FUELEAP Model-Based System Safety Analysis

Kurt P. Woodham,[1] Patrick J. Graydon,[2] and Nicholas K. Borer[3]
NASA Langley Research Center, Hampton, VA, 23681, USA

Kurt P. Papathakis[4]
NASA Armstrong Flight Research Center, Edwards, CA, 93523, USA

and
Tina Stoia[5] and Chellappa Balan[6]
The Boeing Company, Huntington Beach, CA, 92647, USA

NASA researchers, in a partnership with Boeing, are investigating a fuel-cell powered variant of the X-57 "Maxwell" Mod-II electric propulsion aircraft, which is itself derived from a stock Tecnam P2006T. The "Fostering Ultra-Efficient Low-Emitting Aviation Power" (FUELEAP) project will replace the X-57 power subsystem with a hybrid Solid-Oxide Fuel Cell (SOFC) system to increase the potential range of the electric-propulsion aircraft while dramatically improving efficiency and emissions over stock internal-combustion engines.

Our FUELEAP safety analysis faces two primary challenges. First, the Part 23 certificated Tecnam P2006T is undergoing significant modifications to host the hybrid electric-propulsion system, and the challenge is to assure that the safety inherent in the stock aircraft (and subsequently in X-57 Mod-II) is not compromised by changes in avionics, aircraft structural loading, weight and balance, or other considerations. Secondly, because the SOFC power system has little (if any) relevant in-service precedent, our challenge is to assure that we identify and mitigate all reasonably plausible hazards introduced by unique FUELEAP equipage.

We are investigating and utilizing Model-Based Safety Analysis (MBSA) methods to help us address these FUELEAP safety challenges. We captured aircraft-level system hazard conditions using instances of a SysML hazard block via aircraft-level Functional Hazard Analysis (FHA). Then, using SysML models of the FUELEAP architecture, we related the hazard conditions to initiating system events and possible mitigations, such as design architecture modifications or operational constraints. We are continuing to define our approach to MBSA by developing a component-by-component inventory of local failure modes and tracing their possible contribution to hazard conditions.

Finally, we are applying an argument-based approach to FUELEAP assurance. Through a FUELEAP "safety case," we are providing an explicit argument for FUELEAP safety by associating assurance evidence with overarching safety claims through a structured argument.

[1] Safety-Critical Avionics System Branch, kurt.woodham@nasa.gov, non-member.
[2] Safety-Critical Avionics System Branch, patrick.j.graydon@nasa.gov, non-member.
[3] FUELEAP PI Aeronautics Systems Analysis Branch, nicholas.k.borer@nasa.gov, AIAA Senior member.
[4] Flight Instr. and Systems Integration Branch, kurt.papathakis@nasa.gov, AIAA member.
[5] Boeing Defense Systems, 5301 Bolsa Ave. MC H013-C335, non-member.
[6] Boeing Defense Systems, 5301 Bolsa Ave. MC H013-C335, non-member.

I. Nomenclature

ARP	=	Aerospace Recommended Practice
ASRB	=	Airworthiness and Safety Review Board
CFR	=	Code of Federal Regulations
DAC	=	Design Analysis Cycle
DEP	=	Distributed Electric Propulsion
FBO	=	Fixed-Base Operator
FD	=	Flight Demonstrator
FHA	=	Functional Hazard Assessment
FUELEAP	=	Fostering Ultra-Efficient Low-Emitting Aviation Power
GRC	=	Glenn Research Center
ICE	=	Internal Combustion Engine
LaRC	=	Langley Research Center
MBSA	=	Model-Based Safety Analysis
MBSE	=	Model-Based Systems Engineering
PMG	=	Permanent Magnet Generator
SAE	=	Society of Automotive Engineers
SCEPTOR	=	Scalable Convergent Electric Propulsion Technology and Operations Research
SOFC	=	Solid Oxide Fuel Cell
SSA	=	System Safety Assessment
SysML	=	Systems Modeling Language

II. Introduction

The “Fostering Ultra-Efficient Low-Emitting Aviation Power” or “FUELEAP” project is investigating replacing the all-battery X-57 Mod II power subsystem with a Solid-Oxide Fuel Cell (SOFC)/battery hybrid variant to increase the potential range of the electric-propulsion aircraft while dramatically improving efficiency and emissions over stock internal-combustion engines. We completed an initial feasibility study in 2016, Design Analysis Cycle (DAC) iterations in 2017 and 2018, and we are continuing to refine the concept design while performing fuel cell testing at Glenn Research Center (GRC). The reader will find additional information on FUELEAP in Refs. 1–5.

Our FUELEAP safety analysis is concerned with two primary challenges. First, the Part 23-certificated Tecnam P2006T is undergoing significant modifications to host first the X-57 Mod II configuration followed by the FUELEAP SOFC hybrid power subsystem, which we base on the Mod II power subsystem. While both X-57 Mod II and FUELEAP use the stock wing and “engine” nacelle locations, our challenge will be to assure that changes in avionics, aircraft structural loading, aircraft weight and balance, or other considerations do not adversely impact the safety inherent in the stock aircraft. Secondly, because major elements of the SOFC power system has little (if any) in-service history, our challenge is to make sure that we identify all reasonably plausible failure conditions introduced by the FUELEAP modifications and unique equipage and mitigate any related hazard conditions.

We are addressing these challenges using Model-Based Safety Analysis (MBSA) within the context of an overarching Model-Based Systems Engineering (MBSE) approach. First, following the Functional Hazards Assessment (FHA) outlined in Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) ARP 4754A (Ref. 6) and ARP 4761 (Ref. 7), we identify and capture top-level (aircraft) hazards using a SysML hazard meta-model. We annotate each hazard instance with relevant metadata (flight phase, mitigation strategy, verification strategy, etc.) and trace each hazard to initiating events and mitigations provided by the system architecture, specific components, or flight-test operational profiles.

Our approach does not assume that all safety analysis is conducted using the SysML system model (nor that it should be), but that a SysML model can provide an overarching perspective on the state and thoroughness of the system safety analysis. With this in mind, as a view towards future MBSA application at NASA, we plan to investigate ways to expose modeled system attributes relevant to external safety analysis tools and methods and, conversely, provide means to import results from those tools and methods back into the SysML model.

Likewise, as an extension to this effort, we intend to configure the MBSA approach to support automated generation of safety artifacts such as hazard reports, traceability from hazard to safety requirement, and traceability from safety requirements through their realization in the system architecture. This capability will provide the means to extract from the model safety data and/or artifacts necessary to support NASA internal review boards and future evidence for certification as the technologies and systems prototyped under the FUELEAP program transition to civil applications.

Parallel to our MBSE approach, we are tapping expertise within our team in the field of argument-based assurance. Mainstream approaches to safety-critical assurance tend to follow "tried and true" design and development assurance processes that conform to long-standing industry consensus practices endorsed by regulatory agents. While these methods imply, and generally deliver, strong evidence that a system is safe, this evidence is in no small part due to successful fielding of similar systems in the past. Stated differently, because similar systems have shown themselves to be safe in similar operational contexts, the use of similar development and assurance methods on a new system implies that it will be safe as well (if operated in a similar environment and manner). Because FUELEAP has, to our knowledge, little development or operational precedent, we see the application of argument-based assurance as a reasonable and beneficial addition to our approach to assuring FUELEAP safety. The FUELEAP safety case includes an explicit argument that supports a top-level, overarching claim regarding FUELEAP safety using an argument structure that incorporates information about context, operational restrictions, and design features and other evidence. We see this approach as a valuable addition to standard safety assurance methods: where they provide an implicit level of assurance (historically, the use of these methods results in safe fielded systems), a safety case provides explicit assurance in that its argument is based squarely on features of the FUELEAP system and its operational and environmental contexts.

The intent of the FUELEAP project, rooted in its predecessor feasibility study, is to "overcome the adoption barrier to electric flight." While FUELEAP has overcome many technical hurdles, the FUELEAP team has maintained a safety perspective throughout the project to address not only NASA airworthiness considerations but also a forward view towards certification of hybrid-electric propulsion system in a civil aviation context. Although we are still formulating our MBSA models and analysis processes, we feel the use of MBSA, coupled with an explicit safety-case, will provide a strong basis for assuring FUELEAP safety and a basis for supporting future civil certification needs.

We have structured the rest of this paper as follows: Section III provides a brief overview of FUELEAP along with pointers to other more in-depth descriptions. Section IV provides an overview of safety analysis methods and process, based on established guidance for civil aviation application, as well as specific processes we must address for NASA airworthiness. Section V provides a description of our approach to applying the Section III assurance processes to FUELEAP in an MBSA context. Finally, Section VI provides a summary of the topics addressed to date in our analysis of FUELEAP safety, and future objectives and plans.

III. FUELEAP Overview

This narrative provides only a high-level overview of the FUELEAP project, and we encourage the reader to look to Refs. 1–5 for a more detailed description of the project.

