Towards Computational Functional Hazard Assessment (CFHA): A Gap Analysis and Concept for Emerging Aviation Systems

Seydou Mbaye*, Daniel Hulse†, Lukman Irshad‡, Hannah S. Walsh§, Sequoia R. Andrade¶
Intelligent Systems Division, NASA Ames Research Center, Moffett Field, CA, 94035, USA

Given the current evolution of the National Airspace and future trajectory towards novel and evolving operations with varying levels of autonomy, complexity, and acceptable risk, there is an opportunity to support safety assurance by extending existing methodologies, such as Functional Hazard Assessment (FHA). In response to challenges in performing FHA for novel aviation concepts, we propose a concept for Computational Functional Hazard Assessment (CFHA), which provides processes, methods, and tools for incorporating external data to facilitate further exploration of the hazard space iteratively throughout the design process. The core components of CFHA involve knowledge capture from historical and operational data, functional architecture specification via a formal modeling language, and simulation for hazardous scenario analysis. Through this concept, we aim to adapt conventional safety assessment to address the increasingly complex hazard space generated from emerging operations.

I. Introduction

The National Airspace System (NAS) has begun to undergo major changes that will accelerate in the near future due to the introduction of new vehicles, novel operational concepts, and the entry of autonomous and semi-autonomous systems. Specific transformations include intra-urban operations through Urban Air Mobility and inter-urban operations through Regional Air Mobility [1]. In addition, there have been proposed specialized operations for Unmanned Aerial Systems (UAS) that improve logistics delivery and emergency response [2]. These emerging concepts involve increasing levels of autonomy, resulting in an increasingly complex system of systems with novel human-machine and machine-machine collaborative interaction paradigms. These anticipated changes in complexity and levels of autonomy are expected to require advancements in present-day safety assurance approaches [3]. Safety assurance plays a vital role in ensuring that systems perform as expected, satisfy all requirements, and operate safely [3]. Today, safety assurance occurs in separate stages for design and operations in aviation (e.g., 14 CFR Part 25 and 14 Part 91 for aircraft design and operations). However, this approach is at odds with emerging aviation concepts with increasing levels of autonomy, where a given concept's safety (e.g., use of an machine learning-enabled component) may be tied to a particular type of operations (e.g., approved flights, environments, etc.). Thus, assuring these technologies will require a more integrated approach to assurance that considers the interaction between the system(s) and their environment (e.g., weather conditions, airspace, etc.) [4, 5].

Safety assurance in civil aviation involves a variety of procedures and methods specified in ARP 4754B [6] and ARP 4761A [7]. ARP 4761A provides guidance for conducting civil aviation safety assessment [8] using Functional Hazard Assessment (FHA) [9], Preliminary System Safety Assessment (PSSA) [10], and System Safety Assessment (SSA) [11], as shown in Figure 1. Functional Hazard Assessment (FHA) is conducted at both the aircraft level and system level early in the assurance process to understand potential hazards and the safety criticality with the goal of informing safety requirements. FHA is primarily an expert driven process where system functions, applicable phases of operations, failure conditions, propagation effects, and mitigations are identified and listed in a table [12, 13]. FHA is one of the first safety assessments performed in the assurance process, first at an aircraft level and then at a system level which then forms the basis for more detailed safety assessments such as Preliminary Aircraft Safety Assessment (PASA) and PSSA. FHAs are revisited and updated when new information about the system becomes available and changes are required to the underlying system architecture. The results of the FHA process serve three major functions. First, they are used to

*Researcher, NASA Ames Research Center, AIAA Member, seydou.mbaye@nasa.gov.

†Software Systems AST, NASA Ames Research Center, daniel.e.hulse@nasa.gov.

‡Research Engineer, KBR, Inc., AIAA Member, lukman.irshad@nasa.gov, funded Under Prime Contract No. 80ARC020D0010 with the NASA Ames Research Center.

§Computer Engineer, NASA Ames Research Center, hannah.s.walsh@nasa.gov.

¶Research Engineer, HX5 LLC., AIAA Member, sequoia.r.andrade@nasa.gov, funded Under Prime Contract No. 80ARC020D0010 with the NASA Ames Research Center.

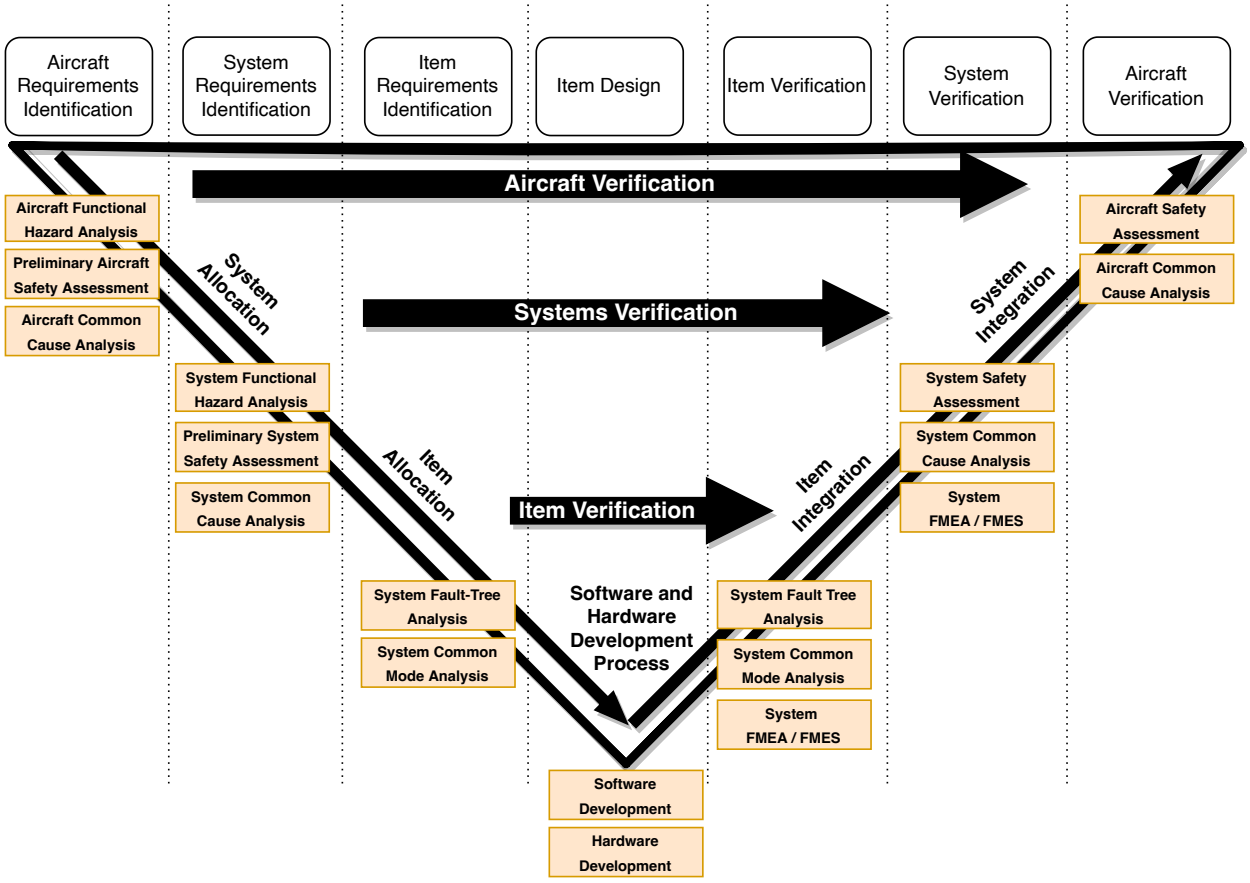

Fig. 1 Systems Engineering V-Model. Functional Hazard Assessment occurs in early design stage, towards the upper left of the V-Model. Aircraft FHA is performed alongside Preliminary Aircraft Safety Assessment (PASA) and System FHA is performed alongside Preliminary System Safety Assessment (PSSA), per ARP 4761A.
Adapted from [15].

identify high-level functional, safety, and performance requirements required to mitigate the identified hazards. Second, the identified hazards act as the top level hazards that are further assessed in downstream safety assessments. Third, the failure classifications form the basis for determining the safety criticality of functions during the PASA and PSSA process, which in turn informs the required rigor for the validation and verification activities. In other words, a poorly performed FHA can lead to the wrong requirements being specified, leading to poor safety even when the system is rigorously tested, verified, and validated. Thus, a well performed FHA is important to ensure that the system will be certified against the right requirements.

