Politecnico di Torino

Corso di Laurea Magistrale in Ingegneria Aerospaziale

A.a. 2023/2024

System-level modelling and safety assessment of a liquid hydrogen fuel cell regional aircraft

Supervisors

Dr. Davide Ferretto

Dr. Roberta Fusaro

Dr. Ricardo Reis

Candidate

Anna Liverani

Acknowledgements

I would like to express my sincere gratitude to the people who contributed to the development of the thesis.

I thank my professors Davide Ferretto and Roberta Fusaro for their kind support and trust.

A special thanks goes to Ricardo Jose Nunes dos Reis for his constant presence and kind words that guided me throughout the work.

I also would like to thank Rafael Maia Altafim, Vinicius Santini Lobo and Ricardo Gandolfi for their cooperation and availability to contribute to the project with their expertise.

Working with the entire team has been a great opportunity I am deeply grateful for.

Abstract

Hydrogen is increasingly making its way into the aviation industry as an opportunity to reduce emissions. Liquid hydrogen fuel cell aircrafts represent a promising technology to pursue the path toward decarbonization. Hydrogen holds great potential as a means of generating electrical energy and powering air transportation; however, it also poses significant challenges to overcome and stringent requirements to be met to reduce associated risks. Safety concerns are indeed a crucial aspect that greatly influences architectural choices. The thesis aims to analyse the safety aspects of a liquid hydrogen PEM fuel cell regional aircraft with a Model-Based System Engineering (MBSE) approach. A reference aircraft is taken into consideration to execute a safety assessment process, identifying potential failure conditions that could compromise flight safety. A functional model of the system architecture is developed with the tool Capella, based on the Arcadia MBSE methodology. The model does not focus on detailing the physics of the components to optimize the design but rather acknowledges their roles within the architecture, their requirements and their constraints. A Functional Hazard Assessment (FHA) is conducted on the system of interest, which includes the Energy generation system, the dedicated Thermal management system and the Energy storage system. The analysis provides an overview of possible failures of all the functions of the system, classifies their severity, and offers a deeper understanding of the requirements of the system, which can be integrated into future design phases.

Index

List of figures

List of tables

1. Introduction

1.1 Background and literature study

Nowadays, the environmental challenge has emerged as one the foremost concerns in technological advancements across various sectors, including aviation. Air transport is a notable source of carbon footprint, and a substantial reduction of the emissions by 2050 can only be accomplished by a combination of different measures and innovative technologies (1). The research is looking into different types of fuel to overcome fossil fuels and propulsive architectures based on electrical sources.

In this scenario, hydrogen has emerged as a valuable solution to contribute to the stated objectives as it represents a zero-emission energy source (2). Hence, new and diverse technologies are being studied to introduce hydrogen into aircraft architectures, both for direct combustion to generate thrust or used into fuel cell systems to produce electricity for an electric motor powertrain (3).

Although hydrogen is an attractive alternative to kerosene, it involves several problems to solve regarding its production, transport and storage. Hydrogen is not a primary energy source, but it needs to be produced by different processes that require an elevated electricity demand. Hydrogen can be considered *green* only when obtained from a renewable or carbon-free energy sources, but the related costs are not yet competitive to overcome the production from fossil fuels (4).

Furthermore, hydrogen molecule is very small and able to permeate into material causing embrittlement. It is odourless and colourless, hence very difficult to detect in case of leaks leading to critical safety concerns due to its flammable condition.

Regarding storage, hydrogen exhibits a density that is four times lower than that of kerosene, necessitating significantly larger storage solutions, which may not be practical for aircraft applications. To mitigate this issue, compressed or liquefied hydrogen storage is essential to reduce tank volume; however, these methods introduce more complex architectures and stringent requirements. In aviation, the preferred form of hydrogen is liquid, which exists in a cryogenic state at approximately 250 K, demanding rigorous specifications concerning materials, thermal management, and safety measures.

At present days, several projects have been developed and various demonstrator aircrafts have flown to test fuel cell propulsion systems, which is the technology the thesis is going to focus on. The first manned prototype was the Boeing Fuel Cell Demonstrator. It first flew in 2008 powered by a compressed hydrogen PEM fuel cell system. An additional battery was required to perform take-off

and climb. The following year the Antares DLR-H2 flew with a fuel cell system without the need of the battery. Moreover, the European project ENFICA-FC (Environmentally Friendly Inter-City Aircraft Powered by Fuel Cells) worked on the retrofit of the Rapid 200 aircraft to develop a compressed hydrogen fuel cell prototype (5). Although, the demonstrator are small-class airplanes, conceptual commercial aircraft projects are being studied with the aim of introducing this technology into air transport. Airbus aims to realize an hydrogen-powered commercial aircraft by 2035 with its ZEROe project. Different concepts are being explored, considering both hydrogen combustion and hydrogen fuel cells. This goal is shared by Embraer company, which is working on the Energia project: different conceptual aircraft able to transport up to 50 passengers, including hybrid electric, H2 fuel cell and H2 gas turbine propulsion system.

1.2 Motivation and goal of the thesis

The technological development of more efficient and carbon free architectures cannot be separated from the safety requirements that a given design entails. Safety is one of the most important aspects to consider, as without its verification, the project lacks a reason to exist. Every single element of the system has specific functions, limits and connections and its own requirements to be achieved to function properly.

During the design phase, it is mandatory to consider aspects related to safety and analyse the chain of events that occur when a particular failure happens. The project must ensure that each failure does not lead to catastrophic consequences but that there are enough redundancies and elements to fulfil the missing function and safely return to the ground to finish the mission.

The present thesis aims to contribute to the technology research and development effort of H2 fuel cell commercial aircraft by analysing safety aspects and identifying failure conditions of the Electric power system of a liquid hydrogen fuel cells aircraft with Model-Based System Engineering approach. The goal is to create a functional architecture of the system to be submitted to the safety analysis to inform research and design decisions, guiding the development of H2 fuel cell aircraft. A deep understanding of the functions of every element is required to develop the analysis of the connections among all the subsystems.

The subject of the study is a PEM fuel cells regional aircraft powered by liquid hydrogen. The reference architecture is going to be defined by analysing existing projects from literature, as the focus is not the specific architecture itself, but the functional analysis that derives from the model.

The objective is to build a model and meticulously analyse its safety, aiming to offer valuable support to the design process for analogous or similar architectures to the one under consideration. This analysis seeks to integrate into the design phase for the successful execution of every aviation mission, facilitating the examination of aspects beyond mere project performance.

The project examines the safety boundaries of the architecture and seeks to understand if useful design recommendations could be derived from such type of investigation.

The work is carried on by two main research questions:

- What major recommendations can be generated, regarding the development of H2 fuel cell aircraft architectures, from conducting safety analysis on reference conceptual designs?
- Does conducting safety assessments of reference conceptual architectures of future propulsion systems provide a meaningful contribution to their technology research and development effort?

As stated, the utilization of hydrogen is a highly promising technology that could help in the environmental and climate crisis by reducing CO_2 emissions. Like all new technologies, it must be thoroughly analysed and studied to enable widespread use within the bounds of safety.

The thesis wants to deepen into the electrical propulsion architecture powered by hydrogen, look into potential solutions to contribute to the development of hydrogen technology into civil air transport. It is desired to understand the safety conditions of such architecture and its requirements focusing on functional aspects.

1.3 Organization of the thesis

The work starts with bibliographic research to better understand both the methodology to be used and the elements involved in the architecture, together with the safety issues related to them. Moreover, similar projects must be considered to serve as a reference for the architecture.

Subsequently, the system architecture is going to be defined following the Arcadia framework. Initially, a basic architecture model will be created. The role of every element of the system is going to be defined, along with the relations between them. The focus of the model is not detailing the physics of the components, but the roles they have in the architecture, their requirements, and constraints.

The system of interest (SOI) is going to be the subject of a Functional Hazard Assessment, to determine the effect on the aircraft of possible failures and understand the severity of the consequences of different outcomes. Finally, operational and design recommendations are derived from the analysis discussion.

1.4 Cooperation

The thesis project is developed under the supervision of Embraer company and its subsidiary Airholding. Embraer is a Brazilian aircraft manufacturer which is currently involved in sustainable projects to reach lower fuel emission, noise emission and fuel consumption. Different concepts of electric and hybrid-electric aircrafts are being explored to contribute to the environmental goal of reducing emissions within 2050 (6).

Although the present study is not directly connected to any of the company internal projects, several experts from the firm have been involved in the architecture development and their cooperation has been fundamental to validate the results of the analysis.

2. Methodology

Before the discussion of the analysis conducted in the project, it is important to outline the methodological approach adopted. The architecture is being developed using the Model-Based Systems Engineering (MBSE) approach, an engineering application that focuses on creating models to support system requirements, design, analysis, verification, and validation. MBSE is intended to replace the traditional document-based approach as a means of exchanging information, and it should not be considered as a universal tool. It requires a well-defined methodology to establish the objectives of the process and to delineate how these objectives will be achieved, as well as the use of a dedicated tool that enhances task efficiency (7). Regarding the exploration of the safety boundaries of the architecture, a safety assessment method was employed to identify potentially critical scenarios within a predetermined mission and environment. In specific, the Arcadia approach and Capella tool are used to conduct MBSE in the thesis.

2.1 MBSE approach: Arcadia methodology

Arcadia (*Architecture Analysis and Design Integrated Approach)* is a Model-Based System Engineering Methodology developed by Thales for the architectural design of systems, hardware and software (8). It provides a structured approach to developing and analysing the design of complex systems. Safety requirements can be identified with the functional assessment of the various functions composing the system model (9).

The methodology is structured into several engineering levels, each addressing different aspects of the system, from a high-level approach to physical one (10). The levels explored in the work are the following:

- **Operational analysis**

  The Operational analysis level focuses on “What the users of the system need to accomplish”. The object of the study is analysed trying to capture the needs of the stakeholders, the capabilities that have to be accomplished and the people, infrastructures or environment which are going to interact with the subject of interest.

- **System analysis**

  “What the system has to accomplish for the users” is the scope of this level analysis. The functions of every element of the system are defined to satisfy the needs determined at the operational level. The system of interest is presented, together with its interactions with all the other elements, which are called Actors.

- **Logical architecture**

  While the first two levels presented are meant to understand the needs of the systems, this level starts to work on its architectural design. It derives from the previous System analysis, trying to define "how the system will work to fulfil the expectations". The architecture of the system and the interaction between components are developed, but still considering only their logical role in the system, independently from the technological implementation (11).

- **Physical architecture**

  The physical architecture represents "how the system will be developed and built". Starting from the Logical architecture, a possible physical architecture of the system is proposed. Every function is associated with a physical component, hardware or software which is able to provide that function. For a single logical architecture, different physical solutions can be developed. At this level, it is possible to perform trade-off analysis between implementations and approaches on the architecture (8).

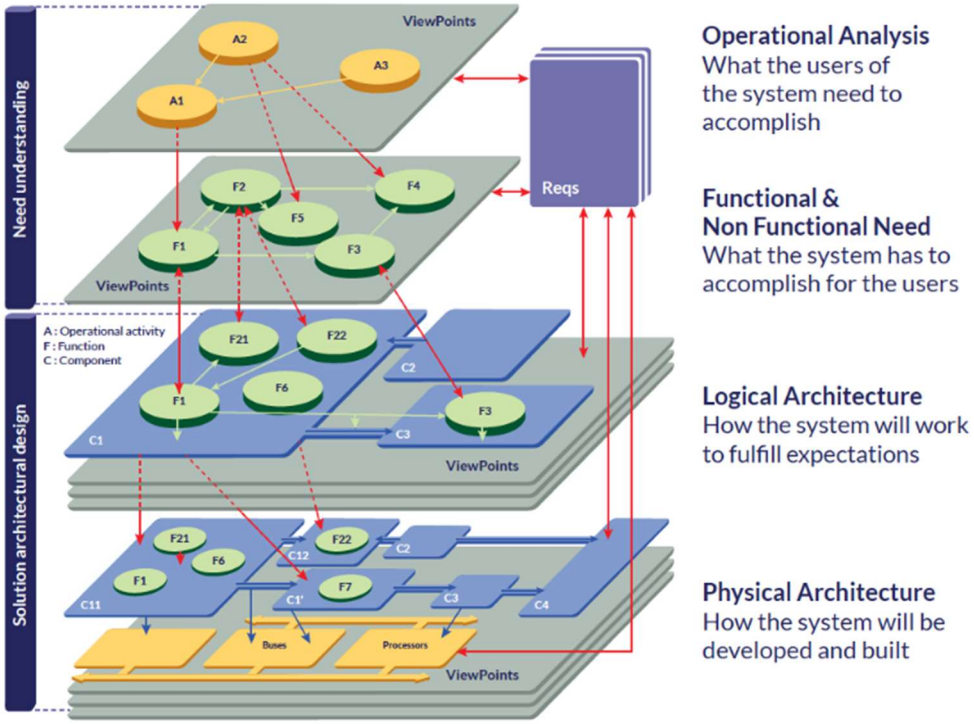

Figure 1. Arcadia engineering levels (12)

2.1.1 Capella software tool

Arcadia is supported by the open-source software Capella. It is the tool that implements the language of Arcadia to support its methodology. This tool enables the graphical representation of the system at every engineering level and is a means to deeply analyse the functional aspects of the architecture (13). The interaction between functions and entities can be represented, from the higher to the lower level. Every stage is based on the above one, and functions and actors can be automatically transitioned from one to the other. Moreover, different modes and states of the system can be expressed. The first are referred to an operating condition that can be set for the system, such as flight phases or a specific functioning of the system under certain conditions. Whereas states concern conditions of the system, something that happens but that cannot be imposed, like a degraded state, a charged or discharged battery, or an environment constraint (14).

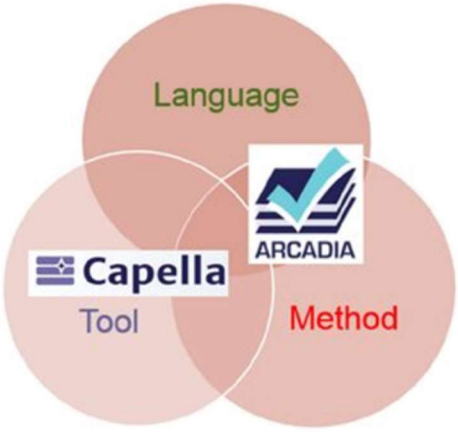

Figure 2. Arcadia/Capella approach on MBSE (15)

2.2 Safety analysis method: Functional Hazard Assessment

The V-diagram presented in Figure 3 shows the hierarchical structure of the safety requirements levels together with the safety assessment methods from the aircraft to the item level. The Functional Hazard Assessment (FHA) is a safety assessment method to be developed at the early stages of the development cycle. The standard guidelines adopted by industry are described in the SAE ARP 4754 (16). The process is useful to determine the functions and identify potential failure conditions related to each of them. The method includes the classification of the failure condition. The FHA can be conducted either at the aircraft level or, as in this work, at the system level. The aircraft-level FHA provides a comprehensive analysis of the entire aircraft, addressing the primary functions of each

system. In contrast, the system-level FHA focuses on individual systems, offering a more detailed examination of a specific system's functions.

The process is a top-down approach and it is based on the following steps, provided by the document "SAE ARP 4761: *Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment"* (17):

a. Identification of the functions;

b. Identification of the failure conditions related to the functions;

c. Description of the effect produced by the failure conditions;

d. Classification of the severity of the failure conditions;

e. Assignment of requirements to the failure conditions (17).

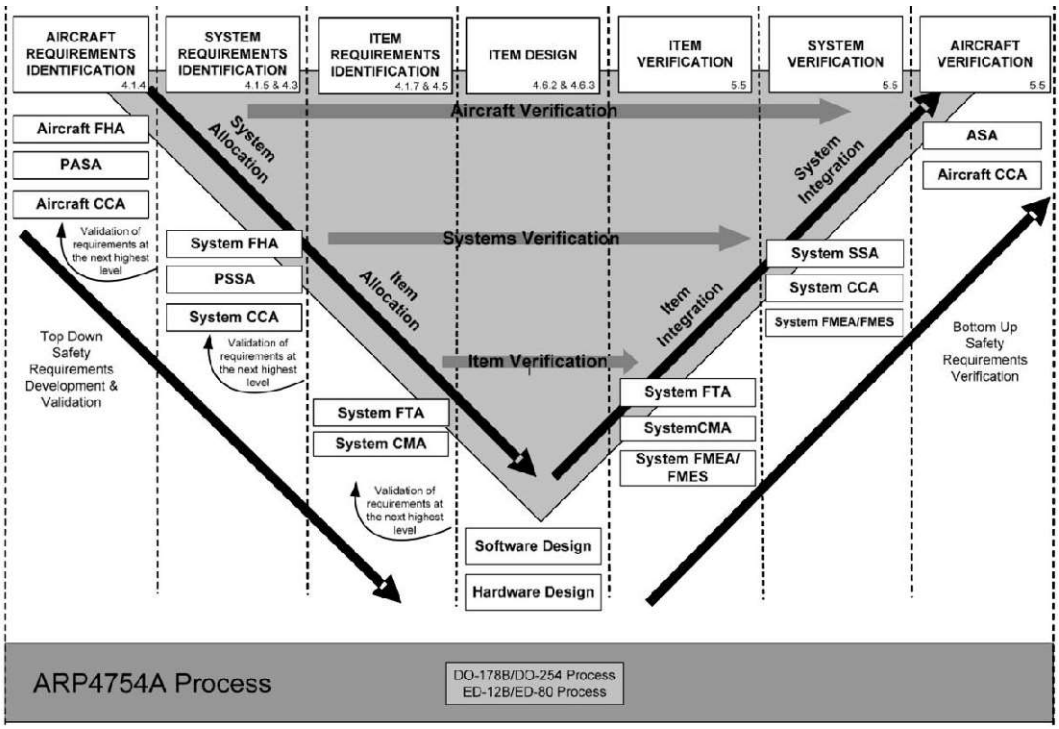

Figure 3. Interaction between safety and development processes (16)

Failure conditions might be different, and their causes depend on the function they are referred to. Typical failure conditions include the total loss of the function, the partial loss of the function, or a malfunction. Some conditions might not lead to the immediate loss of the function but to a degraded

mode of operation. Other cases refer to a possible malfunction related directly to the function under study, but they can also be derived from the failure of another function which has to happen before in the functional chain of the operation. Moreover, some critical conditions might be the consequence of a missing detection of the state of a component. Not being aware of the correct conditions of one of the elements of architecture could be followed by a potential failure.

The classification of the failure condition (d) is based on the standard levels of severity determined by the degradation of the related function and the effect on the aircraft. The levels entail a gradual loss of the safety. The result of a failure might vary from not having consequences in the operations to leading to a catastrophic event. Each failure scenario is analysed with respect to the effect generated on the aircraft. The classification of the effect on the airplane is presented in Table 1.

The analysis of the effect on the system leads to the identification of possible mitigation to restrain the failure condition and avoid the loss of functional capabilities which may be essential for the safety of the mission. Redundancies and different system to implement a function are a valuable way to avoid catastrophic events and guarantee a high level of safety. Another important value to consider is the probability of the occurrence of a failure condition, which should be extremely remote for catastrophe-leading events. The design recommendations provided to the architecture aim to reduce both the severity of the failure and the probability of occurrence.

Classification	**Effect on the airplane**
No safety effect	No effect on operational capabilities or safety
Minor	Slight reduction in functional capabilities on safety margins
Major	Significant reduction in functional capabilities or safety margins
Hazardous	Large reduction in functional capabilities or safety margins
Catastrophic	Normally with hull loss

Table 1. Classification of the effects of the failure conditions (18)

3. H2 fuel cell aircraft challenges

The project has started with bibliographic research, not only on the methodology to be used in the work, but also regarding the state of art of the technology to be included in the architecture. Hydrogen is one of the protagonists of the climate transition and has a great potential when used in fuel cell systems. However, as already explained, this configuration has stringent requirements as far as thermal management and insulation to function properly. The chapter aims to describe the main characteristics and needs of the chosen technologies.

3.1 Hydrogen as fuel

The use of hydrogen fuel is extremely advantageous in terms of climate impact due to the zero CO_2 and NOx direct emissions when used into fuel cell technology. However, as previously mentioned in the introduction, it states several challenges and criticality to be faced.

In Table 2 hydrogen properties in comparison with kerosene's are shown. Liquid hydrogen density (the reported value refers to hydrogen at boiling point and kerosene at 283 K) is very low and require a much larger volume for the storage with respect to the actual fuel tank installed on aircraft. It would be impossible to integrate it into airframes, hence the liquid form of hydrogen is preferred to significantly reduce the space to host the tank and so the weight. Moreover, hydrogen reaches its boiling point at -253 Celsius degrees and must be stored in cryogenic conditions, which increase the complexity of the entire system. Liquid hydrogen storage is feasible for aircraft application, but high thermal insulation is necessary to maintain the condition far from hydrogen boiling point at 20 K. If hydrogen exceeds the limit, it starts boiling and reaches a critical phenomenon called boil-off. Pressure increases causing structural stress on the tank demanding immediate ventilation through a dedicated valve. Furthermore, hydrogen molecules are very small and likely to permeate into material, this is why tanks require the choice of suitable materials to avoid hydrogen permeation into it. If a leakage were to occur, only 4% concentration of dispersed hydrogen in the air would be sufficient for an explosion (19).

The table also shows some advantages of the use of hydrogen. The higher level of specific heat with respect to kerosene's value indicates that liquid hydrogen has a greater potential when used as a cooling source. Its significant cooling capacity can be exploited to absorb heat generated from other components. Finally, the specific energy is extremely elevated and permit a lower amount of fuel under equivalent energy produced (20).

Properties	Hydrogen	Kerosene
Liquid density $[g/cm^3]$	0.071	0.811
Boiling point at 1 atm $[K]$	20.27	$440 - 539$
Specific heat $[J/(gK)]$	9.69	1.98
Specific energy $[kJ/g]$	120	42.8

Table 2. Comparison between the properties of liquid hydrogen and kerosene (20)

3.2 Hydrogen PEM fuel cells

Hydrogen fuel cells are a promising technology for the development of electric and hybrid electric vehicles, in sight of the reduction of fossil fuel-based propulsion systems. Fuel cells can generate electricity through the electrochemical reaction of hydrogen and oxygen, generating water and heat as a waste product. No combustion occurs and carbon and noise emissions are eliminated.

Regarding the type of fuel cell technology implemented, polymer exchange membrane fuel cell (PEM-FC) is considered as compatible with hydrogen fuel. As already mentioned, is an electrochemical device able to produce electrical energy through the chemical reaction between hydrogen and oxygen. Hydrogen enters the fuel cell through the negative electrode, the anode, and its molecules are split into protons and electrons. Air is supplied to the positive electrode, the cathode. Electrons produce electricity in the external circuit and protons migrate to the cathode. The outcome of the reaction is electrical energy and water.

The fuel cell system is composed of the fuel cell stack, where the energy is generated, and its Balance of plant, which includes all the subsystems required for the system's operation. Firstly, the inputs of the reaction must be delivered to the fuel cell, hence an Air supply system and a Hydrogen supply system are present. Moreover, water exiting the fuel cell must be handled by a Water management system, which exploits the excess water to regulate the humidity of the cell through the Air supply system, which is an important parameter to regulate to guarantee the proper functioning of the fuel cell.

As well as humidity, another relevant factor to control in the fuel cell is its temperature. During operation, the temperature of the fuel cell rises and must be properly controlled by a dedicated thermal management system to avoid the overheating of the stack. The operating temperature is 70-80 °C.

This requirement implies that also the air and fuel must enter the fuel cell in the proper temperature conditions.

Finally, the Fuel cell system requires a Control system able to elaborate signals from the electric grid and manage the entire unit in order to produce the demanded power level (21).

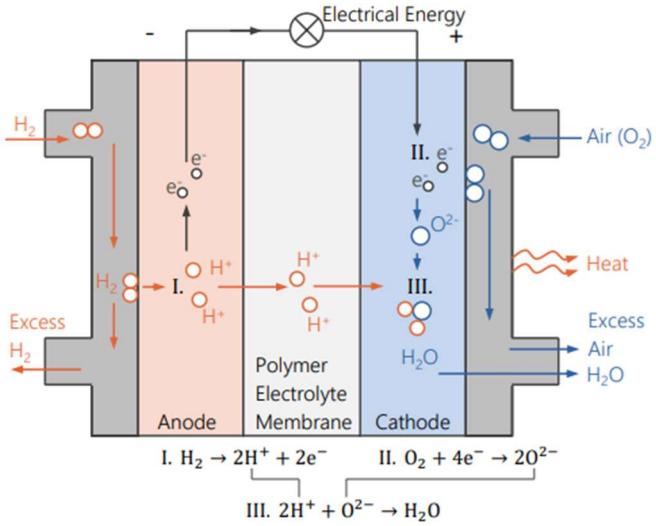

Figure 4. PEM fuel cell working principles (21)

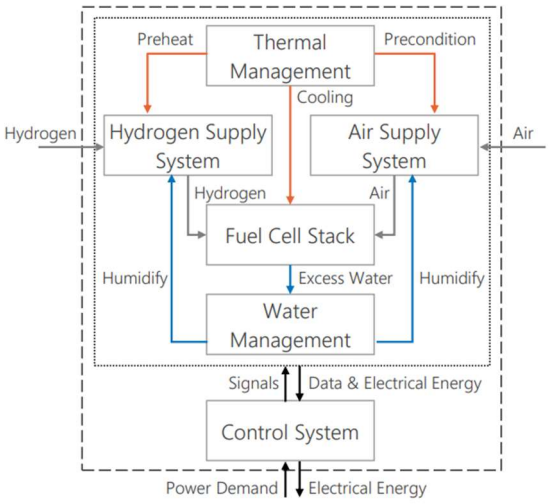

Figure 5. Subsystems of the fuel cell systems (21)

3.3 Thermal management system

As previously mentioned, fuel cell temperature regulation is a critical aspect of the entire system and one of the main focuses of the analysis. The fuel cell stack generates heat during operation which must be absorbed from the thermal management system to avoid the overheating and the degradation of the component. Moreover, hydrogen must feed the fuel cell at the right operating temperature of 70-80 °C; hence it must be converted from cryogenically liquid to gaseous state before entering the stack.