As part of the FUELEAP project, NASA is investigating changing the energy storage system on the NASA X-57 (Maxwell) Mod II configuration. Developed and managed under NASA's Scalable Convergent Electric Propulsion Technology and Operations Research (SCEPTOR) project, X-57 is a series of four modifications (Mods) of a stock Tecnam P2006T. Mod I will consist of the P2006T Tecnam instrumented to establish baseline performance metrics with the stock Rotax 912 100 HP engines. MOD II replaces the Rotax engines in the stock engine nacelles with electric cruise motors produced by Joby Aviation and powered by the X-57 all-battery power subsystem. As such, Mod II is a conversion of the baseline Tecnam from an Internal Combustion Engine (ICE) configuration to an all-electric configuration with the stock aerodynamic profile intact.

Mods III and IV introduce a departure from the stock aerodynamics and propulsion configuration through the integration of a low-area, high-load wing designed to provide a significant reduction in cruise drag. Mod III relocates the electric cruise motors in to the tips of this low-area wing and Mod IV integrates a set of six small boost motors along each leading edge to increase lift during takeoff and landing. These boost motors are equipped with folding-blade propellers that blend with the boost motor nacelles during cruise to provide a clean aerodynamic profile. The overarching goal of X-57, then, is to demonstrate the viability of extended-range, all-electric flight with distributed electric propulsion (DEP) to enhance take-off and landing lift while reducing cruise drag. Fig. 1 provides a rendering of the Mod IV X-57.

NASA anticipates that the low-drag cruise configuration for X-57 Mod IV will demonstrate significant increases the range of electric aircraft without sacrificing safety during low-speed operations. While battery energy densities will certainly increase as battery technology advances, contemporary energy densities cannot support all-electric operation with the range routinely achievable using fossil fuels and ICE or turbine propulsors (Ref. 5).

FUELEAP addresses this limitation by proposing a hybrid fuel-cell/battery power subsystem. In particular, noting the ubiquitous availability of aviation fuels at Fixed-Base Operator (FBO) airports, FUELEAP proposed the

use of Solid-Oxide Fuel Cells (SOFC) with steam reformation to generate power from standard aviation fuel. Ref. 3 provides additional detail regarding the design of the steam-reformation/SOFC FUELEAP system.

FUELEAP team members developing the conceptual design of the power subsystem are also designing the X-57 Mod II power subsystem and are considering using it as the basis for FUELEAP. Fig.2 (from Ref. 2) shows the FUELEAP variant of the X-57 Mod II power subsystem architecture, with FUELEAP specific elements occupying the upper center of the diagram. We note here that, although Fig. 2 shows a dual stack configuration, we use the two SOFC stacks to provide sufficient power and not for redundancy: the stacks cannot be independently isolated from fuel flow; if one fails, both must be shut down.

Fig. 1 X-57 Mod IV Configuration (source NASA)

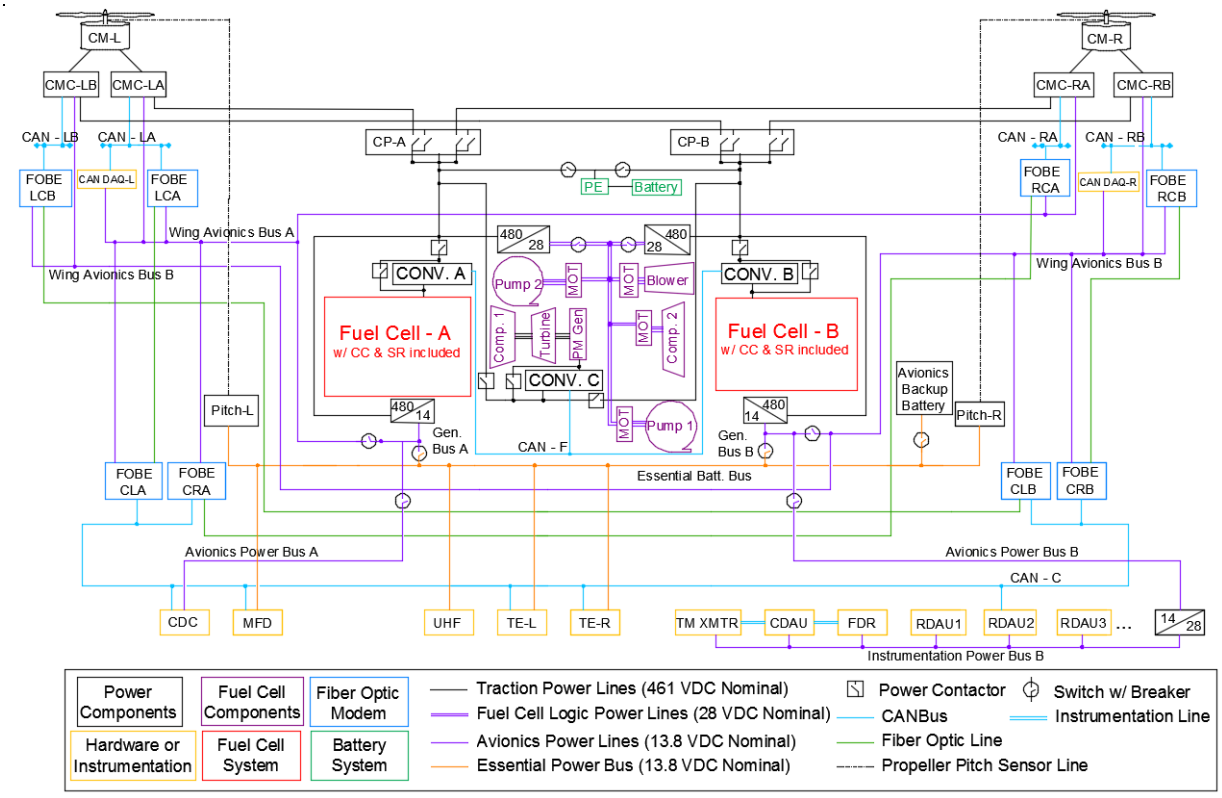

Fig. 2 Diagram of the X-57 Mod II FUELEAP Variant Power Subsystem (See Ref. 2 for nomenclature)

IV. Overview of Safety Analysis for Flight Critical Systems

Our focus for safety analysis on FUELEAP divides among four objectives. First, we seek to assure that project personnel, including ground crew and flight crew, stay as safe as reasonably possible through all aspects of the FUELEAP demonstrator. All other objectives support this overarching perspective.

Secondly, because FUELEAP is a NASA research flight experiment, it must be vetted by NASA airworthiness authorities. At NASA Langley Research Center (LaRC), this authority is the LaRC Airworthiness and Safety Review Board (ASRB), and our second objective, then, is to manage our safety analysis and products in a manner consistent with the expectations of the ASRB.

Our third objective is to provide a path towards civil certification of electric aircraft powered by a hybrid fuel-cell/battery system. With this in view, we want to align the types of safety analysis and products we are generating for FUELEAP with the analysis and evidence that would support a civil aviation certification program.

Finally, our fourth objective is to utilize local expertise at LaRC in argument-based assurance to develop a safety case for the FUELEAP project. This provides an explicit, tailored argument for FUELEAP by defining a top-level safety claim; supporting evidence we develop through our analysis of the system architecture and operational profile; and a description of how the evidence supports the top-level claim.

We provide a brief overview of each of these objectives in the balance of this section.

A. Safety Approach

FUELEAP safety analysis follows the Functional Hazard Assessment (FHA) methodology outlined in ARP 4761 (Ref. 7). As we discuss in the next two subsections, this methodology supports hazards analysis required by the LaRC ASRB; is acknowledged by legacy Part 23 guidance as an acceptable method for initiating safety assessments (Ref. 8); and is suggested as one method for performing failure condition classification in recently developed consensus standards supporting the 2017 Part 23 rule revision (Ref. 9).

Our FHA implementation first identifies a set of high-level functions provided by the aircraft. For each, we evaluate the impact of its failure (loss or malfunction) for a set of operational phases that encompass a representative flight test. Based on this we can identify where these failure conditions represent a hazard condition—defined here as an condition that, without intervention, might lead to loss in the form of damage to the aircraft, injury to the ground or flight crews, or both[7,8]. As an example, FHA analysis of the high-level aircraft function "provide thrust" looks at "loss of adequate thrust" across operational scenarios: identifying this loss as a hazard condition for takeoff but little more than a nuisance for taxiing.

With support from NASA and Boeing team members familiar with the SOFC and power subsystem design and operation, we develop an understanding of the system architecture and operational profile. We decompose the top-level functions into the system architecture to determine lower-level function failures that may contribute to the realization of a hazard conditions and component failures that may introduce additional hazard conditions. An example of the latter would be failure of the piping carrying the reformed fuel from the steam reformer to the SOFC, resulting in the release of heated and potentially toxic gases into the cabin area. A large portion of our safety approach will focus on developing a comprehensive inventory of component failure modes and their influence on hazard conditions.

Because our safety analysis is concurrent with FUELEAP system design, the FUELEAP team can incorporate design features at the architecture and component levels and (where necessary) operational constraints that reduce the likelihood or impact of hazard events. We find it valuable to think of these as falling into the two categories defined in a classic "bow-tie" diagram, such as Fig. 3 (Ref. 10). The diagram defines "barriers" as design features or operational constraints that would prevent the hazard condition (or at least reduce its likelihood) and "mitigations" as features/constraints placed to reduce the likelihood or consequence of a particular potential outcome if an adverse event occurs[9].

