Results in Engineering 25 (2025) 104249

Contents lists available at ScienceDirect

Results in Engineering

journal homepage: www.sciencedirect.com/journal/results-in-engineering

Research paper

Integration of a model-based systems engineering framework with safety assessment for early design phases: A case study for hydrogen-based aircraft fuel system architecting

Nils Kuelper [a,*], Andrew K. Jeyaraj [b], Susan Liscouët-Hanke [b], Frank Thielecke [a]

[a] Institute of Aircraft Systems Engineering, Hamburg University of Technology, Nesspriel 5, Hamburg, 21129, Germany
[b] Department of Mechanical, Industrial, and Aerospace Engineering, Concordia University, 1455 Boul. de Maisonneuve Ouest, Montreal, H3G 1M8, QC, Canada

ARTICLE INFO

Keywords:
Aircraft
Complex system
MBSE
MBSA
Safety
Conceptual design
Hydrogen architecture

ABSTRACT

Novel hydrogen-based aircraft concepts pose significant challenges for the system development process. This paper proposes a generic, adaptable, and multidisciplinary framework for integrated model-based systems engineering (MBSE) and model-based safety assessment (MBSA) for the conceptual design of complex systems. The framework employs a multi-granularity, model-centric approach, whereby the architectural specification is utilized for design as well as query purposes as part of a qualitative and quantitative, graph-based preliminary safety assessment. For the qualitative assessment, design and safety rules based on existing standards and best practices are formalized in the model and applied to a graph-based architecture representation. Consequently, the remaining architectures are quantitatively assessed using automated fault trees. This safety-integrated approach is applied to the conceptual design of a liquid hydrogen fuel system architecture as a novel, uncertain, and complex system with many unknown system interrelations. This paper illustrates the potential of a combined MBSE-MBSA framework to streamline complex, early-stage system design and demonstrates that all qualitatively down-selected hydrogen system architecture variants also satisfy quantitative assessment. Furthermore, it is shown that the design space of novel systems is also constrained by safety and certification requirements, significantly reducing the number of actual feasible solutions.

1. Introduction

Aviation contributes about 5 % of worldwide emissions [1] driving emission reduction targets [2–4]. Expected fuel efficiency improvements until 2050 are insufficient [2,4]. Thus, the research community investigates innovative concepts, e.g., hydrogen-powered fuel cells (FCs) coupled with an electric power train (EPT), based on the assumption of clean hydrogen production [5].

To effectively use hydrogen (H2) in aircraft, research focuses on liquid hydrogen (LH2) [6]. However, no commercial aircraft currently operates on LH2, resulting in a lack of knowledge combined with high uncertainties in designing the LH2 system compliant with safety and certification regulations [7]. Furthermore, integrating novel technologies into an aircraft impacts other systems due to present interrelations and can significantly change systems architectures [8,9]. For example, thermal management and fire protection of the LH2 system will have a significant impact on the environmental control system (ECS).

Novel technologies and architectures are typically investigated during the aircraft conceptual design phase [10]. Engineers face a vast and complex design space with numerous possible solutions [11]. To manage uncertainty and navigate complexity, multiple technology trade studies are conducted in this phase. In addition, safety and redundancy are significant drivers of architectures at the qualitative and quantitative levels; therefore, they need to be included in early trade studies. This ensures that only feasible, i.e., safety- and certification-compliant, architectures are further investigated, preventing late and costly design changes [12]. Hence, viable LH2 architectures are currently unknown, resulting in the first research objective of this work:

Analyze the design space of LH2 fuel system architecture variants and identify variants compliant with design, safety, and certification regulations.

Systems engineering approaches, particularly model-based systems engineering (MBSE[1]) methods, show the potential to handle the complexity of developing novel systems [14]. MBSE offers a structured and

* Corresponding author.
E-mail address: nils.kuelper@tuhh.de (N. Kuelper).

[1] *MBSE* is defined as the use of models to support requirements, design, assessment, evaluation, verification, and validation steps spanning over the entire life cycle [13].

https://doi.org/10.1016/j.rineng.2025.104249
Received 7 October 2024; Received in revised form 22 January 2025; Accepted 2 February 2025

Available online 5 February 2025

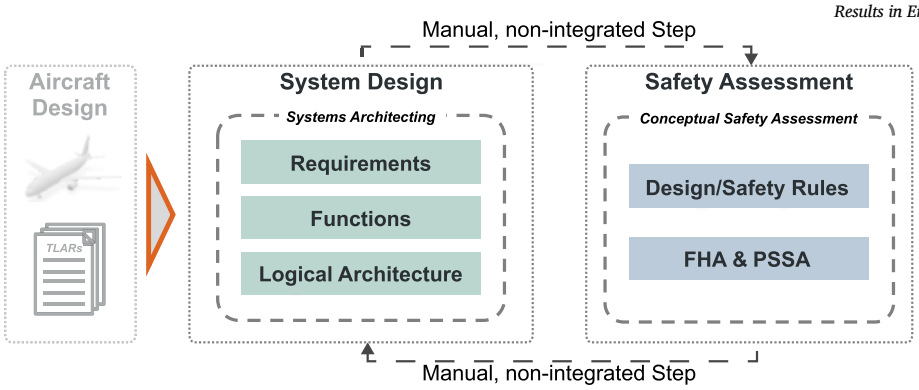

Fig. 1. Schematic representation of a conventional, separated, and non-integrated system development process for conceptual design.

interdisciplinary approach for developing complex systems [13]; this concept has gained attraction recently, e.g., in [9,15,16]. The advantage of MBSE is its model-centric approach, also referred to as a "single source of truth" (SSoT[2]). However, MBSE can also introduce a new level of complexity due to the models' size, which can prove challenging to manage and comprehend.

One such MBSE-driven approach for early systems architecting is the *Systems Architecting Assistant* (*SArA*) methodology proposed by the Hamburg University of Technology [18–20]. *SArA* supports engineers with requirements definition, functional and logical architecture design space exploration, model-based specifications, and early evaluation, including initial down-selections. However, *SArA* is currently a separate silo for systems architecting, as exemplarily shown in Fig. 1 for a conventional, non-integrated systems development process. *SArA* lacks the ability for early, rapid, and flexible safety assessments. Consequently, an integrated model-based safety analysis (MBSA[3]) approach is necessary.

MBSA uses architecture models to conduct safety assessments [22,23], such as modeling nominal and faulty system behavior. The *Aircraft Systems Safety Assessment* (*ASSESS*) framework follows such a safety assessment approach [24], developed by Concordia University. As shown exemplarily in Fig. 1 for a conventional, non-integrated systems development process, *ASSESS* incorporates several modules for a safety-based assessment, including rule-based filtering of design spaces and early architecture safety assessment. However, currently, no MBSE model is used as SSoT to ensure an integrated system design and safety assessment.

Against these challenges, the second research objective is derived: *Develop a generic, adaptable, and semi-automated framework that links and integrates systems architecting and safety assessment based on an underlying SSoT model to assist the engineer during conceptual system development.*

To achieve these objectives, section 2 presents existing MBSE-MBSA approaches, safety standards, rules, and regulations for kerosene and hydrogen, highlights existing gaps in the literature, and defines the research questions. The improvements to *SArA* and *ASSESS* are presented in section 3, including the extension of the graph-based representation, using the architecture model for automated safety assessment, and the formalization of the rules for hydrogen-based fuel systems architecture. The approach is then applied in section 4 on a two-engine mid-size business jet concept to evaluate a design space of system architecture variants. Limitations of the results and the framework are discussed. Finally, section 5 summarizes the work and presents avenues for future research.

[2] *Single source of truth* is defined as a method to ensure that all relevant information for systems architectures is collected, stored, and formalized within one or several interconnected, machine-readable models so that all evaluations and assessment steps use the same data [13,17].

[3] *MBSA* is defined as a collection of methods based on failure propagation models replacing conventional safety assessment methods [21].

2. State of the art

To underline the necessity behind the objective of developing the MBSE-MBSA framework, an overview of existing approaches and studies with their distinct characteristics is presented. In addition, current regulatory texts and engineering standards are provided. The resulting research questions based on the identified gaps are clearly defined.

2.1. Review of existing integrated MBSE-MBSA approaches

In general, SAE ARP4754B [22] describes in combination with SAE ARP4761A [21] guidelines for designing and developing an aircraft and its systems considering safety. In addition, authors present system design approaches that integrate safety (cf. Table 1).

2.1.1. Published approaches by the authors

In addition to the aforementioned literature, the authors already developed approaches. Kuelper et al. [18] present *SArA* as an MBSE-driven approach for functional-logical systems architecting capable of handling uncertainty, complexity, and traceability. *SArA* assists the engineer during design space exploration, systems architecture variants modeling, variants evaluation, and down-selection. Logical architectures are traced back to functions and requirements similar to an RFLP approach [39,40]. Furthermore, *SArA* integrates knowledge to streamline the architecting process and to prevent the investigation of numerous non-beneficial and infeasible solutions [60]. The compliance with design and safety constraints is currently manually assessed with RBDs. However, to fully use the model-centric approach, it is necessary to extend *SArA* to an automated MBSA approach.

Jeyaraj et al. [24,54] present *ASSESS* as safety-focused systems architecting framework for conceptual design, adapting the formal safety assessment process to the conceptual level. The framework introduces rule-based design space filtering followed by representing selected architectures in an MBSE environment. The rule identification and definition process is a multi-step process considering regulatory texts, best practices, existing system architecture specifications, and iterations with experts [24]. The rules are applied to a graph-based architecture description using a set of generic elements while focusing on redundancies and the flow of power and control (*ASSESS* L0) [54]. *ASSESS* also supports the early development of fault trees. ASSESS-L1-M1 [61] focuses on further refining one selected architecture, including a model-driven FHA process. ASSESS L1-M2 [62] focuses on CCA, such as Zonal Safety Assessment (ZSA) and Particular Risk Assessment (PRA) (*ASSESS* L1).

2.2. Review of existing best-practices, standards, and certification texts for hydrogen and aircraft fuel systems

To define design and safety rules, knowledge, best practices, standards, and regulatory texts existing in the literature need to be investigated. According to *ASSESS*, initially, regulatory texts are analyzed for

Table 1
Chronological overview of relevant MBSE-MBSA approaches in the literature.

Reference	Research Focus	MBSE	MBSA	Use Case
Armstrong [25]	- Function-based systems architecting - Off-nominal behavior - Continuous FHA	No	Analog PSSA	MEA[a] systems
Liscouët-Hanke et al. [26,27]	- Simulation-based framework - Physics-based sizing - Failure scenarios	No	Qualitative	MEA systems architectures
Raksch et al. [28,29]	- Multi-criteria optimization of fault-tolerant systems - Redundancy allocation	No	Redundancy	Electrical system of MEA
Chakraborty et al. [30,31]	- Modular aircraft and systems sizing method - Safety heuristics	No	Qualitative	MEA and all-electric systems
Johansson et al. [32,33]	- Architecture optimization based on safety, reliability, costs, mass	No	FTA,[b] RBD[c]	Kerosene fuel system
Bornholdt et al. [34,35]	- Function-based systems architecting - Automated quantitative safety assessment	No	RBD	Multiple aircraft systems
Fusaro et al. [36]	- Approach for safety and reliability assessment - statistical failure rates	SE	FTA	Hypersonic aircraft
Jimeno et al. [37,38]	- RFLP[d] with integrated safety assessment - Semi-automated FHA[e]	Yes	FHA, FTA	Conv. and electrified ECS
Bleu-Laine et al. [41] & Harrison et al. [42]	- MBSE for regulatory rules and compliance facilitation	Yes	No	Novel, disruptive aircraft concepts
Rehfeldt et al. [43]	- Integrated architecting and safety toolchain	Model-based	RBD	Avionic networks
Biggs et al. [44,45]	- Integration of safety and reliability in UML[f]	Yes	FMEA,[g] FTA	Automotive (abstract)
Krishnan et al. [46,47]	- Integrated design and safety framework - Automatically generated FTA	Yes	FMEA, FTA	Car collision warning systems
Ahlbrecht et al. [48,49]	- Safety trade-offs in early development	Yes	Qualitative	Automotive systems
Quamara et al. [50]	- Multi-layered design approach for safety and security of cyber-physical systems	Yes	Qualitative	Connected driving vehicles
Cabaleiro et al. [51]	- Analyzation of certification regulations - Automated RBD	No	RBD	Flight control spoiler
Schaefer et al. [52] & Luebbe et al. [53]	- Integrated MBSE and MBSA approach - Focus on aircraft safety assessment	Yes	FHA, FTA	Flight control system
Jeyaraj et al. [24,54]	- safety-focused systems architecting framework (*ASSESS*)	Yes	FHA, CCA[h]	Multiple aircraft systems
Kuelper et al. [18–20]	- *SArA* for knowledge integrated functional-logical systems architecting	Yes	Manual task	Multiple aircraft systems
Voth et al. [9]	- Function-driven systems architecting	Yes	No	FC cooling
Lai et al. [55]	- Model-based FHA framework with customized profiles and workflows	Yes	FHA	Landing gear system
Schorr et al. [56]	- Redundancy allocation - Architecture evaluation	No	Redundancy	FC system
Piatek et al. [57]	- Pattern-based security and functional safety	Yes	Qualitative	Car braking system
Kang et al. [58]	- Data-driven, scenario-based safety assessment	No	Qualitative	Autonom. vehicles
Kolip [59]	- Integrated MBSE-MBSA - Manual FTA generation	Yes	FTA	Flap system

[a] More-Electric-Aircraft.
[b] An *FTA* (Fault Tree Analysis) is a failure analysis method to identify and assess undesired system events and failures as well as the underlying causes [21].
[c] An *RBD* (Reliability Block Diagram), also called *Dependence Diagram*, is a method to analyze the effect of component failure rates on a system [21].
[d] *RFLP* is a structured design approach considering requirements, functional, logical, and physical product definition during design [39,40].
[e] An *FHA* (Functional Hazard Assessment) identifies and categorizes failure conditions per function. It is performed at aircraft and at system level [21].
[f] Unified Modeling Language.
[g] Failure Mode and Effects Analysis.
[h] Common Cause Analysis.

