L-SYS

Regulations and Standards Gap Analysis Approach

1 Introduction

Traditionally, novel technologies and applications of technologies such as an electric or hybrid-electric powertrain have been accommodated via special conditions which are often written independently of the safety analysis introducing inconsistencies. Also, the means of compliance i.e. consensus standards from organizations such as ASTM may be inappropriate, incomplete or missing details that it is not possible to add until the consensus standards are applied to a system architecture.

The transition from non-performance to performance based regulations is an abstraction which leaves a void to be filled because systems engineering and design assurance objectives dictate that there is traceability from regulations and safety assurance objectives, through requirements tiers, to the software and complex hardware. Also, the Part 33 special conditions that have been developed for inverters and electric motors have been derived from regulations for turbines and reciprocating engines. This assumes that there are parallels between these inherently disparate technologies. In some cases this is true in other cases regulations cannot be simply translated from turbines and reciprocating engines. For example:

33.17 Fire Protection	Is applicable per the MagniX special conditions. However, 33.17 focusses on the use of a firewall to protect against flammable fluids. A firewall is likely to be a wholly ineffective means of protecting against an electrical fire and flammable fluids can be eliminated from inverters and electric motors.
13. Critical and Life Limited Parts	Is applicable per MagniX special condition 13. In a similar manner to other electrical and electronic equipment on an aircraft the inverter and electric motor with the exception of the bearings may not experience a wearout mechanism. Even the bearings may not experience a wearout mechanism during the expected life of the electric motors. This is contrary to turbines and reciprocating engines that have many more moving parts that are life limited.
14. Lubrication Systems	Is applicable per MagniX special condition 14. Lubrication systems are applicable to turbines and reciprocating engines and electric motors if they have, for example, gearboxes for auxiliary systems such as pumps and governors. However, if these systems can be replaced by electric pumps and governors, it is possible to eliminate lubrication systems completely.
18. Ingestion	Is applicable per MagniX special condition 18. Ingestion is applicable to engines with inlet ducts. However, there is no reason to assume that electric motors will have inlet ducts.

The proposal is that a holistic safety approach, similar to that advocated by Moak, L. et al. (2020), is leveraged to derive/ validate requirements that bridge the regulations and standards gap and that are consistent with safety assurance objectives. The underlying assumption is that an aircraft with an electric or hybrid-electric aircraft is not a special class of aircraft under 21.17(b). However, if it were, the same approach could be applied.

The approach compresses the structure of the safety analysis so that more frequent iterations can be completed to derive/ validate requirements and adds techniques to address human factors which are generally missing the

safety analysis. Additionally, it leverages a full aircraft modeling and simulation effort to derive/ validate requirements for the systems and sub-systems that constitute the system architecture.

First, the recent evolution from ARP 4761 to 4761A and the difference between these two approaches is described. This provides the context for the holistic safety approach which is described.

2 Comparison of ARP4761 and ARP4761A

Figure 2-1 is a copy of the ARP4761 safety framework and Figure 2-2 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 2-1 shows 3 levels of FTA/ CCA and Figure 2-2 shows 2 tiers (a PASA and a PSSA) on the left side of the V-model.
- Figure 2-1 shows 3 levels of FTA/ CCA and Figure 2-2 shows 2 tiers (an SSA and a ASA) on the right side of the V-model.
- Figure 2-1 identifies FMEA and FMES items specifically (these can be assumed to be part of the SSA and ASA of Figure 2-2).

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.