While the conventional FHA approach is considered adequate for assuring the safety of conventional aircraft, the emergence of novel aviation concepts with increasing levels of autonomy present challenges to this process. With novel aviation concepts that have increasing levels of autonomy, the responsibility of operating the system is partially or fully allocated to technical systems [14]. Thus, traditionally operator-driven functions and tasks such as hazard detection and contingency management may now be shared between technical systems and operators or fully assigned to technical systems [14]. As a result, what may be considered operational safety conventionally may no longer be restricted to operational assurance, but become a consideration for design assurance [14]. The conventional FHA process needs to be adapted to accommodate this shift in paradigm, so high level hazards and safety requirements are captured accurately.

There have been promising developments in the literature which may be able to address the above challenges if they were made a part of the FHA process. In this paper, we first (in Section II) identify challenges in performing FHA for novel aviation concepts with increasing levels of autonomy, next (in Section III) we explore these hazard analysis approaches (both in academic literature and practice), and then (in Section IV) identify the opportunities they present to the FHA process for the analysis of new and emerging airspace concepts. Given these opportunities, we further (in

Section V) propose a process and paradigm for using these hazard analysis processes called Computational Functional Hazard Assessment (CFHA) which leverages recent contributions in the hazard analysis literature in a computational environment to extend the analyst's ability to analyze hazards. In Section VI, we summarize the findings, highlight limitations, and make recommendations for future work.

II. Functional Hazard Assessment for Novel Aviation Concepts: Barriers and Considerations

The consideration of operational safety during design (as discussed in the previous section) has two major implications for FHA. First, the operational considerations for FHA should be broader than what is considered conventionally. In addition to the conventional considerations (i.e., operational phases, environment, crew, etc.), FHA should account for hazards that originate from disturbances and volatility (when no failures are present), interactions between different system elements (e.g., hardware-human, software-human, hardware-software, etc.), and interactions of the system with its operational environment and conditions, including interactions with external systems [16–18]. Adding these additional considerations in the hazard assessment process can result in a large, potentially complex hazard space [19]. Adding further to the complexity, such information about the operations, including the environment, and resulting interactions may not be available during early design stages [16, 20]. Simply put, the FHA process for novel aviation concepts with increasing autonomy should accommodate the large, potentially complex hazard space that may evolve as more details about the system and its operation environment and conditions emerge.

The second implication of including operational considerations in the FHA process is that the FHA process should help designers define the high level requirements on systems resilience. Resilience is the "ability of an architecture to support the functions necessary for mission success in spite of hostile action or adverse conditions" [21]. In aviation, resilience is traditionally thought of as a characteristic of human operators (such as pilots) to both avoid failures and ensure mission success [22]. Given that increasing levels of autonomy shift the responsibility for operational safety onto design of the aircraft, it is thus important to define high-level requirements on systems resilience as a part of the systems development process. These requirements may in turn flow into resilience-enabling strategies, such as operational hazard prevention as well as masking, recovery, and goal change (see Ref. [23]). These requirements can further be developed during the PASA and PSSA process, and verified and validated during later safety assessments, ensuring that resilient control policies (e.g., contingency management and operational avoidance) proposed earlier in the design process were adequate. Additionally, it may be beneficial to validate that the requirements themselves continue to sufficiently address hazards as safety assessments become more detailed.

The use cases for novel aviation concepts with increasing levels of autonomy may include novel operations such as wildland firefighting, disaster relief, air taxi, package delivery, and many more [2]. An UAS used for wildfire fighting may be used, for example, for surveillance as well as logistics delivery, which have very different mission profiles [2]. These different missions may involve different roles and coordination strategies among aircraft. Thus, the aircraft-level functions may vary aircraft-to-aircraft depending on their use cases and assigned roles. This is further complicated by changes in the defined form of the aircraft concepts (a tube and wings) to much more diverse configurations (e.g., tilt-rotors, powered lifts, etc.) which are likely to have substantially different risks [24]. Without a systematic, rigorous approach to define such functions, the function derivation could (and often does [25]) vary depending on the expert performing the analysis. Thus, there is a need for unified, systematic, and rigorous functional modeling approaches to help identify and characterize functions for the FHA process of novel aviation concepts with increasing levels of autonomy that accommodate these considerations related to use cases, roles, and configurations of the aircraft.

Traditionally, determining the severity of failures in the FHA process accounts for the variations of severity due to operational phases, conditions, and environment through a qualitative assessment [7]. For novel aviation concepts with increasing levels of autonomy, this process may be inadequate because these concepts may be designed to operate in controlled operational domains, such that real-world deviations from intended environment and configuration may cause important variation in failure severity. For example, for an unmanned aircraft performing a disaster response mission, the severity of losing the aircraft may be different depending on if the aircraft is in an urban area versus a rural area [26]. In this case, where no humans are on board the aircraft, the potential to crash into another aircraft or above a populated area becomes a primary consideration for safety [27], which may not be the case in a rural area. Moreover, in a traditional system, failure to effectively perceive and mitigate environmental risk would be considered "human error" and thus an aspect of pilot qualification as opposed to design safety. For example, if an aircraft experiences a severe weather condition, the operator is expected to mitigate any hazards that may arise from this condition. In novel aviation concepts with increasing levels of autonomy, this mitigation task may be the responsibility of the system itself. Thus, when determining failure severity, a more rigorous FHA approach is needed to account for the interactions between

autonomy and its potential uses cases, configuration (e.g., partial versus full autonomy), and operating environment.

Finally, the analysis of safety (including FHA) requires building up safety expertise around particular technologies, which is lacking when the systems being analyzed are particularly novel [19]. Thus, FHA tools and techniques should improve the analyst's understanding of system safety, rather than just formalizing and encoding it. In this way, systematic methodology and analysis tools and techniques can be an important aspect of building up this expertise.

III. Literature Review

In this section, we list issues and perspectives in the related standards, hazard analysis literature, and tools to best understand how FHA practice for civil aviation should advance.

A. Supporting Models, Formalisms, and Discursive Methodologies to Encourage Systematic Failure Reasoning

The goal of the FHA process is to enable the identification and analysis of system hazards at the overall functional level of the system. However, the guidance on how to perform this process in aviation has been limited. For instance, ARP 4761A [7] lays out an expert driven process mainly providing analysis requirements (e.g., what fields must be in the table) and examples, with very little details provided on how to identify functions, manage complexity (if the assessment become complex), or account for system's interactions internally and externally. In contrast, SAE 926–itself a descendent of early FMEA standards–provides much more detail about how to represent the system in a function block diagram to inform the identification and analysis of hazards [13]. Given the assumption that diagrams (such as function-flow block diagrams) can help improve the FHA process–especially for systems with significant interactions [12], there have been significant efforts in the literature to develop diagrams that adequately represent system function for the purpose of hazard analysis, as described next.

1. Energy-Materials-Signals-based Models

One of the major contributions of engineering design theory is the development of systematic design methodologies to encourage the use of functional reasoning in early design to cultivate innovative solutions [28]. This approach relies on "functional models," also known as energy-materials-signals models, to first understand the needed functionalities of the systems and their interactions with each other, which are called flows [28].

Given that hazard analysis is also a process that relies on functional reasoning in the early stages of design, there have thus been a number of approaches in the literature to use these functional models to perform FHA-like analyses. These methods have included discursive table-based approaches such as the function-failure design method (FFDM) [29] and related risk in early design method (RED) [30], which use the functional architecture to identify and assess failure modes, as well as simulation base approaches such as the Functional Failure Identification and Propagation (FFIP) approach [31] and its descendants [32].

2. Socio-technical Models

One of the major issues for maintaining the safety of complex engineered systems (such as aircraft) is the impact of accidents and human error. Presently, human error–as opposed to component failures–are considered a primary cause of safety incidents [33, 34] and there is thus a need to better understand and prevent human-caused failure scenarios. To address these challenges, systems-oriented hazard methodologies have been proposed to analyze human, operational, and organizational causes of incidents and their impact on system safety. One such method, Systems-Theoretic Process Analysis (STPA) [35] considers the operational control structure (e.g., between the pilot and the aircraft) to better understand failures caused by interactions between the system and the operator and/or organization. STPA's ability to consider the entire system and look beyond individual component failures helps with incident analysis [36]. Interactions at various hierarchical levels (pilots, air traffic personnel, aircraft systems and subsystems) are considered. STPA helps with the early identification and elicitation of hazards, and the proposal of mitigative measures during the system design and operation. This process is making its way into hazard analysis standards (such as ISO 21448 [37]); however, there is a question as to how they should integrate with traditional processes for FHA.

