Unifying Functional Hazard Analysis and RAMS Modelling: Bridging the Safety Assurance Gap through Digital System Representations

Rahul Gottumukkala
PHM Technology
rahul.gottumukkala@phmtechnology.com

Cameron Sturgeon
PHM Technology
cameron.sturgeon@phmtechnology.com

Derek Kim
PHM Technology
Derek.Kim@phmtechnology.com

Abstract

Safety assurance in complex, safety-critical systems often suffers from fragmented datasets and inconsistent input data generated by different engineering teams. This lack of alignment between teams leads to disconnected analyses and defects in artefacts, particularly between early-stage functional hazard assessments and downstream reliability, availability, maintainability, and safety (RAMS) evaluations. This paper proposes a unified modelling approach that directly links safety requirements to system representations, enabling traceability, consistency, and quantitative verification across the system lifecycle.

The proposed method establishes a digital representation of the system where functional failures identified through Functional Hazard Analysis (FHA) are systematically mapped to reliability models such as Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), and Reliability Block Diagrams (RBD). This digital model facilitates the propagation of Failure Conditions, supports real-time consistency checks between functional and physical domains, and allows safety requirements to be dynamically evaluated as system designs evolve.

Novel contributions include: (1) a bidirectional traceability framework linking top-down safety requirements with bottom-up failure data; (2) an integrated modelling technique that aligns functional failure severity and probability metrics with reliability assessments.

Case study demonstrates how the method improves transparency in the assurance process, supports early identification of architectural weaknesses, and reduces the overhead of maintaining separate safety and reliability artefacts. By aligning FHA and RAMS activities through a common digital knowledge base, the approach enables more robust and agile system assurance in an era of increasing system complexity and regulation.

1 Introduction

Assuring safety in modern, safety-critical systems is increasingly challenging as architectures become more integrated, software-intensive, and reliant on novel technologies such as electrification and autonomy. Traditional approaches, guided by guidelines/standards like ARP4761A and GEIA-STD-0009 (SAE, 2023; Reliability Program, 2020), rely on sequential analyses including Functional Hazard Assessment (FHA), Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), and Reliability Block Diagrams (RBD). While these methods are mature and well established, they are typically performed in isolation, producing fragmented artefacts that are difficult to maintain and often inconsistent with one another. As a result, safety objectives derived during FHA are not always transparently traceable to the quantitative reliability evidence that demonstrates compliance, creating inefficiencies and gaps in assurance.

This paper proposes a unified modelling approach that embeds FHA outputs directly into reliability models within a digital system representation. The approach creates bidirectional traceability between top-down safety requirements and bottom-up reliability evidence, aligns qualitative hazard severity classifications with quantitative reliability metrics, and supports dynamic consistency checks as designs evolve. A case study of a Battery Management System demonstrates how the method improves transparency, reduces duplication of effort, and enables earlier identification of architectural weaknesses. By operationalising the intent of ARP4761A and GEIA-STD-0009 through model-based practices, the approach provides a pathway to more robust, efficient, and lifecycle-spanning safety assurance.

2 Background and Related Work

2.1 Implementation of FHA

The implementation of FHA begins with careful scoping of the analysis. This involves defining the operational

context, including mission types, flight phases, and environmental assumptions, to ensure all functional requirements are captured. Functions are then decomposed into a hierarchy at a level of detail sufficient to assess potential hazards, but without tying them to specific design solutions. At the aircraft level this functional hierarchy remains allocation-free, while at the system level and item level, functions are refined according to system responsibilities.

For each identified function, failure condition statements are formulated. These typically consider loss of function, malfunction, degradation, or untimely/erroneous execution. Each failure condition is then evaluated for its potential effects on the aircraft, crew, passengers, mission, and environment, taking into account the phase of flight. At this stage, assumptions about crew workload, available reaction time, and detectability are also documented. This structured approach ensures that safety implications are considered consistently across all operational scenarios.

Once failure effects are identified, the criticality of each condition is determined. ARP4761A adopts categories ranging from Catastrophic, Hazardous, Major, and Minor to No Effect. Each classification is supported by a clear rationale and operational assumptions. From these severities, qualitative and quantitative safety objectives are derived, typically expressed as maximum allowable probabilities per flight hour.

2.2 Implementation of RAMS Analysis

The criticality targets established during the Functional Hazard Analysis (FHA) can subsequently be verified through Reliability, Availability, Maintainability, and Safety (RAMS) analysis methods such as Fault Tree Analysis (FTA) and quantitative reliability assessments. These follow-on techniques provide a structured means of demonstrating that the probability of failure of individual items, subsystems, and the overall aircraft remains below the maximum allowable thresholds specified in the FHA. In practice, this creates a direct linkage between the qualitative hazard classifications defined during FHA and the quantitative reliability evidence required to justify compliance with certification objectives (SAE, 2023; FAA, 2002).

The connection between FHA and RAMS analysis is first established by systematically mapping the system-level functions identified in the FHA to their corresponding physical or logical items in the system model. This mapping is a crucial step because it allows criticality values, which originate from functional-level safety objectives, to be translated into quantitative reliability targets at the item, subsystem, and aircraft levels. Through this process, reliability allocation ensures that the cumulative reliability of lower-level items is sufficient to satisfy the safety requirements defined by the higher-level FHA analysis. The outcome is a hierarchy of target reliability values that link functional safety requirements directly to measurable engineering parameters (Kritzinger, 2017; SAE, 2023).

Once these allocations are complete, the reliability of the proposed design can be assessed through the combined application of FTAs and reliability calculations. For each item, subsystem, and the overall aircraft, an FTA is constructed in which the failure conditions identified during the FHA are represented as basic events feeding into the top event of interest. This structure enables a clear traceability path from functional hazard to quantitative reliability demonstration. In order for the FHA to be validated, the probability of each top event in the FTAs must be demonstrated to be less than the maximum allowable failure probabilities derived from the initial FHA-driven allocations.

In addition to FTA, reliability calculations provide a complementary means of verifying FHA objectives. These calculations require the specification of reliability metrics, such as mean time to failure (MTTF), mean time between failures (MTBF), or appropriate failure distribution parameters (e.g., Weibull or exponential distributions) for each low-level component. Reliability Block Diagrams (RBDs) are then developed to capture the logical structure of item states and their influence on system-level performance. Using these inputs, system reliability can be evaluated over the intended mission duration or operational lifecycle. Similar to FTAs, the resulting probabilities of failure must remain below the thresholds defined during the reliability allocation process, thereby demonstrating alignment with FHA-derived safety objectives.

