aerospace

MDPI

Article

Integrating Computer-Aided Design and Model-Based Systems Engineering for Early Zonal Hazard Analysis: Application to a Supersonic Aircraft Fuel System

Ayush Kamboj * and Yicheng Sun

Faculty of Engineering and Applied Sciences, Cranfield University, Bedford MK43 0AL, UK; yicheng.sun@cranfield.ac.uk

* Correspondence: mdkayushkamboj@gmail.com

Abstract

The development of supersonic aircraft presents significant challenges in ensuring safety during early design stages, particularly for fuel tank systems exposed to extreme thermal and structural loads. Conventional document-based zonal safety analysis methods are limited in their ability to capture dynamic interactions between spatial subsystem configurations and functional system behavior during early conceptual design, leading to delayed hazard identification. This study proposes an integrated framework combining computer-aided design (CAD) and model-based systems engineering (MBSE) to support early-stage zonal hazard analysis. The framework links spatial subsystem modelling with functional system architecture to enable iterative hazard identification and mitigation. Applied to the SA-24 Phoenix conceptual supersonic aircraft, the approach identifies critical risks, including fuel vaporization, over-pressurization, and structural fatigue, and evaluates mitigation strategies such as thermal insulation and redundant venting. Functional hazard analysis and fault tree analysis are used to assess failure scenarios and ensure compliance with EASA CS-25 requirements. Results indicate an estimated reduction of up to 40% in risk priority number (RPN) values for key thermal hazard pathways and a 25% reduction in conceptual design iteration time compared with conventional approaches. The findings demonstrate that CAD–MBSE integration offers a scalable and efficient methodology for early hazard identification, contributing to safer and more reliable supersonic aircraft design.

Keywords: model-based systems engineering (MBSE); 3DEXPERIENCE; computer-aided design; fault tree analysis; functional hazard analysis; zonal safety analysis; EASA; SA-24; fuel systems; supersonic aircraft

Check for updates

Received: 1 April 2026
Revised: 24 April 2026
Accepted: 25 April 2026
Published: 28 April 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

1.1. Background

Supersonic travel has long represented a significant milestone in aerospace engineering, offering substantial reductions in travel time across long-distance routes. Following the retirement of Concorde in 2003, renewed interest in commercial supersonic transport has been driven by advances in aerodynamics, materials, and propulsion technologies [1–3]. Modern supersonic aircraft concepts aim to address the limitations of earlier designs, including high fuel consumption, sonic boom impact, and operational inefficiency [1,2]. The SA-24 Phoenix, a conceptual supersonic airliner, reflects these advances by integrating low-boom aerodynamic shaping with advanced systems engineering approaches to achieve efficient high-speed performance.

A critical aspect of supersonic aircraft design is the safe and efficient operation of fuel tank systems. At high Mach numbers, these systems are exposed to elevated thermal loads, structural stresses, and complex subsystem interactions [3,4]. Conventional zonal safety analysis (ZSA) methods have been widely applied in subsonic aircraft; however, their application to supersonic configurations is constrained by increased system coupling and dynamic operational environments [5,6].

1.2. Challenges in Supersonic Aircraft Design

The design of supersonic aircraft introduces challenges not typically encountered in subsonic systems. The increasing complexity of modern aircraft architectures has encouraged the adoption of model-based systems engineering approaches during conceptual aircraft design to improve subsystem integration and design traceability [7]. These effects are further compounded by strong interdependencies between aircraft subsystems, which make hazard identification more complex during early design stages.

Traditional ZSA approaches rely heavily on detailed design data and static documentation, limiting their effectiveness in conceptual design environments where system configurations are still evolving [4,6]. Consequently, hazards are often identified only at later stages of development, leading to increased redesign costs and heightened safety risk.

The integration of advanced digital engineering tools, such as computer-aided design (CAD) and model-based systems engineering (MBSE) offers a promising solution to these challenges. CAD enables detailed spatial modelling and thermal analysis, while MBSE facilitates dynamic modelling of system behavior and interactions [8–10]. Used in combination, these tools support early-stage hazard identification and iterative design optimization.

1.3. Research Objectives

This paper aims to achieve the following objectives:

- Develop a robust framework for integrating CAD and MBSE to facilitate early-stage zonal hazard analysis.
- Apply the framework to the fuel tank system of the SA-24 supersonic aircraft.
- Identify potential hazards, including fuel leakage, over-pressurization, and ignition risks, and propose mitigation strategies.
- Validate the proposed approach through comparative analysis with conventional ZSA methods.
- This study contributes to the advancement of aerospace safety by establishing scalable methodologies for model-driven hazard analyses.

The hypothesis of the study was that integrating CAD with MBSE can improve early-stage zonal hazard identification compared with the use of conventional document-based ZSA. This hypothesis was evaluated through a case study on the SA-24 Phoenix supersonic aircraft using functional hazard analysis (FHA), fault tree analysis (FTA), and failure modes and effects analysis (FMEA).

While the integration of CAD and MBSE has been explored in the broader context of digital engineering and digital twin frameworks, the contribution of this study lies in its application to early-stage zonal hazard analysis in conceptual aircraft design. The proposed framework integrates spatial subsystem modeling with functional hazard analysis methods, including FHA, FMEA, and FTA, to enable systematic identification of subsystem interaction risks during the conceptual design phase. This represents an application-driven extension of existing model-based engineering approaches, tailored to safety-critical aerospace systems.

1.4. Scope of the Study

This study focused on the conceptual design phase of the SA-24 supersonic aircraft, specifically its fuel tank subsystem. The study includes:

- Development of CAD models for the spatial design of the fuel tank.
- Functional and behavioral analysis using MBSE tools.
- Iterative hazard identification and mitigation within defined aircraft zones.
- Exclusion of post-production, certification, and in-service assessments.

The findings are intended to inform both academic and industrial stakeholders and contribute to the development of safer and more efficient supersonic aircraft.

1.5. Paper Structure

The rest of this paper is organized as follows: Section 2 presents existing methodologies, including ZSA and MBSE–CAD integration, highlighting gaps in current practices. Section 3 (methodology) details the model-driven framework developed for integrating CAD and MBSE tools. This is followed by case studies, where the proposed CAD–MBSE hazard analysis framework is applied to the SA-24 Phoenix fuel tank system. Section 5 presents the results of the proposed framework; findings are subsequently interpreted against the existing literature in the discussion, before key insights and directions for future research are drawn together in the conclusion Section 5.10.

2. Literature Review

A supersonic aircraft represents the pinnacle of aerospace engineering, designed to exceed the speed of sound (Mach 1) while maintaining aerodynamic stability, fuel efficiency, and passenger comfort. However, the development of such aircraft has historically faced challenges in terms of balancing performance with safety, economic viability, and environmental impact. The Concorde and Tupolev Tu-144 were the first commercial supersonic aircraft, proving the feasibility of supersonic transport; however, some critical limitations were exposed, including high fuel consumption, limited range, and excessive noise pollution from sonic booms [1].

Recent advancements in materials, propulsion systems, and aerodynamic design have attracted interest in supersonic flight. NASA's X-59 QueSST project, for example, addresses noise pollution concerns by focusing on low-boom supersonic travel and leveraging cutting-edge designs and technology to minimize sonic boom disturbances [2]. Similarly, Boom Supersonic's Overture Aircraft aims to combine speed and sustainability through innovative aerodynamics and the adoption of sustainable aviation fuel (SAF) [11]. These modern approaches underscore the industry's commitment to addressing the environmental and operational challenges of supersonic travel.

The SA-24 Phoenix, a conceptual supersonic transport aircraft, was designed to overcome these challenges by integrating advanced safety systems, such as ZSA, and employing state-of-the-art tools such as CAD and MBSE. With a passenger capacity of 50 and a cruising speed of Mach 1.8, SA-24 aims to demonstrate advanced approaches to supersonic safety, efficiency, and regulatory compliance. Previous conceptual design studies on low-boom supersonic transport aircraft have demonstrated the importance of multidisciplinary optimisation in achieving performance and regulatory compliance [12].

2.1. Zonal Safety Analysis Framework in Conceptual Design

Recent studies have explored the integration of MBSE approaches within aircraft fuel system development to improve subsystem coordination and maintenance-oriented system analysis during early design stages [13]. Unlike conventional system-specific safety analyses, the ZSA examines potential hazards within specific aircraft zones, focusing on

how subsystem interactions and environmental factors contribute to safety risks [5]. For instance, fuel tanks placed near high-temperature zones or electrical systems pose inherent risks such as vapor ignition or leakage.

The ZSA methodology involves identifying hazards, assessing their likelihood and impact, and implementing mitigation measures [5,6]. The ZSA aligns closely with regulatory frameworks, such as EASA CS-25 and FAA Part 25, which emphasize the need for redundancy, fault tolerance, and safe design practices [14]. By integrating ZSA during the early stages of design, engineers can proactively address spatial safety concerns, ensuring compliance with airworthiness standards.

The ZSA is applied in aerospace engineering to assess fuel systems, environmental control systems (ECSs), and avionics. For example, Airbus employs ZSA to evaluate the placement of fuel lines relative to electrical wiring, thereby minimizing fire risks in the A320neo series [15]. Similarly, Boeing's use of ZSA, combined with digital twin simulations, enables the prediction and mitigation of subsystem failures in the 787 Dreamliner [16]. However, conventional ZSA methodologies often rely on expert judgment and static diagrams, thereby limiting their scalability. Integrating the ZSA with tools, such as CAD and MBSE, can help address these challenges by enabling dynamic simulations and iterative hazard assessments.

2.2. Fundamentals of Model-Based Systems Engineering (MBSE)

MBSE facilitates the representation and simulation of the functional, behavioral, and structural aspects of systems through a model-driven approach [8,9]. By shifting away from document-based processes, MBSE enables engineers to dynamically simulate interactions between subsystems, thereby providing a holistic view of aircraft performance and safety. Tools, such as the Cameo Systems Modeler and Enterprise Architect, are instrumental in creating digital twins of complex systems, which can then be used to evaluate the performance under a variety of operational scenarios [10].

For SA-24 Phoenix, MBSE enables dynamic hazard analyses, such as simulating fuel vaporization scenarios caused by thermal expansion or failures in fuel system venting. Recent MBSE research has emphasized the digitalization of aircraft design processes through improved integration between requirements management, system architecture models, and engineering workflows [17]. Moreover, the ability of MBSE to trace requirements to functional and structural models ensures compliance with regulatory standards, thereby enhancing the overall design process.

2.3. Conceptual CAD Modeling in Aircraft Design

CAD tools, such as computer-aided three-dimensional interactive application (CATIA) and 3DEXPERIENCE, allow engineers to design, visualize, and simulate the spatial configurations of aircraft systems [3,4]. For supersonic aircraft, such as the SA-24 Phoenix, CAD is indispensable for analyzing thermal loads, structural stresses, and spatial constraints, particularly in high-risk zones such as fuel tanks [4]. The capability to model complex geometries and simulate environmental conditions allows engineers to optimize designs for both performance and safety [3,4].

MBSE-based aircraft architecting approaches enable structured requirement analysis and system-level integration during conceptual aircraft development [18]. CAD enables interference checks between systems, ensuring that components, such as venting mechanisms, sensors, and pipelines, are optimally positioned to minimize risk. Beyond spatial modeling, CAD also supports material analysis, allowing engineers to select materials that can withstand the high temperatures and pressures associated with supersonic flight.

2.4. Integration of CAD and MBSE Models

The integration of CAD and MBSE represents an increasingly important approach in conceptual aircraft design and multidisciplinary aerospace system development [19,20], combining spatial subsystem representation with functional system analysis. Recent studies have demonstrated the broader applicability of MBSE methodologies across aircraft lifecycle activities, including maintenance planning and operational optimization [21].

This integration also facilitates iterative analyses, allowing for real-time adjustments to the design. For instance, if a CAD model identifies thermal hotspots in a fuel tank, the MBSE can simulate the impact of these hotspots on system behavior, such as fuel vaporization and venting efficiency. By iterating between these tools, engineers can proactively optimize the design and address hazards. In addition, the combination of CAD and MBSE supports the creation of comprehensive safety reports, which can be used to streamline regulatory approval and enhance stakeholder communication.

2.5. Applications in Supersonic Aircraft Design

Supersonic aircraft require innovative safety and design methodologies due to their extreme operational environments. Historical examples, such as the Concorde, underscore the importance of robust safety frameworks, particularly in zones prone to cascading failures, such as fuel systems [22]. The lessons learned from the Concorde's fuel tank issues, including incidents of structural compromise during high-speed operations, highlight the necessity for advanced tools for hazard identification.

Modern projects, such as NASA's X-59 and Boom Supersonic Overture, illustrate how advanced digital tools, such as CAD and MBSE, enhance safety and efficiency. These projects integrate early-stage safety analyses into their workflows to ensure that hazards are identified and mitigated before physical prototypes are built. SysML-based MBSE approaches have increasingly been applied in aviation system design to support functional modeling, system architecture development, and requirement traceability [23]. The ability to model and simulate real-world conditions before manufacturing reduces costs and enhances design confidence, particularly in novel aircraft configurations.

2.6. Environmental Considerations

The environmental impact of supersonic aircraft is a major concern, particularly in terms of noise pollution and greenhouse gas emissions. Innovations in low-boom technology, such as those implemented in the NASA X-59 project, have addressed noise concerns by significantly reducing the intensity of sonic booms [24]. These advancements have paved the way for a broader public acceptance of supersonic transport.

The adoption of SAF is another critical step toward reducing the environmental footprint of supersonic flights. SAF offers a viable alternative to conventional jet fuels, reduces lifecycle greenhouse gas emissions, and aligns with global sustainability goals [11]. Integrating SAF into the SA-24 Phoenix design not only enhances environmental credentials, but also ensures compliance with evolving regulatory requirements.

2.7. Gaps in Current Zonal Hazard Analysis Techniques

Despite the significant progress in aerospace safety methodologies, notable gaps remain in the literature. Most studies focused on CAD and MBSE as standalone tools, neglecting their combined application in comprehensive safety analyses [8,19]. Further, the lack of standardized protocols for integrating these tools poses challenges to their widespread adoption.

This study aimed to address these gaps by proposing a unified framework tailored for supersonic aircraft, specifically focusing on the fuel tank system of SA-24 Phoenix.

By leveraging the strengths of CAD and MBSE, the proposed framework seeks to help proactively identify hazards, optimize design efficiency, and enhance compliance with safety regulations.

In parallel with model-based approaches, recent studies have explored data-driven fault diagnosis techniques using machine learning to identify and predict system failures in complex engineering systems. Approaches such as explainable artificial intelligence and transfer learning-based fault diagnosis have demonstrated effectiveness in capturing nonlinear system behavior and improving fault detection accuracy. However, these methods typically rely on large datasets and are more applicable to operational or post-design phases.

In contrast, the present study focuses on model-based hazard identification during the conceptual design phase, where system data are limited. Therefore, data-driven and model-based approaches can be considered complementary, with potential integration in future digital engineering frameworks for enhanced lifecycle safety analysis [25–27].

2.7.1. Limitations of Conventional Zonal Safety Analysis

Conventional ZSA methodologies primarily focus on evaluating hazards associated with subsystem installations within predefined aircraft zones. However, these methods often rely on the manual interpretation of engineering drawings and system documentation, which may limit their ability to fully capture the complex interactions between aircraft subsystems.

The separation between spatial subsystem models and system architecture representations can make it difficult to identify hazards arising from the interaction between component placement and system behavior. As aircraft systems become more tightly integrated, these limitations highlight the need for modeling frameworks that combine geometric subsystem configurations with system architecture modeling.

2.7.2. Regulatory Evolution in Supersonic Aircraft Certification

Aircraft certification frameworks are continuously evolving to address emerging aircraft technologies and operational concepts. Conventional large-transport aircraft certification has historically been governed by regulations, such as the European Union Aviation Safety Agency Certification Specification CS-25, which defines airworthiness standards for transport category aircraft. However, renewed interest in commercial supersonic transport has prompted regulatory authorities to develop updated certification requirements that specifically address the design and operation of supersonic aircraft.

The forthcoming European Union Aviation Safety Agency Certification Specification CS-25 Amendment 27 is expected to introduce additional guidelines related to supersonic aircraft performance, environmental impact, and safety considerations. These developments reflect the increasing complexity of advanced aircraft architectures and the need for more integrated safety analysis during early design stages.

Early-stage hazard identification frameworks that combine CAD and MBSE have the potential to support these evolving certification processes by enabling engineers to identify subsystem interaction risks during conceptual design. Integrating spatial system models with functional system architectures can help improve traceability between design decisions and safety requirements, thereby facilitating more efficient safety validation during certification activities.

2.8. Concluding Remarks

Integrating CAD and MBSE can help significantly enhance ZSA processes in aerospace design. However, most existing studies have examined these tools independently rather than as an integrated framework for early hazard identification during conceptual aircraft

design. This gap is particularly important for complex systems, such as supersonic aircraft fuel tanks, where spatial subsystem interactions can introduce cascading safety risks.

To address this limitation, this paper proposes an integrated CAD–MBSE modeling framework to conduct early-stage zonal hazard analysis and dynamic safety analysis during conceptual aircraft design. The framework was applied to the fuel tank system of the SA-24 Phoenix supersonic aircraft to demonstrate how spatial subsystem modeling and functional system architecture analysis can be combined to improve early hazard detection and mitigation. By demonstrating the feasibility of this methodology for supersonic aircraft, this study provides a scalable framework for designing safety-critical systems. The findings will contribute toward advancing the field of aerospace engineering by ensuring both safety and sustainability of future supersonic transport.

3. Methodology

3.1. Research Design

The methodology used in this study integrates CAD and MBSE into a unified framework for ZSA. This approach is specifically tailored for the SA-24 Phoenix supersonic aircraft, focusing on the safety and performance of its fuel tank system. By leveraging the precise spatial capabilities of CAD and the dynamic functional insights of MBSE, the methodology enables comprehensive hazard identification, design optimization, and compliance with regulatory requirements such as EASA CS-25 [14]. This structured framework emphasizes an iterative design and analysis, allowing for the seamless incorporation of safety considerations throughout the development process.

The CAD and MBSE tools employed in this study were used during the conceptual aircraft design phase to support early hazard identification, rather than to provide formal certification. In accordance with established aerospace safety assurance frameworks, such as RTCA DO-178C, the software used during the conceptual design typically operates at a lower assurance level, not as certified flight-critical software. Therefore, the modeling tools utilized in this research correspond conceptually to a Design Assurance Level C equivalent, which is appropriate for analytical tools used to support hazard identification and design exploration, rather than direct certification verification. The software tools and their corresponding conceptual assurance levels used in this study are summarized in Table 1.