---

[7] Many more precise (and verbose) definitions exist in safety literature for the terms "hazard" or "hazard condition" We provide this definition as an informal working definition adequate for this discussion.

[8] The term "hazardous" is used in safety literature in a general sense, as well as a specific sense as a failure classification, such as "negligible," "minor," "major," "hazardous," and "catastrophic." The use of the term should be apparent in context.

[9] Safety literature often addresses these collectively as "mitigations." We will also use the term "mitigation" generically, but note that a mitigation can (a) reduce the likelihood of or eliminate a hazard condition, or (b) reduce the likelihood of or eliminate a particular outcome, or reduce its consequence.

Recognizing that FUELEAP system weight and volume considerations cannot support complete system redundancy, we assess the functional impact of single failures as their effect propagates through the system behavior to show that, through mitigations in the form of design features and operational constraints, no single failure[10] will result in unacceptable loss or injury. This means that mitigations are in place to address the immediate effects of a hazard (such as a firewall between the experiment pallet and the crew, and adequate cabin venting) and any associated reduction in performance will not inhibit safe landing and egress.

The process described in the previous paragraph is a largely based on qualitative analysis. Because of the lack of in-service history for a number of FUELEAP components, we are unable to use probabilistic methods to show quantitatively that the likelihood of a particular failure leading to a hazard event is sufficiently low. As an extension to our initial approach, we may be able to supplement our safety analysis with reasonably conservative estimates of component reliability data and perform Fault Tree Analysis (FTA) to look at system-level reliability. Additionally, we believe that FUELEAP SOFC testing at NASA Glenn Research Center (GRC), FUELEAP flight test data, and potential follow-on experiments and testing will provide a basis for probabilistic analysis in the future.

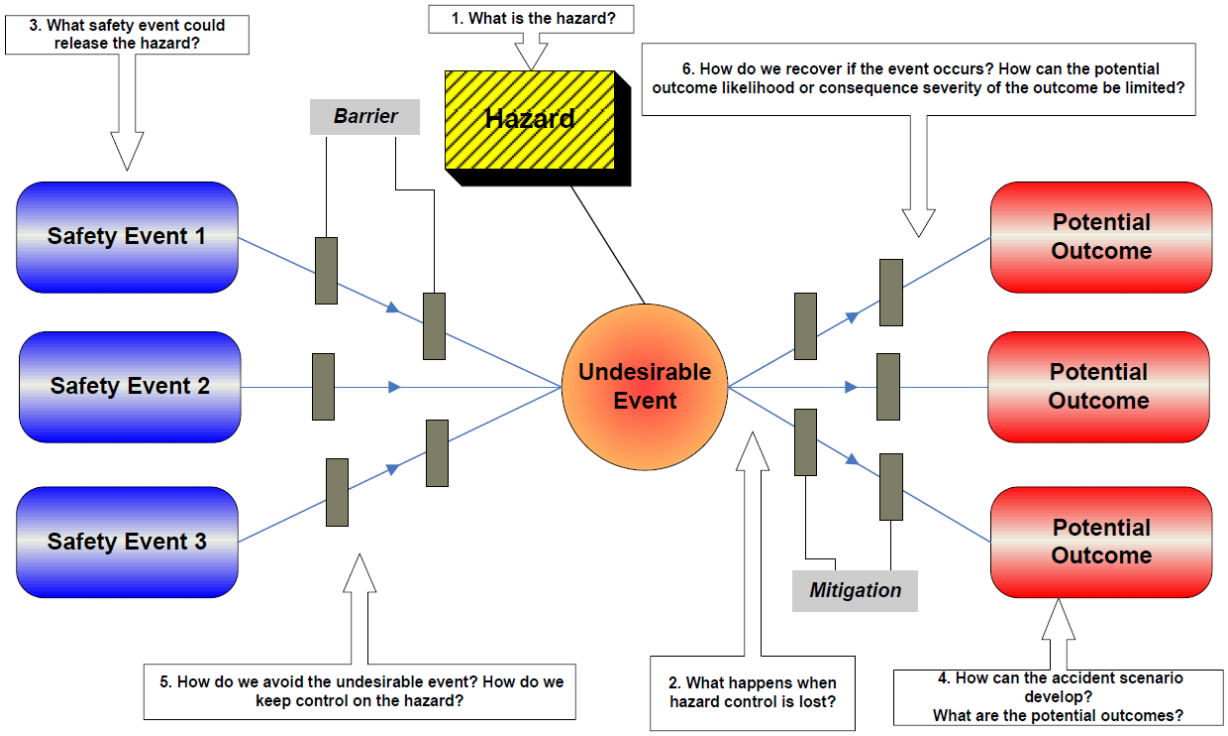

Fig. 3 Hazard "bow-tie" diagram (Ref. 10 – use unrestricted)

B. NASA Airworthiness Considerations

NASA manages agency aircraft and the safety of flight research projects at the Agency level in part through NASA Policy Directive (NPD) 7900.4 "NASA Aircraft Operations Management," (Ref. 11) and NPD 8700.1 "NASA Policy for Safety and Mission Success" (Ref. 12). For each NASA center conducting flight operations or flight research, NPR 7900.4 delegates to the Center Director the responsibility for ensuring that all flight operations, including those involving research aircraft, are conducted consistent with Agency level directives for operations and safety. As part of this, 7900.4 instructs that all flight research projects be evaluated for approval through local airworthiness and aircraft management organizations.

While specific implementations of this policy may vary center-to-center, NASA's safety culture requires that risks for a particular mission are well understood, unnecessary risks are eliminated, and necessary risks are reduced to an acceptable level. Here, risk is defined as the overlay of the likelihood of an adverse event and its consequences, with consequence viewed from two perspectives: asset damage/loss costs and crew injury/fatality. Hazard analysis

[10] We do not generally consider two concurrent, independent failures but address the possibility of common-mode failures and zonal safety considerations per safety assessment techniques defined in ARP 4761.

identifies specific adverse hazard conditions, their initiating events, and potential outcomes. For each outcome, the combination of its likelihood and consequence classify the risk level. If a risk is unacceptable, further system refinement may be necessary to reduce the likelihood of the particular outcome, its consequence, or both.

As an example of center-level implementation of the directives specified in NPD 7900.4, flight research projects at LaRC must be reviewed and approved by the LaRC Airworthiness and Safety Review Board (ASRB). Langley maintains local center procedures and forms that support the ASRB review process, including a hazard analysis and risk classification form completed by the prospective flight project for each hazard condition. Information on this form maps very closely to the hazard-related information supporting the ARP 4671 FHA process in general. However, given that NASA flight research projects often consist of new operational profiles, equipment, and aircraft modifications with little or no in-service history, hazards analysis supporting the ASRB review are often restricted to qualitative methods, and supporting evidence must be collected to justify a particular classification. Although we see the current ASBR process as thorough and effective, we intend to develop a "safety case" for FUELEAP that will supplement the ASRB review package: because much of the safety analysis is qualitative in nature, the justification for the claim that an acceptable level of safety is achieved for FUELEAP may be well documented as the structured safety case. Subsection D describes this approach in more detail.

C. FAA Certification Considerations

The Code of Federal Regulations (CFR) Title 14 Part 23 (Ref. 13) establishes Federal Aviation Administration (FAA) airworthiness regulations for normal category aircraft, such as the Tecnam P2006T. Prior to 2017, §23.1309 "Equipment, systems, and installations" provided specific regulations for system safety evidence that would be required in applying for certification of a normal category aircraft. These rules include (in part):

> (c) The airplane systems and associated components considered separately and in relation to other systems, must be designed and installed so that:
>
> (1) Each catastrophic failure condition is extremely improbable and does not result from a single failure;
>
> (2) Each hazardous failure condition is extremely remote; and
>
> (3) Each major failure condition is remote.

An extended discussion of these regulations are outside the scope of this paper, but we wish to highlight a couple points. First, safety analysis of the system design and installation much consider not just local failures (such as component-level) but also the potential for cascading failures and the potential effect of a failure on other equipage in close proximity. Secondly, it should be extremely improbable that a single failure will results in a catastrophic failure condition. Because FUELEAP is not a fully redundant system, the analog for our safety analysis is to show sufficient mitigations are in place to assure that a safe landing and egress is highly likely for every plausible single failure condition. Additionally, because we do not have reliability data on a number of system components, we must make these assertions via qualitative reasoning, as we discussed above in Subsection A.

The FAA subsequently published Advisory Circular (AC) 23.1309 (Ref. 8) to define an acceptable means for showing compliance with §23.1309. This AC provides an extended set of terms and definitions related to safety, and quantitative definitions for minor, major, hazardous, and catastrophic failure conditions. It also discusses analysis methods that comprise a System Safety Assessment (SSA), and acknowledges guidance in ARP 4754A (Ref. 6) and ARP 4761 (Ref. 7) as acceptable means for conducting the SSA.