If either the FTA or the reliability calculations indicate that the specified requirements from the FHA are not met, corrective actions are necessary. These reconfigurations may involve design modifications, such as introducing redundancy or altering architecture, as well as operational interventions such as scheduled maintenance activities that improve effective reliability. In some cases, it may also be appropriate to revisit and adjust the criticality values or assumptions defined in the FHA to ensure that they remain realistic in the context of design maturity. Through this iterative process, FHA and RAMS analysis remain tightly integrated, ensuring that functional safety objectives are both practically achievable and demonstrably satisfied within the system design (SAE, 2023; Kritzinger, 2017).

2.3 Integration of Safety and Reliability Guidelines/Standards

The alignment between safety assessment and reliability engineering is reinforced through international guidelines/standards that provide structured guidance for system developers. SAE ARP4761A defines the accepted industry process for performing safety assessments of civil aircraft and systems. It introduces a tiered approach in which hazards are first identified at the aircraft level through the Aircraft Functional Hazard Assessment (AFHA) and then progressively refined through the Preliminary System Safety Assessment (PSSA) and the final System Safety Assessment (SSA). Each step ensures that hazards are traced down to specific system and equipment implementations, enabling the derivation of safety requirements that are both comprehensive and verifiable.

In parallel, GEIA-STD-0009 establishes requirements for a reliability program that spans design, production, and in-service operation. Unlike ARP4761A, which is focused on certification compliance and hazard management, GEIA-STD-0009 emphasizes the establishment of a Reliability Program Plan (RPP), a Reliability Case, and closed-loop processes that ensure failures are

systematically identified, mitigated, and tracked through design, manufacturing, and field operation. A key contribution of GEIA-STD-0009 is its insistence on "closed-loop failure mode mitigation," requiring that identified weaknesses be corrected and verified rather than merely documented. This emphasis on corrective action ensures that reliability targets are not treated as abstract predictions but as outcomes demonstrably achieved in practice.

Together, ARP4761A and GEIA-STD-0009 provide complementary perspectives: the former ensures that catastrophic hazards are eliminated or adequately mitigated through safety analysis, while the latter ensures that the system can meet its intended reliability performance across the entire lifecycle. The challenge in practice, however, lies in bridging these frameworks. Safety assessments often stop once compliance with probability thresholds is demonstrated, while reliability programs may not explicitly preserve the hazard classifications that motivated their requirements. This disjunction underscores the need for integrated methods capable of ensuring traceability between hazard severity classifications and reliability performance evidence.

2.4 Model-Based Safety Analysis and Digital Continuity

Model-Based Safety Assessment (MBSA) has emerged as a promising approach to address the limitations of document-centric processes. Traditional safety and reliability artefacts, such as FMEAs, FTAs, and RBDs, are often generated in isolation using disparate tools and are manually cross-referenced to functional hazard analyses. This manual integration is error-prone and difficult to maintain as designs evolve. MBSA introduces digital continuity by representing system functions, architectures, and failure logic within a unified model. From this model, safety and reliability artefacts can be automatically generated and kept consistent as the system design changes.

ARP4761A Rev A (2023) acknowledges MBSA as a valid technique for safety assessments, particularly in the construction of fault trees and dependency models. Similarly, GEIA-STD-0009 highlights the importance of maintaining a living reliability model that is updated with test, analysis, and in-service data. By embedding FHA outputs directly into MBSA environments, it becomes possible to perform real-time consistency checks between the functional and physical domains, ensuring that safety requirements flow seamlessly into reliability assessments.

The principal benefit of MBSA is the ability to propagate hazards across abstraction layers. For example, a functional hazard such as "loss of braking capability" can be linked directly to a network of lower-level failure modes in hydraulic, electrical, or control subsystems. As design alternatives are evaluated, the model can dynamically recompute the impact on hazard probabilities, thereby reducing the gap between qualitative hazard classification and quantitative reliability demonstration. This automated propagation provides the continuity that traditional FHA and RAMS integration often lacks.

2.5 Tool Support: MADE

Practical realization of MBSA principles is enabled by specialized tools, MADE (Maintenance Aware Design Ecosystem) software is one among such. MADE provides a model-driven environment for constructing digital representations of system functions, architectures, and missions, from which a wide range of safety and reliability analyses can be automatically derived. The tool supports the generation of FHA, FMEA, FTA, Reliability Block Diagrams, and Reliability Predictions, all from a common system model. This ensures that artefacts share a consistent underlying representation rather than being created as standalone documents.

A unique strength of MADE is its support for automated diagnostic and prognostic assessments. By linking sensor sets, test points, and fault detection coverage, MADE enables users to evaluate the maintainability and testability of system designs in addition to their safety and reliability; aligning closely with the GEIA-STD-0009 closed-loop framework, as diagnostic capabilities directly influence the effectiveness of corrective actions and maintenance strategies.

Moreover, MADE's mission modelling features allow reliability evaluations to be tailored to specific operational scenarios. This ensures that safety objectives are not only allocated correctly but are also evaluated in a contextually accurate manner. As such, MADE represents an exemplar of how digital tools can operationalize the integration of FHA and RAMS, supporting the unified modelling approach proposed in this paper.

2.6 Summary of Gaps in Current Practice

While the guidelines/standards and tools described above offer robust guidance, their implementation in industrial practice often remains fragmented. Safety engineers may focus narrowly on meeting ARP4761A compliance, producing FHAs and FTAs that are sufficient for certification but not systematically linked to reliability allocations. Conversely, reliability engineers may maintain detailed RBDs and reliability predictions without clear traceability back to the hazard classifications that justified those requirements. The result is a disjoint assurance process in which artefacts exist in parallel rather than as a coherent body of evidence.

The reviewed literature and guidelines/standards converge on the recognition that safety and reliability must be tightly integrated across the lifecycle, yet they stop short of prescribing a unified modelling framework. This gap motivates the method proposed in the subsequent sections of this paper: a digital, model-based approach in which FHA outputs are directly embedded into RAMS analyses, enabling bidirectional traceability, dynamic consistency checks, and quantitative verification.

