SAFETY ANALYSIS (CCA) OF THE AIR SUPPLY SYSTEM OF A FUEL CELL-POWERED AERO ENGINE FOR ELECTRIC REGIONAL AIRCRAFT

Stefan Kazula

German Aerospace Center (DLR), Institute of Electrified Aero Engines, Cottbus, Germany

Abstract

By means of a Common Cause Analysis (CCA), potential safety challenges of the air supply system for polymer electrolyte membrane fuel cell systems (PEMFCSs) as the primary energy provider in electric aero engines are identified and mitigated. The design of an exemplary hydrogen-fuelled PEMFCS-powered aero engine is described, focusing on the air supply system. The safety assessment method CCA, consisting of a Zonal Safety Analysis (ZSA), a Particular Risk Analysis (PRA) and a Common Mode Analysis (CMA), is described and conducted on the PEMFCS aero engine's air supply system. Failure modes and external events, which can have safety effects are identified, and potential design adaptations for mitigation are presented.

Keywords: Hydrogen Aircraft, Common Cause Analysis, Safe and Sustainable Aviation

1. Introduction

It is crucial that the aviation industry contributes towards mitigating the impact of climate change by reducing its CO_2 emissions. The European commission's "Flightpath 2050" [1] and the aviation industry's "Waypoint 2050" [2] have established emission reduction goals that necessitate a shift towards electrified aero engines and sustainable energy sources. A wide variety of electrified powertrain topologies have been identified [3] to meet diverse requirements in terms of passenger capacity and flight range, some of which involve hydrogen fuel cell systems (FCS). The FCSs are intended to provide electrical power for electrically driven propulsors. However, several challenges regarding air, fuel, water, and thermal management need to be addressed to comply with the strict reliability, safety and weight requirements in aviation. Consequently, FCSs have not yet been used in commercial aircraft.

This paper examines PEMFCSs as the primary energy provider for electrified aircraft propulsion, focusing on the air supply system. It identifies potential safety challenges and suggests potential solutions. A preliminary example of a design of a hydrogen-fuelled low-temperature PEMFCS-powered aero engine is described, emphasising its air supply system. The process, advantages and limitations of the CCA as an essential part of the safety assessment process in aviation according to Aerospace Recommended Practices ARP4754A [4] is presented. The CCA includes:

- the ZSA, which determines hazards resulting from failure modes of adjacent systems, as well as maintenance and installation errors,
- the PRA, which identifies external events, and
- the CMA, which verifies the independence of functions.

Subsequently, a CCA is conducted on the air supply system of an exemplary PEMFCS-powered aero engine in accordance to ARP4761 [5]. The CCA highlights the design challenges that emerge when utilising PEMFCSs as the main energy source for electric propulsion and enables design adjustments to address functional independence, foreign object damage mitigation, and optimised heat transfer.

2. Electrified Aircraft Propulsion

The topologies of electrified powertrains can be categorised as turbo-electric, all-electric and hybrid-electric architectures [6]. Turbo-electric architectures use generators driven by gas turbines to supply electrical energy to electric motors, which drive the propulsors. All-electric architectures rely solely on galvanic cells, such as batteries and FCSs, to power propulsors. In this context, PEMFCS are the preferred choice due to their high power density and advanced technology readiness level (TRL) [7]. Hybrid-electric architectures combine internal combustion engines, e.g. gas turbines or piston engines with galvanic cells to provide energy to the propulsors. Thereby, the utilisation of synergies between FCSs and a potential gas turbine compressor or turbine is enabled. Additional thermal management systems like heat exchangers and cooling/heating systems are also necessary. The propulsion system can be partially integrated into the fuselage, wings, or traditional nacelles, as shown in Figure 1 left, with nacelle-integrated systems offering advantages concerning thermal management. This paper presents the CCA on the air supply system of the nacelle-integrated PEMFCS-powered aero engine described in earlier publications [8], [9], [10], shown in Figure 1 right. The sizing of the propulsion system components is based on a preliminary design that was conducted in the DLR-internal project PEMScale 1.5. The arrangement of the components and their proportions shall support an easier understanding of the air supply system concept and serve as an initial starting point for further more detailed analyses.