Table 2
Relevant standards for H2 storage, distribution, refueling, and usage.

Year	Standard	Description	Ref.
ANSI Standards			
2017	ANSI/AIAA G-095A-2017	Guidelines on designing, handling, controlling, transporting, and using hydrogen systems safely.	[63]
2023	CSA/ANSI HGV 2	Requirements for the material, design, manufacture, and testing of refillable containers intended for the storage of compressed hydrogen of road vehicles.	[64]
EN Standards			
2010	EN 406/2010	Requirements for an hydrogen-powered ground vehicle.	[65]
2019	EN 2019/2144	Requirements for a type-approval for vehicles and their systems, including hydrogen-powered vehicles (replaces EN 406/2010).	[66]
FAA Standards			
2017	DOT/FAA /TC-19/16	Recommendations of the rulemaking committee for airworthiness standards for energy supply devices to be installed on airplanes, focussing on hydrogen-powered fuel cells.	[67]
ISO Standards			
2006	ISO 13985	Requirements and testing methods for a refillable LH2 tank for land vehicles.	[68]
2015	ISO/TR 15916	Rules for the safe use of GH2 and LH2 based on known safety aspects, hazards, and risks.	[69]
2018	ISO 19881	Requirements for the material, design, manufacture, and testing of refillable containers for compressed hydrogen gas for land vehicles.	[70]
2020	ISO 17268	Overview of design, safety, and operational aspects for GH2 refueling and refueling devices.	[71]
NASA Standards			
1996	NSS 1740.16	Guidelines for hydrogen system design, materials, transportation, storage, and usage.	[72]
NFPA Standards			
2015	NFPA 2	Guidelines for the safe generation, installation, storage, distribution, and use of GH2 and LH2 in buildings and structures.	[73]
SAE Standards			
2019	SAE AIR7765	Experiences gained from existing applications from using FCs in other industries sectors, such as terrestrial applications, to be applied in aviation.	[74]
2020	SAE AIR6464	Provides guidelines for Proton Exchange Membrane Fuel Cells (PEMFCs), hydrogen fuel (liquid or compressed gaseous), tanks, distribution, and an appropriate electrical system.	[75]
2023	SAE AS6858	Guidelines for safely integrating gaseous PEMFCs in aircraft.	[76]
2023	SAE J2578	Requirements for integrating FCs, H2 storage, and high voltage electrical systems into vehicles, covering design aspects.	[77]
2023	SAE J2579	Requirements for designing, operating, and maintaining a hydrogen system in road vehicles, including verification requirements and test protocols.	[78]
Under development	SAE AS6679	Guidelines for the safe integration, operation, maintenance, refueling, and certification of liquid hydrogen in commercial aviation.	[79]
Under development	SAE AS7373	Guidelines for the safe integration, operation, maintenance, refueling, and certification of gaseous hydrogen in general aviation.	[80]
UN Standards			
2023	UN GTR 13	General technical regulations for H2 vehicles so they are at least as safe as conventional vehicles.	[81]

definitions of redundancy and power allocation requirements for an LH2 fuel system onboard an aircraft; however, as of today, no such texts are available.

Dedicated standards for designing the LH2 fuel system are still being developed. Relevant standards about H2 storage, distribution, and usage, mainly from a non-aerospace context, are listed in Table 2.

Additionally, the literature includes initial design guidelines and experiences for H2. Brewer [82] summarizes past research and design studies. His book covers both low-fidelity hydrogen system architectures and high-fidelity component designs. Klein et al. [83] describe potential applications in aircraft and vehicles. They review fundamental safety strategies, such as aiming for novel systems that are at least as safe as current ones. Verstraete [84] explores LH2 for long-range aircraft based on aircraft design, engine performance, and a detailed tank design. Saffers et al. [85] introduce an H2 safety engineering approach that addresses H2-specific phenomena through a qualitative design review, quantitative safety analysis, and evaluation of designs against acceptance criteria. Dincer et al. [86] present extensive information on clean energy topics in general, e.g., batteries and hydrogen. They also briefly mention H2 components, their usage, and safety rules and tests. San Marchi et al. [87] provide a review of advances toward hydrogen regulations and standards focusing on hydrogen release, risk assessment, materials, and fuel quality. Adler et al. [88] present an overview of hydrogen-powered aircraft, including the physical basics and current technological advancements. Genovese et al. [89] give an overview of hydrogen fueling station regulations and safety standards.

Table 3
Relevant fuel system standards derived from kerosene systems.

Year	Standard	Description	Ref.
Certification Specifications			
2023	CS-25 Amendment 28	Large aeroplanes certification specification including fuel system requirements.	[90]
2025	14 CFR Part 25	Airworthiness standards for transport category airplanes.	[91]
SAE Fuel System Standard			
2019	SAE AIR7975	Guidelines, design drivers, and safety aspects that must be considered in a conventional kerosene-based fuel system design.	[92]

International (ISO, IEC, SAE), European (CEN/CENELEC), and Italian standards are evaluated to identify insights for technology development.

Given the lack of standards for the LH2 fuel system and the assumption that novel safety-critical systems will face at least the same, if not stricter, safety requirements as conventional ones, design and safety rules are also derived from existing aircraft fuel system standards and regulations as listed in Table 3.

Additional fuel system characteristics, design principles, components, and initial rules are presented by Moir et al. [93], Langton et al. [94], and Rodriguez [95,96].

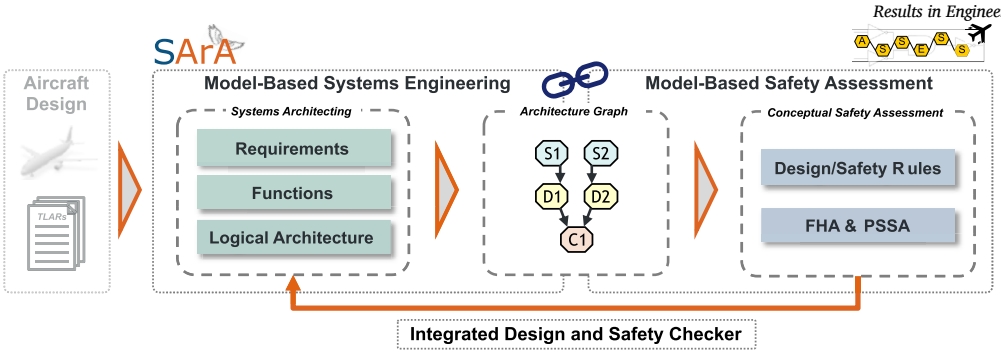

Fig. 2. Integrated, multi-environment MBSE-MBSA framework for conceptual systems architecting.

2.3. Observations and defined research questions

Based on the review, it can be observed that conceptual design is moving towards a model-centric design process. Key observations from the literature are:

- Only a few literature sources, e.g., [24,37,38,52,53], consider systems design with MBSE and safety assessment with MBSA as an integrated approach during conceptual design.
- Using a holistic approach with a standardized architecture model as SSoT for both qualitative and quantitative safety assessment is scarce.
- The reviewed approaches predominantly emphasize individual, self-contained frameworks. However, in practice, diverse methodologies and tools are employed across different departments and organizations requiring multi-environment frameworks.
- Some approaches are demonstrated on aerospace systems, others on automotive. The aerospace-based approaches are typically demonstrated on conventional, well-known systems, such as the flight control system or ECS (cf. [37,38,59]). In a few cases, the approaches are demonstrated on disruptive aviation technologies, such as fuel cells (cf. [9,56]). However, it has not yet been demonstrated for an LH2 fuel system architecture with high uncertainties.
- Standards and guidelines for hydrogen are available but primarily not for aerospace. Moreover, no specific regulations have yet been established for LH2 fuel system design in aircraft.
- A gap exists with respect to standardized, model-based methods for formalizing design and safety rules during conceptual design. Such a method is needed to enable the systematic collection, organization, and preservation of these rules in a machine-readable and updatable format.

Based on these observations and in alignment with the research objective, the core research question of this work is defined as:
How can a generic, adaptable, and semi-automated framework be developed that seamlessly links and integrates conceptual systems architecting and conceptual safety assessment while ensuring applicability for novel technologies, such as the LH2 fuel system?

For this research question, certain derived ones are identified:

1. *How can the existing MBSE-driven SArA methodology be combined with the MBSA-driven ASSESS framework to ensure a generic, adaptable, and multi-environment MBSE-MBSA framework for conceptual systems architecting as sketched in Fig. 2? What are the necessary adaptations to ensure interoperability?*
2. *How can an architecture model serve as an SSoT also for qualitative and quantitative safety assessments during the conceptual design phase? What is the required data and information that needs to be stored and exchanged?*
3. *How can hydrogen-related design and safety rules be formalized within an MBSE-driven architecture model? What rules are relevant for an LH2 fuel system architecture during conceptual design?*

These research questions guide the engineer in solving the present LH2 system development question, which motivates this work:
How is a minimal viable LH2 fuel system architecture characterized which meets both qualitative and quantitative safety requirements as well as boundary conditions while considering high uncertainties inherent in the LH2 design as well as the lack of detailed certification specifications?

3. Integrated MBSE-MBSA framework - methodology improvements

To address the defined research questions, this paper proposes the holistic and integrated MBSE-MBSA framework for conceptual systems architecting to assist the engineer in architecting novel, uncertain systems. The framework enhances the state of the art by providing the following novelties:

1. Enhance the standardized modeling approach of *SArA* to function as SSoT for both the specification and safety assessment by storing safety information already in the architecture model. This ensures consistency, traceability, and a seamless link between MBSE and MBSA. It also enables the automated generation and provision of safety artifacts.
2. Enhance the graph-based architecture descriptor of *ASSESS* to allow for LH2 as a fuel type.
3. Identify a list of openly accessible LH2-related design and safety rules for aerospace.
4. Develop a method to formalize the identified rules in the model to ensure a machine-readable and modifiable knowledge repository, reusable also for future studies and developments.
5. Enhance quantitative conceptual safety assessment robustness of uncertain technologies by including component failure rate scenarios.
6. Identify minimal viable and safety-compliant LH2 fuel system architectures.

The core elements of the framework, as shown in Fig. 2, are MBSE, MBSA, the adapted graph, and the selected toolchain. These elements are described in the following subsections.

3.1. MBSE-driven systems architecting

Systems architecting of this framework is performed using *SArA* with inputs from the separate aircraft design process. These inputs include top-level aircraft requirements and geometrical aircraft information.