The dedicated thermal management system could be developed exploiting the thermal load of the fuel cell and the cryogenic hydrogen. It can indeed use the heat generated by the fuel cell to evaporate the hydrogen. Two different technologies are being developed for hydrogen conversion: an integrated heat exchanger inside the hydrogen tank or an external heat exchanger. In the second solution a cryo-pump to withdraw hydrogen from the tank is needed (22). Hydrogen is stored at minus 253 °C and its temperature must be heated up to 70-80 °C before entering the fuel cell. The fluid used to transfer

the thermal load in the conversion must be carefully selected as many fluids freeze when getting in contact with the cryogenic temperature.

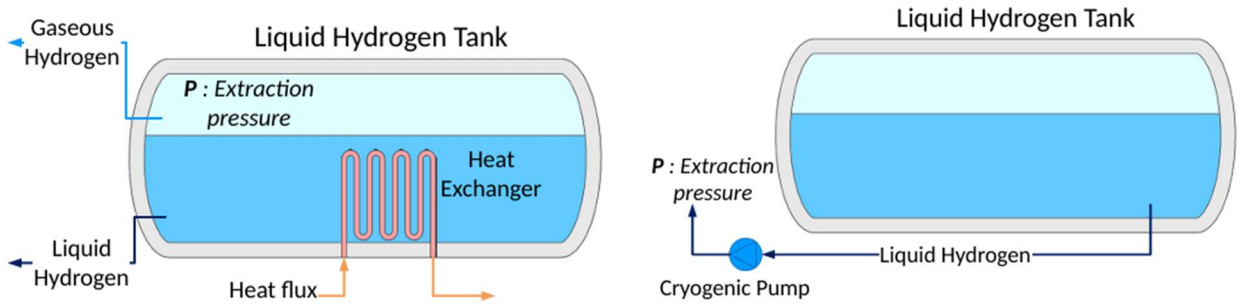

Figure 6. Extraction from a liquid hydrogen tank using the self-pressurization method (left) and a cryogenic pump (right) (22)

4. Case of study: LH2 PEM-FC regional aircraft

At this stage, the model of the system architecture is described. It has been developed thanks to the contribution of the bibliographic research of exiting projects. As stated, the scope of the model is not to depict a feasible architecture to propose a detailed conceptual design. It aims to provide a reference for conducting the safety analysis. It represents a possible example of a new propulsive aircraft configuration, in which the research is currently working on to advance to a more sustainable air transport. The target is not the design and the optimization of the architecture, but the related safety analysis which is going to be one the essential aspects to be considered for future design process.

4.1 Bibliographic research and reference projects

The model of the case of study has been developed by collecting information from different projects and conceptual designs of fuel cell systems and dedicated thermal management architectures. The target vehicle is a regional aircraft powered by liquid hydrogen PEM fuel cell system for 50-70 passengers.

The most relevant reference that has been considered is FutPrInt50: a European project with the aim of contributing to the development of a hybrid-electric aircraft for 50 passengers within 2035-2040 (23). FutPrInt50 is cooperation between international companies, universities and research centres. The project has developed several publications and articles to communicate its progress on the studies. FutPrInt50's *Deliverable 2.1 Requirements and Reference Aircraft* (24) provides a deep analysis of the top-level requirements and defines potential flight missions for 400 to 800 kilometres design range. The study has been considered to provide a variety of external conditions, both from an environmental and geographical point of view. The aircraft systems must perform safe flight during take-off and landing in extreme weather conditions with very hot or very cold ambient temperature and extreme air density and pressure conditions.

Figure 7. FutPrInt50 logo

While FutPrInt50 represents the main reference as far as the entire aircraft configuration and its mission design, the development of the Electric power system has been influenced by different publications proposing potential architectures. In Figure 8, a thermal management system architecture proposed by Embraer is shown. The integration between the thermal management of the cell and the

hydrogen conversion can be observed. Moreover, the cooling capacity of hydrogen is exploited to absorb heat to other systems: electric motors, batteries and electric engine (25).

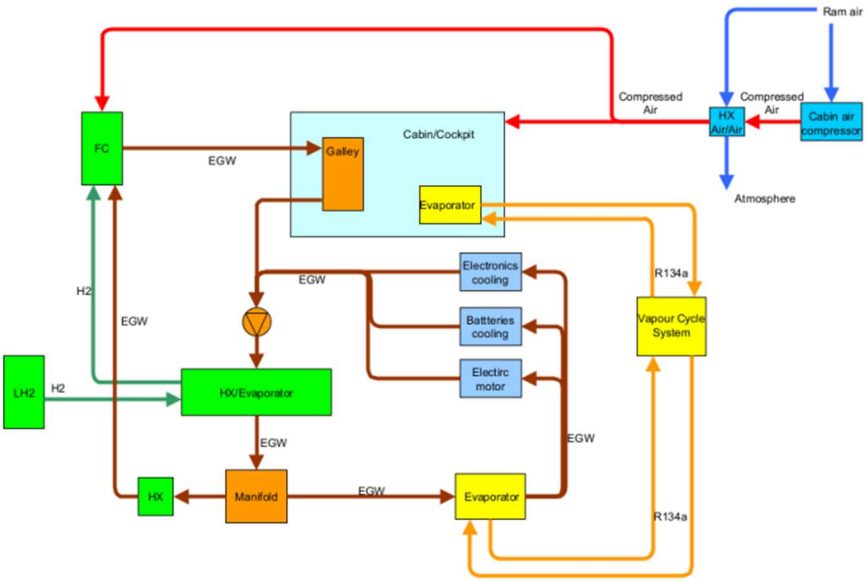

Figure 8. TMS architecture based on liquid hydrogen fuel cell (25)

A different solution of fuel cell thermal management is presented in Figure 9. The system is divided into two cooling loops. The primary one collects the heat generated by the fuel cell during operation. Part of the collected heat load is used to increase the hydrogen temperature, while the excess part is dissipated into the atmosphere. The secondary loop has to condition air and hydrogen to supply the fuel cell. Ram air must be compressed to increase pressure, but the compression implicates a rise in the temperature that must be managed. The heat is used to heat hydrogen, and the rest is dissipated to the external environment (26).

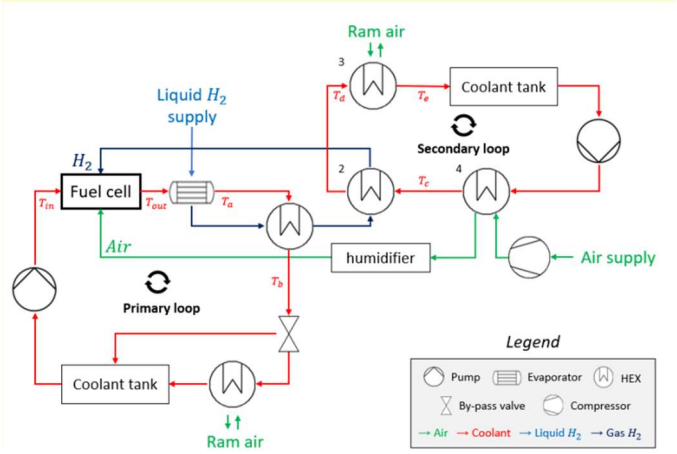

Figure 9. Liqud-cooling thermal management system for fuel cells (26)

4.2 LH2 PEM fuel cell regional aircraft

The liquid hydrogen PEM fuel cell regional aircraft for 50-70 passengers is presented in this section. A main energy system, supported by the auxiliary energy system in the most power-demanding phases, powers the electric engines to produce thrust and all the aircraft systems which require electrical energy to operate.

The aircraft power demand is generated by the fuel cell system, sustained by the battery system, which represents the auxiliary source of energy. The combination of different technologies is necessary to avoid the weight penalty of an oversized fuel cell and mitigate its slow dynamic response characteristic (27). The battery system has also the function of storing electric energy, both by being charged on the ground before the mission, but also during less power-demanding phases of the flight. Another important role of the battery is the stabilization of the electric grid on the aircraft. Batteries are able to absorb and release energy rapidly, hence they represent an essential instrument to maintain voltage and frequency stable. It is underlined that batteries could also be substituted by supercapacitor, or even both components could be included in the architecture.

Even though the FHA procedure is going to focus only on the architecture of the systems in charge of the production of the power on board, the total configuration of the aircraft must be defined for the sake of the analysis.

The proposed architecture is composed of two independent Electrical power systems, positioned on the left and on the right side of the aircraft. Each system is able to generate energy, store energy and provide a dedicated thermal management. Fuel cells are in charge of the generation process, while

the storage function refers to both the energy that has to be converted, the hydrogen, and the "ready to use energy" from the battery system. The thermal management system is dedicated to only the fuel cell and the hydrogen storage, whereas the battery thermal management is not included in the Electric power system. The battery system has a dedicated TMS which is not considered in the analysis. The two systems feed the electric grid which is going to distribute the energy to the electric engines, to all the other systems of the aircraft and to the Electric power system's components. The entity of the electric grid and its distribution is not provided in detail as it is not part of the focus of the analysis. The same occurs for the number of electric engines that generate thrust, although they must be at least more than one to comply with safety requirements specifications. The definition of two separated systems entails that any failure related to one of the two systems on board is not going to compromise the fully functioning one.

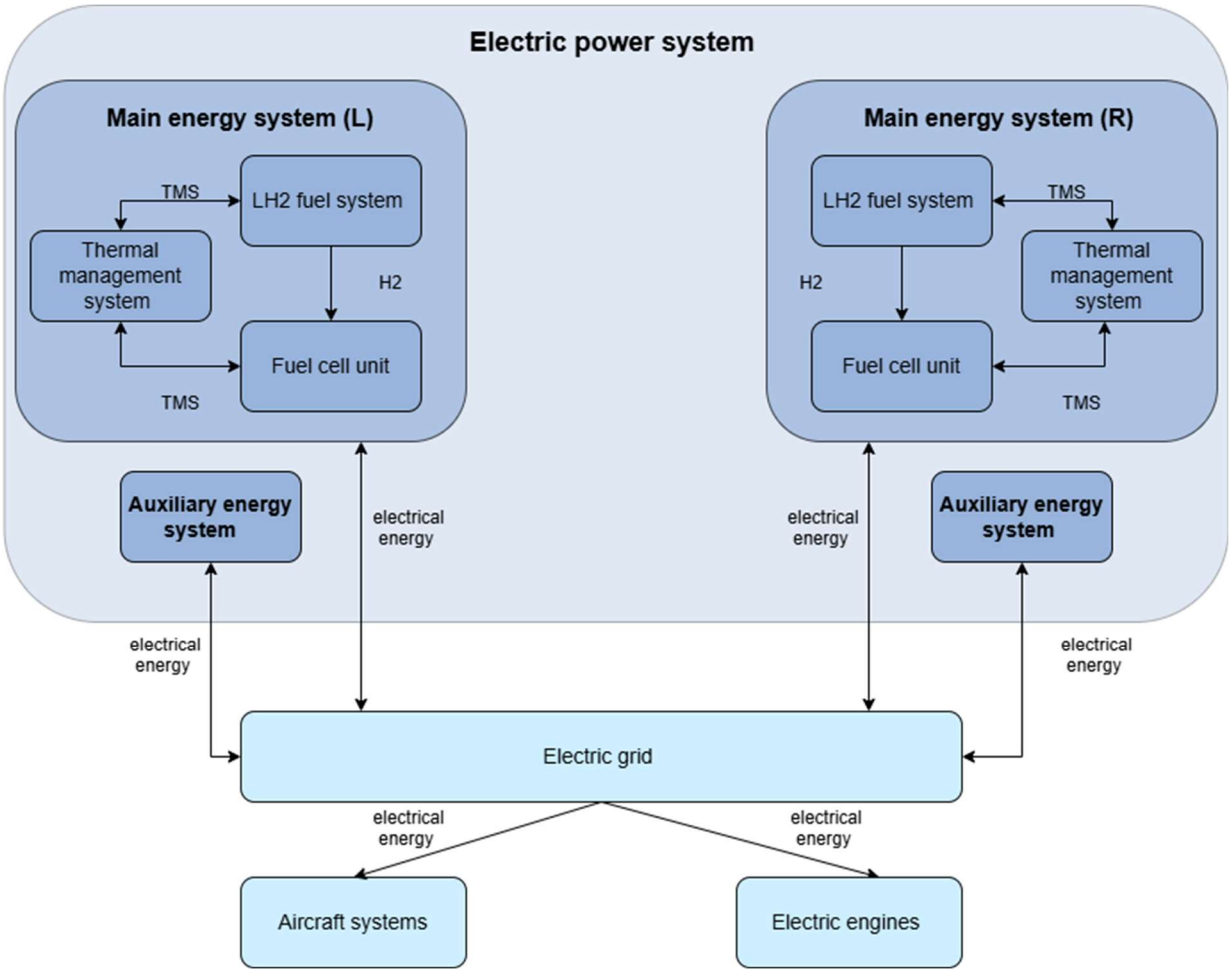

Figure 10. Aircraft configuration

4.2.1 Assumptions

The assumptions have been defined to comply with the Certification Specification for large airplanes CS-25 (28) of the European Aviation Safety Agency (EASA). As stated in the CS 25.903, the engines are required to be independent from each other to guarantee safe operation in case a failure or a malfunction affects one of the engines. The aircraft must be indeed able to take-off and perform operations with only one engine. This fundamental requirement must be preserved also in the considered electric engines architecture. Hence, each fuel cell system is assumed to be designed to generate enough thrust to perform take-off with only one engine. This requirement is essential to reduce the probability of a catastrophic event. Even in case of the loss of the auxiliary energy systems and one of the main energy sources, the remaining fuel cell system alone must be able to take-off and then conclude the mission within the boundaries of safety.

4.2.2 Energy management strategy

The Electric power system of the aircraft is composed of a Main energy system, the fuel cell system, and an Auxiliary energy system, the battery system. The required power varies among the different phases of the flight, fuel cells and batteries are not always active at the same time. Different modes of operation can be defined to fulfil different powered demands during the mission. Energy management strategies derive from the analysis of the required power. The highest power demand is expected at the early stages of flight, take-off and climb and go-around. Cruise is a constant energy phase, and finally there is a reduction of the necessary energy at descent and landing (Figure 11).

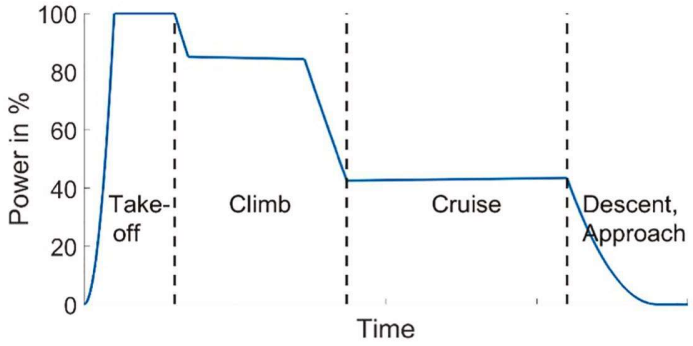

Figure 11. Required power as a percentage of maximum system power during different flight phases of a possible flight profile plotted against flight duration (29)

Fuel cells are best operated at constant level of generated energy; hence, it is chosen to design them to match with the required power during the cruise. Hence, take-off and climb, which require higher power demand, are covered by both fuel cells and batteries. Whereas the excess energy generated in the stack during descent and landing is used to charge the storage system. Although charging in flight

might not be the best solutions in terms of efficiency, it guarantees that the batteries have the energy to provide enough power in case of a go-around scenario. It is also established that the battery is going to be charged before the flight on the ground by an external source of energy from the airport infrastructures.

These configuration leads to the definition of the different modes of operation during flight:

- *Fuel cell mode*: only the fuel cell system powers the aircraft. It is used in cruise, when the energy generated by the fuel cell is equal or higher than the requested;
- *Combined mode*: both the fuel cell and the battery supply the aircraft. It is active during take-off, climb and go-around;
- *Battery mode*: only the battery system is active. It is used during fuel cell failure conditions;
- *Battery charging*: both the fuel cell and the battery are active, but the battery is not supplying the aircraft. It is used during descent and landing, when the energy generated by the fuel cell is higher than the requested and it is transferred to the battery to be stored (29).

The systems should be sized not only to fulfil the power demand combined, but also when a failure occurs and either one of the two redundant systems is missing, to avoid a catastrophe. As mentioned, fuel cells are dimensioned for powering the cruise phase and batteries are going to supply the power needed to take off. It is assumed that a single fuel cell system should have sufficient power to sustain one engine at take-off. In this way, if a failure were to occur, both energy systems will be able to continue the take-off and land safely. It is taken for granted that, as conventional aircraft, take-off can be performed by a single engine in case of failure. The systems conditions of operation with respect to the phases of the flight are summarized in Table 3.

Flight phase	**Fuel cell**	**Battery**
Take-off	ON	ON
Climb	ON	ON
Cruise	ON	STAND-BY
Descent	ON	CHARGING
Landing	ON	CHARGING

Table 3. Fuel cell and battery state with respect to the phases of the flight

4.3 Capella model of the reference system

The Electric power system of the aircraft has been developed with the software tool Capella. The model represents one of the two redundant systems that are part of the aircraft architecture. It has been designed starting from an aircraft-level point of view as far as the operational analysis, and then it has moved on the system-level, gradually in a more detailed approach.

4.3.1 Operational Analysis

The operational level identifies the operational needs to fulfil the requirements established by the stakeholders. This stage of the model offers an overall view of the aircraft, in which the system of interest is contained but it is not considered independently yet.

First, Operational Actors and Entities are defined in the *[OEBD] Operational Entity Breakdown diagram.* All the elements, like humans, vehicles, infrastructures and the environment, which interact in the system must be included in the model. Operational Actors are in this case the pilots, whereas Operational Entities are the Aircraft, the Airport facilities and the Atmosphere.

Figure 12. [OEBD] Operational Entity Breakdown diagram

The following step is the definition of the Operational Capabilities (OC) of the defined Actors or Entities in the *[OCB] Operational Capabilities Blank* diagram. The OCs represent the operational needs or services that must be provided by the elements acting in the system. The diagram reveals the high-level goals to be fulfilled to comply with the operational requirements requested by the stakeholders (9).

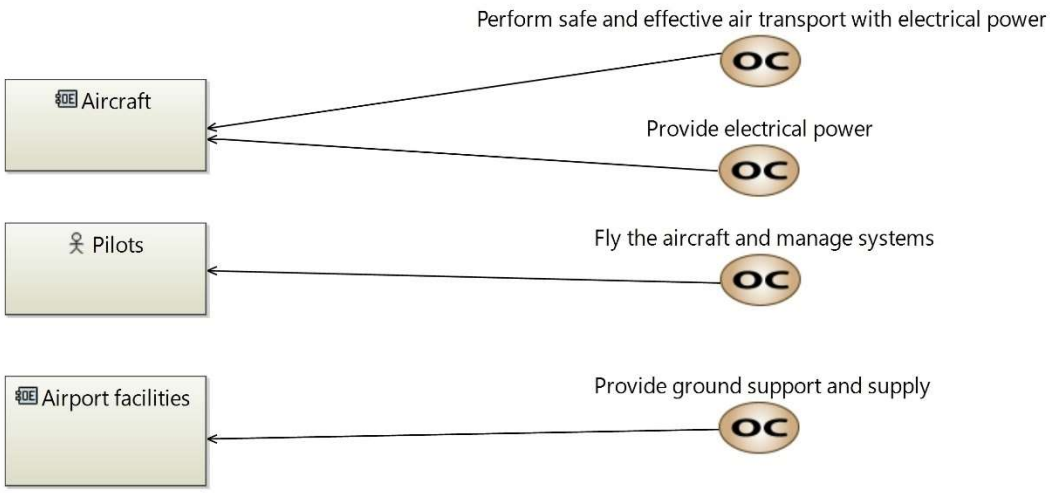

Figure 13. [OCB] Operational Capabilities Blank diagram

Subsequently, the *[OAB] Operational Architecture Blank* diagram is developed. In this part of the model, each Actor or Entity is associated with Operational Activities (OA) that are required to achieve their capabilities. Although the structure is still modelled considering the aircraft-level, the focus starts to shift to the functions of the system of interest. The operational activities in the [OAB] diagram are the following:

Aircraft

- *Provide electrical energy*: the system must be able to generate electrical energy to be used by all the aircraft systems that require it;
- *Provide thermal management*: the system must regulate the thermal load of all the elements of the aircraft;
- *Store energy*: the system must be able to store both electrical energy and fuel that will produce electrical energy;
- *Regulate power distribution*: the system must be able to control the energy distribution;
- *Distribute electrical energy*: the system must be able to transmit the electrical energy to all the systems that require it;
- *Generate thrust*: the system must be able to transform electrical energy into thrust force;
- *Provide other support function*: this operational activity encloses all the other functions essential on the aircraft which are not relevant for the analysis.

Pilots

- *Fly the aircraft and manage the systems*: the pilots must drive the air transport and control the systems;

Airport facilities

- *Provide ground support*: the facilities must assist the air transport and provide refueling and recharging;

Atmosphere

- *Provide environment*: atmosphere provides air for systems and an ambient to discharge heat load.

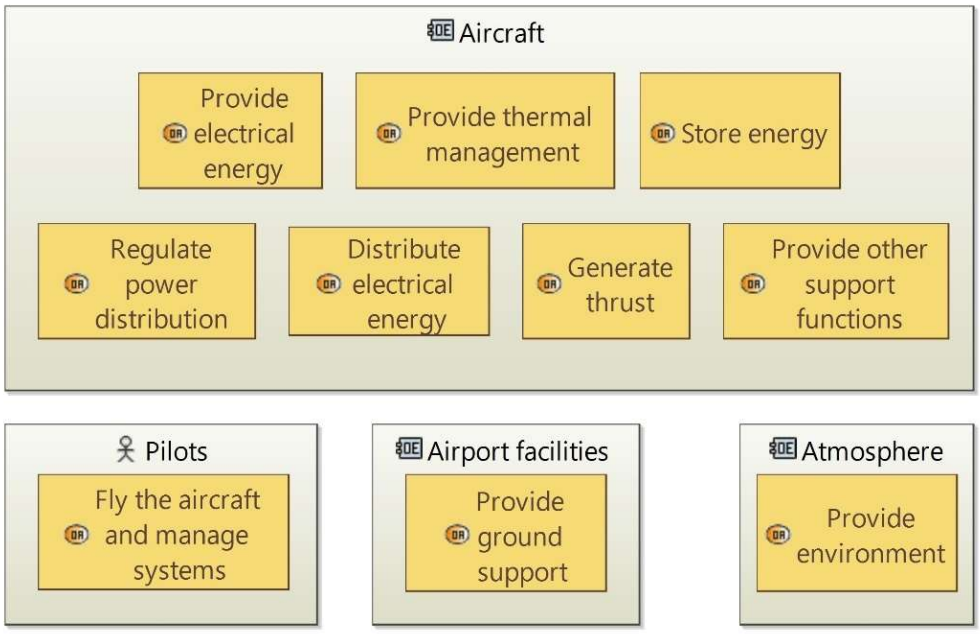

Figure 14. [OAB] Operational Architecture Blank

4.3.2 System Analysis

As already mentioned, in this level the functions of every element of the system are identified. Operational Entities/Actors are transitioned into System Actors and Operational Activities into System Functions.

The system of interest has to be defined in the *[SAB] System Architecture Blank diagram* and it does not coincide with the entire aircraft, as the safety analysis is going to focus only on one system of the aircraft. The system of interest is, in fact, the Electric power system (EPS), and it includes all the

functions related to the supply of electrical energy and the related subsystems. Even though the EPS is physically contained inside the airframe, from a functional point of view the aircraft is considered as an external actor with whom the system of interest interacts and exchanges information. In the [SAB] diagram is shown that some of the functions of the aircraft in the previous level are associated with EPS. Considering that the analysis will not be focused on the effect on the people on board, pilots are omitted in this representation. The lines connecting the functions are Functional exchanges and are used to explain what type of connection relates those functions or what is the means to exchange information among them.