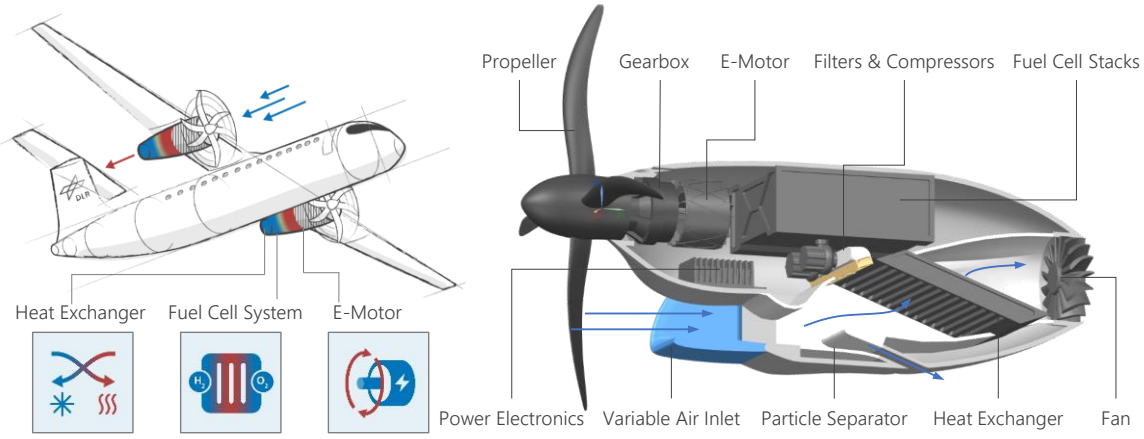

Figure 1 – Exemplary fuel cell-powered aircraft (left) and fuel cell-powered aero engine (right).

2.1 Fuel Cell-powered Propulsion System

The main energy provider of the propulsion system is the PEMFCS, which consists of the fuel cell stacks and Balance of Plant (BoP) components for optimal operation. The BoPs include air and fuel supply, water and thermal management systems as well as controls and sensors, as displayed in Figure 2 left. Fuel cell stacks consist of multiple fuel cells arranged together to achieve higher voltage output. The cells of PEMFCS convert the chemical energy of hydrogen by redox reactions with oxygen into electrical energy and water as a by-product. This conversion has an efficiency of 40-60%, the remaining energy being released as heat [7]. This excess heat must be managed using heat exchangers. The cells also require filters for fuel and air impurities, such as dirt and carbon monoxide. Furthermore, conditioning concerning pressure, temperature and humidity of the reactants is necessary to ensure a reliable operation with about 80° C. The PEMFCS can be assisted by a secondary energy storage like a buffer battery. All provided electrical energy is conditioned by the power electronics and supplied via electrical wires to the electric motors that drive the propulsors. The cooling systems of power electronics and electric motors also require respective heat exchangers.

The air supply system depicted in Figure 2 right provides the necessary air mass flow to fuel cell stacks as well as the heat exchangers of fuel cell system, power electronics and electric motor [9]. The air supply system collects air from the environment by a scoop inlet with variable entry area and removes potential foreign objects through an inertial particle separator [10]. Downstream the inlet

duct, the majority of the air flow is utilised in the respective heat exchangers. Depending on the operating conditions, an activatable fan assists in drawing the air through the heat exchangers. The remaining air flow is filtered, compressed and conditioned in terms of temperature and humidity to be supplied to the fuel cell stacks. Additionally, pressurised air for the cabin could be harvested here. Further secondary air inlets can become necessary for the ventilation of the nacelle. Ventilation may be required in certain zones of the aero engine to prevent the accumulation of flammable fluids such as hydrogen.

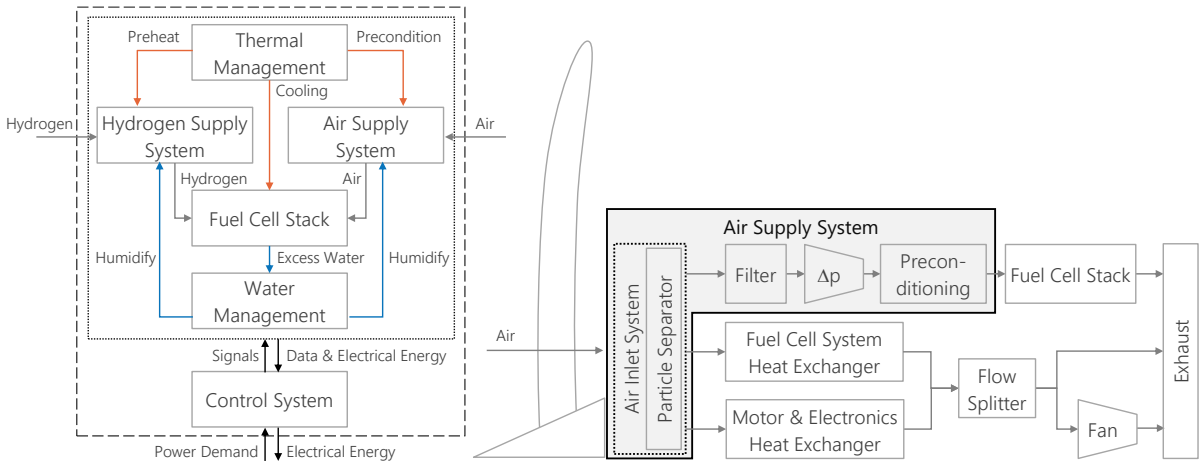

Figure 2 – Subsystems of a fuel cell system (left) and air supply system (right).