The MBSE-driven *SArA* methodology includes an RFLP-like approach for defining traceable architecture variants with a design rationale, as shown in Fig. 3. This work follows an ORFL (operations, requirements,

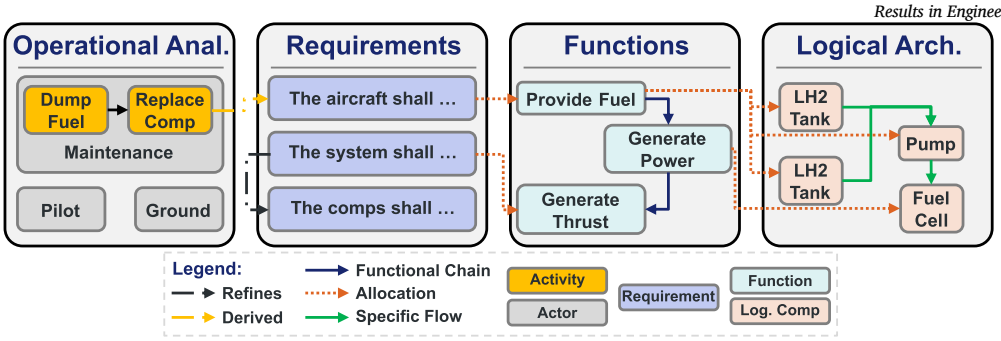

Fig. 3. Schematic representation of the MBSE-driven ORFL systems architecting process with *SArA* to ensure traceability.

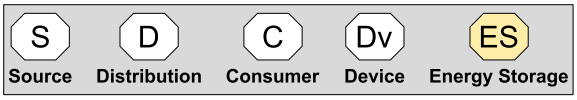

Fig. 4. Extended version of generic elements used to represent system architectures from [24].

functions, logic) approach since an operational analysis is included and the physical architecture step is neglected during very early conceptual design.

3.1.1. Operational analysis

An operational analysis captures stakeholder objectives and needs [97,98]. Based on this analysis, stakeholder-induced requirements can be derived. To include this analysis in *SArA*, the modeling method is extended by the new, color-coded stereotypes *actor*, *activity*, and *interrelation* connection to highlight and clearly model them (cf. Fig. 3).

3.1.2. Requirements collection

Derived operational requirements, as well as known aircraft and systems requirements, are collected in a formalized and standardized manner with *SArA* in the MathWorks Requirements Editor. This initial requirements set is categorized into the aircraft systems and is continuously updated and extended. It includes the description of the requirement, a rationale, the modification date, and potentially a link to other requirements or models to demonstrate relationships and dependencies.

3.1.3. Functional architecture

For novel systems, a functional analysis to identify and formalize functional needs is performed. Functions can be assigned to stakeholders, and linked to requirements. The functions and their interrelations are modeled as a functional architecture. The *SArA* methodology is extended with a new connections stereotype to highlight functional chains[4] so that they are machine-readable and can be investigated.

3.1.4. Logical architecture

Logical architecture variants, fulfilling the defined functional architecture, are developed, starting at a low level of detail, i.e., at the overall systems level. The level of detail is iteratively increased. Functions are mapped to logical components for traceability (cf. Fig. 3). This information is stored in a traceability matrix, describing a 1-n relation, since multiple logical elements can be required to fulfill a certain function. Together, this forms the functional-logical systems architectures.

To store and provide additional information, the model is extended by stereotypes, such as “compSpec,” “parentUID,” and “wingSide,” as already described in [18]. However, to accommodate safety assessment in MBSE, the generic elements of *ASSESS*, as presented in Fig. 4, and component failure rates are added as new stereotypes, as shown in Table 4. The generic elements are implemented as an enumeration so that the engineer can only select one of them. Failure rates are an empty double value and must be filled by the engineer per technology. Further stereotypes and attributes, such as safety zones, can be flexibly added. However, these are not necessary for the present work. They support future MBSA activities focusing on ZSA and PRA.

Table 4
Exemplary stereotype information in architecture model for an LH2 pump.

Stereotype	Attribute
compSpec	lh2_pump
parentUID	fuselage
wingSide	center
...	
element_powerView	Consumer
element_fuelView	Source
failureRate	1×10^{-4} 1/fh

These new stereotypes are key attributes for using the architecture model at the core of the integrated MBSE-MBSA framework. The element attribute can be left empty so that only components relevant for conceptual safety assessment are used to create the architecture graph. Typically, components, such as sensors, are neglected on a logical level and are only considered at a more detailed level.

3.2. Adaptation of graph-based architecture descriptor

The generic element descriptor of *ASSESS* was developed to capture the interface between aircraft secondary power systems and power-consuming systems. It represents power flows through generic elements, abstracting components and subsystems in aircraft secondary power systems. The elements are shown in Fig. 4.

For aircraft fuel system architecture, to assess the minimum number of fuel pumps per tank during safety assessment or the linking of tanks together, a new representation in *ASSESS* focusing on the fuel flow is developed. It includes a new generic element, “Energy Storage” (ES), representing chemical energy stores like fuel or batteries to improve the flexibility of use for fuel system architectures. The ES element can be both an origin and terminal component to capture fuel flow from a tank through a distribution system to the engine while also representing fuel transfer from one tank to another.

Fig. 5 a) shows a section of the “power flow view” using the generic elements. Here, the connections between the source and distribution elements represent electrical power from the engines distributed through the electric power supply system (EPSS). In contrast, the consumers represent the pumps in the fuel system. These fuel pumps are further associated with a fuel tank.

Fig. 5 b) shows the “mass flow view” where the source elements are fed by a fuel tank represented by the new ES element. Here the source

[4] A *functional chain* is defined as a collection and interaction of safety functions that ensure the successful operation of a system should an event arise [99]. It provides the engineer with the information on which functions are affected if a loss of a certain function occurs and therefore eases safety assessment [100].

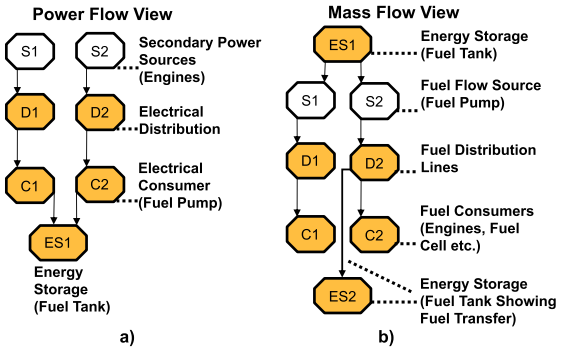

Fig. 5. Power flow and mass flow captured using the generic element descriptor.

elements are defined as sources of fuel flow and further supply fuel distribution lines represented by the distribution elements. The distribution elements supply the fuel-consuming elements, for example, engines or fuel tanks. In addition, the transfer of fuel from one tank to another can also be shown by linking the distribution element to an ES. The adapted views can now be used to assess the fuel system architecture variants.

The graph-based architecture representation enables the dependencies between components to be identified and used for safety analysis. The graph nodes and edges are used to store information such as the type of component, the type of power that a component requires, or the type of power that is exchanged between different components. These properties can either be specified by the system architect or can be inferred based on the type of component being used.

Therefore, the state of a component represented by the graph nodes will depend on whether it receives the required type of power, which can be identified by inspecting the properties of incoming edges. Thus, to enable the development of a fault tree, a safety model is automatically created by parsing through the graph-based descriptor. The resulting model contains the properties of all constituent elements, including descriptions of inputs and outputs that enable the component to be in an operational state.

3.3. MBSA for conceptual systems architecting

To ensure the development of only feasible system architecture variants, compliance with design and safety requirements needs to be assessed. Non-compliant variants are either adapted or eliminated from further investigations. This paper includes a two-phase MBSA down-selection process: a qualitative, fast, rule-based assessment and a preliminary quantitative approach (cf. Fig. 2).

3.3.1. Model-based formalization of design and safety rules

To include design and safety rules in the integrated MBSE-MBSA framework, it becomes imperative to formalize the rules with *SArA*. Design and safety rules are derived from regulatory texts, engineering standards, functional hazard analyses, and experts' knowledge [24]. The identified rules include the following standardized information:

- a brief textual description
- the mathematical-logical equation-based description
- the reference or rationale behind the rule

These three rule characteristics are added to the architecture model as shown in Fig. 6.

The rules are formalized within the model by storing the textual description and rationale of each rule in the MathWorks Requirements Editor. This textual description is implemented by mathematical-logical equations directly in MATLAB. By linking the logical rule to the textual description, machine-readable querying capabilities are enabled.

The formalized rules are directly evaluated on the architecture graph that is automatically derived from the architecture model. The graph

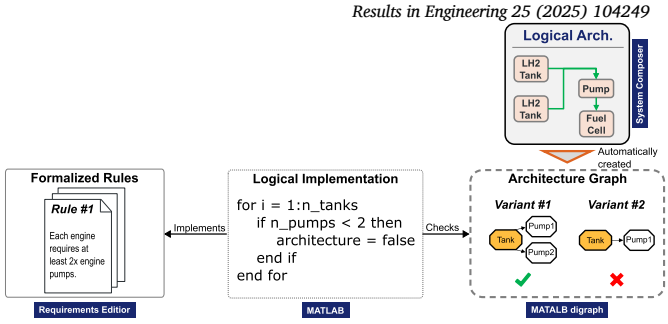

Fig. 6. Model-based formalization of the design and safety rules in the framework.

is built based on an algorithm that considers only model components, which are assigned generic elements. This automated graph generation ensures fast rule-checking for each rule while using the logical architecture model in System Composer as SSoT. Additionally, the model-based formalization serves as a means to conserve knowledge about the identified rules for future developments in an updatable manner. If opposing rules are added, currently, no architecture variants will be compliant with the rules. In the future, a rule consistency checker shall be developed to assist the engineer further.

3.3.2. Automated preliminary system safety analysis

A qualitative, rule-based safety assessment offers preliminary insights into architectural variants and aids the down-selection process. However, it is crucial to ensure that the remaining variants also quantitatively meet safety and reliability constraints based on assessing critical and typical failure cases. Following SAE ARP4754B [22], an PSSA as a quantitative safety assessment step is performed.

To perform the automated and simplified PSSA, different methods can be used [21]. In this paper, an FTA is employed. Its logical tree structure facilitates the comprehensive representation and examination of failure combinations. Deriving minimum cutsets enables a direct inspection of component failures that lead to vulnerabilities in the architecture and also determines the impact on the top-level failure event. This approach allows for a more comprehensive analysis than possible with RBDs.

To ensure a seamless process and to prevent the need to manually create an FTA for each variant and each failure condition, the developed toolchain in Fig. 7 is applied. First, the logical systems architecture, modeled in MathWorks System Composer (R2024b [104]), is automatically converted into the graph, using MATLAB digraph (R2024b [105]). The graph represents a significant simplification compared to the MBSE representation. Second, the design and safety rules are assessed on the graph. Third, architecture variants compliant with these qualitative rules are converted to a standardized graph modeling language (GML) interface file to ensure the architecture can be understood and handled by the Python-implemented *ASSESS*. This third step represents a tool shift from MATLAB to Python and is the interface between the two tool environments. This step also characterizes which information, i.e., components, connections, generic element type, and failure rates, must be transferred from MBSE to MBSA. Fourth, the GML file is the input for *ASSESS* L1-Module 1 implemented with *NetworkX*, a python package used to create and manipulate graphs [102] (version 3.3). The generic elements of *ASSESS* are represented as graph nodes, with the edges between the nodes representing the flow from one node to another. NetworkX is used to add information from the FHA to the graph information. The Python code was created in Visual Studio Code (version 1.92.0). To facilitate the implementation within Python, the packages Jinja2 (version 3.1.4), matplotlib (version 3.9.0), and pandas (version 2.2.2) are implemented. Fifth, based on the created document with NetworkX containing all information required for an FTA, *AltaRica* [103] (version 1.2.0) is used to compile and build the fault tree so that the quantitative analysis can be performed. Arbre-Analyst [106]

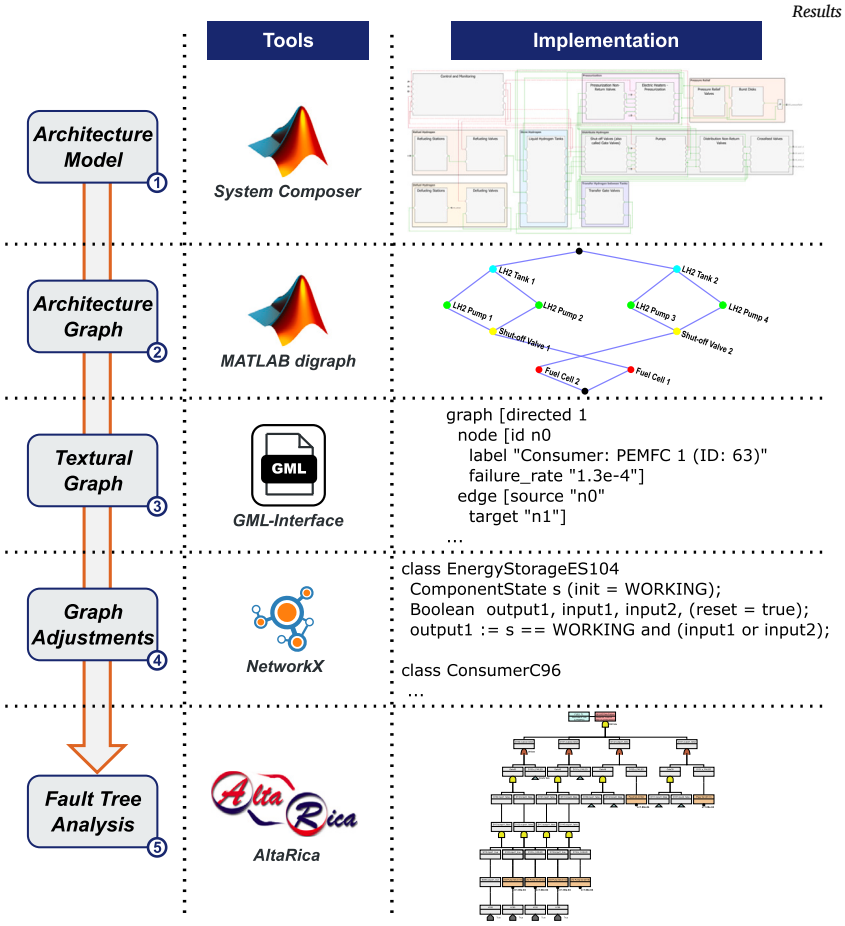

Fig. 7. Integrated MBSE and MBSA tool chain - tool images from [101–103].