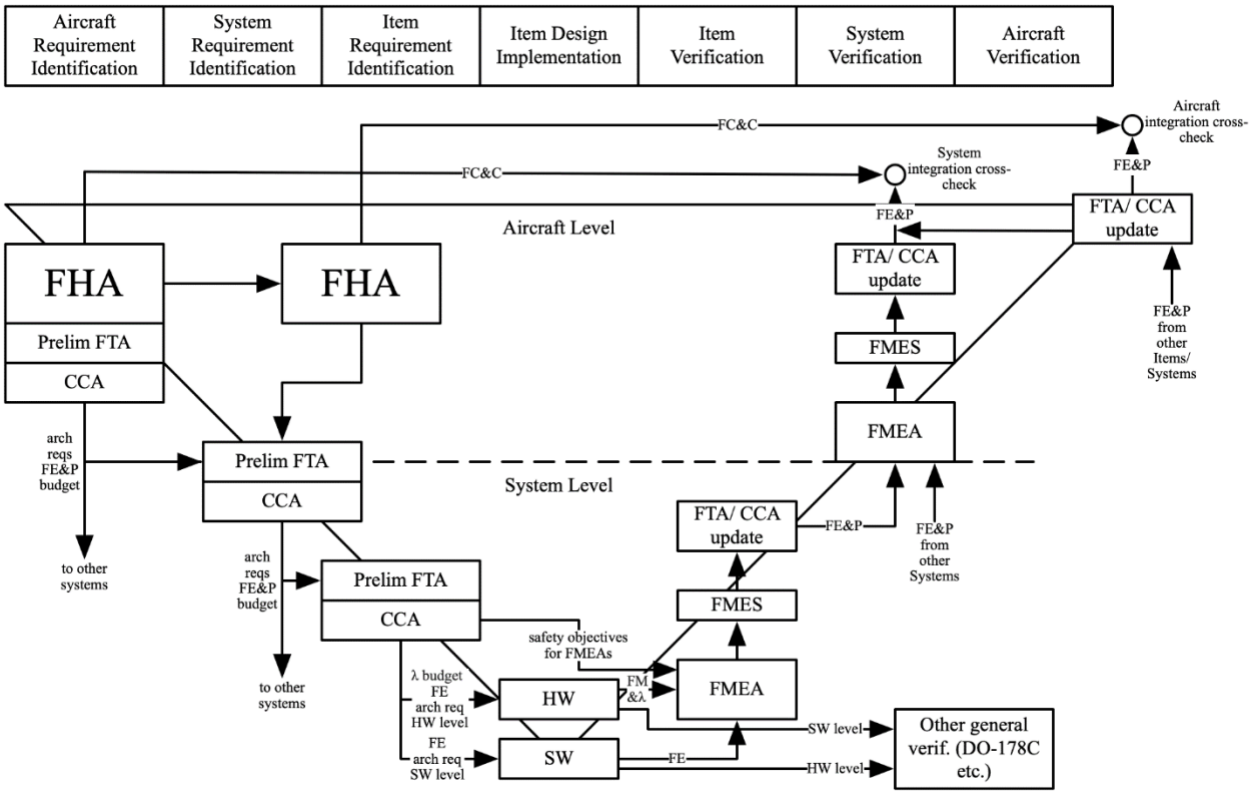

Figure 2-1: ARP4761 topology

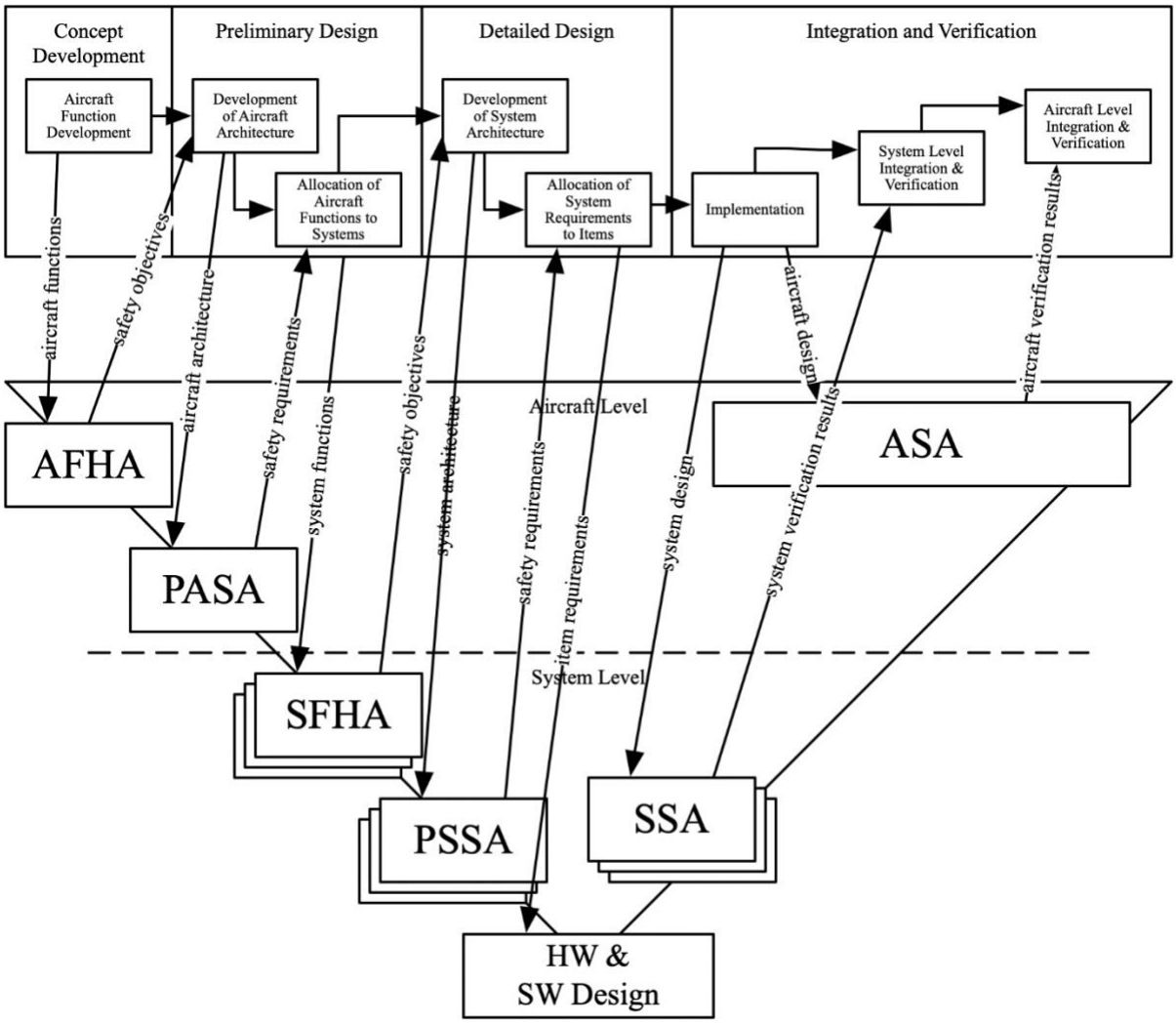

Figure 2-2: ARP4761A topology

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

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

Subject	ARP4761	ARP4761A
		Airplanes in Commercial Service" 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[1].	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 2-1: main difference between ARP4761 and ARP4761A

3 Systems Theoretic Process Analysis

Systems Theoretic Process Analysis (STPA) is a relatively new safety analysis technique which has a controls theory foundation. A control structure is created for a system or sub-system (see Figure 3-1). This control structure is then analyzed for control actions and unsafe control actions focusing on the following:

- Not providing the control action.
- Providing the control action incorrect.
