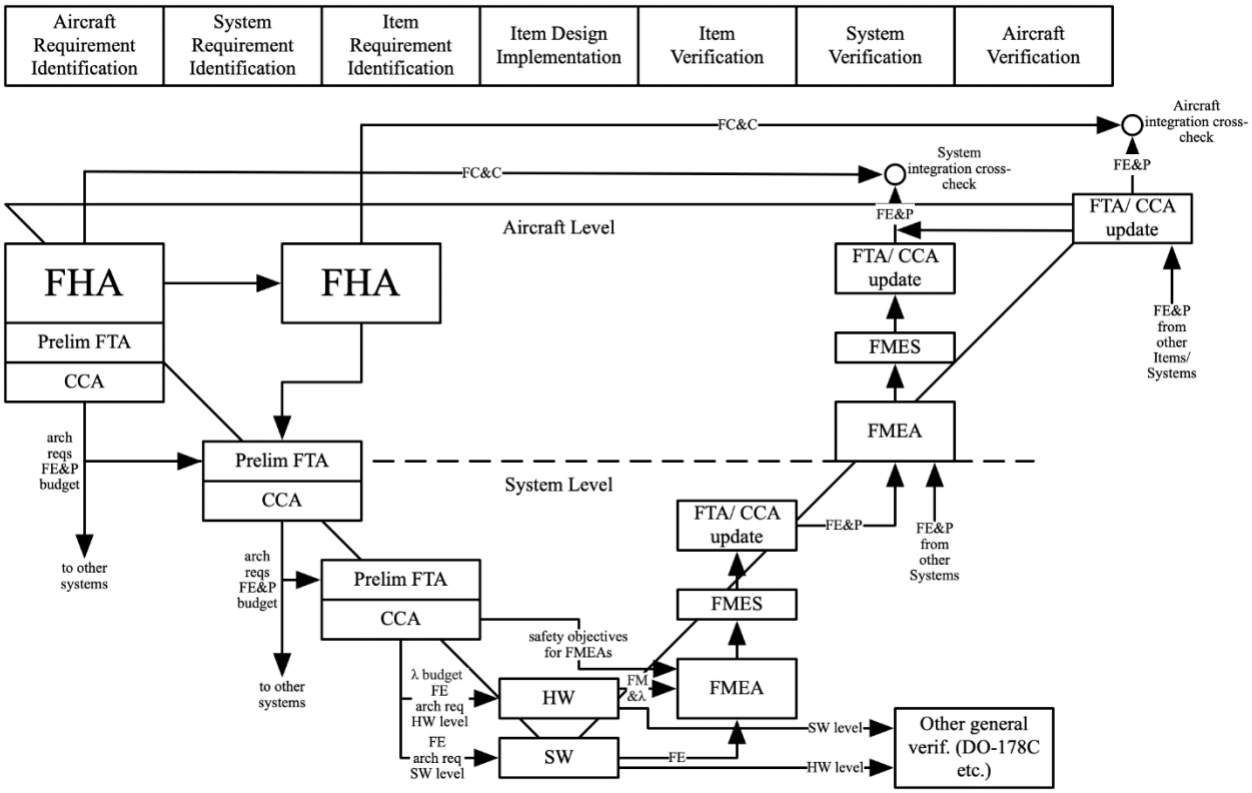

Figure 11-1: ARP4761 topology

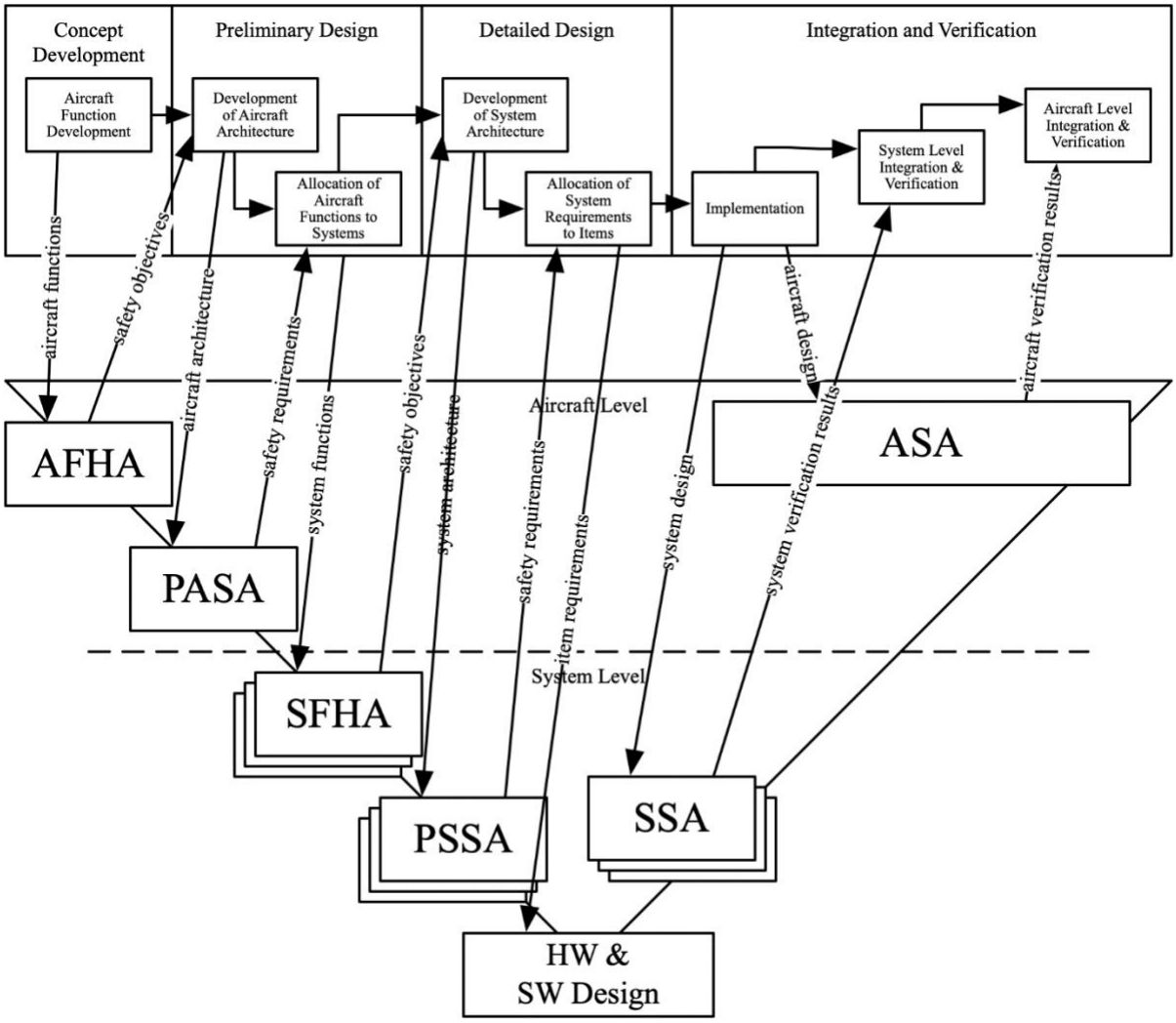

Figure 11-2: ARP4761A topology

In addition to the differences depicted, Table *11-1* identifies differences that are not represented by Figure 11-1 and Figure 11-2.