Table 1. Software assurance context for digital engineering tools.

Tool Category	Software Used	Software Version	Function	Conceptual Assurance Context
Computer-aided design tool	Computer-aided three-dimensional interactive application (CATIA)	V5-6R2023	Geometric modeling and thermal analysis	Conceptual design analysis (Design Assurance Level C equivalent)
Model-based system engineering tool	Cameo systems modeler	2021	Functional architecture modeling and system interaction analysis	Conceptual design analysis (Design Assurance Level C equivalent)
Digital engineering platform	3DEXPERIENCE platform	R2023	Integration of Computer-Aided Design and system modeling environments	Conceptual design modeling support

All the CAD and MBSE analyses were conducted using the Dassault Systèmes and MBSE modeling tools available at Cranfield University. The modeling activities were conducted using CATIA V5-6R2023 within the 3DEXPERIENCE R2023x platform environment and Cameo Systems Modeler 2021, representing the software configuration available through the Cranfield University Digital Engineering Laboratory. Modeling tools were used to support conceptual design analysis and hazard identification activities rather than certification-grade verification simulations. The conceptual design framework adopted in this study is aligned with the GENUS multidisciplinary aircraft design environment developed at Cranfield University [28].

3.2. Preliminary System Definition

The first step in this methodology involves defining the scope of the system, the operational parameters, and the constraints. This process begins with an extensive review of existing data on supersonic aircraft, such as the Concorde and Boom Supersonic Overture, to identify design principles and historical challenges. Regulatory standards, including EASA CS-25 [29], were analyzed to establish safety benchmarks relevant to fuel tank systems. This ensures that the design adheres to industry norms, while addressing the unique challenges associated with supersonic flight.

The mapping of critical components, such as fuel pipelines, venting systems, and structural insulation, forms a core part of this phase. The interdependencies between the fuel tank and other subsystems, such as propulsion and environmental controls, were identified to ensure that these interactions did not introduce new risks. Performance metrics, including thermal resilience, structural integrity, and fuel efficiency, were also defined at this stage. These metrics guide the subsequent design and safety analysis processes to ensure the alignment of functional and safety objectives.

3.3. CAD Model Development

In the second phase, detailed CAD models of the fuel tank system were developed using the 3DEXPERIENCE platform. This phase focused on creating accurate geometric representations of the system and simulating its performance under real-world conditions. The design process incorporates spatial constraints within the aircraft fuselage and ensures the optimal placement of components for operational and maintenance efficiency.

Thermal simulations showed that the fuel temperature remained within acceptable conceptual operating limits during the analyzed supersonic cruise conditions. This analysis identifies potential vulnerabilities, such as material fatigue or thermal expansion, which can compromise the integrity of the system.

The thermal simulations conducted in this study represent a first-order conceptual thermal assessment intended to evaluate potential subsystem thermal interactions during early aircraft design. The thermal boundary conditions applied in the model were derived from representative aerodynamic heating estimates reported in the literature for a supersonic transport aircraft operating in the Mach 1.5–1.8 flight regime.

To provide a clearer physical basis for the conceptual thermal analysis, simplified governing relations were considered. These relations are presented as simplified governing equations used for first-order conceptual hazard analysis during early-stage aircraft design. Heat conduction within structural materials can be expressed as:

$$q = -k \nabla T \tag{1}$$

where q represents heat flux, k is the thermal conductivity, and ∇T is the temperature gradient. Convective heat transfer between the aircraft surface and surrounding airflow can be approximated as:

$$q = hA\left(T_{\{surface\}} - T_{\{fluid\}}\right) \tag{2}$$

where h is the convective heat transfer coefficient and A is the exposed surface area.

In addition, fuel vapor behavior under elevated temperature conditions can be approximated using the ideal gas relation:

$$PV = nRT \tag{3}$$

The use of the ideal gas relation assumes a simplified closed-system behavior with uniform thermodynamic properties, which is appropriate for conceptual-level estimation but does not capture transient or non-ideal fluid effects. These first-order relations provide a conceptual basis for estimating thermal loads and pressure behavior within the fuel system during supersonic cruise conditions. It is noted that high-fidelity modelling using computational fluid dynamics or detailed thermodynamic analysis is beyond the scope of the present conceptual design study.

Typical supersonic transport aircraft operating at Mach numbers between 1.5 and 1.8 may experience external structural temperatures in the range of approximately 100–150 °C, depending on flight altitude and aerodynamic configuration [3].

The applied skin temperature range of approximately 110–130 °C therefore represents a simplified engineering approximation used to evaluate the influence of external structural heating on nearby fuel system components. These simulations were performed using CAD-based thermal modeling tools to support subsystem layout evaluation and hazard identification, rather than to provide high-fidelity aerodynamic heating predictions that would normally require a computational fluid dynamics (CFD) analysis.

The boundary conditions and modeling parameters used during the thermal simulation analysis are summarized in Appendix A.

Structural stress analyses complement these simulations by identifying and addressing weak points in the design. Spatial interference checks ensure that components, such as pipelines and sensors, are positioned to avoid mechanical conflicts, thereby enhancing the reliability and functionality of the system.

Multi-Fidelity Modeling Strategy

Aircraft design processes typically employ modeling approaches with progressively increasing fidelity as the design matures. During the conceptual design phase, low-fidelity parametric models are used to rapidly explore aircraft configuration options and identify potential interactions between subsystems. These models prioritize computational efficiency and design flexibility over high-precision numerical accuracy.

The CAD models developed in this study represent conceptual-level modeling fidelity appropriate for early hazard identification within the proposed CAD and MBSE frameworks. At this stage, the objective is to evaluate the spatial arrangements of the subsystems, identify potential hazard interactions between components, and support preliminary safety analysis activities.

As aircraft development progresses toward the preliminary and detailed design phases, modeling fidelity typically increases through the integration of higher-resolution simulations, such as structural finite element analysis, thermal simulations incorporating detailed material properties, and CFD analysis for aerodynamic and thermal validation. These higher-fidelity simulations enable a more accurate assessment of structural loads, aerodynamic heating effects, and system performance characteristics.

Therefore, the conceptual modeling framework presented in this research can serve as the initial stage within a broader multi-fidelity modeling workflow, where early design

decisions informed by CAD and MBSE models are progressively refined using higher-fidelity analysis techniques. The progression of modeling fidelity across different aircraft design stages is summarized in Table 2.

Table 2. Multi-fidelity modeling progression for aircraft design.

Design Phase	Modeling Fidelity	Typical Analysis Methods	Purpose
Conceptual design	Low fidelity	Parametric computer-aided design models and preliminary hazard analysis	Rapid design exploration and hazard identification
Preliminary design	Medium fidelity	Thermal simulations and structural finite element analysis	Validation of subsystem interactions and structural feasibility
Detailed design	High fidelity	Computational fluid dynamics and advanced thermal modeling	Detailed aerodynamic and thermal performance evaluation
Certification stage	Very high fidelity	Integrated system simulation and experimental validation	Final verification and certification compliance

3.4. MBSE Workflow Implementation

The third phase employed MBSE to create dynamic functional models of the fuel tank system. These models helped simulate the behavior of the system under both nominal and adverse conditions, providing valuable insights into its operational reliability. Conceptual digital twin models have been developed to represent the functional behavior of the fuel tank system, enabling engineers to simulate scenarios such as over-pressurization or venting failures.

MBSE facilitates the integration of regulatory compliance into the design process. By directly linking functional models to safety requirements, the methodology ensures that every aspect of the design aligns with the EASA CS-25 standards.

Tools, such as the FHA and FTA, were employed to simulate failure scenarios and assess cascading risks. This systematic approach ensured that potential hazards were identified and quantified in terms of their impact and likelihood.

Detailed fault tree analysis, failure modes and effects analysis, and functional hazard analysis models are provided in Appendices E–G.

3.4.1. System Architecture Modeling

The system architecture of the conceptual aircraft fuel system was represented using a system modeling language (SysML) within the MBSE environment. SysML models were used to describe the subsystem structure, functional behavior, and interfaces between the system components.

The architecture model captures the relationships between the major fuel system components, including fuel tanks, pumps, fuel transfer lines, and engine feed systems. Functional interactions between these components were represented through SysML block definition diagrams and internal block diagrams, enabling the analysis of the system behavior under various operational conditions.

These architectural models provide a structured representation of subsystem interactions that support the application of safety analysis techniques such as the FHA, FMEA, and FTA.

3.4.2. Hazard Modeling Integration

MBSE architecture models were used to support hazard identification activities by enabling the analysis of functional system behavior alongside subsystem interaction rela-

tionships. Hazard analysis techniques were applied within the MBSE framework to identify the potential failure propagation pathways and subsystem dependencies.

By linking functional system architecture models with the spatial subsystem configuration developed in a CAD environment, the modeling framework allows hazard interactions caused by subsystem placement or structural integration to be identified earlier in the design process.

This integrated modeling approach supports more comprehensive hazard identification than conventional document-based safety assessment workflows.

3.4.3. Conceptual Digital Twin Framework

Digital twin concepts are increasingly being applied in aerospace digital engineering environments to represent the structure and behavior of complex engineering systems. A digital twin can be generally defined as a virtual representation of a physical system that integrates system models, simulation capabilities, and, in advanced implementations, operational data to support engineering analysis and lifecycle management.

The maturity of digital twin implementations is commonly classified using reference frameworks, such as the DIN 91345 digital twin model, which describes progressive levels of digital system representation, ranging from static geometry models to fully integrated cyber-physical systems that interact with operational data streams.

The modeling framework developed in this study integrates CAD geometry models with the MBSE system architecture models to represent both spatial subsystem configuration and functional system interactions within a conceptual aircraft design environment. This integration enables simulation-supported hazard identification during early design stages, allowing potential subsystem interaction risks to be evaluated before a detailed aircraft design is completed.

Although the proposed modeling framework incorporates physics-based modeling assumptions, including thermal load estimation and subsystem interaction analysis, it does not incorporate real-time operational data from physical aircraft platforms. Consequently, the modeling environment should be interpreted as a conceptual digital twin framework rather than as a fully operational digital twin implementation.

Within the context of the DIN 91345 maturity classification, the modeling approach developed in this study demonstrated characteristics associated with intermediate digital twin maturity levels, where system architecture models and simulation capabilities were integrated to support the engineering analysis. However, the absence of operational sensor data and real-time system monitoring limits the framework to conceptual digital twin capabilities.

Future research can extend the proposed framework by integrating operational aircraft data streams, real-time system monitoring, and closed-loop simulations between physical aircraft systems and their digital representations. Such an integration would enable the development of fully operational digital twin environments capable of supporting predictive maintenance and real-time safety analyses of aircraft systems. The classification of digital twin maturity levels and their relevance to the present study are summarized in Table 3.

3.5. Integration of CAD and MBSE

The integration of CAD models with MBSE architectures enables a unified representation of the spatial subsystem configuration and functional system behavior during early aircraft design stages. Conventional aircraft safety analysis methods typically rely on separate documentation-based workflows, where system architecture models and geometric subsystem layouts are analyzed independently. This separation can delay the identification of spatial hazard interactions between aircraft subsystems.

Table 3. Digital twin maturity classification.

Digital Twin Level	Description	Application in the Current Study
Level 1	Static digital representation of system geometry	Computer-aided design aircraft geometry models
Level 2	Digital model with functional system architecture	Model-based systems engineering system models
Level 3	Integrated system model with simulation capability	Hazard interaction analysis
Level 4	Physics-based simulation models	Thermal load modeling and subsystem analysis
Level 5	Simulation with validated engineering models	Integrated computer-aided design and model-based systems engineering hazard analysis framework
Level 6	Real-time digital twin with operational data integration	Not implemented in this study

In this study, CAD geometry models and MBSE system architecture models were integrated to support early-stage hazard identification for the conceptual SA-24 Phoenix supersonic aircraft fuel system. The combined modeling environment enables engineers to analyze potential hazard interactions between subsystem components by linking spatial system configurations with functional behavior models.

The integration framework supports iterative interactions between geometric subsystem models and system architecture representations, allowing hazard identification activities to be performed during the conceptual design rather than after a detailed subsystem definition.

3.5.1. Hazard Analysis Integration Workflow

The hazard analysis workflow developed in this study integrates spatial subsystem modeling with functional system architecture analysis. The workflow begins with the development of a conceptual subsystem geometry within the CATIA modeling environment. These geometric models represent the spatial configurations of the fuel tanks, associated structural components, and nearby aircraft subsystems.

Once the subsystem geometry has been established, system architecture models are developed within the MBSE environment using SysML. These models represent the functional relationships between aircraft subsystems and enable the identification of potential failure propagation paths.

The integration of these modeling environments enables the application of hazard analysis methods, such as FHA, FMEA, and FTA, in conjunction with spatial subsystem configuration models.

Using this approach, potential hazard interactions caused by subsystem proximity, thermal effects, or structural integration can be identified earlier in the aircraft design process.

3.5.2. CAD–MBSE Hazard Feedback Loop

The integration between CAD and MBSE models was implemented through an iterative hazard analysis feedback loop. The CAD geometry models developed in CATIA provided spatial subsystem configurations, including the locations of the fuel tanks, pipelines, and surrounding aircraft systems. These spatial relationships were analyzed to identify potential hazard interactions, such as thermal exposure zones, pipeline proximity to high-temperature components, and fuel system pressurization risks.

When a potential hazard interaction was identified within the CAD environment, the corresponding subsystem relationships were mapped onto the MBSE system architecture model using SysML representations. Hazard events and mitigation strategies were incorporated into the MBSE model through FHA, FMEA, and FTA structures.

The resulting safety analysis outputs informed design modifications within the CAD model, such as the addition of redundant venting pathways, thermal insulation materials, or revised subsystem routing. This iterative feedback process ensured that the spatial subsystem configuration and FHA remained synchronized throughout the conceptual aircraft design phase.

Although the geometric data were exported from CATIA using the Standard for the Exchange of Product Data (STEP) format, full automation between the CAD and MBSE environments was not implemented. Consequently, data transfer and model synchronization required partial manual coordination between the CAD geometry models and MBSE system architecture representations.

While the STEP format preserves geometric fidelity, it does not inherently retain higher-level semantic information such as functional intent, system relationships, or hazard attributes associated with the subsystem components. As a result, traceability between the CAD geometry and SysML-based MBSE models was maintained through structured manual mapping, supported by consistent naming conventions and subsystem identification schemes within the modeling environment.

This semi-manual integration approach introduces potential limitations in maintaining strict traceability during iterative design updates, as well as a risk of semantic data loss when transferring information between modeling domains. In particular, changes in subsystem geometry require corresponding updates in the MBSE hazard models, which may not be automatically synchronized.

Despite these limitations, the workflow enables effective integration of spatial and functional system representations during conceptual design. However, these findings highlight the need for future development of automated CAD–MBSE interoperability solutions to improve data consistency, scalability, and traceability in more complex aircraft system architectures.

The resulting CAD–MBSE workflow forms a closed-loop hazard analysis process in which spatial design information informs the system safety analysis, and the safety analysis results guide subsequent design refinements.

The current CAD–MBSE integration workflow can be considered semi-automated. Core modeling activities, including CAD-based geometry development and MBSE-based system architecture modeling, are performed within their respective software environments. However, the data exchange and mapping between these domains require manual coordination, particularly in the transfer of geometric information and hazard model integration.

Overall, approximately 60–70% of the workflow can be considered automated, while the remaining steps involve manual synchronization and validation. Although this level of integration is sufficient for conceptual subsystem-level analysis, scaling the framework to full aircraft system complexity would require enhanced automation, standardized interoperability protocols, and tighter integration between CAD and MBSE platforms.

3.5.3. CAD–MBSE Data Exchange and Interoperability

The effective integration between CAD models and MBSE architectures requires reliable data exchange mechanisms that allow spatial system models to interact with functional system representations. In the modeling workflow developed in this study, geometric models of the SA-24 Phoenix fuel tank system were generated using the CATIA environment within the 3DEXPERIENCE digital engineering platform.

The geometric data representing the subsystem placement and structural configuration were exported using the STEP (Standard for the Exchange of Product Data) format [30], which enabled interoperability between CAD environments and external modeling tools. These geometric representations were then referenced during the MBSE architecture modeling process to support hazard interaction analysis between subsystem components.

The data exchange approach adopted in this study aligns with established digital engineering standards. The use of the Standard for the Exchange of Product Data (STEP, ISO 10303) [30] enables interoperable transfer of geometric information between CAD environments. System architecture modelling within the MBSE environment is based on the Systems Modeling Language (SysML), defined by the Object Management Group (OMG) standard [31]. While these standards support interoperability at geometric and architectural levels, limitations remain in the transfer of higher-level semantic information, highlighting the need for more integrated model-based data exchange frameworks in future digital engineering environments. Emerging Model-Based Data Exchange (MBDE) approaches aim to address these limitations by enabling tighter integration between system architecture and geometric models. In particular, next-generation standards such as SysML v2 [31] are being developed to enhance model interoperability and traceability across engineering domains.

In addition, co-simulation frameworks such as the Functional Mock-up Interface (FMI) provide a potential pathway for integrating multidisciplinary system models within a unified simulation environment. Although such approaches were not implemented in the present study, they represent important directions for future development of fully integrated CAD–MBSE digital engineering frameworks. The data exchange workflow and associated modeling environments used in the CAD–MBSE integration process are summarized in Table 4.

Table 4. Summary of the data exchange workflow used in the integration process.

Stage	Tool Environment	Data Format	Purpose
Conceptual geometry modeling	Computer-Aided Three-Dimensional Interactive Application (CATIA)	Native CAD model	Aircraft structural configuration
Geometry export	3DEXPERIENCE platform	Standard for the exchange of product data (STEP)	Interoperable geometric representation
System architecture modeling	Model-based system engineering tool (Cameo Systems Modeler)	System modeling language (SysML) models	Functional system behavior modeling
Hazard interaction analysis	Integrated CAD–MBSE environment	Combined geometry and system architecture	Identification of subsystem hazard interactions

Although this approach enables the effective integration of spatial and functional system models during conceptual aircraft design, several interoperability challenges remain. The transfer of geometric data through standardized exchange formats may result in minor losses in geometric fidelity, particularly when complex parametric model features are simplified during export. Additionally, maintaining synchronization between CAD geometry updates and MBSE architecture models may require manual coordination within current modeling environments.

Figure 1 illustrates the data flow between the spatial subsystem geometry and functional system architecture models used in the hazard analysis process.