3 Problem Statement

Safety assurance in complex systems spans functional, physical, and operational domains. While processes such as ARP4761A and GEIA-STD-0009 are mature, they are often applied as parallel streams of activity. This separation creates discontinuities that undermine both efficiency and credibility.

3.1 Discontinuity Between Functional and Physical Domains

FHA provides the initial anchor for safety by identifying hazards, but these are not always systematically carried into reliability artefacts such as FMEA, FTA, and RBD. Analyses are often developed in different tools, by separate teams, and at different lifecycle stages, weakening traceability between safety objectives and reliability evidence.

3.2 Duplication of Effort and Inconsistency

Because artefacts are generated independently, the same failure conditions are re-entered multiple times. This leads to inconsistent assumptions—for example, a failure mode classified as catastrophic in the FHA may be treated differently in reliability models—creating rework and undermining confidence in the assurance case.

3.3 Limited Traceability and Verification

Regulators require a transparent chain from hazard classifications to reliability results. In practice, this is usually maintained through spreadsheets or static cross-references that are difficult to keep current as designs evolve. As a result, verification often lags behind design changes, limiting the ability to perform real-time consistency checks.

3.4 Impact on Early Design Decisions

Quantitative reliability models often arrive late in the lifecycle, leaving architectural weaknesses hidden until corrective action is costly. Without a method to dynamically evaluate hazards within evolving architectures, assurance activities cannot effectively influence early design decisions.

3.5 Challenges in Lifecycle Integration

Although both ARP4761A and GEIA-STD-0009 emphasise lifecycle coverage, safety artefacts are frequently archived after certification while reliability programs continue in isolation. This separation prevents in-service data from refining hazard models and breaks the closed-loop feedback needed to ensure alignment between design intent and operational performance.

3.6 Summary

The challenge is not a lack of analytical techniques but the absence of meaningful continuity between them. Current practices produce fragmented artefacts, duplicated effort, and missed opportunities for early intervention. A unified, model-based approach is therefore required to deliver bidirectional traceability, real-time consistency checks, and dynamic verification across the system lifecycle.

4 Proposed Unified Modeling Approach

The proposed approach seeks to unify Functional Hazard Assessment (FHA) with downstream Reliability, Availability, Maintainability, and Safety (RAMS) analyses through the establishment of a common digital representation of the system. By embedding hazard classifications directly into reliability models, the method provides bidirectional traceability, dynamic consistency checks, and quantitative verification as the design evolves. This section describes the conceptual framework, methodological steps, and supporting mechanisms that underpin the approach.

4.1 Conceptual Framework

At the core of the method is a digital system model that captures functions, architectures, and failure mechanisms within a single environment. Unlike traditional document-centric approaches, which require artefacts such as FMEAs and FTAs to be constructed independently, the digital model serves as the source of truth from which these artefacts are automatically derived.

The conceptual framework has three main pillars:

1. **Bidirectional Traceability** – Safety requirements flow top-down from FHA into RAMS analyses, while reliability evidence flows bottom-up to demonstrate satisfaction of safety objectives.
2. **Hazard-Reliability Alignment** – Severity classifications and probability thresholds from FHA are directly mapped onto reliability models, ensuring consistency between qualitative and quantitative domains.
3. **Dynamic Verification** – Because artefacts are generated from a shared model, they remain synchronized with the evolving system design, allowing real-time consistency checks across lifecycle stages.

This integrated approach closes the loop between early safety assessments and downstream reliability activities, addressing the discontinuity, duplication, and verification challenges described in Section 3.

4.2 Bidirectional Traceability

Bidirectional traceability is achieved by explicitly linking each FHA-identified functional hazard to the physical or logical items responsible for implementing the function. These links are preserved in the digital system model and inherited by downstream analyses.

- **Top-down flow:** Starting from the FHA, each hazard classification (e.g., Catastrophic, Hazardous, Major) is mapped to a corresponding reliability target. These targets are then allocated across system items through reliability allocation.
- **Bottom-up flow:** As reliability models (e.g., FTA or RBD) are populated with failure data, the resulting probabilities are automatically rolled up and compared against the top-down targets. If discrepancies are found, the digital model highlights the inconsistencies and traces them back to the originating FHA requirements.

This bidirectional structure ensures that every reliability calculation has an explicit safety rationale, and every safety requirement is backed by measurable reliability evidence.

4.3 Alignment of Hazard Severity and Reliability Metrics

The method addresses a long-standing difficulty in safety engineering: aligning qualitative hazard severity categories with quantitative reliability metrics. In ARP4761A, hazard classifications are associated with maximum allowable failure probabilities per flight hour. However, ensuring these thresholds are properly translated into item-level reliability requirements has historically been error-prone.

The proposed approach embeds this translation directly into the digital model:

- Severity categories (Catastrophic, Hazardous, Major, etc.) are represented as constraints in the system model.
- Reliability metrics such as Mean Time to Failure (MTTF), failure rate (λ), or distribution parameters (e.g., Weibull) are attached to items.
- Allocation algorithms distribute reliability budgets across subsystems in proportion to their contribution to the top-level hazard probability.

4.4 Real-Time Consistency Checks

A critical feature of the digital model is its ability to perform real-time consistency checks as designs evolve. Traditional assurance processes rely on periodic reviews, where artefacts are manually reconciled and updated. In contrast, the proposed approach automates this process:

- If a system function is modified, the associated hazards are automatically re-evaluated.
- If an architectural element change (e.g., redundancy is added or removed), the fault tree and reliability block diagram are updated to reflect the new structure.
- If failure data changes (e.g., updated MTBF from suppliers), the quantitative analysis is re-run, and compliance with FHA targets is re-verified.

These automated consistency checks allow engineers to rapidly explore design alternatives while maintaining continuous assurance that safety objectives remain satisfied.

4.5 Methodological Steps

The unified modelling approach proceeds through the following steps:

1. **Functional Hazard Identification** – Conduct FHA at the aircraft or system level, defining failure conditions, severities, and safety objectives.
2. **Digital System Representation** – Build a system model including functions, architectures, mission profiles, and environments.
3. **Hazard-to-Architecture Mapping** – Link each functional hazard to the system items responsible for implementing the function.
4. **Reliability Allocation** – Translate safety objectives into quantitative reliability targets, allocating them across subsystems and items.
5. **Model-Based Analyses** – Generate FMEAs, FTAs, RBDs, and reliability predictions automatically from the system model.
6. **Dynamic Verification** – Continuously compare analysis results with FHA-derived targets as the system evolves.
7. **Feedback and Iteration** – If requirements are not met, implement corrective actions (e.g., redundancy, design change, maintenance strategy) and re-run analyses until closure is achieved.