Another systems-oriented hazard assessment approach is Functional Resonance Analysis Method (FRAM) [38], which uses a functional representation in which functions are described through six characteristics (i.e., inputs, outputs, preconditions, resources, time, and control). The interactions are represented through connections between these characteristics where hazards originate from variations of these interactions. Like STPA, FRAM considers the entire

system in the hazard analysis and capable of capture hazards beyond component failures. Unlike STPA, FRAM is also capable of accounting for the dynamic behaviors of systems, allowing for simulation-based hazard assessments.

B. Model-based Engineering to Improve Traceability and Analysis Flexibility

Given that hazard analysis occurs in many places through the design process as a part of the safety assessment process, it is important to ensure that analysis artifacts are traceable to the design of the system and flexible enough to readily re-analyse the system when the design changes. To enable this, the literature has pursued frameworks for performing hazard analysis in an MBSE paradigm.

The use of MBSE promises to make team communication and collaboration easier throughout the lifecycle of the system by providing a better understanding of system knowledge, thus rendering knowledge dissemination more efficient [39]. MBSE further promises to make the design and development of complex systems more manageable by offering a virtual model that serves as a "single point of truth" [40] during the different phases of the system (concept, requirements and design, verification and validation). A review of the literature has shown that the adoption and application of MBSE significantly increases the return on investments in terms of consistency [41], test and evaluation [42], communication [43, 44], early concept exploration [45], design reusability [46], system analysis [47], verification and validation [48, 49], and traceability [50]. However, reviews of these studies have shown that the effectiveness of MBSE can vary depending on implementation [51, 52].

For hazard analysis, MBSE promises to enable a more efficient analysis process by using a comprehensive and integrated model representing the system, its components, and their interactions to an early identification of potential hazards and their proposed management [53]. This model can then be used to perform safety critical analyses via an iterative application of MBSE called Model-Based Mission Assurance (MBMA) [53].

SysML is the most-used language for MBSE. As a result, a number of frameworks in the literature have been used to perform FHA using SysML models [54–56]. However, SysML does not have built-in constructs for representing functions or performing hazard analysis. Thus, Numerous extensions and adaptations to SysML have been proposed to enable hazard assessments. One such popular adaptation is the Risk Analysis and Assessment Modeling Language (RAAML). RAAML is an extension of SysML that enables the representation of risk analysis-oriented diagrams such as fault trees and FMEA tables [57] and can be used to support hazard assessment. Outside of this, there have been some examples in the literature for how to use SysML to support the use of EMS-based FFIP functional-failure models for hazard analysis [58].

C. Computational Support to Expand the Scope and Improve the Consideration of Hazardous Scenarios

The digitization of engineering processes has broadly led to the increasing use of software to assist the construction of hazard analyses. These tools essentially can help organize the analysis, integrate it with other analyses (e.g., that may justify assumptions or validate results) and can encourage MBSE by linking the analysis with a system model. Some existing tools that assist with this process include:

- FMEA tools (Reliasoft XFMEA [59], Ansys Medini [60], Sphera [61]), MBSE (RAAML [57], Cameo [62], Jama [63]),
- Safety case development tools (i.e., AdvoCATE [64]).
- STPA tools (e.g., SafetyHAT [65], RM Studio [66], XSTAMPP [67], CAIRIS [68], Visualpro SA *, STAMP Workbench [69], SpecTRM [70],
- Safety tools such as Safety Assessment Software Tool from Ald Services [71], RASWin [72], and Maintenance Aware Design environment (MADe) tools from Siemens [73], which include specific capabilities for performing FHA.

While these tools can support hazard analysis and safety assessment, they are mostly focused on assisting the user with data entry and organization as opposed to improving the analysis itself. That is, in these tools, the user enters in the hazards, associated losses, and connections in a diagram, then the tool assists with creating tables, diagrams, and documentation from the user input, rather than providing support to improve the analysis process itself (e.g., by helping identify hazards or potential impacts). To realize the true potential of software and computing more generally to support the FHA process, there have been two major avenues in the literature–modeling and simulation and data-informed analysis, described below.

*https://eng.vway.co.kr/solutions/visualpro-stpa

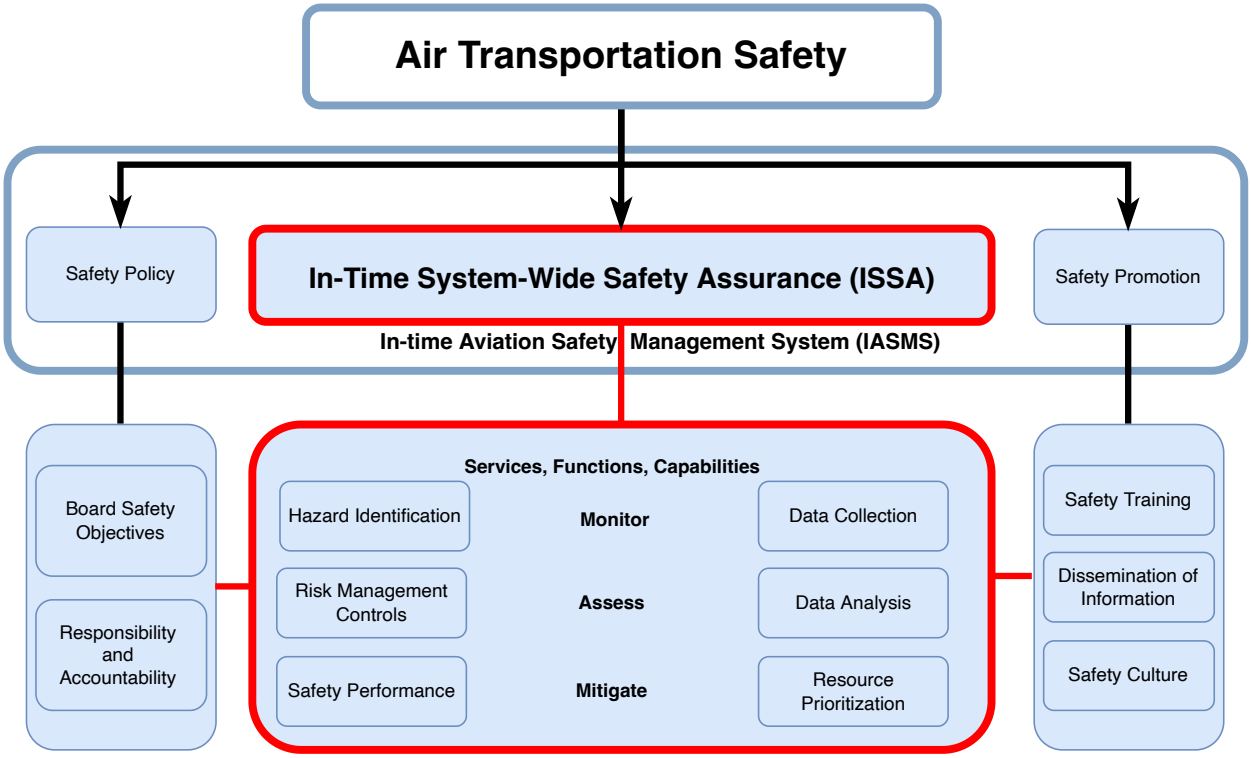

Fig. 2 An In-Time Aviation Safety Management System (IASMS) automates and combines monitor, assess, and mitigate safety functionality under the Risk Management and Safety Assurance pillars. The IASMS also has interfaces to the Safety Policy and Safety Promotion pillars.

1. Modeling and Simulation

The potential for modeling and simulation to improve FHA is to enable rapid re-analysis of design changes, expand the space of potential hazards that can be analyzed from experts alone, and enable the consideration of system behavior (which may be complex, emergent, or otherwise difficult to understand without a model) in hazard analysis. Modeling and simulation for FHA has been explored in the FFIP methodology [31] and its descendants [32] in a variety of ways, enabling the ability to analyze how fault modes cause functional failures and evaluate their dynamic effects at the system level [74]. Modeling and simulation further support a number of capabilities which can be used both for hazard analysis and for the wider design process. For hazard analysis, simulations can be used to explore large spaces of hazardous scenarios [75, 76] that would not have otherwise been tractable to analyze. Simulations can additionally be used to perform trade studies comparing and optimizing the usefulness of hazard mitigations [77]. However, a limitation of many of these simulation-based approaches is that they require significant effort to set up and validate, and still ultimately reflect the assumptions of the analyst.