(version 3.1.0) is used to clearly visualize the resulting fault tree and to calculate system failure rates. These selected tools are the author's preferences, but other tools may be used.

3.4. Identified design and safety rules for hydrogen fuel system

As a link between the integrated MBSE-MBSA approach and the case study, the identified and formalized rules for LH2 are presented. Most of the rules may also be applicable to GH2. The rules are categorized into "power flow view" and "mass flow view". The following list describes the seven identified rules for "power flow view":

1. Each engine supplied by at least two pumps requires at least two independent power distribution networks [92]
2. Each engine supplied by at least two pumps requires at least two independent power generation sources [92]
3. Each tank requires the Fuel Quantity Indication (FQI) sensors to be supplied with power from at least two independent power distribution networks [92]
4. Each tank requires the FQI sensors to be supplied with power from at least two independent power generation sources [92]
5. For Extended-range Twin-engine Operations Performance Standards (ETOPS) certified aircraft, at least three independent power generation sources are required for supplying power to the fuel system [91,92]
6. For ETOPS 180 certified aircraft, at least one pump and one crossfeed valve of each tank require at least one additional independent source of power, and it is, therefore, an addition to rule 5) [91,92]
7. For valves, check valves, shut-off valves, and regulators used in the logical architectures that are remotely controlled and actuated, an electric or pneumatic power supply is required [69]

The eleven identified "mass flow view" rules are:

1. Fuel shall be fed independently to each engine, meaning that each pump shall supply only one engine directly in nominal operation [91,90,69]
2. The number of tanks shall be greater or equal to the number of engines [92,69]
3. Each engine requires at least one fuel tank [92,96]
4. During take-off, each engine needs to be supplied by an isolated fuel tank [92]
5. Each engine requires at least two pumps for feeding the fuel [91,90,92,69,82]
6. Each auxiliary power unit (APU) requires fuel supply independent of normal engine fuel supply or requires an APU shutoff valve [90]
7. Each APU requires feed from at least two pumps [90]
8. The number of shutoff valves in the fuel system shall be greater or equal to the number of engines [96]
9. Each engine requires at least one dedicated shutoff valve to stop fuel flow [96]
10. Each pump feeding an engine shall be connected and, therefore, be able to supply fuel to any engine. This can be achieved by using crossfeed valves [92]
11. To prevent engine power loss from fuel starvation due to pump pressure loss during takeoff, each engine shall be supplied by two pumps running simultaneously from the same tank [82]

Additional rules applicable to more detailed architecture models are listed in Appendix A and assessed directly on the logical architecture model.

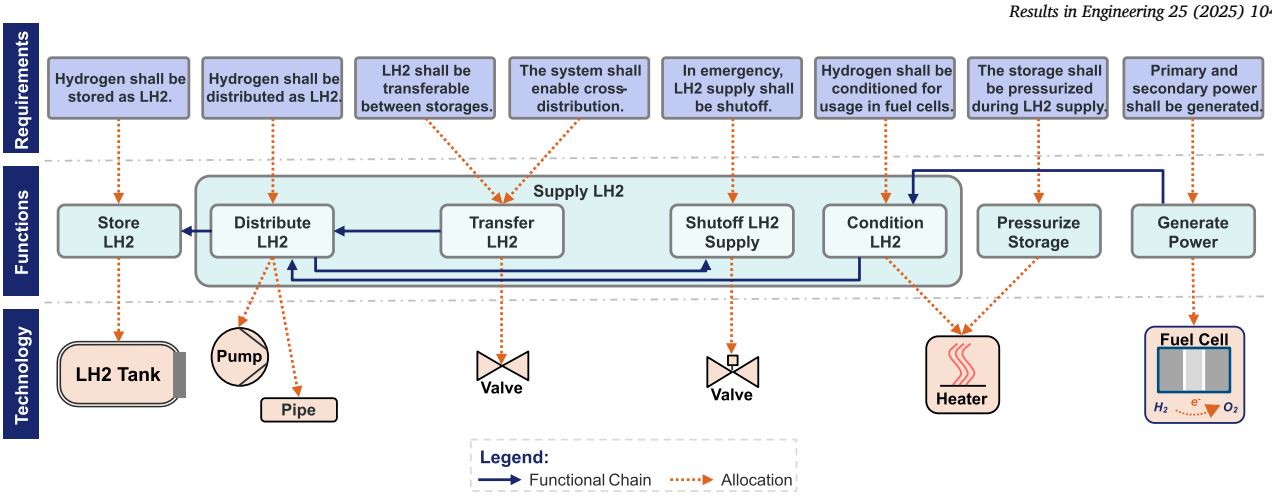

Fig. 8. Allocation of requirements to LH2 system functions to logical technologies.

Table 5
Characteristics and assumption for the hydrogen-powered concept aircraft.

System/Subsystem	Characteristics/Assumptions
Fuel	Hybrid - LH2 and kerosene
Engine	2x Turbofan with electric power train
Power Generation	2x H2-PEMFC + 1x kerosene-based APU
Flight Control System	Mechanically controlled
Electrical System	28 VDC
Hydraulic System	Electro-motor pump supply
Air Conditioning	Single, electrified pack

4. Case study

The integrated MBSE-MBSA framework assesses system architecture models during conceptual design for design and safety. Applied to a mid-size business aircraft, the case study introduces the aircraft, presents LH2 fuel system architecture variants, and demonstrates safety assessment.

4.1. Hydrogen-powered concept aircraft

The presented case study focuses on a mid-size business aircraft with two aft-fuselage mounted engines, similar to a *Bombardier Challenger 300*. This aircraft type typically operates a range of a few hundred miles but has a much longer design range. Fully powering it with LH2 is currently unfeasible due to the wide range profile and low volumetric energy density of LH2 [88], but a hybrid configuration seems promising. This study decouples aircraft from systems design, focusing on LH2 fuel system architectures rather than layout or physical integration, as this will be part of future work. The created architectures apply to most other aircraft with two engines designed according to 14 CFR Part 25 [91] or CS-25 [90]. For Part/CS 23 aircraft, adaptations are needed due to lower criticalities.

In this study, maintaining turbofan engines to burn both LH2 and kerosene is not feasible due to their differing fuel characteristics [88,82]. Each engine includes an EPT powered by LH2-driven PEMFCs for normal operation, as outlined in Table 5, and a kerosene-powered APU as a range extender.

Most aircraft systems remain unchanged unless noted to focus on LH2 system architecture variants. A mechanically controlled and partly actuated flight control system (FCS) is included, reducing the criticality of its power supply. The EPSS has two electric networks providing 28 VDC, with power supplied by PEMFCs and the APU instead of engine generators. To meet the high power demands for thrust, the EPT supply voltage is increased to 270 VDC. Electric motor pumps replace engine-driven pumps in the hydraulic system due to the EPT. The ECS, originally powered by a single bleed-powered pack, is electrified to compensate for the lack of bleed air from the PEMFCs. It can be seen that adding a new system affects other systems due to interrelations.

4.2. Logical LH2 system architecture variants

Stakeholder needs and requirements from aircraft fuel systems [93,94], and for the LH2 system [82] are formalized in the model-based requirements set and schematically shown in Fig. 8. Functions for the LH2 and influenced systems are identified and linked to the requirements. Each function is assigned a high-level technology, partially based on [82], to define the logical architecture design space. Further technological options, such as “pressure-feed,” could be explored in the future.

The design space focusing on redundancies is created as shown in Fig. 9. The number of tank instances is traded from one to three. Each tank is assumed to have its independent supply subsystem with cross-feeds similar to a kerosene fuel system. The number of LH2 pumps per tank (one to three) is investigated; Brewer [82] proposes three pumps per tank. Additionally, the number of distribution lines from the LH2 system to the PEMFCs, ranging from one fuel supply line per pump to all pumps feeding the PEMFCs via combined distribution lines. Electric power for the consumer is supplied by network “E1” or “E2”.

Combinatorially, nearly 9000 options are possible. Nevertheless, non-beneficial, mirrored, or infeasible variants are included, requiring a knowledge-based pre-down-selection with a focus on symmetric and close-to-kerosene-based fuel system architectures. Novel and unconventional, i.e., asymmetric, solutions are also considered. Overall, 18 variants are modeled. In the future, the design space could be directly created from the rules, advancing the framework to a knowledge-driven design space generation method.

For easy identification of the variants, a standardized naming convention is used: *2T4P2D_asy3and1P* describes a variant that includes two tanks (2T), four pumps in total (4P), two fuel distribution lines (2D), and highlights that it is an asymmetric concept with three pumps at one tank and one pump at the other (asy3and1P).

4.3. MBSA approach for the LH2 system architectures

Based on the defined LH2 fuel system architectures, the two-step conceptual safety assessment is conducted.

4.3.1. Qualitative rule-based design and safety assessment

The directed graphs of the architecture variants are automatically created from the architecture model as shown exemplarily in a partly simplified way in Fig. 10 and in Fig. 11 for the variant *2T4P2D*.

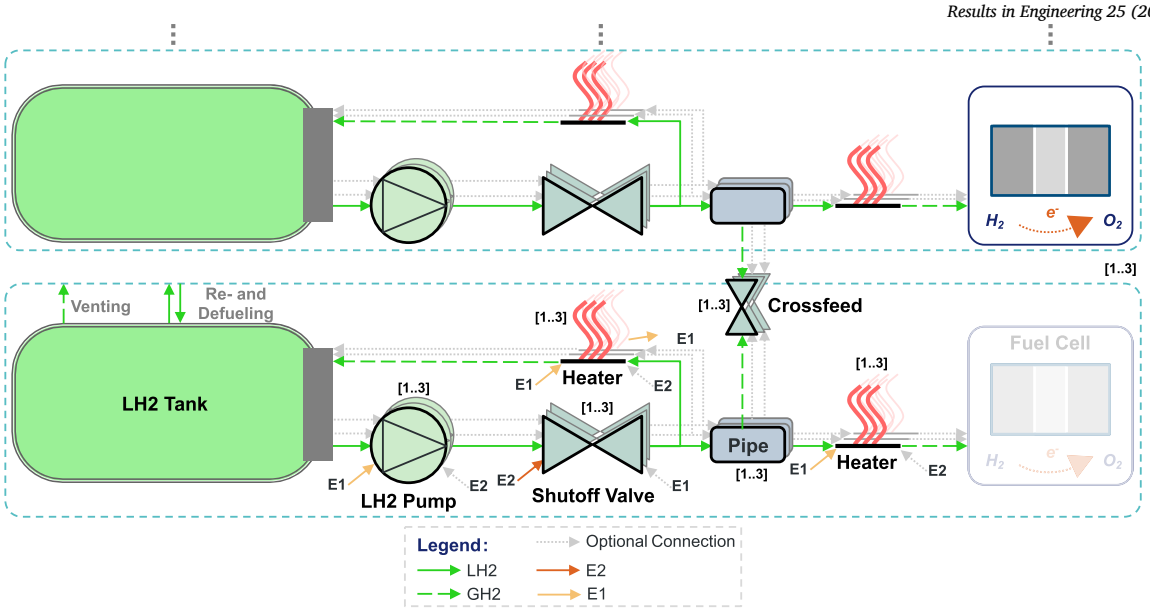

Fig. 9. Schematic representation of design space of logical LH2 system architectures.