- Providing a potentially safe control action but too early, too late, or in the wrong order.

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

- The control action is stopped too soon or applied too long.

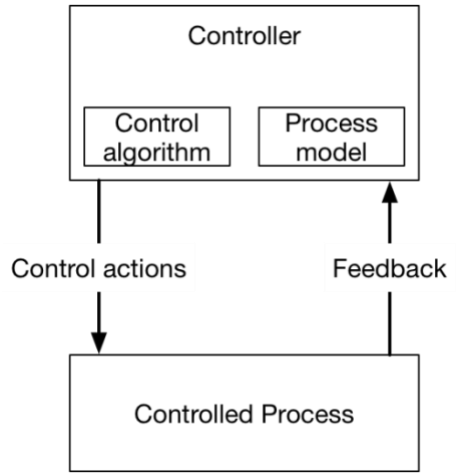

Figure 3-1: example control structure

STPA will be used to identify regulations and standards gaps. Also, it will be used to identify missing failure conditions and identify safety requirements including human factors. Figure 3-2 and Figure 3-3 are examples of STPA applied to an Electrical Propulsion System (EPS) and an Energy Storage System (ESS) to identify missing failure conditions. The integration of STPA with traditional safety analysis techniques in this way is innovative and is expected to result in a more holistic safety analysis approach that can be used to bridge the regulations and standards gap.