In August of 2017, the FAA released a major revision of Part 23 in response to the Small Airplane Revitalization Act of 2013. The reformed regulation removes previous normal category (utility, aerobatic, and commuter) classifications and replaces them with four levels of performance risk, based on the aircraft's maximum seating and on maximum cruise speed. In addition, in response to the congressional mandate, the FAA greatly simplified Part 23 by removing prescriptive material and replacing it with minimum performance standards that the certification applicant must meet for compliance.

The FAA deferred definition of representative means for demonstrating compliance to the new performance-based rules to industry consensus standards, managed by ASTM. ASTM has released a few consensus standards for small aircraft development since the new Part 23 rules went into effect, such as ASTM F3230-17 "Standard Practice for Safety Assessment of Systems and Equipment in Small Aircraft" (Ref. 9). At this time, we are not aware of FAA acknowledgment of ASTM F3230 as acceptable means for demonstrating compliance with what is now §23.2510 "Equipment, systems, and installations." However, F3230-17 addresses many of the same topics as AC 23.1309. It also suggests the FHA process from ARP 4761 as a viable approach for classifying failure conditions (§4.1) and the ARP 4761 SSA process as a means for conducting a safety assessment for hazardous and catastrophic failure conditions (§4.2.4).

We should note, in comparison to AC 23.1309, ASTM F3230-17 provides additional latitude for systems and installations that are simple and conventional, or similar to previous design. For instance, qualitative analysis alone is satisfactory for analyzing hazardous and catastrophic failure conditions in systems that are both simple and conventional. We cannot make this blanket claim for FUELEAP; however, we can (judiciously) point to favorable service histories for components of similar designs operating in similar environments, and reference X-57 Mod II power subsystem flight service history in assessing the FUELEAP variant of the same architecture.

D. Safety Case

The FUELEAP project faces unique challenges in safety assurance, including novelty and the need to address both short-term and long-term safety concerns. To address these, we are producing a safety case that comprises both evidence of safety—including MBSA results—and a structured *safety argument* recorded in a combination of prose text and *Goal Structuring Notation* (GSN) figures (Ref. 15). Fig. 4 presents as an example an excerpt from the highest level of the FUELEAP Flight Demonstrator (FD) safety argument.

The novelty of both the hybrid electric power and propulsion system and MBSA complicates understanding of the aircraft's design and safety evidence by depriving readers of a familiar story frame into which to fit the aircraft's particulars. Aviation specialists will already share some understanding of the safety and functional implications and tradeoffs surrounding traditional aviation fuels and ICEs. But many FUELEAP stakeholders—systems engineers, electrical and avionics engineers, pilots, safety specialists, and regulators—will be unfamiliar with both the safety and operational concerns surrounding hybrid electric propulsion and the relative merits of means of addressing these. Such stakeholders might benefit from a guide to how power system design fit into in the 'big picture' of aircraft safety. One way the safety argument augments our modeling and safety assessment activities is by explaining that story to readers.

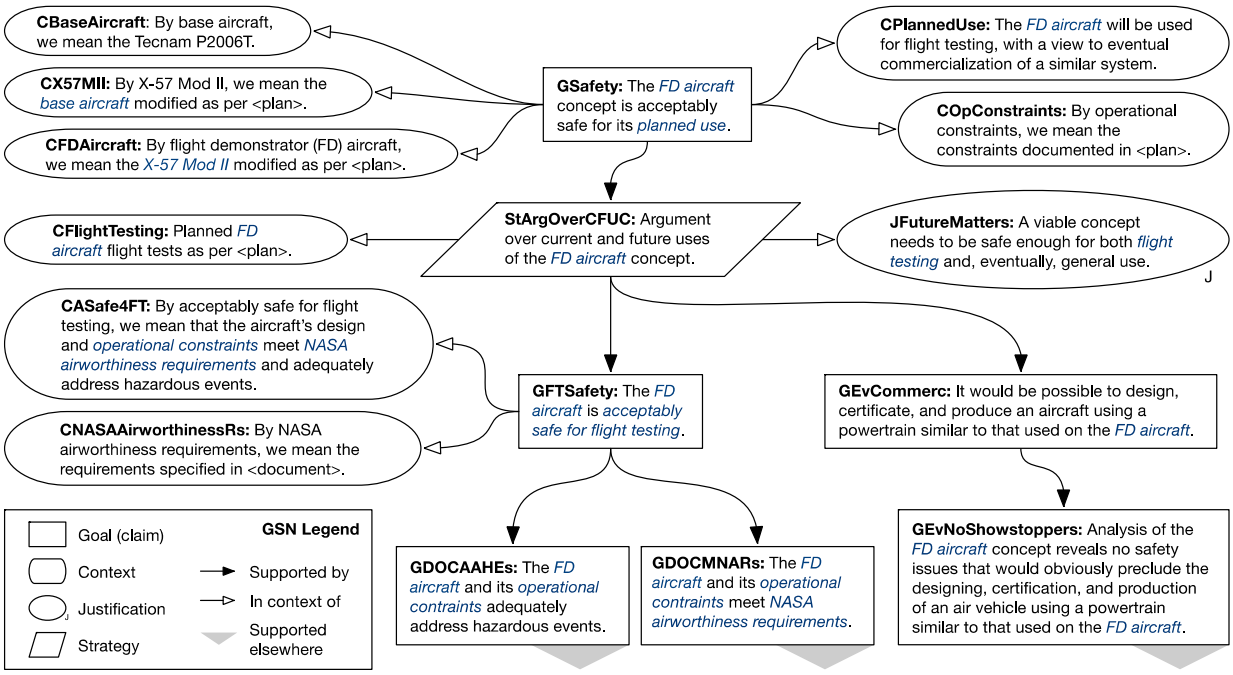

Fig. 4 The top-level of the FUELEAP safety argument in the Goal Structuring Notation (Ref 15)

When means of addressing aircraft hazards or assessing aircraft safety are familiar, it may not be necessary to explain these to readers beyond, perhaps, referencing applicable standards. Safety-related standards and regulations often serve to define best practice, capturing judgments about which hazards require mitigation and sometimes what mitigations are advisable and how they should be assessed. But these judgments might not be universally applicable. For example, 14CFR §23.2430.a.2 requires that aircraft fuel systems be "designed and arranged to prevent ignition of the fuel within the system by direct lightning strikes … or by corona or streamering at fuel vent outlets," thus implicitly presuming both a liquid fossil fuel energy source and an attendant fire hazard. But it makes no mention of the hazards introduced by the use of a battery pack of the construction and capacity required by a hybrid power

system. By capturing the hazards that FUELEAP's project team envision and relating these hazards to mitigations, the safety argument records the team's contention as to which unique hazards require mitigation and what means of mitigation should be considered sufficient. The argument will thus serve as the starting point for discussing these matters with relevant regulators, including the NASA ASRB.

FUELEAP's nature as a demonstrator project also poses challenges such as assessing the adequacy of operational constraints and tracking different short-term and long-term safety aims. The project's goal is to assess the viability of the hybrid power system concept, not to develop an aircraft type that can be put into production. The power system concept is not viable if it will not be possible to (with further development) implement a sufficiently safe production version. Yet an aircraft built to assess a novel concept must, by nature, fly in order to accumulate the very experience that will provide a sound basis for assessing the reliability and other safety properties of the concept in question. Thus, adequate safety in flight test operations might be best achieved with a different set of mitigations than might be prudent in a production aircraft. For example, flight test operations might be conducted solely from runways long enough to permit landing straight ahead should the power system fail during takeoff. These considerations yield the safety aims embodied in the claims shown at the bottom of Fig. 9. In the argument supporting GDOCAAHEs—not shown here—we trace hazards in the flight demonstrator aircraft to their mitigations and the related evidence to allow readers to understand how we have addressed the safety of flight test operations and to judge whether we have done so as well as reasonably practicable. At the same time, we must meet existing regulations for flight test. In the argument supporting GDOCMNARs, we trace NASA airworthiness requirements to evidence of their satisfaction. Finally, in the argument supporting GEvNoShowstoppers, we explore what the experience of designing the FUELEAP aircraft portends for future efforts' ability to engineer a sufficiently safe production aircraft using a similar concept.

V. MBSA on FUELEAP

Section IV provided an overview of our FUELEAP safety analysis, which we have structured to support compliance with NASA airworthiness requirements, and an eye towards civil aviation certification of hybrid electric aircraft. This section provides an overview of progress we have made to date in implementing safety analysis described in Subsection IV.A as a Model-Based Safety Analysis (MBSA) implementation.

A. Aircraft Functions

Our MBSA approach begins with capturing a SysML representation of the aircraft system functions to support the top-level Functional Hazards Assessment (FHA). Examples and illustrations in ARP 4754A and ARP 4761 provide insight into how the SAE SA-18 Working Group viewed the aircraft functional decomposition. Additionally, we found helpful the decomposition approach provided by Romli (Ref. 14).

Our SysML decomposition models starts by defining a function block stereotype as a refinement of a general SysML block stereotype. We used this stereotype to define an aircraft function superclass and three subclasses covering ground, flight, and crew operations, and created our inventory of top-level aircraft functions as instances of these subclasses. Fig. 5 shows the resulting set of 13 aircraft functions. Note that the "provide thrust" function is necessary for ground and flight operations and so it is typed by both subclasses.