2. Data-Informed Analysis

One major opportunity for hazard analysis is the incorporation of existing data and reports to inform the analysis, and help identify potential failure scenarios which the analyst might not otherwise have identified. Identifying relevant high-impact failure scenarios is a major difficulty when analyzing novel systems, where there is little prior experience, and the safety analyst must reason about safety with limited knowledge [19]. To address this problem, design-oriented function failure methods have proposed the use of existing resources such as component tables to help inform the analysis [29, 30] by correlating the functions with potential embodying components. While this is helpful for understanding risks from defined component modes which may impact system functionality, failure scenarios often result from a broader scope of causes, including external/environmental conditions as well as operator/human error.

Given that these external sources of hazards are often much more difficult to characterize from an engineering standpoint, much of the existing data exists in accident logs and reports, which are not always easy to access, learn from,

and apply to the design of a new system. Towards this goal, the Manager for Intelligent Knowledge Access (MIKA) [78] was developed, which is an open-source software tool that leverages natural language processing to mine large incident report datasets for hazard analysis. Using Knowledge Discovery and Information Retrieval, MIKA has been applied to various databases from the National Transportation Safety Board [78], the Aviation Safety Reporting System [79], and the Aviation Safety Communiqué [80]. The promise of NLP-based tools like MIKA is the ability to take data from a wide range of operational sources (incident and accident reports) and synthesize them on new (but ultimately analogous) systems to help identify potential hazard considerations, including hazardous conditions, failure conditions and causes, and potential failure effects.

IV. Opportunities for the Next Generation of Functional Hazard Assessment

Given the contributions of the hazard analysis literature presented in Section III, there are a number of opportunities for the adaptation and use of these tools, techniques, and methodologies for FHA in aviation. Particularly, these techniques can help address the challenges that new and emerging airspace concepts with increasing levels of autonomy impose on the safety assurance process. The next subsections lists these potential opportunities and discusses their promise towards addressing the challenges identified in Section II.

A. Using computation to support hazard assessments

The FHA process standardized in ARP 4761A is an expert driven process that is heavily reliant on the use of expert knowledge for the assessment. Techniques in the literature described in Section III, including modeling and simulation-based hazard analysis methods and data-informed analysis can help complement this expert driven process by helping analyst identify and assess hazards that might have otherwise missed due to the large and complex hazard space. However, these tools require maturation and integration to fully realize the opportunity to support the iterative design assurance and support ongoing operational safety. Using computational support during the FHA process can help address some of the challenges identified in Section II.

1. Help manage the large, potentially complex hazard space

As discussed in Section II, with novel aviation concepts that have increasing levels of autonomy, the hazard space can be large and potentially complex. Especially, with the need to consider all system elements (i.e., hardware, software, and human), the operational environment and conditions, the systems' internal (i.e., human-hardware, human-software, etc.) and external interactions (i.e., external systems, environment, etc.), it may become extremely hard or impossible for any human or team of humans to identify the potential hazard space fully. Using computational support to identify hazards (e.g., from historic data or scenario generation) can help reduce the burden on human analysts and complement their knowledge-driven process. The key here is the computational approaches should not aim to replace the existing expert driven process but to complement it by providing additional support for hazard elicitation and analysis. Even when such additional support is present, given the large and complex nature of the hazard space for novel aviation systems with increasing levels of autonomy [19], it is entirely possible that the hazard space may not be fully identified early in design. This shortcoming means that the FHA will have to be iterative, where the analysis is updated as more and more system details emerge, leading to another utility of using computational support for FHA.

2. Enabling rapid re-analysis and adaptation

One of the major opportunities presented by using computational support for performing FHA is the ability to enable a more iterative and dynamic analysis process that better enables design activities (such as optimization and trades assessment) as well the carrying over and use of hazard analyses from design into operations. Of particular interest for new and emerging airspace concepts is the ability to rapidly update safety assessments as (1) more details about the system's design and potential hazards emerge during design or operations that were not envisioned previously–which is often expected of new technologies– and (2) the intended configuration or operating environment and conditions are expected to change–which is a major challenge for the assurance of autonomous systems [3]. This concept can further support the paradigm of in-time safety management, i.e., the In-Time Safety Management System (IASMS) discussed by the National Academies and developed at NASA [5]. In this concept, safety management is to be transformed from a static, reactive paradigm (where changes are made after accidents happen) to a dynamic, proactive, and sometimes predictive paradigm (where changes are made to prevent accidents) [81]. The IASMS concept proposes to monitor, assess, and mitigate safety risks through operational data streams (Fig. 2) [82].

3. Enable the identification and assessment of resilience-related requirements

As discussed in Section II, with the responsibility for operations in novel aviation concepts shifting towards systems autonomy, FHA needs to help designers identify appropriate requirements for resilient operations, such as requirements for hazard avoidance and contingency management. Additionally, it will be beneficial for them to validate that these requirements adequately address hazards as the understanding of potential hazards becomes more detailed and complete. Computational support can thus support the FHA process by helping designers identify and validate such requirements. For example, if simulation support is used, they may try out alternative hazard mitigation policies and compare the resulting system response to optimize their requirements. They may further dynamically simulate the response of the system given particular requirements to validate that they will adequately mitigate hazards. If a data-driven approach is taken, designers may analyze existing data to see what resilience strategies are already employed in analogous systems to derive related requirements requirements. They may additionally study operations and failure data of such systems to validate if resilience requirements have had the intended effects on the analogous systems and learn if there is room for improvement.

4. Enabling the assessment of severity of failure effects

As described in Section II, one of the challenges of using conventional FHA for novel aviation concepts with increasing levels of autonomy is in the need to factor in use-cases, configurations, and operating environments of aircraft in the severity assessment. This challenge is further exacerbated by novel aviation concepts with increasing levels of autonomy since the input space for autonomy-enabling technologies may be large and difficult to tractably characterize. Thus, the failure effects may vary depending on the configuration, environment, and mission of the system, making it difficult to tractably assess the severity of failure conditions. Using computation to support FHA can help analysts develop metrics to quantify the severity of failures based on the operation, environment, and objectives of the system, which then can be used to classify these failure conditions over large spaces of scenarios. Additionally, as the design evolves and the system is adapted to new operating environments and roles, the failure severity metrics may be updated and re-evaluated, making the adaptation of failure condition classification relatively quick and straight forward.

B. Standardizing model capture and representation

Unlike ARP 926, ARP 4761A does not specify a diagram or model to use in the FHA process, leaving the door open to multiple analysis methods. Given that different modeling methodologies can help inform the hazard analysis process in different ways (e.g., traditional FHA and STPA [83]), it may be helpful to provide a unified framework that bridges these approaches to solve the challenges expected of novel aviation concepts. Providing a standardized means of capturing models would enable better adaptation of hazard analysis to new aviation concepts (with less-understood functionality) while also addressing some major challenges for autonomous aircraft. Some particular opportunities are provided next:

1. Incorporating human and operational hazards

While traditional FHA techniques have been based on analyzing system functionality of the technical system, new techniques for hazard analysis described in Section III.A.2 have attempted to consider the operational context into the process. These approaches promise to help analysts understand and mitigate operational causes of hazards, but as of now exist as separate processes, which hinders the ability to analyze joint failure causes and behaviors while also leading to potential duplication between analyses. A unified modeling approach, such as that described in Reference [17] could help bridge these perspectives, bringing socio-technical hazards into FHA, enabling the joint consideration of these hazards with functional failures, and also reducing the duplication of performing these analyses separately.

2. Deriving and Decomposing system functions

As discussed in Section II, the functions of novel aviation concepts with increasing levels of autonomy may vary depending on the use cases and roles of aircraft. Unified functional modeling approaches such as ones discussed in Section III (e.g., Ref. [17]), can help designers systematically derive and decompose functions for systems based on their use cases and roles, while accounting for the operating conditions and systems interactions with humans, environment, and external systems.