Subject	**ARP4761**	**ARP4761A**
Applicability	"It is primarily associated with showing compliance with FAR/JAR 25.1309. The methods outlined here identify a systematic means, but not the only means, to show compliance. A subset of this material may be applicable to non-25.1309 equipment."	"It may be used when addressing compliance with certification requirements (e.g., 14 CFR/CS Parts 23, 25, 27, 29 and 14 CFR Parts 33, 35, CS-E and CS-P). It may also be used to assist a company in meeting its own internal safety assessments standards."
In-service safety assessment.	No mention of a separate in-service safety assessment.	References ARP5150 "Safety Assessment of Transport Airplanes in Commercial Service"

Subject	ARP4761	ARP4761A
		and ARP5151 “Safety Assessment of General Aviation Airplanes and Rotorcraft in Commercial Service.”
Tiers.	Two tiers are shown (see ARP4761 Fig. 3).	Two tiers are shown (see ARP 4761A Fig. 1 and 2). However, there is now an AFHA and SFHA as opposed to just an FHA and the concept of a PASA and ASA is introduced to analyze integrated systems.
Model-based safety analysis	No mention of model-based safety analysis.	The concept of a model-based safety analysis and a Failure Propagation Model (FPM) is introduced. It’s hierarchical, iterative and progressive nature are highlighted as advantages versus other analysis techniques.
STPA	No mention of STPA.	SAE AIR6913 “Using STPA During Development and Safety Assessment of Civil Aircraft” and ASTM WK60748 “New Guide for Application of Systems-Theoretic Process Analysis to Aircraft” exist separately, but in order to remain “technology neutral” are not referenced.
Single event effects analysis	No mention of single event effects analysis.	AIR6219 “Development of Atmospheric Neutron Single Event Effects Analysis for use in Safety Assessments” is referenced.
Analysis of development and design errors i.e. FDAL/ IDAL	Is in ARP4754A and not in ARP4761.	Is in ARP4761A and not in ARP4754B. However, the FDAL/ IDAL approach has not changed and doesn’t account for the Part 23 airworthiness level 1-4 and Part 27 class I-IV FDAL/ IDAL reductions.
Depth of analysis	Specifies that the approach i.e. qualitative, quantitative or both should be established. ARP4761 Fig. 4 provides guidance on MAJ failure condition.	Is more explicit about the relationship between the failure condition classification and the depth of analysis. Also, it defers to advisory circular material.

Subject	ARP4761	ARP4761A
Minimum Equipment List (MEL)/ Master Minimum Equipment List (MMEL)	Mentioned by ARP4761 F.5.2 “a scheduled maintenance example.”	The relationship between dispatch relief time and exposure time derived from a fault tree analysis is explained. The concept of a specific risk analysis as opposed to an average risk analysis to derive exposure time is introduced. Also, ARP5107B “Guidelines for Time-Limited-Dispatch (TLD) Analysis for Electronic Engine Control Systems” is referenced.
Electrical Wiring Interconnect System (EWIS)	ARP4761 precedes regulatory changes introducing EWIS concept[14].	Applies safety analysis techniques to EWIS. However, EWIS applies to Part 25 not Part 23. Regardless, the EWIS concept is particularly relevant to a UAM aircraft.
Human factors	Mentioned by ARP4761 D.6 “FTA analysis definition.” Otherwise, not considered or mentioned.	Credit is taken that flight crew and maintenance crew follow documented procedures. Evaluation of human factors is deferred. Both intentional and unintentional deviation is not considered.
Cascading effects analysis	No explicit mention of cascading effect analysis. However, consideration of the cascading effects of a failure condition is standard practice.	Explicitly requires the analysis of the system level, aircraft level and multi-system effects of failure modes, combinations of failure modes and failure conditions.

Table 11-1: main difference between ARP4761 and ARP4761A

[14] The EWIS concept and it’s associated regulatory changes were introduced following TWA 800, 1996 and SA111, 1998.