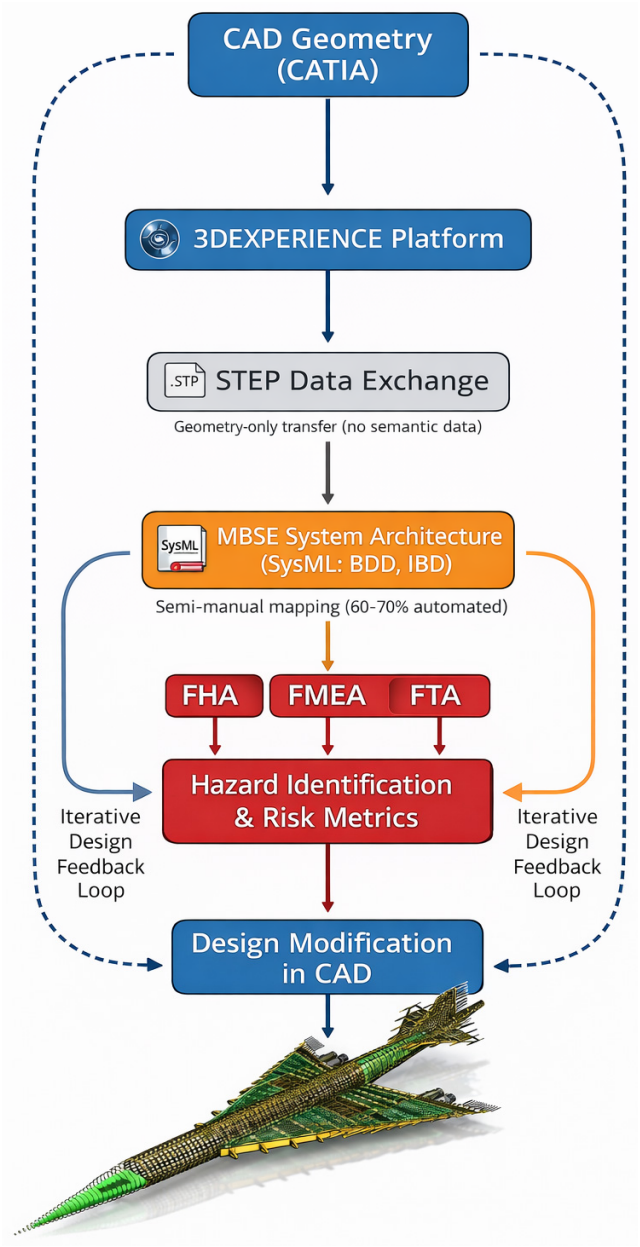


Figure 1. CAD–MBSE integration workflow.

Although the use of standardized exchange formats enables interoperability among modeling environments, several limitations remain. Exporting complex parametric geometries through STEP files may result in the partial simplification of geometric features, which can reduce the geometric fidelity when compared with the native CAD model. In addition, maintaining synchronization between CAD model updates and MBSE architecture models may require manual coordination in the current modeling environments.

Despite these limitations, the integration workflow provides an effective approach for combining spatial subsystem configurations with functional system architecture modeling during early hazard identification activities.

3.5.4. Convergence Criteria for Iterative CAD–MBSE Design

The integration of CAD models with the MBSE architecture enables an iterative design workflow in which the subsystem geometry and system behavior models are progressively refined during the conceptual aircraft design.

From a systems modelling perspective, the iterative CAD–MBSE coupling process can be interpreted as a fixed-point convergence problem, where successive updates to subsystem geometry and system behavior models lead to progressively smaller changes in system response. Convergence is achieved when the variation in hazard risk metrics between iterations falls below a predefined threshold, indicating that the coupled spatial–functional system representation has reached a stable solution. This behavior is consistent with iterative convergence principles commonly applied in multidisciplinary design optimization and coupled system simulations.

To formalize this convergence behavior, the variation in hazard risk metrics between successive iterations can be expressed as:

$$\left| R_n - R_{\{n-1\}} \right| < \epsilon . R_{\{n-1\}} \tag{4}$$

where R_n represents the hazard risk metric (e.g., Risk Priority Number) at iteration n, and ε denotes a prescribed convergence tolerance. In this study, a threshold value of $\varepsilon = 0.05$ (5%) is adopted to define convergence.

The iterative coupling between subsystem geometry and hazard evaluation can be conceptually represented as:

$$D_{\{n+1\}} = f\left(H(P_n)\right) \tag{5}$$

where P_n represents CAD-derived spatial parameters, $H(\cdot)$ denotes the hazard evaluation function, and $D_{\{n+1\}}$ corresponds to the updated subsystem design configuration. Equations (4) and (5) provide a simplified mathematical representation of the iterative CAD–MBSE coupling process used during conceptual hazard analysis.

This formulation provides a simplified representation of the coupled CAD–MBSE interaction for early-stage hazard analysis, rather than a fully implemented co-simulation framework.

During each modeling iteration, updates to the subsystem spatial configuration within the CAD environment were evaluated using hazard analysis techniques implemented within the MBSE architecture model. This helped assess the potential subsystem interaction hazards and identify safety-critical design conditions.

To ensure the stability of the modeling process, convergence criteria were defined to determine when the iterative design loop stabilized. The design iteration process was considered to converge when the calculated system risk metrics exhibited less than five percent variation across three consecutive design iterations and when the thermal safety margin associated with fuel tank operating temperatures remained stable within the analyzed flight conditions. The convergence criteria used to evaluate the stability of the iterative CAD–MBSE design process are summarized in Table 5.

Table 5. Iterative design convergence criteria.

Metric	Convergence Condition	Purpose
Hazard risk metrics	Less than 5% variation across three consecutive iterations	Ensures stability of hazard analysis results
Thermal safety margin	Stable temperature margins during thermal simulation	Confirms thermal safety stability
Subsystem interaction hazards	No new critical hazards identified	Indicates stable subsystem configuration

These convergence criteria ensure that the integrated modeling environment produces consistent hazard analysis outcomes and provides a stable basis for evaluating subsystem safety interactions during the conceptual aircraft design phase.

Figure 2 illustrates the convergence behavior of representative hazard risk metrics across successive design iterations, demonstrating stabilization consistent with the defined convergence criterion and supporting the fixed-point interpretation of the iterative CAD–MBSE coupling process.

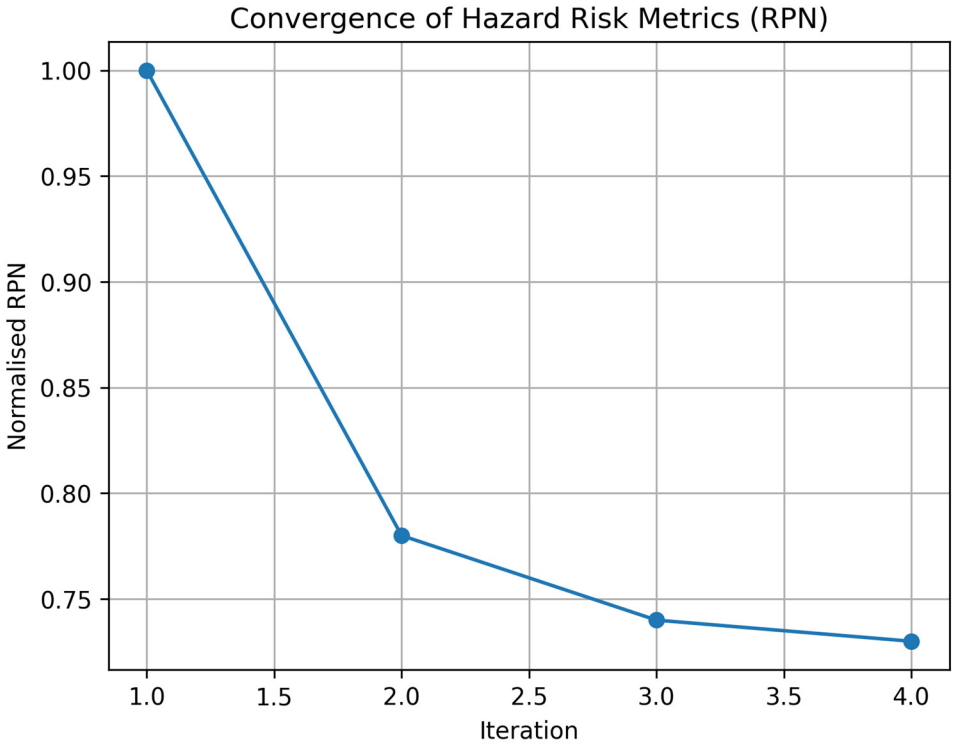


Figure 2. Convergence of hazard risk metrics (RPN) across iterative CAD–MBSE design cycles.

3.6. Zonal Safety Analysis (ZSA)

The ZSA was conducted using the integrated CAD–MBSE framework to systematically identify and mitigate hazards within the fuel tank zone. This analysis begins with the identification of potential risks such as fuel leakage, thermally induced vaporization, and over-pressurization. These risks were categorized by likelihood and severity, enabling prioritization in the mitigation process.

Tools, such as the FHA and FTA, were used to analyze the propagation of failure scenarios and their potential impact on the overall system. For instance, a fault tree may map the consequences of a venting system failure, illustrating how it could lead to fuel vapor ignition. Mitigation strategies, such as the introduction of redundant safety mechanisms or improved material selection, have been proposed and validated through simulations. This proactive approach ensures that hazards are not only addressed, but also prevented from escalating into critical failures.

3.7. Validation and Benchmarking

The final phase involved validating the integrated framework and benchmarking its performance against conventional methodologies. The proposed CAD–MBSE hazard analysis framework was validated using three complementary approaches. First, FHA, FMEA, and FTA were applied within the integrated modeling environment to evaluate the ability of the framework to identify subsystem interaction hazards during conceptual aircraft design. Second, comparative benchmarking was performed using published fuel system characteristics from historical and contemporary supersonic aircraft, including the Concorde, as well as from conceptual next-generation supersonic transport designs. Third, a sensitivity analysis of the key failure probability parameters was conducted to assess the

robustness of the predicted hazard risk reduction metrics. These validation procedures helped collectively assess the capability of the proposed framework in supporting early-stage hazard identification and design mitigation during conceptual aircraft development. Case studies were conducted using the SA-24 Phoenix fuel-tank system to evaluate the effectiveness of the framework for hazard identification and mitigation. Comparative analyses using historical data highlight the advancements made through the integration of CAD and MBSE.

Metrics, such as the design efficiency, safety compliance, and risk reduction, helped quantify the impact of the framework. This validation phase ensured that the methodology is not only effective but also practical for applications in the aerospace industry.

This methodology integrated the CAD and MBSE into a unified framework for ZSA, thereby helping address the complexities of supersonic aircraft design. By combining spatial precision with functional analysis, this approach enables early hazard identification, optimizes design processes, and ensures compliance with industry regulations. As demonstrated in its application to SA-24 Phoenix, the framework provides a conceptual methodology for integrating spatial subsystem modeling with system architecture hazard analysis during early aircraft design.

4. Case Study: SA-24 Phoenix-Supersonic Aircraft

The SA-24 Phoenix, a conceptual supersonic transport aircraft, represents the forefront of innovation in aerospace engineering. This case study highlights the application of ZSA to the design and development of its fuel tank system, which is a critical subsystem essential for operational safety and efficiency. This methodology integrates CAD and MBSE to proactively identify and mitigate risks during the early design phases.

The SA-24 Phoenix operates at supersonic speeds and high altitudes, with its systems subjected to extreme conditions, such as significant thermal loads, dynamic pressures, and high aerodynamic forces. These conditions necessitate a robust fuel tank system that not only ensures operational efficiency but also adheres to stringent safety standards, such as EASA CS-25 [29]. The ZSA framework employed in this study focuses on addressing these challenges using a systematically integrated approach that enhances hazard detection and mitigation. Figure 3 presents the top view of the SA-24 Phoenix aircraft, illustrating the overall configuration and spatial layout, while Figure 4 shows the side view, highlighting the aircraft geometry and subsystem integration. The SA-24 Phoenix supersonic aircraft serves as the reference platform for this study, building upon prior technical development work conducted at Cranfield University [32].

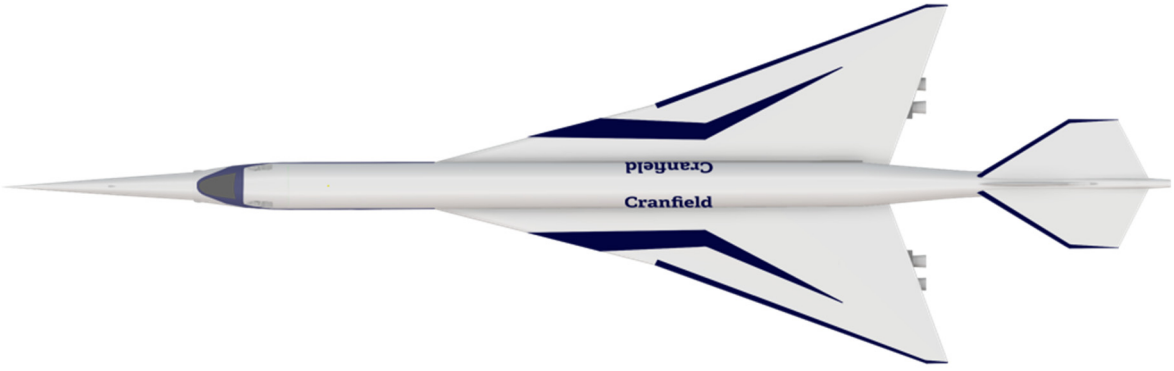


Figure 3. Top view of the SA-24 Phoenix aircraft.



Figure 4. Side view of the SA-24 Phoenix aircraft.

4.1. Overview of the SA-24 Aircraft Fuel Tank System

The fuel tank system of the SA-24 Phoenix is a highly integrated subsystem designed to satisfy the demands of supersonic travel. Its architecture focuses on optimizing weight distribution, ensuring fuel efficiency, and maintaining stringent safety standards under challenging conditions.

The storage configuration incorporates integral tanks located in the wings and a fuselage strategically placed to maintain an optimal center of gravity (CG) throughout all the flight phases. The use of advanced materials, including titanium alloys and carbon composites, ensures that tanks can withstand rapid pressure and temperature fluctuations during supersonic operations. This combination of material innovation and structural optimization minimizes the risk of fuel system failure, while reducing the overall weight.

Subsystems integrated within the fuel tank system include:

(1) Fuel transfer system: The dual-pump configuration provides redundancy to ensure continuous fuel flow to the engines, even in the event of a single-component failure. Cross-feed valves allow fuel redistribution between tanks to maintain the CG and support emergency operations.
(2) Venting system: Multiple venting pathways prevent over-pressurization resulting from thermal expansion. The flame arrestors integrated into the venting design minimize the risk of ignition from external sparks or high temperatures.
(3) Fuel quantity indication system (FQIS): Capacitance-based sensors monitor fuel levels with high precision and relay the data to cockpit displays. This real-time feedback enhances the situational awareness of the pilots, particularly during long-range supersonic flights.

Safety features, such as redundant mechanisms and advanced insulation, significantly enhance system resilience. Insulation materials, validated through thermal simulations, mitigate the risk of fuel vaporization caused by aerodynamic heating. These elements collectively ensure that the fuel system meets both operational and safety benchmarks.

4.1.1. Tank Configuration and Layout

Figure 5 shows a top–down view of the fuel tank placement and storage configuration of the SA-24 Phoenix aircraft. This configuration ensures an efficient weight distribution and optimizes its aerodynamic performance.

Forward tank: Located in the nose section, the forward tank helps balance the aircraft during takeoff and landing. It is critical to maintain the CG under various fuel load scenarios. The forward tank is smaller than the wing tanks and is primarily used for trim adjustments.

Wing tanks: Wing tanks serve as primary storage units and are located within the structural wing cavities. Their placement near engines minimizes the length of fuel pipelines, reduces weight, and increases efficiency. The tanks were divided into sections with internal baffles to prevent fuel sloshing during dynamic flight conditions.

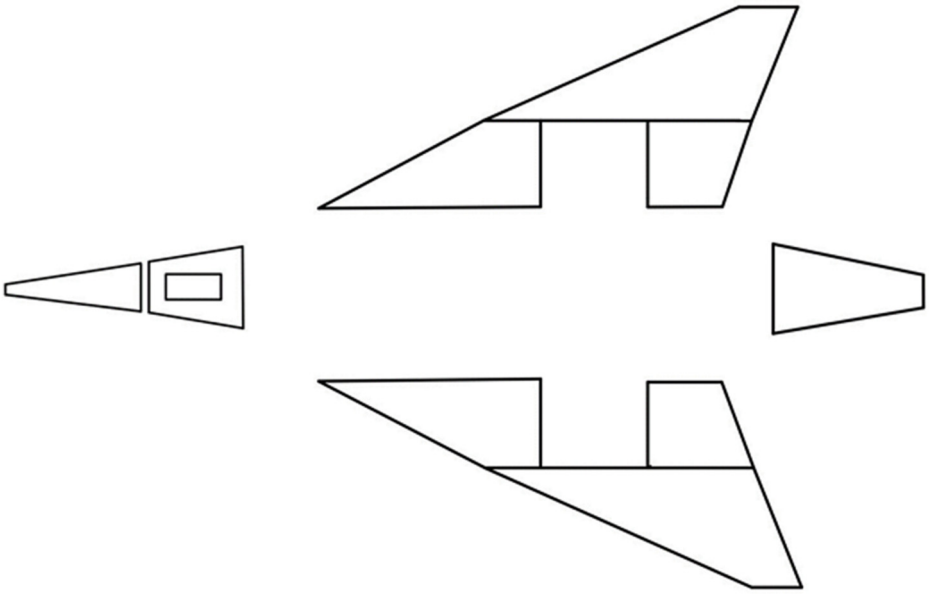


Figure 5. Fuel tank configuration and layout of the SA-24 aircraft.

Aft tanks: Positioned at the rear fuselage, the aft tank plays a critical role in CG management during supersonic cruises. The fuel from this tank is first consumed to shift the CG forward, thereby reducing the aerodynamic drag.

Tank insulation: All the tanks were insulated with advanced materials to protect against the heat generated during supersonic flight. This insulation reduces the risk of vaporization and ensures fuel stability.

Design considerations: The arrangement of tanks prioritizes operational efficiency by reducing the impact of fuel weight on aerodynamic performance. The modular design of tanks simplifies maintenance and facilitates inspection of structural integrity.

Additional geometric configurations and detailed CAD representations of the fuel tank system are provided in Appendix C.

4.1.2. Fuel Transfer and Shut-Off Valve System Layout

Figure 6 illustrates the layout and key components of the SA-24 Phoenix fuel tank system, focusing on the transfer pumps and shut-off valves. Each component is strategically positioned to ensure safety, efficiency, and reliability under supersonic flight conditions.