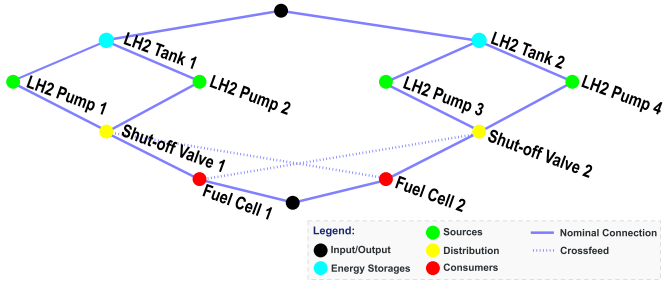

Fig. 10. Simplified "mass flow view" architecture graph for the LH2 variant *2T4P2D*.

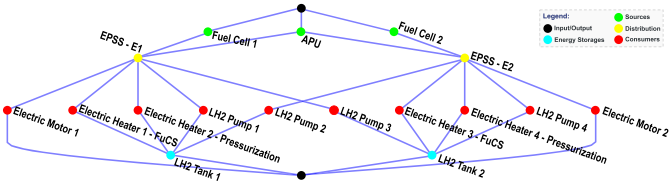

Fig. 11. Simplified "power flow view" architecture graph for the LH2 variant *2T4P2D*.

Different colors distinguish the various node types representing the generic elements of *ASSESS*. The "mass flow view" shows the reduced LH2 fuel system architecture graph relevant for conceptual safety assessment. The nominal connections are highlighted with a solid line, whereas the redundant cross-feed connections are highlighted with a dotted line. As described in subsection 3.2, the graph is direct from top to bottom if not shown otherwise. It can be seen that the graph clearly highlights the connections between the safety-relevant components. Hence, the fulfillment of the rules is directly checked with these graphs.

Rule fulfillment is rated "0" if the architecture does not comply with a rule, "1" if it complies, and "3" if the rule is not applicable, e.g., "power flow view" *Rule 1* requires two pumps to be applicable. The results are exemplarily demonstrated in Fig. 12 and fully in Appendix B (see Table B.10).

In total, seven variants, among others *2T4P2D*, *2T4P3D*, and *2T4P4D*, fulfill the qualitative assessment and will be further analyzed with the quantitative PSSA.

4.3.2. Developed multi-system FHA

To conduct the quantitative, integrated, and automated PSSA, critical failure conditions must be identified with a system FHA. Besides the LH2 fuel system, secondary power generation and supply is considered. Consequently, a multi-system FHA is created, as shown in Table 6.

Two catastrophic and one hazardous failure conditions are identified. Three failure observers, as the machine-readable representation of the top event in an FTA, are created:

1. for FHA item *#1*, loss of all LH2 distribution nodes or its predecessors in the "mass flow view" graph
2. for FHA item *#2*, loss of all consumers nodes or its predecessors in the "mass flow view" graph
3. for FHA item *#3*, loss of all-electric distribution nodes or its predecessors in the "power flow view" graph

4.3.3. Results of automated PSSA using FTA

The automated FTA, including component failure rates, is performed to preliminarily and quantitatively assess the compliance of the remaining architecture variants after rule-based down-selection. Failure rates for kerosene or oil-based systems are available [107,108] but not for LH2 components. Thus, the failure rates of LH2 components are assumed to be in a similar order of magnitude as kerosene components in an "optimistic" scenario; however, in reality, initial LH2 component failure rates are likely higher. Consequently, besides these "optimistic" failure rates, two additional pessimistic failure rate scenarios are investigated as shown in Table 7: one magnitude higher ("average") and even stricter failure rates ("conservative"). These three scenarios are used to handle the significant uncertainty during conceptual design. The three scenarios combined can be viewed as failure rate intervals. Calculating the system failure rate for all three scenarios provides a sensitivity analysis to show the engineer the effect of different failure rates. The focus in this work is on the order of magnitude, which is more relevant during conceptual design than precise quantitative failure rates. This order-of-magnitude-focused approach provides another rough failure rate interval.

The EPSS of the reference aircraft is considered safety-compliant and is not traded here. This includes the simplified two electric networks with a combined failure rate of 1×10^{-9} 1/fh and existing electric heaters. Moreover, the PEMFC failure rate is also kept constant for all three scenarios since the focus is on the LH2 system architecture. Additionally, pipes are usually represented as connections in a logical

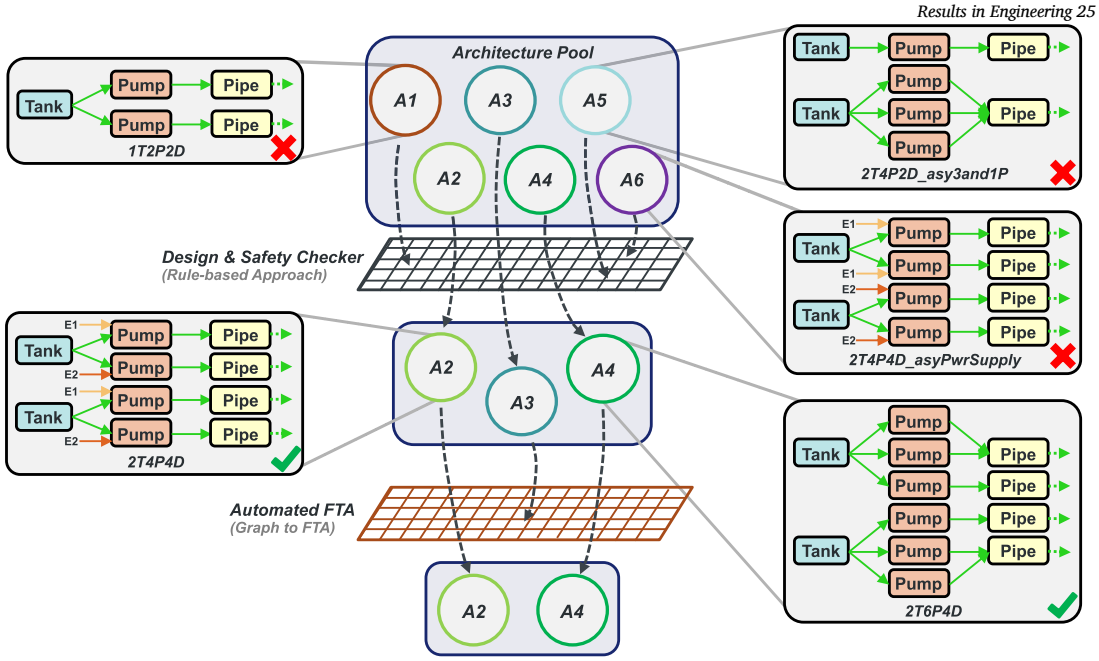

Fig. 12. Down-selection process with exemplary architecture variants.

Table 6
Developed high-level, multi-system FHA.

ID	Failure Condition	Flight Phase	Failure Effects	Classification
System: Fuel system				
Function: Supply LH2 fuel				
#1	Total loss of fuel flow to FCs; crew unaware	Takeoff, Climb, Cruise, Descent	Aircraft: potential loss of powered flight; Crew: Significant increase in workload; Occupants: potential severe injuries and fatalities if loss of altitude and flight into terrain	Hazardous
System: Secondary Power Distribution System				
Function: Provide electrical power				
#2	Total loss of electric power supply; crew unaware	Climb, Cruise, Descent	Aircraft: loss of EPT-powered flight; Crew: Significant increase in workload; Occupants: potential multiple fatal injuries if loss of altitude and flight into terrain	Catas-trophic
System: Secondary Power Generation System				
Function: Generate electrical power				
#3	Total loss of electric power generation; crew unaware	Climb, Cruise, Descent	Aircraft: loss of EPT-powered flight; Crew: Significant increase in workload; Occupants: potential multiple fatal injuries if loss of altitude and flight into terrain	Catastrophic

Table 7
Scenario-based LH2 component failure rates in [1/fh] to tackle uncertainties - data for non-traded components taken from [82,107,108].

Component	Conservative	Average	Optimistic
LH2 Pump	1×10^{-4}	1×10^{-5}	1×10^{-6}
Valve/Piping	1×10^{-4}	1×10^{-5}	1×10^{-6}
Electric Heater	1.1×10^{-5}		
PEMFC	1.3×10^{-4}		
APU	1.4×10^{-5}		
El. Power Supply	3.1×10^{-5}		

Table 8
FTA-based determined failure rates in [1/fh] for the failure *Total Loss of Electric Power Generation*.

LH2 Architectures	conservative	average	optimistic
2T4P2D	3×10^{-12}	4×10^{-13}	3×10^{-13}
2T4P3D	2×10^{-12}	4×10^{-13}	3×10^{-13}
2T4P4D	2×10^{-12}	4×10^{-13}	3×10^{-13}
2T5P4D	2×10^{-12}	4×10^{-13}	3×10^{-13}
2T6P2D	3×10^{-12}	4×10^{-13}	3×10^{-13}
2T6P4D	2×10^{-12}	4×10^{-13}	3×10^{-13}
2T6P6D	2×10^{-12}	4×10^{-13}	3×10^{-13}
Required	1×10^{-9}		

architecture model without a failure rate, so the failure rate of the *valves* is assumed to represent the pipes. The LH2 tank shall be designed for the full life of the aircraft (≈50 000 fh [82]) and positioned outside the rotor burst zone to minimize hazards [90–92]. Therefore, the LH2 tank is not considered in this PSSA but has been qualitatively assessed with the rules. The authors note that even though data exists for these components with a fixed failure rate and an average value has been determined, uncertainties are still present, and confidence intervals should normally be considered. However, the error included here is the same for all three scenarios and is, therefore, ignored in this case study to focus purely on the LH2 system architecture.

In total, 63 FTAs are automatically generated and assessed for each variant and graph view, the three failure rate scenarios, and the three observers. The determined system failure rates are presented without decimal places in Table 8, Table 9, and Table C.11, as the order of magnitude is relevant at this early stage, and decimal-based results would imply a false precision.

Table 9
FTA-based determined failure rates in [1/fh] for the failure *Total Loss of LH2 Supply to PEMFCs*.

LH2 Architectures	conservative	average	optimistic
2T4P2D	1×10^{-8}	1×10^{-10}	1×10^{-12}
2T4P3D	4×10^{-12}	4×10^{-15}	4×10^{-18}
2T4P4D	2×10^{-15}	2×10^{-19}	2×10^{-23}
2T5P4D	8×10^{-16}	8×10^{-20}	8×10^{-24}
2T6P2D	1×10^{-8}	1×10^{-10}	1×10^{-12}
2T6P4D	4×10^{-16}	4×10^{-20}	4×10^{-24}
2T6P6D	7×10^{-23}	7×10^{-29}	5×10^{-34}
Required	1×10^{-7}		

All variants that fulfill the qualitative assessment also comply with the PSSA. Highly redundant architectures, such as *2T6P6D* proposed by Brewer [82], achieve very low failure rates due to extensive crossfeed connections and redundant paths; however, when looking at high-level metrics, such as complexity, an overly redundant variant is not beneficial. Complexity can be estimated as the number of components times the number of connections (cf. [20]). The variant *2T4P2D* sores 16 ($2 * 4 * 2$). In contrast, the highly redundant variant *2T6P6D* scores 72 ($2 * 6 * 6$). The goal of combined MBSE-MBSA during conceptual design is not to perform a complete trade study, which would also require an assessment at the physical level, but to identify and eliminate infeasible variants reducing the design space. Furthermore, the goal is not to identify the safest solution but rather to find architectures that are safe enough according to certification regulations and stated design assurance levels. Hence, the *2T4P2D* architecture, i.e., two tanks, four pumps, and 2 normal distribution lines, is selected here, as it provides a reasonable safety margin and is the least complex architecture of the remaining variants. The authors state that this case study illustrates the framework's capabilities and is not a complete trade study. Further activities on a physical level are required.