5 Implementation Using Model-Based Tools

The success of the unified modelling approach depends on practical mechanisms for embedding safety requirements within system representations and generating reliability artefacts directly from these representations. Model-based environments provide these mechanisms by enabling functions, architectures, failure logic, and mission profiles to coexist in a single, analyzable model. Among existing tools, PHM Technology's MADE exemplifies how such integration can be realized in practice.

5.1 Digital Representation of System and Mission

Implementation begins with the construction of a **digital system model**, which combines functional, physical, and mission-level views of the system.

- **Functional Model:** System-level functions are defined in alignment with the FHA. Each function includes normal operational behaviour, input/output flows, and failure conditions (loss, degradation, malfunction, untimely operation).
- **Physical Model:** System architecture is represented by subsystems, components, and their interconnections. These items are directly linked to the functions they implement, creating a traceability bridge between functional and physical domains.
- **Mission Profile:** Operating scenarios are captured through mission definitions, flight phases, duty cycles, and environmental assumptions. These profiles ensure that reliability analyses reflect the operational stresses identified in FHA.

By modelling system and mission data together, the environment ensures that safety and reliability analyses are contextualized within realistic operating conditions, consistent with ARP4761A's emphasis on phase-of-flight considerations and GEIA-STD-0009's requirements for life-cycle load estimation.

5.2 FHA to RAMS mapping

The unified approach requires that failure conditions identified in the FHA be explicitly mapped to reliability artefacts. In MADE, this mapping occurs automatically once functional hazards are linked to their implementing items:

1. **Failure Mode Derivation:** From the functional model, MADE derives potential failure modes

such as “loss of power supply” or “erroneous command.” These are linked to failure effects at local, next-higher, and end-effect levels.

2. **FMEA Generation:** Using the functional/physical links, the tool automatically generates Failure Modes and Effects Analyses in tabular form, preserving FHA severity classifications and adding reliability attributes such as occurrence likelihood and detectability.
3. **FTA Construction:** Fault trees are generated where FHA failure conditions become top events, and basic events are populated by the associated item-level failures. The structure is directly inherited from the system model, ensuring traceability.
4. **RBD Development:** Reliability Block Diagrams are derived from the architecture, showing the logical success/failure dependencies of items and subsystems.

This automated mapping eliminates the need for manual duplication of data across FHA, FMEA, FTA, and RBD artefacts.

5.3 Reliability Allocation and Quantitative Verification

Once FHA severities are embedded in the model, they can be translated into quantitative targets.

- **Top-Down Allocation:** MADE supports allocation of reliability budgets across subsystems and items, ensuring that cumulative probabilities meet FHA-derived objectives.
- **Bottom-Up Verification:** With failure-rate data (e.g., MTTF, Failure distributions) assigned to items, MADE runs quantitative analyses. Reliability predictions, and fault trees provide evidence that the allocated requirements are satisfied.

The integration of allocation and verification ensures that reliability evidence is directly traceable to safety objectives, creating the bidirectional linkage central to the unified approach.

5.4 Dynamic Consistency Checks

Traditional assurance requires manual reconciliation between artefacts when system designs evolve. In contrast, a model-based environment automatically re-propagates changes across analyses:

- **Architecture Changes:** Adding redundancy updates both the RBD structure and FTA logic, recalculating system reliability instantly.
- **Failure Data Updates:** Replacing a component with new reliability data automatically updates allocations and quantitative results.
- **Functional Changes:** Modifying a function in the FHA triggers updates in linked failure modes, FMEA tables, and FTAs.

These dynamic updates ensure that FHA requirements remain validated throughout design evolution.

6 Case Study

To illustrate the unified modelling approach, this section presents a case study involving the development of a Battery Management System (BMS) for a safety-critical application such as hybrid-electric propulsion or large-scale energy storage in aerospace. The BMS is responsible for monitoring, balancing, and protecting lithium-ion battery modules. Its safe and reliable operation is essential to ensure both aircraft-level safety and mission continuity.

6.1 System Description

The BMS performs several key functions:

- Monitoring cell voltages, temperatures, and currents.
- Controlling contactors to connect/disconnect packs.
- Managing charge and discharge cycles to optimize performance and life.

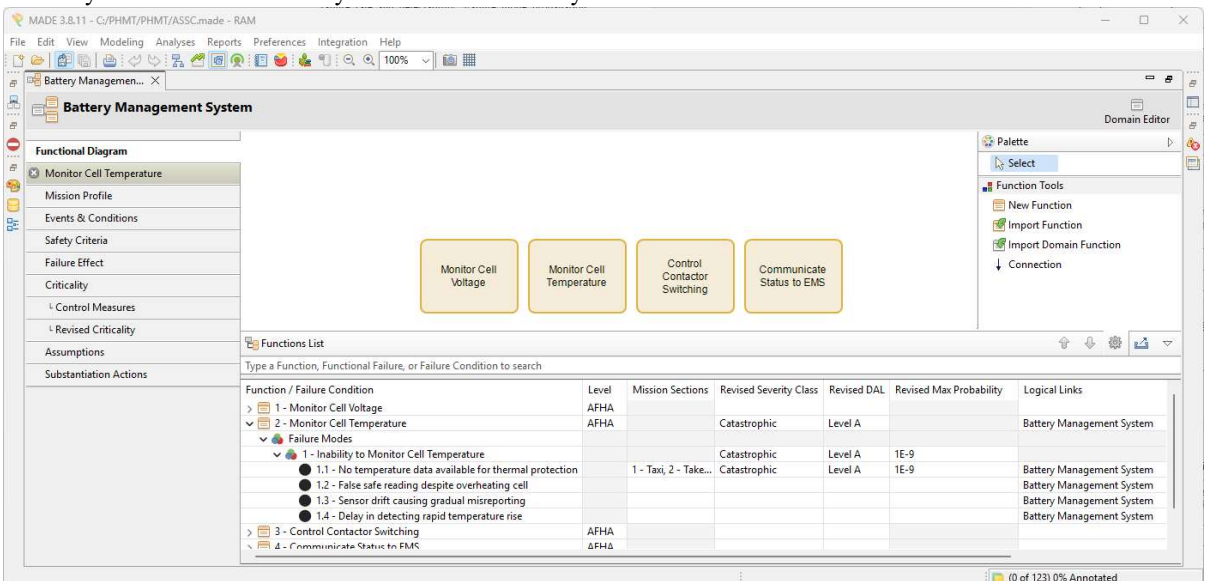


Figure 1: FHA - Battery Management System

- Detecting and mitigating abnormal conditions such as thermal runaway, over-voltage, or short-circuit.
- Communicating with higher-level energy management systems.