From these 13 functions, we show in Fig. 5 those we anticipate as being "touched" by the FUELEAP integration. For instance, "provide situation awareness" requires that the crew is cognizant of the status of the FUELEAP equipment pallet so that they could initiate contingency operations as necessary. Functions shaded green in Fig. 5 likely require safety focus, whereas tan functions are provided by the stock Tecnam aircraft or X-57 Mod-II modifications and are likely to require little safety analysis specific to FUELEAP.

We note that FUELEAP considerations for some "green" functions can probably be dispatched with relative ease. For instance, "provide aerodynamic stability" requires only that we comply with Tecnam specifications for total weight and center of gravity (CG) location, as we are not modifying any control surfaces or linkages and the aerodynamic configuration of the Tecnam is essentially unchanged[11]. Conversely, "provide habitable crew environment" and "provide thrust" will occupy much of our functional hazard analysis, as the SOFC/battery pallet mounts in the aircraft cabin behind the crew and it generates power for thrust.

Finally, we note that downstream safety analysis such as a zonal safety analysis will trace to these top-level functions as well. For instance, we will consider the proximity of empennage control linkage to the experiment pallet to evaluate the potential loss of aerodynamic control in explosion or fire-related failure scenario.

[11] Per Ref. 3, we plan to incorporate a small ram-air inlet to assist in cooling the recycle flow.

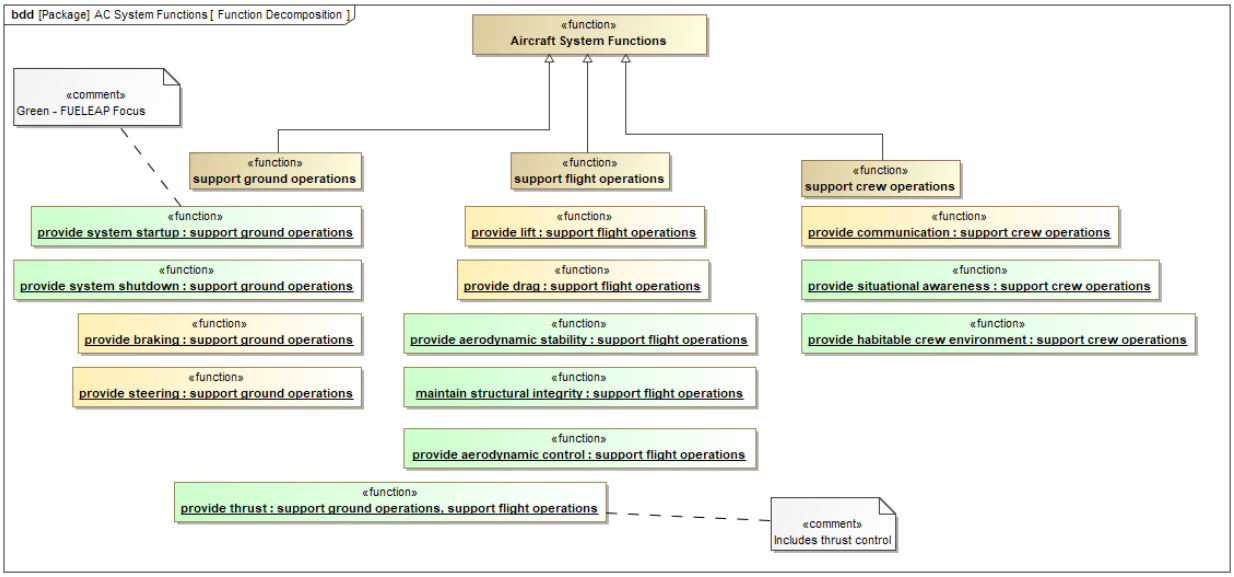

Fig. 5 Top-level Aircraft Function Decomposition Block Definition Diagram

B. Hazard Meta-Model

Fig. 6 defines the SysML hazard meta-model we defined for use in our FHA, which includes "parts" representative of the type of information required by the ASRB hazard form. The "Aircraft System Functions" block, shown in Fig. 5, provides access to the 13 aircraft function instances. We define all other hazard parts using integer, text, or enumerated value types and we use multiplicity relationships ("1..*" read as "one or more…") for aircraft functions, operational phases, verification, and mitigation properties.

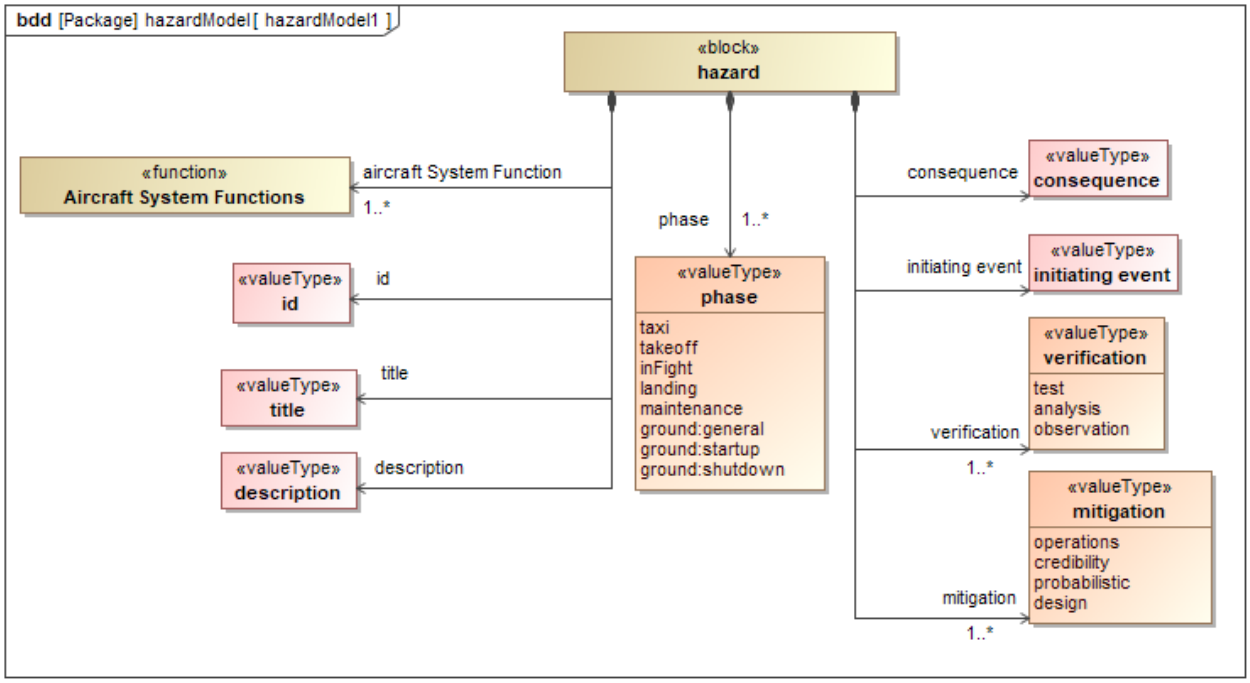

Fig. 6 Hazard Meta-Model Block Definition Diagram

C. Hazard Identification

Using instances of the hazard meta-model defined in Fig. 6, we performed an aircraft-level FHA across the functions defined in Fig. 5. Our initial analysis includes “loss of” and “malfunction” for aircraft functions as well as high-level hazard conditions potentially introduced by the FUELEAP architecture. Although Boeing and NASA teammates continue to refine the FUELEAP architecture, the only practical location, from weight and balance as well as volumetric considerations, for the SOFC/hybrid system is within the cabin. As such, we include potential hazard conditions introduced by the SOFC, supporting turbomachinery and other assemblies, and battery that may affect the “provide habitable crew environment” aircraft function.

Fig. 7 is a SysML package diagram showing the 11 hazards we identified against the top-level aircraft functions. By exposing the hazard block “slot” properties, we can view all of the hazard information in this diagram. Alternatively, by using a non-graphical SysML instance table we have more flexibility in filtering and tailoring the hazard data, as well as exporting the table data to external tools such as Microsoft Excel. For example, Fig. 8 shows a SysML instance table of hazards we map to “support ground operations” aircraft function classes, and Fig. 9 shows a matrix of hazards mapped to operational phases generated in Microsoft Excel directly from the SysML instance table export data.

Looking at Fig. 9, note that we consider only hazard 6 to be present across all operational phases, assuming the battery stores dangerous levels of energy even if the system is in shutdown. Otherwise, most functional failure conditions become a hazard condition only in a subset of operational phases, with almost all of them resulting in hazard conditions during critical flight operations (take-off, flight, and landing). This view of hazards mapped to operational phases provides a means for discussing phase-specific consequences and specific mitigations strategies.