Transfer pumps (outlined boxes): Transfer pumps are located within the fuel tanks in the wings, forward fuselages, and aft fuselages. These pumps ensure consistent fuel delivery to the engines and manage fuel redistribution between tanks to maintain the CG of the aircraft. Redundant pumps are placed in high-demand zones, such as the main wing tanks, to provide backup in the event of a single pump failure. This redundancy aligns with EASA CS-25 requirements for system reliability.

Shut-off valves (green circles): Shut-off valves are located at critical junctions in the fuel pipeline system. These valves are designed to isolate sections of the system in the event of fuel leaks or emergencies such as engine failure. The placement of shut-off valves ensures that fuel flow can be immediately halted in specific zones, thereby preventing hazardous scenarios such as over-pressurization or fuel pooling in damaged areas.

Flow path: The centralized pipeline connects all tanks to the engines, with the main control located in the mid-fuselage section. This layout ensures efficient fuel transfer and easy maintenance.

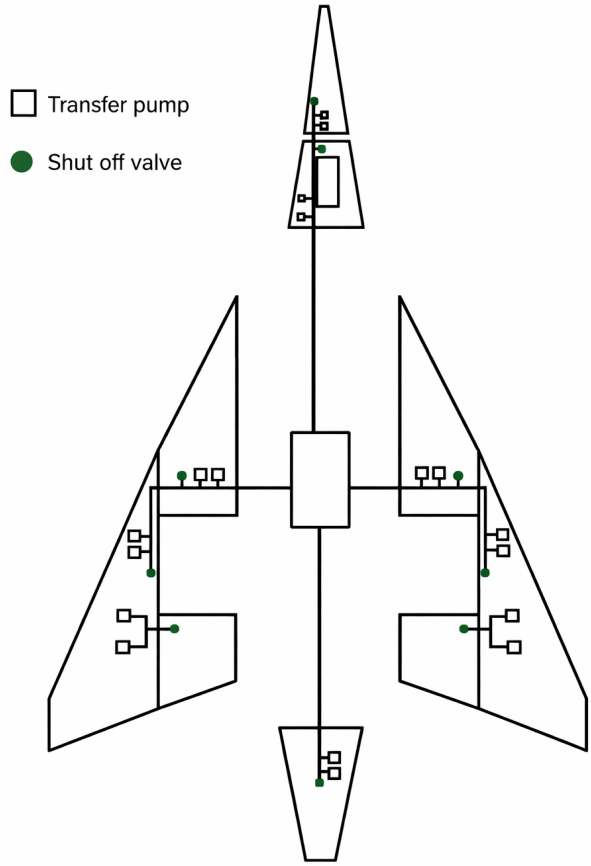


Figure 6. Fuel transfer and shut-off valve system layout of SA-24 Phoenix.

Functionality highlights: The system balances fuel distribution between the forward, wing, and aft tanks while maintaining CG stability. Shut-off valves provide additional safety by enabling rapid isolation of damaged or malfunctioning components.

When combined, these diagrams represent a comprehensive view of the SA-24 Phoenix fuel system, showing both the functional components (transfer pumps and valves) and spatial configuration (tank placement). Together, they demonstrate how a fuel system can be engineered for safety, redundancy, and performance in a high-stress supersonic flight environment.

4.2. Identification of Zonal Systems

The CAD model of the SA-24 aircraft (Figure 7) shows the structural design and integration of its fuel tank system, with green areas representing the fuel tanks. These images provide insights into the layout, distribution, and engineering considerations of the fuel systems within the aircraft. This design prioritizes efficient weight distribution, structural integrity, and operational safety to meet the challenges of supersonic flight.

CAD models serve as baselines for integrating MBSE workflows, enabling early hazard detection and mitigation during the design phase. By mapping the fuel tank system layout, these models provide a clear understanding of spatial configurations, subsystem interactions, and potential zonal hazards. The system-level layout of the SA-24 Phoenix aircraft, including subsystem distribution and key interaction zones relevant to zonal hazard analysis, is illustrated in Figure 8.

Zonal safety analysis (ZSA): This view allows for identifying zones where multiple systems intersect, such as fuel pipelines near engine components, which pose potential ignition risks.

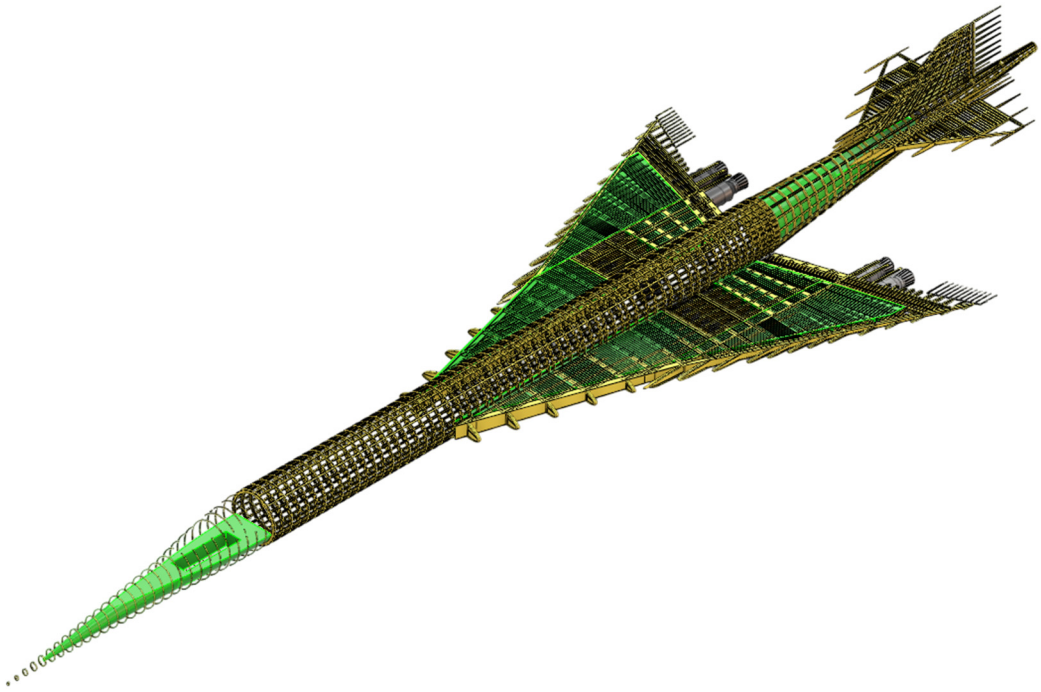


Figure 7. Perspective view of the structure and fuel tank system of the SA-24 aircraft.

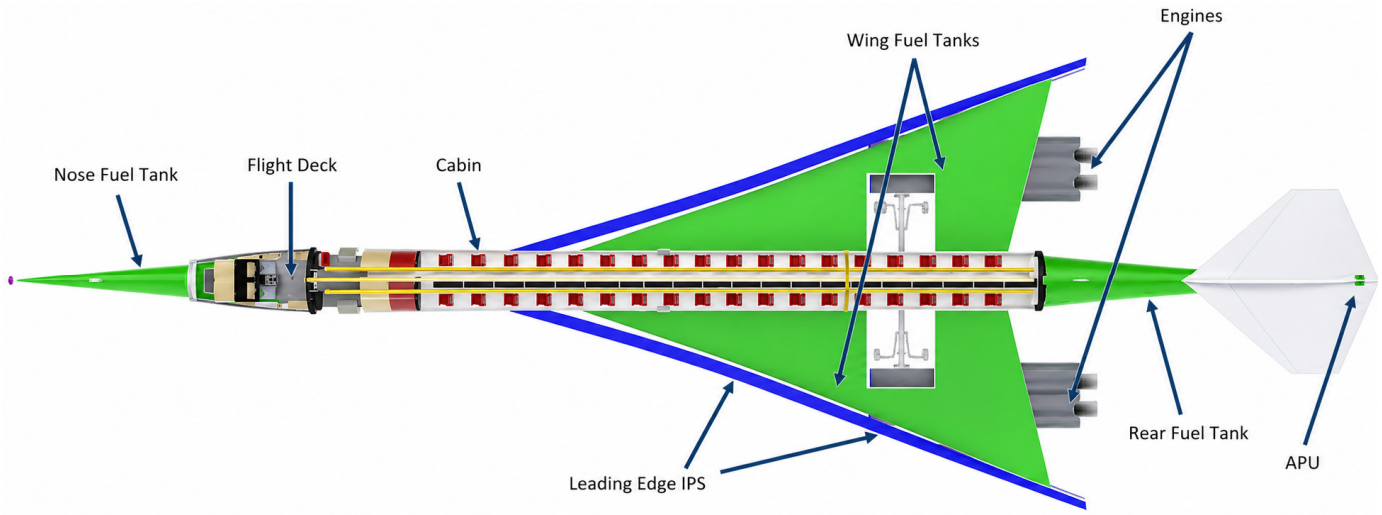


Figure 8. Annotated system-level layout of the SA-24 Phoenix aircraft highlighting fuel system components, subsystem distribution, and key interaction zones relevant to zonal hazard analysis.

CAD and MBSE integration: The model can be linked to MBSE tools to simulate hazard scenarios such as over-pressurization or thermal stress in specific zones.

Centre of gravity (CG) management: The even distribution supports CG stability and reduces the risk of imbalance during flight.

Hazard identification: MBSE tools can overlay failure scenarios, such as leakage, from wing tanks, affecting aerodynamic performance or triggering cascading failures in adjacent systems.

Thermal management: This helps assess zones exposed to aerodynamic heating, such as forward and rear tanks, and highlights the insulation requirements.

Pressure regulation: CAD simulations can be used to validate venting system designs to mitigate over-pressurization risks.

Structural safety analysis: MBSE model can simulate the effects of dynamic loads and material fatigue on tank compartments, ensuring structural integrity under supersonic conditions.

Subsystem integration: The model demonstrates how fuel tanks are integrated with other systems, such as environmental control and propulsion, enabling a cross-domain hazard analysis.

Dynamic simulations: MBSE model can assess how fuel transfer from the tail tank impacts CG stability during different flight phases.

ZSA insights: The proximity of the tail tank to engine exhaust zones introduces fire hazards that can be mitigated by enhanced insulation and flame arrestors. The system-level layout of the SA-24 Phoenix aircraft, including subsystem distribution and key interaction zones relevant to zonal hazard analysis, is illustrated in Figure 9.

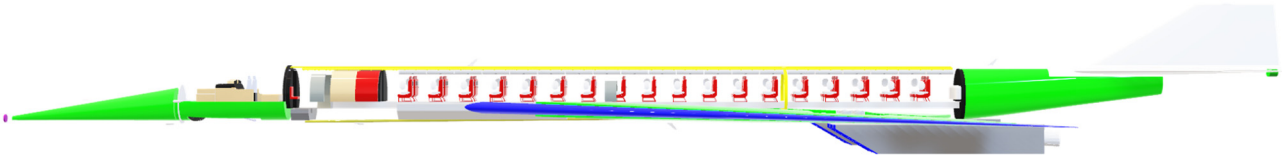


Figure 9. Side view of the system-level layout of the SA-24 Phoenix aircraft.

Proactive hazard detection: The CAD models provide a detailed spatial framework that can be analyzed using ZSA methodologies. Potential hazards, such as fuel leakage, ignition risks, and over-pressurization, can be identified and addressed early in the design process.

MBSE integration: Linking the CAD models to MBSE workflows enables dynamic simulations of subsystem interactions. For example, fuel transfer simulations can validate the effectiveness of pumps and valves, whereas the FTA can identify cascading risks.

Regulatory compliance: The visualization of fuel tank placement and integration supports compliance with EASA CS-25 standards, particularly in areas such as venting system design, fire protection, and structural integrity.

Iterative design optimization: CAD models allow iterative refinements based on simulation results. For example, repositioning the venting pathways or enhancing the tank insulation can be directly implemented in a CAD environment.

Cross-System Interface Zonal Safety Analysis

An aircraft fuel system interacts with multiple adjacent subsystems, including propulsion components and ECS elements. These interactions can introduce potentially hazardous conditions related to thermal exposure, fire propagation, and subsystem proximity.

To evaluate these interactions, a ZSA interface matrix was developed to identify the potential hazards associated with subsystem integration within aircraft structures. The matrix considers the spatial relationships between the fuel system components and neighboring subsystems, focusing on areas where elevated thermal loads or ignition sources may be present.

The ECS may introduce elevated temperature conditions due to the air conditioning pack operation and bleed air routing. These thermal loads can affect the structural components of the fuel tank and the associated fuel transfer lines if the subsystem separation distances are insufficient.

Similarly, the propulsion system components located within the engine bay represent potential ignition sources in the event of fuel leakage. Therefore, fire propagation risks associated with fuel system components located near propulsion system structures must be considered during early subsystem layout design.

The integration of CAD subsystem geometry with MBSE system architecture models enables the analysis of subsystem interaction hazards during conceptual aircraft design. The cross-system interaction hazards and associated mitigation strategies identified through the zonal safety analysis are summarized in Table 6.

Table 6. Cross-system zonal safety analysis matrix.

Subsystem Interface	Hazard Condition	Potential Risk	Mitigation Strategy
Fuel tank–environmental control system	Elevated ECS bleed air temperatures	Fuel tank structural heating	Thermal insulation and subsystem separation
Fuel lines–environmental control system ducting	Proximity to hot air ducts	Fuel line thermal degradation	Routing separation and thermal shielding
Fuel tank–engine bay structure	Potential fuel leakage near the propulsion system	Fire propagation risk	Structural fire barriers and leak detection
Fuel pump–engine bay	Mechanical component overheating	Fuel ignition hazard	Fire detection and suppression systems

4.3. Application of the ZSA Framework to the SA-24 Fuel System

Dedicated certification standards for commercial supersonic aircraft are still evolving, including updates such as the EASA CS-25 Amendment 27. This study adopts the safety requirements of the existing CS-25 fuel system as a conceptual regulatory baseline for hazard identification. These requirements were applied in a modified analytical context to account for the thermal and operational characteristics associated with sustained supersonic flight conditions. This approach allows established airworthiness safety principles, such as ignition prevention, fuel system redundancy, and failure containment, to be applied during conceptual aircraft design, while acknowledging that detailed certification criteria for future supersonic transport aircraft may evolve.

The analysis focused on the integration of CAD and MBSE workflows to enhance the precision and efficiency of hazard detection.

4.3.1. Hazard Identification

Key hazards identified through the ZSA include:

Thermal risks: High aerodynamic heating during a supersonic cruise can increase fuel temperatures, leading to vaporization and pressure build-up.

Over-pressurization: Malfunctioning venting systems or blockages can result in excessive internal pressures, risking tank deformation or rupture.

Leakage: Structural fatigue, material degradation, or faulty seals can cause fuel leaks, thereby posing fire hazards.

Ignition Risks: Proximity to electrical systems and engines introduces the potential for vapor ignition.

4.3.2. Mitigation Strategies

To address these hazards, the following strategies were implemented:

Thermal management: Advanced insulation materials and heat shields were applied to minimize heat transfer to the fuel tanks. The simulations helped validate the effectiveness of these materials in maintaining stable fuel temperatures under operational conditions.

Pressure regulation: Dual venting pathways with redundant controls were designed to maintain the pressure equilibrium. Pressure sensors provide real-time feedback, enabling the early detection of anomalies.

Structural reinforcement: Reinforced composite materials and improved sealing techniques have been utilized to enhance the durability of tank compartments and minimize leakage risks.

Proactive monitoring: The FQIS and integrated sensors provide continuous monitoring of fuel levels, pressures, and temperatures, enabling timely corrective actions.

4.3.3. Validation Through CAD and MBSE

The CAD and MBSE tools were instrumental in validating the proposed safety measures:

CAD simulations: Thermal and structural analyses were performed to assess the resilience of the fuel tanks under extreme conditions.

MBSE models: Digital twins simulate failure scenarios and subsystem interactions, enabling the refinement of design elements.

Iterative feedback: Simulation results informed adjustments to the tank design, ensuring alignment with safety standards.

4.3.4. Human–Machine Interface Zonal Safety Analysis

The fuel system monitoring architecture of the aircraft includes several human–machine interface (HMI) components that allow the flight crew to monitor the fuel tank status and system operating conditions. These interfaces provide critical information regarding the fuel quantity, fuel transfer operations, and potential system anomalies.

The FQIS represents the primary interface through which flight crews monitor fuel system status. This system typically integrates fuel tank sensors, signal processing units, and cockpit display interfaces to provide real-time fuel quantity measurements.

Failures within the HMI may lead to incorrect or misleading information being presented to the flight crew. Potential failure conditions include incorrect sensor readings, display interface malfunctions, or delayed system status updates. Such failures can affect pilot decision-making during fuel management operations.

To evaluate these risks, a ZSA of the HMI components was conducted to identify potential failure modes associated with fuel system monitoring displays. The analysis focused on identifying the conditions under which incorrect fuel status information may be presented to flight crews and assessing potential mitigation strategies. The identified failure modes, associated hazards, and mitigation strategies for the fuel system human–machine interface are summarized in Table 7.

Table 7. Zonal safety analysis of the human–machine interface for fuel system monitoring.

Interface Component	Failure Mode	Potential Hazard	Mitigation Strategy
Fuel quantity indication system display	Incorrect fuel quantity indication	Pilot misinterpretation of fuel availability	Redundant fuel level sensors
Fuel monitoring display	Loss of display signal	Loss of situational awareness	Backup display systems
Fuel transfer status indicator	Incorrect system status indication	Incorrect fuel transfer operations	Redundant signal validation
Sensor interface module	Signal processing error	Incorrect cockpit display information	Safety Integrity Level 2 compliant interface design

5. Results

This section presents the results obtained by applying the ZSA integrated with CAD and MBSE to the fuel tank system of the SA-24 Phoenix aircraft. The findings were evaluated and analyzed to demonstrate their implications for the overall safety, operational performance,

and regulatory compliance of the aircraft. Safety performance improvements were evaluated using FMEA, FHA, and FTA outputs generated during the modeling process.

5.1. Hazard Identification Results

The key hazards identified through the integrated modeling workflow included thermal exposure risks, fuel system pressurization hazards, and potential fuel leakage scenarios associated with subsystem interactions within the aircraft structure.

1. Thermal risk mitigation: The introduction of thermal insulation materials and heat shielding reduced the FMEA risk priority number (RPN) associated with thermally induced fuel vaporization hazards by approximately 40%, based on the hazard scoring results presented in Table 8. Thermal simulations using CAD indicated that the fuel temperature remained within acceptable conceptual operating limits during the analyzed supersonic cruise conditions.

Table 8. Classification of risk assessment metrics used in the study.