The automatically determined failure rates are checked and validated using the external safety assessment tool *SyRelAn* [109,110]. Furthermore, the results are validated based on the author's experience in the industry. In addition, the two most promising architectures, i.e., *2T4P2D* and *2T4P4D*, have been discussed with industry experts who agreed on the findings and the selection of these architectures.

The case study shows that the rules already effectively reduce the theoretically large design space to only a few feasible variants; the viable design space is more strictly limited with respect to redundancies than it initially appears. Considering existing knowledge remains essential, even for novel systems. Furthermore, it can be concluded that both research objectives (cf. section 1) have been achieved since it was possible to identify feasible architectures with the developed framework.

4.4. Discussion and limitations of the MBSE-MBSA framework

The case study demonstrates that the integrated MBSE-MBSA framework effectively narrows the design space for novel systems by leveraging existing knowledge, standards, and certification rules. Rapid and automated safety assessments use the architecture model as an SSoT, enabling iterative validation alongside design to identify issues early and potentially reduce costly redesigns. The framework shows that design spaces, even for new systems, are constrained by established rules and regulations.

However, the framework is complex, requiring expert knowledge and adherence to the modeling standards with *SArA* to avoid errors in the automatically created architecture graphs and FTAs. The framework is currently also tool-dependent, requiring significant implementation changes for alternative tools. However, other tools are possible since the case study has shown which information and steps are required for integrated MBSE with MBSA. Future work aims to explore broader tool applicability.

The case study illustrates the framework's capabilities through the LH2 fuel system architecture use case. While it can be applied to more complex systems in aerospace and beyond, adaptations to graph representations may be necessary. Furthermore, updates to design and safety rules are needed for other applications, such as gaseous hydrogen or novel propulsion technologies. Collecting these rules is a time-consuming process, but the model-based formalized rules create a valuable knowledge base for future case studies.

Modeling complex systems becomes challenging as model complexity and variants increase, a common issue in MBSE for large systems. The framework currently applies to early conceptual design at the logical level but possibly struggles with detailed physical architectures due to abstracted aspects like system behavior and preliminary technology selections. Future work will address these limitations by incorporating physical and geometric aspects to expand the applicability of the framework.

5. Conclusion and outlook

This work presents a framework that integrates Model-Based Systems Engineering (MBSE) and Model-Based Safety Assessment (MBSA) during aircraft conceptual design. By linking the MBSE-driven *SArA* methodology with the MBSA framework *ASSESS*, this integrated MBSE-MBSA framework enables the design of complex, novel systems compliant with safety requirements. The effectiveness of this approach is demonstrated on liquid hydrogen fuel system architectures for a two-engine mid-size business aircraft and is applicable to most two-engine aircraft under Part/CS 25.

The integrated MBSE-MBSA framework supports engineers in efficiently narrowing down the design space for novel systems during early design phases by leveraging existing knowledge and established standards. By automating conceptual safety assessments and using the architecture model as a single source of truth, the framework enables early, concurrent, and iterative validation of system architectures, reducing costly late-stage design iterations. However, the framework's complexity requires significant expertise in systems architecting, safety assessment, and tool and methodology-specific modeling standards.

The authors focused on LH2 fuel system architecture variants based on redundancy. Other safety aspects, including zonal safety assessment and particular risk analysis, as well as technologies, should be addressed in future work. Moreover, the rules focus on liquid hydrogen and should be extended to gaseous hydrogen and other means of conditioning, requiring additional rules that can be readily incorporated due to the model-based approach.

Overall, the presented work contributes to increasing the maturity of hydrogen fuel system architectures for aircraft conceptual design studies and speeds up their exploration, development, and concurrent safety assessment process.

CRediT authorship contribution statement

Nils Kuelper: Writing – review & editing, Writing – original draft, Visualization, Software, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Andrew K. Jeyaraj:** Writing – original draft, Validation, Software, Methodology, Investigation, Data curation, Conceptualization. **Susan Liscouët-Hanke:** Writing – review & editing, Validation, Supervision, Project administration, Methodology, Funding acquisition, Conceptualization. **Frank Thielecke:** Writing – review & editing, Validation, Supervision, Project administration, Methodology, Funding acquisition, Conceptualization.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Nils Kuelper reports financial support was provided by Mitacs Canada. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors express their thanks to Mitacs Globalink Research Award for research in Canada (Application Ref. IT38773) for funding this collaborative research. Furthermore, the authors express their thanks to the student *Pierre-Olivier Paquette* who assisted with tool implementations. Publishing fees supported by Funding Programme Open Access Publishing of Hamburg University of Technology (TUHH) (Grant number OA08/2025).

Appendix A. Detailed design and safety rules for LH2 logical architecture models

1. Each LH2 tank requires at least one pressure relief system (PRS) [65,66,69,91]
2. Each LH2 distribution using piping requires at least one PRS [63, 65,69,73,81]
3. Each pressure relief system (PRS) typically requires at least one pressure-relief device (PRD) and one burst disk (BD) [65,69]
4. Each upstream PRS typically requires the PRD and BD to be in series to prevent any air ingress [69]
5. Each downstream LH2 system PRS typically requires the PRD and BD to be in parallel [69]
6. A shutoff valve is not allowed between the component requiring release and the environment to prevent blocking. The only exceptions are maintenance shutoff valves, locked in an open position [63,69,73]
7. Each LH2 distribution system requires at least one shutoff valve, e.g., an emergency valve, as close as possible to the LH2 tank [63, 73]
8. Each LH2 distribution system requires at least one shutoff valve, e.g., an emergency valve, as close as possible to the point of use, e.g., power generation [73]

Appendix B. Detailed results of the rule-based assessment

Table B.10
Results of rule-based assessment.

		1T1P1D	1T2P2D	2T2P2D	2T3P2D	2T3P3D	2T4P2D	2T4P2D -asy3and1P	2T4P3D	2T4P4D	2T4P4D -1P1T1FC	2T4P4D -pwrFCcross	2T4P4D -asyElPwr	2T5P4D	2T6P2D	2T6P4D	2T6P4D -noXfeed	2T6P6D	3T3P3D
Power Flow View	Rule 1	3	1	0	0	0	1	0	1	1	1	1	0	1	1	1	1	1	0
	Rule 2	3	1	0	0	0	1	0	1	1	1	1	1	1	1	1	1	1	0
	Rule 3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	Rule 4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	Rule 5	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	Rule 6	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	Rule 7	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Fuel Flow View	Rule 1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Rule 2	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Rule 3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Rule 4	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Rule 5	0	0	0	0	0	1	0	1	1	1	1	1	1	1	1	1	1	0
	Rule 6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Rule 7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Rule 8	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Rule 9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Rule 10	3	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1
	Rule 11	0	0	0	0	0	1	0	1	1	0	0	0	1	1	1	1	1	0
Summary		0	0	0	0	0	1	0	1	1	0	0	0	1	1	1	0	1	0

Appendix C. Detailed results of the FTA in [1/fh] for the failure *total loss of electric power supply*

Table C.11
FTA-based determined failure rates in [1/fh] for the failure *Total Loss of Electric Power Supply*.

LH2 Architectures	conservative	average	optimistic
2T4P2D	9×10^{-10}	9×10^{-10}	9×10^{-10}
2T4P3D	9×10^{-10}	9×10^{-10}	9×10^{-10}
2T4P4D	9×10^{-10}	9×10^{-10}	9×10^{-10}
2T5P4D	9×10^{-10}	9×10^{-10}	9×10^{-10}
2T6P2D	9×10^{-10}	9×10^{-10}	9×10^{-10}
2T6P4D	9×10^{-10}	9×10^{-10}	9×10^{-10}
2T6P6D	9×10^{-10}	9×10^{-10}	9×10^{-10}
Required	1×10^{-9}		

Appendix D. Logical architecture model snapshots for the variant *2T4P4D*

In aerospace, systems architectures are typically modeled at different levels of detail to effectively represent the hierarchy and manage complexity. These levels generally include:

1. Overall Systems Level: This high-level perspective captures the complete systems at the aircraft level, focusing on overarching goals, functionality, and interactions with external systems or environments (cf. Fig. D.13).
2. System Level: At this level, the system is broken down into its major subsystems, defining its internal relationships and interactions while focusing on the system's intended functionality and architecture (cf. Fig. D.14).
3. Components Level: This detailed perspective dives into the individual components or elements within an aircraft system, specifying their internal structure, redundancy, behavior, and technical details (cf. Fig. D.15).

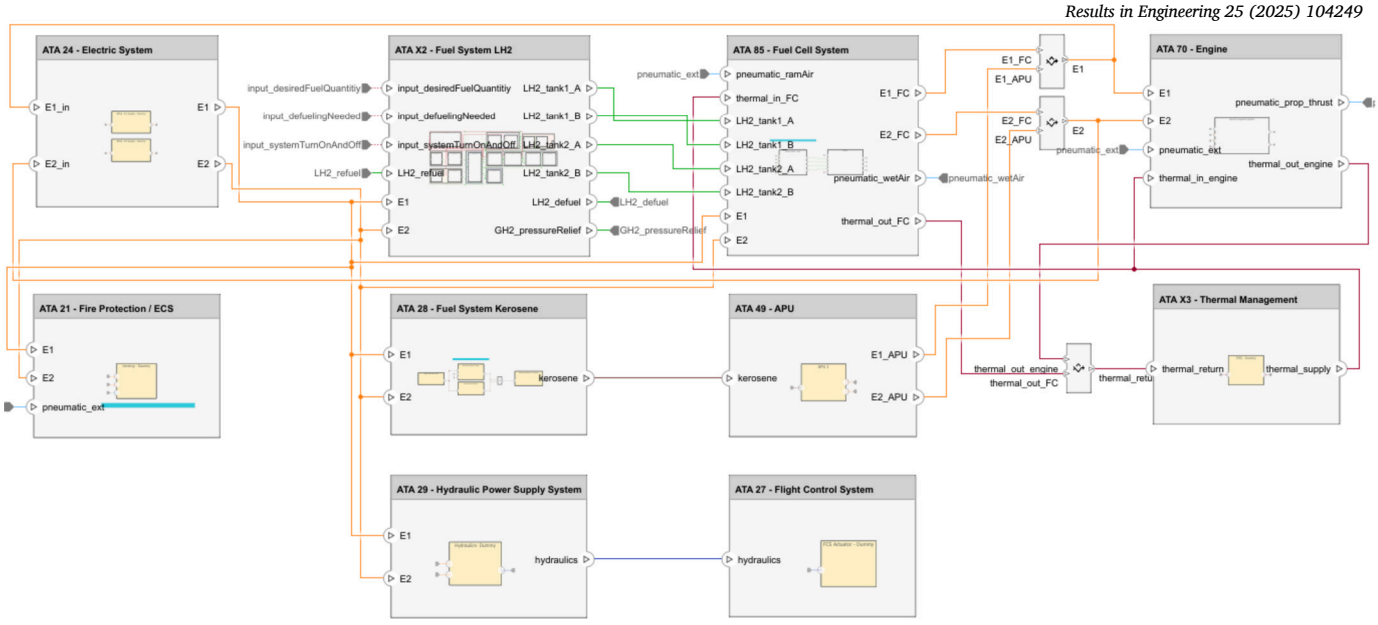

Fig. D.13. Exemplary model representation of the overall systems level of the architecture variant *2T4P4D* in System Composer.