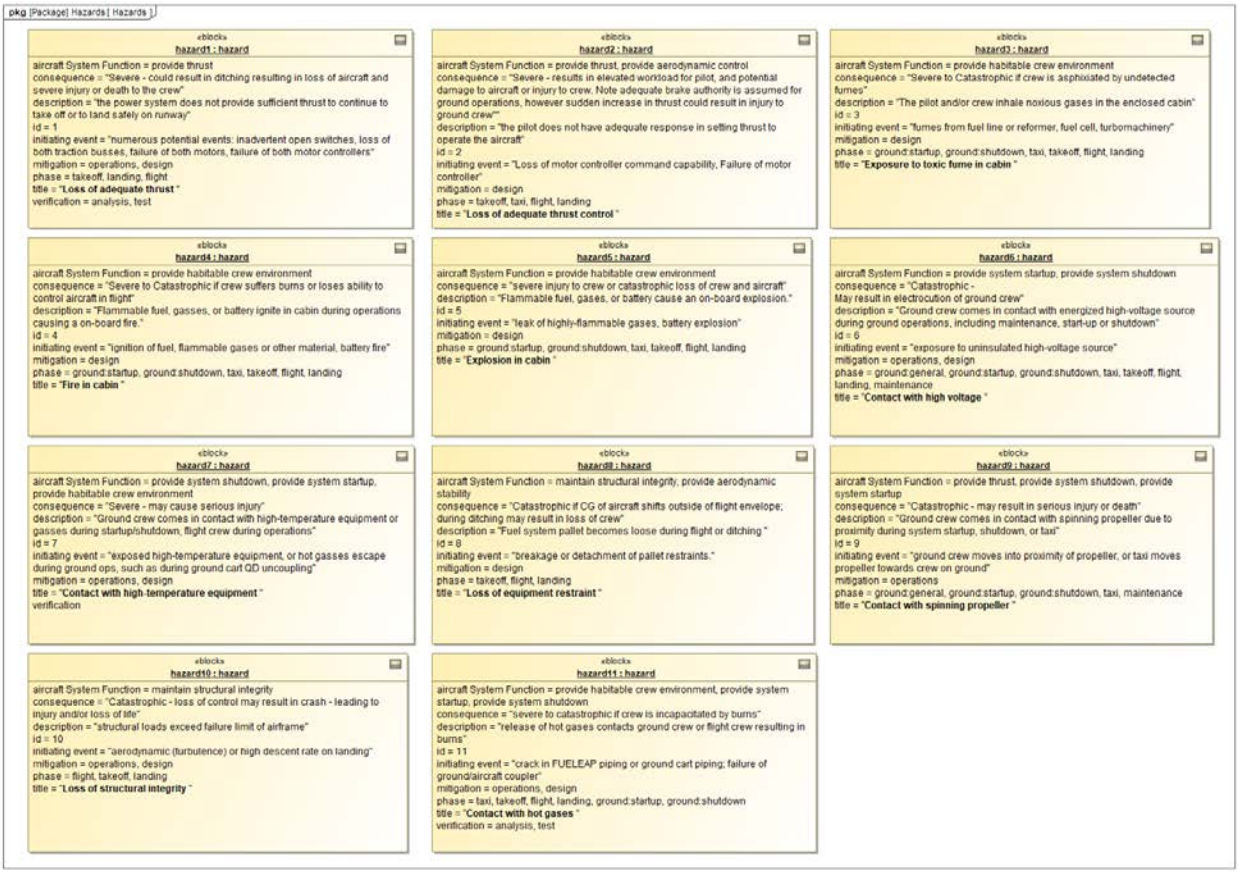

Fig. 7 Top-Level FUELEAP Hazards Package Diagram

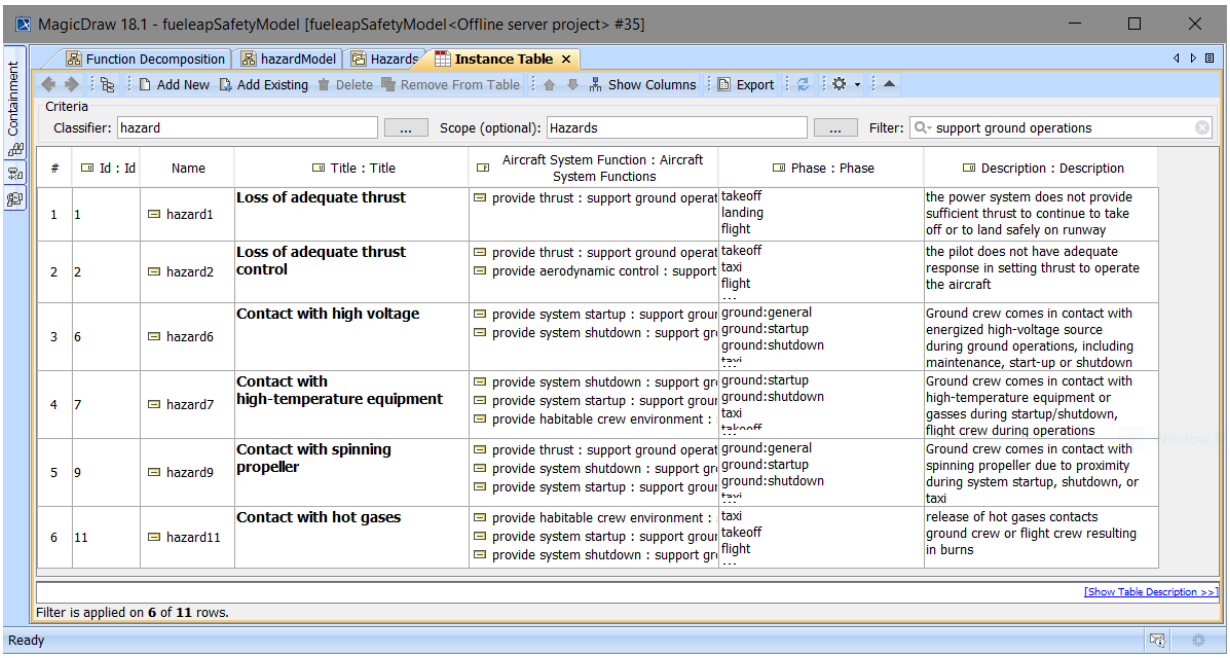

Fig. 8 Hazard Instance Table (filter applied)

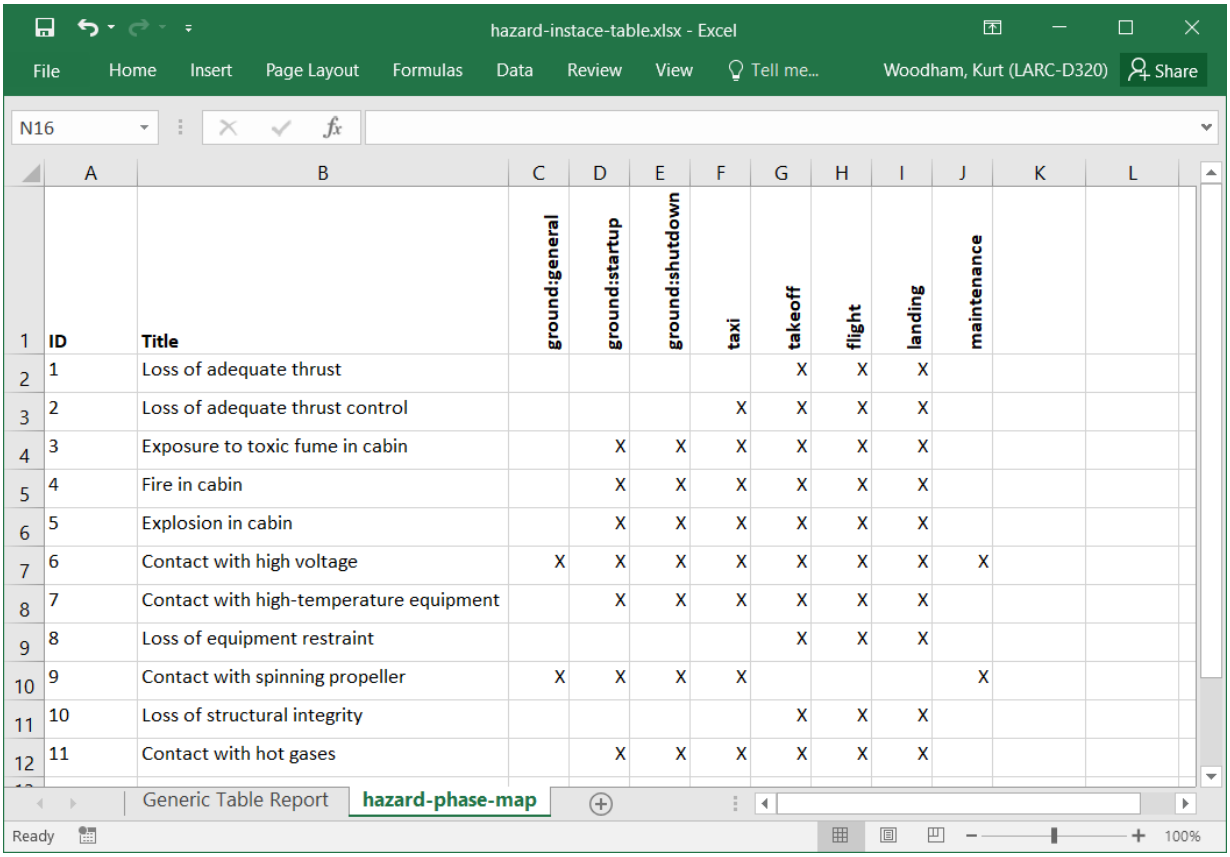

Fig. 9 Hazards mapped to Operational Phase (From SysML Instance Table Export Data)

D. Initiating Events

The bow-tie diagram of Fig. 3 shows that a hazard condition results from one or more initiating events ("safety event" in Fig. 3). If an initiating event can be eliminated or made suitably unlikely (through operational restrictions, design features, increased part reliability, etc.), or its contribution to a hazard condition eliminated, then the hazard condition may be effectively controlled (see "barriers" in Fig. 3).