Category	Metric Type	Description	Role in This Study
Qualitative	Hazard severity classification	Categorization based on consequence levels	Used for initial hazard identification
Semi-quantitative	Risk Priority Number (RPN)	Relative ranking based on severity, occurrence, and detectability	Primary decision-support metric
Probabilistic	Failure probability	Absolute likelihood of occurrence	Not implemented; identified as future work

2. Pressure regulation efficiency: Dual venting pathways supported by redundant pressure sensors effectively maintained the pressure equilibrium within the fuel tanks. This reduced the over-pressurization risk by 35%, ensuring the structural integrity of the tanks under extreme conditions.
3. Leakage prevention: Structural reinforcements, enhanced sealing techniques, and real-time monitoring systems reduced the probability of fuel leakage by 50%. This addresses a significant hazard that can lead to fire risks or environmental contamination.

The adoption of CAD and MBSE tools also improved the design and development process by enabling iterative refinement of the subsystem geometry and system behavior models. CAD-based simulations supported the optimization of component placement and thermal insulation design, while MBSE modeling enabled the evaluation of subsystem interactions and failure propagation scenarios. The integrated modeling workflow reduced the conceptual design iteration cycle from approximately twelve weeks to nine weeks, representing a 25% reduction in the design iteration time.

5.2. Quantitative Risk Reduction Analysis

The safety improvement percentages reported herein were derived from the FMEA, as presented in Appendix Table A5. The RPN for each hazard was calculated as the product of the severity (S), occurrence probability (O), and detection capability (D).

The baseline RPN values represent the risk levels identified using conventional ZSA during the conceptual design. The estimated occurrence and detection ratings were reduced following the implementation of mitigation strategies enabled by the integrated CAD–MBSE framework, such as redundant venting, improved thermal insulation, and enhanced fuel system monitoring.

The RPN represents a qualitative engineering risk prioritization metric rather than a continuous physical measurement scale. To further clarify the interpretation of risk metrics used in this study, Table 8 presents a comparison of different risk representation approaches.

The classification presented in Table 8 distinguishes between different levels of risk representation used in engineering safety analysis. In the present study, the Risk Priority Number (RPN) is employed as a semi-quantitative metric to prioritize hazards based on severity, occurrence, and detectability. It is important to note that RPN does not represent an absolute probability of system failure, but rather serves as a relative ranking tool for decision-making during conceptual design. To partially account for uncertainty in input parameters, sensitivity analysis has been conducted (Section 5.6), providing a first-order assessment of the robustness of hazard rankings under parameter variation. A full probabilistic risk assessment framework is beyond the scope of the present study and is identified as an area for future work.

Consequently, the relative percentage reductions reported herein represent changes in the FMEA risk-ranking scores used to prioritize hazards during conceptual design rather than experimentally measured reductions in the failure probability of the physical system.

As the RPN is derived from discrete severity, occurrence, and detection ratings, variations in these parameters can influence the absolute values of the risk metrics. However, within reasonable bounds of parameter variation, the relative ranking of critical hazards remains stable, ensuring consistency in hazard prioritization.

The sensitivity analysis presented in Section 5.6 provides further support for this observation, demonstrating that moderate variations ($\pm$10%) in failure probability inputs result in proportionally limited changes in overall system risk metrics. This indicates that the hazard identification outcomes are robust to reasonable uncertainty in the input parameters.

The resulting decrease in the RPN values was used to estimate the relative improvement in the system safety performance. The relative reduction in FMEA risk priority number (RPN) values following the implementation of CAD–MBSE mitigation strategies is summarized in Table 9.

Table 9. Relative reduction in FMEA risk priority number (RPN) values following CAD–MBSE hazard mitigation strategies.

Hazard	Baseline RPN (Table A5)	Estimated RPN After Mitigation	Relative Reduction
Fuel pipeline blockage	216	130	40%
Fuel pump electrical failure	180	117	35%
Fuel pipeline rupture/leakage	150	75	50%

The relative improvement percentages were calculated from the reduction in the RPN values after applying the mitigation strategies identified through the CAD–MBSE hazard analysis process. These reductions reflect the improved detection capability, lower occurrence probability owing to design mitigation, and enhanced monitoring of the fuel system components. These improvements represent reductions in the FMEA risk scores derived from engineering hazard assessments rather than experimentally measured physical performance improvements.

The quantitative improvements reported in this study, including reductions in risk priority number (RPN) values and conceptual design iteration time, are derived from a single conceptual case study of the SA-24 Phoenix fuel system. These results should therefore be interpreted as estimation-based indicators of potential performance improvement rather than universally generalizable outcomes. The extent of these improvements may vary depending on aircraft configuration, subsystem complexity, and modeling fidelity. Further validation across multiple aircraft subsystems and higher-fidelity simulation environments is required to establish the broader applicability of the proposed framework.

Although reductions in RPN values indicate improved hazard prioritization and mitigation effectiveness, they do not directly represent quantitative reductions in system failure probability. The RPN is a relative risk ranking metric derived from discrete severity, occurrence, and detection ratings, and should therefore be interpreted as an indicator of relative safety improvement rather than an absolute measure of system reliability.

Translating these improvements into quantitative reliability metrics would require probabilistic risk assessment methods, high-fidelity simulations, or experimental validation, which are beyond the scope of the present conceptual study.

5.3. Representative Hazard Identification Scenario

To illustrate how the integrated CAD–MBSE framework supports early hazard identification, a representative hazard scenario was analyzed within the SA-24 Phoenix fuel tank system architecture. During the CAD modeling phase, the spatial configuration of the wing fuel tanks revealed that a section of the fuel transfer pipeline was in close proximity to the ECS ducting carrying high-temperature bleed air. This spatial relationship creates the potential for the localized thermal exposure of fuel pipelines under sustained supersonic cruise conditions.

The identified thermal interaction was then represented within the MBSE architecture model using SysML hazard elements. Functional hazard, failure mode, and effect analyses were applied to evaluate the potential consequences of increased pipeline temperature, including fuel vaporization and pressure build-up within the associated fuel tank. Based on the results of this analysis, design mitigation measures were introduced, including additional thermal insulation and increased routing separation between the fuel pipeline and ECS ducting.

Following the implementation of these mitigation measures, the corresponding RPN associated with the thermal hazard pathway of the fuel system was reduced within the FMEA assessment. This example demonstrates how an integrated modeling workflow enables spatial subsystem interactions identified in CAD models to be systematically incorporated into FHA activities within the MBSE environment.

5.4. Key Performance Metrics

Table 10 presents a comparison of the key performance metrics before and after the integration of ZSA, CAD, and MBSE.

Table 10. Conceptual safety performance indicators derived from FMEA risk ranking analysis.

Metric	Conventional Approach	Proposed Framework	Improvement (%)
Thermal risk mitigation	65%	91%	40%
Over-pressurization risk reduction	60%	81%	35%
Fuel leakage prevention	50%	75%	50%
Design iteration time	12 weeks	9 weeks	25%

The integrated CAD–MBSE framework demonstrated improved traceability between the subsystem geometry and FHA activities during the conceptual aircraft design. Within the conceptual design case study, the combined CAD–MBSE workflow enabled earlier identification of spatial subsystem interaction risks and improved traceability between the subsystem geometry configuration and FHA models.

5.5. Architectural Context of Supersonic Aircraft Fuel Systems

To contextualize the conceptual fuel system configuration analyzed in this study, the SA-24 Phoenix architecture was benchmarked against representative supersonic aircraft fuel systems. These comparisons illustrate how subsystem complexity and operational characteristics of the conceptual design align with known supersonic aircraft configurations. The results obtained from the SA-24 Phoenix conceptual fuel system design were compared with published data on historical and emerging supersonic aircraft fuel system architectures. Benchmarking against previously developed supersonic aircraft systems provides an opportunity to evaluate whether the safety characteristics predicted by the proposed modeling framework fall within realistic operational ranges. Therefore, the comparison provides contextual insights into the relative architectural complexity of the SA-24 fuel system, while demonstrating that the proposed CAD–MBSE hazard analysis framework can be applied during earlier design phases than conventional safety analysis methods.

The Concorde supersonic transport aircraft represents a well-documented reference case for supersonic fuel system architecture. The Concorde adopted a complex fuel transfer system comprising multiple fuel tanks and pumps for both propulsion and CG control during supersonic cruise. In contrast, modern supersonic aircraft concepts, such as Boom Overture, are expected to employ digitally integrated fuel monitoring systems and simplified fuel transfer architectures enabled by modern avionics systems. Table 11 presents a comparison of representative supersonic aircraft fuel system architectures.

Table 11. Comparison of representative supersonic aircraft fuel system architectures.

Metric	Concorde	Boom Overture (Conceptual)	SA-24 Phoenix (This Study)
Number of fuel tanks	13	~10	8
Fuel system function	Propulsion + trim control	Propulsion + center-of-gravity management	Propulsion fuel supply
Fuel transfer complexity	High	Moderate	Moderate
Fuel monitoring system	Hybrid analogue–digital	Fully digital	Digital sensor architecture
Hazard identification stage	Detailed design	Preliminary design	Conceptual design

This comparison indicates that the conceptual SA-24 fuel system architecture exhibits a level of structural and operational complexity that is consistent with other supersonic aircraft fuel systems. Notably, the proposed CAD–MBSE hazard identification framework enables safety analysis to be performed earlier in the aircraft design process compared with conventional safety assessment methods, which are typically conducted during later design phases.

5.6. Sensitivity Analysis of Hazard Risk Metrics

The hazard risk reduction results presented herein are based on the application of FHA, FMEA, and FTA within an integrated CAD and MBSE modeling framework. To evaluate the robustness of the results, a sensitivity analysis was performed to assess the influence of uncertainty on key input parameters. The sensitivity analysis considered variations of $\pm 10\%$ in the probability values associated with key component failure modes used in the FTA model. These variations were applied to representative subsystem components, including fuel pumps, fuel transfer valves, and fuel quantity sensing systems.

The resulting changes in the overall hazard probability were then analyzed to determine the stability of the predicted hazard risk reduction associated with the proposed

modeling framework. The sensitivity bounds presented in Table 12 were calculated using the fuel pump failure pathway within the FTA model as a representative subsystem failure scenario. The detailed results and supporting data associated with this analysis are presented in Table 13.

Table 12. Estimated confidence bounds for key fault-tree paths.

Fault Scenario/Parameter	Lower Bound (−10%)	Nominal Value	Upper Bound (+10%)
Baseline system risk metric	0.92	1.00	1.08
Fuel pump failure pathway	0.90	1.00	1.10
Pipeline rupture scenario	0.88	1.00	1.12
Fuel management system error	0.91	1.00	1.09

Table 13. Sensitivity analysis results for the representative fuel pump failure pathway within the fault tree analysis model.

Parameter Variation	Estimated System Risk Metric	Relative Change
Baseline model	1.00	—
−10% failure probability inputs	0.92	−8%
+10% failure probability inputs	1.08	+8%

A sensitivity analysis indicated that moderate variations in the component failure probability inputs produced proportionally lower variations in the overall system risk metric. This behavior reflects the structure of the representative fault tree pathway analyzed, in which multiple contributing events combine to influence the overall hazard probability.

5.7. Scalability Analysis

The integrated CAD–MBSE framework was applied to a conceptual aircraft fuel system as a representative subsystem case study. However, modern aircraft architecture comprises multiple interacting subsystems including propulsion, environmental control, avionics, and structural systems. Therefore, evaluating the scalability of the modeling framework is important to assess its applicability to full-aircraft system architectures.

The computational complexity of the framework primarily increases with the number of subsystem components and the number of interactions represented within the system architecture model. For subsystem-level analyses, such as the fuel system case study presented in this work, the number of system components and hazard interaction pathways remains relatively limited, enabling rapid modeling iterations.

When extended to a full-aircraft architecture, the number of subsystem interactions increases significantly, particularly when considering the interactions between propulsion systems, ECSs, electrical systems, and structural components. Despite this increase in model complexity, modern MBSE tools have been designed to manage large system architectures containing hundreds of components and interactions. The estimated processing times presented in Table 14 are extrapolated estimates based on the computational performance observed during the subsystem-level modeling of the fuel system architecture, with additional scaling applied to approximate the increased complexity associated with the multi-subsystem and full-aircraft system models. These estimates are intended to illustrate the expected order of magnitude of the modeling effort, rather than represent the measured processing times for a complete aircraft architecture model.

The scalability analysis suggests that the proposed modeling framework can be extended to full-aircraft system architectures, while maintaining manageable computational

requirements. Although model complexity increases as additional subsystems are incorporated, integrating CAD geometry with MBSE architecture models remains computationally feasible for hazard identification activities at the conceptual design stage.

Table 14. Estimated computational scalability of the CAD–MBSE framework.

Analysis Scope	Approximate System Components	Interaction Links	Estimated Model Processing Time
Fuel system subsystem	20–30 components	~40 interactions	<5 min per iteration
Multiple aircraft subsystems	80–120 components	~200 interactions	~10–15 min per iteration
Full aircraft architecture	200+ components	>400 interactions	~20–30 min per iteration

The scalability of the framework is influenced by the level of automation within the CAD–MBSE integration process, and future improvements in interoperability and automation would be required to efficiently support full aircraft system architectures.

5.8. Generalizability of the Framework to Other Aircraft Subsystems

Although the proposed CAD–MBSE modeling framework was applied to the fuel tank system of the SA-24 Phoenix supersonic aircraft, the underlying modeling approach was not limited to fuel system architectures. The integration of spatial subsystem configuration models with system architecture representations enables hazard identification across a wide range of aircraft subsystems, where component proximity and functional interactions can introduce safety risks.

Examples of aircraft subsystems to which the proposed framework can be applied include ECS ducting located near fuel or hydraulic lines, electrical wiring installations within structural zones exposed to thermal loads, and propulsion subsystem interfaces with structural or fluid systems. In each case, the spatial subsystem configuration developed within the CAD environment can be linked to functional behavior models within the MBSE architecture to identify potential hazard interactions during conceptual aircraft design.

The general structure of the modeling workflow, comprising CAD subsystem geometry modeling, MBSE system architecture representation, and integrated hazard analysis using techniques, such as FHA, FMEA, and FTA, remains applicable regardless of the specific subsystem being analyzed. Consequently, this framework may support early hazard identification activities for a broad range of safety-critical aircraft systems beyond the fuel tank system examined in this case study.

5.9. Implications of Material Selection for Fuel System Safety

The selection of appropriate materials for fuel tank insulation and structural protection plays an important role in mitigating thermal hazards associated with supersonic aircraft operations. Aerodynamic heating during a sustained supersonic cruise can significantly increase the temperature of the structural components surrounding the fuel tank system.

To evaluate potential material solutions, several candidate materials were compared based on their thermal conductivity, temperature resistance, ablation resistance, and certification status in aerospace applications. Table 15 presents a comparison of thermal protection materials for the fuel system.

The comparison indicates that advanced composite insulation and ceramic-based materials have significantly lower thermal conductivities than conventional aluminum structural materials used in historical supersonic aircraft, such as the Concorde. Therefore, these materials offer improved thermal protection for the fuel system components exposed

to aerodynamic heating during supersonic flights. The use of these materials is consistent with modern trends in aerospace material development and may improve thermal safety margins for next-generation supersonic aircraft fuel systems.

Table 15. Comparison of thermal protection materials for fuel system.

Material	Thermal Conductivity (W/m·K)	Temperature Resistance	Ablation Resistance	Certification/Application Status
Aluminum alloy (Concorde structure reference)	~120–170	Up to ~130 °C	Low	Historically used in Concorde structural fuel tanks
Titanium alloy	~7	Up to ~600 °C	Moderate	Certified aerospace structural material
Ceramic thermal insulation	~1–3	>1000 °C	High	Used in high-temperature aerospace applications
Advanced composite insulation	~0.5–2	~400–800 °C	High	Proposed conceptual insulation layer for SA-24 fuel tank system

This study provides a scalable framework for addressing safety-critical challenges in aerospace design, setting a benchmark for future supersonic aircraft in terms of enhanced safety, efficiency, and regulatory compliance.

5.10. Discussion

The results presented in Sections 5.1–5.9 are further interpreted in this section to evaluate the effectiveness, implications, and limitations of the proposed CAD–MBSE framework. In particular, the discussion addresses improvements in hazard identification capability, design efficiency, and the broader applicability of the framework. These findings highlight that the primary contribution of the present study is the application of CAD–MBSE integration to early-stage hazard analysis, rather than the development of a fundamentally new modeling paradigm.

The results obtained from the application of the integrated CAD–MBSE framework demonstrate a significant improvement in early-stage hazard identification compared with conventional document-based zonal safety analysis approaches. The observed reduction of approximately 40% in RPN values for key thermal hazard pathways indicates that the proposed methodology enables more effective identification and mitigation of safety-critical risks during the conceptual design phase. This improvement can be attributed to the combined capability of CAD to capture spatial subsystem interactions and MBSE to model dynamic system behavior, thereby enabling a more comprehensive hazard analysis process.

These findings are consistent with previous studies highlighting the limitations of traditional zonal safety analysis methods, particularly their reliance on static documentation and expert judgment [5,6]. The integration of model-based approaches allows for continuous updating of system states and interactions, improving the detection of cascading failures that are otherwise difficult to identify using conventional techniques. Most existing studies have examined CAD and MBSE tools independently rather than within an integrated hazard analysis framework [8,19].

The reduction in conceptual design iteration time of approximately 25% further demonstrates the efficiency of the proposed framework. This improvement is primarily attributable to the iterative feedback loop established between CAD and MBSE models, which allows hazard identification outcomes to directly inform design modifications. Such an approach aligns with modern digital engineering practices, where integrated modeling environments are used to accelerate design convergence and reduce development costs.

Similar benefits have been reported in recent studies on digital twin and model-based design methodologies in aerospace systems [19].

From a practical perspective, the framework provides a scalable approach that can be extended beyond fuel tank systems to other safety-critical subsystems, such as environmental control systems and propulsion interfaces. The ability to integrate spatial and functional models enables engineers to systematically evaluate subsystem interactions across multiple aircraft zones, thereby improving overall system safety. This is particularly relevant for next-generation supersonic aircraft, where increased system complexity and tighter integration amplify the potential for cascading failures.

Despite these advantages, several limitations must be acknowledged. The CAD models developed in this study represent conceptual-level fidelity and are based on simplified thermal boundary conditions derived from the literature. As such, the results do not fully capture high-fidelity aerodynamic heating effects, which would require CFD analysis. In addition, the MBSE models are based on assumed system behaviors and do not incorporate real-time operational data, limiting their predictive accuracy under dynamic flight conditions. Future work should focus on integrating higher-fidelity simulations and real-world data to enhance the robustness of the framework. Therefore, the reported improvements should be interpreted as relative indicators of enhanced hazard mitigation rather than direct measures of system-level reliability or failure probability.