Given its role, BMS failures can propagate rapidly to catastrophic aircraft-level events such as loss of propulsion or onboard fire, making it an excellent candidate for demonstrating continuity between FHA and RAMS analyses.

6.2 Functional Hazard Assessment

The FHA begins with a high-level decomposition of BMS functions:

- Function 1: Monitor Cell Voltage
- Function 2: Monitor Cell Temperature
- Function 3: Control Contactor Switching
- Function 4: Communicate Status to EMS (Energy Management System)

For each function, failure conditions are identified:

- Loss of monitoring (undetected over-temperature).
- Erroneous measurement (false safe voltage reported).
- Untimely execution (delay in opening contactor during fault).
- Malfunction (contactors stuck closed).

Effects are then evaluated in the operational context of flight phases (take-off, cruise, landing). For example, "Loss of temperature monitoring" could result in undetected thermal runaway, classified as Catastrophic. "Erroneous voltage reporting" may lead to incorrect state-of-charge estimation, causing unexpected loss of power, classified as Hazardous.

Based on ARP4761A guidance, safety objectives are derived:

- Catastrophic FCs: $\leq 1 \times 10^{-9}$ per flight hour.
- Hazardous FCs: $\leq 1 \times 10^{-7}$ per flight hour.
- Major FCs: $\leq 1 \times 10^{-5}$ per flight hour.

6.3 Hazard-to-Architecture Mapping

The functional failures identified in the FHA are mapped to BMS architecture elements:

- Voltage monitoring → ADC circuitry, sensors, and microcontroller.
- Temperature monitoring → thermistors, signal conditioning circuits, software routines.
- Contactor control → driver circuits, relays, power electronics.
- Communication → CAN bus, transceivers, software protocol stack.

This mapping creates explicit traceability between functional hazards and the physical items responsible for implementing them. For example, the Catastrophic hazard "undetected thermal runaway" is linked to the temperature sensing chain, meaning its reliability must be verified at item level.

6.4 FMEA and Failure Mode Propagation

Using the model, MADE automatically generates an FMEA:

- *Failure Mode:* Thermistor open-circuit.
- *Local Effect:* Loss of temperature input to microcontroller.
- *Next Higher Effect:* BMS unable to detect cell overheating.
- *End Effect:* Undetected thermal runaway → Catastrophic.

Each FMEA entry preserves the severity classification from the FHA while adding reliability attributes such as failure rate and detectability. Failure mode propagation ensures that item-level failures are directly tied to system-level hazards.

6.5 Fault Tree Analysis (FTA)

The hazard "No temperature data available for thermal protection" is treated as a top event in a fault tree. The tool auto-populates contributing basic events:

- Temperature sensor failure (λ = 1.5 failures per million hour)

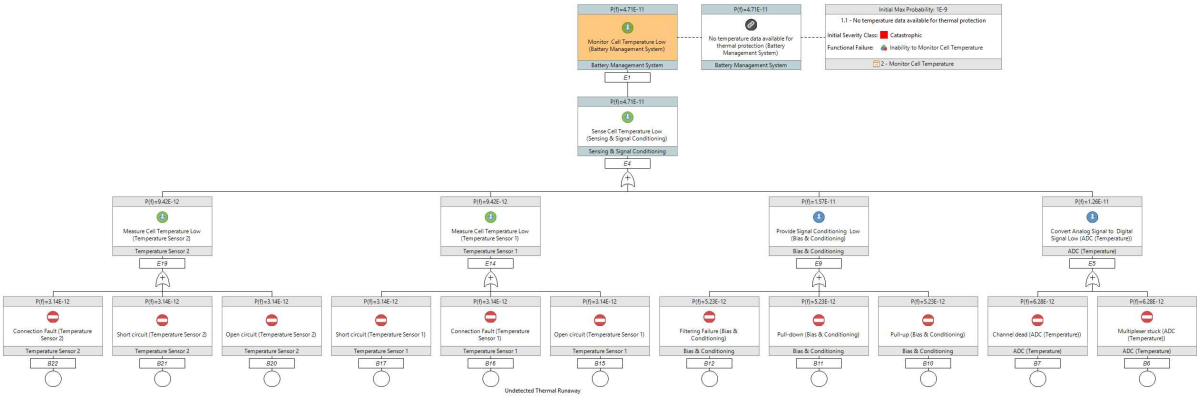
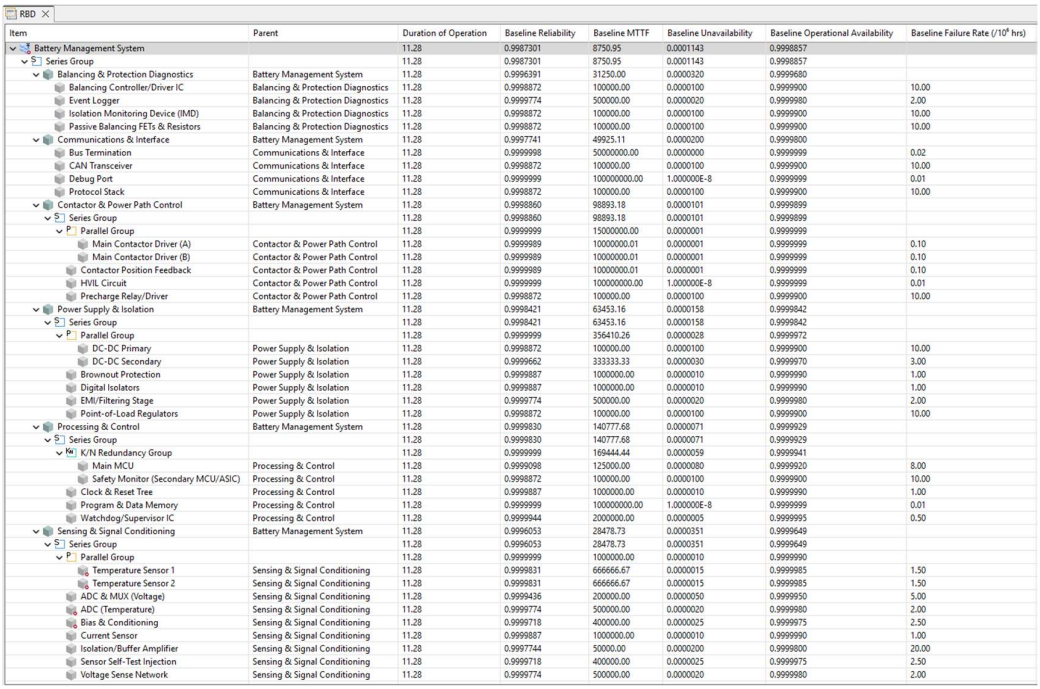