3. Enabling traceability through Model-Based Engineering

Improved model capture also promises to enable traceability by enabling model-based engineering, providing the benefits described in Section III.B. Specifically, when a standardized ontology (or, modeling language) is agreed upon for hazard analysis, that enables the creation of tools (such as those described in Section III.C) that can aide in the process, providing the ability to link external evidence and data, develop a rigorous (and, perhaps, simulable) failure model, and be adapt to changes in design and operations. Depending on how the ontology is implemented, it could also enable the trades analysis and comparison of different concepts.

C. Incorporating existing knowledge and data

Since FHA is an early design safety assessment, it is subject to uncertainties since needed information related to the design (such as component embodiment [84]) is not yet available and design decisions are not made. This is further exacerbated when considering novel systems since historic knowledge about the system can be minimal. As described in Section III.C.2, a number of methods have been proposed for taking existing data from a broad array of sources (e.g., tables, unstructured hazard logs, or data from analogous fields) and using it to inform the hazard analysis process. These methods present an opportunity to extend the analyst's knowledge of potential hazards and thus reduce the impact of so-called "black swan" risk (that is, surprising high-impact events [85]). However, when considering existing data, the quality and completeness of the data must be accounted for. For instance, submissions to certain datasets are voluntary, which means they are by nature incomplete and therefore inappropriate for certain analyses. In such data assessments, the integrity of the data is vital to the integrity of the resulting hazards (or knowledge). The use of data to inform FHA also enables one to calibrate analyses during operations when unforeseen hazards inevitably arise, making them vital for in-time safety management, as described in Section IV.A.2. Some of the needs related to this opportunity are discussed below.

1. Improving completeness of knowledge capture by incorporating broad and analogous data sources

While data has the opportunity to better inform hazard analysis, as systems become more novel, the existing data is sparse or not available. In this scenario, there remains an opportunity to find data from analogous applications. For autonomous aircraft, for example, there is an opportunity to use data from piloted aircraft to identify functional failures related to operating the aircraft – a function performed by both pilots and autonomy. However, this data may not be entirely well-structured and it may not be clear what is or is not relevant to the application. Given this, there is an opportunity for data mining technologies to extract, process, and synthesize relevant information to help the analyst identify potential hazards. These technologies, such as Natural Language Processing (NLP), have the demonstrated ability to parse, process, and extract knowledge from high volumes of reports, though they are also subject to errors. Given this, it is important for the analysts to control, filter, and contextualize the outputs of these approaches.

V. Towards Computational Functional Hazard Assessment

Given the opportunities that the contributions of new hazard analysis methodologies, tools, and techniques have towards addressing the unique challenges of new aircraft concepts and technologies, we propose the synthesis of these methods in a new Computational Functional Hazard Assessment (CFHA) paradigm. The goal of Computational Functional Hazard Assessment is to leverage the opportunities that computation presents to hazard analysis (as listed in Sections III and IV) in a unified framework that extends the analyst's ability to identify, characterize, mitigate, and assure the system against hazards. That is, as opposed to supplanting or automating the job of hazard analysis, the goal of CFHA is to improve the adaptability of the process while extending the analyst's ability to identify and characterize hazards with computational tools, techniques, and methodology. We propose that CFHA should use the process in Figure 3. As shown, this process captures data from historical documents, uses it to specify the functional architecture of the system and identify hazards, and then uses simulation to assess the impact of these hazards. Given that this process is performed in a model-based paradigm, it can iteratively adapt through the design process and into operations through the incorporation of new operational data which may then be used to update models and re-simulate hazards. The details of these steps are provided below.

A. Capture knowledge from operational data

The first step of CFHA will be to capture knowledge from operational data, which can come from a variety of sources including relevant and analogous systems, to be used to help identify hazards and behaviors in the FHA process.

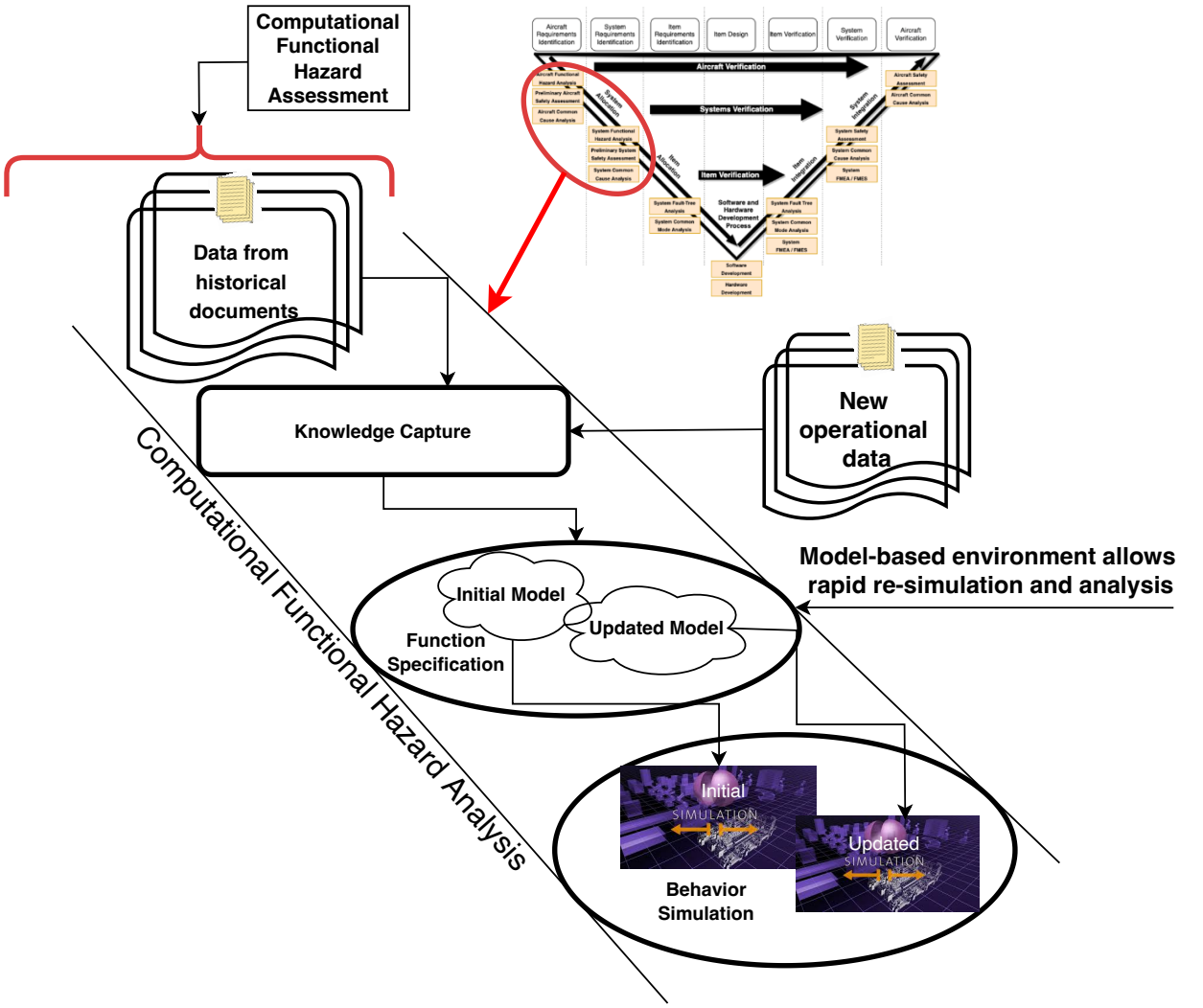

Fig. 3 Recommended concept for Computational Functional Hazard Assessment.

This information-gathering process should be tailorable to a given concept and focused on supporting, rather than supplanting, analyst expertise, as well as providing evidence which may be used to justify analysis assumptions that otherwise would have no concrete basis. In this process, operational data, lessons learned documentation, incident reports, and other sources could be used along with NLP and other AI/ML technologies and algorithms to extract relevant information for a given hazard analysis. The analyst would guide this process and act as a curator and filter between the results of a given algorithm (which may or may not be relevant and exist outside of judgement) and the assumptions of the hazard analysis (which is an outcome of analyst judgement). At design time, this would form the assumptions and basis of the FHA, however, as the system evolves into operations, this process could be performed iterative with data returned from monitoring a system during operation and collecting safety data to build knowledge over time, like in programs such as NASA's Aviation Safety Reporting System (ASRS).