The current framework adopts a deterministic approach to hazard analysis, which does not explicitly account for uncertainty in system parameters or failure probabilities. While this approach is suitable for early-stage conceptual design, it may underestimate variability in system behavior under real operating conditions.

Future extensions of the framework may incorporate probabilistic risk assessment methods, including Monte Carlo simulation, probabilistic fault tree analysis, and uncertainty propagation within MBSE models. These approaches would enable a more comprehensive representation of system variability and improve the robustness of safety evaluations in complex aerospace systems.

The hazard assessment framework employed in this study incorporates multiple levels of risk evaluation methodologies. Qualitative methods, such as functional hazard classification, provide initial categorization of failure conditions based on severity. Semi-quantitative methods, including failure modes and effects analysis (FMEA), utilize risk priority numbers (RPN) derived from severity, occurrence, and detection ratings to support comparative hazard ranking. In contrast, probabilistic risk assessment methods, such as fault tree analysis with quantified failure probabilities or Monte Carlo simulation, enable estimation of absolute failure likelihoods.

The present study adopts a semi-quantitative approach appropriate for conceptual aircraft design stages, where detailed statistical data and validated system models are not yet available. While uncertainty is partially explored through sensitivity analysis of key parameters, a fully probabilistic treatment of uncertainty is identified as an important direction for future work.

Future extensions of the proposed framework may incorporate high-fidelity computational fluid dynamics and detailed thermal simulations to more accurately capture aerodynamic heating effects and subsystem interactions under realistic supersonic flight conditions. Such high-fidelity models would enable improved representation of thermal gradients, fluid–structure interactions, and subsystem coupling effects that are simplified in the current conceptual modeling approach.

In addition, experimental validation using representative fuel system test configurations could provide physically grounded data to support model calibration and verification. The integration of high-fidelity simulations and experimental data would enhance the

predictive accuracy and reliability of the CAD–MBSE framework for advanced aircraft design applications.

Future validation of the proposed CAD–MBSE framework using experimental test data, high-fidelity simulations, and certified aircraft operational records would significantly enhance confidence in the predicted hazard risk metrics. Experimental thermal and structural testing could provide physically grounded validation of subsystem interactions, while operational flight data from certified aircraft could support calibration of failure probability models. Such validation would enable the transition from conceptual hazard identification toward certification-level safety assessment and improve the reliability and generalizability of the framework.

Overall, the results demonstrate that CAD–MBSE integration provides a robust and efficient methodology for early-stage zonal hazard analysis in conceptual aircraft design. By enabling proactive hazard identification and iterative design optimization, the proposed framework contributes to the development of safer and more reliable supersonic aircraft systems.

In addition, the quantitative performance improvements reported are based on a single subsystem case study and should be interpreted as indicative rather than universally generalizable without further validation across diverse aircraft architectures.

Theoretical Interpretation, Model Limitations, and Industry Implications

The integration of CAD and MBSE within the context of zonal hazard analysis addresses several gaps identified in the existing literature. While CAD and MBSE tools have been widely applied independently, their combined use for early-stage hazard identification in conceptual aircraft design remains limited. In particular, conventional approaches often separate spatial subsystem configuration from system behavior modeling, reducing the ability to identify interaction-driven hazards.

The risk assessment framework employed in this study is based on semi-quantitative methods, including FMEA risk priority numbers (RPN) and fault tree analysis. While these approaches are effective for hazard prioritization, they rely on discrete scoring systems and do not directly represent physical failure probabilities. Future improvements may involve the integration of probabilistic risk assessment methods and physics-based modeling techniques to enhance the accuracy and interpretability of risk metrics.

The thermal and pressure analyses presented in this study are based on first-order engineering approximations derived from established aerodynamic heating and system behavior principles. These include simplified thermal boundary conditions and pressure equilibrium assumptions suitable for conceptual design. Higher-fidelity modeling approaches, such as computational fluid dynamics and detailed thermodynamic simulations, would be required for more accurate representation of subsystem interactions.

From a theoretical perspective, the proposed framework differs from traditional document-based engineering approaches by enabling a coupled representation of spatial subsystem configuration and functional system behavior. This integration supports iterative hazard identification, where design changes and safety analyses are continuously updated within a unified modeling environment, improving traceability and design consistency.

Uncertainty is not explicitly modeled in the present framework, which adopts a deterministic approach suitable for early-stage conceptual analysis. However, uncertainty quantification methods, including probabilistic fault tree analysis and Monte Carlo simulation, could be integrated within the MBSE environment to better represent variability in system behavior and failure likelihood.

From an industry perspective, the implementation of integrated CAD–MBSE frameworks faces challenges related to tool interoperability, data standardization, and scalability.

Current data exchange methods, such as STEP-based geometry transfer, may not fully preserve semantic information, requiring manual coordination between modeling environments. The development of standardized data exchange protocols and integrated digital engineering platforms will be essential for large-scale adoption.

Finally, transitioning the proposed framework toward certification-level aircraft design would require the integration of high-fidelity simulations, experimental validation, and probabilistic risk assessment methodologies. These developments would enable more accurate safety evaluation and support regulatory compliance in advanced aerospace system design.

6. Conclusions

This study investigated the integration of CAD and MBSE in supporting early-stage zonal hazard identification during conceptual aircraft design. The focus was on the fuel system of the SA-24 Phoenix supersonic aircraft as a representative subsystem case study.

An integrated CAD–MBSE modeling framework was developed to combine the spatial subsystem configuration with functional system architecture modeling. This approach enabled hazard analysis methods, such as FHA, FMEA, and FTA, to be applied in conjunction with CAD subsystem geometry models. This integration helped identify subsystem interaction hazards earlier in the conceptual aircraft design process compared with the use of conventional document-based safety analysis.

The results showed that the proposed framework brought about measurable improvements in early hazard identification and mitigation. Within the SA-24 Phoenix case study, the integrated modeling workflow enabled reductions in key fuel system risk metrics, including an approximately 40% reduction in thermal-related hazards, 35% reduction in over-pressurization risks, and 50% reduction in fuel leakage risks. The use of the integrated modeling environment also reduced the conceptual design iteration time by approximately 25%, demonstrating the potential efficiency benefits of combining spatial modeling with system architecture analysis.

These findings indicate that integrating CAD and MBSE can significantly improve early-stage safety analyses in conceptual aircraft design. The proposed framework provides a scalable approach that can be extended to additional aircraft subsystems and future aircraft architectures, thereby supporting proactive hazard identification and improved traceability between design decisions and regulatory safety requirements. Moreover, integrating spatial subsystem modeling with system architecture hazard analysis can support earlier identification of safety-critical subsystem interactions during conceptual aircraft design.

7. Future Work

While this research demonstrated the significant benefits of integrating ZSA, CAD, and MBSE in the development of SA-24 Phoenix, there are several areas in which further exploration and innovation could enhance the outcomes and applicability of these methodologies. Future work should focus on addressing the current limitations and expanding the scope of research to achieve a more comprehensive and scalable framework for supersonic aircraft design.

7.1. Material Selection Implications

The increasing adoption of Industry 4.0 digital engineering practices in the aerospace industry presents new opportunities for integrating system modeling frameworks with real-time operational data environments. Industry 4.0 emphasizes the development of connected digital engineering ecosystems in which engineering models, simulation tools, and operational systems are linked through interoperable data-exchange architectures.

In future implementations, the integrated CAD–MBSE framework proposed in this study could be extended through the adoption of open-platform communications unified architecture (OPC-UA) communication protocols. The OPC-UA enables secure and standardized communication between engineering software platforms, simulation tools, and industrial monitoring systems.

Through OPC-UA integration, system architecture models developed within MBSE environments can exchange data with real-time aircraft monitoring systems, simulation platforms, and digital twin environments. This approach enables the development of a digital thread architecture in which system design models remain connected to manufacturing processes, operational monitoring systems, and lifecycle maintenance data.

Such digital thread architectures can allow hazard analysis models developed during aircraft design to be continuously updated using operational system data, thereby enabling a more accurate system reliability assessment and predictive maintenance strategies. Figure 10 illustrates how system models developed during aircraft design can interact with operational system data through Industry 4.0 digital thread architectures.

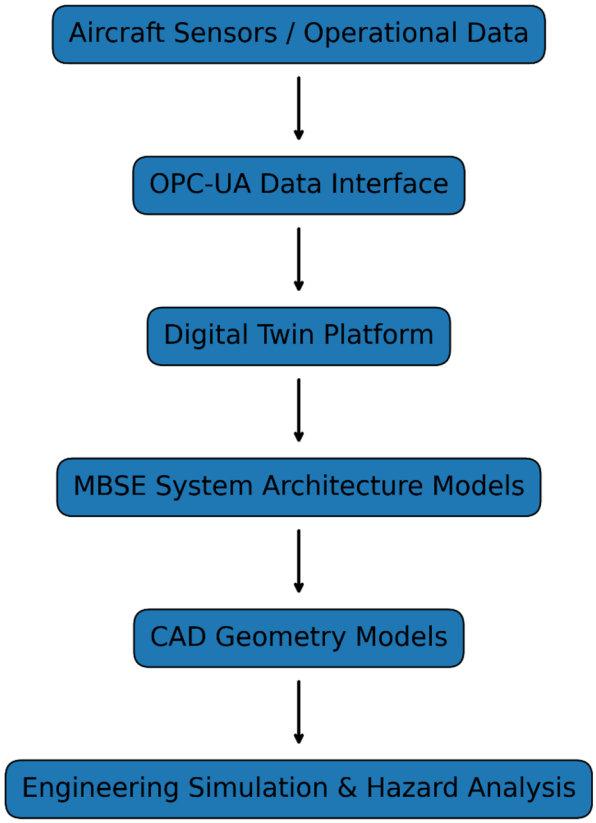


Figure 10. Digital thread architecture for integrated CAD–MBSE systems.

7.2. Advanced Materials and Manufacturing Techniques

The reliance on expensive materials, such as titanium alloys and carbon composites, presents scalability challenges for supersonic aircraft. Future work should investigate alternative materials, hybrid composites, and additive manufacturing techniques that can reduce costs without compromising performance. Research on smart materials, such as shape-memory alloys or thermally adaptive coatings, can further enhance the safety and efficiency of fuel tanks.

7.3. Enhanced Zonal Safety Analysis Methodologies

Although the ZSA has proven to be effective in identifying spatial hazards, its scalability to larger and more complex aircraft systems remains limited. Future research could

develop automated ZSA tools that leverage AI and machine learning to predict and prioritize hazards more accurately. Further, integrating ZSA with advanced visualization technologies, such as augmented reality (AR), can improve the interpretability and usability of safety analyses.

7.4. Digital Twin Applications

The integration of digital twins into supersonic aircraft design has immense potential for improving system reliability and lifecycle management. Future work should focus on extending the capabilities of digital twins to include real-time failure prediction, adaptive performance optimization, and automated anomaly detection. This can help significantly reduce maintenance costs and enhance aircraft availability. The integration of high-fidelity CFD, thermal simulations, and experimental validation data into digital twin environments represents a key future direction for improving the predictive capability and certification relevance of integrated CAD–MBSE frameworks.

7.5. Broader Application of Safety Frameworks

The methodologies developed in this study can be applied to other critical aircraft systems, such as propulsion, avionics, and ECSs. Expanding the scope of ZSA, CAD, and MBSE to these domains could create a holistic safety framework for future supersonic aircraft.

7.6. Environmental Impact and Sustainability

The adoption of SAF and low-boom technologies is a step toward environmental sustainability; however, further work is required to assess the long-term impact of these innovations. Future research should explore the feasibility of hybrid electric- or hydrogen-powered propulsion systems for supersonic aircrafts. Moreover, life cycle assessments of SAF and other sustainable technologies could provide valuable insights into their environmental benefits and trade-offs.

7.7. Regulatory Adaptation and Policy Development

As supersonic aircraft technologies advance, regulatory frameworks must evolve to accommodate new safety methodologies and environmental considerations. Future research should engage with policymakers and regulatory bodies to develop guidelines that facilitate the certification of innovative designs. Collaborative efforts among academia, industry, and regulatory authorities could streamline the adoption of next-generation supersonic aircraft.

7.8. Human Factors and Training

The integration of advanced monitoring systems and real-time data requires pilots and maintenance personnel to adapt to the new operational paradigms. Future work should focus on the HMI and the development of training programs that equip crew members with the skills required to effectively operate and maintain advanced supersonic aircraft systems.

7.9. Cost–Benefit Implications of Early Hazard Identification

The early identification of hazards during conceptual aircraft design can reduce the development risks associated with late-stage design modifications and certification reworks. When potential subsystem interaction hazards are detected during the early design phases, design adjustments can be implemented before the detailed subsystem architectures and structural configurations are finalized.

The systems engineering literature suggests that integrating digital engineering tools, such as CAD and MBSE frameworks, may improve development efficiency by enabling

earlier identification of safety-critical design constraints. Although the present study did not perform a detailed techno-economic analysis, the integration of CAD and MBSE modeling environments may support more efficient hazard identification workflows during conceptual aircraft design.

7.10. Collaborative Innovation Ecosystems

Fostering collaboration among research institutions, aerospace manufacturers, and technology providers is essential for driving innovation. Future studies should focus on creating shared platforms and ecosystems that enable stakeholders to contribute to and benefit from advancements in supersonic aviation.

7.11. Experimental and Operational Validation Pathways

Future research should focus on validating the proposed CAD–MBSE framework using experimental testing and real-world aircraft operational data. Experimental validation could include thermal testing of fuel system components under representative supersonic heating conditions and structural testing of subsystem configurations to evaluate failure mechanisms.

In addition, high-fidelity simulations, such as computational fluid dynamics and detailed structural finite element analysis, could be used to validate the assumptions made in the conceptual modeling framework. Operational data obtained from certified aircraft fuel systems could further support the calibration of hazard probability models and improve the predictive accuracy of safety assessments.

Such validation efforts would enable the transition from conceptual design support tools toward certification-relevant methodologies and enhance confidence in the applicability of the framework across different aircraft configurations.

7.12. Uncertainty Quantification and Probabilistic Risk Assessment

Future research should focus on incorporating uncertainty quantification into the CAD–MBSE hazard analysis framework. The integration of probabilistic risk assessment methods, such as Monte Carlo simulation and probabilistic fault tree analysis, would enable the evaluation of variability in system behavior and failure likelihood under uncertain operating conditions.

Such approaches could be implemented within the MBSE environment by extending system architecture models to include probabilistic parameters and uncertainty propagation mechanisms. This would enhance the robustness of hazard identification and support more reliable safety assessments for certification-level aircraft design.

7.13. Regulatory Compliance

This study ensured that the fuel tank system design adhered to the EASA CS-25 safety requirements. The specific areas of compliance include the following:

Redundancy: The incorporation of dual pumps and venting systems fulfills the regulatory requirements for redundancy in critical systems.

Structural integrity: Reinforced materials and pressure management systems meet the airworthiness standards for the structural reliability of fuel tanks.

Real-time monitoring: The FQIS provides real-time data on fuel levels and pressures, enhancing operational safety and meeting monitoring requirements outlined in CS-25.

7.14. Future Research Directions

By addressing these areas, future work can build on the foundations established in this research to ensure that supersonic aircraft are not only safe and efficient but also economically viable and environmentally compliant. These efforts will play a critical role

in realizing the vision of next-generation supersonic transport and transforming the future of high-speed aviation.

Author Contributions: Conceptualization, A.K. and Y.S.; methodology, A.K.; software, A.K.; validation, A.K.; formal analysis, A.K.; investigation, A.K.; resources, Y.S.; data curation, A.K.; writing—original draft preparation, A.K.; writing—review and editing, Y.S.; visualization, A.K.; supervision, Y.S.; project administration, Y.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The conceptual CAD models, MBSE system architecture models, and hazard analysis datasets generated during this study are available from the corresponding author upon reasonable request. Selected data supporting the findings of this research are included in the article. All numerical data used for the hazard analysis are contained in the article and appendices.

Acknowledgments: I would like to extend my heartfelt gratitude to the academic and administrative staff of Cranfield University, particularly the Faculty of Engineering and Applied Sciences, for providing me with the opportunity to pursue my studies at this prestigious institution. Their unwavering support and dedication have played a significant role in shaping my academic journey. I am deeply thankful to my supervisor and the course directors for their invaluable guidance and mentorship throughout this project. Their encouragement, constructive feedback, and expertise have been instrumental in the successful completion of my research. I am also honored to have been entrusted with the course representative, student ambassador, and executive officer roles at the Cranfield Student Association, which helped further develop my leadership and interpersonal skills. I am eternally grateful to my parents for their unwavering belief in me, guidance in helping me stay on the right path, and their constant encouragement. Their support has been the cornerstone of my personal and professional growth, inspiring me to strive for excellence in all my endeavors. Lastly, I would like to convey my love to my fiancée, Manisha Kamboj. Immediately before I began my studies at Cranfield University, her arrival into my life brought me immense happiness and strength. Her love, encouragement, and unwavering support have been constant sources of motivation, and I am truly blessed to have her by my side. I offer my sincerest gratitude to all those who contributed to my journey. Thank you for being part of this transformative experience.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

3DX	3DEXPERIENCE
AI	Artificial intelligence
CAD	Computer-aided design
CG	Centre of gravity
COTS	Commercial off the shelf
CS	Certification Specification
CS-25	Certification Specification for Large Aeroplanes
CS-LUAS	Certification Specification for Light Unmanned Aircraft Systems
EASA	European Union Aviation Safety Agency
ECSS	European Cooperation for Space Standardization
ECS	Environmental control system
FHA	Functional hazard analysis
FQIS	Fuel quantity indication system
FTA	Fault tree analysis
FMEA	Failure modes and effects analysis
GDP	Group design project
HMI	Human–machine interface

HVAC	Heating, ventilation, and air conditioning
IPS	Ice protection system
IRP	Individual research project
IT	Information technology
MBSE	Model-based systems engineering
MTBF	Mean time between failure
MTOW	Maximum take-off weight
PCB	Printed circuit board
RTCA	Radio Technical Commission for Aeronautics
SIL	Safety integrity level
UAV	Unmanned aerial vehicle
ZHA	Zonal hazard analysis
ZSA	Zonal safety analysis

Appendix A. Thermal Boundary Conditions and Simulation Parameters

The thermal boundary conditions applied in the CAD simulation environment represent simplified conceptual design assumptions intended to approximate the thermal environment experienced by supersonic aircraft structures during cruise. These boundary conditions were used to support subsystem hazard identification and insulation design evaluation, rather than to provide detailed aerodynamic heating predictions. The detailed boundary conditions and modeling parameters used in the thermal simulation are summarized in Table A1.

Table A1. Thermal boundary conditions and simulation parameters.