3.1 Electrical Propulsion System STPA Example

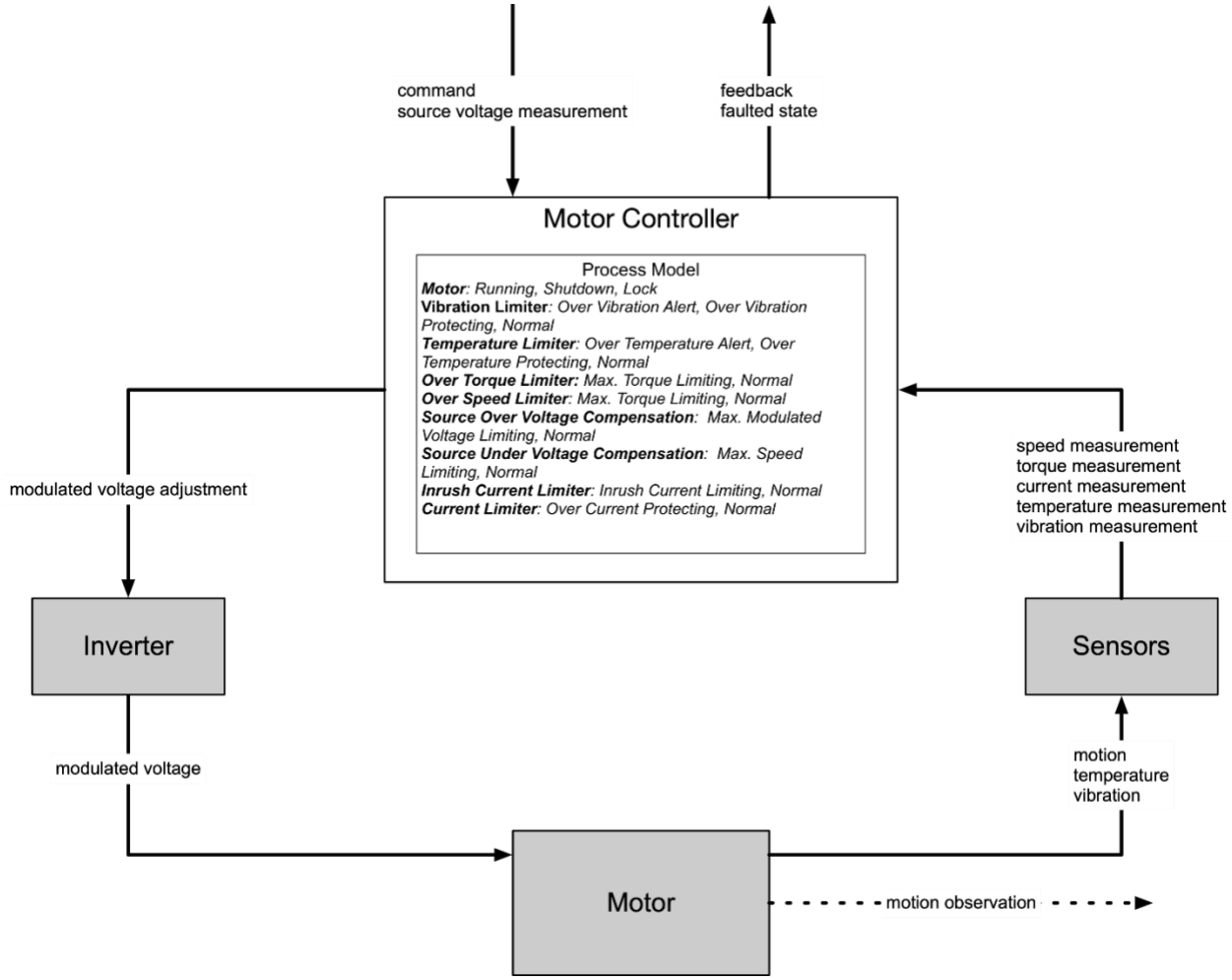

Figure 3-2: EPS STPA example

Unsafe Control Actions	**Failure Condition**
No motor shutdown by aircrew when over temperature alert	Overtemperature
No motor shutdown by aircrew when over vibration alert	Unbalanced motor
No motor shutdown by aircrew when over speed alert	Overspeed
No motor shutdown by aircrew when over torque alert	Overtorque
No motor shutdown by aircrew when over current alert	Overtemperature
No voltage modulation when motor running	Loss of thrust
Incorrect voltage modulation when motor shutdown	Uncommanded thrust
Incorrect voltage modulation when motor locked	Uncommanded thrust