B. Specify functional architecture in a formal modelling language

The second step of CFHA will be to specify the functional architecture in an ontology (or, modeling language) specifically dedicated for this process. This ontology will enable the high-level representation of the system functions and their interactions with each other, operators, and the environments, realizing the opportunity (outlined in Section IV.B to improve model capture and traceability in the context of hazard analysis. It will further enable the use of simulation to extend the ability of the analyst to uncover more hazards than they could have otherwise and enable the assessment to be

iteratively updated and maintained throughout the design process and even after the system is deployed.

In this way, the functional hazard assessment can further become one piece in a much larger modeling paradigm. Using a high-level functional model in this manner (in addition to using individual detailed subsystem models for analysis of each subsystem) could further enable all system elements- i.e., hardware, software, human operator, and environment–to be represented in the same model so interactions and failure propagation at the system level can be studied. This is enabled through the encoding of the functional architecture in an adaptable, flexible, and simulable ontology, which should further account for the lessons in the literature listed in Section III.A.

C. Simulate and analyze hazardous scenarios and behavior

The third step of CFHA will be to use the modeled functions of the system (as well as identified hazards) to simulate and analyze hazardous systems behavior. A simulation based FHA can help assess system behavior over a wide variety of operating scenarios, allowing for a more detailed and behavior-based hazard assessment early in design. Scenarios can cover cover single faults, joint faults, varying operating conditions (e.g., change in weather), and any other disturbances that may affect system performance, which can help practitioners assess a wide range of conditions that otherwise would have been out of reach. Additionally, the use of simulation enables hazard analysis to be repeated easily as more system details become available, known unknowns become known knowns, and unknown unknowns become known unknowns throughout the design process and during operations to ensure that the safety requirements continue to be valid and mitigations appropriately address potential hazards.

Simulation should facilitate the assessment of a wide range of potential operational (including both nominal and hazardous) scenarios to ensure that the operational variability and uncertainties are accounted for and addressed through safety requirements early in design. In particular, with emerging operational paradigms such as m:N and differing roles for the human operator in interacting with automation, it will become important to understand both human error and potential human contribution to safety in a wide range of operational scenarios. This will allow analysts to more accurately capture changes to overall system safety expected (see [86]) from increased automation. Given the ability to simulate wide ranges of scenarios, CFHA should further enable one to make sense of these scenarios through aggregated as well as worst-case statistical analyses.

VI. Conclusion

In this paper, we outlined some of the current practices and opportunities for the FHA process presented in the hazard analysis literature. Given these opportunities, we further proposed a Computational Functional Hazard Assessment process to realize these opportunities and ultimately improve the FHA process to address the challenges imposed by future airspace concepts, such as autonomy and EVTOL. This process involves the use of external (qualitative and quantitative) data sources to inform the analysis, the specification of a formalized hazard model enabling traceability and iterative updates with new information, and the simulation and analysis of a wide range of hazardous scenarios. Rather than rely solely on expert knowledge in the FHA, CFHA aims to assist the expert by providing tools for further exploring the increasingly complex hazard space.

While there have been early efforts by the authors to explore the use of related tools and methodologies in an integrated process (see: [87]), these efforts lacked sufficient integration to deliver on some of the important opportunities listed in Section IV (i.e., enabling an iterative update process from data to models). At this time, the concept is evolving from the initial efforts to incorporate the other key components of CFHA. Therefore, to realize the vision for CFHA, there is a need for an overall process and technical toolchain which resolves each of these issues to enable a more expansive, formalized, flexible, and data-informed analysis process. Future work will focus on formalizing and maturing the process and technical toolchain to enable widespread use.

Acknowledgments

This research was funded by the System-Wide Safety project in the NASA Aeronautics Research Mission Directorate. The findings herein represent the research of the authors and do not necessarily represent the view of the U.S. Government or NASA. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement by the U.S. Government.

References

[1] Mathur, A., Panesar, K., Kim, J., Atkins, E., Sarter, N., Ballin, M., and Goodrich, K., "Paths to Autonomous Vehicle Operations for Urban Air Mobility," 2019. https://doi.org/10.2514/6.2019-3255.

[2] Walsh, H. S., Spirakis, E., Andrade, S. R., Hulse, D. E., and Davies, M. D., "SMARt-STEReO: Preliminary concept of operations," Tech. Rep. NASA/TM-20205007665, National Aeronautics and Space Administration (NASA), September 2020.

[3] Agogino, A., Brat, G., He, Y., Hulse, D., Lipkis, R., Pressburger, T., Gopinath, D., Irshad, L., Kadis, A., Mavridou, A., Pai, G., Păsăreanu, C., and Šljivo, I., "Challenges and Proposed Solutions to Development and Assurance of Autonomy in Aviation," Tech. rep., NASA, 2024.

[4] Hall, J. G., and Rapanotti, L., "Assurance-Driven Design," *2008 The Third International Conference on Software Engineering Advances*, 2008, pp. 379–388. https://doi.org/10.1109/ICSEA.2008.69.

[5] Young, S. D., Quach, C., Goebel, K., and Nowinski, J., "In- Time Safety Assurance Systems for Emerging Autonomous Flight Operations," *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, 2018, pp. 1–10. https://doi.org/10.1109/DASC.2018.8569689.

[6] S-18, Aircraft And System Development And Safety Assessment Committee, "Guidelines for Development of Civil Aircraft and Systems," Aerospace Recommended Practice ARP4754 Rev. B, Oct. 2023.

[7] SAE S-18 Committee, "ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," SAE International, 1996.

[8] Sun, R., Zhong, D., Li, W., Lu, M., Ding, Y., Xu, Z., Gong, H., and Zha, Y., "A Safety Analysis Method of Airborne Software Based on ARP4761," *Journal of Physics: Conference Series*, Vol. 1673, No. 1, 2020, p. 012045. https://doi.org/10.1088/1742-6596/1673/1/012045, URL https://dx.doi.org/10.1088/1742-6596/1673/1/012045.

[9] Kritzinger, D., "Chapter 3 - Functional Hazard Analysis," *Aircraft System Safety*, edited by D. Kritzinger, Woodhead Publishing, 2017, pp. 37–57. https://doi.org/https://doi.org/10.1016/B978-0-08-100889-8.00003-9, URL https://www.sciencedirect.com/science/article/pii/B9780081008898000039.

[10] Wang, P., "Chapter 5 - Preliminary System Safety Assessment," *Civil Aircraft Electrical Power System Safety Assessment*, edited by P. Wang, Butterworth-Heinemann, 2017, pp. 101–156. https://doi.org/https://doi.org/10.1016/B978-0-08-100721-1.00005-4, URL https://www.sciencedirect.com/science/article/pii/B9780081007211000054.

[11] Wang, P., "Chapter 8 - System Safety Assessment," *Civil Aircraft Electrical Power System Safety Assessment*, edited by P. Wang, Butterworth-Heinemann, 2017, pp. 217–238. https://doi.org/https://doi.org/10.1016/B978-0-08-100721-1.00008-X, URL https://www.sciencedirect.com/science/article/pii/B978008100721100008X.

[12] Wilkinson, P., and Kelly, T., "Functional hazard analysis for highly integrated aerospace systems," *IEE Certification of Ground/Air Systems Seminar (Ref. No. 1998/255)*, 1998, pp. 4/1–4/6. https://doi.org/10.1049/ic:19980312.

[13] SAE International, "ARP 926: Fault/Failure Analysis Procedure," 2018.

[14] Prinzel, L., Ellis, K., Koelling, J., Krois, P., Davies, M., and Mah, R., "Examining the changing roles and responsibilities of humans in envisioned future in-time aviation safety management systems," *International Symposium on Aviation Psychology*, 2021.

[15] Kulabukhov, V., "Mathematical foundation of system design regulatory controls based on ARP4754A," *IOP Conference Series: Materials Science and Engineering*, Vol. 1027, 2021, p. 012015. https://doi.org/10.1088/1757-899X/1027/1/012015.

[16] Irshad, L., and Hulse, D., "Resilience Modeling in Complex Engineered Systems With Human-Machine Interactions," *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, Vol. 86212, American Society of Mechanical Engineers, 2022, p. V002T02A024.

[17] Hulse, D., Mbaye, S., and Irshad, L., "Defining A Modelling Language to Support Functional Hazard Assessment," *International Design Engineering Technical Conferences & Computers and Information in Engineering Conference (IDETC-CIE)*, 2024.

[18] Schwalb, E., "Analysis of hazards for autonomous driving," *Journal of Autonomous Vehicles and Systems*, Vol. 1, No. 2, 2021, p. 021003.