3. Safety Assessment Process in Aviation

In Europe, the European Union Aviation Safety Agency (EASA) establishes safety regulations for commercial aircraft through Certification Specifications (CS), such as CS-25 for large aeroplanes [11]. Compliance with these regulations must be demonstrated during the certification process for obtaining flight approval. To facilitate this, the EASA proposes acceptable means of compliance (AMC), which can include calculations, analyses and tests. Paragraph CS-25 AMC 25.1309 and ARP 4754A [4] describe the safe design process in aviation based on the V-model of systems engineering [12]. This process involves the development, validation and verification of requirements, functions and architectures at different levels of detail, ranging from aircraft to system to element level, as depicted in Figure 3.

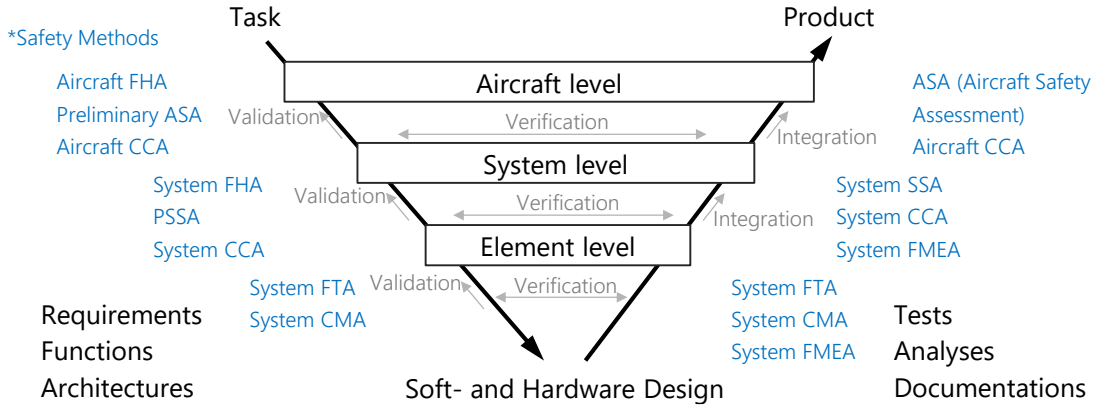

Figure 3 – V-model of systems engineering.

ARP 4761 describes the corresponding methods used in each development phase of this process [5]. During the preliminary design phase, the Functional Hazard Assessment (FHA) and the Preliminary System Safety Assessment (PSSA), conducted through a Fault Tree Analysis (FTA) are key methods. The application of these methods for FCSs along with potential design adaptations has been published previously [8]. Further important safety methods are the System Safety

Assessment (SSA), the Failure Mode and Effects Analysis (FMEA) and the Common Cause Analysis (CCA). The CCA is an iterative safety assessment method performed from early stages of the development process onward. It encompasses the ZSA, the PRA and the CMA, which are the focus of this study.

3.1 Particular Risk Analysis

The ARP 4761 [5] characterises particular risks as events that occur outside of the immediate system boundaries, but can impact the requirement that no single failure event can lead to hazardous conditions. These events can affect also several zones simultaneously. Typical events are fire, high pressure air duct rupture, leakage of fuel, hydraulic oil, water and hot air, aerodynamic friction, friction between moving parts, hail, ice, snow, water ingestion, icing of operating equipment, high ambient temperatures, bird strike, lightning strike, electromagnetic interference (EMI), high intensity radiated fields (HIRF) and bulkhead rupture [5], [13]. Some of these events, e.g. leaking fluids, may also be identified in a ZSA.

The goal of the PRA is to identify all particular risks concerning a design. Once these risks have been identified, each risk is examined separately through a primarily qualitative analysis. This way, each safety-related effect can be excluded or shown to be acceptable based on its probability of occurrence. The steps required to perform a PRA are summarised in Figure 4.

The PRA should be performed throughout the development process of a new aircraft and whenever a major modification is made to the aircraft [5]. In the initial stages of the design process, a PRA can reduce development costs by identifying weaknesses in the design. As the development process progresses, the design becomes more detailed. While potentially remaining weaknesses can be identified easier at this stage, their mitigation can only be achieved through more cost-intensive design changes, complex simulations or tests. On the one hand, a PRA requires a lot of experience to identify all potential events and their effects, as well as high effort and cost to perform all necessary analyses and tests. On the other hand, this method enables the assessment of the impact of unrelated systems on each other by crossing system boundaries, allowing the simultaneous investigation of several zones and facilitating the identification of vulnerabilities to external interferences [13].