Table 3-1: example of how STPA can be used to identify missing EPS failure conditions

3.2 Energy Storage System STPA Example

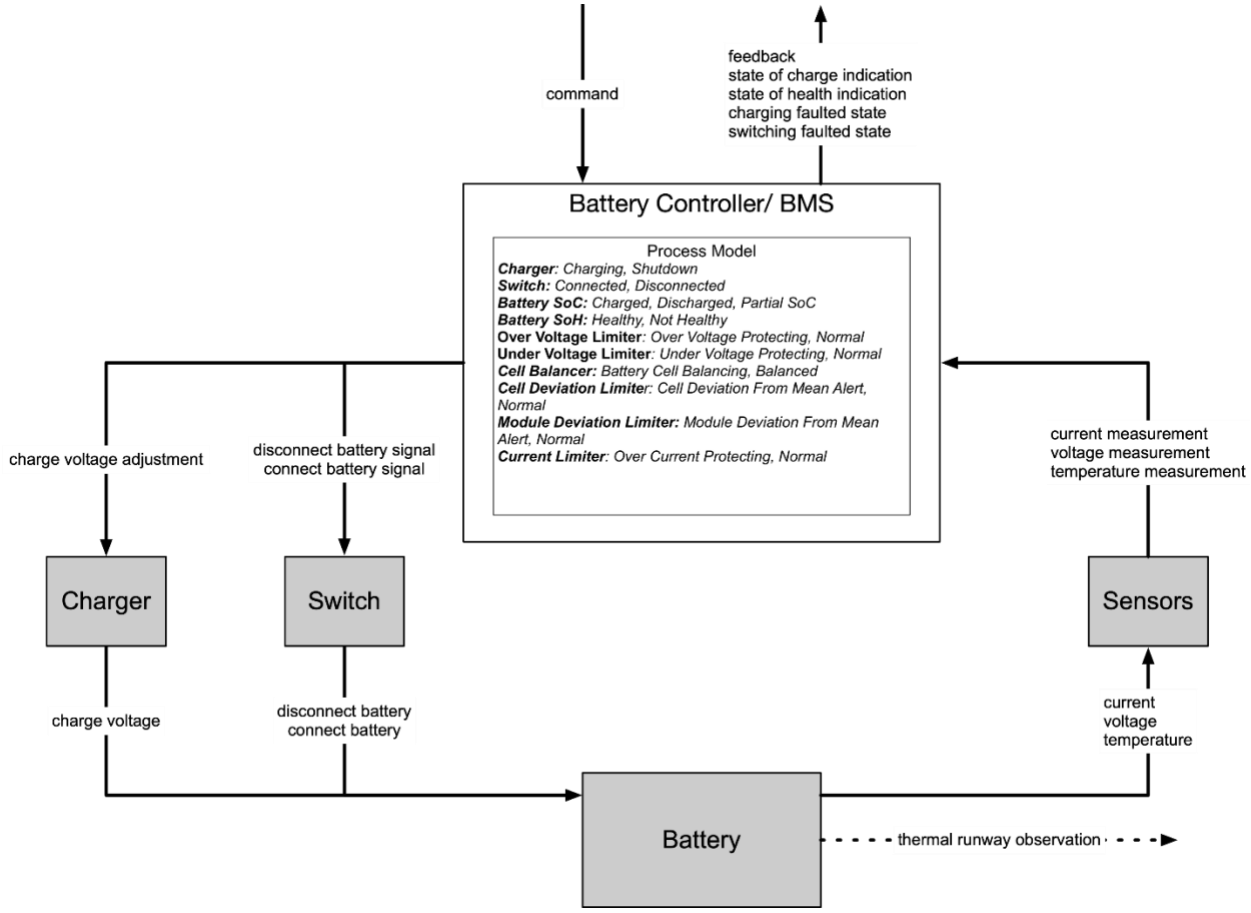

Figure 3-3: ESS STPA example

Unsafe Control Actions	**Failure Condition**
No charger shutdown by BMS when battery charged	Uncontained thermal runaway
No switch disconnect by BMS when battery discharged	Uncontained thermal runaway
Charger shutdown too early by BMS when battery discharged	Loss of thrust
Switch disconnect too early by BMS when battery charged	Loss of thrust
No cell deviation limiting when cell deviation from mean alert	Uncontained thermal runaway
No module deviation limiting when module deviation from mean alert	Uncontained thermal runaway
No emergency procedure by aircrew when battery unhealthy	Loss of thrust

Table 3-2: example of how STPA can be used to identify missing ESS failure conditions

4 Holistic Safety Analysis Approach

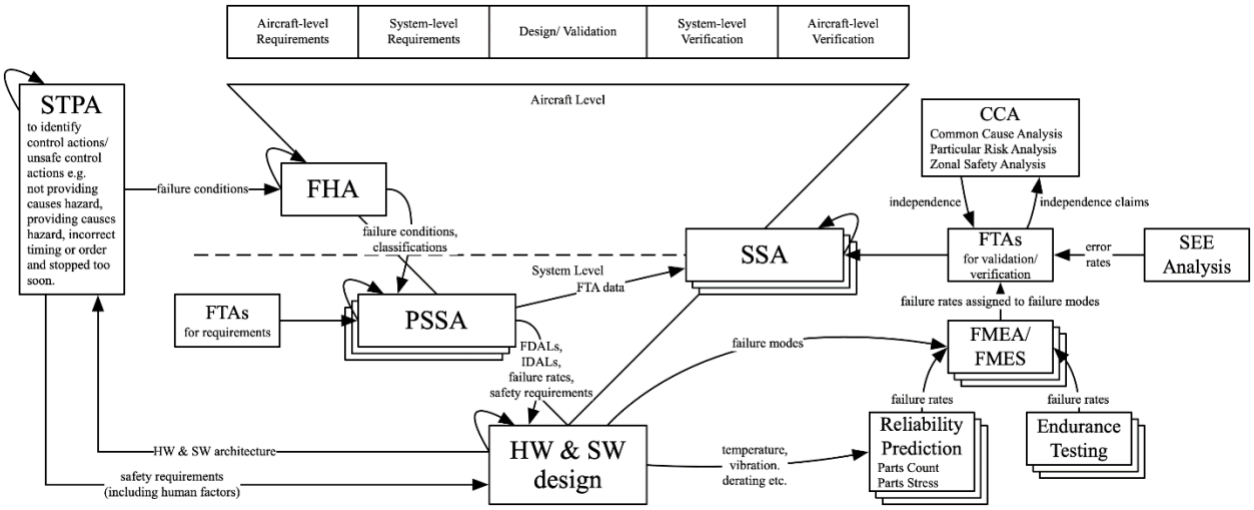

Figure 4-1: holistic safety analysis framework

The holistic safety analysis 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.
- Compresses 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 identifies missing system, hardware and software requirements, validates those that already exist and bridges the regulations and standards gap.

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. Also, it enables a complete iteration of the safety analysis to derive/ validate requirements and bridge the regulations and standards gap at the beginning of the engineering lifecycle prior to a formal System Requirement Review (SRR). After, the SRR it enables additional iterations that add detail and inform the software and complex hardware processes in a consistent and coordinated manner. Additionally, a parallel modeling and simulation effort is being completed. This effort is specific to the system architecture under development and ensures the end-to-end consistency of requirements. In the absence of a full set of regulation and standards, the modeling and simulation effort ensures system, high-level and low-level requirement coverage. Also, the output from the modelling and simulation effort can specifically the functions and their interdependency can be used as an input to the STPA effort.

The benefit of the holistic safety analysis is that it is agnostic to the system architecture. Therefore, it can be applied without a full set of regulations and standards. Once complete, the framework of system and sub-system requirements can be abstracted and applied to similar system architectures.