While we have provided high-level descriptions of the types of initiating events for each hazard condition (shown in Fig. 6), we intend to develop a list of specific initiating events through systematic analysis of the FUELEAP system. This is in the form of a component-level Failure Modes and Effects Analysis (FMEA), which inventories all relevant system components and their specific failure modes, and analyze the way that these failures might trigger a hazard condition, either directly or through propagation.

In order to support this systematic analysis, we are developing SysML models of FUELEAP, focusing on the FUELEAP power subsystem. For analysis purposes, we have partitioned it into (a) SOFC/battery power generation and (b) distribution of power. (See Ref. 1 for additional details.) Referring to Fig. 2, the former portion contains the SOFC stacks, pumps, turbine, battery, battery power electronics, 28V Fuel Cell Logic Power, and 460V output, and the latter consists of converters and traction (460V), avionics (14V), and essential (14V) power buses. The 460V traction bus, then, provides the interface between these analysis partitions. The advantage of this partition is that the SOFC/battery portion includes physical "flows" in addition to the electrical power, and the outer focuses exclusively on electrical power conversion and distribution. (Note that "digital" control and monitoring "flows" will eventually overlay both partitions).

To represent the flows involved in the transformation from liquid aviation fuel to exhaust gases, we first defined SysML flow specifications for each physical flow and used these to type ports for each component block model. (Note that these blocks are only abstract representations and that we are not modeling physical/thermal/chemical reactions.) Next, we defined the interconnections between components through a SysML Internal Block Diagram (IBD) (Fig. 10). Note that Fig. 10 shows an older configuration of the system and does not reflect recent refinements described by Boeing in Ref. 3.

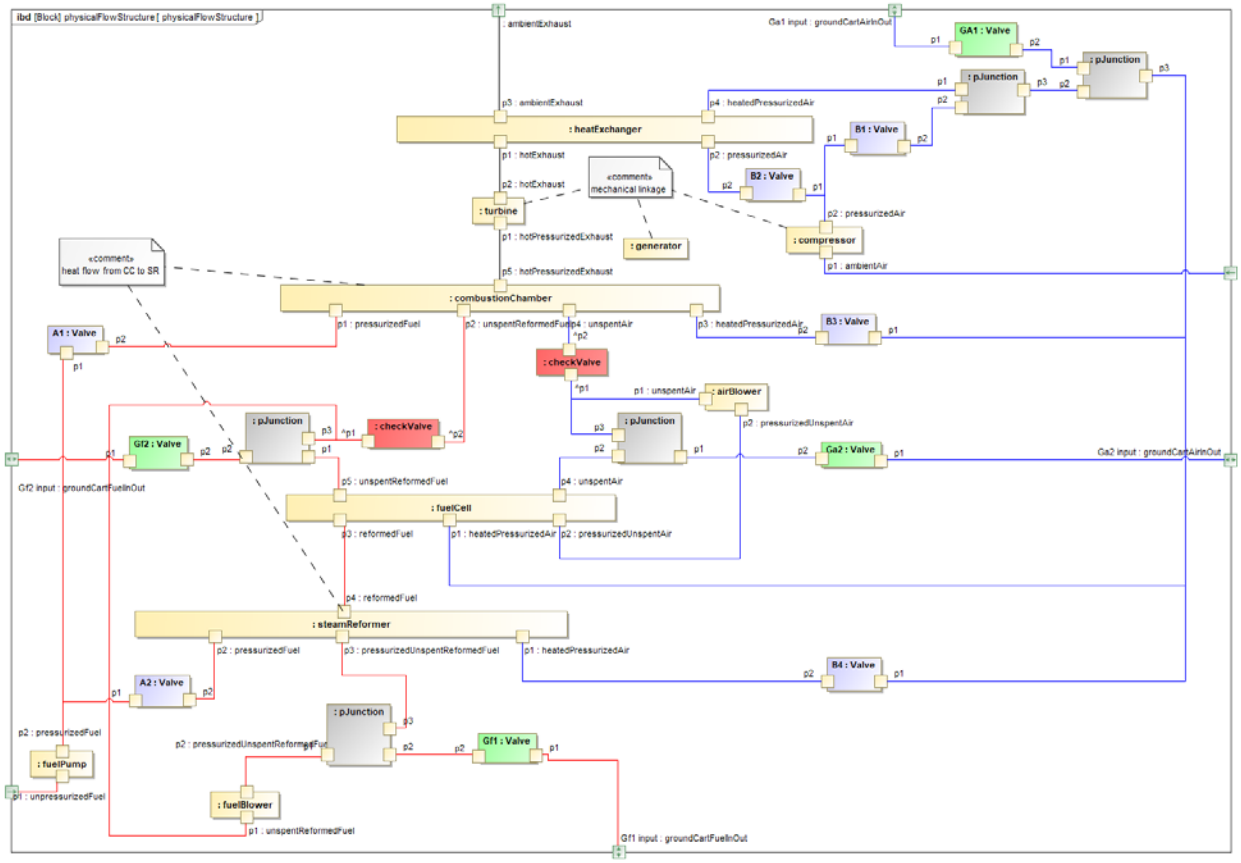

Fig. 10 SOFC Physical Flow Internal Block Diagram

The physical boundary ports shown in Fig. 10 include the interfaces between the FUELEAP on-board system and the start-up ground cart along with the fuel intake from the aircraft fuel tanks and the eventual exhaust of the exhaust gases. Using SysML use case and activity diagrams, we have captured Boeing's description of a representative start up procedure for startup, which include the configuration of the interface ports defined in Fig. 10. As Boeing refines the ground card interfaces and the startup procedure, we will refine the SysML representation and identify potential failure modes and effects that may be associated with components such as ground cart controls, valves, and interface couplers.

In addition to physical flow properties, we have also defined electrical flows through the SOFC/hybrid system and have modeled the electrical flows from the energy sources to the 460V traction bus. Fig. 11 shows the IBD of this model. Note that we have included the relevant portion of the power subsystem diagram (Fig. 2) in the lower-left corner.

While we represent the "nominal" flow for the Fig. 11 IBD as left-to-right, we do not model the block associations with directionality unless it is clear that the flow direction is constrained. Current will flow in the direction of a voltage drop, so we model flows as bidirectional and evaluate each interconnection accordingly. In some instances, this bidirectional flow is intentional, as is the case for the battery discharging and charging through through the battery power electronics. In other cases, we may identify flow paths that are unintentional and will then assess the need for current backflow protection. Note that this same comment applies to the physical flows in Fig. 10, where we look for the presence of backflows cause by unintended pressure differentials and assess the need for protection such as check-valves.