[19] McCormick, F., Graydon, M., Neogi, N., Miner, P., and Maddalon, J., "Safety Expertise and the Perils of Novelty," *2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC)*, IEEE, 2023, pp. 1–10.

[20] Denney, E., Pai, G., and Habli, I., "Dynamic safety cases for through-life safety assurance," *2015 IEEE/ACM 37th IEEE International Conference on Software Engineering*, Vol. 2, IEEE, 2015, pp. 587–590.

[21] of Defense, U. S. D., "FACT SHEET: Resilience of Space Capabilities," Tech. rep., 2011. URL https://dod.defense.gov/Portals/1/features/2011/0111_nsss/docs/DoD%20Fact%20Sheet%20-%20Resilience.pdf.

[22] Holbrook, J. B., Stewart, M. J., Smith, B. E., Prinzel, L. J., Matthews, B. L., Avrekh, I., Cardoza, C. T., Ammann, O. C., Adduru, V., and Null, C. H., "Human performance contributions to safety in commercial aviation," Tech. rep., 2019.

[23] Johnson, S. B., Gormley, T., Kessler, S., Mott, C., Patterson-Hine, A., Reichard, K., and Scandura Jr, P., *System health management: with aerospace applications*, John Wiley & Sons, 2011.

[24] Bauranov, A., and Rakas, J., "Urban air mobility and manned eVTOLs: Safety implications," *2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)*, IEEE, 2019, pp. 1–8.

[25] Kurfman, M. A., Stone, R. B., Rajan, J. R., and Wood, K. L., "Functional modeling experimental studies," *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, Vol. 80258, American Society of Mechanical Engineers, 2001, pp. 267–279.

[26] Ellis, K., Johnson, M., Neogi, N., and Homola, J., "NASA Research to Expand UAS Operations for Disaster Response," ????

[27] Gigante, G., Bernard, M., Palumbo, R., Travascio, L., and Vozella, A., "Current approaches in UAV Operational Risk Assessment and Practical Considerations," *Journal of Physics: Conference Series*, Vol. 2716, IOP Publishing, 2024, p. 012055.

[28] Pahl, G., and Beitz, W., *Engineering design: a systematic approach*, Springer Science & Business Media, 2007.

[29] Stone, R. B., Tumer, I. Y., and Van Wie, M., "The function-failure design method," *Journal of Mechanical Design*, , No. 3, 2005, pp. 397–407.

[30] Lough, K. G., Stone, R., and Tumer, I. Y., "The risk in early design method," *Journal of engineering design*, Vol. 20, No. 2, 2009, pp. 155–173.

[31] Kurtoglu, T., and Tumer, I. Y., "A graph-based fault identification and propagation framework for functional design of complex systems," *Journal of Mechanical Design*, , No. 5, 2008, p. 051401.

[32] Jensen, D., Van Bossuyt, D. L., Bello, O., O'Halloran, B. M., and Papakonstantinou, N., "A Survey of Function Failure Identification and Propagation Analysis Methods for System Design," *Journal of Computing and Information Science in Engineering*, Vol. 24, No. 9, 2024.

[33] Kohn, L. T., Corrigan, J. M., Donaldson, M. S., et al., "Errors in health care: a leading cause of death and injury," *To err is human: Building a safer health system*, National Academies Press (US), 2000.

[34] Högberg, L., "Root causes and impacts of severe accidents at large nuclear power plants," *Ambio*, Vol. 42, No. 3, 2013, pp. 267–284.

[35] Ishimatsu, T., Leveson, N. G., Thomas, J., Katahira, M., Miyamoto, Y., and Nakao, H., "Modeling and hazard analysis using STPA," 2010.

[36] Markov, A., Bendarkar, M. V., and Mavris, D. N., "Improved Hazard Analysis for Novel Vehicle Configurations Using the Systems-Theoretic Process Analysis," *AIAA SCITECH 2022 Forum*, 2022, p. 0260.

[37] ISO, "ISO-21448 Road vehicles — Safety of the intended functionality," 2022.

[38] Frost, B., and Mo, J. P., "System hazard analysis of a complex socio-technical system: the functional resonance analysis method in hazard identification," *Proc. of Australian System Safety Conference, Melbourne Australia*, 2014, pp. 28–30.

[39] SEBoK, "Model-Based Systems Engineering (MBSE) — SEBoK," , 2024. URL https://sebokwiki.org/w/index.php?title=Model-Based_Systems_Engineering_(MBSE)&oldid=71378, [Online; accessed 27-September-2024].

[40] D'Ambrosio, J., and Soremekun, G., "Systems engineering challenges and MBSE opportunities for automotive system design," *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, IEEE, 2017, pp. 2075–2080.

[41] Vipavetz, K., Murphy, D., and Infeld, S., *Model-Based Systems Engineering Pilot Program at NASA Langley*, ???? https://doi.org/10.2514/6.2012-5165, URL https://arc.aiaa.org/doi/abs/10.2514/6.2012-5165.

[42] Bjorkman, E. A., Sarkani, S., and Mazzuchi, T. A., "Using model-based systems engineering as a framework for improving test and evaluation activities," *Systems Engineering*, Vol. 16, No. 3, 2013, pp. 346–362. https://doi.org/https://doi.org/10.1002/sys.21241, URL https://incose.onlinelibrary.wiley.com/doi/abs/10.1002/sys.21241.

[43] Ryan, M., Cook, S., and Scott, W., "Application of MBSE to Requirements Engineering—Research Challenges," 2013.

[44] Bijan, Y., Yu, J., Graves, H., Stracener, J., and Woods, T., "6.6.1 Using MBSE with SysML Parametrics to Perform Requirements Analysis," *INCOSE International Symposium*, Vol. 21, No. 1, 2011, pp. 769–782. https://doi.org/https://doi.org/10.1002/j.2334-5837.2011.tb01242.x, URL https://incose.onlinelibrary.wiley.com/doi/abs/10.1002/j.2334-5837.2011.tb01242.x.

[45] Bayer, T., Chung, S., Cole, B., Cooke, B., Dekens, F., Delp, C., Gontijo, I., Lewis, K., Moshir, M., Rasmussen, R., and Wagner, D., "Early Formulation Model-Centric Engineering on NASA's Europa Mission Concept Study," *INCOSE International Symposium*, Vol. 22, 2012, pp. 1695–1710. https://doi.org/10.1002/j.2334-5837.2012.tb01431.x.

[46] Góngora, H. G. C., Ferrogalini, M., and Moreau, C., "How to Boost Product Line Engineering with MBSE - A Case Study of a Rolling Stock Product Line," *Complex Systems Design & Management*, edited by F. Boulanger, D. Krob, G. Morel, and J.-C. Roussel, Springer International Publishing, Cham, 2015, pp. 239–256.

[47] Bayer, T. J., Chung, S., Cole, B., Cooke, B., Dekens, F., Delp, C., Gontijo, I., Lewis, K., Moshir, M., Rasmussen, R., and Wagner, D., "Model Based Systems Engineering on the Europa mission concept study," *2012 IEEE Aerospace Conference*, 2012, pp. 1–18. https://doi.org/10.1109/AERO.2012.6187337.

[48] Wibben, D. R., and Furfaro, R., "Model-Based Systems Engineering approach for the development of the science processing and operations center of the NASA OSIRIS-REx asteroid sample return mission," *Acta Astronautica*, Vol. 115, 2015, pp. 147–159. https://doi.org/https://doi.org/10.1016/j.actaastro.2015.05.016, URL https://www.sciencedirect.com/science/article/pii/S0094576515001988.

[49] Khan, M. O., Dubos, G. F., Tirona, J., and Standley, S., "Model-based verification and validation of the SMAP uplink processes," *2013 IEEE Aerospace Conference*, 2013, pp. 1–9. https://doi.org/10.1109/AERO.2013.6496913.

[50] Cole, B., Mittal, V., Gillespie, S., La, N., Wise, R., and MacCalman, A., "Model-based systems engineering: application and lessons from a technology maturation project," *Procedia Computer Science*, Vol. 153, 2019, pp. 202–209. https://doi.org/https://doi.org/10.1016/j.procs.2019.05.071, URL https://www.sciencedirect.com/science/article/pii/S1877050919307306, 17th Annual Conference on Systems Engineering Research (CSER).