12 Holistic Safety Analysis for a UAM aircraft

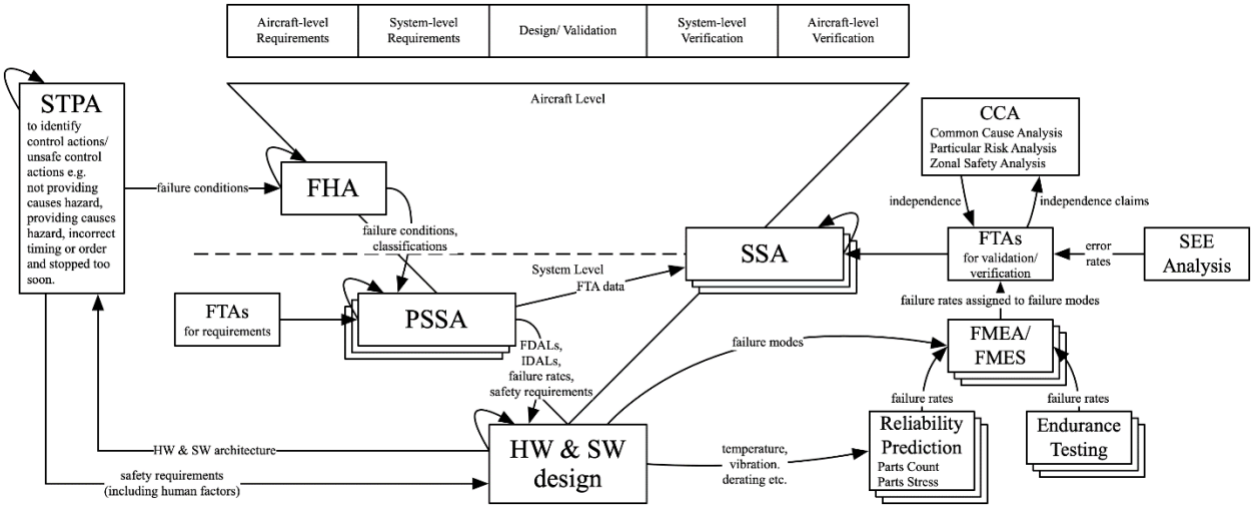

Figure 12-1: holistic safety analysis framework

The holistic safety analysis framework introduces the following changes compared to ARP4761 and ARP4761A:

- Adds STPA to address human factors, identify missing failure conditions plus hardware and software requirements and validates those that already exist.
- Flattens the structure of the safety analysis.
- Depicts the relationship between the reliability prediction, endurance testing, Single Event Effect (SEE) analysis and other safety analysis activities.

STPA is selected because of its relative maturity and regulatory acceptance compared to other model-based systems/ safety techniques. Also, it addresses human factors, identifies missing failure conditions plus hardware and software requirements and validates those that already exist.

The flattening of the structure to one tier instead of two tiers for ARP4761 and three tiers for ARP4761A streamlines the safety analysis, accommodates more frequent iterations and can be used to shorten the design and development lifecycle. This is possible because of the relative complexity of a UAM aircraft compared to a traditional Part 25 aircraft and even a traditional Part 23 aircraft. Also, it is necessary because of the level of systems integration which means that more than ever the effect of a failure is expected to manifest itself at the aircraft level as opposed to the system level. Furthermore, the flattening of the structure will enable a more proactive safety analysis and one that informs as opposed to reacts to the hardware and software design processes.

The SEE analysis over recent years has been applied to Part 25 aircraft flying at high altitudes and high geographic latitudes (north and south). Atmospheric particles (mainly neutrons and protons) have become more of a risk as a result of the reduction in the feature size of devices and the number of devices per aircraft. Devices that make use of technology that is immune to atmospheric particles are preferred. Per SAE AIR6219, an aircraft at ~40,000ft ASL (e.g. Part 25 aircraft) is exposed to relative atmospheric particle flux of ten times that of an aircraft at ~10,000ft ASL (e.g. UAM aircraft). However, the following factors will increase the risk of a UAM aircraft to atmospheric particles:

- The number of devices is expected to be high for a UAM aircraft compared to a Part 25 aircraft.
- It may not be possible to select technology that is immune to atmospheric particles.
- Mitigations such as the derating of power electronics may not be possible.