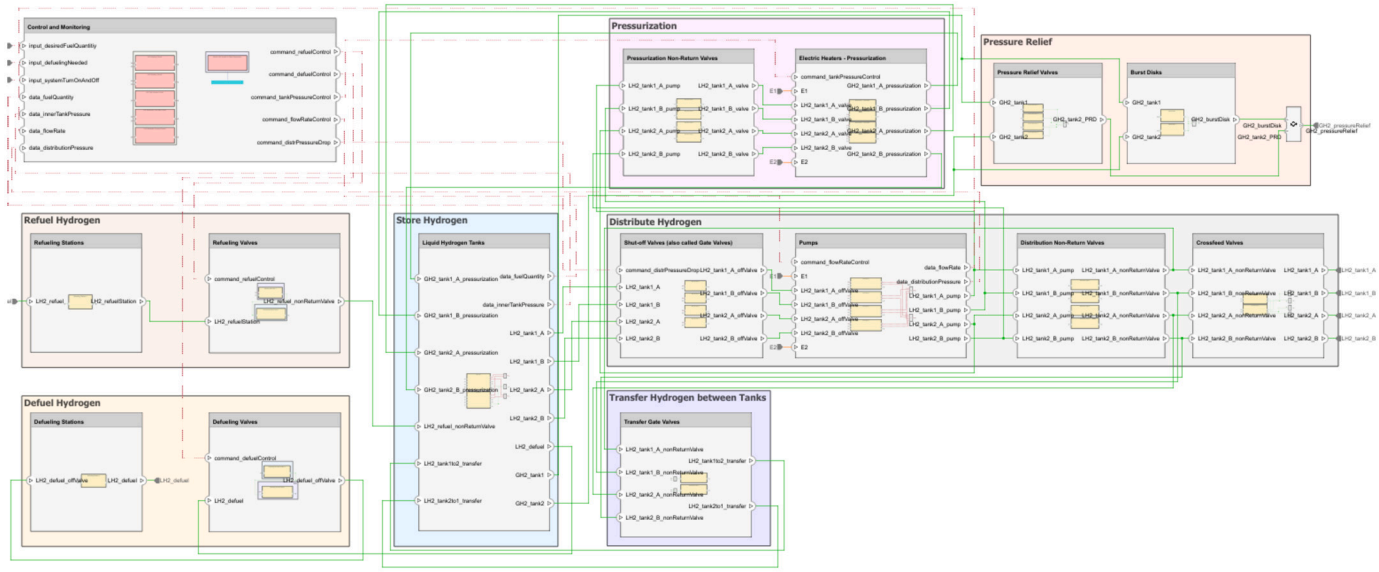

Fig. D.14. Exemplary model representation of the system level (LH2 fuel system) of the architecture variant *2T4P4D* in System Composer.

These three levels are implemented in System Composer, and each level is exemplary and shown once.

Data availability

Data will be made available on request.

References

[1] D.S. Lee, D.W. Fahey, P.M. Forster, P.J. Newton, R.C. Wit, L.L. Lim, B. Owen, R. Sausen, Aviation and global climate change in the 21st century, Atmos. Environ. 43 (22) (2009) 3520–3537.

[2] Air Transport Action Group, Waypoint 2050: Balancing growth in connectivity with a comprehensive global air transport response to the climate emergency: vision of net-zero aviation by mid-century, 2021.

[3] Environment and Climate Change Canada, A healthy environment and a healthy economy, Canada, 2020.

[4] European Commission, Flightpath 2050: Europe's vision for aviation, Luxembourg, 2011.

[5] A. Marimuthu, P.K. Govindasamy, Hydrogen towards sustainable transition: a review of production, economic, environmental impact and scaling factors, Results Eng. 20 (2023) 101456.

[6] Airbus, ZEROe: towards the world's first zero-emission commercial aircraft [Online]. Available at https://www.airbus.com/en/innovation/zero-emission/hydrogen/zeroe, 2022.

[7] J. Hoelzen, D. Silberhorn, T. Zill, B. Bensmann, R. Hanke-Rauschenbach, Hydrogen-powered aviation and its reliance on green hydrogen infrastructure: review and research gaps, Int. J. Hydrog. Energy 47 (5) (2022) 3108–3130.

[8] H.-H. Altfeld, Commercial Aircraft Projects: Managing the Development of Highly Complex Products, Ashgate, 2010.

[9] V. Voth, S.M. Lübbe, M. Schäfer, A. Berres, O. Bertram, Functional approach to a fuel cell thermal management system in safety-critical applications, in: AIAA Aviation 2023 Forum, San Diego, California, USA, 2023.

[10] N. Kuelper, V. Kriewall, K. Beschorner, F. Thielecke, TechMAPS – technology management for the architecting process of aircraft on-board systems, in: 34th Congress of the International Council of the Aeronautical Sciences, Florence, Italy, 2024.

[11] D.M. Judt, C. Lawson, Development of an automated aircraft subsystem architecture generation and analysis tool, Eng. Comput. 33 (5) (2016) 1327–1352.

[12] T.S. Geiger, D.M. Dilts, Automated design-to-cost: integrating costing into the design decision, Comput. Aided Des. 28 (6–7) (1996) 423–438.

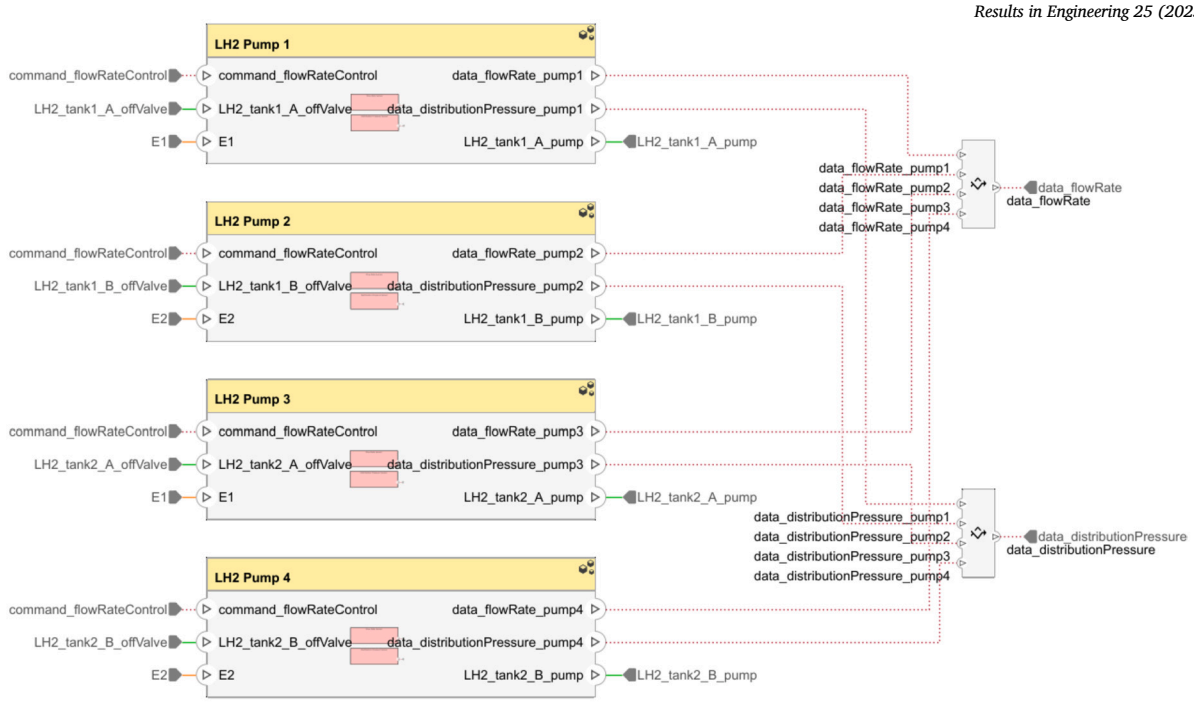

Fig. D.15. Exemplary model representation of the component level (LH2 pumps) of the architecture variant *2T4P4D* in System Composer.

[13] International Council on Systems Engineering, Systems engineering vision 2020, 2007.
[14] D.D. Walden (Ed.), Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, fifth edition, Wiley, Hoboken, NJ, 2023.
[15] J.-C. Chaudemar, P. de Saqui-Sannes, MBSE and MDAO for early validation of design decisions: a bibliography survey, in: 2021 IEEE International Systems Conference (SysCon), Virtual Conference, 2021.
[16] P. Nowodzienski, J. Navas, From model-based to model and simulation-based systems architectures – achieving quality engineering through descriptive and analytical models, INCOSE Int. Symp. 32 (1) (2022) 1247–1266.
[17] J. Holt, S. Perry, Model-Based Requirements Engineering, IET Professional Applications of Computing Series, vol. 9, Institution of Engineering and Technology, Stevenage, United Kingdom, 2012.
[18] N. Kuelper, J. Broehan, T. Bielsky, F. Thielecke, Systems Architecting Assistant (SArA) - enabling a seamless process chain from requirements to overall systems design, in: 33rd Congress of the International Council of the Aeronautical Sciences, Stockholm, Sweden, 2022.
[19] N. Kuelper, T. Bielsky, J. Broehan, F. Thielecke, Model–based framework for data and knowledge–driven systems architecting demonstrated on a hydrogen–powered concept aircraft, INCOSE Int. Symp. 33 (1) (2023) 666–688.
[20] N. Kuelper, V. Starke, J. Broehan, F. Thielecke, Evaluation metrics for systems architecting demonstrated on cooling system of hydrogen-powered concept aircraft, in: AIAA Science and Technology Forum and Exposition (AIAA SciTech Forum), Orlando, USA, 2024.
[21] SAE International, ARP4761A: Guidelines for conducting the safety assessment process on civil aircraft, systems, and equipment, 2023.
[22] SAE International, ARP4754B: Guidelines for development of civil aircraft and systems, 2023.
[23] A. Joshi, M.P.E. Heimdahl, S.P. Miller, M.W. Whalen, Model-based safety analysis.
[24] A.K. Jeyaraj, S. Liscouët-Hanke, A safety-focused system architecting framework for the conceptual design of aircraft systems, Aerospace 9 (12) (2022) 791.
[25] M.J. Armstrong, Identification of emergent off-nominal operational requirements during conceptual architecting of the more electric aircraft, Dissertation, Georgia Institute of Technology, Atlanta, Georgia, USA, 2011.
[26] S. Liscouet-Hanke, A model-based methodology for integrated preliminary sizing and analysis of aircraft power system architecture, Dissertation, Institut National des Sciences Appliquées de Toulouse, Toulouse, France, 2008.
[27] S. Liscouët-Hanke, J.-C. Maré, S. Pufe, Simulation framework for aircraft power system architecting, J. Aircr. 46 (4) (2009) 1375–1380.
[28] C. Raksch, F. Thielecke, Optimierung fehlertoleranter Flugzeugsysteme mit mehrfachen Sicherheits- und Zuverlässigkeitsanforderungen, in: German Aerospace Congress, Hamburg, Germany, 2010.
[29] C. Raksch, Eine Methode zur optimalen Redundanzallokation im Vorentwurf fehlertoleranter Flugzeugsysteme, Dissertation, Hamburg University of Technology, Hamburg, Germany, 2013.
[30] I. Chakraborty, Subsystem architecture sizing and analysis for aircraft conceptual design, Dissertation, Georgia Institute of Technology, Atlanta, Georgia, USA, 2015.
[31] I. Chakraborty, D.N. Mavris, Heuristic definition, evaluation, and impact decomposition of aircraft subsystem architectures, American Institute of Aeronautics and Astronautics, 2016.
[32] C. Johansson, On System Safety and Reliability Methods in Early Design Phases: Cost Focused Optimization Applied on Aircraft Systems, 1st ed., Linköping University Medical Dissertations Ser., vol. 1600, Linkopings Universitet, Linköping, 2013.
[33] C. Johansson, M. Derelöv, J. Ölvander, How to use an optimization-based method capable of balancing safety, reliability, and weight in an aircraft design process, Nucl. Eng. Technol. 49 (2) (2017) 404–410.
[34] R. Bornholdt, T. Kreitz, F. Thielecke, Function-driven design and evaluation of innovative flight controls and power system architectures, in: SAE 2015 AeroTech Congress & Exhibition, Seattle, Washington, USA, 2015.
[35] R. Bornholdt, Systemübergreifende Analyse und Bewertung von Architekturvarianten neuartiger Flugzeugsysteme anhand von Sicherheits- und Betriebsaspekten, Dissertation, Hamburg University of Technology, Hamburg, Germany, 2021.
[36] R. Fusaro, N. Viola, D. Ferretto, S. Cresto Aleina, M. Fioriti, L. Boggero, Methodology for the safety and reliability assessment of hypersonic transportation systems in conceptual design activities, in: 21st AIAA International Space Planes and Hypersonics Technologies Conference, Xiamen, China, 2017.
[37] S. Jimeno, A. Molina-Cristobal, A. Riaz, M. Guenov, Incorporating safety in early (airframe) systems design and assessment, in: AIAA Science and Technology Forum and Exposition (AIAA SciTech Forum), San Diego, California, USA, 2019.
[38] S. Jimeno, A. Riaz, M. Guenov, A. Molina-Cristobal, Enabling interactive safety and performance trade-offs in early airframe systems design, in: AIAA Science and Technology Forum and Exposition (AIAA SciTech Forum), Orlando, Florida, USA, 2020.
[39] Dassault Systèmes, Dassault systèmes introduces v6 to the market: sixth generation solution brings plm 2.0 to life [Online]. Available at https://www.3ds.com/newsroom/press-releases/dassault-systemes-introduces-v6-market, 2008.
[40] S. Kleiner, C. Kramer, Model based design with systems engineering based on RFLP using v6, in: Smart Product Engineering, 2013, pp. 93–102.
[41] M.-H. Bleu-Laine, M.V. Bendarkar, J. Xie, S.I. Briceno, D.N. Mavris, A model-based system engineering approach to normal category airplane airworthiness certification, in: AIAA Aviation 2019 Forum, Dallas, Texas, USA, 2019.
[42] E. Harrison, M.V. Bendarkar, A. Baker, M. Misra, L. Paulson, E. Garcia, D. Mavris, Development of aircraft architecture descriptions to support model-based regulatory analysis, in: AIAA Aviation 2024 Forum, Las Vegas, Nevada, USA, 2024.
[43] F. Rehfeldt, F. Thielecke, Architecting of databus networks for flight control systems with smart actuation, in: German Aerospace Congress, Darmstadt, Germany, 2019.
[44] G. Biggs, T. Juknevicius, A. Armonas, K. Post, Integrating safety and reliability analysis into MBSE: overview of the new proposed OMG standard, INCOSE Int. Symp. 28 (1) (2018) 1322–1336.
[45] G. Biggs, K. Post, A. Armonas, N. Yakymets, T. Juknevicius, A. Berres, OMG standard for integrating safety and reliability analysis into MBSE: concepts and applications, INCOSE Int. Symp. 29 (1) (2019) 159–173.
[46] R. Krishnan, S.V. Bhada, An integrated system design and safety framework for model-based safety analysis, IEEE Access 8 (2020) 146 483–146 497.