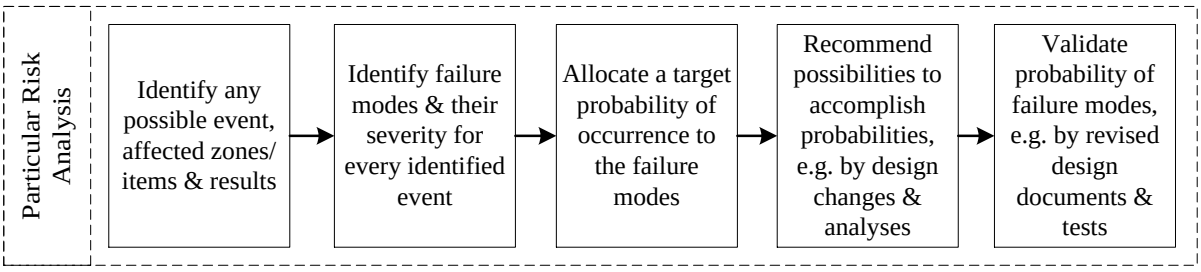

Figure 4 – Summarised process steps of the Particular Risk Analysis.

3.2 Zonal Safety Analysis

The purpose of the ZSA is to provide guidelines for design and installation, to identify interferences between systems installed in the vicinity, as well as to detect maintenance and installation errors [11]. This way, it can be ensured that failures are independent of other systems or, if this is not possible, can be accepted with a certain probability of occurrence. A ZSA is a primarily qualitative analysis performed for each zone of the aircraft and should be carried out throughout the development process [5]. Early in the development process, the ZSA is used to establish design and installation guidelines and to examine preliminary drawings or models. In later phases, the ZSA is based on more detailed design information, e.g. mock-ups and actual components. The summarised process of the ZSA is illustrated in Figure 5.

At the beginning of the ZSA, the preparation of design and installation guidelines should consider aircraft level requirements, the results from previous safety assessments, as well as available maintenance and operational data from previous designs. These guidelines may be divided into

general, system-specific or zone-specific. General guidelines for design and installation may include equipment installation (e.g. including pipes, ducts, wires, cables), maintenance and servicing, as well as drainage guidelines [5]. Additionally, zones of the aircraft have to be defined, e.g. according to the Joint Aircraft System/Component (JASC) or the Air Transport Association of America (ATA) code tables. A list of systems and items should be prepared for each zone of the aircraft. Furthermore, failure modes that could have a safety effect on external systems or items installed in close proximity should be listed. Subsequently, each aircraft zone is checked against the design and installation guidelines. Any deviation of the design from these guidelines should be considered for a design modification. The effects of the identified failure modes on external systems, items and eventually the aircraft should be investigated, mitigated and if necessary validated [5].

The ZSA is best carried out, when all items and systems can be examined [13]. As this is usually only the case in later development phases, the necessary design changes are likely to be cost-intensive. Besides, this method requires a lot of experience with the system under investigation to be performed successfully [13]. Nevertheless, the ZSA is an invaluable safety analysis method that can be used in system integration. With the help of the ZSA, complex interactions between systems can be considered. In addition, potential safety-relevant events from adjacent systems can be identified, e.g. heating pipes near sensitive electronic equipment, hot air leaks and electromagnetic interference effects [13].

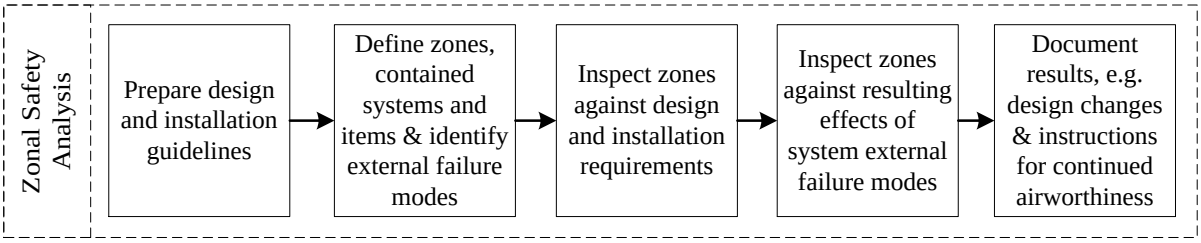

Figure 5 – Summarised process steps of the Zonal Safety Analysis.

3.3 Common Mode Analysis

The CMA is a method that contributes to a safe design throughout the design process. It is a qualitative method for verifying independence of functions and thus events and failure modes. Independence can be achieved by utilising fail-safe or independence principles [14], the most commonly used principle being redundancy, i.e. the mechanically and electrically segregated duplication of systems or components. However, there are various threats to the independence of redundant systems and unintended dependency can result in even higher failure rates than for individual elements [14]. Hence, the effects of design, manufacturing and maintenance errors, and failures of system components must be considered [5]. For example, generic faults of a specific hard- or software can lead to malfunctions in multiple systems that use this specific hard- or software [5]. The CMA should be carried out throughout the safety assessment process, while being performed best at later stages. This way, inputs from the Functional Hazard Assessment (FHA) and the Preliminary System Safety Assessment (PSSA) can be used to identify issues concerning independency [5]. The steps required to conduct a CMA are illustrated in Figure 6.