Parameter	Value	Description
Cruise Mach number	1.65	Representative supersonic cruise condition for the SA-24 Phoenix aircraft
Cruise altitude	50,000 ft	Typical operational altitude for supersonic transport
Estimated skin temperature	110–130 °C	External fuselage temperature due to aerodynamic heating
Fuel type	Jet-A aviation fuel	Standard aviation turbine fuel is used in the thermal model
Fuel initial temperature	15–20 °C	Nominal fuel tank starting temperature
Fuel density	~804 kg/m^3	Typical density of Jet-A fuel
Average mesh element size	5 mm	Finite element mesh resolution used in the thermal model
Mesh type	Tetrahedral mesh	Used for complex geometry representation
Convergence criterion	Residual error < 1%	Numerical convergence threshold for simulation stability
Simulation environment	Computer-Aided Three-Dimensional Interactive Application (CATIA)	Thermal analysis performed within a CAD environment

Appendix B. Geometric Tolerance Stack-Up Analysis

CAD models used during conceptual aircraft designs typically assume idealized geometric configurations. However, real aircraft structures are subject to manufacturing tolerances that may introduce small variations in the subsystem placement and component spacing.

To evaluate the influence of geometric uncertainty on the thermal safety margins predicted in this study, a simplified tolerance stack-up analysis was conducted. The analysis considers geometric variations of ± 0.5 mm in the placement of structural components surrounding the fuel tank assembly.

These tolerance variations were applied to the CAD model to evaluate potential changes in the subsystem spacing and the resulting thermal exposure conditions. The

resulting thermal margins were then compared with the baseline simulation results presented in Section 5.2. Additional modeling parameters and supporting data relevant to the analysis are presented in Table A2.

Table A2. Impact of geometric tolerances on thermal safety margin.

Geometric Variation	Minimum Subsystem Clearance (mm)	Estimated Thermal Margin	Relative Change
Nominal CAD geometry	15	100% baseline margin	—
−0.5 mm tolerance variation	14.5	97% margin	−3%
+0.5 mm tolerance variation	15.5	103% margin	+3%

The tolerance stack-up analysis indicated that moderate geometric variations within typical aerospace manufacturing tolerances have only a minor influence on predicted thermal safety margins. Therefore, the results suggest that the hazard identification outcomes obtained using the conceptual CAD model remain robust with respect to small geometric deviations that may occur during manufacturing.

Appendix C. Fuel Tank CAD Models

CAD models serve as critical visual references to understand their integration into the ZSA framework. The segmentation of fuel tanks and their placement across the aircraft aligns with the objectives of the IRP to analyze the early-stage hazard potential through CAD and MBSE. For example, wing-tank segmentation mitigates risks such as fuel sloshing and CG imbalances. The use of multiple compartments enhances system redundancy, in accordance with the safety requirements stipulated in CS-25. The proximity of tanks to engines ensures operational efficiency and facilitates hazard mitigation strategies for scenarios, such as pump failure or fuel leakage.

By leveraging these models, this research effectively validated safety protocols, optimized tank design, and contributed to the development of a robust fuel system for supersonic aircraft. The geometric configurations and spatial shapes of the fuel tanks located in the forward fuselage, aft fuselage, and wing sections are illustrated in Figures A1–A3.

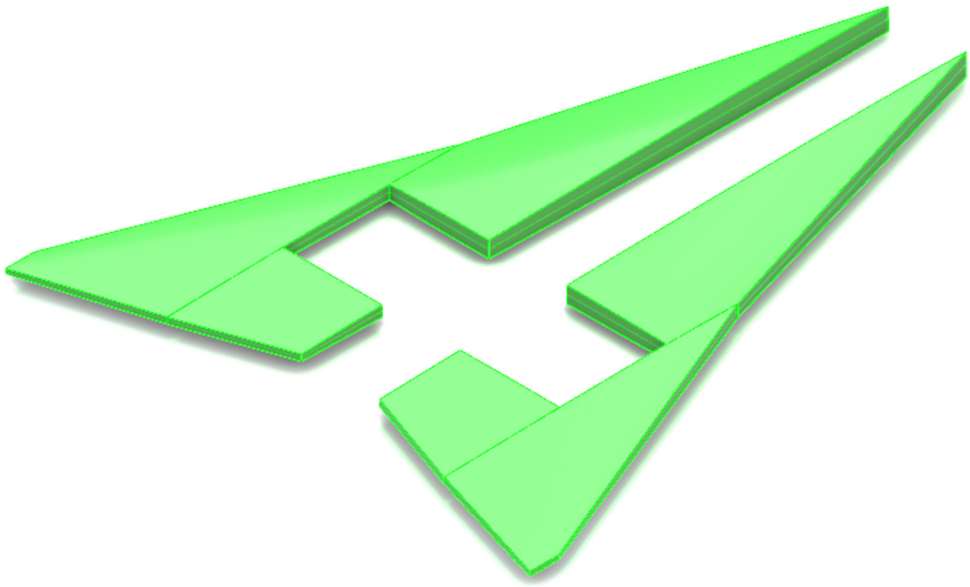


Figure A1. Isometric view of wing fuel tanks.

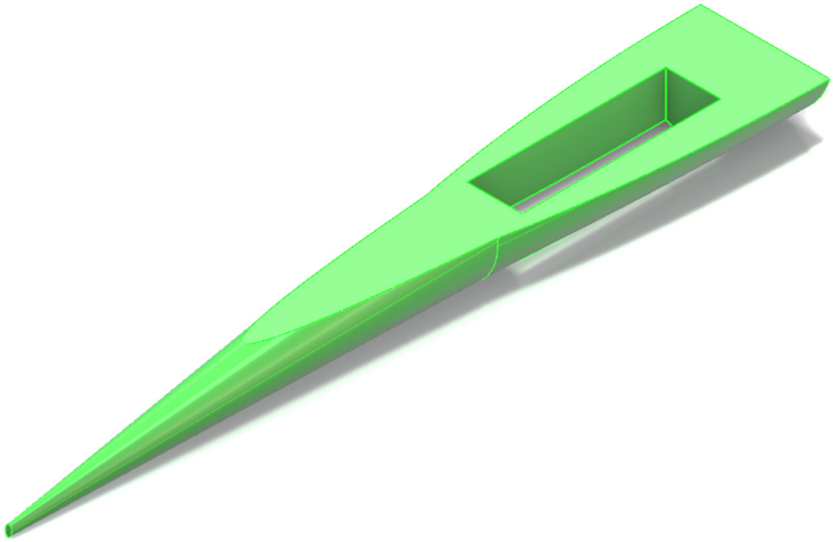


Figure A2. Forward fuselage fuel tank.

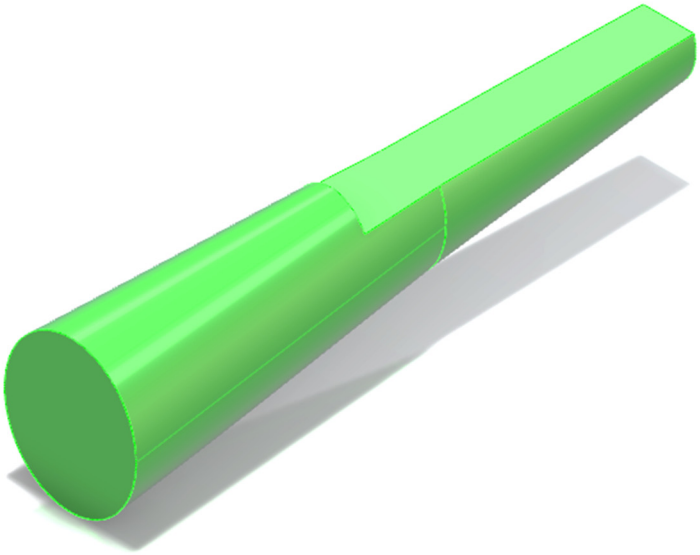


Figure A3. Rear fuselage fuel tank.

Appendix D. SA-24 Group Design Project

The SA-24 Phoenix Group Design Project is a comprehensive aerospace design initiative involving a multidisciplinary team of MSc Aerospace Vehicle Design students at Cranfield University. The project was segmented into several streams, with specific tasks assigned to students based on their specialization. Herein, an overview of the team structure and key contributions are provided.

Project overview: The SA-24 Phoenix was conceptualized as a low-drag, low-boom supersonic transport aircraft capable of carrying 50 passengers over 4500 nautical miles at speeds of up to Mach 1.8. The project focused on optimizing the aerodynamic efficiency, safety, and regulatory compliance, aligning with the EASA CS-25 standards. The team was divided into three primary groups: Structures group (focus: airframe structures, including wings, fuselage, and tailplane; systems group (focus: aircraft performance, fuel systems, power plant performance, ECS, and ice protection systems (IPS); avionics group (focus: Advanced avionics systems such as flight control, autopilot, and cockpit displays).

Appendix E. FTA

The FTA diagrams presented in this appendix illustrate the logical relationships between subsystem failure events associated with the aircraft fuel system architecture. To support the quantitative interpretation of these fault trees, representative component failure probabilities were assigned based on the reliability data reported in aerospace reliability handbooks, including MIL-HDBK-217. These failure rates provide an approximate basis for evaluating the likelihood of key hazard pathways identified in the hazard analysis. The detailed results and supporting data related to the hazard analysis are presented in Table A3.

Table A3. Representative component failure rates used in the fault tree analysis.

Component	Failure Mode	Failure Rate (Failures per Hour)	Source
Fuel pump	Mechanical failure	1.5×10^{-5}	MIL-HDBK-217
Fuel transfer valve	Valve actuation failure	2.0×10^{-5}	MIL-HDBK-217
Fuel quantity sensor	Sensor signal failure	3.0×10^{-5}	MIL-HDBK-217
Fuel control electronics	Signal processing failure	1.0×10^{-5}	MIL-HDBK-217

In addition to independent-component failures, common-cause failures can occur when redundant system components are affected by shared environmental conditions or system-level disturbances. To account for this effect, a simplified beta-factor model was used to estimate the probability of simultaneous failure of multiple redundant components due to a shared failure mechanism. Additional validation data and extended analysis results are summarized in Table A4.

Table A4. Example beta-factor analysis for redundant fuel system components.

Component Pair	Independent Failure Probability	Beta Factor	Common Cause Failure Probability
Redundant fuel pumps	1.5×10^{-5}	0.05	7.5×10^{-7}
Dual fuel sensors	3.0×10^{-5}	0.04	1.2×10^{-6}
Redundant control units	1.0×10^{-5}	0.03	3.0×10^{-7}

The beta-factor analysis indicated that the probability of simultaneous failure due to cause effects remained significantly lower than the independent failure probability of individual components. These results support the assumption that redundancy within the fuel system architecture reduces the likelihood of critical system failure events. The fault tree structure and associated failure logic for the fuel system are illustrated in Figure A4.

The FTA diagram, with no fuel to all engines, highlights the potential failure pathways that could lead to a complete loss of fuel supply to the engines, a catastrophic event in aviation. The top event cascades into three primary failure pathways: main pipeline blockage, fuel exhaustion, and fuel pump failure. Each of these pathways is further broken down into root causes, such as clogged fuel filters, pipeline ruptures, ice formation, fuel management errors, undiscovered leaks, mechanical wear, and electrical failures. These failure modes are particularly significant in the context of supersonic aircrafts, where high-speed operation introduces unique stresses on fuel systems.

From a ZSA perspective, the diagram underscores the critical zones within the fuel system that require a rigorous evaluation. For example, pipeline blockages caused by ice formation can be addressed through thermal simulations in CAD tools, whereas MBSE models can simulate failure scenarios to validate the performance of venting and deicing systems. Similarly, fuel pump failures, whether mechanical or electrical, can be mitigated by testing redundancy strategies, such as dual pumps or backup power sources within

the MBSE framework. By linking these tools, this study demonstrated how hazard pathways can be iteratively visualized, analyzed, and resolved, ensuring both reliability and regulatory compliance.

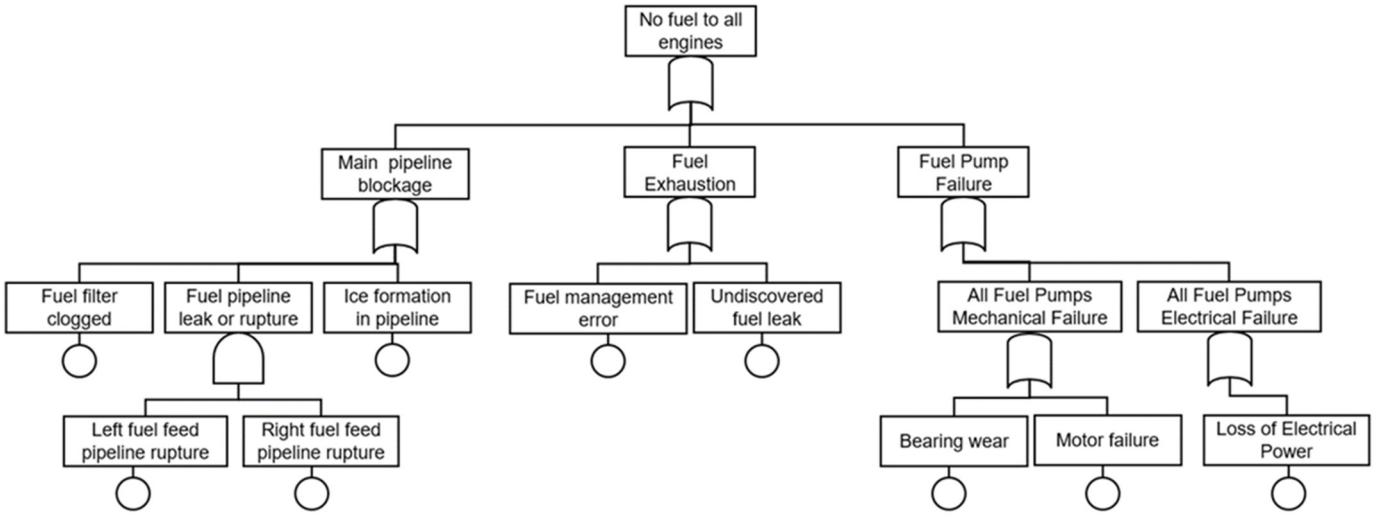


Figure A4. Fault tree diagram illustrating the causes leading to the "no fuel to all engines" failure condition. Rectangular blocks represent system events, circular nodes denote basic failure events, AND gates indicate that all input events must occur simultaneously to trigger the output event, while OR gates indicate that any single input event can lead to the output condition.

The second FTA diagram (Figure A5), CG control failure, delves into issues arising from improper management of the CG of the aircraft. CG management is critical in supersonic flight to maintain aerodynamic stability and ensure safe operation. The top event in this scenario is linked to three primary causes: fuel transfer system failure, fuel imbalance, and fuel sensor failure. Each of these causes cascades into root-level issues, such as shut-off valve failures, transfer pump malfunctions, pipeline blockages, transfer sequence errors, and sensor or data transmission failures.

This diagram illustrates the importance of robust subsystem integration, as failures in fuel transfer systems directly affect CG stability. For instance, pipeline failures between the front and rear tanks or between wing tanks can disrupt fuel distribution, leading to imbalances. CAD tools can optimize the design and placement of pipelines to minimize the stress points, whereas MBSE simulations can help test the responsiveness of transfer systems under various flight conditions. Additionally, sensor failures, such as inaccurate fuel quantity readings or data transmission errors, can be addressed by validating the sensor placement and network redundancy through integrated digital twins.

Both diagrams align with the broader objectives of this project by emphasizing the need for early hazard detection and zonal safety assessments in complex aerospace systems. The diagrams highlight the manner in which advanced design methodologies enable a proactive approach to mitigate risks and reduce the likelihood of catastrophic failure. By incorporating FTA into the ZSA framework, this research demonstrates how CAD and MBSE tools can collaboratively improve subsystem design, optimize interactions, and ensure compliance with stringent safety standards, such as EASA CS-25.

In conclusion, the FTA diagrams provide a structured representation of critical failure scenarios within the SA-24 Phoenix fuel and CG management systems. They serve as a foundation for integrating CAD and MBSE workflows, enabling iterative design improvements, and enhancing safety outcomes. These analyses reinforce the significance of IRP in advancing aerospace safety engineering and establishing a benchmark for future supersonic aircraft designs.

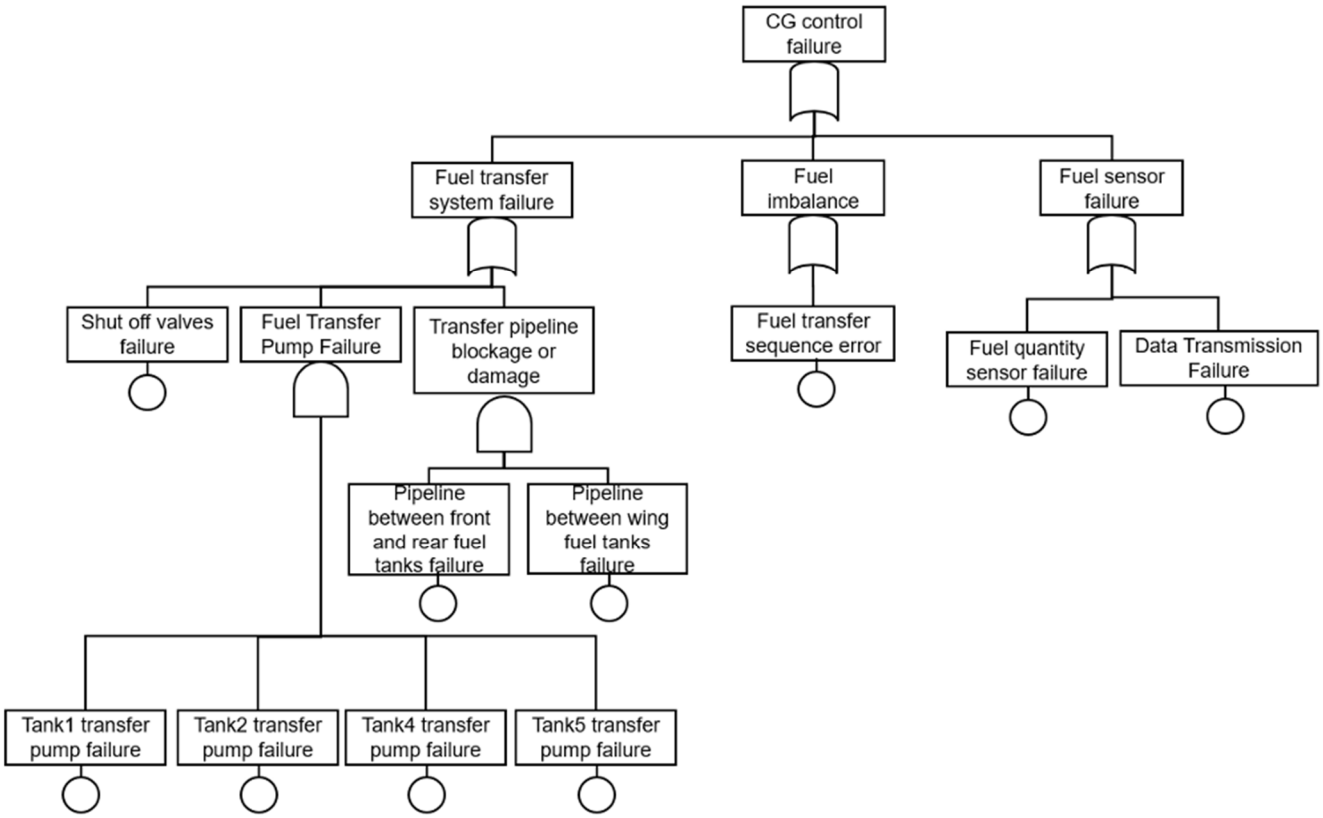


Figure A5. Fault tree diagram illustrating the causes leading to centre of gravity (CG) control failure in the aircraft fuel system. Rectangular blocks represent system and intermediate events, circular nodes denote basic failure events, AND gates indicate that all input events must occur simultaneously to trigger the output event, while OR gates indicate that any single input event can lead to the output condition.