Figure 2: FTA - BMS Monitor Cell Temperature Failure



RBD

Item	Parent	Duration of Operation	Baseline Reliability	Baseline MTTF	Baseline Unavailability	Baseline Operational Availability	Baseline Failure Rate (/10^6 hrs)
Battery Management System		11.28	0.9987301	8750.95	0.0001143	0.9998857	
Series Group		11.28	0.9987301	8750.95	0.0001143	0.9998857	
Balancing & Protection Diagnostics	Battery Management System	11.28	0.9996391	31250.00	0.0000320	0.9999680	
Balancing Controller/Driver IC	Balancing & Protection Diagnostics	11.28	0.9998872	100000.00	0.0000100	0.9999900	10.00
Event Logger	Balancing & Protection Diagnostics	11.28	0.9999774	500000.00	0.0000020	0.9999980	2.00
Isolation Monitoring Device (IMD)	Balancing & Protection Diagnostics	11.28	0.9998872	100000.00	0.0000100	0.9999900	10.00
Passive Balancing FETs & Resistors	Balancing & Protection Diagnostics	11.28	0.9998872	100000.00	0.0000100	0.9999900	10.00
Communications & Interface	Battery Management System	11.28	0.9997741	49925.11	0.0000200	0.9999800	
Bus Termination	Communications & Interface	11.28	0.9999998	50000000.00	0.0000000	0.9999999	0.02
CAN Transceiver	Communications & Interface	11.28	0.9998872	100000.00	0.0000100	0.9999900	10.00
Debug Port	Communications & Interface	11.28	0.9999999	100000000.00	1.000000E-8	0.9999999	0.01
Protocol Stack	Communications & Interface	11.28	0.9998872	100000.00	0.0000100	0.9999900	10.00
Contactor & Power Path Control	Battery Management System	11.28	0.9998860	98893.18	0.0000101	0.9999899	
Series Group		11.28	0.9998860	98893.18	0.0000101	0.9999899	
Parallel Group		11.28	0.9999999	15000000.00	0.0000001	0.9999999	
Main Contactor Driver (A)	Contactor & Power Path Control	11.28	0.9999989	10000000.01	0.0000001	0.9999999	0.10
Main Contactor Driver (B)	Contactor & Power Path Control	11.28	0.9999989	10000000.01	0.0000001	0.9999999	0.10
Contactor Position Feedback	Contactor & Power Path Control	11.28	0.9999989	10000000.01	0.0000001	0.9999999	0.10
HVIL Circuit	Contactor & Power Path Control	11.28	0.9999999	100000000.00	1.000000E-8	0.9999999	0.01
Precharge Relay/Driver	Contactor & Power Path Control	11.28	0.9998872	100000.00	0.0000100	0.9999900	10.00
Power Supply & Isolation	Battery Management System	11.28	0.9998421	63453.16	0.0000158	0.9999842	
Series Group		11.28	0.9998421	63453.16	0.0000158	0.9999842	
Parallel Group		11.28	0.9999999	3564110.26	0.0000028	0.9999972	
DC-DC Primary	Power Supply & Isolation	11.28	0.9998872	100000.00	0.0000100	0.9999900	10.00
DC-DC Secondary	Power Supply & Isolation	11.28	0.9999662	333333.33	0.0000030	0.9999970	3.00
Brownout Protection	Power Supply & Isolation	11.28	0.9999887	1000000.00	0.0000010	0.9999990	1.00
Digital Isolators	Power Supply & Isolation	11.28	0.9999887	1000000.00	0.0000010	0.9999990	1.00
EMI/Filtering Stage	Power Supply & Isolation	11.28	0.9999774	500000.00	0.0000020	0.9999980	2.00
Point-of-Load Regulators	Power Supply & Isolation	11.28	0.9998872	100000.00	0.0000100	0.9999900	10.00
Processing & Control	Battery Management System	11.28	0.9999830	140777.68	0.0000071	0.9999929	
Series Group		11.28	0.9999830	140777.68	0.0000071	0.9999929	
K/N Redundancy Group		11.28	0.9999999	169444.44	0.0000059	0.9999941	
Main MCU	Processing & Control	11.28	0.9999098	125000.00	0.0000080	0.9999920	8.00
Safety Monitor (Secondary MCU/ASIC)	Processing & Control	11.28	0.9998872	100000.00	0.0000100	0.9999900	10.00
Clock & Reset Tree	Processing & Control	11.28	0.9999887	1000000.00	0.0000010	0.9999990	1.00
Program & Data Memory	Processing & Control	11.28	0.9999999	100000000.00	1.000000E-8	0.9999999	0.01
Watchdog/Supervisor IC	Processing & Control	11.28	0.9999944	2000000.00	0.0000005	0.9999995	0.50
Sensing & Signal Conditioning	Battery Management System	11.28	0.9996053	28478.73	0.0000351	0.9999649	
Series Group		11.28	0.9996053	28478.73	0.0000351	0.9999649	
Parallel Group		11.28	0.9999999	1000000.00	0.0000010	0.9999990	
Temperature Sensor 1	Sensing & Signal Conditioning	11.28	0.9999831	666666.67	0.0000015	0.9999985	1.50
Temperature Sensor 2	Sensing & Signal Conditioning	11.28	0.9999831	666666.67	0.0000015	0.9999985	1.50
ADC & MUX (Voltage)	Sensing & Signal Conditioning	11.28	0.9999436	200000.00	0.0000050	0.9999950	5.00
ADC (Temperature)	Sensing & Signal Conditioning	11.28	0.9999774	500000.00	0.0000020	0.9999980	2.00
Bias & Conditioning	Sensing & Signal Conditioning	11.28	0.9999718	400000.00	0.0000025	0.9999975	2.50
Current Sensor	Sensing & Signal Conditioning	11.28	0.9999887	1000000.00	0.0000010	0.9999990	1.00
Isolation/Buffer Amplifier	Sensing & Signal Conditioning	11.28	0.9997744	50000.00	0.0000200	0.9999800	20.00
Sensor Self-Test Injection	Sensing & Signal Conditioning	11.28	0.9999718	400000.00	0.0000025	0.9999975	2.50
Voltage Sense Network	Sensing & Signal Conditioning	11.28	0.9999774	500000.00	0.0000020	0.9999980	2.00