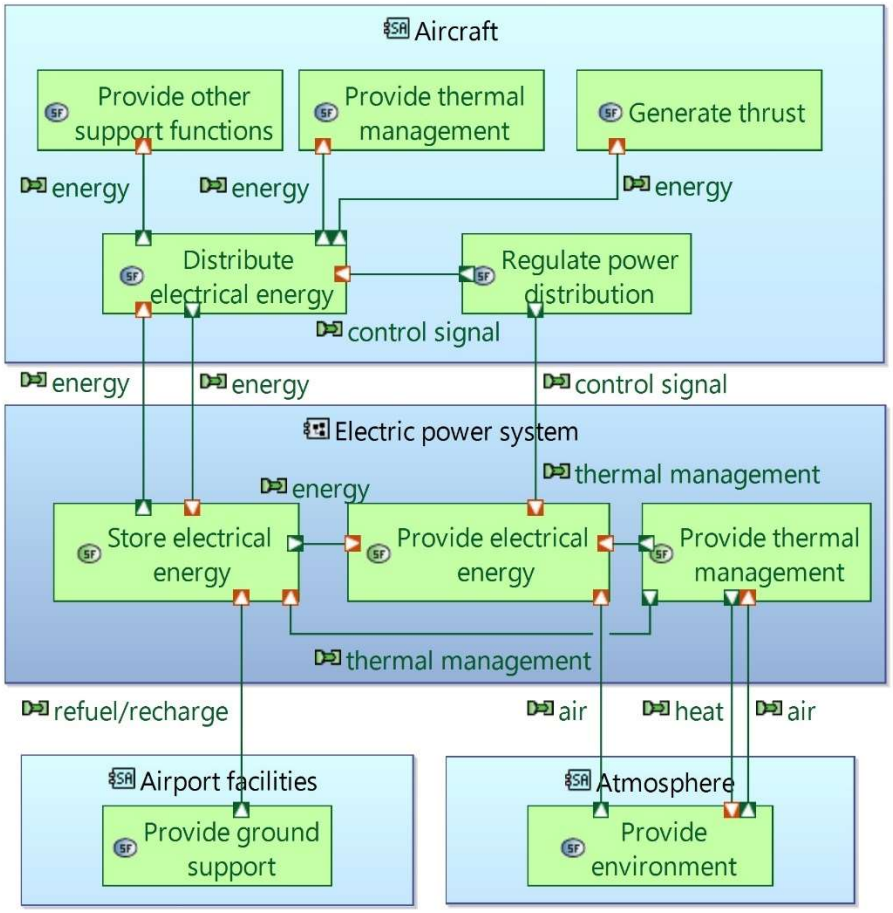

Figure 15. [SAB] System Architecture Blank

In Table 4 the correspondence between operational level and system level is represented. The first two columns include the Operational actors and their OA, which are transformed into System functions into the third column. System functions are enclosed in the system of interest or in the System actors. The function "provide thermal management" is the only action that has been considered both in the EPS and in the aircraft. In the first one, it is referred to a dedicated thermal

management required and provided inside the system, whereas in the second one it is related to the more general needs of the thermal regulation in any of the other systems which are inside the aircraft.

Operational Actor/Entity	**Operational activity**	**System function**	**System of interest/ System Actor**
Aircraft	Provide electrical energy	Provide electrical energy	Electric power system (SOI)
	Store electrical energy	Store electrical energy	
	Provide thermal management	Provide thermal management	
		Provide thermal management	Aircraft
	Distribute electrical energy	Distribute electrical energy	
	Regulate power distribution	Regulate power distribution	
	Generate thrust	Generate thrust	
	Provide other support functions	Provide other support functions	
Airport facilities	Provide ground support	Provide ground support	Airport facilities
Atmosphere	Provide environment	Provide environment	Atmosphere
Pilots	Fly the aircraft and manage systems	\	\

Table 4. Transition from Operational analysis to System analysis

At system level, capabilities from the operational level can be transitioned into missions. As in the [SAB] diagram, the focus moves to the system of interest. In the *[MCB] Mission Capabilities Blank* diagram the mission of the system is identified with the provision of electrical power which can be fulfilled with the main capabilities of the system. Each capability is implemented by the system of interest (which is implicit and not visually represented in this diagram) and by the involved actors.

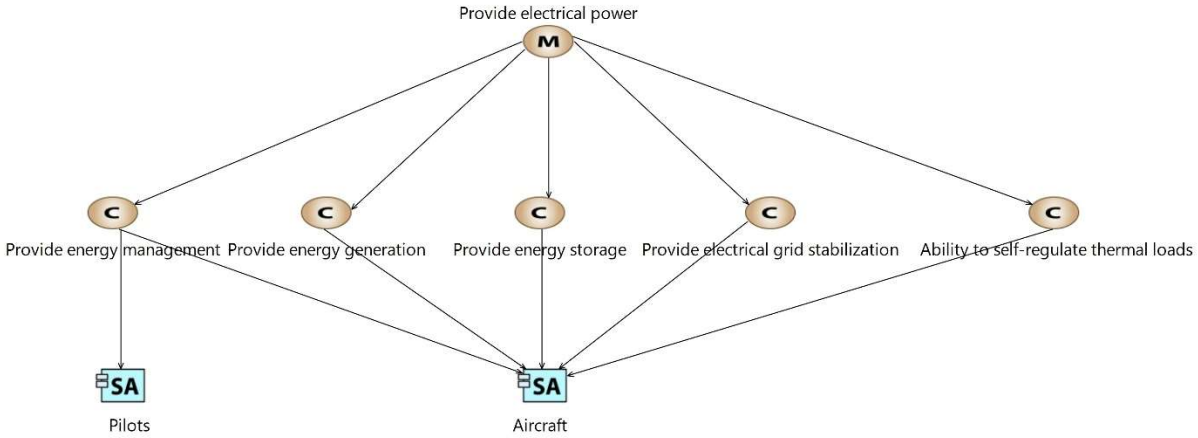

Figure 16. [MCB] Mission Capabilities Blank diagram

4.3.3 Logical architecture

In this level the system of interest is transitioned into a Logical Component, whereas all the elements that are not the primary focus of the analysis become Logical Actors. The system of interest, the Electric power system, is divided in two main subsystems: the Main energy system and the Auxiliary energy system. As stated, the logical level requires a functional analysis of the system which does not concern the implementation of design choices. However, the technology that is going to be developed is already known and some specific related issue starts to be included in the model. In fact, the Main energy system includes all the subsystem related to the main source of energy, which is going to be a fuel cell energy generation system. The logical component includes the elements that are going to manage inputs and outputs of the fuel cell system.

The Auxiliary energy system includes the secondary source of energy of the aircraft with the capability of storing the electric energy, which might be a battery or a supercapacitor component, or even both of them if needed.

The organization of the system of interest is shown in the extract of the *[LCBD] Logical Component Breakdown Diagram.*

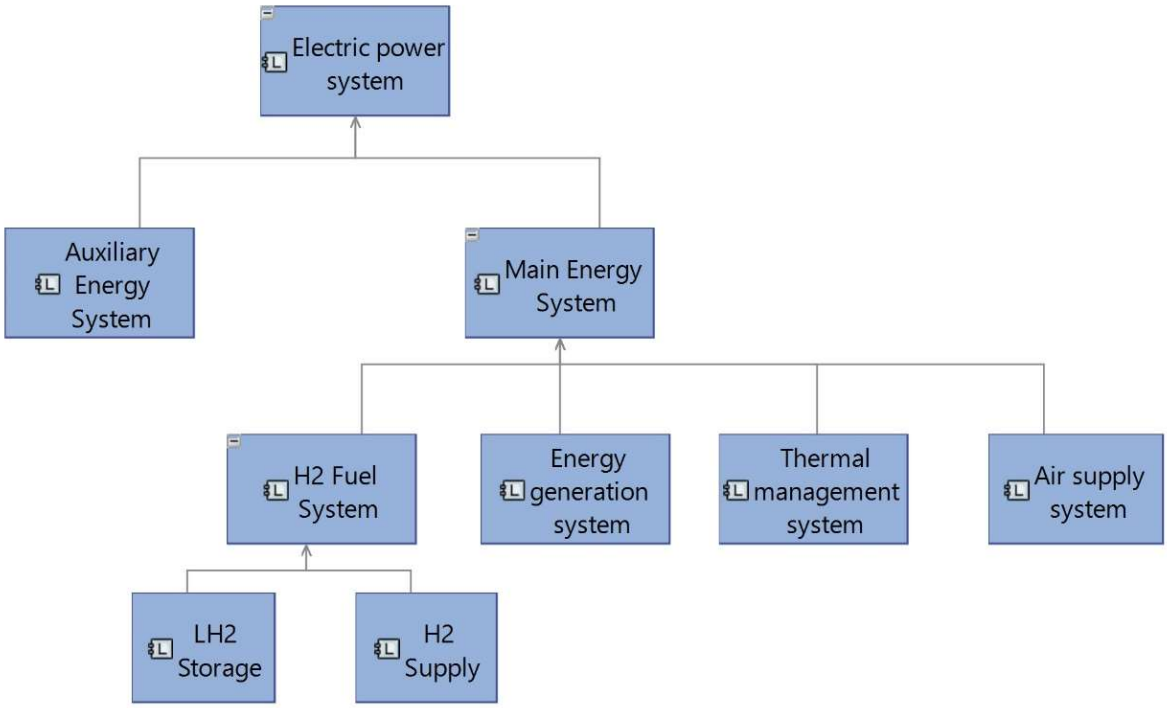

Figure 17. [LCBD] Logical Component Breakdown Diagram

System functions from the higher level are transitioned and developed in more detailed Logical functions. It is underlined that, even that some functions acquire new names or are divided into more detailed functions, Capella tool functionalities permit to link and refer to the corresponding functions in the above level to keep track of the development of the system.

As far as the external actors, the aircraft functions are divided into the ones related to the energy management and distribution and the ones that regards power receiver elements of the aircraft.

In Table 5, the transition from system to logical level is shown. It might be noticed that the “store energy” function concerns both the storage of the auxiliary energy system and the “energy” of the hydrogen that still needs to be converted into electricity. At this level the functions shift from a general description to a more detailed one.

System of interest/ System Actor	System function	Logical function	Logical component		
Electric power system (SOI)	Store energy	Store electrical energy	Auxiliary energy system		Electric power system (SOI)
		Provide stored electrical energy			
		Store LH2	H2 Fuel system	Main energy system	
	Provide electrical energy	Provide LH2			
		Provide GH2			
		Provide electrical energy from H2	Energy generation system		
		Control energy generation			
		Manage water output			
		Provide pressurized air	Air supply system		
		Regulate air temperature			
		Manage humidity			
	Provide thermal management	Provide heat	Thermal management system		
		Absorb heat			
		Dissipate heat			
Aircraft	Provide thermal management	Provide thermal management	Electric-powered systems		Aircraft
	Generate thrust	Generate thrust			
	Provide other support functions	Provide other support functions			
	Distribute electrical energy	Transmit electrical power	Electric grid		
	Regulate power distribution	Manage electric grid			
Airport facilities	Provide ground support	Supply power-grid electrical energy	Airport facilities		
		Supply hydrogen			
Atmosphere	Provide environment	Provide environment	Atmosphere		
		Absorb heat			
		Provide ram air			

Table 5. Transition from System analysis to Logical architecture

Logical components and functions are represented in the [*LAB] Logical architecture blank* diagram. The coloured lines visible in Figure 18 are called Functional Chains and are used to depict the connection between different functions which are one consequent the other. Functional chains are shown in *[LFCD] Logical Functional Chain Description diagrams.*

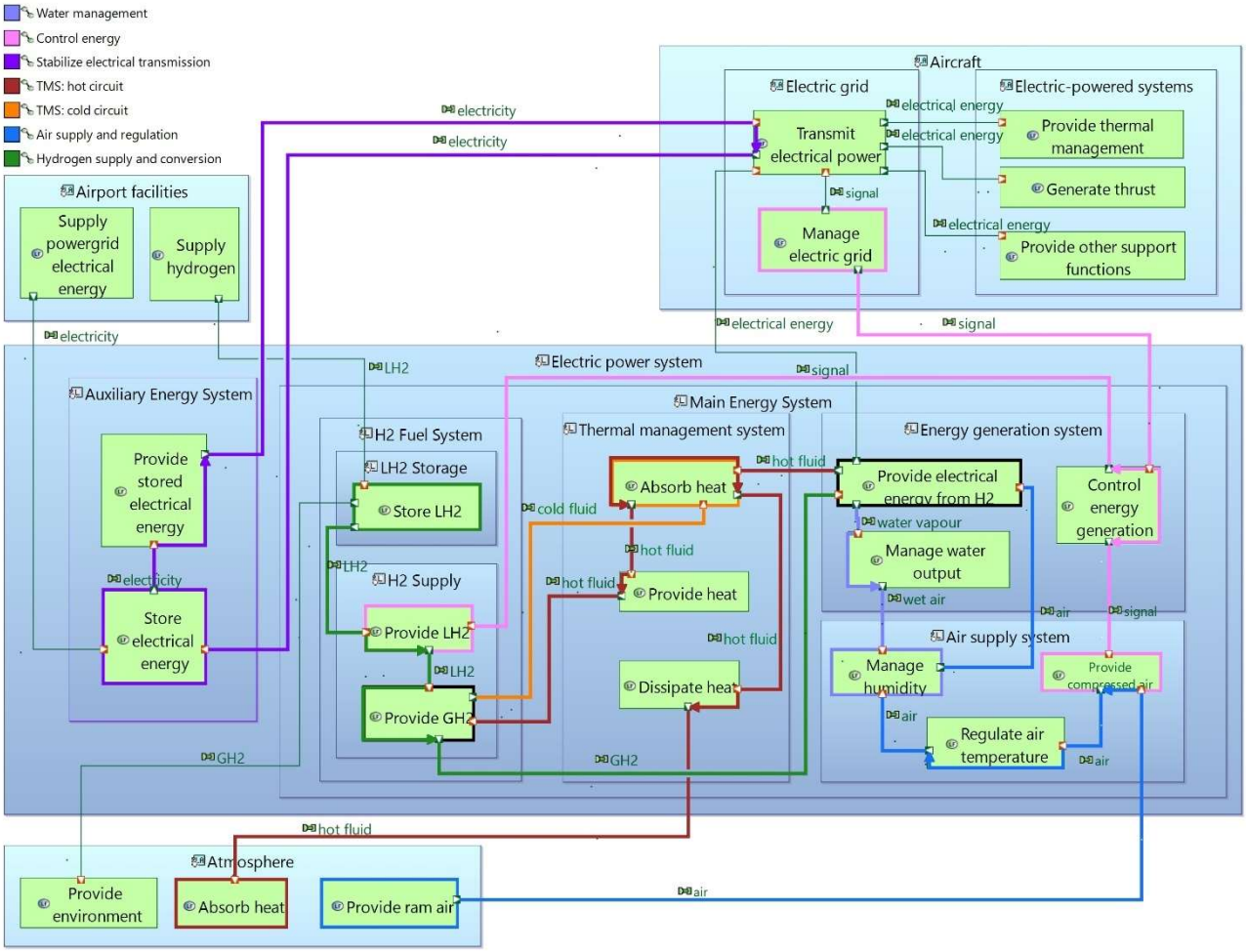

Figure 18. [LAB] Logical Architecture Blank

[LCFD] Stabilize electrical transmission

Electrical energy from the Auxiliary energy system is provided to the aircraft electrical power transmission. The electric grid present on board, which is responsible for the distribution of the electrical energy to the system on board and to the thrust generation, is not part of the system of interest. However, the grid stability level concerns the energy storage as it is responsible of the rapid absorption or release of electrical energy whenever is needed to maintain the level of voltage and frequency stable.

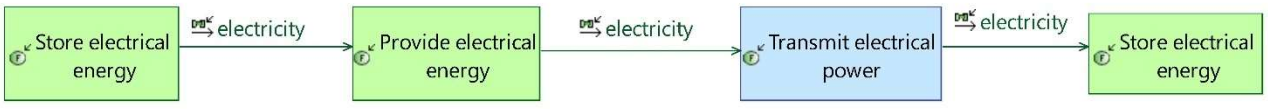

Figure 19. [LCFD] Stabilize electrical transmission

[LFCD] Hydrogen supply and conversion

Hydrogen, stored in cryogenic liquid condition, must be converted to supply the energy generation system at the required temperature range. Liquid hydrogen is converted through the thermal management system and then provided to the energy generation system in gaseous state.

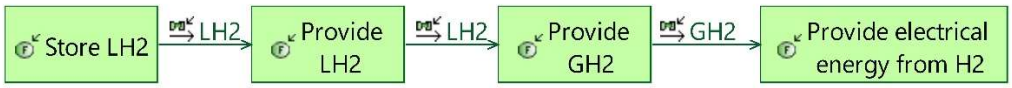

Figure 20. [LFCD] Hydrogen supply and conversion

[LCFD] Air supply and regulation

The air supply is provided by the Logical actor "Atmosphere" and conditioned to reach the correct level of pressure, temperature and humidity. Humidity level is achieved by the management of the exhaust water released in the energy generation system.

Figure 21. [LCFD] Air supply and regulation

[LFCD] Water management

The exhaust water exiting the fuel cell during operation is managed by the system and exploited to control the level of humidity inside the energy generation system.

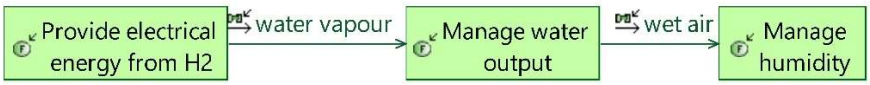

Figure 22. [LCFD] Water management

[LFCD] TMS: Hot circuit

The part of the thermal management system that transports hot fluids is presented in the chain. The heat generated in the energy generation system during operation is managed by the thermal management system. Part of the heat transported by the hot fluid is exploited to fulfil the function of hydrogen conversion and the excess heat that is not needed for the conversion is expelled and dissipated into the external environment.

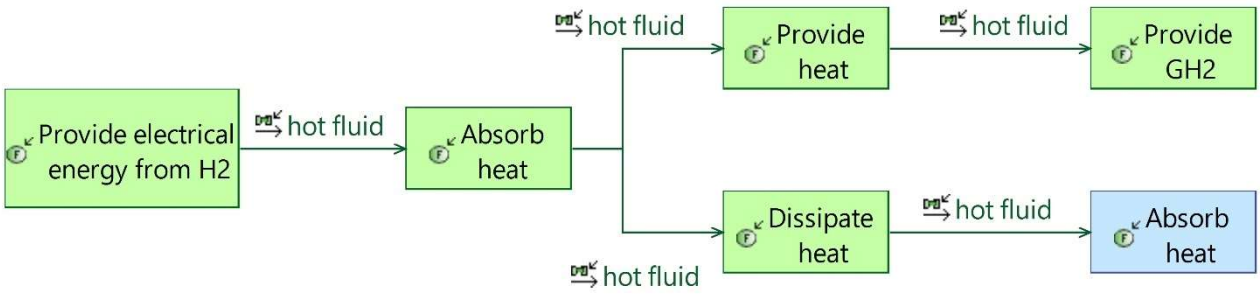

Figure 23. [LFCD] TMS: Hot circuit

[LFCD] TMS: Cold circuit

The thermal management function of heat absorption from the energy generation system exploits the cold temperature of hydrogen for the thermal exchange.

Figure 24. [LFCD] TMS: Cold circuit

4.3.4 Physical architecture

The physical architecture is based on the logical level and has the aim to represent a feasible architecture that realizes the functions identified in the high level. The presented physical model is only one of the possible physical architectures that can be designed with the above logical model.

The Logical functions are transitioned into Physical functions. Afterwards, the physical elements that execute the functions are created. Two possible types of components can be defined: Nodes and Behaviours. The first ones represent physical elements, such as hardware or material resources, whereas the second ones are used to diagram a *behaviour* of the system, like a software element (12). Behaviours are included inside the Nodes. In Table 6 the evolution from logical level to the physical implementation is presented. The external actors are not detailed into physical elements as they are not the focus of the analysis.

Logical component			Logical function	Physical functions	Physical Behaviours	Physical nodes		
Electric power system (SOI)	Auxiliary energy system		Store electrical energy	Store electrical energy	Energy storage	Supercapacitor and/or battery		
			Provide stored electrical energy	Provide stored electrical energy	Energy supply			
	Main energy system	H2 Fuel system	Store LH2	Store LH2	Hydrogen storage	Hydrogen tank		Hydrogen storage
				Vent hydrogen	Pressure regulation	Vent valve		
				Heat hydrogen	Pressure regulation	Hydrogen preheater		
			Provide LH2	Provide LH2	Provide LH2	Pump		
			Provide GH2	Provide heat	Hydrogen conversion	Hydrogen heat exchanger		Hydrogen TMS
				Provide GH2	Hydrogen supply	Valve		
		Energy generation system	Provide electrical energy from H2	Provide electrical energy from H2	Energy generation	Fuel cell stack		Fuel cell unit
			Control energy generation	Control energy generation	Electrical energy control	Fuel cell controller		
			Manage water output	Separate water from vapour	Water separator	Vapour-liquid separator	Water management	
				Store water	Water storage	Water tank		
		Air supply system	Provide compressed air	Regulate air flow	Air intake regulation	Inlet valve	Air supply unit	
				Provide compressed air	Air compression	Compressor		
			Regulate air temperature	Absorb heat	Thermal management	Air supply heat exchanger		
				Dissipate heat				
			Manage humidity	Manage humidity	Membrane humidification	Humidifier		
				Adjust air supply	Air supply	Valve		
		Thermal management system	Provide heat	Provide heat	Thermal management	FC heat exchanger	FC dedicated TMS	
			Absorb heat	Absorb heat				
			Dissipate heat	Dissipate heat				
Aircraft		Electric-powered systems	Provide thermal management	Provide thermal management	Aircraft			
			Generate thrust	Generate thrust				
			Provide other support functions	Provide other support functions				

Logical component		Logical function	Physical functions	Physical Behaviours	Physical nodes
	Electric grid	Transmit electrical power	Transmit electrical power		
		Manage electric grid	Manage electric grid		
Airport facilities		Supply power-grid electrical energy	Supply power-grid electrical energy	Airport facilities	
		Supply hydrogen	Supply hydrogen		
Atmosphere		Provide environment	Provide environment	Atmosphere	
		Absorb heat	Absorb heat		
		Provide ram air	Provide ram air		

Table 6. Transition from Logical architecture to Physical architecture

Figure 26 shows the physical architecture of only the hardware components, represented by the Nodes. The connections among them are Physical paths and represent the exchange that occur among those elements. Whereas, in Figure 27 the Energy generation system is being developed as a Fuel cell System. The main function of energy generation is fulfilled by the fuel cell stack. The Air supply system is physically included in the Fuel cell system in a dedicated internal Node called Air supply unit: ram air enters a compressor through the inlet valve, the compressor increases the pressure of the air. This phase leads to an increase in the temperature which is managed by a ram air heat exchanger (26). Then, the air goes through the humidifier, and it is ready to supply the fuel cell through a dedicated valve.

The Water management system is connected to the Air supply unit. Water and vapour mixture exiting the fuel cell is collected and separated through a water-vapour liquid separator. Excess water is stored in a water tank and the wet air is transferred to the humidifier to regulate the level of humidity inside the fuel cell.

The fuel cell unit includes the dedicated thermal management system (Figure 25) in charge of the heat absorption from the fuel cell when it is operating. A heat exchanger prevents the overheating of the stack, exploiting the cold condition of the hydrogen in the tank.

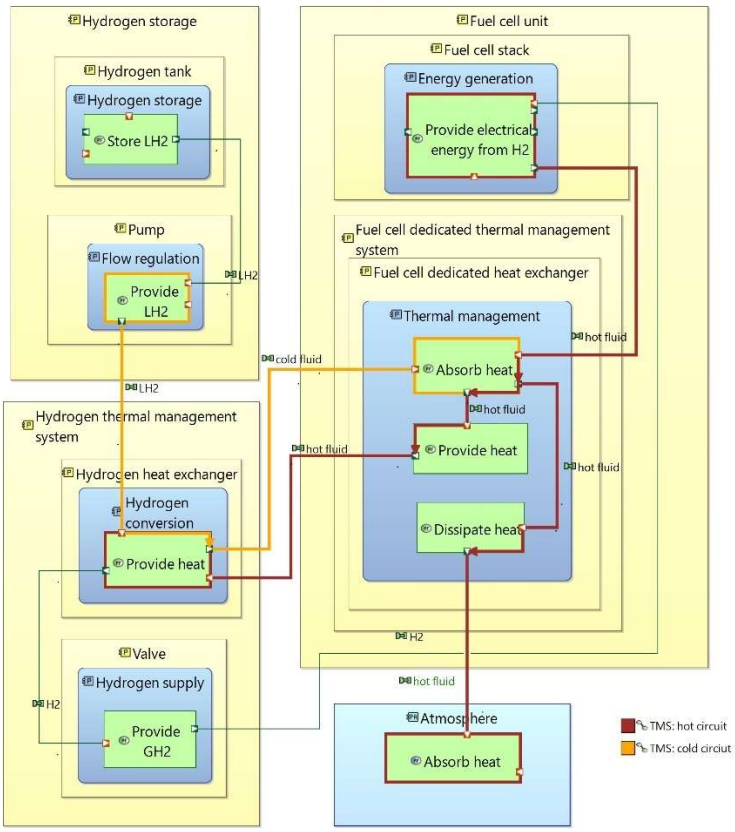

Figure 25. Extract of the Physical architecture: thermal management system

Finally, the fuel cell controller is in charge of the regulation of the energy generation process. It receives the target power level and sends signals to the supply systems. The regulation controls the amount of fuel and air which enters the fuel cell. The air level is controlled by the regulation of the air inlet valve. The amount of hydrogen is managed by the quantity extracted from the storage tank by a pump.

The hydrogen storage is made of a liquid hydrogen tank, able to insulate and maintain the cryogenic condition stable. Hydrogen is extracted from the tank with a cryogenic pump, which receives the input from the fuel cell controller. While hydrogen is collected, the internal pressure of the tank needs to be kept constant, this is why a preheater integrated in the tank heats the hydrogen to increase the pressure. On the contrary, if the pressure rises a vent valve operates to manage the potential boil-off condition and expels hydrogen into the atmosphere.

The hydrogen dedicated thermal management system is composed of a heat exchanger, in which the hot circuit is dependent from the fuel cell excess heat and uses it to increase hydrogen temperature to reach the fuel cell input requirement.

Before entering the fuel cell, hydrogen goes through a valve. This component has the function of shutting the line that connects the pump and the fuel cell in case of a failure in the hydrogen storage or in the fuel cell stack. It is the element that shuts off the system when needed.

As far as the electrical energy storage system, battery (or supercapacitor) is present to store the energy generated from the fuel cell, supply the aircraft when the only battery mode is requested and stabilize the grid to keep the transmission stable.