[51] Carroll, E. R., and Malins, R. J., "Systematic Literature Review: How is Model-Based Systems Engineering Justified?." 2016. URL https://api.semanticscholar.org/CorpusID:96425861.

[52] Henderson, K., and Salado, A., "Value and benefits of model-based systems engineering (MBSE): Evidence from the literature," *Systems Engineering*, Vol. 24, No. 1, 2021, pp. 51–66. https://doi.org/https://doi.org/10.1002/sys.21566, URL https://incose.onlinelibrary.wiley.com/doi/abs/10.1002/sys.21566.

[53] Evans, J., Cornford, S. L., JPL, and Feather, M. S., "Model Based Mission Assurance (MBMA) : NASA' s Assurance Future," 2015. URL https://api.semanticscholar.org/CorpusID:5878632.

[54] Maitrehenry, S., Metge, S., Bieber, P., and Ait-Ameur, Y., "Towards model-based functional hazard assessment at aircraft level," *Advances in Safety, Reliability and Risk Management: ESREL 2011*, 2011, p. 390.

[55] Schäfer, M., Berres, A., and Bertram, O., "Integrated model-based design and functional hazard assessment with SysML on the example of a shock control bump system," *CEAS Aeronautical Journal*, Vol. 14, No. 1, 2023, pp. 187–200.

[56] Jiang, Y., Bai, N., Yang, H., Zhang, H., Wang, Z., and Liu, X., "MBSE-based functional hazard assessment of civil aircraft braking system," *2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*, IEEE, 2020, pp. 460–464.

[57] Group, T. O. M., "Risk Analysis and Assessment Modeling Language (RAAML) Libraries and Profiles," https://www.omg.org/spec/RAAML/1.1/Beta1/PDF, March 2024.

[58] Jiao, J., Pang, S., Chu, J., Jing, Y., and Zhao, T., "An improved FFIP method based on mathematical logic and SysML," *Applied Sciences*, Vol. 11, No. 8, 2021, p. 3534.

[59] Hottinger Brüel & Kjær, "FMEA and Related Analyses," https://www.hbkworld.com/en/products/software/reliability/xfmea-failure-mode-effects-analysis-fmea-software, 2024.

[60] Ansys, "Ansys medini analyze: Safety & Security for Electronic Systems ," https://www.ansys.com/products/safety-analysis/ansys-medini-analyze, 2024.

[61] Sphera, "Process Hazard Analysis (PHA-Pro) & HAZOP," https://sphera.com/solutions/operational-risk-management/advanced-risk-assessment-software-and-services/process-hazard-analysis-pha-pro-hazop/, 2024.

[62] Dassault Systèmes, "Cameo Safety & Reliability Analyzer Plugin," https://www.3ds.com/products/catia/no-magic/cameo-safety-reliability-analyzer-plugin, 2024.

[63] Jama Software, "Simplify Compliance With Proactive Risk Management Software," https://www.jamasoftware.com/solutions/risk-management/, 2024.

[64] Denney, E., Pai, G., and Pohl, J., "AdvoCATE: An assurance case automation toolset," *Computer Safety, Reliability, and Security: SAFECOMP 2012 Workshops: Sassur, ASCoMS, DESEC4LCCI, ERCIM/EWICS, IWDE, Magdeburg, Germany, September 25-28, 2012. Proceedings 31*, Springer, 2012, pp. 8–21.

[65] U.S. Department of Transportation Volpe Center, "SafetyHAT: A Transportation System Safety Hazard Analysis Tool," https://www.volpe.dot.gov/infrastructure-systems-and-technology/advanced-vehicle-technology/safetyhat-transportation-system, 2023.

[66] Risk Management Studio., "Centralized Risk Management and Guidance to Implement ISO 27001," https://www.riskmanagementstudio.com/, 2022.

[67] Abdulkhaleq, A., and Wagner, S., "XSTAMPP: an eXtensible STAMP platform as tool support for safety engineering," 2015.

[68] CAIRIS, "An Open Source Platform for Building Security and Usability into your Software," https://cairis.org/, 2024.

[69] Information-technology Promotion Agency, J., "Enabling digital transformations in industries and a society," https://www.ipa.go.jp/en/digital/complex_systems/stamp.html, 2023.

[70] NASA SPINOFF , "Building Safer Systems With SpecTRM," https://spinoff.nasa.gov/spinoff2003/ct_10.html, 2003.

[71] ALD Services, "Safety Assessment Software Tool," https://aldservice.com/Reliability-Products/safety.html, 2024.

[72] Rockwell Automation, "RASWin Software Tool: Document the Entire Safety Lifecycle," https://www.rockwellautomation.com/en-us/capabilities/industrial-safety-solutions/risk-assess-software-tool.html, 2024.

[73] Siemes, "Maintenance Aware Design Ecosystem (MADE)," https://plm.sw.siemens.com/en-US/simcenter/integration-solutions/maintenance-aware-design-ecosystem/, 2024.

[74] Hulse, D., Walsh, H., Dong, A., Hoyle, C., Tumer, I., Kulkarni, C., and Goebel, K., "fmdtools: A fault propagation toolkit for resilience assessment in early design," *International Journal of Prognostics and Health Management*, Vol. 12, No. 3, 2021.

[75] Hulse, D., and Irshad, L., "Synthetic fault mode generation for resilience analysis and failure mechanism discovery," *Journal of Mechanical Design*, Vol. 145, No. 3, 2023, p. 031707.

[76] Girshfeld, I., Hulse, D., and Irshad, L., "Uncovering Hazards Using a Multi-Objective Optimization to Explore the Faulty State-Space," *AIAA SCITECH 2023 Forum*, 2023, p. 2578.

[77] Hulse, D., Hoyle, C., Goebel, K., and Tumer, I. Y., "Quantifying the resilience-informed scenario cost sum: A value-driven design approach for functional hazard assessment," *Journal of Mechanical Design*, Vol. 141, No. 2, 2019, p. 021403.

[78] Andrade, S., and Walsh, H., "MIKA: Manager for Intelligent Knowledge Access Toolkit for Engineering Knowledge Discovery and Information Retrieval," *INCOSE International Symposium*, Vol. 33, No. 1, 2023, pp. 1659–1673. https://doi.org/https://doi.org/10.1002/iis2.13105, URL https://incose.onlinelibrary.wiley.com/doi/abs/10.1002/iis2.13105.

[79] Mbaye, S., Walsh, H. S., Davies, M., Infeld, S. I., and Jones, G., *From BERTopic to SysML: Informing Model-Based Failure Analysis with Natural Language Processing for Complex Aerospace Systems*, 2024. https://doi.org/10.2514/6.2024-2700, URL https://arc.aiaa.org/doi/abs/10.2514/6.2024-2700.

[80] Andrade, S. R., and Walsh, H. S., *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*, ????

[81] National Academies of Sciences, Engineering, and Medicine, *In-Time Aviation Safety Management: Challenges and Research for an Evolving Aviation System*, The National Academies Press, Washington, DC, 2018. https://doi.org/10.17226/24962, URL https://nap.nationalacademies.org/catalog/24962/in-time-aviation-safety-management-challenges-and-research-for-an.

[82] Ellis, K. K., Krois, P., Koelling, J., Prinzel, L. J., Davies, M., and Mah, R., *A Concept of Operations (ConOps) of an In-time Aviation Safety Management System (IASMS) for Advanced Air Mobility (AAM)*, 2021. https://doi.org/10.2514/6.2021-1978, URL https://arc.aiaa.org/doi/abs/10.2514/6.2021-1978.

[83] Graydon, M., Neogi, N. A., and Wasson, K., "Guidance for designing safety into urban air mobility: Hazard analysis techniques," *AIAA Scitech 2020 Forum*, 2020, p. 2099.

[84] O'Halloran, B. M., Hoyle, C., Tumer, I. Y., and Stone, R. B., "The early design reliability prediction method," *Research in Engineering Design*, Vol. 30, 2019, pp. 489–508.

[85] Aven, T., "On the meaning of a black swan in a risk context," *Safety science*, Vol. 57, 2013, pp. 44–51.

[86] Holbrook, J., "Exploring methods to collect and analyze data on human contributions to aviation safety," *49th International Symposium on Aviation Psychology*, 2021, pp. 110–115.

[87] Andrade, S., Hulse, D., Irshad, L., and Walsh, H. S., "Supporting Hazard Analysis for Wildfire Response Using fmdtools and MIKA," Tech. Rep. NASA/TM-20220014099, NASA, 2022.