First, a checklist of specific common mode types, sources and failures should be established. Examples for common modes that should be investigated include requirement errors, software or hardware development errors, installation errors, hardware failures, production or repair flaws, stress related events, environmental factors such as temperature, vibration and humidity, cascading faults, as well as common external source faults [5]. Furthermore, requirements for probabilities of occurrence of common modes have to be determined, e.g. by deriving them from an FTA. Then, the common mode checklist is utilised to analyse the design for compliance with the common mode requirements, e.g. independence of functions. Finally, required design adjustments should be carried out and documented.

Performing a CMA systematically and rigorously can be difficult, as it requires detailed knowledge of the investigated systems and relies on the assumption that unlikely events will occur [13]. While the

use of a CMA cannot guarantee that all common failure modes can be identified and thus mitigated, it provides a good approach to identify common development errors. It also establishes functional requirements for the separation and isolation of systems [13]. Finally, a CMA supports the verification of independence of events, supports the selection of a suitable system architecture.

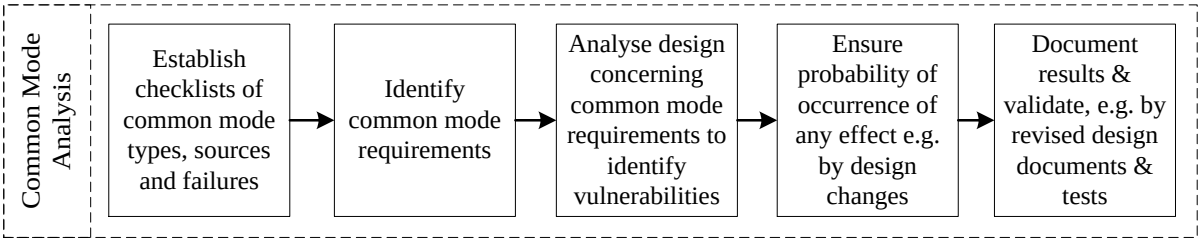

Figure 6 – Summarised process steps of the Common Mode Analysis.

4. Selected Results from the Common Cause Analysis

4.1 Particular Risk Analysis

While many events, e.g. hail impact, have a similar influence on the air supply system of a PEMFCS-powered aero engine like on a conventional turboprop engine, there are still huge differences. These arise due to the requirements of the fuel cell for filtered, humidified and conditioned air. For the investigated air supply system concept with a variable inlet lip, the most critical events with a direct influence on the system are bird strike, icing, lightning, electromagnetic interference (EMI), e.g. with the adjustment system, and friction between moving parts. These events, the severity of the particular consequences and the derived probability of occurrence requirements are presented in Table 1. This table lists merely an excerpt from the PRA, showing events to be observed during take-off, as this is a very safety-critical flight phase.

Table 1 – Excerpt from the Particular Risk Analysis (PRA) for the air supply system.

Risk	Event	Consequences	Failure mode severity	Probability requirement [Events/ flight hour]
Icing	Large ice accumulation on inlet of all engines	Potential spalling ice can affect the inlet flow, damage downstream components and potentially cause loss of thrust on all engines.	Hazardous effect during take-off	< 1.0E-07
Bird strike	Large bird strike on inlet of a single engine	Impact can cause loss of inlet parts. This can affect the air flow, damage downstream components and potentially cause loss of thrust on a single engine.	Minor effect during take-off	< 1.0E-03
Bird strike	Large bird strike on inlet of all engines	Impact can cause loss of inlet parts. This can affect the air flow, damage downstream components and potentially cause loss of thrust on all engines.	Hazardous effect during take-off	< 1.0E-07
Lightning strike	Direct strike and indirect effects on a single engine.	Damage to actuators, sensors or seals due to temperature peaks can lead to a loss of inlet adjustment capability, affect the air flow and potentially cause loss of thrust on a single engine.	Minor effect during take-off	< 1.0E-03
Friction between moving parts	Friction between inlet segments	Movable inlet parts getting caught on each other can lead to a loss of inlet adjustment capability and potentially cause loss of thrust on a single engine.	Minor effect during take-off	< 1.0E-03
Electromagnetic interference	Interference with inlet control	Interfering magnetic fields can lead to a loss of inlet adjustment capability, affect the air flow and potentially cause loss of thrust on a single engine.	Minor effect during take-off	< 1.0E-03

Severe Icing has a probability of 10-2 per flight and normal icing can potentially occur during every flight [11], [13]. Hence, inlet anti-icing systems are usually integrated in modern aircraft, mostly covering the area around the inlet lip. Depending on the selected anti-icing system type further particular risks can be identified. If an electric anti-icing system is preferred, lightning strike and high intensity radiated fields should be inspected more closely. Also waste heat from the fuel cells could

be synergistically used. However, when using hot air anti-icing systems, high pressure and high temperature air duct leakage should be further examined [5].