As it can be observed, the thermal management system is integrated with the system as the hot source is managed exploiting the fuel cell chemical reaction waste heat, whereas the cold source derives from the hydrogen storage temperature. The detailed architecture is shown in Figure 27. As in the Logical architecture, functional chains describe the path connecting the involved functions. The chains are coherent with the above level, even though some functions have been detailed to better describe the role of the components inside the configuration.

As in the logical level, functional chains are present in this level and are described in section 5.2.

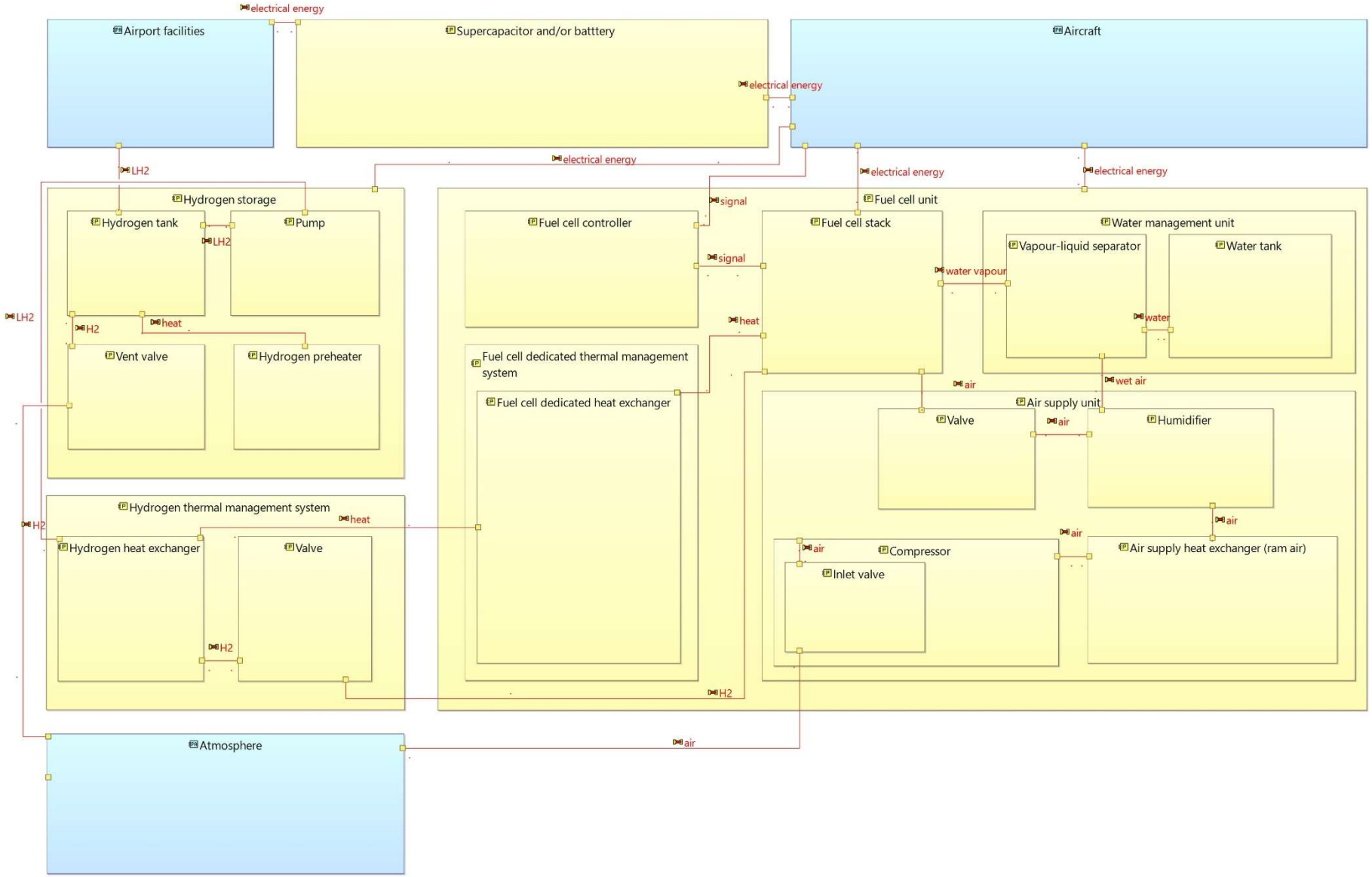

Figure 26. [PAB] Hardware components

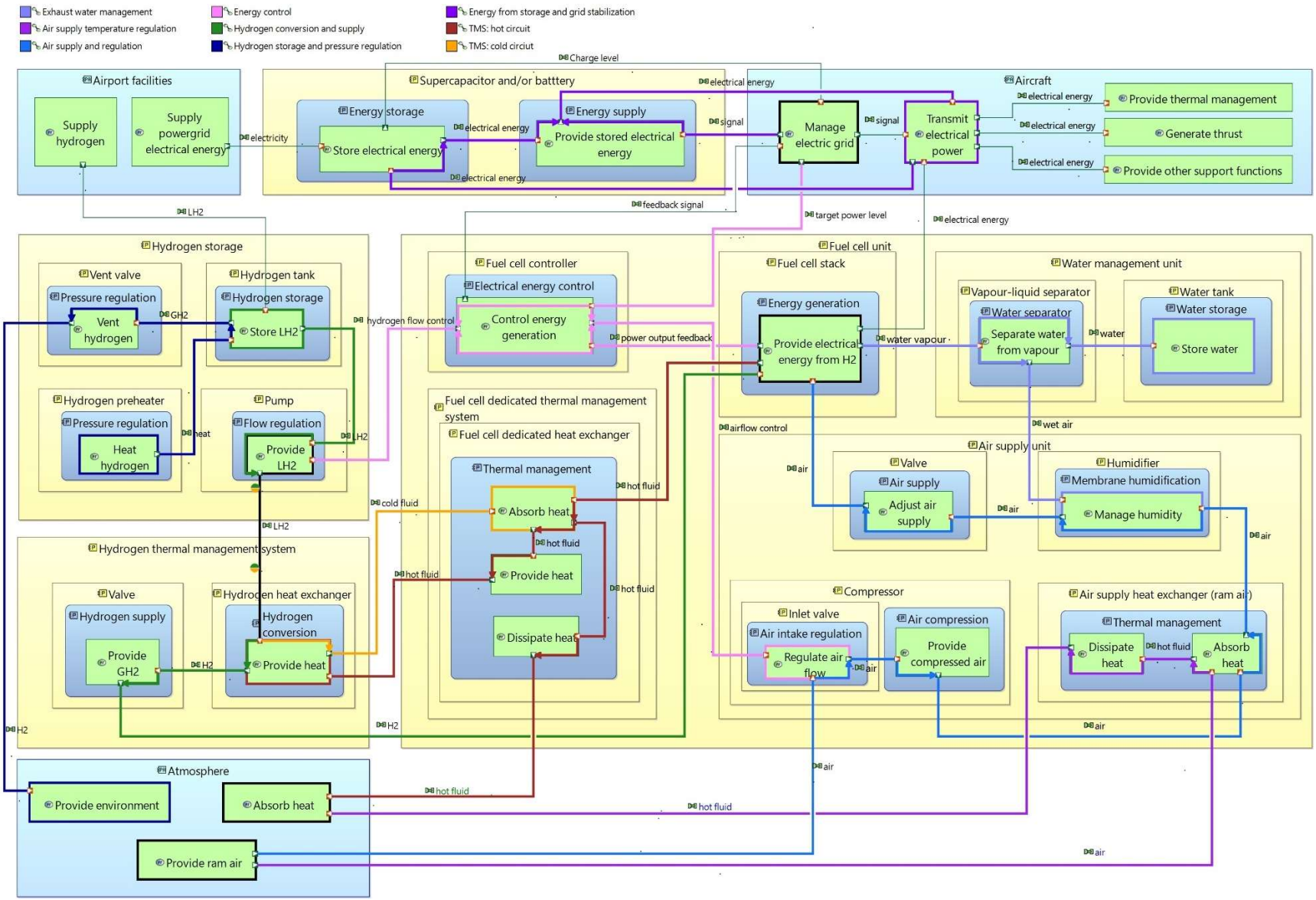

Figure 27. [PAB] Physical architecture blank diagram

5. FHA: application to the reference system

The system of interest developed in the model is the subject of the Functional Hazard Assessment. The scope of the analysis is the identification of possible failure conditions and the effects on the aircraft into different phases of the flight. The consequences that might occur determine the severity classification of each scenario.

The analysis is based on the steps described in section 2.2 and is conducted both on the logical and on the physical level.

Each function of the system of interest has been assigned to an identification (ID) code and analysed to determine potential related failure conditions, which are also distinguished by an ID. The functions ID code is composed as following:

- The first letter represents the Arcadia engineering level, L as logical or P as physical;
- The following three letters are referred to the logical subsystem at which the function is related, GEN = energy generation, TMS = thermal management system, STO = energy storage, AUX = auxiliary energy system;
- The numbers are dedicated to the single function. The functions in the physical level are derived from the allocated ones in the logical.

Logical level			
Logical component	**Logical function ID**	**Logical function**	**Function description**
Energy generation system	LGEN - 100	Provide electrical energy from H2	Electrical energy is generated through the chemical reaction between hydrogen and oxygen
	LGEN - 200	Control energy generation	Regulate the amount of energy that must be generated
	LGEN - 300	Provide compressed air	Compress ram air to supply the energy generation system
	LTMS - 400	Regulate air temperature	Manage the air temperature to supply the energy generation system efficiently
	LGEN - 500	Manage humidity	Regulate the humidity level inside the energy generation system

Logical level			
Logical component	**Logical function ID**	**Logical function**	**Function description**
	LGEN - 600	Manage water output	Manage the water exiting the fuel cell to provide vapour for humidity regulation
Thermal management system	LTMS – 100	Absorb heat	Absorb the heat generated by the energy generation system
	LTMS - 200	Provide heat	Provide the heat generated to the hydrogen conversion process
	LTMS - 300	Dissipate heat	Dissipate the excess heat into the atmosphere
LH2 Fuel system	LSTO - 100	Store LH2	Store liquid hydrogen cryogenically and provide adequate insulation
	LSTO - 200	Provide LH2	Provide the necessary amount of liquid hydrogen to be converted into gaseous form
	LSTO - 300	Provide GH2	Provide gaseous hydrogen to the energy generation system
Auxiliary power system	LAUX - 100	Provide stored electrical energy	Provide electrical energy from the auxiliary energy system
	LAUX - 200	Store electrical energy	Store electrical energy from ground charging, energy generation or electric grid stabilization

Physical level			
Physical component	**Physical function ID**	**Physical function**	**Function description**
Fuel cell stack	PGEN - 100	Provide electrical energy from H2	Electrical energy is generated through the chemical reaction between hydrogen and oxygen
Fuel cell controller	PGEN -200	Control energy generation	Manage the amount of energy generated by the fuel cell through the reactant regulation

Physical level			
Physical component	**Physical function ID**	**Physical function**	**Function description**
Compressor	PGEN - 300	Provide compressed air	Compress the ram air to supply the fuel cell
Compressor inlet valve	PGEN - 310	Regulate air flow	Collect the requested amount of ram air
Compressor dedicated heat exchanger	PTMS - 410	Absorb heat	Absorb the excess heat generated by the air compression
	PTMS - 420	Dissipate heat	Dissipate heat from air thermal management
Humidifier	PGEN - 500	Manage humidity	Regulate the humidity level inside the fuel cell
Air supply valve	PGEN - 510	Adjust air supply	Regulate the amount of air entering the fuel cell
Vapour-liquid separator	PGEN - 610	Separate water from vapour	Manage the output water from the fuel cell to recover vapour and water
Water tank	PGEN - 620	Store water	Contain excess water from the fuel cell
Fuel cell dedicated heat exchanger	PTMS - 100	Absorb heat	Absorb the heat generated by the fuel cell
	PTMS - 200	Provide heat	Provide the heat generated by the fuel cell to the hydrogen conversion process
	PTMS - 300	Dissipate heat	Dissipate the excess heat into the atmosphere
Liquid Hydrogen tank	PSTO - 100	Store LH2	Store liquid hydrogen cryogenically ad provide adequate insulation
Vent valve	PSTO -110	Vent hydrogen	Expel hydrogen in case of pressure rising above tank maximum's limits
Hydrogen tank electrical preheater	PTMS - 120	Heat hydrogen	Provide heat to increase the internal pressure of the tank
Hydrogen pump	PSTO - 200	Provide LH2	Extract the requested amount of hydrogen from the tank to be converted into gaseous form
Hydrogen dedicated heat exchanger	PTMS - 210	Provide heat	Provide heat to hydrogen to reach gaseous state at the target temperature

Physical level			
Physical component	**Physical function ID**	**Physical function**	**Function description**
Valve	PSTO - 300	Provide GH2	Provide gaseous hydrogen at pressures within acceptable limits to the fuel cell and prevent hydrogen flow to the fuel cell in case of upstream failure
Battery and/or supercapacitor	PAUX- 100	Provide stored electrical energy	Provide electrical energy from the battery system
	PAUX - 200	Store electrical energy	Store electrical energy from ground charging, fuel cell energy generation or electric grid stabilization

Table 7. Identification and description of the functions

The failure conditions considered in the analysis can be classified as following:

Failure mode ID	Type of failure	Description
FM 01	Total loss	The function is lost on both the redundant systems
FM 02	Partial loss	The function is lost on only one of the two independent systems
FM 03	Malfunction	The function is being executed but it results an incorrect behaviour; parameters does not comply with requirements
FM 04	Undetected condition	The system or the crew are unaware of a system condition

Table 8. Identification and categorization of the failure modes

The analysis is based on the functions defined in the model and on the functional chains that connects them. It has been conducted on both the logical and the physical level, to determine potential operational and design recommendations.

The analysis has been conducted following the *Guidelines and methods for aerospace for conducting the safety assessment process on civil airborne systems and equipment* provided by the SAE International (17).

It is underlined that in the thesis only the analysis of the system of interest has been provided. Any function which is outside the system of interest is not going to be considered. For greater

readability of the document, all tables are placed at the end in the annexes, and only examples are provided in this chapter.

5.1 Logical level FHA

Even though the physical level analysis provides a more detailed overview of the system with respect to the logical one, it is useful to consider firstly the higher level to develop the analysis step-by-step. Moreover, the logical analysis is independent from the specific physical architecture that can be derived from it, so it remains valid in case a different design configuration is developed on the basis of the previous level.

In this case the functions have been considered by following the logical components they are related to. Failure conditions have been analysed and catalogued into tables describing the following categories:

- Failure mode ID
- Failure mode type
- Phase
- Effect on the airplane
- Classification
- Assumptions
- Preliminary operational mitigation

Table 9 provides an example focused on the analysis of the “provide electrical energy from H2” function, emphasizing the distinction between the severity of a total loss with respect to a partial loss of the function. Both cases lead to a minor severity scenario when the failure occurs during the take-off run before the velocity V1, as it is possible to abort take-off a the aircraft before leaving the ground. Whereas, after V1, the total loss implies a catastrophic event because the energy provided by the auxiliary power systems alone is not enough to perform take-off. When the loss is only partial, the remaining main energy system is instead able to provide enough power to safely take-off and land with a reduction of safety margins. In this case, the scenario is classified as minor for all phases because of the requirement on the capability of the system to conclude the mission safely in case of a partial failure of the main power source. This implies that the system must be designed to fulfil this requirement.

[LGEN – 100] Provide electrical energy from H2						
Failure ID	**Failure**	**Phase**	**Effect**	**Classification**	**Assumptions**	**Preliminary operational mitigation**
FM 01	Total loss of energy supply from H2	Take-off before V1	Loss of power	Minor	The auxiliary energy systems supply the aircraft	The auxiliary energy systems supply the aircraft, RTO if the failure occurs before V1
		Take-off after V1, Climb	Loss of power, inability to perform take-off	Catastrophic	The auxiliary energy systems alone are not able to take-off	The auxiliary energy systems supply the power demand for the onboard systems, abort the mission and land as soon as possible
		Cruise	Loss of power	Catastrophic	The auxiliary energy systems supply for the aircraft for a limited amount of time	See above
		Descent, Landing	Loss of power, energy, energy storage systems charging process is stopped	Catastrophic	The auxiliary energy systems supply for the aircraft for a limited amount of time	See above
FM 02	Partial loss of energy supply from H2	Take-off before V1	Potential loss of power	Minor	The auxiliary systems and the partial main energy system supply the aircraft	The auxiliary energy systems and the partial main energy system supply for the power demand, RTO if the failure occurs before V1
		Take-off after V1, Climb	Potential loss of power	Minor	The auxiliary systems and the partial main energy system are able to take-off	The auxiliary energy systems and the partial main energy system supply for the power demand, abort the mission and land as soon as possible

[LGEN – 100] Provide electrical energy from H2						
Failure ID	**Failure**	**Phase**	**Effect**	**Classification**	**Assumptions**	**Preliminary operational mitigation**
		Cruise	Potential loss of power	Minor	The auxiliary energy systems and the partial main energy system supply the aircraft	See above
		Descent, Landing	Potential loss of power, energy storage systems charging process is stopped	Minor	See above	See above

Table 9. Extract from the logical FHA

5.2 Physical level FHA

The safety assessment conducted of the physical level aims to provide a more detailed analysis of potential critical scenarios. The failure conditions are associated with each component present in the Capella model.

The physical analysis has been conducted with a different approach with respect to the logical level. The functions are considered as elements of the functional chains identified in the model at physical level. The functions are connected by functional exchanges to perform all the necessary actions needed to the system to realize the main capabilities. In this way, it is underlined the connection between the functions and the consequences a failure might have on the functions downstream the one considered. A failure can affect the success of an entire chain.

At physical level, also the potential root cause of the failure is investigated. Examples from different functional chains of the model are described in this section.

Energy control

The amount of energy generated by the fuel cell is determined by the control command imparted from the fuel cell controller. It acts on the hydrogen pump and on the air intake of the compressor. The loss of this signal to start the collection of the reactant for the fuel cell could determine the loss of the power generated. The example provided depicts a failure on one fuel cell controller caused by an internal degradation. However, it could also be generated by a wrong control imparted by the electric grid management.

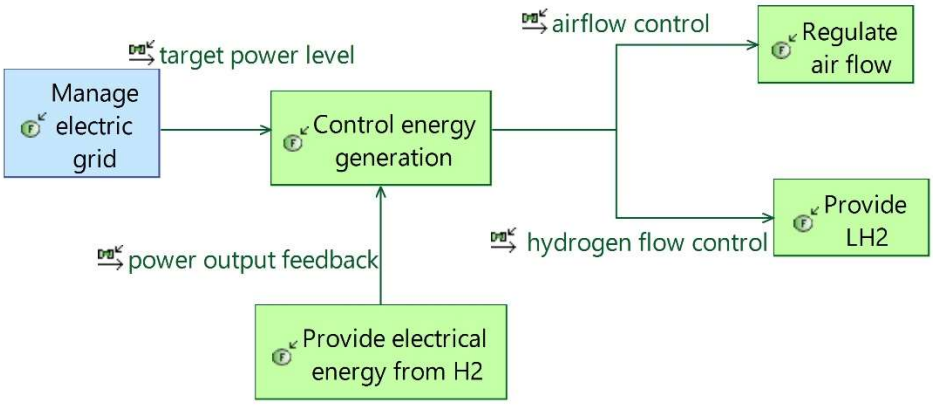

Figure 28. [PFCD] Energy control

[PGEN – 200] Control energy generation						
Failure ID	**Failure**	**Phase**	**Effect**	**Classification**	**Assumptions**	**Preliminary operational mitigation**
FM 02	Partial loss of the reactant supply control function	Take-off before V1	No signal to collect ram air, potential loss of power	Minor	Remaining fuel cell and battery systems supply the power demand	Partial reactant flow is interrupted, RTO if failure occurs before V1
		Take-off after V1, Climb	See above	Minor	Remaining fuel cell and battery systems are able to perform take-off	Partial reactant flow is interrupted, abort the mission and land as soon as possible
		Cruise	See above	Minor	Remaining fuel cell and battery systems supply for the power demand	Partial reactant flow is interrupted, battery systems are activated, abort the mission and land as soon as possible
		Descent, Landing	No signal to collect ram air, potential loss of power, battery systems charging process is stopped	Minor	See above	See above

Table 10. Extract of the physical FHA of the Energy control functional chain

Hydrogen storage and pressure regulation

A critical component of the *Hydrogen storage and pressure regulation* is the hydrogen storage tank which must store and insulate hydrogen at cryogenic conditions. The loss of the storage function might be caused by a leakage or tank rupture and might lead to a loss of power if the fuel feeding process is stopped. LH2 leaks might also cause hazardous effects depending on the nature of the release. In the worst-case scenario, a fire or an explosion might occur (30). Hence, a high level of severity is considered due to the dangerous condition. A distinction has been made between the take-off run before velocity V1 and the other phases of the flight. If a potential explosion occurs on the ground, there is still a chance to stop the aircraft and immediately start emergency operations.

The insulation function might occur due to degradation of the storage tank and cause the loss of the cryogenic condition. Temperature rise and the vent valve system is active to regulate the pressure.

In Table 11, the pressure regulation failure is also analysed. The vent valve is an essential component of the hydrogen storage unit, essential to overcome the boil-off phenomenon. The vent valve can fail in case of a blockage in the vent valve or in the vent line occurs. It can be caused, for instance, by a freezing generated by the contact with cryogenic air.

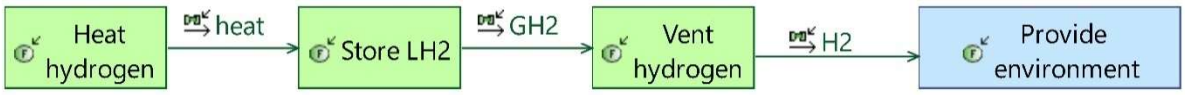

Figure 29. [PFCD] Hydrogen storage and pressure regulation

[PSTO – 100] Store LH2						
Failure ID	**Failure**	**Phase**	**Effect**	**Classification**	**Assumptions**	**Preliminary operational mitigation**
FM 01	Total loss of the hydrogen storage	Take-off before V1	Loss of power, potential fire and explosion	Hazardous	Battery systems supply for power demand	Fuel flow is interrupted, fuel cell systems are shut down, RTO if the failure occurs before V1
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Fuel flow is interrupted, fuel cells systems are shut down, abort the mission and perform emergency landing
FM 01	Total loss of storage tank insulation	Take-off before V1	Temperature rise, pressure rise which requires venting, potential fire and explosion, loss of fuel reserve	Major	The hydrogen tank must maintain insulation at cryogenic condition	Vent system is active, RTO if the failure occurs before V1
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Hazardous	See above	Vent system is active, abort the mission as soon as possible

[PSTO -110] Vent hydrogen						
Failure ID	**Failure**	**Phase**	**Effect**	**Classification**	**Assumptions**	**Preliminary operational mitigation**
FM 01	Total loss of tank venting	Take-off before V1	Boil-off condition, potential explosion	Major	The venting pressure is the maximum allowable pressure for the tank	Fuel is shut off, RTO, power is provided by remaining fuel cell and battery system
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Fuel is shut off, emergency descent and landing, power is provided by remaining fuel cell and battery system

Table 11. Extract of the physical FHA of the Hydrogen storage and pressure regulation functional chain

Hydrogen conversion and supply

The pump in charge of the extraction of the hydrogen from the tank is controlled by the Fuel cell controller. The loss of the hydrogen extraction could prevent the feeding of one the fuel cell and block the energy generation. The pump is a critical component as it is contact with a cryogenic fluid. A blockage or an obstruction into the line could determine the loss of the function.

Figure 30. [PCFD] Hydrogen conversion and supply

[PSTO – 200] Provide LH2						
Failure ID	**Failure**	**Phase**	**Effect**	**Classification**	**Assumptions**	**Preliminary operational mitigation**
FM 01	Total loss of liquid hydrogen extraction from the tank	Take-off before V1	Absence of hydrogen flow, loss of power	Minor	Battery systems supply the aircraft	Reactant flow is interrupted, battery systems supply onboard systems, RTO if failure occurs before V1
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	Battery systems supply the aircraft for a limited amount of time	Reactant flow is interrupted, battery systems supply onboard systems, abort and land as soon as possible

Table 12. Extract from the Hydrogen conversion and supply functional chain

Air supply and regulation

If a failure occurs in the humidifier, an incorrect humidity regulation will affect the fuel cell, potentially causing deterioration during operation. In cases of insufficient humidity, the membrane may become dehydrated, restricting proton movement within the stack. Conversely, an excessive humidity level could result in flooding, thereby reducing electricity generation. The duration of operation under degraded conditions cannot be determined and require detailed consultation with the fuel cell manufacturer. Therefore, the worst-case scenario is assumed, representing a high level of severity. Although the fuel cell is expected to continue operating, the extent of its functionality remains uncertain.

This condition may be caused by the component itself, which could deteriorate over time due to regular usage, or it may result from an incorrect upstream regulation of the vapor supply to the humidifier.

Figure 31. [PFCD] Air supply and regulation

[PGEN -400] Manage humidity						
Failure ID	**Failure**	**Phase**	**Effect**	**Classification**	**Assumptions**	**Mitigation**
FM 03	Failure to provide the correct level of humidity in the fuel cell stack	Take-off before V1	Reduction of the performance of the fuel cell, potential loss of power	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required, RTO
		Take-off after V1, Climb, Cruise, Descent, Landing	Reduction of the performance of the fuel cell, potential loss of power	Major	See above	If the fuel cell degradation exceeds the limits, emergency shutdown is required

Table 13. Extract from the physical FHA of the Air supply and regulation functional chain

Air supply temperature regulation

The air feeding the fuel cell require thermal regulation after the compression. Air enters the heat exchanger and transfer its thermal load to the fresh ram air, which is then dissipated into the atmosphere. A failure in the heat exchanger operation would compromise the correct regulation of the air supply. The excessive temperature in the air entering the fuel cell could cause damage in the stack and reduce the performance.