[47] R. Krishnan, S.V. Bhada, Integrated system design and safety framework for model-based safety assessment, IEEE Access 10 (2022) 79 311–79 334.
[48] A. Ahlbrecht, O. Bertram, Evaluating system architecture safety in early phases of development with mbse and stpa, in: 2021 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 2021, pp. 1–8.
[49] A. Ahlbrecht, U. Durak, Integrating safety into mbse processes with formal methods, in: IEEE/AIAA 40th Digital Avionics Systems Conference (DASC), San Antonio, Texas, USA, 2021, pp. 1–9.
[50] M. Quamara, G. Pedroza, B. Hamid, Multi-layered model-based design approach towards system safety and security co-engineering, in: 2021 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C), Fukuoka, Japan, 2021, pp. 274–283.
[51] C. Cabaleiro, M. Fioriti, L. Boggero, Methodology for the automated preliminary certification of on-board systems architectures through requirements analysis, in: 33rd Congress of the International Council of the Aeronautical Sciences, Stockholm, Sweden, 2022.
[52] M. Schäfer, A. Berres, O. Bertram, Integrated model-based design and functional hazard assessment with sysml on the example of a shock control bump system, CEAS Aeronaut. J. 14 (1) (2022) 187–200.
[53] S.M. Lübbe, M. Schäfer, O. Bertram, Coupling of model-based systems engineering and safety analysis in conceptual aircraft system design, in: 33rd Congress of the International Council of the Aeronautical Sciences, Stockholm, Sweden, 2022.
[54] A.K. Jeyaraj, J. Bussemaker, S. Liscouët-Hanke, L. Boggero, Systems architecting: a practical example of design space modeling and safety-based filtering within the AGILE4.0 project, in: 33rd Congress of the International Council of the Aeronautical Sciences, Stockholm, Sweden, 2022.
[55] K. Lai, T. Robert, D. Shindman, A. Olechowski, Mbfha: a framework for model–based functional hazard assessment for aircraft systems, INCOSE Int. Symp. 33 (1) (2023) 431–447.
[56] M. Schorr, V. Voth, C. Gentner, Effects on the design of aeronautical fuel cell systems by inclusion of reliability requirements, CEAS Aeronaut. J. (2024).
[57] P. PiąTek, P. Mydłowski, A. Buczacki, S. Moskwa, Concept of using the mbse approach to integrate security patterns in safety-related projects for the automotive industry, IEEE Trans. Intell. Transp. Syst. 25 (11) (2024) 15 477–15 492.
[58] M. Kang, S. Eom, K. Hwang, Advancing autonomous vehicle safety assessment: a novel methodology for moving from functional to concrete scenarios using kinetic 3d-lidar and shap, Results Eng. 24 (2024) 103364.
[59] E. Kolip, Improving model-based system architecture specification to enable fault tree analysis, Master Thesis, Concordia University, Montreal, Québec, Canada, 2024.
[60] M. Juenemann, F. Thielecke, F. Peter, M. Hornung, F. Schültke, E. Stumpf, Methodology for design and evaluation of more electric aircraft systems architectures within the avacon project, in: German Aerospace Congress, Darmstadt, Germany, 2019.
[61] N. Tabesh, A.K. Jeyaraj, S. Liscouët-Hanke, A. Tamayo, Integration of the functional hazard assessment within a model-based systems engineering framework, J. Aerosp. Inform. Syst. (2024) 1–13.
[62] P. Bamrah, S. Liscouet-Hanke, A. Tfaily, A. Tamayo, Zonal safety and particular risk analysis for aircraft conceptual design, in: AIAA Aviation 2023 Forum, San Diego, California, USA, 2023.
[63] Guide to safety of hydrogen and hydrogen systems (ANSI/AIAA G-095A-2017), Guide to Safety of Hydrogen and Hydrogen Systems, ANSI/AIAA G. Reston, vol. 71, American Institute of Aeronautics and Astronautics, Va, 2017, p. 73.
[64] CSA America, HGV 2: Compressed hydrogen gas vehicle fuel containers.
[65] European Parliament and Council, EN406/2010: Type-approval of hydrogen-powered motor vehicles.
[66] European Parliament and Council, EU 2019/2144: Type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users.
[67] Federal Aviation Administration, Dot/faa/tc-19/16: Energy supply device aviation rulemaking committee.
[68] International Organization for Standardization, ISO 13985:2006: Liquid hydrogen - land vehicle fuel tanks.
[69] International Organization for Standardization, ISO/TR 15916:2015: Basic considerations for the safety of hydrogen systems.
[70] International Organization for Standardization, ISO 19881:2018: Gaseous hydrogen - land vehicle fuel containers.
[71] International Organization for Standardization, ISO 17268:2020: Gaseous hydrogen land vehicle refuelling connection devices.
[72] National Aeronautics and Space Administration, NSS 1740.16: Safety standard for hydrogen and hydrogen systems.
[73] National Fire Protection Association, NFPA 2: Hydrogen technologies code, Quincy, Massachusetts.
[74] SAE International, AIR7765: Considerations for hydrogen fuel cells in airborne applications.
[75] SAE International, AIR6464: Eurocae/sae wg80/ae-7afc hydrogen fuel cells aircraft fuel cell safety guidelines.
[76] SAE International, AS6858: Installation of fuel cell systems in large civil aircraft.
[77] SAE International, J2578: Recommended practice for general fuel cell vehicle safety.
[78] SAE International, J2579: Standard for fuel systems in fuel cell and other hydrogen vehicles.
[79] SAE International, AS6679: Liquid hydrogen storage for aviation- wip.
[80] SAE International, AS7373: Gaseous hydrogen storage for general aviation - wip.
[81] United Nations, Addendum 13: UN Global Technical Regulation No. 13: Hydrogen and fuel cell vehicles.
[82] G.D. Brewer, Hydrogen Aircraft Technology, 1st ed., CRC Press LLC, Bosa Roca, 1991.
[83] G. Klein, B. Zapf, T. Weidl, Hydrogen applications to aircrafts and cars - basic safety aspects, 2005.
[84] D. Verstraete, The potential of liquid hydrogen for long range aircraft propulsion, Dissertation, Cranfield University, Cranfield, United Kingdom, 2009.
[85] J.-B. Saffers, V.V. Molkov, Hydrogen safety engineering framework and elementary design safety tools, Int. J. Hydrog. Energy 39 (11) (2014) 6268–6285.
[86] I. Dincer, C.O. Colpan, O. Kizilkan, M.A. Ezan, Progress in Clean Energy, Springer, Cham, 2015.
[87] C. San Marchi, E.S. Hecht, I.W. Ekoto, K.M. Groth, C. LaFleur, B.P. Somerday, R. Mukundan, T. Rockward, J. Keller, C.W. James, Overview of the doe hydrogen safety, codes and standards program, part 3: advances in research and development to enhance the scientific basis for hydrogen regulations, codes and standards, Int. J. Hydrog. Energy 42 (11) (2017) 7263–7274.
[88] E.J. Adler, J.R. Martins, Hydrogen-powered aircraft: fundamental concepts, key technologies, and environmental impacts, Prog. Aerosp. Sci. 141 (2023) 100922.
[89] M. Genovese, V. Cigolotti, E. Jannelli, P. Fragiacomo, Current standards and configurations for the permitting and operation of hydrogen refueling stations, Int. J. Hydrog. Energy 48 (51) (2023) 19 357–19 371.
[90] European Union Aviation Safety Agency, CS-25 amendment 28 [Online]. Available at https://www.easa.europa.eu/en/document-library/certification-specifications/cs-25-amendment-28.
[91] Federal Aviation Administration, 14 CFR part 25: airworthiness standards: transport category airplanes [Online]. Available at https://www.ecfr.gov/current/title-14/chapter-I/subchapter-C/part-25.
[92] SAE International, AIR7975: Aircraft fuel system design guidelines.
[93] I. Moir, A. Seabridge, Aircraft Systems: Mechanical, Electrical and Avionics Subsystems Integration, 3rd ed., Aerospace Series, vol. 52, John Wiley & Sons Incorporated, New York, USA, 2011.
[94] R. Langton, Aircraft Fuel Systems, 1st ed., Aerospace Series, vol. 24, John Wiley & Sons Incorporated, Hoboken, 2009.
[95] C.D. Rodriguez, Architecture-based fuel system conceptual design tool for hybrid-electric aircraft, in: AIAA Aviation 2021 FORUM, Virtual Conference, 2021.
[96] C.D. Rodriguez, An architecture-based weight estimation method for aircraft fuel systems, Master Thesis, Concordia University, Montreal, Québec, Canada, 2022.
[97] J. Holt, S. Perry, SysML for Systems Engineering, Professional Applications of Computing Series, vol. 7, Institution of Engineering and Technology, Stevenage, 2008.
[98] J.-L. Voirin, Model-Based System and Architecture Engineering with the Arcadia Method, Elsevier, 2018.
[99] A. Elbayoumi, T. Tahvonen, Novel methodology for functional design chain analysis of a nuclear power plant: a new built Finnish power plant case study, Nucl. Eng. Des. 393 (2022) 111795.
[100] J. Hooman, K. Kanters, A. Vasenev, J. Verriet, MBSE-based design space exploration for productivity improvement using workflow models, in: D. Verma, A.M. Madni, S. Hoffenson, L. Xiao (Eds.), 2023 Conference on System Engineering Research, Hoboken, New Jersey, USA, 2024, pp. 35–46.
[101] The MathWorks, Creating the Matlab logo [Online]. Available at https://de.mathworks.com/help/matlab/visualize/creating-the-matlab-logo.html, 2023.
[102] NetworkX: network analysis in python [Online]. Available at https://networkx.org/.
[103] AltaRica Association, Tools: altarica wizard [Online]. Available at https://www.altarica-association.org/Products/products.html.
[104] The MathWorks, System composer: design, analyze, and simulate system and software architectures: R2024b [Online]. Available at https://de.mathworks.com/help/systemcomposer/, 2024.
[105] The MathWorks, Digraph: graph with directed edges: R2024b [Online]. Available at https://de.mathworks.com/help/matlab/ref/digraph.html, 2024.
[106] E. Clement, Arbre anlyst: Capitaliser et standardiser les modélisations par arbres de défaillances!, [Online]. Available at https://www.arbre-analyste.fr/en.html, 2023.
[107] D. Mahar, W. Fields, J. Reade, Nonelectronic Parts Reliability Data: NPRD, Reliability Databook Series, Quanterion Solutions Incorporated, Utica, USA, 2016.
[108] OREDA, Offshore Reliability Data Handbook, 4th ed., OREDA, Hovik, 2002, distributed by Det Norske Veritas.
[109] A. Vahl, Interaktive Zuverlässigkeitsanalyse von Flugzeug-Systemarchitekturen, Dissertation, Technische Universität Hamburg-Harburg, Hamburg, Germany, 1998.
[110] D. Rehage, Zustandsmodellierung und Zuverlässigkeitsanalyse fehlertoleranter Systemarchitekturen auf Basis Integrierter Modularer Avionik, Dissertation, Technische Universität Hamburg-Harburg, Aachen, Germany, 2009.