5 Highest priority regulations and standards

The known gaps described by the following sections are of highest priority. However, the holistic safety analysis approach is expected to identify additional gaps.

5.1 Turbo Generator System

TSO-C77b exists for gas turbine Auxiliary Power Units (APUs). It provides a useful foundation. However, the application of a gas turbine supporting a powertrain versus the APU application to provide electrical, mechanical or pneumatic power to support aircraft system and sub-system operation have different requirements. For example:

- Safety assurance requirements such as probability budgets are design assurance levels are different.
- Environmental requirements such as altitude are different (the APU application may not require that the gas turbine operates at maximum cruise altitude).
- There is no equivalent to 33.28(d)(2) which requires that the engine control system is single fault tolerant with respect to loss of thrust control and loss of power control events.
- TSO-C77b and 33.49(b) have an equivalent of 150 hours endurance testing. However, the schedules are different. For example, TSO-C77b is twenty periods of 7.5 hours and 33.49(b) is one period of 30 hours followed by six periods of 20 hours. Therefore, TSO-C77b is less stringent versus 33.49(b).

5.2 Electrical Propulsion System

Magnix special conditions were derived from turbine and reciprocating engine regulations. This approach is effective for failure conditions where there are parallels between turbine/ reciprocating technology and inverters and electric motors, but inappropriate where parallels don't exist. For example, fires caused by flammable fluids and their mitigations and for electric fires and their mitigations. Additionally, 33.17 Fire Protection, 13. Critical and Life Limited Parts, 14. Lubrication Systems, 18. Ingestion are have been applied to inverters and electric motors per the MagniX special conditions. However, these regulations/ special conditions are still heavily influenced by turbine and reciprocating engine technology.

Also, the failure conditions of 33.75(g)(2) have been revised by the MagniX special conditions. However, they are still heavily influenced by turbine and reciprocating engine failure conditions. There are missing failure conditions that are not in the revised set of failure conditions. For example, corona discharge, over voltage, overvoltage caused by uncontrolled regenerative voltage and partial discharge.

SAE E-40 Electrified Propulsion Committee relevant activities:

- AIR8678, Architecture Examples for Electrified Propulsion Aircraft (WIP).
- ARP8676, Nomenclature & Definitions for Electrified Propulsion Aircraft (WIP).
- ARP8677, Safety Considerations for Electrified Propulsion Aircraft (WIP).
- ARP8689, Endurance tests for Aircraft Electric Engine (WIP).

5.3 Energy Storage System

The introduction of rechargeable lithium-ion batteries onto aircraft with a standard airworthiness certificate has been plagued by issues. RTCA DO-311/ DO311A were written in response to these issues. Arguably, the battery thermal runaway containment test of RTCA DO-311A 2.2.2.4 per the dissenting opinion of DO-311A Appendix D ignores standard aerospace practice of relating probability severity to

probability objectives and is unrealistic in that it assumes test conditions that are not expected to be encountered in service. DO-311A Appendix C proposes alternative more realistic test conditions, but it has not been approved by the FAA.

Additionally, the revision from AC 20-184 to AC 20-184A that is expected to clarify the application of DO-311A is still in draft format. Also, draft AC 20-184A Appendix F includes Table G-. However, it includes the caveat "(2) Available paths to respective normal category airplane certification level in Table G-1 may not map to electric (or hybrid) airplane directly."

5.4 Hydrogen Fuel Cell System

SAE AE-7AFC Fuel Cell Task Group relevant activities:

- AIR6464, Hydrogen Fuel Cells Aircraft Fuel Cell Safety Guidelines.
- AIR7765, Considerations for Hydrogen Fuel Cells in Airborne Applications.
- AS6858, Installation of Fuel Cell Systems in Large Civil Aircraft.
- AS6679, Liquid Hydrogen Storage For Aviation (WIP).

Note: SAE AE-7AFC is for onboard applications, but not specifically onboard inverter and electric motor applications.

Another source of guidance is the Energy Supply Device (ESD) Aviation Rulemaking Committee (ARC) report to FAA December 8, 2017. The report has been used to validate and identify missing failure conditions and it has been compared to RTCA DO-160G to identify regulations and standards gaps.