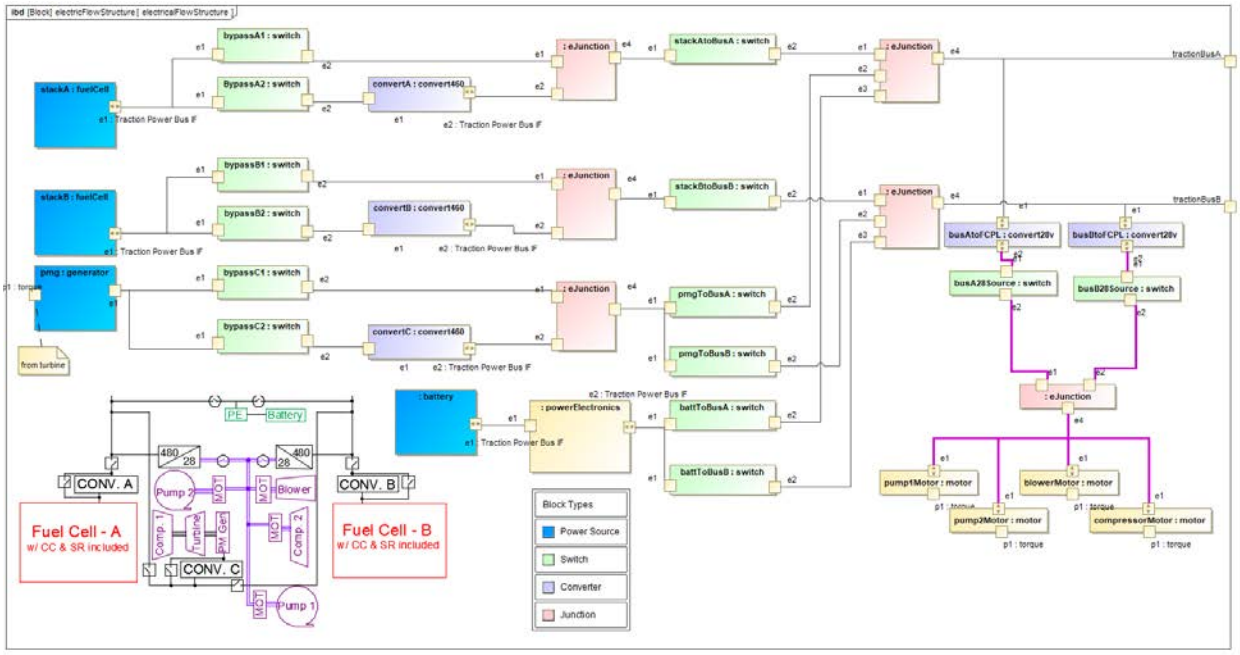

Fig. 11 SOFC Electrical Flow Internal Block Diagram

E. Mitigations

As described above, we have developed models of physical and electrical flows and will in near-term focus on modeling monitor/control flow as well. As with the initial analysis of the startup process we outline in Subsection D, we will use SysML behavior diagrams (such as activity, sequence and state) to model the dynamic state of the system for nominal and failure conditions. This provides us with a way to describe how the system might get into a hazard condition through a sequence of behaviors, and (with monitoring flows in place) precursors that might be available to anticipate a hazard condition.

Similarly, we can use characteristics of a component or system monitors to mitigate a particular hazard condition. A key feature of SysML is that a model is a collection of blocks, features, and associations that exist independently from a given model view (diagram). The modeler can choose the attributes of a block to expose within a particular diagram. As such, we can define failure and monitor properties for a block and the properties are

then available for use in any relevant SysML diagram; providing insight into not only the development of a hazard condition but its mitigation as well.

Additionally, if mitigation properties are dependent on certain environmental conditions, we can track these conditions as "liens" against the system operational profile. For instance, as discussed in Ref. 3, Boeing expressed concern regarding the reliability of the foil bearing in a hot-recycle blower, noting that the anticipated operating range extended to around 900C. By including an intermediate cooler aided by a ram air intake, Boeing anticipates that the recycle blower will operate in the 150-200C range, where there is significant service history for similar foil bearing applications. As part of our system modeling, we might define, for example, a safety constraint that the operation range of the "warm" recycle blower does not extend beyond 200C.

F. MBSA Summary

Subsections A through E describe our accomplishments to date for implementing an MBSA approach on FUELEAP. Our approach is to develop and maintain these models as part of an overarching MBSE structure, rather than developing traditional "safety models" in isolation from those used by systems engineers. Again, we emphasize here that the SysML models used for our safety analysis contain abstractions of the FUELEAP system and its components: we do not model the underlying physics, chemistry, or electrical circuitry. Instead we use abstractions of these phenomenon to describe the nominal system, how it might fail, how these failures contribute to hazard conditions, and how these failure incidences might mitigated. We then look to other analysis conducted by FUELEAP team members for confirmation that our assumptions and abstractions are consistent with their domain-specific analyses. Our overarching intent for MBSA is, then to have a "top-down" FHA perspective coupled with a "bottom-up" FMEA analysis, which looks at failures of components or low-level functions and how these relate to the hazard conditions captured by the FHA. We have hurdles to address (described in Section VI), but are confident that our MBSA approach will continue to be a valuable tool for assuring that FUELEAP is developed and operated safely.

VI. Conclusion

In this paper, we provided an overview of the MBSA approach we are taking for safety analysis of the FUELEAP system. We have structured this as an extension of the overarching MBSE effort, described in Ref. 1. Our approach is continuing to evolve, particularly as we seek to tie top-level FHA results down to lower-level aspects of the system by tracing between FHA and FMEA results. Although we see some hurdles, we do not see any of these as impediments to a viable approach. Rather, we see strong benefit in modeling system aspects relative to safety, such as hazard conditions, component failures, mitigations, operational restrictions, and environmental considerations, and capturing a defensible safety narrative to support NASA and eventually civil airworthiness considerations. We also see much value in developing a safety case to provide an explicit argument for safety. This is particularly relevant to airworthiness considerations for unique "one-off" NASA flight experiments or emerging civil aviation designs that use new technologies with little in-service history.

Our near-term plans for FUELEAP include investigating how to included additional modeling features to help enhance the safety analysis. We are investigating how to represent component failure semantics and propagate then through the system flows. We have identified some promising techniques but are concerned that some may require a significant departure from our current modeling approach through, for example, the required use of very specialized stereotypes.

Similarly, we are considering options for how to define failure semantics for interconnections (or "lines of flows"), recognizing that these associations are more than "virtual" connections but are often representations of physical system elements. For instance, associations in the physical flow IBD (Fig. 10) exist in the physical system as pipes, and block ports as pipe connections. Although FUELEAP pressures are relatively low, we must account for pipe failure conditions such as cracking/bursting to perform a thorough review of failure modes that could lead to hazard conditions. Currently we are not aware of a capability for assigning physical properties to these associations other than to create a "pipe" block and insert instances between component blocks. Similar issues exist for electrical flows, which exist as wires or power buses in the physical system and which have physical failure properties (arcing, grounding, etc.).

While much of the FUELEAP safety analysis is well served by the approach describe in Section V, we intend to extent our approach, as we have resources, to address additional MBSA features. For instance, given that our FHA approach produces results relevant to what ASTM guidance acknowledges as a viable means for performing the assessment and to what the ASRB requires for airworthiness review input, we intend to look at the template scripting capability within MagicDraw to auto-generate safety-related artifacts.

Finally, we see much value in defining an approach for interfacing between the SysML safety model and other high-fidelity tools that support safety-related analyses. NASA FUELEAP team members that are supporting safety modeling and analysis are also conducting parallel research in tool interoperability and data standards. We hope to leverage this research to benefit FUELEAP.

References

[1] Gough, K. and Phojanamongkolkij, N., "Employing Model-Based Systems Engineering (MBSE) on a NASA Aeronautic Research Project: A Case Study," *2018 AIAA Aviation Forum*, June 25-29, 2018, Atlanta, GA (to be published).

[2] Papathakis K., Shnarr, O., Lavelle, T., Borer N., Stoia, T., and Atreya S., "Integration Concept for a Hybrid-Electric Solid-Oxide Fuel Cell Power System into the X-57 'Maxwell'," *2018 AIAA Aviation Forum*, June 25-29, 2018, Atlanta, GA (to be published).

[3] Stoia, T., Balan, C., Atreya, S., Mata, M., and O'Neil P., "Solid Oxide Fuel Cell – Steam Reformation Power System Configuration Options for an All-Electric Commuter Airplane Flight Demonstrator," *2018 AIAA Aviation Forum*, June 25-29, 2018, Atlanta, GA (to be published).

[4] Goldsby, J., et al, "Evaluation studies of a 1 kW solid oxide-based fuel cells stack for electrical power in aviation," *2018 AIAA Aviation Forum*, June 25-29, 2018, Atlanta, GA (to be published).

[5] Borer, N. et al, "Performance and Design of Candidate FUELEAP Flight Demonstrator Concepts," *2018 AIAA Aviation Forum*, June 25-29, 2018, Atlanta, GA (to be published).

[6] Society of Automotive Engineers. "Aerospace Recommended Practice (ARP) 4754A, Guidelines for Development of Civil Aircraft and Systems," Dec. 2010.

[7] Society of Automotive Engineers. "Aerospace Recommended Practice (ARP) 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," Dec. 1996.

[8] FAA, Advisory Circular (AC). 23.1309-1E "System Safety Analysis and Assessment for Part 23," Nov. 2011. https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/1019681 [retrieved 30 April 2018]

[9] ASTM F3230-17, "Standard Practice for Safety Assessment of Systems and Equipment in Small Aircraft," Aug. 2017.

[10] European Commercial Aviation Safety Team (ECAST) European Strategic Safety Initiative (ESSI), "Guidance on Hazards Identification," Mar. 2009.

[11] NASA: NASA Policy Directive (NPD) 7900.4D "*NASA Aircraft Operations Management*," Mar. 2015, https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=7900&s=4D [retrieved 30 April 2018]

[12] NASA: NASA Policy Directive (NPD) 7900.4D "*NASA Policy for Safety and Mission Success*," Revalidated Dec. 2013, https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=8700&s=1E [retrieved 30 April 2018]

[13] FAA, "Code of Federal Regulations (CFR) Title 14 Part 23 Airworthiness Standards: Normal Category Airplanes," Revised 2017. https://www.ecfr.gov [retrieved 30 April 2018].

[14] F. I. Romli, "Functional Analysis for Conceptual Aircraft Design," *Journal of Advanced Management Science*, Vol. 1, No. 4, pp. 349-353, 2013.

[15] Attwood, K. et al., *GSN Community Standard Version 1*, Origin Consulting Ltd., York, UK, 2011.