Figure 3: System Level Reliability Prediction Result

- ADC Failure ($\lambda = 2$ failures per million hour)
- Bias & Conditioning Failure ($\lambda = 2.5$ failures per million hour)

The fault tree structure allows quantification of the top event probability. With redundancy (e.g., dual temperature sensors per module), cut-set analysis shows that the probability of the No temperature data event is reduced to 4.71×10^{-11} failures per hour, satisfying the Catastrophic hazard objective.

6.6 Reliability Block Diagram (RBD)

An RBD is derived from the architecture, showing series/parallel relationships among BMS elements:

- Monitoring chain (sensors, ADCs, microcontroller).
- Contactor actuation chain (drivers, relays).
- Communication subsystem.

The RBD allows mission reliability evaluation over the duration of a typical flight. For example, the BMS reliability for a 11.28-hour mission is calculated at 0.9987301 given current MTTF values. Allocations ensure this exceeds the threshold derived from the FHA classification of Major and Hazardous FCs.

6.7 Reliability Allocation and Verification

Quantitative allocations are made from top-level safety objectives:

- "Loss of monitoring" allocated budget.
- Split across sensor chain, processing chain, and software, each item is allocated reliability equally.

Verification:

- Supplier failure data indicates temperature sensor at $\lambda = 15$ failures per million hours (not compliant).
- Solution: introduce sensor redundancy + diagnostics.
- Updated allocation demonstrates compliance with FHA-derived probability objectives.

This illustrates how the unified approach supports early identification of weaknesses and design iteration.

6.8 Results and Observations

The integrated modelling approach demonstrated clear, tangible benefits in the case study. The most significant outcome was the early identification of an architectural weakness in the temperature sensing chain. When quantitative reliability data from suppliers was incorporated into the allocation model, it became evident that the baseline thermistor failure rate ($\lambda = 15$ failures per million hours) exceeded the allocated budget derived from the Catastrophic hazard classification in the FHA. This discrepancy highlighted that the system, as initially designed, could not meet the required safety objective of $\leq 1 \times 10^{-9}$ per flight hour for undetected thermal runaway.

Because the FHA, allocation, FTA, and RBD analyses were all integrated in a common model, the weakness was revealed systematically and traceably, rather than being buried in separate documents. The model showed how a single thermistor failure could propagate to the top event in the FTA and compromise mission reliability in the RBD. This prompted the introduction of dual-sensor redundancy and diagnostic cross-checks, which reduced the probability of undetected thermal runaway to 4.71×10^{-11} per flight hour, thereby restoring compliance.

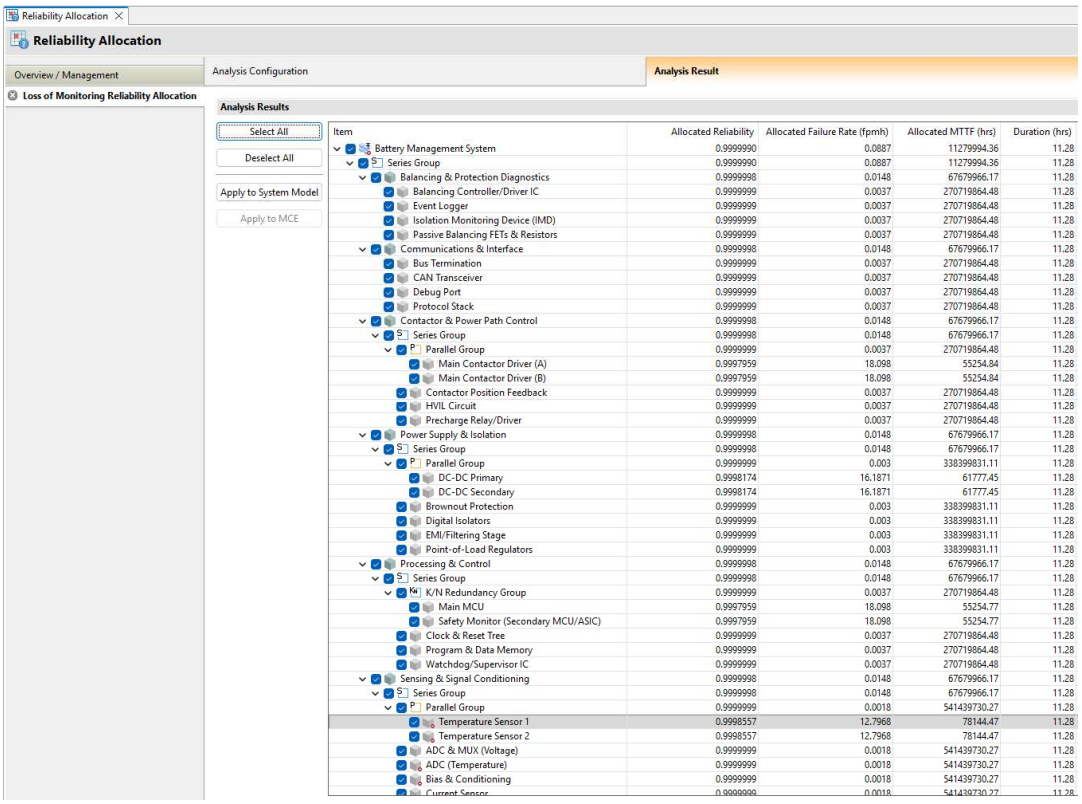


Figure 4: System Level Reliability Allocation Result

In a traditional, document-centric process, this weakness might have been missed or discovered much later. FMEAs, FTAs, and reliability predictions are often created by different teams, with hazard objectives referenced only indirectly. As a result, the misalignment between supplier failure data and FHA-derived safety budgets could easily have gone unnoticed until final verification, at which point design changes would have been far more costly. The integrated approach therefore not only ensured compliance but also enabled cost-effective design iteration at an early stage.

