Co-funded by the European Union

Ref. Ares(2026)750789 - 22/01/2026

ALBATROS



Deliverable D3.2

Assessment of strategies to mitigate the risks of aircraft with new fuels and energy systems

Abstract:

This report describes the overall risks and associated mitigations associated to novel fuels and energy systems (i.e. hydrogen storage and large lithium batteries). Analysis will focus on the identification of risks, passing through proposals of health and fault monitoring systems to mitigate any possible failure modes.

Complementary to this report is Deliverable D3.3 – Assessment of results from demonstrations on technologies to mitigate risks to future aircraft – which provides the results of the identified risks and proposed mitigations from this report.

Coordinator	Wouter van Engelen , NLR
WP Manager	Emmanuel Laroche , Onera
Grant Agreement No.	101077071
Document Identification	Deliverable Number D3.2
Status	Approved
Version	1.0
Classification	Public

This page is intentionally left blank

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

Contributing partners

Company	Name
DLR	Stephan Rempe
ONERA	Marcos Onofre
Pipistrel	Emil Jabbawi
Pipistrel	Nina Pavlovska
Pipistrel	Saidu Bashir Bello
Pipistrel	Tibor van Steenis
Pipistrel	Vincent Van Hasselt
Pipistrel	Žiga Kreuzer

Document Change Log

Version No.	Issue Date	Remarks
Draft-v1	17-nov-2025	PMT review
Draft-v2	01-dec-2025	Q review
Final		

Approval status

Prepared by: *(name)*	**Company**	**Role**	**Date**
Contributing partners	DLR, ONERA, Pipistrel	Main Author	
Concurred by: *(name)*	**Company**	**Role**	**Date**
	NLR	Quality Assurance	
Approved by: *(name)*	**Company**	**Role**	**Date**
Emmanuel Laroche	ONERA	Work Package Manager	
Wouter van Engelen	NLR	Coordinator	

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

Acronyms

Acronym	Definition
ACU	Air Control Unit
ARIA	Analysis, Research, and Information on Accidents
ATEX	Atmospheres Explosibles
BAT	Battery
BMS	Battery Management System
BMU	Battery Management Unit
CA	Control Action
CAN	Controller Area Network
CAT	Catastrophic
CFD	Computational Fluid Dynamics
CREEP	Container, Restraint, Environment, Energy Absorption, Post-crash actors
CS-23	EASA Certification Specifications CS-23 Normal, Aerobatic and Commuter Airplanes
CT	Computed Tomography
CVM	Cell Voltage Monitor
DC	Direct Current
DEP	Distributed Electric Propulsion
eMARS	Major Accident Reporting System
EMI	Electro Magnetic Interference
EPCU	Electric Propulsion Control Unit
EPS	Electric Propulsion System
EPU	Electronic Propulsion Unit
FC	Fuel Cell
FCC	Flight Control Computer
FCCU	Fuel Cell Control Unit
FCS	Fuel Cell System
H2	Hydrogen
HAZ	Hazardous
HCU	Hydrogen Control Unit
HMI	Humane Machine Interface

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

HSS	Hydrogen Storage System
HV	High Voltage
LH2	Liquid hydrogen
LV	Low Voltage
MAJ	Major
MIN	Minor
PEM	Proton Exchange Membrane
PMCU	Power Management Control Unit
RPM	Revolutions Per Minute
RTCA DO-160G	Radio Technical Commission for Aeronautics - Environmental Conditions and Test Procedures for Airborne Equipment
RTCA DO-311A	Radio Technical Commission for Aeronautics - Minimum Operational Performance Standards for Rechargeable Lithium Batteries and Battery Systems
RTD	Resistance Temperature Detector
SC	System Constraint
SOC	State of Charge
SOH	State of Health
STPA	System-Theoretic Process Analysis
T_onset	Time at which the thermal runaway is triggered
TBD	To Be Determined
TMS	Thermal Management System
TMU	Thermal Management Unit
TR	Thermal Runaway
TRB	Thermal Runaway Bed
UCA	Unsafe Control Action
V	Volt
ZEMA	Zentrale Melde- und Auswertestelle für Störfälle und Störungen

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

EXECUTIVE SUMMARY

Problem Area

The aviation industry is undergoing a transformative shift towards sustainable energy systems, including hydrogen fuel and large-scale lithium battery technologies. While these innovations promise significant environmental benefits, they also introduce complex safety challenges. The lack of comprehensive understanding of failure modes and risk profiles for these novel systems poses a barrier to their safe and effective integration into future aircraft.

Description of Work

This deliverable outlines the planned ALBATROS investigations into the risks associated with hydrogen storage and large lithium battery systems in aviation. It identifies potential hazards and failure modes, proposes initial mitigation strategies, and defines the scope of future assessments. The work is structured to support subsequent deliverables, particularly D3.3, which will present the results of demonstrations and validation activities based on the risks identified here.

Results & Conclusions

As a forward-looking document, this deliverable does not present empirical results but establishes a framework for future risk analysis and mitigation validation. It concludes that a structured and scenario-based approach is essential to address the safety implications of novel energy systems. The identified risks and proposed mitigation strategies will be further explored and validated in upcoming project phases.