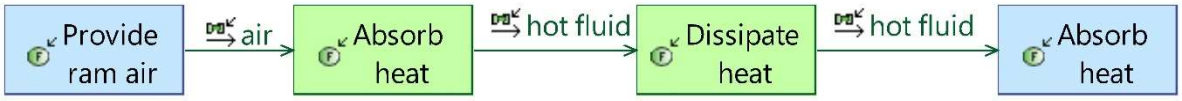

Figure 32. [PFCD] Air supply temperature regulation

[PTMS – 400] Absorb heat						
Failure ID	**Failure**	**Phase**	**Effect**	**Classification**	**Assumptions**	**Preliminary operational mitigation**
FM 03	Failure to regulate air at acceptable temperature range	Take-off before V1	Reduction of the fuel cell performance, potential fuel cell degradation, potential loss of power	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	See above

Table 14. Extract from the physical FHA of the Air supply temperature regulation functional chain

Exhaust Water management

If a failure were to occur on the water tank, it would not have a great impact on the energy generation provided by the fuel cell. However, a potential water dispersion caused by a leakage or the rupture of the tank could damage electrical surrounding components and endanger the reliability of other parts of the architecture. It is indeed recommended to accurately define the position of the storage far from any electrical devices or circuits.

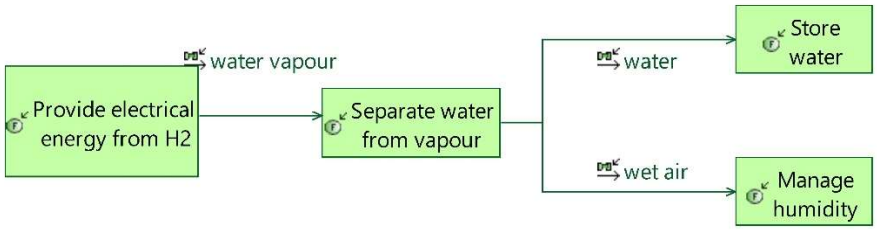

Figure 33. [PFCD] Exhaust water management

[PGEN – 620] Store water						
Failure ID	**Failure**	**Phase**	**Effect**	**Classification**	**Assumptions**	**Preliminary operational mitigation**
FM 01	Total loss of water storage	Take-off before V1	Potential damage in electrical components	Minor	The tank must provide storage and prevent water to damage other systems	Shutdown of electrical components and related systems damaged by the water leak
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	See above

Table 15. Extract from the physical FHA of the Exhaust water management functional chain

TMS: Hot circuit

Another cause of failure of the fuel cell systems leading to the loss of electrical power is the overheating scenario. Not absorbing the heat generated by the fuel cell will damage the stack during operation and cause a reduction of the performance and the power generated. The loss of a heat exchanger is attributable to a leakage, rupture or corrosion of the component.

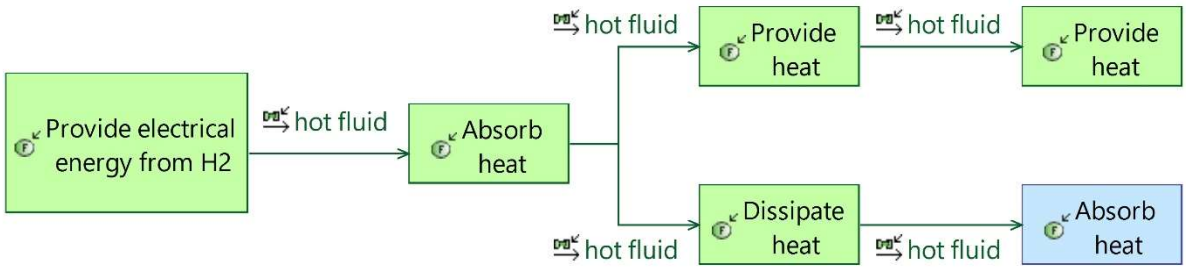

Figure 34. [PFCD] TMS: Hot circuit

[PTMS - 100] Absorb heat						
Failure ID	**Failure**	**Phase**	**Effect**	**Classification**	**Assumptions**	**Preliminary operational mitigation**
FM 02	Partial loss of heat absorption to manage the fuel cell thermal load	Take-off before V1	Overheating of the fuel cell, potential malfunction and damage in the fuel cell	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required, RTO
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	If the fuel cell degradation exceeds the limits, emergency shutdown is required

Table 16. Extract from the physical FHA of the TMS: Hot circuit functional chain

TMS: Cold circuit

The cold circuit deals with the transport of the cooling capacity provided by liquid hydrogen. It is exploited to avoid the overheating of the fuel cell and at the same time to increase the hydrogen temperature before entering the stack. The example provided refers to a potential loss of the work of the heat exchanger dedicated to the fuel cell. Losing such component not only would imply an overheating of the fuel cell but also issues derived from the missing heat load on the hydrogen conversion. Liquid hydrogen which is not properly converted could damage downstream components and moreover, the generation of energy would be compromised. This scenario must be mitigated with the activation of the valve to close the fuel cell feeding line.

Figure 35. [PFCD]TMS: Cold circuit

[PTMS - 200] Provide heat						
Failure ID	**Failure**	**Phase**	**Effect**	**Classification**	**Assumptions**	**Preliminary operational mitigation**
FM 01	Total loss to provide heat for hydrogen conversion	Take-off before V1	Potential freezing of the downstream components, loss of power	Minor	Hydrogen should be heated to the target temperature before entering the fuel cell systems	Reactant flow is interrupted, RTO if failure occurs before V1
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Reactant flow is interrupted, abort the mission and land as soon as possible

Table 17. Extract from the physical FHA of the TMS: cold circuit functional chain

Energy from storage and grid stabilization

The auxiliary power system functions can be fulfilled by battery system or supercapacitor, or both. The present analysis has considered the battery as a reference.

As regards the energy storage function, particular attention is posed on the overheating scenario. Overheating of the battery can be caused by defects in manufacturing or internal shorts generated by dendrites or mechanical stresses. It is the first stage of thermal runway and the containment of this phenomenon is extremely important to avoid heat accumulation and gas release processes and, then, combustion and explosion.

In the table, it is underlined the difference between cruise and the other phases of the flight. It has been observed that the burning rate depends on the environment, the higher the pressure the higher the burning rate of cells. Hence, cruise has been considered has a less severe scenario due to the greater time to reach a thermal runway with respect to the other phases at lower altitudes.

Furthermore, the missed detection of the level of charge of the battery might become a critical condition in case the battery is full. The pilots might not be aware that it is impossible to store energy for the stabilization function. Peaks in the electrical grid will not be absorbed by the battery system.

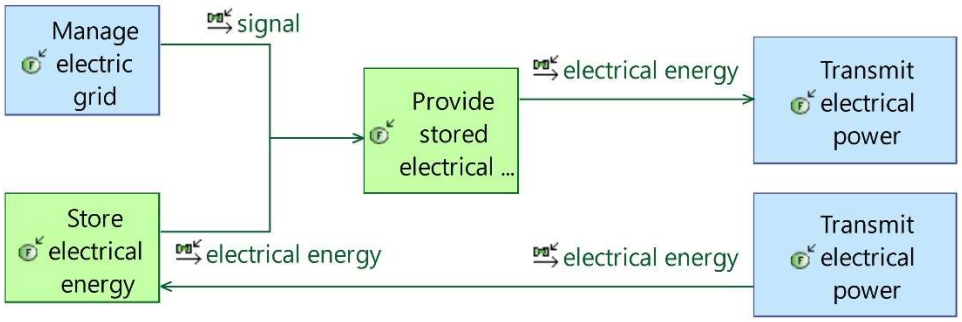

Figure 36. Energy from storage and grid stabilization

[PAUX – 120] Store electrical energy						
Failure ID	**Failure**	**Phase**	**Effect**	**Classification**	**Assumptions**	**Preliminary operational mitigation**
FM 03	Overheating of the battery unit	Take-off, Climb, Descent, Landing	Potential heat accumulation, explosion, Potential loss of the storage system (higher burning rate due to higher pressure)	Hazardous	The battery system has a dedicated thermal management system	Containment of the hazard
		Cruise	Potential heat accumulation, explosion, Potential loss of the storage system	Major	See above	Containment of the hazard
FM 04	Undetected full battery	Descent, Landing	Inability to charge battery	Minor	The system (and the crew) must always be aware of the state of the battery system	Emergency mode in case of go-around, the energy storage system is not charged for take-off
		All phases	Loss of the stabilization function in case of peaks (battery system cannot store more energy)	Minor	The energy storage system must be able to stabilize the grid	The electric grid is able to work in degraded mode within its operation limits

Table 18. Extract from the physical FHA of the Energy storage and grid stabilization functional chain

5.3 Software safety analysis integration

Capella tool has been explored to design the model of the system beyond the Arcadia engineering level. The software includes other functionalities which can be acquired by the introduction of plugins. For instance, Atica4Capella plugin introduces a model-based safety assessment (MBSA) toolbox to perform safety analysis directly on the model developed in the tool. This functionality has been explored to introduce the safety assessment into the model. In particular, the logical level has been replicated exploiting the tool's functionality (31).

Atica4Capella enables the analysis of safety conditions of the functions of the model to comply with the aerospace standards. Failure conditions are defined and described in terms of type of modes, type of failure and severity. Each function can be associated with a failure condition that can be described and categorized according to the parameters highlighted in the analysis.

The tool enables the definition of customized types of failure and severity, which have been defined to reflect the existent logical FHA. Hence, total loss, partial loss, malfunction and undetected conditions are introduced as possible types of failure, whereas the severity has been considered as catastrophic, hazardous, major, minor or with no safety effect. As far as the modes, the flight phases are considered in order to be coherent with the analysis proposed in the previous sections.

An extract of the FHA generated with Atica is proposed to show the characteristics of the tool. Different functional failures are associated with the function "provide electrical energy form H2". The failure conditions are introduced in the model as shown in Figure 38 and each of them is automatically included in a Logical FHA table generated by the software. It is now possible to characterize each scenario with the previously defined categories and provide a description of the effect. In Figure 37, an extract of the table is provided.

	Modes	Failure Type	Effect of functional failure	Severity
Provide electrical energy from H2	[Take-off run (before V1), Take-off, Cruise, Climb, Descent, Landing]			
Failure to generate energy from H2	[Take-off run (before V1), Take-off, Climb, Cruise, Descent, Landing]	Partial loss	Partial loss of energy	Minor
Failure to generate energy from H2	[Take-off run (before V1)]	Total loss	Loss of energy, rejected take-off is required	Minor
Failure to generate energy from H2	[Take-off, Cruise, Climb, Descent, Landing]	Total loss	Loss of energy	Catastrophic

Figure 37. Extract of FHA using Atica4Capella

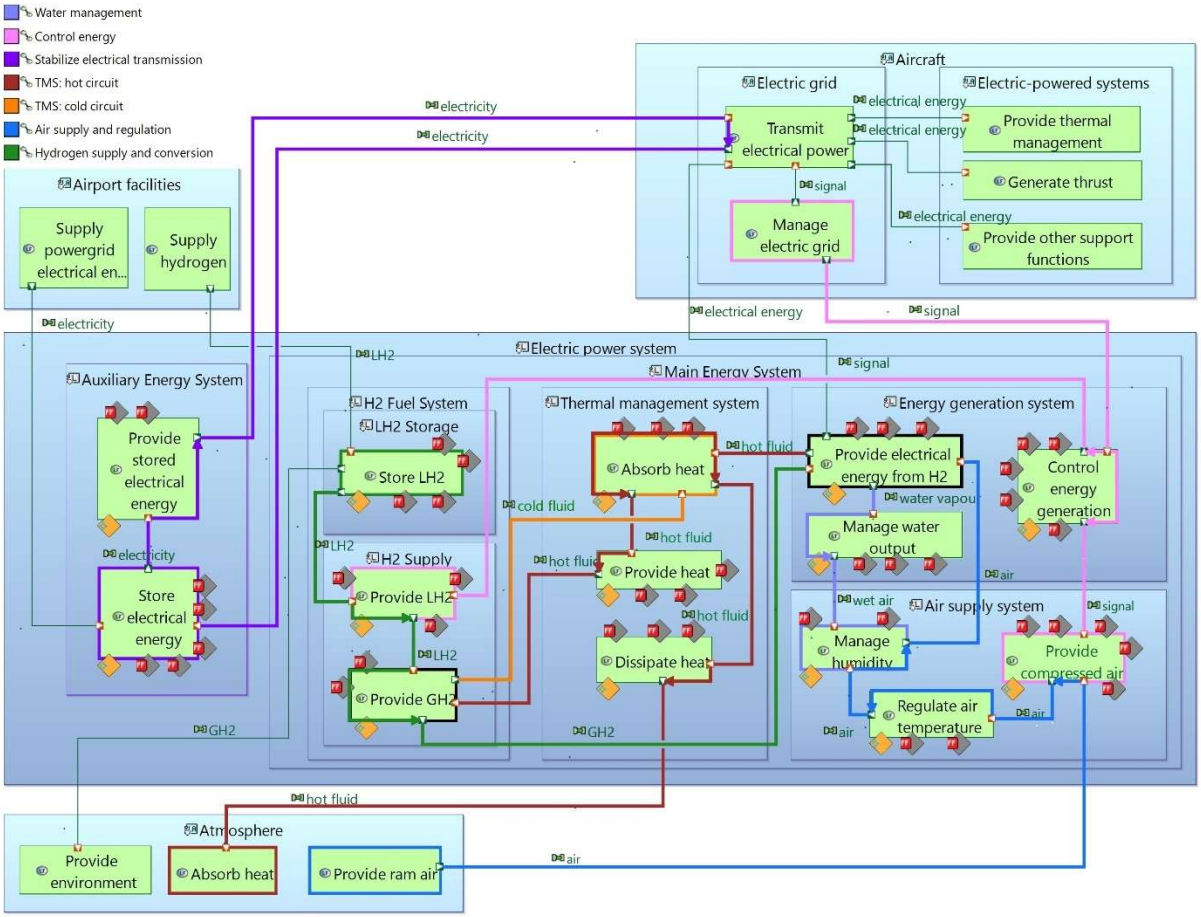

Figure 38. [LAB] Logical architecture blank diagram with failure conditions

6. Results and discussion of the analysis

The Functional Hazard Assessment reveals the most critical components and the failure conditions which might undermine the safety of the mission. The analysis aims to provide a comprehensive overview of potential scenarios in order to derive requirements and design features that enhance project safety.

Although the FHA conducted on the model pertains to an early stage of the design protocol, operational mitigation strategies have been derived to propose preliminary operations that can be done by the system and the crew. It can be observed that failures classified as major or higher severity require landing as soon as possible to abort the mission safely. However, also some scenarios concerning the loss of only one of the fuel cell systems considers the abortion of the mission as an adequate mitigation, even though the classification is defined as “minor” in according to the certifications. It is considered that even if the aircraft is able to complete the mission within safety boundaries by design, such type of loss could lead to critical situation if the remaining part of the system is subjected to another failure.

As anticipated in the introduction, the motivation of the thesis includes the exploration of design requirements derived from the safety assessment. The design proposals are meant to lower the severity associated with potentially dangerous scenarios. Starting from the architecture modelled in Capella, the analysis underlines the criticality which might require the introduction of redundancies, error detection systems, fault containment systems or in some cases, also different approaches to the architecture could be taken into consideration.

6.1 Design recommendations

The assessment can be exploited to identify critical conditions and derive design measures to overcome a potential catastrophe. Some preliminary design recommendations have been developed to support the following phases of the design process.

As expected, dealing with hydrogen entails criticalities and potential failure conditions that must be avoided. One of the most severe aspects is hydrogen storage and the related consequences that a failure might have on the aircraft. The design of the hydrogen tank must be accurate and focused on maximizing safety, in order to prevent any type of leakage that could potentially cause fire and explosion. The choice of material is very important to minimize the phenomenon of embrittlement, in which hydrogen molecules permeate into the structure of the tank making it more and more fragile. The choice of material is also important as far as the

insulation that it must be provided to the liquid hydrogen to maintain the cryogenic conditions stable.

Not only the material has an impact on the quality of the design but also the shape of the tank has a significant role both in terms of structural resistance and boil-off mitigation. Minimizing the surface area for a given volume with spherical tanks could reduce the passive heat into the tank, hence the boil-off of hydrogen (32). Moreover, the tank volume required for the venting must be considered during the design. The redundancy of the vent valve is considered to reduce the probability of severe consequences due to the loss of the venting function.

Furthermore, each main cryogenic pump must be redundant in the system. The need of having a secondary pump to feed the fuel cell is also required according to CS-25.991 (28).

As depicted in the analysis of the functional chains, a potential failure along the hydrogen or the air path to the fuel cell might block one of the reactants to feed the fuel cell or impede the proper regulation of the thermodynamic characteristics that must be ensured before entering the stack. Both chains must include filter components to avoid particle accumulation which might obstruct the components. In addition, any kind of leakage should not interfere with electrical components. This scenario has been highlighted when considering the storage of the water management unit of the fuel cell system. The severity of a potential water leakage can be mitigated by positioning the tank away from any electrical devices.

As far as the fuel cell stack, mitigation strategies on the upstream components are useful to prevent some of the potential degradation processes that might occur in the fuel cell, such as flooding or contamination. However, some precaution measures could also be adopted on the fuel cell to resist mechanical stress and enhance the durability of the component. The study "Research progress of proton exchange membrane failure and mitigation strategies" (33) proposes solutions to increase crack resistance. For instance, the inclusion of edge protection on the electrodes and the membrane is useful to reduce mechanical failure and extend the life of the fuel cell in long-term operations.

It is underlined that the components mounted in the architecture are subject to a wide range of atmospheric conditions. The meteorological characteristics of the airport in which they take-off and land can vary from very hot to very cold environment. Furthermore, the external conditions are not the same during the phases of the flight. The components must be designed to resist to thermal and mechanical stress and be adequate for the fluid they will be in contact with.

Moreover, the heat transfer for the hydrogen conversion cannot be performed by a conventional fluid, which might freeze when in contact with cryogenic temperatures. Liquid helium, for instance, represent a valuable solution because it can operate at cryogenic conditions.

Concerning the auxiliary energy system, battery design recommendations are identified. A lower level of severity can be achieved by the correct installation of the battery system. It should not be too close to any heat sources, fluids or hazardous materials (34). Moreover, the role of thermal management is very important to maintain the battery temperature level within its boundary (15°C – 35°C) to reduce deterioration and guarantee the performance along its life (35). The thermal management system of the battery unit has not been characterized in the model because it has not been considered part of the system of interest. However, its role is fundamental to guarantee the correct heat management during charging and discharging cycles. Heat might also increase due to exposure to external sources or internal short circuits. As depicted in the FHA analysis, overheating condition is very hazardous because if not circumscribed it could lead to a thermal runway. Once the heat accumulation and gas release have started, the phenomenon might be controlled with a cell-venting mechanism to release the gas in a controlled manner. In any case, if the combustion and explosion stage arise, the activation of fire protection systems are essential to prevent the propagation of the fire (36). Finally, detection systems could be installed to be aware of the state of the battery and avoid failure conditions.

6.2 Comparison between different architectural configurations

The Functional Hazard Assessment has been conducted on the aircraft architecture which has been developed in the project and presented in section 4.2. The Electric power system is considered as the composition of two redundant systems that include both the main and the auxiliary energy units. The two parts of the system have been considered as physically independent one from the other. Hence, a partial failure on one side of the aircraft does not affect the other redundant components (except from a major fire or explosion which might spread all over the airframe). This configuration is not the only feasible solution which complies with the high-level requirements of the reference vehicle, but different design choices could have been selected. In this paragraph, other possible configurations are going to be analysed to provide information for future design trade-offs. The proposals are not going to consider any

change in the number of components and redundancies, to comply with safety requirements, but include some possible synergies among the systems.

Cross-feed of the hydrogen storage with the fuel cell units

A cross connection between systems can be considered to reduce the severity of a partial loss of one of the functions regarding energy generation components and hydrogen storage. The architecture is inspired from conventional aircraft fuel system, in which fuel can be transferred between tanks and it is used to feed the engine on the opposite side of the aircraft in the event that a malfunction occurs. In this case, connecting lines between the liquid hydrogen tank and the opposite fuel cell systems are included with the aim of increasing the safety level of the aircraft.

For instance, if a failure takes place in one of the components of the fuel cell system and leads to the loss of one of the main energy systems, the hydrogen contained in the dedicated hydrogen tank can still be used to feed the remaining fuel cell. This connection enhances the level of safety of the aircraft as all the transported fuel remains available to produce electric energy. In the event of a go-around scenario, the total remaining supply of hydrogen will be readily available. Moreover, the cross connection could result advantageous regarding the weight distribution along the structure of the aircraft, which would be unequal in case only the fuel of one side of the aircraft was being consumed.

On the other hand, an additional line entails complexity in the system and weight, which is not to be neglected in aviation. The complexity is also increased by the fact that the fuel is stored at cryogenic conditions.

Similar assumptions might be considered in case a failure in one hydrogen tank occurs. The fact that both fuel cell systems could be supplied by the remaining tank implies a greater level of safety because a potential failure of the opposite fuel cell system would not leave the aircraft without its main energy source.

Even in this case, a trade-off between the higher level of safety and the implications a complex system entails are mandatory to find a compromise between the weight penalty and the advantages that a cross-feed architecture carries to the design.

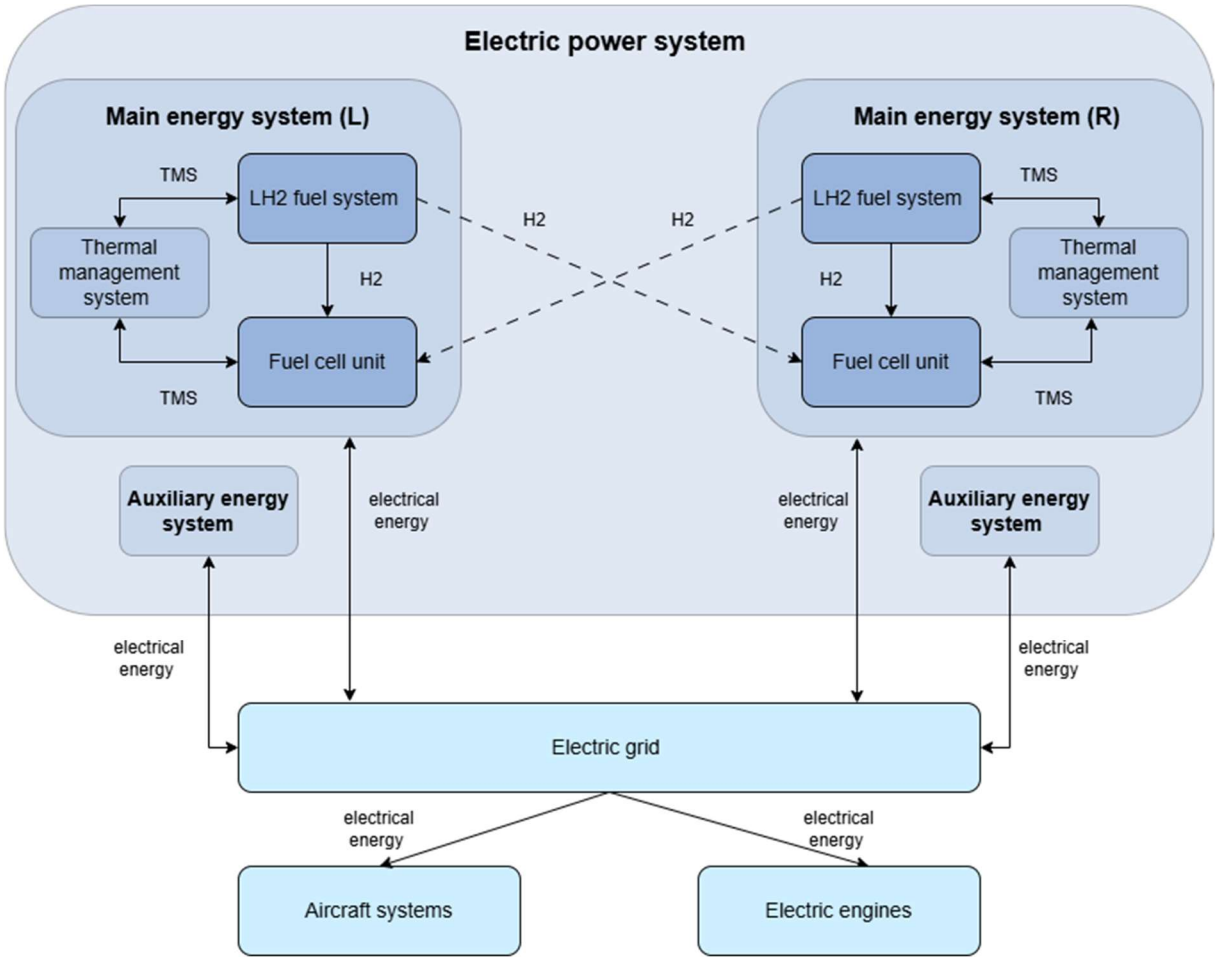

Figure 39. Aircraft configuration with LH2 tank system cross-feed

Battery synergistic thermal management system

An alternative synergy solution to consider in the model regards the thermal management of the auxiliary energy system. It has been assumed that thermal load generated by the battery during operation is managed by an independent system which is not part of the main analysis. It must provide the correct thermal regulation to maintain the battery within the optimal temperature range to work properly.