13 Abbreviations, Applicable Industry Standards and References

13.1Abbreviations

Abbreviation	Meaning
AC	Advisory Circular
AFHA	Aircraft-level Functional Hazard Analysis
Arch. Req.	Architecture Requirements
ASA	Aircraft Safety Assessment
CCA	Com mon Cause Analysis
CCA	Common Cause Analysis
COTS	Commercial Off The Shelf
DAL	Development Assurance Level
EASA	European Union Aviation Safety Agency
FAA	Federal Aviation Administration
FC&C	Failure Conditions and Classifications
FDAL	Function Development Assurance Level
FE	Failure Effects
FE&P	Failure Effects and Probability
FHA	Functional Hazard Analysis
FM	Failure Modes
FMEA	Failure Modes and Effects Analysis
FMES	Failure Modes Effects Summary
FTA	Fault Tree Analysis
HW	Hardware
IDAL	Item Development Assurance Level
PASA	Preliminary Aircraft Safety Assessment
PSSA	Preliminary System Safety Assessment
SC VTOL	Special Conditions Vertical Takeoff and Landing
SEE	Single Event Effects
SFHA	System-level Functional Hazard Analysis
SSA	System Safety Assessment
STPA	Systems Theoretic Process Analysis
SW	Software
UAM	Urban Air Mobility
λ	Failure Rate

Table 13-1: abbreviations

13.2Applicable Industry Standards

SAE ARP 4754A, “Guidelines for Development of Civil Aircraft and Systems”

- Recognized by AC 20-174 as an acceptable means of compliance
- Being updated by SAE S18 to ARP 4754B

SAE ARP 4761, “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne System and Equipment”

- Recognized by ARP 4754
- Being updated by SAE S18 to ARP 4761A

ASTM F3061-19a, “Standard Specification for Systems and Equipment in Small Aircraft.”

ASTM F3230-17, “Standard Practices for Safety Assessment for Systems and Equipment in Small Aircraft.”

SAE AIR6913, “Using STPA During Development and Safety Assessment of Civil Aircraft.”

ASTM WK60748, “New Guide for Application of Systems-Theoretic Process Analysis to Aircraft.”

SAE AIR6219, “Incorporation of Atmospheric Neutron Single Event Effects Analysis into a Safety Assessment”

ARP5150 “Safety Assessment of Transport Airplanes in Commercial Service.”

ARP5151, “Safety Assessment of General Aviation Airplanes and Rotorcraft in Commercial Service.”

ASTM F3254, “Aircraft Interaction of Systems and Structures.”

DO-178C, “Software Considerations in Airborne Systems and Equipment Certification.”

DO-330, “Software Tool Qualification Considerations.”

DO-331, “Model-Based Development and Verification Supplement to DO-178C and DO-278A.”

DO-332, “Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A.”

DO-333, “Formal Methods Supplement to DO-178C and DO-278A.”

DO-254, “Design Assurance Guidance for Airborne Electronic Hardware.”

DO-160G, “Environmental Conditions and Test Procedures for Airborne Equipment.”

13.3References

Mackworth N. H. 1948. “The breakdown of vigilance during prolonged visual search. Quarterly Journal of Experimental Psychology.”

Moak L. et al. 2020. “Official Report of the Special Committee to review the Federal Aviation Administration’s Aircraft Certification Process”

Parasuraman R. 1997, Humans and Automation; Use, Misuse, Disuse, Abuse. Human Factors and Ergonomics Society.

AC 23.1309-1E, 2011. “System Safety Analysis and Assessment for Part 23 Airplanes.”

PS-ASW-27-15, 2017. “Safety Continuum for Part 27 Normal Category Rotorcraft Systems and

Equipment.”

RAIC, 2015. “RAIC’s Reliability Prediction Methodology” Reliability Information Analysis Center, 2015.”

SWCEH-001 Issue 1, Revision 2, 2018. “Development Assurance of Airborne Electronic Hardware.”

SC VTOL, 2019. “Special Condition for Small-category VTOL aircraft.”