Bird strikes are a widely recognised risk in aviation, with and 37% of incidents impacting the engine or its inlet [15]. For certification of an aircraft compliance with CS 25.631 must be demonstrated by analyses and tests. In CS 25.631 bird strikes are treaded as ultimate loads that permit deformation but not fracture of components [11]. Consequently, material strengths or thicknesses must be adequate, leading to increased weight and reduced design space.

In the European Union, aircraft experience lightning strikes with a frequency of up to 1 strike every 2400 flight hours [13]. To mitigate the negative effects of these strikes, it is crucial to employ temperature resistant materials and lightning protection measures, such as the integration of bonding straps in the inlet cowl to create a Faraday cage. Additionally, electric components, like electric motors, must be grounded.

To minimise the friction between movable inlet parts the application of coatings or lubrication can be beneficial.

However, there are further events that can affect the membrane electrode assembly of fuel cell stacks or the heat exchangers downstream of the air supply system. Particle separators are necessary to protect these components and to mitigate the effects of events like the impact of foreign objects, sand and bird strikes. In the case of the fuel cell stacks filters must also be integrated to reduce the influence of smoke, sand, dust, salt fog and organic impurities on the cells. As heat exchangers in low-temperature PEMFCS-powered aero engines require significantly higher air mass flows than fuel cell stacks, filters are unfeasible. Hence, organic substances like fungi, salt fog, sand and dust can result in fouling of the heat exchangers. Fouling refers to the accumulation of undesired deposits on heat transfer surfaces, leading to various issues such as reduced heat transfer efficiency, increased flow resistance, and pressure drops.

4.2 Zonal Safety Analysis

The purpose of the ZSA is to provide guidelines for design and installation, to identify interferences Due to extensive nature of the subject, this study presents exemplary design and installation guidelines. General design guidelines for equipment installation, such as pipes, ducts, hoses, wires and cables, include requirements for minimising stresses, obstruction and fluid accumulation for both, static and moving parts [5]. In areas or components where fluid accumulation can lead to fires, corrosion or rot, drainage should be implemented. Furthermore, redundant systems should be segregated and isolated to prevent events and failures affecting both systems [5]. Vulnerable components should have a minimum clearance from potential hydrogen leakage zones. Areas prone to accumulating dust, dirt or other contamination require a forced air ventilation to prevent the build-up of such substances on surfaces.

While it is possible to define the entire aero engine as a single zone, this study focusses on the air supply system as a distinct zone. The necessary subsystems within the air supply system zone include:

- an adjustable scoop inlet with electric adjustment system and electric anti-icing system,
- an inertial particle separator,
- the air ducts,
- an air filter for the fuel cell stacks,
- a two-staged radial compressor for the fuel cell stacks,
- a preconditioning system for the fuel cell stacks, including valves, sensors, a humidifier and a precooler/preheater, as depicted in Figure 2.

Each of these subsystems comprises additional components, such as ducts, tube, valves, controllers, sensors, seals and wires. The air supply system zone interfaces functionally with the fuel cell stacks, cabin air offtakes and the heat exchangers of fuel cell system, electric motors and power electronics.

Table 2 lists exemplary results from the inspection of the air supply system zone against the design guidelines and potential system interferences. It also considers the resulting effects on the aircraft

and proposes design precautions to address, prevent or mitigate these issues. In later design phases particular attention should be given to the risk of fire and explosions due to undetected hydrogen leakage.

Secondary functions of the FCS can introduce additional safety-critical events. This applies for functions, such as provide ice protection, provide cabin air, provide electrical energy to onboard electronics or generate reverse thrust. For example, the loss of ice protection capability can result in wing and empennage icing, posing a risk of "loss of aircraft control" [8].

Table 2 – Excerpt from the Zonal Safety Analysis (ZSA) for the air supply system.