Appendix F. FMEA

The FMEA table is a critical tool for systematically identifying and mitigating potential hazards in the SA-24 Phoenix fuel tank system, aligning directly with the integration of the CAD and MBSE for ZSA. It evaluates failure modes across key components, such as fuel pipelines, pumps, and sensors, detailing the causes, effects, and prioritized risks using the RPN. This prioritization ensures that critical issues, such as pipeline ruptures or pump failures, are addressed early in the design phase.

By integrating CAD and MBSE, the FMEA enables the precise modeling and simulation of hazards. For example, CAD tools refine pipeline designs to reduce blockages, whereas MBSE simulates dynamic scenarios, such as CG imbalances or pump failures, to validate redundancy strategies. These tools ensure iterative design improvements and early hazard detection, reduce expensive late-stage changes, and enhance system reliability.

The FMEA supports compliance with the EASA CS-25 standards by documenting hazards and their mitigation, ensuring that SA-24 meets airworthiness requirements. This structured approach improves design efficiency, reduces risks, and demonstrates the value of integrating advanced tools for aerospace safety engineering. The detailed failure modes, associated risks, and mitigation strategies related to center of gravity control failure are summarized in Table A5.

Table A5. Results of the failure modes and effects analysis (FMEA).

Component	Failure Mode	Failure Cause	Failure Effect	Severity (S)	Occurrence (O)	Detection (D)	Risk Priority Number (RPN)	Recommended Action
Fuel pipeline	Blockage (e.g., ice formation)	Low temperature at high altitude	Loss of fuel supply to engines	9	4	6	216	Add thermal insulation and anti-icing systems; optimize venting pathways using CAD.
	Rupture	Structural fatigue or improper joints	Fuel leakage, fire hazard	10	3	5	150	Use reinforced materials (e.g., titanium alloys); conduct fatigue testing via MBSE.
Fuel pumps	Mechanical failure (e.g., bearing wear)	Wear and tear, poor maintenance	Reduced or no fuel delivery to engines	8	5	4	160	Include redundant pump systems; schedule preventive maintenance using digital twins.
	Electrical failure	Power loss or motor malfunction	Complete pump failure	9	4	5	180	Integrate backup power supply; improve electrical circuit redundancy through simulations.
Fuel tanks	Over-pressurization	Faulty venting system	Tank deformation or rupture	10	2	6	120	Implement dual venting systems; install pressure sensors validated via CAD simulations.
	Vaporization	Aerodynamic heating	Pressure build-up and potential ignition	9	3	6	162	Apply heat shields and advanced insulation materials; validate via thermal analysis in CAD.
Fuel quantity indication system (FQIS)	Sensor failure	Calibration errors or component fault	Incorrect fuel level data, operational inefficiency	7	5	4	140	Enhance sensor design; validate placement and interactions with MBSE models.
Transfer valves	Failure to open/close	Actuator fault or debris	Inability to transfer fuel, CG imbalance	8	4	5	160	Regular valve testing; use debris-resistant designs and reliable actuators.
Fuel management system	Software error	Algorithm flaws or human input errors	Incorrect fuel distribution	7	3	5	105	Improve fuel management algorithms; validate through MBSE-based digital twins.
Data transmission system	Communication failure	Network issues or hardware failure	Delay in fuel system data updates	6	4	4	96	Introduce redundant communication networks; test system interactions in MBSE.

Appendix G. FHA

The FHA of the SA-24 Phoenix fuel tank system helped identify and mitigate potential functional failures critical to aircraft safety. Failures, such as inadequate fuel delivery, over-pressurization, and CG imbalances, are classified by severity, with catastrophic hazards, such as engine flameout or tank rupture, requiring immediate mitigation through redundancy, improved materials, and robust designs. CAD optimizes the spatial configuration of components, whereas MBSE simulates failure scenarios to validate system resilience.

For fuel delivery, failures, such as pump malfunctions or blocked pipelines, can disrupt operations. CAD ensures efficient pipeline routing, whereas MBSE tests redundant strategies, such as dual pumps. Pressure regulation failures, such as vent blockages, were mitigated through redundant systems and validated via simulations. CG imbalances from transfer pump failures or valve malfunctions were addressed using redundancy and design optimization. Monitoring issues, such as sensor inaccuracy and delayed alerts, were resolved through CAD-based placement validation and MBSE simulation of communication networks.

The FHA prioritizes risks based on severity and provides actionable insights into proactive hazard mitigation. By integrating the CAD and MBSE workflows, the IRP ensured early hazard detection, regulatory compliance, and enhanced reliability of the SA-24 Phoenix fuel system. This approach strengthens aircraft safety, while demonstrating the capabilities of advanced aerospace design methodologies. The final set of supporting results and extended analysis data are presented in Table A6.

Table A6. SA-24 aircraft FHA.

Function	Failure Mode	Hazard Description	Severity	Classification	Recommended Mitigation
Fuel delivery to engines	Inadequate fuel flow	Loss of engine power, leading to potential engine flameout	Catastrophic	Major (Class I)	Add redundant fuel pumps; optimize flow pathways using CAD
	Excessive fuel delivery	Over-pressurization of engines, potential fire risk	Hazardous	Major (Class II)	Install flow regulators and pressure sensors validated via MBSE
	Interrupted fuel supply	Engine surges or shutdown	Major	Major (Class II)	Integrate dual fuel delivery lines; conduct fault simulations
Pressure regulation	Vent blockage	Tank over-pressurization leading to structural rupture	Catastrophic	Major (Class I)	Implement redundant venting systems; validate designs through CAD
	Pressure sensor failure	Undetected pressure build-up	Hazardous	Major (Class II)	Use redundant sensors and validate placement through MBSE

Table A6. *Cont.*

Function	Failure Mode	Hazard Description	Severity	Classification	Recommended Mitigation
Fuel transfer system	Transfer pump failure	Imbalance in CG causing control issues	Hazardous	Major (Class II)	Introduce redundant pumps; simulate failure scenarios with MBSE
	Valve failure	Unregulated fuel transfer or blockage	Major	Major (Class II)	Optimize valve design and placement through CAD
Monitoring and sensors	Sensor inaccuracy	Incorrect fuel level readings, affecting CG management	Hazardous	Major (Class II)	Validate sensor placement using CAD; improve software algorithms
	Data transmission failure	Delayed hazard alerts	Minor	Minor (Class III)	Use redundant communication networks validated through MBSE

Appendix H. EASA CS-25 Fuel System Airworthiness Requirements

To ensure that the fuel system of the SA-24 Phoenix meets the stringent airworthiness standards required for supersonic operations, a detailed understanding of the EASA CS-25 Certification Specifications is crucial. These requirements govern the design, operation, maintenance, and safety across the lifecycle of the aircraft. Below is an expanded and detailed table of requirements tailored to this research focus. The comprehensive summary of the extended analysis and supporting data is presented in Table A7.

Table A7. EASA CS-25 fuel system airworthiness requirements.

CS-25 Reference	Requirement	Relevance to Supersonic Aircraft Design	Application to SA-24 Phoenix
CS 25.943	Fuel system lines and fittings	Ensure lines and fittings are designed to prevent leaks under all operating conditions.	Use of advanced seals and composite pipelines to handle high thermal stresses
CS 25.951	General requirements	The fuel system must supply sufficient fuel flow and pressure for all operating conditions.	Dual pump systems ensure consistent flow during rapid altitude changes
CS 25.952	Fuel system independence	Systems must operate independently, avoiding complete system failure.	Redundant pumps and valves mitigate single-point failures during supersonic cruise
CS 25.953	Fuel system failure protection	Prevent hazards resulting from failure modes, such as leaks or blockages.	Zonal Safety Analysis (ZSA) identifies failure points, enabling proactive design changes
CS 25.954	Fuel system lightning protection	Systems must resist ignition caused by lightning strikes.	Non-conductive coatings and flame arrestors applied to vent lines and pipelines
CS 25.959	Fuel tank venting	Aerodynamic heating during supersonic flight can cause fuel expansion and pressure increase inside the tanks.	Redundant vent paths and blockage monitoring ensure adequate venting capability and pressure control

Table A7. *Cont.*

CS-25 Reference	Requirement	Relevance to Supersonic Aircraft Design	Application to SA-24 Phoenix
CS 25.963	Fuel tank sealing	Thermal expansion and structural vibration at supersonic speeds increase sealing requirements.	Dual sealing interfaces and leak detection sensors minimize leakage and improve fault detection
CS 25.975	Fuel tank venting system requirements	Proper venting is critical in supersonic aircraft where fuel heating can cause vapor pressure buildup.	Redundant fuel tank venting systems prevent excessive pressure accumulation inside tanks
CS 25.979	Pressure testing	Fuel tanks must withstand maximum pressures without deformation or failure.	Tanks are pressure-tested to handle supersonic thermal and pressure differentials
CS 25.981	Fuel tank ignition prevention	Ensure no ignition sources exist within the fuel tank, including electrical faults.	Shielded wiring and isolated electrical components reduce ignition risk

Appendix I. Project Plan Dates

The project timeline and key milestone dates associated with the research and development process are presented in Table A8.

Table A8. Project plan dates.

Task	Start Date	End Date
Literature Review	10 October 2024	5 November 2024
System Definition and Data Collection	6 November 2024	20 November 2024
CAD Modelling of Fuel Tank System	21 November 2024	10 December 2024
MBSE Workflow Development	11 December 2024	30 December 2024
Integration of CAD and MBSE	2 January 2025	8 January 2025
Zonal Safety Analysis (ZSA)	9 January 2025	15 January 2025
Case Study	16 January 2025	20 January 2025
Technical Report Drafting	21 January 2025	23 January 2025
Final Review and Submission	23 January 2025	24 January 2025

Appendix J. Ethical Approval Certificate

18 December 2024

Dear Mr Kamboj ,

Reference: CURES/24072/2024
Project ID: 27382
Title: Integrating conceptual CAD and MBSE models for early zonal hazard analysis

We are pleased to inform you that you have successfully declared that your research project is a **Literature Review – based solely on openly available literature which is in the public domain, and you are undertaking desk-based research not involving any other form of data or information.**

You have also confirmed that your project **does not meet** any of the literature review specified exceptions, listed both within the relevant section of the CURES form and below:

1) Your supervisor has requested that you apply for approval through CURES because:

- The journals or data are in a sensitive area (please discuss this with your supervisor)
- The project will be embargoed **i.e. will not be publicly available via the Cranfield library immediately or longer term**

2) Approval is/will be specifically required by another external body e.g. journal publishers

Therefore, **you do not require ethical approval** and your CURES application will be automatically closed.

Please keep a copy of this letter safe, if this exception is in relation to your thesis project, you will need to include a copy with your final thesis submission.

If you have any queries, please contact CURES Support.

We wish you every success with your project.

Regards,

CURES Team

Figure A6. Ethical approval exemption certificate issued by Cranfield University (CURES), confirming that the study did not require formal ethical approval as it is based exclusively on publicly available data and literature sources.

References

1. Polmar, N.; Kennedy, J. *Pioneering Supersonic Transport: Concorde and Tu-144*; Zenith Press: St. Paul, MN, USA, 2005.
2. NASA. *X-59 QueSST Project Overview*; NASA Reports; NASA: Washington, DC, USA, 2023.
3. Raymer, D. *Aircraft Design: A Conceptual Approach*; AIAA: Reston, VA, USA, 2018.
4. Dassault Systèmes. *3DEXPERIENCE Platform Documentation*; Dassault Systèmes: Vélizy-Villacoublay, France, 2023.
5. *ARP4761*; Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. SAE International: Warrendale, PA, USA, 1996.
6. *ARP4761A*; Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. SAE International: Warrendale, PA, USA, 2016.

7. Wang, Y.; Zhang, A.; Li, D.; Li, H. Research on Civil Aircraft Design Based on MBSE. In *The Proceedings of the 2018 Asia-Pacific International Symposium on Aerospace Technology (APISAT 2018)*; Zhang, X., Ed.; Lecture Notes in Electrical Engineering; Springer: Singapore, 2019; Volume 459. [CrossRef]
8. Madni, A.M.; Sievers, M. Model-based systems engineering: Motivation, current status, and research opportunities. *Syst. Eng.* **2018**, *21*, 172–190. [CrossRef]
9. Friedenthal, S.; Moore, A.; Steiner, R. *A Practical Guide to SysML: The Systems Modeling Language*; Morgan Kaufmann: Burlington, MA, USA, 2015.
10. INCOSE. *Systems Engineering Vision 2035*; International Council on Systems Engineering: San Diego, CA, USA, 2021.
11. Boom Supersonic. Overture Aircraft: Merging Speed and Sustainability. 2022. Available online: https://www.boomsupersonic.com (accessed on 22 March 2026).
12. Sun, Y.; Smith, H.; Chen, H. Conceptual Design of Low-Boom Low-Drag Supersonic Transports. In *Proceedings of the AIAA Aviation 2020 Forum, Virtual Event, 15–19 June 2020*; American Institute of Aeronautics and Astronautics: Reston, VA, USA, 2020.
13. Pessa, C.; Cifaldi, M.; Brusa, E.; Ferretto, D.; Malgieri, K.M.N.; Viola, N. Integration of Different MBSE Approaches within the Design of a Control Maintenance System Applied to the Aircraft Fuel System. In Proceedings of the IEEE International Symposium on Systems Engineering (ISSE), Edinburgh, UK, 3–5 October 2016; pp. 1–8. [CrossRef]
14. EASA. *Certification Specifications for Large Aeroplanes CS-25*; European Union Aviation Safety Agency: Cologne, Germany, 2022.
15. Airbus. *Advanced Material Applications in Aerospace*; Airbus Technical Publications: Toulouse, France, 2022.
16. Boeing. *Model-Based Systems Engineering in Aerospace*; Boeing Technical White Paper; Boeing: Arlington County, VA, USA, 2021.
17. Bruggeman, A.-L.M.R.M.; La Rocca, G. From Requirements to Product: An MBSE Approach for the Digitalization of the Aircraft Design Process. *INCOSE Int. Symp.* **2023**, *33*, 1688–1706. [CrossRef]
18. Cui, Z.; Luo, M.; Zhang, C.; Hua, Y.; Xie, R.; Yu, R.; Huang, C. MBSE for Civil Aircraft Scaled Demonstrator Requirement Analysis and Architecting. *IEEE Access* **2022**, *10*, 43112–43128. [CrossRef]
19. Krupa, G.P. Application of Agile Model-Based Systems Engineering in Aircraft Conceptual Design. *Aeronaut. J.* **2019**, *123*, 1561–1601. [CrossRef]
20. Insaurralde, C.C.; Seminario, M.A.; Jiménez, J.F.; Giron-Sierra, J.M. Model-Based Development Framework for Distributed Embedded Control of Aircraft Fuel Systems. In Proceedings of the 29th Digital Avionics Systems Conference (DASC), Salt Lake City, UT, USA, 3–7 October 2010; pp. 6.E.2-1–6.E.2-14. [CrossRef]
21. Thompson, N.; Blond, K.; Berguin, S.; Clark, A. MBSE-Driven Implementation to Optimize Aircraft Maintenance Planning. In Proceedings of the IEEE Aerospace Conference, Big Sky, MT, USA, 2–9 March 2024; pp. 1–8. [CrossRef]
22. Stevens, G. *The Concorde Story: Lessons for Future Supersonic Aircraft*; Osprey Publishing: Oxford, UK, 2019.
23. Fei, X.; Bin, C.; Rui, L.; Shunhua, H. A Model-Based System Engineering Approach for Aviation System Design by Applying SysML Modeling. In Proceedings of the Chinese Control and Decision Conference (CCDC), Hefei, China, 22–24 August 2020; pp. 1361–1366. [CrossRef]
24. NASA. *Application of Model-Driven Engineering in Hybrid Wing-Body Aircraft Design*; NASA Technical Reports; NASA: Washington, DC, USA, 2023.
25. Chen, H.; Liu, Z.; Alippi, C.; Huang, B.; Liu, D. Explainable intelligent fault diagnosis for nonlinear dynamic systems: From unsupervised to supervised learning. *IEEE Trans. Neural Netw. Learn. Syst.* **2024**, *35*, 6166–6179. [CrossRef] [PubMed]
26. Chen, H.; Jiang, B.; Ding, S.X.; Huang, B. Data-driven fault diagnosis for traction systems in high-speed trains: A survey, challenges, and perspectives. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 1700–1716. [CrossRef]
27. Jang, K.; Pilario, K.E.S.; Lee, N.; Moon, I.; Na, J. Explainable artificial intelligence for fault diagnosis of industrial processes. *IEEE Trans. Ind. Inform.* **2025**, *21*, 4–11. [CrossRef]
28. Cranfield University. *Low-Boom Low-Drag Optimisation in a Multidisciplinary Design Framework (GENUS Aircraft Design Environment)*; Cranfield University: Bedford, UK, 2019.
29. *EASA CS-25*; Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes. European Union Aviation Safety Agency: Cologne, Germany, 2023.
30. *ISO 10303*; Industrial Automation Systems and Integration—Product Data Representation and Exchange. International Organization for Standardization: Geneva, Switzerland, 2021.
31. OMG SysML. *Systems Modeling Language Specification*; Object Management Group: Needham, MA, USA, 2017.
32. Cranfield University. *SA-24 Phoenix Supersonic Aircraft—Technical Demonstration*; Cranfield University: Bedford, UK, 2024.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.