A feasible configuration could include the battery thermal management in the synergistic TMS dedicated to the fuel cell unit and hydrogen conversion. In this way, the regulation could exploit the thermal load already in use in the system. The complexity of the architecture might increase, but the weight might be lowered thanks to the integration of the system into an existing component.

This solution might result more efficient, but, in terms of the failure analysis, a dependency in the systems undermine the safety level of the system. If a failure were to occur to the hydrogen tank or to the hydrogen dedicated heat exchanger, not only the thermal management of the fuel cell will be lost (the fuel cell is not going to operate without hydrogen anyway), but also the battery system one.

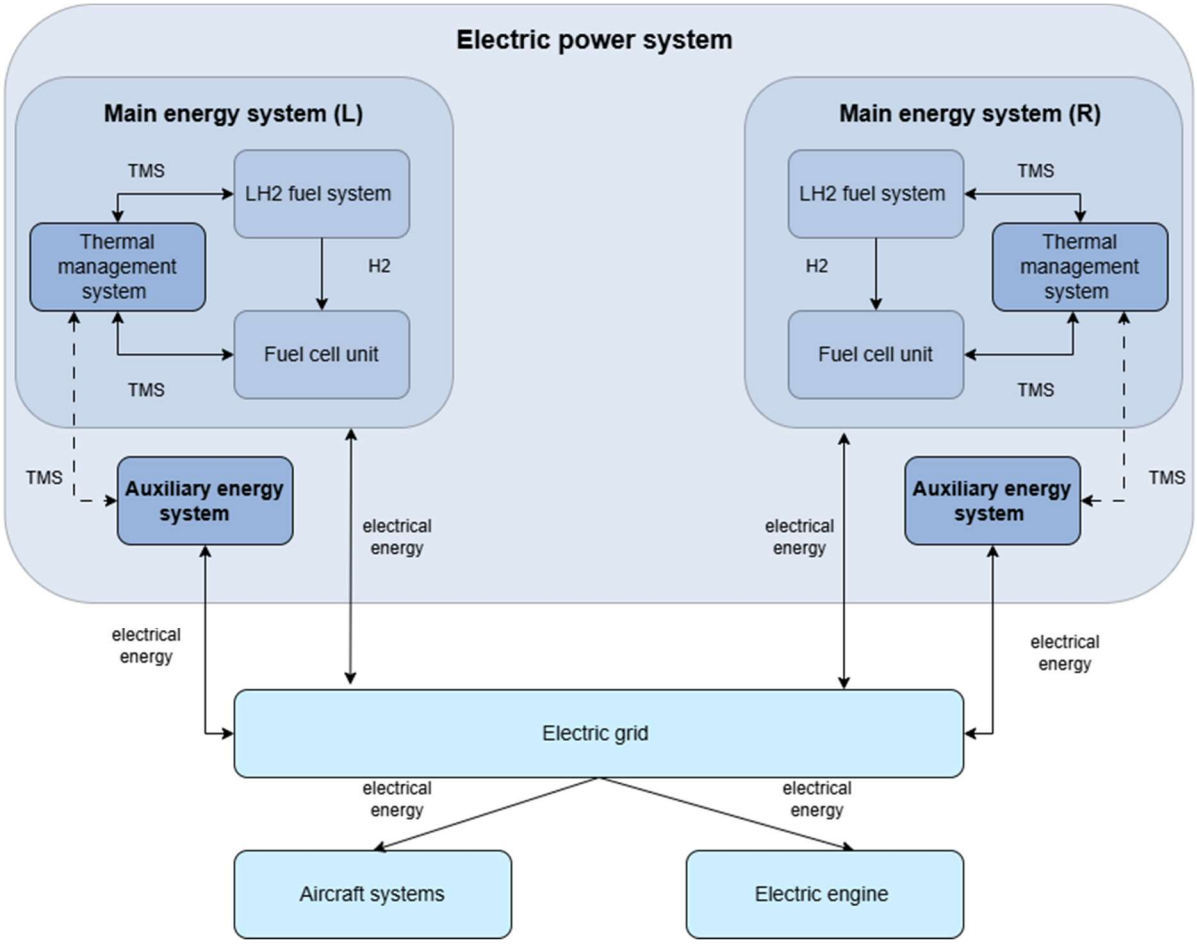

Figure 40. Aircraft configuration with synergistic battery thermal management system

6.3 Final Discussion

By employing the Arcadia methodology and its tool Capella, it has been possible to develop the functional architecture of the reference aircraft, which is not directly related to any existing conceptual design. It embraces different conceptual studies to represent a potential aircraft

configuration to be developed to contribute to the industry's zero-emission challenge. The model does not aim to include all the physical components that would be included in a detailed design of the system. It focuses on the main elements that are going to be the subject of the failure scenario analysis.

The scope of the project is the analysis of the level of safety of a reference architecture to provide information for future design choices. The aim is not to give results and solutions but to offer documentation to contribute to the definition of those solutions. This is the reason why this type of safety assessment is integrated into design process starting from the early stages of its development. The role of the work is also to provide insight to better understand the extent in which design solutions are derived from the safety analysis. The thesis starts posing questions on what types of recommendations could be derived from such safety assessment.

6.3.1 Results discussion

As described in the previous sections, preliminary operational mitigations can be determined. These considerations are limited by the fact that, at this early stage, the detailed behaviour of the components is not known. Each component will have characteristics coming from the manufacturer. For example, when a malfunction influences the state of a components and a degraded mode is indicated, at this stage it is difficult to have an esteem of how the degradations of the element will proceed and for how much time it will keep working within safety limits. This is the reason why in such cases the worst-case scenario is always being considered. However, in other cases the loss of a function could be categorised by an elevated level of severity which can only be mitigated by landing as soon as possible.

As far as design recommendations, some redundancies and dissimilarities have been identified. As occurred for the preliminary operational mitigations, in some cases the recommendations are more general and must be adapted at the future configuration that will be developed. It is stressed the importance of being aware of the state of the systems and monitoring its operation. Redundancies are extremely relevant to avoid catastrophic scenarios, but also different ways to provide a function are explored. One of the most important aspects is considering the environment in which the system will work, which ranges from very different conditions along the mission.

6.3.2 Embraer's feedback

The work has been revised by the subject matter experts from Embraer to provide feedback on the effectiveness of the project. The MBSE methodology applied on the model has stated all the interaction throughout the engineering level. In particular, the logical architecture has captured the main point by giving a functional and holistic approach view of the system of interest. As far as the FHA development, it has been suggested to focus only on one of the levels to improve consistency in the classification of the analysis. The design recommendations have provided some additional insights into the fuel cell system integration and substantiate the firm's knowledge regarding hydrogen fuel cells systems. Finally, the interactions and discussions carried on during the meeting are considered as enriching and useful to provide a better understanding of the interfaces of the electric power system in hydrogen fuel cell aircraft.

6.3.3 Future recommendations

The Functional Hazard Assessment gives a high-level panorama of the potential fault scenarios that can affect the mission and endanger the people inside and outside the aircraft.

During the future design process, the insight identified in the thesis might be useful to perform trade-offs of the new architectural solutions. The introduction of hydrogen in the aviation industry entails technological challenges to overcome. High-level of safety must be guaranteed to enhance the development this type of vehicles from prototypes to civil air transport.

As stated, the scope of the thesis is the development of the model of the system dedicated to the energy supply of the aircraft and the performance of the Functional Hazard Assessment on the defined architecture. The FHA process is only one of the first steps to analyse the compatibility of safety requirements with the design into consideration. In Figure 3, the V-diagram shows the processes to be performed, related to all the stages of the design. In particular, it is underlined the importance of conducting the FHA at aircraft-level. The level of detail is lower with respect to the system-level, but this type of study gives a different insight regarding the integration among different systems and the consequences of a single system failure to the other ones. Moreover, in the analysis each failure condition in a determined phase of the flight has been associated with a level of severity according to the characteristics of the effect on the aircraft presented in Table 1. It can be noticed that some of the scenarios presented are described with a "Catastrophic" level of severity. A such serious potential condition could not be accepted in the design of the aircraft if it were not for the extremely high probability of that event. If the

possibility of such event is remote, the configuration passes the safety requirements. Otherwise, the measures to overcome the worst level of severity would be limiting the realization of the design. The number of redundancies and reinforcement on the components would be uselessly elevated and deteriorate the performances and the feasibility of the project due to the excessive weight. Accepting a potentially catastrophic event does not mean that the design is unsafe because the probability of such event to happen is below the safety requirements to categorize the configuration as safe. Furthermore, the probability of an event, called the Primary event, to happen depends on the probability of occurrence of other failures connected to the event under analysis and must be below the requested requirement. This type of study can be developed in the Fault Tree Analysis (FTA), a top-down procedure useful to determine undesired events and related causes. This methodology represents the next step to be performed after the FHA.

Furthermore, the tool Capella could be used to provide an integrated Functional Hazard Analysis by using software plugin, like Atica4Capella. As shown in section 5.3 the safety analysis could be performed directly on the system of interest and support the development of the complex system. Information and traceability of the work could be managed by a single instrument to enhance the collaboration between system engineers and safety specialists (31).

7. Conclusion

The thesis aims to contribute to the existing research landscape supporting the development of sustainable air mobility, seeking to provide an analysis that could be useful for the design process of aircraft similar to the model under consideration.

The Arcadia MBSE methodology has been employed to develop a functional model of the Electric power system of a regional aircraft powered by liquid hydrogen PEM fuel cells. Arcadia's dedicated software tool, Capella, has been used to define the architecture starting from the operational level and then focusing on the potential physical development of the system of interest: the Electric power system. The model focuses on the definition of the functions that the system must comply with to perform safe flight powered by a zero-emission power system. It is important to define all the connections between the components and their role in the architecture. PEM fuel cells are the main source of energy of the aircraft by producing electricity with the reaction of hydrogen and oxygen. Hydrogen is stored in liquid form at cryogenic conditions to reduce the volume of the tank. This type of storage solution requires the conversion of the hydrogen into gaseous form before entering the fuel cell. A dedicated thermal management system is developed to exploit the cold temperatures of the cryogenic hydrogen to cool the fuel cell system and the heat load generated by the fuel cell during operation to raise the hydrogen temperature. In addition, the other reactant of the fuel cell, oxygen, is provided by the collection of ram air from the atmosphere, which is compressed, and thermally regulated to reach the correct condition to enter the fuel cell. Before feeding the stack, humidity level of the air is controlled by using the water output generated by the fuel cell.

The functional model is the subject of the safety analysis to provide safety considerations useful for the design. A Functional Hazard Assessment has been developed to determine failure conditions associated with the functions of the system. Each failure scenario has been analysed considering the effect on the airplane in different phases of the flight and the severity classification has been derived. Preliminary operational mitigations are identified to clarify the possible actions to be taken by the system and the crew to deal with the failure condition.

Moreover, the resulting failure conditions have been considered to provide some design recommendations to lower the level of severity by providing solutions to strengthen the design and lowering the probability of the failure to happen. Components that result having a crucial role in the success of a functional chain are identified and research on to find potential solutions to overcome the critical result in case of failure. Redundancies and instructions are provided to

be integrated into future design discussion to offer insights to inspire the project. Redundant components are suggested for those elements that could lead to the loss of the downstream function. However, not all the components should be duplicated in the architecture to avoid an unnecessary weight penalty. For example, the position inside the aircraft of critical devices, the shape of the tanks and the choice of the right material for the application are, for instance, valuable recommendations to be taken into account in the design process.

The entire project has been supervised by subject matter experts from Embraer company and its subsidiary Airholding. Their constant collaboration has been essential to capture the right direction of the work and validate it. The expertise they provided in different fields has been a key element to improve the quality of the model and the analysis. On the other hand, the project has been developed to become a resource for current and future research by furnishing different insights and recommendation to contribute to the path of a more sustainable air transport.

8. References

1. M. Dareki, I. King, C. Edelstenne, P. Ky, T. Edelstenne, M. Mathieu, E. Fernandez, G. Orsi, P. Hartman, G. Schotman, J.P. Herteman, C. Smith, M. Kerlloh, J.D. Worner. *Flightpath 2050. Europe's vision for aviation*. 2011.

2. Kabeyi, Moses Jeremiah Barasa. *Fuel cells design, operations and applications*. 2023.

3. Saurav Tiwari, Micheal J. Pekris, John J. Doherty. *A review of liquid hydrogen aircraft and propulsion technologies*. 2023.

4. Talal Yusaf, Abu Shadate Faisal Mahamude, Kumaran Kadirgama, Devarajan Ramasamy, Kaniz Farhana, Hayder A. Dhahad, ABD Rahim Abu Talib. S*ustainable energy in aviation - A narrative review.* 2022.

5. Hoogerdijk, T.L.C. *Aircraft integration of air-based thermal management systems for propulsive fuel cell systems.* 2023.

6. *Embrear Future air concepts*. [Online] https://embraercommercialaviationsustainability.com/concepts/.

7. CEI. I*ntroduction, MBSE*. 2020.

8. Claude Baron, Lorenzo Grenier, Vitalina Ostapenko, Rui Xue. *Using the ARCADIA/Capella Systems Engineering Method and Tool to Design Manufacturing Systems—Case Study and Industrial Feedback*. 2023.

9. George, Mathew Prince. *Model-Based System Engineering Methodology for Implementing Networked Aircraft Control System System on Integrated Modular Avionics - Environmental Control System Case Study.* 2019.

10. ROQUES, Pascal. M*BSE with the ARCADIA Method and the Capella Tool*. 2016.

11. Carrie, Matthieu. *Autonomic framework for safety management in the autonomous vehicle*. 2019.

12. CEI. *ARCADIA Primer.*2020

13. *Capella.* [Online] https://mbse-capella.org/.

14. Stéphan Bonnet, Jean-Lu Voirin, Daniel Exertier Véronique Normand. *Modeling system modes, states, configurations with Arcadia and Capella: method and tool perspectives*. 2017.

15. Max Cichocki, Christian Landschutzer, Hannes Hick. *Development of a sharing concept for industrial compost turners using Model-Based Systems Engineering, under consideration of technical and logistical aspects* . 2022.

16.SAE Aerospace. *Guidelines for Development of Civil Aircraft and Systems*, ARP-4754.

17. SAE Aerospace. G*uidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, ARP-4761*.

18. *What is Functional Hazard Assessment and how to perform it?* DMD Solutions. [Online] https://dmd.solutions/blog/2023/12/19/what-is-functional-hazard-assessment/.

19. Tim Hoff, Florian Becker, Alireza Dadashi, Kai Wicke, Gerko Wende. *Implementation of Fuel Cells in Aviation from a Maintanance, Repair and Overhaul Perspective.* 2022.

20. Kristina Kossarev, Anna Elena Scholz, Mirko Hornung. *Comparative environmental life cycle assessment and operating cost analysis of long-range hydrogen and biofuel fueled transport aircraft*. 2022.

21. Stefan Kazula, Martin Staggat, Stefanie de Graaf. *Functional and Safety Challenges of Hydrogen Fuel Cell Systems for Application in Electrified Regional Aircraft*. 2023.

22. Dimitrios Dimos, Stefanie de Graaf. *Overview of safety challenges associated with integration of hydrogen-based propulsion systemsfor climate neutral aviation*. 2024.

23. *FutPrInt50: project overview*. [Online] https://futprint50.eu/about/project-overview.

24. Ricardo dos Reis, Felipe Odaguil, Evert Windels, Yorick Teeuwen, Jenny van der Pols, Panagiotis Laskaridis, Dominique Bergmann, Dominik Eisenhut, Nicolas Moebs. *Deliverable 2.1 Requirements and Reference Aircraft, Future propulsion and integration: towards a hybrid-electric 50-seat regional aircraft*. 2021.

25. W. Affonso Jr., R. T. Tavares, F. R. Barbosa, R. Gandolfi, R. J. N. dos Reis, C. R. I. da Silva, T. Kipouros, P. Laskaridis, H. Balaghi Enalou, A. Chekin, A. Kurovinets, K. Gubernatorov, Y. Ravikovich, N. Ivanov, L. Ponyae, D. Holobtsev. *System architectures for thermal management of hybrid-electric aircraft - FutPrint50*. 2022.

26. Valentine Habrard, Ion Hazyuk Jr., Valérie Pommier-Budinger, Joel Jézégou, Emmanuel Bernard. *Sensitivity Analysis and Optimization of a Liquid Cooling Thermal Management System for Hybrid Fuel Cell Aircraft*. 2023.

27. Shuangqi Li, CHenghong Gu, Pengfei Zhao, Shuang Cheng. *A novel hybrid propulsion system configuration and power distribution strategy for light electric aircraft.* 2021.

28. EASA. *Certification Specification for large airplanes*

29. Pia Hoenicke, Debjani Ghosh, Adel Muhandes, Sumatra Bhattachrya, Christiane Bauer, Josef Kallo, Caroline Willich. *Power management control and delivery module for a hybrid electric aircraft usign fuel cell and battery.* 2021.

30. P G Holborn, J M Ingram, CB Benson. *Modelling studies of the hazards posed by liquid hydrogen use in civil aviation.* 2022.

31. *Atica4Capella* . [Online] https://www.anzenengineering.com/anzen-wiki/atica4capella/introduction/.

32. Subodh K. Mital, John Z. Gyekenyesi, Steven M. Arnold, Roy M. Sullivan, Jane M. Manderscheid, Pappu L.N. Murthy. *Review of current state of the art and key design issues with potential solutions for liquid hydrogen cryogenic storage tank structures for aircraft applications*. 2006.

33. Yijing Xing, Haibin Li, George Avgouropoulos. *Reasearch progress of proton exchange membrane failure and mitigation strategies*. 2021.

34. Malinge, Yannik. *Safery first. Lithium batteries: safe to fly? The airbus safety magazine* . 2016.

35. Majid Asli, Paul König, Dikshant Sharma, Evangelia Pontika, Jon Huete, Karunakar Reddy Konda, Akilan Mathiazhagan, Tianxiao Xie, Klaus Höschler, Panagiotis Laskaridis. *Thermal management challenges in hybrid-electric propulsion aircraft*. 2023.

36. Shashank Sripad, Alexander Bills, Venkatasubramanian Viswanathan. *A review of safety considerations for batteries in aircraft with electric propulsion.* 2021.

37. Soccimaro, Antonio. *Preliminary design methods for the themal management of fuel cell powered aeroengines (Master thesis)*. 2023 .

38. *Model-based system engineering methodology for implementing networked aircraft control system on integrated modular avionics - Environmental control system case study.* Mathew, Prince George. 2019.

9. Annexes

9.1 Annexes 1: Logical FHA

Logical component	Function ID	Function	Function description
Main energy system – Energy generation system	LGEN-100	Provide electrical energy from H2	Electrical energy is generated through the chemical reaction between hydrogen and oxygen

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 01	Total loss of energy supply from H2	Take-off before V1	Loss of power	Minor	The auxiliary energy systems supply the aircraft	The auxiliary energy systems supply the power demand of the onboard systems, RTO if the failure occurs before V1
		Take-off after V1, Climb	Loss of power, inability to perform take-off	Catastrophic	The auxiliary energy systems are not able to take-off	The auxiliary energy systems supply the power demand for the onboard systems, abort the mission and land as soon as possible
		Cruise	Loss of power, limited amount of power reserve	Catastrophic	The auxiliary energy systems supply the aircraft for a limited amount of time	See above
		Descent, Landing	Loss of power, energy storage systems charging process is stopped, inability to perform take-off in case of go-around scenario	Catastrophic	See above	See above

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 02	Partial loss of energy supply from H2	Take-off before V1	Potential loss of power	Minor	The remaining main energy and auxiliary energy systems supply the aircraft	The remaining main energy and auxiliary energy systems supply the power demand, RTO if the failure occurs before V1
		Take-off after V1, Climb	Potential loss of power	Minor	The remaining main energy and auxiliary energy systems are able to take-off	The remaining main energy and auxiliary energy systems supply the power demand, abort the mission and land as soon as possible
		Cruise	Potential loss of power	Minor	The remaining main energy and auxiliary energy systems supply the aircraft	See above
		Descent, Landing	Potential loss of power, auxiliary energy systems charging process is stopped, limited amount of power in case of go-around scenario	Minor	See above	See above

Logical component	Function ID	Function	Function description
Main energy system – Energy generation system	LGEN-200	Control energy generation	Regulate the amount of energy that must be generated

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 01	Total loss of energy control function	Take-off before V1	Loss of power, the control logic does not start or command on the generation process	Minor	Auxiliary energy systems are able to supply the aircraft	Energy generation system is shut off, the auxiliary energy systems supply for the power demand, RTO if the failure occurs before V1
		Take-off after V1, Climb	See above	Catastrophic	Auxiliary energy systems alone are not able to perform take-off	Energy generation system is shut off, the auxiliary energy systems supply for the power demand, abort the mission and land as soon as possible
		Cruise	See above	Catastrophic	Auxiliary energy systems are able to supply for the aircraft for a limited amount of time	See above
		Descent, Landing	Loss of power, the control logic does not start or command on the generation process, auxiliary energy systems charging process is stopped	Catastrophic	See above	See above

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 02	Partial loss of energy control function	Take-off before V1	Potential loss of power	Minor	Remaining main energy and auxiliary energy systems supply the aircraft	Remaining main energy system is shut off, the auxiliary energy system supply for the power demand, RTO if the failure occurs before V1
		Take-off after V1, Climb	Potential loss of power	Minor	Remaining main energy and auxiliary energy systems are able to perform take-off	Remaining main energy system is shut off, the auxiliary energy system supply for the power demand, abort the mission and land as soon as possible
		Cruise	Potential loss of power	Minor	Remaining main energy and auxiliary energy systems supply the aircraft	See above
		Descent, Landing	Potential loss of power, auxiliary energy systems charging process is stopped	Minor	See above	See above
FM 03	Erroneous control action on the energy generation system	Take-off before V1	Potential malfunction and damage in the energy generation system, potential loss of power	Minor	Energy generation system is able to work in degraded mode with its operation limits	If the energy generation system degradation exceeds the limits, emergency shutdown is required, RTO
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	If the energy generation system degradation exceeds the limits, emergency shutdown and emergency landing

Logical component	Function ID	Function	Function description
Main energy system – Energy generation system	LGEN-300	Provide compressed air	Compress ram air to supply the energy generation system

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 01	Total loss of air supply to energy generation system	Take-off before V1	Air supply systems do not feed the energy generation system, potential loss of power	Minor	The auxiliary energy systems supply the aircraft	Reactant flow is stopped, the auxiliary energy systems supply the power demand, RTO if the failure occurs before V1
		Take-off before V1	See above	Catastrophic	The auxiliary energy systems are not able to take-off	Reactant flow is stopped, the auxiliary energy systems supply for the power demand for a limited amount of time
		Cruise	See above	Catastrophic	The auxiliary energy systems supply the aircraft	Reactant flow is stopped, the auxiliary energy systems supply power demand for a limited amount of time
		Descent, Landing	Air supply systems do not feed the energy generation system, potential loss of power, auxiliary energy systems charging process is stopped	Catastrophic	See above	See above

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 02	Partial loss of air supply to energy generation system	Take-off before V1	Air supply system does not feed the fuel cell, potential loss of power	Minor	Remaining main energy and auxiliary energy systems supply the aircraft	Remaining main energy and auxiliary energy systems supply for the power demand, RTO if the failure occurs before V1
		Take-off before V1	See above	Minor	Remaining main energy and auxiliary energy systems are able to take-off	Remaining main energy and auxiliary energy systems supply for the power demand
		Cruise	See above	Minor	Remaining main energy and auxiliary energy systems supply the aircraft	See above
		Descent, Landing	Air supply system does not feed the fuel cell, potential loss of power, auxiliary energy systems charging process is stopped	Minor	See above	See above
FM 03	Erroneous air supply to energy generation system (higher air level, lower air level, air supplied in the wrong pressure/temperature condition	Take-off before V1	Potential malfunction and damage in the fuel cell system, potential loss of energy generation	Minor	Energy generation system is able to work in degraded mode with its operation limits	If the energy generation system degradation exceeds the limits, emergency shutdown is required, RTO
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	If the energy generation system degradation exceeds the limits, emergency shutdown and emergency landing

Logical component	Function ID	Function	Function description
Main energy system – Energy generation system	LTMS-400	Regulate air temperature	Manage the air temperature to supply the energy generation system

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 03	Erroneous thermal regulation of the air supply	Take-off before V1	Potential malfunction and damage in the energy generation system, potential loss of power	Minor	Energy generation system is able to work in degraded mode with its operation limits	If the energy generation system degradation exceeds the limits, emergency shutdown is required, RTO
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	If the energy generation exceeds the limits, emergency shutdown is required, abort the mission and land as soon as possible

Logical component	Function ID	Function	Function description
Main Energy System – Air supply system	LGEN – 500	Manage humidity	Regulate the humidity level inside the energy generation system

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 03	Erroneous level of humidity (too humidity/low humidity)	Take-off before V1	Potential malfunction and damage in the energy generation system, potential loss of power	Minor	Energy generation system is able to work in degraded mode with its operation limits	If the energy generation system degradation exceeds the limits, emergency shutdown is required, RTO
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	If the energy generation system degradation exceeds the limits, emergency shutdown and emergency landing

Logical component	Function ID	Function	Function description
Main energy system – Thermal management system	LGEN – 600	Manage water output	Manage the water exiting the fuel cell to provide vapour for humidity regulation