Ref_EAFC	EAFC_D	Failure Condition	RTCA DO-160G Section Title
F10	electrical hazards	Uncontrolled LVPD over current, Uncontrolled HVPD over current, Uncontrolled HVPD to LVPD wire-to-wire short, Uncontrolled LV arcing, Uncontrolled HV arcing, Uncontrolled HVPD over voltage, Uncontrolled LVPD over voltage	Explosion proofness
F2.2.1	hydrogen jet fire	Hydrogen jet fire/ microflame	Fire, flammability
F2.2.2	microflames	Hydrogen jet fire/ microflame	Fire, flammability
F2.2.3	hydrogen deflagration	Hydrogen fuel deflagration	Fire, flammability
F2.2.5	hydrogen detonation	Hydrogen fuel detonation	Fire, flammability
F2.3.1	ignition due to electrical sources	Uncontrolled LVPD over current, Uncontrolled HVPD over current, Uncontrolled HVPD to LVPD wire-to-wire short, Uncontrolled LV arcing, Uncontrolled HV arcing, Uncontrolled	Explosion proofness

		HVPD over voltage, Uncontrolled LVPD over voltage	
F2.3.1.5	electrostatic discharge		Electrostatic discharge
F2.3.1.7	lightning		Lightning induced transient susceptibility, Lightning direct effects
F2.3.1.8	corona discharge		Temperature and altitude, Temperature variation, Explosion proofness
F2.3.1.9	HIRF		Radio frequency susceptibility (radiated and conducted)
F2.3.2	ignition due to thermal sources		Explosion proofness
F2.3.3	ignition due to mechanical sources		Explosion proofness
F3.1.1	embrittlement		
F3.1.2	diffusion/ permeation		
F3.2	failure of gaseous storage systems and failure of pressure relief valves	Hydrogen fuel leak, Loss of hydrogen overpressurisation safety release, Inadvertent hydrogen overpressurisation safety release	
F3.4	crashworthiness	Structure fails to dissipate crash survivable loads	
F4	implementation/ application		
F6	maintenance induced hazards/ ground crew and air crew errors		

F7	failure of fire suppression	Loss of fire suppression	
F8	failure of cryogenic cooling of hydrogen fuel	Loss of cryogenic hydrogen fuel cooling	
F9	non-hydrogen fuel and oxygen hazards	Loss of non-hydrogen fuel and oxygen status, Misleading non-hydrogen fuel and oxygen status, Loss of non-hydrogen fuel and oxygen distribution, Inability to shutdown non-hydrogen fuel and oxygen, Non-hydrogen fuel and oxygen leak, Non-hydrogen fuel and oxygen jet fire/ microflame, Non-hydrogen fuel and oxygen fuel detonation, Non-hydrogen fuel and oxygen deflagration, Loss of non-hydrogen fuel and oxygen overpressurisation safety release, Inadvertent non-hydrogen fuel and oxygen overpressurisation safety release, Loss of non-hydrogen fuel and oxygen leak detection, Erroneous non-hydrogen fuel and oxygen leak detection	
F5	physiological		

Table 5-1: use of ESD ARC to identify regulations and standards gaps

5.5 Part 23

It is a misconception that Part 23 Amendment 64 is a performance-based regulatory framework. In reality many of the performance-based regulations 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 intent is to use the holistic safety approach to bridge the gap particularly in the following areas:

- Integration of the Electrical Propulsion System.
- Integration of the Energy Storage System.
- Integration of the Turbo Generator System.

5.6 Part 25

Unlike Part 23, Part 23 has not undergone a rewrite to convert it from a non-performance to a performance based regulatory framework. Therefore, it cannot accommodate novel technology and novel applications of technology the same way that Part 23 can. It is possible that the hydrogen fuel cell

system powertrain can be accommodated via 21.17(b). Regardless, the holistic safety approach to bridge the gap particularly in the following areas:

- Integration of the Electrical Propulsion System.
- Integration of the Hydrogen Fuel Cell System.
- Hydrogen Storage.

Other areas that may require novel technology and novel applications of technology include the cooling system and distribution of hydrogen.