Component(s) in zone	Potential issue(s) of concern/ failure mode(s)	Effect(s) on the aircraft	Means of correction, prevention or mitigation
Adjustable scoop inlet with electric adjustment system and electric anti-icing system	Accumulations of ice, dust and dirt between movable inlet segments can cause a loss of inlet adjustment capability and decrease the air mass flow	Overheating due to decreased air mass flow and spalling ice can both damage downstream components and potentially cause loss of thrust on all engines.	Integration of an anti-icing system, dirt-repellent coatings, ventilation and minimisation of gaps, cleaning during maintenance
All components, especially air ducts and filters	Accumulation of water, chemicals and organic substances, can cause rot and corrosion and loss of function	Depending on the component a loss of function can potentially cause loss of thrust on a single engine	Integration of drainage, grounding of electric components and waterproof component casings, e.g. IP55 (International Protection Code)
Inertial particle separator	Insufficient separation of foreign objects, sand and birds can cause damage to downstream components such as heat exchangers, filters and compressors	Depending on the damaged component a loss of function can lead to overheating and potentially fire, decreased pressure and performance up to loss of thrust on a single engine	Integration of an inlet grid, redundant downstream systems, secondary energy storage, integration of fire walls, fire detection, fire extinguishing system and heat protection, e.g. bulkheads
Air filter for the fuel cell stacks	Accumulation of dirt can cause blockage or structural damage leading to fuel cell damage	Decreased pressure and performance up to loss of thrust on a single engine	Regular maintenance, active filter regeneration, redundant energy storage
Compressor for the fuel cell stacks and connected ducts	Leakage of any fluid, e.g. hot air and hydrogen, in proximity to electrical equipment can cause damage to components or fire	Decreased cabin pressure and decreased fuel cell performance up to loss of thrust, an uncontrolled fire can result in hazardous effects	Secondary energy storage, ventilation, drainage, potentially integration of fire walls, fire detection, fire extinguishing system and heat protection, e.g. bulkheads
Preconditioning system for the fuel cell stacks, including valves, sensors, a humidifier and a precooler/preheater	Electromagnetic interference (EMI) can cause control malfunctions, leading to fuel cell membrane damage	Decreased fuel cell performance up to loss of thrust, direct contact of hydrogen and air can lead to an uncontrolled fire that can have hazardous effects	Secondary energy storage, EMI shielding, filtering, grounding and bonding, cable routing, EMI filters, coatings, ventilation, hydrogen supply emergency cut off

4.3 Common Mode Analysis

The first step of the CMA is to prepare a checklist that identifies common mode types, sources and failures, as presented in Table 3. It is advisable to undertake this step from the early stages of the design process to prevent the need for costly implementation of safety design features in later design phases. This checklist serves as a tool to identify common mode requirements. Among the most critical failures of the air supply system are those that cause fire or loss of thrust on all engines.

Table 3 – Excerpt from the Checklist of Common Mode Types, Sources and Failures/Errors.

Common mode types	Common mode subtypes	Example of common mode sources	Example of common mode failures/errors
Concept and design	System architecture	Equipment protections	Failure due to missing prediction of an event by designers
Concept and design	System architecture	Common software	Software error
Concept and design	Technology	New/sensible technology	General design error due to insufficient experience
Manufacturing	Manufacturer	Common manufacturer	Common error due to manufacturer, e.g. due to inadequately trained staff

Environmental	Mechanical and thermal	Unsuitable temperature, dust, dirt, vibration, humidity, pressure, stresses	Structural failure or overheating
Environmental	Electromagnetic fields	High amounts of electric energy	Malfunction of controls due to electromagnetic interference
Environmental	Chemical	Corrosion (e.g. embrittlement, oxidation)	Moisture or hydrogen around components

One CMA requirement derived from a similar study [16] is that the air supply systems of engines on the left and on the right side of the fuselage must be independent. This requirement, among others, has been reviewed and addressed in the CMA process to mitigate potential risks, as shown Table 4.

Table 4 – Excerpt from the Common Mode Analysis (CMA) for the air supply system.

Requirement: air supply systems of engines on the left and on the right side of the fuselage must be independent		
Common mode subtype	**Common mode error**	**Means of correction, prevention or mitigation**
System architecture	Local event affecting electrical routes	Use independent electrical routes and connectors (mechanical and electrical segregation of separate sides)
Technology	Development Error	If achievable, utilise conventional technology, perform tests to assure correct operation
Manufacturer	Faulty manufacture affecting similar equipment on both sides	Different manufacturers for each side, certification of manufacturing process and its quality, incoming goods inspection
Environmental factors	Large bird strike on both sides	Secondary energy storage; fall back inlet geometry when losing adjustment capability

In order to prevent common mode vulnerabilities, it is crucial to incorporate fail-safe design principles, such as redundancy, segregation and isolation, right from the beginning of the development process, as emphasised by Kritzinger [14]. By adhering to these safe design principles, potential risks and vulnerabilities can be effectively mitigated, ensuring the overall safety and reliability of the system.

5. Conclusions

The applicability of PEMFCSs as the primary energy source for electric aircraft propulsion was examined, focusing on the air supply system. During this investigation, potential safety challenges were identified, and corresponding solutions were proposed. A comprehensive CCA was conducted on the air supply system of an exemplary PEMFCS-powered aero engine in accordance to ARP4761, including a ZSA, a PRA and a CMA. The CCA shed light on the design challenges that arise when integrating PEMFCSs into electric propulsion systems, and it facilitated necessary design adjustments to ensure functional independence, mitigate foreign object damage, and optimise heat transfer. The identified risks from the PRA were mitigated through design precautions such as inclusion of filters and particle separators. The ZSA outputs led to the implementation of EMI protection and fire treatment measures. Additionally, the CMA mitigated dependence risks by incorporating fail-safe design principles, including redundancy. To prevent hazardous events due to loss of thrust caused by a malfunction of the FCS, integration of multiple independent FCSs or sufficiently large buffer batteries is necessary. It is crucial to achieve independence among the FCSs of different aero engines for all essential subfunctions, including fuel storage.