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 01	Total loss of water management	Take-off before V1	Potential improper humidification, potential deterioration of the energy generation system	Minor	Energy generation system is able to work in degraded mode with its operation limits	If the energy generation system degradation exceeds the limits, emergency shutdown is required, RTO if failure occurs before V1
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	If the energy generation system degradation exceeds the limits, emergency shutdown is required, abort the mission and land as soon as possible
FM 02	Partial loss of heat absorption to manage energy generation system thermal load	Take-off before V1	Potential improper humidification, potential deterioration of the energy generation system	Minor	Energy generation system is able to work in degraded mode with its operation limits	If the energy generation system degradation exceeds the limits, emergency shutdown is required, RTO if failure occurs before V1
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Minor	See above	If the energy generation system degradation exceeds the limits, emergency shutdown is required, abort the mission and land as soon as possible

Logical component	Function ID	Function	Function description
Main energy system – Thermal management system	LTMS – 100	Absorb heat	Absorb heat generated by the energy generation system

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 01	Total loss of heat absorption to manage energy generation system thermal load	Take-off before V1	Overheating of the energy generation system, potential malfunction and damage in the system	Minor	Energy generation system is able to work in degraded mode with its operation limits	If the energy generation system degradation exceeds the limits, emergency shutdown is required, RTO if failure occurs before V1
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Hazardous	See above	If the energy generation system degradation exceeds the limits, emergency shutdown is required, abort the mission and land as soon as possible
FM 02	Partial loss of heat absorption to manage energy generation system thermal load	Take-off before V1	Overheating of the energy generation system, potential malfunction and damage in the system	Minor	Energy generation system is able to work in degraded mode with its operation limits	If the energy generation system degradation exceeds the limits, emergency shutdown is required, RTO if failure occurs before V1
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Minor	See above	If the energy generation system degradation exceeds the limits, emergency shutdown is required, abort the mission and land as soon as possible

Logical component	Function ID	Function	Function description
Main energy system – Thermal management system	LTMS – 200	Provide heat	Provide the heat generated to the hydrogen conversion process

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 01	Total loss to provide heat for hydrogen conversion	Take-off before V1	Potential freezing of downstream components, loss of power	Minor	Hydrogen should be heated to the target temperature before entering the energy generation system	Reactant flow is interrupted, emergency shutdown is required, RTO if failure occurs before V1
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Reactant flow is interrupted, emergency shutdown is required, abort the mission and land as soon as possible
FM 02	Partial loss to provide heat for hydrogen conversion	Take-off before V1	Potential freezing of downstream components, potential loss of power	Minor	Hydrogen should be heated to the target temperature before entering the energy generation system	Partial reactant flow is interrupted, abort the mission and land as soon as possible
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Minor	See above	See above

Logical component	Function ID	Function	Function description
Main energy system – Thermal management system	LTMS – 300	Dissipate heat	Dissipate the excess heat into atmosphere

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 01	Total loss of heat dissipation	Take-off before V1	Overheating of the system, potential damage and reduction of performance	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the energy generation system degradation exceeds the limits, emergency shutdown is required
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	See above
FM 02	Partial loss of heat dissipation	Take-off before V1	Overheating of the system, potential damage and reduction of performance	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the energy generation system degradation exceeds the limits, emergency shutdown is required
		Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	See above

Logical component	Function ID	Function	Function description
Main energy system – LH2 fuel system	LSTO – 100	Store LH2	Store liquid hydrogen cryogenically and provide insulation

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 01	Total loss of storage function	Take-off before V1	Potential unsafe scenario due to hydrogen dispersion, fire and explosion, potential loss of power	Hazardous	Hydrogen tank must provide insulation	Fuel flow is interrupted, energy generation system is shut down, RTO if failure occurs before V1
		Take-off-after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Fuel flow is interrupted, energy generation system is shut down, abort the mission and land as soon as possible
FM 02	Partial loss of storage function	Take-off before V1	Potential unsafe scenario due to hydrogen dispersion or heating, potential loss of power	Hazardous	Hydrogen tank must provide insulation	Partial fuel flow is interrupted, energy generation system is shut down, RTO
		Take-off-after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Partial fuel flow is interrupted, energy generation system is shut down, abort the mission and land as soon as possible

Logical component	Function ID	Function	Function description
Main energy system – LH2 fuel system	LSTO – 200	Provide LH2	Provide the necessary amount of liquid hydrogen to be converted into gaseous form

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 01	Total loss of hydrogen supply to the energy generation system	Take-off before V1	No fuel is delivered to the energy generation systems, potential loss of power	Minor	The auxiliary energy systems supply the aircraft	Reactant flow is stopped, the auxiliary systems supply for the power demand, RTO if the failure occurs before V1
		Take-off after V1	See above	Catastrophic	The auxiliary systems are able not to take-off	Reactant flow is stopped, the auxiliary energy systems supply for the power demand for a limited amount of time
		Cruise	See above	Catastrophic	The auxiliary energy systems supply the aircraft	See above
		Descent, Landing	No fuel is delivered to the energy generation systems, potential loss of power, auxiliary energy charging systems process is stopped	Catastrophic	See above	See above

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 02	Partial loss of hydrogen supply to the energy generation system	Take-off before V1	No fuel is delivered to the energy generation system, potential loss of power	Minor	Remaining main energy and auxiliary energy systems supply the aircraft	Partial reactant flow is stopped, remaining main energy and auxiliary energy systems supply for the power demand, RTO if the failure occurs before V1
		Take-off after V1	See above	Minor	Remaining main energy and auxiliary energy systems are able to take-off	Partial reactant flow is stopped, remaining main energy and auxiliary energy systems supply for the power demand, abort the mission and land as soon as possible
		Cruise	See above	Minor	Remaining main energy and auxiliary energy systems supply the aircraft	See above
		Descent, Landing	No fuel is delivered to the energy generation system, potential loss of power, energy storage charging systems process is stopped	Minor	See above	See above

Logical component	Function ID	Function	Function description
Main energy system – LH2 fuel system	LSTO – 300	Provide GH2	Provide gaseous hydrogen to the energy generation system

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 03	Erroneous fuel supply to the energy generation system	Take-off before V1	Potential damage and malfunction in the energy generation system	Minor	Energy generation system is able to work in degraded mode with its operation limits	If the energy generation system degradation exceeds the limits, emergency shutdown is required, RTO
		Take-off after V1, Climb, Cruise, Descent, Landing	Potential damage and malfunction in the energy generation system	Major	See above	If the energy generation system degradation exceeds the limits, emergency shutdown and landing

Logical component	Function ID	Function	Function description
Auxiliary energy system	LAUX – 100	Provide stored electrical energy	Provide electrical energy from the auxiliary energy system

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 01	Total loss of stored electrical energy	Take-off before V1	Loss of power and loss of electric grid stabilization	Minor	The main energy systems supply for the aircraft	The main energy systems supply power demand, RTO if the failure occurs before V1
		Take-off after V1	Loss of power and loss of electric grid stabilization	Minor	The main energy systems are able to take-off	The main energy systems supply for the power demand
		Cruise	Loss of electric grid stabilization	Minor	The main energy systems supply the aircraft	See above
		Descent, Landing	Loss of electric grid stabilization, auxiliary energy systems charging process is stopped	Minor	See above	See above

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 02	Partial loss of electrical energy from the battery	Take-off before V1 (FC and battery on)	Potential loss of power, potential loss of grid stabilization	Minor	The remaining auxiliary and the main energy systems supply for the aircraft	The remaining auxiliary and the main energy systems supply for the power demand, RTO if the failure occurs before V1
		Take-off after V1	Potential loss of power, potential loss of grid stabilization	Minor	The remaining auxiliary and the main energy systems are able to take-off	The remaining auxiliary and the main energy systems supply for the power demand
		Cruise	Potential loss of grid stabilization	Minor	The remaining auxiliary and the main energy systems supply for the aircraft	See above
		Descent, Landing	Potential loss of grid stabilization, auxiliary energy systems charging process is stopped	Minor	See above	See above

Logical component	Function ID	Function	Function description
Auxiliary energy system	LAUX - 200	Store electrical energy	Store electrical energy from ground charging, the energy generation system or electric grid stabilization

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 01	Total loss of storage function	Take-off before V1	Potential loss of power, loss of grid stabilization function	Minor	The main energy systems supply for the aircraft	The main energy systems supply power demand, RTO if the failure occurs before V1
		Take-off after V1	See above	Major	The main energy systems are able to take-off	The main energy systems supply for the power demand, abort the mission and land as soon as possible
		Cruise	Potential loss of power, loss of grid stabilization function	Minor	The main energy systems supply the aircraft	See above
		Descent, Landing	Potential loss of power, loss of grid stabilization function, auxiliary energy systems charging process is stopped	Minor	See above	See above

Failure ID	Failure	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation
FM 02	Partial loss of storage function	Take-off before V1	Potential loss of power, loss of grid stabilization function	Minor	The remaining auxiliary and the main energy systems supply for the aircraft	The remaining auxiliary and the main energy systems supply for the power demand, RTO if the failure occurs before V1
		Take-off after V1	Potential loss of power, loss of grid stabilization function	Minor	The remaining auxiliary and the main energy systems are able to take-off	The remaining auxiliary and the main energy systems supply for the power demand
		Cruise	See above	Minor	The remaining auxiliary and the main energy systems supply for the aircraft	See above
		Descent, Landing	Potential loss of power, loss of grid stabilization function, auxiliary energy systems charging process is stopped	Minor	See above	The energy generation system and partial storage system supply for the power demand
FM 04	Undetected full battery	Descent, Landing	Inability to charge battery	Minor	The crew and the system must always be aware of the state of the battery	The electric grid is able to work in degraded mode within its operation limits
		All phases	Loss of the stabilization function in case of peaks (battery cannot store energy)	Minor	See above	See above

9.2 Annexes 2. Physical FHA

9.2.1 Energy control functional chain

Component	Function ID	Function	Function description	Functional chain
Fuel cell controller	PGEN – 200	Control energy generation	Manage the amount of energy generated by the fuel cell through the reactant (hydrogen and air) regulation	Energy control

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of reactant supply control function	Internal degradation, error in the upstream component	Take-off before V1	No signal to collect ram air, loss of power	Minor	Battery systems supply for the power demand	Reactant flow is interrupted, RTO if failure occurs before V1	Redundancy of the control logic
			Take-off after V1, Climb	See above	Catastrophic	Battery systems are not able to take-off	Reactant flow is interrupted, abort the mission and land as soon as possible	
			Cruise	See above	Catastrophic	Battery systems supply for the power demand for a limited amount of time	Reactant flow is interrupted, battery systems are activated, abort the mission and land as soon as possible	
			Descent, Landing	See above, battery systems charging process is stopped	Catastrophic	See above	See above	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 02	Partial loss of the hydrogen supply control function	See above	Take-off before V1	No signal to collect ram air, potential loss of power	Minor	Remaining fuel cell and battery systems supply for the power demand	Partial reactant flow is interrupted, RTO if failure occurs before V1	See above
			Take-off after V1, Climb	See above	Minor	Remaining fuel cell and battery systems are able to perform take-off	Partial reactant flow is interrupted, abort the mission and land as soon as possible	
			Cruise	See above	Minor	Remaining fuel cell and battery systems supply for the power demand	Partial reactant flow is interrupted, battery systems are activated, abort the mission and land as soon as possible	
			Descent, Landing	No signal to collect ram air, potential loss of power, battery systems charging process is stopped	Minor	See above	See above	
FM 03	Failure to allow correct amount of air flow	See above	Take-off before V1	Potential damage in the fuel cell, degraded mode	Minor	Fuel cell is able to work in degraded mode with its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required, RTO	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	Potential damage in the fuel cell, degraded mode	Major	Fuel cell is able to work in degraded mode with its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required	

Component	Function ID	Function	Function description	Functional chain
Compressor inlet valve	PGEN – 310	Provide air	Collect the requested amount of ram air	Energy control

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Toral loss of ram air collection	Blockage in the valve, mechanical damage	Take-off before V1	Absence of air flow to the fuel cell system, loss of power	Minor	Battery systems supply the aircraft	Reactant flow is interrupted, battery systems supply the onboard systems, RTO if failure occurs before V1	Redundancy of the valve
			Take-off after V1, Climb	See above	Catastrophic	Battery systems is not able to perform take-off	Reactant flow is interrupted, battery systems supply the onboard systems, abort the mission and land as soon as possible	
			Cruise	See above	Catastrophic	Battery systems supply the aircraft for a limited amount of time	See above	
			Descent, Landing	Absence of air flow to the fuel cell system, loss of power, battery system charging process is stopped	Catastrophic	See above	See above	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 02	Partial loss of ram air collection	See above	Take-off before V1	Partial absence of air flow to the fuel cell system, potential loss of power	Minor	Remaining fuel cell and battery systems supply the aircraft	Reactant flow is partially interrupted, remaining fuel cell and battery systems supply the onboard systems, RTO if failure occurs before V1	See above
			Take-off after V1, Climb	See above	Minor	Remaining fuel cell and battery systems are able to perform take-off	Reactant flow is partially interrupted, remaining fuel cell and battery systems supply the onboard systems, abort the mission and land as soon as possible	
			Cruise	See above	Minor	Remaining fuel cell and battery systems supply the aircraft	See above	
			Descent, Landing	Partial absence of air flow to the fuel cell system, loss of power, battery system charging process is stopped	Minor	See above	See above	

Component	Function ID	Function	Function description	Functional chain
Hydrogen pump	PSTO – 200	Provide LH2	Extract the requested amount of hydrogen from the tank to be converted into gaseous form	Energy control

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of liquid hydrogen extraction from the tank	Blockage or obstruction in the pump	Take-off before V1	Absence of hydrogen flow, loss of power	Minor	Battery systems supply the aircraft	Reactant flow is interrupted, battery systems supply onboard systems, RTO if failure occurs before V1	Redundancy of the hydrogen pump
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	Battery systems supply the aircraft for a limited amount of time	Reactant flow is interrupted, battery systems supply onboard systems, abort and land as soon as possible	
FM 02	Partial loss of hydrogen extraction from the tank	See above	Take-off before V1	Partial absence of hydrogen flow, loss of power	Minor	Remaining fuel cell and battery systems supply the aircraft	Reactant flow is interrupted, remaining fuel cell and battery systems supply onboard systems, RTO if failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	Remaining fuel cell and battery systems supply the aircraft for a limited amount of time	Reactant flow is interrupted, remaining fuel cell and battery systems supply onboard systems, abort and land as soon as possible	

Component	Function ID	Function	Function description	Functional chain
Fuel cell stack	PGEN – 100	Provide electrical energy from H2	Electrical energy is generated through the chemical reaction between hydrogen and oxygen	Energy control

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of energy generation from H2	Fuel cell internal damage (cracking, pinholes, ...), failure of upstream components	Take-off before V1	Loss of power	Major	Battery systems supply the aircraft	Battery systems supply the power demand of the onboard systems, RTO if the failure occurs before V1	Design considering all flight atmosphere conditions to resist mechanical and thermal stress. Protect the edges across the electrodes and the membrane to increase crack resistance
			Take-off after V1, Climb	Loss of power, inability to perform take-off	Catastrophic	Battery systems alone are not able to perform take-off	Battery systems supply the power demand of the onboard systems	
			Cruise	Loss of power	Catastrophic	Battery system supply the power demand for a limited amount of time	Battery system is activated to supply the power demand	
			Descent, Landing	Loss of power, battery charging process is stopped, inability to perform take-off in case of go-around	Catastrophic	See above	See above	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 02	Partial loss of energy generation from H2	See above	Take-off before V1	Potential loss of power	Minor	Remaining fuel cell and battery systems supply the aircraft	Remaining fuel cell and battery systems supply the power demand of the onboard systems, RTO if the failure occurs before V1	See above
			Take-off after V1, climb	Potential loss of power supplied by the remaining fuel cell and battery	Minor	Remaining fuel cell and battery systems are able to perform take-off	Remaining fuel cell and battery systems supply the power demand, abort the mission and land as soon as possible	
			Cruise	Potential loss of power	Minor	Remaining fuel cell and battery systems supply power demand	See above	
			Descent, Landing	Potential loss of power, battery charging process is stopped, limited amount of power in case of go-around scenario	Minor	See Above	See above	

9.2.2 Hydrogen storage and pressure regulation

Component	Function ID	Function	Function description	Functional chain
Hydrogen tank	PSTO – 100	Store LH2	Store liquid hydrogen cryogenically and provide adequate insulation	Hydrogen storage and pressure regulation

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of the hydrogen storage	LH2 leakage/rupture of the tank	Take-off before V1	Potential fire and explosion, loss of power,	Hazardous	Battery systems supply the aircraft	Emergency fire systems are activated, reactant flow is interrupted, battery systems supply the power of the onboard systems, RTO if the failure occurs before V1	Material selection to minimize embrittlement. Spherical or cylindrical-shaped tank
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	Battery systems alone supply for the power demand	Emergency fire systems are activated, reactant flow is interrupted, battery systems supply the power of the onboard systems, abort the mission and land as soon as possible	
FM 02	Partial loss of the hydrogen storage	See above	Take-off before V1	Potential fire and explosion, potential loss of power	Hazardous	Remaining fuel cell and battery systems supply the aircraft	Emergency fire systems are activated, reactant flow is partially interrupted, remaining fuel cell and battery systems supply the power of the onboard systems, RTO if the failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Emergency fire systems are activated, reactant flow is partially interrupted, remaining fuel cell and battery systems supply the power of the onboard systems, abort the mission and land as soon as possible	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of insulation	Degradation	Take-off before V1	Temperature rise, pressure rise which requires venting, potential fire and explosion, loss of fuel reserve	Major	The hydrogen tank must maintain insulation at cryogenic condition	Vent system is activated, RTO if the failure occurs before V1	Material selection to minimize embrittlement
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Hazardous	The hydrogen tank must maintain insulation at cryogenic condition	Vent system is activated, abort mission and land as soon as possible	
FM 02	Partial loss of insulation	See above	Take-off before V1	Temperature rise, pressure rise which requires venting, potential fire and explosion, loss of fuel reserve	Major	The hydrogen tank must maintain insulation at cryogenic condition	Vent system is activated, RTO if the failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Hazardous	The hydrogen tank must maintain insulation at cryogenic condition	Vent system is activated, abort mission and land as soon as possible	

Component	Function ID	Function	Function description	Functional chain
Vent valve	PSTO – 110	Vent hydrogen	Expel hydrogen in case of pressure rising above tank's maximum limits	Hydrogen storage and pressure regulation

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of tank venting	Blockage of the vent valve or vent line (dendrites, freezing by air at cryogenic temperatures)	Take-off before V1	Boil-off condition, potential explosion	Hazardous	The venting pressure is the maximum allowable pressure for the tank	Reactant flow is interrupted, battery systems supply the aircraft, RTO if failure occurs before V1	Redundancy of the vent valve Tank shape designed to minimize surface and heat load Design considering vent volume and vent pressure
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Reactant flow is interrupted, battery systems supply the aircraft, abort the mission and land as soon as possible	
FM 02	Partial loss of tank venting	See above	Take-off before V1	Boil-off condition, potential explosion	Hazardous	The venting pressure is the maximum allowable pressure for the tank	Reactant flow is interrupted, remaining fuel cell and battery systems supply the aircraft, RTO if failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Reactant flow is interrupted, remaining fuel cell and battery systems supply the aircraft, abort the mission and land as soon as possible	

Component	Function ID	Function	Function description	Functional chain
Hydrogen electrical preheater	PTMS – 120	Heat hydrogen	Provide heat to increase the internal pressure of the tank	Hydrogen storage and pressure regulation

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of pressure increase function	Internal damage, loss of electrical power	Take-off before V1	Potential pressure drop, potential loss of energy generation	Major	Minimum tank pressure must be slightly higher than the maximum ambient pressure expected	Fuel flow is interrupted, fuel cell systems are shut down, RTO if the failure occurs before V1	Redundancy of the component, design the component to withstand aircraft vibrations, provide protection in case of overload or short circuits
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Hazardous	See above	Fuel flow is interrupted, fuel cell systems are shut down, emergency descent and landing	
FM 02	Partial loss of pressure increase function	See above	Take-off before V1	Potential pressure drop, potential loss of energy generation	Minor	Minimum tank pressure must be slightly higher than the maximum ambient pressure expected	Fuel flow is interrupted, fuel cell systems are shut down, RTO if the failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	Fuel flow is interrupted, fuel cell systems are shut down, emergency descent and landing	

9.2.3 Hydrogen conversion and supply

Component	Function ID	Function	Function description	Functional chain
Hydrogen tank	PSTO – 100	Store LH2	Store liquid hydrogen cryogenically and provide adequate insulation	Hydrogen conversion and supply

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of the hydrogen storage	LH2 leakage/rupture of the tank	Take-off before V1	Potential fire and explosion, loss of power,	Hazardous	Battery systems supply the aircraft	Emergency fire systems are activated, reactant flow is interrupted, battery systems supply the power of the onboard systems, RTO if the failure occurs before V1	Material selection to minimize embrittlement. Spherical or cylindrical-shaped tank
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	Battery systems alone supply for the power demand	Emergency fire systems are activated, reactant flow is interrupted, battery systems supply the power of the onboard systems, abort the mission and land as soon as possible	
FM 02	Partial loss of the hydrogen storage	See above	Take-off before V1	Potential fire and explosion, potential loss of power	Hazardous	Remaining fuel cell and battery systems supply the aircraft	Emergency fire systems are activated, reactant flow is partially interrupted, remaining fuel cell and battery systems supply the power of the onboard systems, RTO if the failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Emergency fire systems are activated, reactant flow is partially interrupted, remaining fuel cell and battery systems supply the power of the onboard systems, abort the mission and land as soon as possible	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of insulation	Degradation	Take-off before V1	Temperature rise, pressure rise which requires venting, potential fire and explosion, loss of fuel reserve	Major	The hydrogen tank must maintain insulation at cryogenic condition	Vent system is activated, RTO if the failure occurs before V1	Material selection to minimize embrittlement
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Hazardous	See above	Vent system is activated, abort mission and land as soon as possible	
FM 02	Partial loss of insulation	See above	Take-off before V1	Temperature rise, pressure rise which requires venting, potential fire and explosion, loss of fuel reserve	Major	The hydrogen tank must maintain insulation at cryogenic condition	Vent system is activated, RTO if the failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Hazardous	See above	vent system is activated, abort mission and land as soon as possible	

Component	Function ID	Function	Function description	Functional chain
Hydrogen pump	PSTO – 200	Provide LH2	Extract the requested amount of hydrogen from the tank to be converted into gaseous form	Hydrogen conversion and supply

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of liquid hydrogen extraction from the tank	Blockage or obstruction in the pump	Take-off before V1	Absence of hydrogen flow, loss of power	Minor	Battery systems supply the aircraft	Reactant flow is interrupted, battery systems supply onboard systems, RTO if failure occurs before V1	Redundancy of the hydrogen pump
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	Battery systems supply the aircraft for a limited amount of time	Reactant flow is interrupted, battery systems supply onboard systems, abort and land as soon as possible	
FM 02	Partial loss of hydrogen extraction from the tank	See above	Take-off before V1	Partial absence of hydrogen flow, loss of power	Minor	Remaining fuel cell and battery systems supply the aircraft	Reactant flow is interrupted, remaining fuel cell and battery systems supply onboard systems, RTO if failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	Remaining fuel cell and battery systems supply the aircraft for a limited amount of time	Reactant flow is interrupted, remaining fuel cell and battery systems supply onboard systems, abort and land as soon as possible	

Component	Function ID	Function	Function description	Functional chain
Hydrogen dedicated heat exchanger	PTMS – 210	Provide heat	Provide heat to hydrogen to reach gaseous state at the target temperature	Hydrogen conversion and supply

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss to provide heat for hydrogen conversion	Leakage, rupture, corrosion, degradation	Take-off before V1	Potential freezing of downstream components, loss of power	Minor	Hydrogen should be heated up to the target temperature before entering the fuel cell	Reactant flow is interrupted, fuel cell systems are shut down, RTO if the failure occurs before V1	Selection of material to minimize hydrogen embrittlement and resist thermal stress
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Hazardous	See above	Reactant flow is interrupted, fuel cell systems are shut down, emergency descent and landing	
FM 02	Partial loss to provide heat for hydrogen conversion	See above	Take-off before V1	Potential freezing of downstream components, potential loss of power	Minor	Hydrogen should be heated up to the target temperature before entering the fuel cell	Reactant flow is interrupted, fuel cell systems are shut down, RTO if the failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	Reactant flow is interrupted, fuel cell systems are shut down, emergency descent and landing	

Component	Function ID	Function	Function description	Functional chain
Valve	PSTO – 300	Provide GH2	Provide gaseous hydrogen to the fuel cell and prevent hydrogen flow to the fuel cell in case of upstream failure condition	Hydrogen conversion and supply

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of hydrogen supply to the fuel cell	Blockage/obstruction in the valve	Take-off before V1	Absence of hydrogen flow, loss of power	Minor	Battery systems supply the aircraft	Reactant flow is interrupted, battery systems supply onboard systems, RTO if failure occurs before V1	Redundancy of the valve
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	Battery systems supply the aircraft for a limited amount of time	Reactant flow is interrupted, battery systems supply onboard systems, abort and land as soon as possible	
FM 02	Partial loss of hydrogen supply to the fuel cell	See above	Take-off before V1	Partial absence of hydrogen flow, loss of power	Minor	Remaining fuel cell and battery systems supply the aircraft	Reactant flow is interrupted, remaining fuel cell and battery systems supply onboard systems, RTO if failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	Remaining fuel cell and battery systems supply the aircraft for a limited amount of time	Reactant flow is interrupted, remaining fuel cell and battery systems supply onboard systems, abort and land as soon as possible	

Component	Function ID	Function	Function description	Functional chain
Fuel cell stack	PGEN – 100	Provide electrical energy from H2	Electrical energy is generated through the chemical reaction between hydrogen and oxygen	Hydrogen conversion and supply