7 Discussion

The case study illustrates how the unified modelling approach delivers measurable improvements in continuity, transparency, and efficiency of the safety assurance process. Beyond the specifics of the Battery Management System example, the method highlights several broader implications for system safety and reliability engineering practice.

7.1 Benefits Over Traditional Methods

One of the clearest benefits is the elimination of duplication. Traditionally, hazard analyses, FMEAs, FTAs, and RBDs are produced as separate artefacts, often re-deriving the same information with the risk of introducing inconsistencies. By generating these artefacts from a single digital model, duplication is avoided, and consistency is preserved. This directly addresses one of the persistent challenges identified in Section 3.

The approach also improves transparency. Every safety objective identified in the FHA is traceable through to reliability allocations, quantitative analyses. This creates a clear assurance chain that is auditable by regulators and comprehensible to stakeholders. In a certification environment where credibility of evidence is paramount, this traceability significantly strengthens the assurance argument.

Another benefit is agility. Because artefacts are dynamically updated, engineers can rapidly explore architectural alternatives and immediately observe their impact on safety compliance. In contrast, traditional methods often require weeks of manual rework to reflect even minor design changes, limiting the ability to make informed trade-offs early in the lifecycle.

Finally, the approach supports lifecycle continuity. The digital model can absorb updates from production and in-service phases, ensuring that assurance evidence remains current. This aligns with the closed-loop reliability principles of GEIA-STD-0009 and extends the utility of ARP4761A analyses beyond certification milestones.

7.2 Challenges and Limitations

Despite these advantages, several challenges must be acknowledged.

- **Data Fidelity:** The accuracy of quantitative verification depends on the quality of failure rate data, which is often uncertain or unavailable in early stages. While allocations can highlight weak areas, true compliance may remain unverified until test or field data become available.

- **Tool Adoption:** Shifting from document-centric to model-based assurance requires investment in tools, training, and cultural change. Organizations accustomed to spreadsheet-driven processes may face resistance in adopting model-based practices.
- **Integration Across Disciplines:** Safety engineers, reliability engineers, and maintainers often operate in silos. A unified modelling approach requires tighter collaboration and shared ownership of the model, which may challenge existing organizational structures.
- **Complexity Management:** For very large systems, maintaining a fully integrated digital model can itself become complex. Appropriate modularisation, libraries, and abstraction techniques are necessary to prevent the model from becoming unwieldy.

These challenges do not negate the value of the approach but underscore the need for careful planning and incremental adoption.

7.3 Implications for Industry Practice

The broader implication is a shift toward assurance as a continuous activity rather than a sequence of disconnected deliverables. With increasing system complexity particularly in electrification, autonomy, and highly integrated avionics, fragmented approaches will struggle to maintain credibility. Unified modelling allows assurance to scale with complexity by reducing manual effort and ensuring consistency across domains.

However, adoption will require organizations to rethink not only their tools but also their workflows and responsibilities. Safety and reliability engineers must collaborate around a shared model, supported by strong configuration management and governance. Early adopters may experience initial overheads, but the long-term efficiency gains and reduction in certification risk provide a compelling incentive.

8 Conclusion

This paper has proposed a unified modelling approach that bridges the long-standing divide between Functional Hazard Assessment (FHA) and downstream Reliability, Availability, Maintainability, and Safety (RAMS) analyses. By embedding FHA outputs directly into a digital system model, the method enables bidirectional traceability, alignment of qualitative hazard classifications with quantitative reliability metrics, and dynamic consistency checks as designs evolve.

The case study on a Battery Management System demonstrated how the approach strengthens assurance by providing a transparent chain of evidence from hazard identification to quantitative verification. Architectural weaknesses were detected early, corrective actions were evaluated systematically, and diagnostic strategies were optimised to support closed-loop reliability management. The results confirmed that the method improves transparency, reduces duplication of effort, and sustains assurance evidence across the system lifecycle.

Importantly, the approach does not displace existing guidelines/standards but rather operationalises their intent. ARP4761A's structured safety assessment process and GEIA-STD-0009's reliability program principles are reinforced through a model-based environment, creating a living assurance artefact that remains credible from concept through in-service operation.

Future work will extend the proposed method along three strategic directions. First, tighter integration with both Model-Based Systems Engineering (MBSE) and digital twin technologies will provide end-to-end continuity across the lifecycle. MBSE offers the design-time system model, defining architectures, functions, and failure logic in a rigorous and traceable way. Digital twins, by contrast, extend these models into operations, synchronising them with real-time sensor and usage data so that hazard probabilities and reliability predictions remain valid under actual conditions. Together, they will transform assurance from a static, certification-driven activity into a dynamic, continuously updated capability. Second, the development of automated assurance metrics and dashboards will allow proactive monitoring of compliance, providing early warnings when design changes or in-service data threaten to erode safety margins. Third, formal engagement with certification authorities will be essential to establish acceptable practices for model-based evidence, ensuring regulatory recognition of digital continuity in safety assurance. These extensions will not only strengthen technical rigor but also create the ecosystem necessary for widespread adoption of unified, model-based safety and reliability practices.

In an era of rapidly increasing system complexity and regulatory scrutiny, unified modelling offers a robust and agile foundation for system assurance. By aligning FHA and RAMS activities within a common digital knowledge base, the approach represents a decisive step toward safer, more reliable, and more certifiable systems.

9 References

- SAE International (2023). *ARP4761A: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. Warrendale, PA: SAE International.
- SAE International (2020). GEIA-STD-0009: *Reliability Program Standard for System Design, Development and Manufacturing.*
- FAA (2002). *Advisory Circular AC 25.1309-1A: System Design and Analysis*. Washington, DC: Federal Aviation Administration.
- Kritzinger, D. (2017). *Aircraft System Safety: Assessments for Initial Airworthiness Certification*. 2nd ed. Oxford: Butterworth-Heinemann.