Although challenges remain in the design of PEMFCSs for aviation, such as increasing power density, addressing limited operating conditions, managing high electric energy and heat production, and utilizing hydrogen as fuel, this study demonstrates that conducting a CCA on the air supply system of a PEMFCS-powered aero engine enables the identification of means to improve safety and reliability.

In later design phases, the conducted analyses should be complemented by the bottom up method FMEA and further iterations of the CCA and FTA. This approach would help to identify additional potential failure modes and develop design solutions to mitigate their effects. In this way, the application of PEMFCSs in commercial aviation can be enabled and become a way to achieve the ambitious ecological, safety and economic goals for future sustainable aviation.

6. Copyright Issues

The copyright statement is included in the template and must appear in your final pdf document in the position, style and font size shown below. If you do not include this in your paper, ICAS is not allowed and will not publish it.

7. Contact Author Email Address

mailto: Stefan.Kazula@dlr.de

8. Copyright Statement

9. References

1. European Commission. Flightpath 2050: Europe's vision for aviation. Luxembourg: Publ. Off. of the Europ. Union; 2011.
2. ATAG. Waypoint 2050. Switzerland: Air Transport Action Group; 2021.
3. Jansen R, Bowman C, Jankovsky A, Dyson R, Felder J. Overview of NASA Electrified Aircraft Propulsion (EAP) Research for Large Subsonic Transports. In: 53rd AIAA/SAE/ASEE Joint Propulsion Conference; Atlanta, GA. Reston, Virginia: American Institute of Aeronautics and Astronautics; 2017. doi:10.2514/6.2017-4701.
4. SAE Aerospace. ARP4754A. Guidelines for Development of Civil Aircraft and Systems. Warrendale, PA, United States: SAE International; 2010.
5. SAE Aerospace. ARP4761. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. Warrendale, PA, United States: SAE International; 1996.
6. Sahoo S, Zhao X, Kyprianidis K. A Review of Concepts, Benefits, and Challenges for Future Electrical Propulsion-Based Aircraft. Aerospace. 2020;7:44. doi:10.3390/aerospace7040044.
7. Kazula S, de Graaf S, Enghardt L. Review of fuel cell technologies and evaluation of their potential and challenges for electrified propulsion systems in commercial aviation. J. Glob. Power Propuls. Soc. 2023;7:43–57. doi:10.33737/jgpps/158036.
8. Kazula S, de Graaf S, Enghardt L. Preliminary Safety Assessment of PEM Fuel Cell Systems for Electrified Propulsion Systems in Commercial Aviation. Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022) 2022. doi:10.3850/978-981-18-5183-4_S16-02-019-cd.
9. Sain CK, Hänsel J, Kazula S. Conceptual Design of Air and Thermal Management in a Nacelle-Integrated Fuel Cell System for an Electric Regional Aircraft. In: AIAA AVIATION 2023 Forum; San Diego, CA and Online. Reston ,VA: AIAA; 2023. doi:10.2514/6.2023-3875.
10. Hintermayr D, Kazula S. Design and Analysis of the Air Inlet System for Fuel Cell Powered Electric Propulsion Systems in Regional Aircraft. Proceedings of DLRK 2023. 2023.
11. European Union Aviation Safety Agency. Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes (CS-25): Amendment 28; 2023.
12. Kazula S. Variable Pitot-Triebwerkseinlässe für kommerzielle Überschallflugzeuge. Wiesbaden: Springer Fachmedien Wiesbaden; 2022.
13. Kritzinger D. Aircraft system safety: Assessments for initial airworthiness certification. Duxford: Woodhead Publishing; 2016.
14. Kritzinger D. Aircraft system safety: Military and civil aeronautical applications. Cambridge: Woodhead Publishing Limited; 2006.
15. Hedayati R, Sadighi M. Bird strike: An experimental, theoretical and numerical investigation. Cambridge: Woodhead Publishing; 2016.
16. Kazula S, Grasselt D, Mischke M, Höschler K. Preliminary safety assessment of circular variable nacelle inlet concepts for aero engines in civil aviation. In: Haugen S, Barros A, van Gulijk C, Kongsvik T, Vinnem JE, editors. Safety and reliability - safe societies in a changing world: Proceedings of the 28th International European Safety and Reliability Conference (ESREL 2018), Trondheim, Norway, 17-21 June 2018. Boca Raton, London, New York, Leiden: CRC Press, Taylor et Francis Group; 2018. p. 2459–2467. doi:10.1201/9781351174664-309.