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of energy generation from H2	Fuel cell internal damage (cracking, pinholes, ...). Failure of upstream components	Take-off before V1	Loss of power	Major	Battery systems supply the aircraft	Battery systems supply the power demand of the onboard systems, RTO if the failure occurs before V1	Design considering all flight atmosphere conditions to resist mechanical and thermal stress. Protect the edges across the electrodes and the membrane to increase crack resistance
			Take-off after V1, Climb	Loss of power, inability to perform take-off	Catastrophic	Battery systems alone are not able to perform take-off	Battery systems supply the power demand of the onboard systems	
			Cruise	Loss of power	Catastrophic	Battery system supply the power demand for a limited amount of time	Battery system is activated to supply the power demand	
			Descent, Landing	Loss of power, battery charging process is stopped, inability to perform take-off in case of go-around	Catastrophic	See above	See above	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 02	Partial loss of energy generation from H2	See above	Take-off before V1	Potential loss of power	Minor	Remaining fuel cell and battery systems supply the aircraft	Remaining fuel cell and battery systems supply the power demand of the onboard systems, RTO if the failure occurs before V1	See above
			Take-off after V1, Climb	Potential loss of power supplied by the remaining fuel cell and battery	Minor	Remaining fuel cell and battery systems are able to perform take-off	Remaining fuel cell and battery systems supply the power demand, abort the mission and land as soon as possible	
			Cruise	Potential loss of power	Minor	Remaining fuel cell and battery systems supply power demand	See above	
			Descent, Landing	Potential loss of power, battery charging process is stopped, limited amount of power in case of go-around	Minor	See Above	See above	

9.2.4 Air supply and regulation

Component	Function ID	Function	Function description	Functional chain
Compressor inlet valve	PGEN – 310	Regulate air flow	Collect the requested amount of ram air	Air supply and regulation

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Toral loss of ram air collection	Blockage in the valve, mechanical damage	Take-off before V1	Absence of air flow to the fuel cell system, loss of power	Minor	Battery systems supply the aircraft	Reactant flow is interrupted, battery systems supply the onboard systems, RTO if failure occurs before V1	Redundancy of the valve
			Take-off after V1, Climb	See above	Catastrophic	Battery systems is not able to perform take-off	Reactant flow is interrupted, battery systems supply the onboard systems, abort the mission and land as soon as possible	
			Cruise	See above	Catastrophic	Battery systems supply the aircraft for a limited amount of time	See above	
			Descent, Landing	Absence of air flow to the fuel cell system, loss of power, battery system charging process is stopped	Catastrophic	See above	See above	

FM 02	Partial loss of ram air collection	See above	Take-off before V1	Partial absence of air flow to the fuel cell system, potential loss of power	Minor	Remaining fuel cell and battery systems supply the aircraft	Reactant flow is partially interrupted, remaining fuel cell and battery systems supply the onboard systems, RTO if failure occurs before V1	See above
			Take-off after V1, Climb	See above	Minor	Remaining fuel cell and battery systems are able to perform take-off	Reactant flow is partially interrupted, remaining fuel cell and battery systems supply the onboard systems, abort the mission and land as soon as possible	
			Cruise	See above	Minor	Remaining fuel cell and battery systems supply the aircraft	See above	
			Descent, Landing	Partial absence of air flow to the fuel cell system, loss of power, battery system charging process is stopped	Minor	See above	See above	

Component	Function ID	Function	Function description	Functional chain
Compressor	PGEN – 300	Provide compressed air	Compress ram air to supply the fuel cell	Air supply and regulation

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of ram air compression	Blockage in the component, mechanical damage	Take-off before V1	Potential absence of air flow, loss of power	Minor	Battery system supply the aircraft	Reactant flow is interrupted, RTO if failure occurs before V1	Selection of material to resist mechanical and thermal stress, introduce debris filter and anti-icing elements
			Take-off after V1, Climb	See above	Catastrophic	Battery systems are not able to take-off	Reactant flow is interrupted, emergency descent and landing	
			Cruise	See above	Catastrophic	Battery systems supply the power demand for a limited amount of time	See above	
			Descent, Landing	Potential absence of airflow, potential loss of power, battery systems charging process is stopped	Catastrophic	See above	See above	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 02	Partial loss of air compression	See above	Take-off before V1	Potential absence of air flow, potential loss of power	Minor	Remaining fuel cell and battery system supply the aircraft	Partial reactant flow is interrupted, RTO if failure occurs before V1	See above
			Take-off after V1, Climb	See above	Minor	Remaining fuel cell and battery systems are able to take-off	Partial reactant flow is interrupted, emergency descent and landing	
			Cruise	See above	Minor	Remaining fuel cell and battery systems supply the power demand	See above	
			Descent, Landing	Potential absence of airflow, potential loss of power, battery systems charging process is stopped	Minor	See above	See above	
FM 03	Failure to compress ram air to acceptable pressure range	Obstruction, deterioration, controller failure	Take-off before V1	Reduction of fuel cell performance, potential fuel cell degradation, potential loss of power	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required, RTO if failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	If the fuel cell degradation exceeds the limits, emergency shutdown is required, abort the mission and land as soon as possible	

Component	Function ID	Function	Function description	Functional chain
Compressor dedicated heat exchanger	PTMS – 400	Absorb heat	Absorb the excess heat generated by the air compression	Air supply and regulation

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 03	Failure to regulate air at acceptable temperature range	Deterioration, corrosion	Take-off before V1	Reduction of the fuel cell performance, potential fuel cell degradation, potential loss of power	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required	Choice of material to resist a wide temperature range, position filter components to avoid dendrites
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	See above	

Component	Function ID	Function	Function description	Functional chain
Humidifier	PGEN – 500	Manage humidity	Regulate the humidity level inside the fuel cell	Air supply and regulation

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 03	Failure to regulate air supply at acceptable humidity level	Deterioration, corrosion, incorrect amount of vapour received from upstream	Take-off before V1	Too low humidity: dehydration of the membrane, drop of power density, potential reduction of electricity Excessive humidity: fuel cell flooding, potential reduction of electricity	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required	Implement water and air filters and detection systems in the chain
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	See above	

Component	Function ID	Function	Function description	Functional chain
Air supply valve	PGEN – 510	Adjust air supply	Regulate the amount of air entering the fuel cell	Air supply and regulation

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of air supply	Obstruction	Take-off before V1	Absence of air flow to the fuel cell, loss of power	Minor	Battery systems supply the aircraft	Reactant flow is interrupted, RTO if failure occurs before V1	Redundancy of the component
			Take-off after V1, Climb	See above	Catastrophic	Battery systems are not able to take-off	Reactant flow is interrupted, abort mission and land as soon as possible	
			Cruise	See above	Catastrophic	Battery systems supply the aircraft for a limited amount of time	Reactant flow is interrupted, battery systems are activated, abort mission and land as soon as possible	
			Descent, Landing	Absence of air flow, loss of power, battery systems recharging process is stopped	Catastrophic	See above	See above	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 02	Partial loss of air supply	See above	Take-off before V1	Absence of air flow to the fuel cell, potential loss of power	Minor	Remaining fuel cell and battery systems supply the aircraft	Partial reactant flow is interrupted, RTO if failure occurs before V1	See above
			Take-off after V1, Climb	See above	Minor	Remaining fuel cell and battery systems are able to take-off	Partial reactant flow is interrupted, abort mission and land as soon as possible	
			Cruise	See above	Minor	Remaining fuel cell and battery systems supply the aircraft	See above	
			Descent, Landing	Absence of air flow to the fuel cell, potential loss of power, battery system charging process is stopped	Minor	See above	See above	

Component	Function ID	Function	Function description	Functional chain
Fuel cell stack	PGEN – 100	Provide electrical energy from H2	Electrical energy is generated through the chemical reaction between hydrogen and oxygen	Air supply and regulation

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of energy generation from H2	Fuel cell internal damage (cracking, pinholes, ...). Failure of upstream components	Take-off before V1	Loss of power	Major	Battery systems supply the aircraft	Battery systems supply the power demand of the onboard systems, RTO if the failure occurs before V1	Design considering all flight atmosphere conditions to resist mechanical and thermal stress. Protect the edges across the electrodes and the membrane to increase crack resistance
			Take-off after V1, Climb	Loss of power, inability to perform take-off	Catastrophic	Battery systems alone are not able to perform take-off	Battery systems supply the power demand of the onboard systems	
			Cruise	Loss of power	Catastrophic	Battery system supply the power demand for a limited amount of time	Battery system is activated to supply the power demand	
			Descent, Landing	Loss of power, battery charging process is stopped, inability to perform take-off in case of go-around	Catastrophic	See above	See above	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 02	Partial loss of energy generation from H2	See above	Take-off before V1	Potential loss of power	Minor	Remaining fuel cell and battery systems supply the aircraft	Remaining fuel cell and battery systems supply the power demand of the onboard systems, RTO if the failure occurs before V1	See above
			Take-off after V1, climb	Potential loss of power supplied by the remaining fuel cell and battery	Minor	Remaining fuel cell and battery systems are able to perform take-off	Remaining fuel cell and battery systems supply the power demand, abort the mission and land as soon as possible	
			Cruise	Potential loss of power	Minor	Remaining fuel cell and battery systems supply power demand	See above	
			Descent, Landing	Potential loss of power, battery charging process is stopped, limited amount of power in case of go-around	Minor	See Above	See above	

9.2.5 Air supply temperature regulation

Component	Function ID	Function	Function description	Functional chain
Compressor dedicated heat exchanger	PTMS – 400	Absorb heat	Absorb the excess heat generated by the air compression	Air supply temperature regulation

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 03	Failure to regulate air at acceptable temperature range	Deterioration, corrosion	Take-off before V1	Reduction of the fuel cell performance, potential fuel cell degradation, potential loss of power	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required	Choice of material to resist a wide temperature range, position filter components to avoid dendrites
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	See above	

Component	Function ID	Function	Function description	Functional chain
Compressor dedicated heat exchanger	PTMS – 420	Dissipate heat	Dissipate heat generated from air thermal management	Air supply temperature regulation

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 03	Failure to regulate air at acceptable temperature range	Deterioration, corrosion	Take-off before V1	Overheating of the component, wrong air supply temperature regulation	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required	Choice of material to resist a wide temperature range, position filter components to avoid dendrites
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	See above	See above

9.2.6 Exhaust water management

Component	Function ID	Function	Function description	Functional chain
Fuel cell stack	PGEN – 100	Provide electrical energy from H2	Electrical energy is generated through the chemical reaction between hydrogen and oxygen	Exhaust water management

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of energy generation from H2	Fuel cell internal damage (cracking, pinholes, ...). Failure of upstream components	Take-off before V1	Loss of power	Major	Battery systems supply the aircraft	Battery systems supply the power demand of the onboard systems, RTO if the failure occurs before V1	Design considering all flight atmosphere conditions to resist mechanical and thermal stress. Protect the edges across the electrodes and the membrane to increase crack resistance
			Take-off after V1, Climb	Loss of power, inability to perform take-off	Catastrophic	Battery systems alone are not able to perform take-off	Battery systems supply the power demand of the onboard systems	
			Cruise	Loss of power	Catastrophic	Battery system supply the power demand for a limited amount of time	Battery system is activated to supply the power demand	
			Descent, Landing	Loss of power, battery charging process is stopped, inability to perform take-off in case of go-around	Catastrophic	See above	See above	

FM 02	Partial loss of energy generation from H2	See above	Take-off before V1	Potential loss of power	Minor	Remaining fuel cell and battery systems supply the aircraft	Remaining fuel cell and battery systems supply the power demand of the onboard systems, RTO if the failure occurs before V1	See above
			Take-off after V1, climb	Potential loss of power supplied by the remaining fuel cell and battery	Minor	Remaining fuel cell and battery systems are able to perform take-off	Remaining fuel cell and battery systems supply the power demand, abort the mission and land as soon as possible	
			Cruise	Potential loss of power	Minor	Remaining fuel cell and battery systems supply power demand	See above	
			Descent, Landing	Potential loss of power, battery charging process is stopped, limited amount of power in case of go-around	Minor	See Above	See above	

Component	Function ID	Function	Function description	Functional chain
Vapour-liquid separator	PGEN – 610	Separate water from vapour	Manage the output wate from the fuel cell to recover vapour and water	Exhaust water management

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 03	Failure to separate output water	Leakage, obstruction, rupture, corrosion, degradation	Take-off before V1	Potential lack of water supply for the humidifier, improper humidification, potential fuel cell degradation, potential loss of power	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required	Selection of material to resist thermal stress and corrosion, introduce debris filters
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	See above	See above

Component	Function ID	Function	Function description	Functional chain
Water tank	PGEN – 620	Store water	Contain excess water from the fuel cell	Exhaust water management

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of water storage	Leakage, rupture	Take-off before V1	Potential damage in electrical components	Minor	The tank must provide storage and prevent water to damage other systems	Shutdown of electrical components and related systems damaged by the water leak	Position the water tank far from any electrical component
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	See above	
FM 02	Partial loss of storage water	See above	Take-off before V1	Potential damage in electrical components	Minor	The tank must provide storage and prevent water to damage other systems	Shutdown of electrical components and related systems damaged by the water leak	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Minor	See above	See above	

Component	Function ID	Function	Function description	Functional chain
Humidifier	PGEN – 500	Manage humidity	Regulate the humidity level inside the fuel cell	Exhaust water management

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 03	Failure to regulate air supply at acceptable humidity level	Deterioration, corrosion, incorrect amount of vapour received from upstream	Take-off before V1	Too low humidity: dehydration of the membrane, drop of power density, potential reduction of electricity Excessive humidity: fuel cell flooding, potential reduction of electricity	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required	Implement water and air filters and detection systems in the chain
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	See above	See above

9.2.7 TMS: hot circuit

Component	Function ID	Function	Function description	Functional chain
Fuel cell stack	PGEN – 100	Provide electrical energy from H2	Electrical energy is generated through the chemical reaction between hydrogen and oxygen	TMS: hot circuit

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of energy generation from H2	Fuel cell internal damage (cracking, pinholes, ...). Failure of upstream components	Take-off before V1	Loss of power	Major	Battery systems supply the aircraft	Battery systems supply the power demand of the onboard systems, RTO if the failure occurs before V1	Design considering all flight atmosphere conditions to resist mechanical and thermal stress. Protect the edges across the electrodes and the membrane to increase crack resistance
			Take-off after V1, Climb	Loss of power, inability to perform take-off	Catastrophic	Battery systems alone are not able to perform take-off	Battery systems supply the power demand of the onboard systems	
			Cruise	Loss of power	Catastrophic	Battery system supply the power demand for a limited amount of time	Battery system is activated to supply the power demand	
			Descent, Landing	Loss of power, battery charging process is stopped, inability to perform take-off in case of go-around	Catastrophic	See above	See above	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 02	Partial loss of energy generation from H2	See above	Take-off before V1	Potential loss of power	Minor	Remaining fuel cell and battery systems supply the aircraft	Remaining fuel cell and battery systems supply the power demand of the onboard systems, RTO if the failure occurs before V1	See above
			Take-off after V1, climb	Potential loss of power supplied by the remaining fuel cell and battery	Minor	Remaining fuel cell and battery systems are able to perform take-off	Remaining fuel cell and battery systems supply the power demand, abort the mission and land as soon as possible	
			Cruise	Potential loss of power	Minor	Remaining fuel cell and battery systems supply power demand	See above	
			Descent, Landing	Potential loss of power, battery charging process is stopped, limited amount of power in case of go-around	Minor	See Above	See above	

Component	Function ID	Function	Function description	Functional chain
Fuel cell dedicated heat exchanger	PTMS – 100	Absorb heat	Absorb heat generated by the fuel cell	TMS: hot circuit

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of heat absorption to manage fuel cell thermal load	Leakage, rupture, degradation, corrosion	Take-off before V1	Overheating of the fuel cell systems, potential malfunction and damage	Minor	Fuel cell systems are able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required, RTO if failure occurs before V1	Redundancy of the component, selection of material to resist thermal stress
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Hazardous	See above	If the fuel cell degradation exceeds the limits, emergency shutdown is required, abort the mission and land as soon as possible	
FM 02	Partial loss of heat absorption to manage fuel cell thermal load	See above	Take-off before V1	Overheating of the fuel cell system, potential malfunction and damage	Minor	Fuel cell system is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required, RTO if failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Minor	Remaining fuel cell and battery systems supply the aircraft for a limited amount of time	If the fuel cell degradation exceeds the limits, emergency shutdown is required	

Component	Function ID	Function	Function description	Functional chain
Fuel cell dedicated heat exchanger	PTMS – 200	Provide heat	Provide the heat generated by the fuel cell to the hydrogen conversion process	TMS: hot circuit

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss to provide heat for hydrogen conversion	Leakage, rupture, degradation, corrosion	Take-off before V1	Potential freezing of the downstream components, loss of power	Minor	Hydrogen should be heated to the target temperature before entering the fuel cell systems	Reactant flow is interrupted, RTO if failure occurs before V1	Redundancy of the component, selection of material to resist thermal stress
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Reactant flow is interrupted, abort the mission and land as soon as possible	
FM 02	Partial loss to provide heat for hydrogen conversion	See above	Take-off before V1	Overheating of the fuel cell system, potential malfunction and damage	Minor	Fuel cell system is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required, RTO if failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Minor	Remaining fuel cell and battery systems supply the aircraft for a limited amount of time	If the fuel cell degradation exceeds the limits, emergency shutdown is required	

Component	Function ID	Function	Function description	Functional chain
Fuel cell dedicated heat exchanger	PTMS – 300	Dissipate heat	Dissipate excess heat into the atmosphere	TMS: hot circuit

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of heat dissipation	Leakage, rupture, degradation, corrosion	Take-off before V1	Overheating in the system, potential damage and reduction of the performance	Minor	Fuel cell is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required	Redundancy of the component, selection of material to resist thermal stress
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	See above	See above	
FM 02	Partial loss of heat dissipation	See above	Take-off before V1	Overheating in the system, potential damage and reduction of the performance	Minor	Fuel cell system is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Minor	See above	See above	

9.2.8 TMS: cold circuit

Component	Function ID	Function	Function description	Functional chain
Hydrogen pump	PSTO – 200	Provide LH2	Extract the requested amount of hydrogen from the tank to be converted into gaseous form	TMS: cold circuit

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of liquid hydrogen extraction from the tank	Blockage or obstruction in the pump	Take-off before V1	Absence of hydrogen flow, loss of power	Minor	Battery systems supply the aircraft	Reactant flow is interrupted, battery systems supply onboard systems, RTO if failure occurs before V1	Redundancy of the hydrogen pump
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	Battery systems supply the aircraft for a limited amount of time	Reactant flow is interrupted, battery systems supply onboard systems, abort and land as soon as possible	
FM 02	Partial loss of hydrogen extraction from the tank	See above	Take-off before V1	Partial absence of hydrogen flow, loss of power	Minor	Remaining fuel cell and battery systems supply the aircraft	Reactant flow is interrupted, remaining fuel cell and battery systems supply onboard systems, RTO if failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Major	Remaining fuel cell and battery systems supply the aircraft for a limited amount of time	Reactant flow is interrupted, remaining fuel cell and battery systems supply onboard systems, abort and land as soon as possible	

Component	Function ID	Function	Function description	Functional chain
Hydrogen dedicated heat exchanger	PTMS – 200	Provide heat	Provide heat to hydrogen to reach gaseous state at target temperature	TMS: cold circuit

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of hydrogen conversion	Leakage, rupture, degradation, corrosion	Take-off before V1	Potential freezing of the downstream components, loss of power	Minor	Hydrogen should be heated to the target temperature before entering the fuel cell systems	Reactant flow is interrupted, RTO if failure occurs before V1	Selection of material to minimize hydrogen embrittlement and resist thermal stress
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Reactant flow is interrupted, abort the mission and land as soon as possible	
FM 02	Partial loss of hydrogen conversion	See above	Take-off before V1	Overheating of the fuel cell system, potential malfunction and damage	Minor	Fuel cell system is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required, RTO if failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Minor	Remaining fuel cell and battery systems supply the aircraft for a limited amount of time	If the fuel cell degradation exceeds the limits, emergency shutdown is required	

Component	Function ID	Function	Function description	Functional chain
Fuel cell dedicated heat exchanger	PTMS – 200	Provide heat	Provide the heat generated by the fuel cell to the hydrogen conversion process	TMS: cold circuit

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss to provide heat for hydrogen conversion	Leakage, rupture, degradation, corrosion	Take-off before V1	Potential freezing of the downstream components, loss of power	Minor	Hydrogen should be heated to the target temperature before entering the fuel cell systems	Reactant flow is interrupted, RTO if failure occurs before V1	Selection of material to resist thermal stress
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Catastrophic	See above	Reactant flow is interrupted, abort the mission and land as soon as possible	
FM 02	Partial loss to provide heat for hydrogen conversion	See above	Take-off before V1	Overheating of the fuel cell system, potential malfunction and damage	Minor	Fuel cell system is able to work in degraded mode within its operation limits	If the fuel cell degradation exceeds the limits, emergency shutdown is required, RTO if failure occurs before V1	See above
			Take-off after V1, Climb, Cruise, Descent, Landing	See above	Minor	Remaining fuel cell and battery systems supply the aircraft for a limited amount of time	If the fuel cell degradation exceeds the limits, emergency shutdown is required	

9.2.9 Energy storage

Component	Function ID	Function	Function description	Functional chain
Battery (supercapacitor)	PAUX – 200	Store electrical energy	Store electrical energy from ground charging, the fuel cell or electric grid stabilization	Energy storage

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of electrical energy storage function	Battery damage, mishandling, poor manufacturing, failed thermal management	Take-off before V1	Loss of power, loss of electric grid stabilization	Minor	Fuel cell systems supply the aircraft	Fuel cell system supply the power demand, RTO if failure occurs before V1	Provide accurate thermal management to the battery to uniform temperature distribution. Position the battery system far from any heat source and hazardous material
			Take-off after V1, Climb	See above	Minor	Fuel cell systems are able to perform take-off	Fuel cell system supply the aircraft, abort the mission and land as soon as possible	
			Cruise	Loss of electric grid stabilization	Minor	Fuel cell systems supply the aircraft	Fuel cell systems supply the power demand, abort the mission and land as soon as possible	
			Descent, Landing	Loss of electric grid stabilization, battery systems charging process is stopped	Minor	See above	See above	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 02	Partial loss of electrical energy storage function	See above	Take-off before V1	Potential loss of power, loss of grid stabilization	Minor	Remaining battery and fuel cell systems supply the aircraft	Fuel cell systems supply for the power demand, abort the mission and land as soon as possible	See above
			Take-off after V1, Climb	See above	Minor	Remaining battery and fuel cell systems are able to take-off	See above	
			Cruise	Loss of grid stabilization	Minor	Remaining battery and fuel cell systems supply the aircraft	See above	
			Descent, Landing	Loss of grid stabilization, battery charging process is stopped	Minor	See above	See above	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 03	Overheating	Defects from manufacturing, internal shorts, mechanical stress	Take-off, Climb, Descent, Landing	Potential heat accumulation, explosion, potential loss of storage system (high burning rate due to lower altitude)	Hazardous	Battery system must be thermally regulated by its dedicated thermal management system	Containment of the hazard	High quality control standards, dedicated thermal management system and cell-venting system, accurate degradation prediction and state estimation
			Cruise	Potential heat accumulation, explosion, potential loss of storage system	Major	See above	See above	
FM 04	Undetected full state of charge of the battery	Failure in the battery management system	Descent, Landing	Inability to charge battery	Minor	The system (and the crew) must always be aware of the state of the battery system	Emergency mode in case of go-around, the energy storage system is not charged for take-off	Redundant battery management system to monitor the state of the system
			All phases	Loss of the grid stabilization function in case of peaks to be absorbed (battery system cannot store more energy)	Minor	The energy storage system must be able to stabilize the grid	The electric grid is able to work in degraded mode within its operation limits	

Component	Function ID	Function	Function description	Functional chain
Battery (supercapacitor)	PAUX – 100	Provide stored electrical energy	Provide electrical energy from the battery system	Energy storage

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 01	Total loss of electrical energy from the battery	Battery damage, mishandling, poor manufacturing, failed thermal management	Take-off before V1	Loss of power, loss of electric grid stabilization	Minor	Fuel cell systems supply the aircraft	Fuel cell system supply the power demand, RTO if failure occurs before V1	Provide accurate thermal management to the battery to uniform temperature distribution. Position the battery system far from any heat source and hazardous material
			Take-off after V1, Climb	See above	Major	Fuel cell systems are able to perform take-off	Fuel cell system supply the aircraft, abort the mission and land as soon as possible	
			Cruise	Loss of electric grid stabilization	Major	Fuel cell systems supply the aircraft	Fuel cell systems supply the power demand, abort the mission and land as soon as possible	
			Descent, Landing	Loss of electric grid stabilization, battery systems charging process is stopped	Major	See above	See above	

Failure ID	Failure	Potential root cause	Phase	Effect	Classification	Assumptions	Preliminary operational mitigation	Design recommendation
FM 02	Partial loss of electrical energy from the battery	See above	Take-off before V1	Potential loss of power, loss of grid stabilization	Minor	Remaining battery and fuel cell systems supply the aircraft	Remaining battery and fuel cell systems supply the power demand, RTO if failure occurs before V1	See above
			Take-off after V1, Climb	See above	Minor	Remaining battery and fuel cell systems are able to take-off	Remaining battery and fuel cell systems supply the aircraft, abort the mission and land as soon as possible	
			Cruise	Loss of grid stabilization	Minor	Remaining battery and fuel cell systems supply the aircraft	See above	
			Descent, Landing	Loss of grid stabilization, battery charging process is stopped	Minor	See above	See above	