Applicability

The findings and methodologies outlined in this report are applicable to aircraft design, certification processes, and operational safety planning for future aviation systems. They provide a foundation for industry stakeholders, regulatory bodies, and research partners to collaboratively address the challenges of integrating hydrogen and battery technologies into commercial and experimental aircraft platforms.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

This page is intentionally left blank

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

TABLE OF CONTENTS

Executive Summary 6

List of Figures 9

List of Tables 11

1 Introduction 12

2 Survivability of UAM: Battery Fire modelling 14

3 Characterisation of battery risks 23

4 Post impact conditions of large battery systems 25

5 Hydrogen-Electric Powered Aircraft 28

6 Conclusion 92

7 References 93

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

LIST OF FIGURES

FIGURE 1: SCHEMATIC REPRESENTATION OF HOW A LITHIUM-ION BATTERY WORKS. 16
FIGURE 2: PROPAGATION AND ATTENUATION OF THERMAL RUNAWAY. 17
FIGURE 3: 2D AXISYMMETRIC MESH OF THE 18650 CELL FOR MODETHEC (3225 CELLULES). 21
FIGURE 4: LEFT: DIAGRAM OF THE DISCRETIZED CALCULATION DOMAIN FOR SIMULATING THE FIRST AND SECOND DEGASSING. RIGHT: DIAGRAM OF THE STRUCTURE OF A MODERATELY UNDER-EXPANDED JET. 21
FIGURE 5: SIMPLIFIED TRB TEST BENCH MESH WITH REFINEMENT CRITERIA USED: A) OVERVIEW OF THE MESH THROUGH THE SECTIONS, B) ZOOM ON A SECTION OF THE MESH INSIDE THE INYECTOR, C) REFINEMENT CRITERIA INSIDE THE JET REGION FOR SHOCK WAVE CAPTURE. 22
FIGURE 6: ELECTRONICS IN TEMPERATURE CHAMBER 24
FIGURE 7: BRACKETS USED FOR THE DROP TEST INDICATING THE CELL SUPPORT AREA 25
FIGURE 8: BATTERY THERMAL RUNAWAY CONTAINMENT TEST 26
FIGURE 9: THE FOUR STEPS OF STPA [36]. 29
FIGURE 10: BASIC CONTROL LOOP [36] 29
FIGURE 11: UNIFIER 19 CONCEPT [37]. 30
FIGURE 12: CONTROL STRUCTURE. 34
FIGURE 13: CA.1 SET AIRCRAFT THRUST. 37
FIGURE 14: CA.2 SET FUEL CELL POWER. 38
FIGURE 15: CA.3 SET AIR MASS FLOW RATE. 38
FIGURE 16: CA.4 SET AIR PRESSURE. 39
FIGURE 17: CA.5 SET DC/DC CURRENT DRAW. 39
FIGURE 18: CA.6 SET H2 MASS FLOW RATE. 40
FIGURE 19: CA.7 SET TANK PRESSURE. 40
FIGURE 20: CA.8 SET INVERTER CURRENT DRAW. 41
FIGURE 21: CA.9 SET BAT DC CURRENT DRAW 41
FIGURE 22: CA.10 SET REQUIRED BAT POWER. 42
FIGURE 23: CA.11 SET EPU POWER 42
FIGURE 24: CA.12 SET COOLANT MASS FLOW. 43
FIGURE 25: CA.13 SET POSITION OF MIXING VALVE. 43
FIGURE 26: DLR STUDY, AFT FUSELAGE LH2 TANKS (LIGHT BLUE COLOR). [42] 74
FIGURE 27: DLR STUDY, TANK MOUNTING STRUCTURE. LEFT: SPOKE TYPE, RIGHT: X-ROD TYPE. [42] 75
FIGURE 28: DLR STUDY: LH2 TANK CRASH STRUCTURE. [42] 76
FIGURE 29: CONFIGURATION 1: MID-FUSELAGE, ISO LEFT VIEW. [43] 79
FIGURE 30: CONFIGURATION 1: MID-FUSELAGE, SIDE VIEW. [43] 79
FIGURE 31: CONFIGURATION 2: AFT-FUSELAGE, ISO LEFT VIEW. [43] 80
FIGURE 32: CONFIGURATION 2: AFT-FUSELAGE, SIDE VIEW. [43] 80
FIGURE 33: CONFIGURATION 3: FRONT-FUSELAGE, ISO LEFT VIEW. [43] 81
FIGURE 34: CONFIGURATION 3: FRONT-FUSELAGE, SIDE VIEW. [43] 82

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

FIGURE 35: CONFIGURATION 4: POD-WINGS, ISO LEFT VIEW. [43] 83
FIGURE 36: CONFIGURATION 4: POD-WINGS, SIDE VIEW. [43] 83
FIGURE 37: DUAL MOTOR ASSEMBLY. 87
FIGURE 38. 4-BLADED PROPELLER. 88
FIGURE 39. TEST RIG ASSEMBLY 88
FIGURE 40: DUAL MOTOR TEST 1 @2300RPM. 90

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

LIST OF TABLES

TABLE 1: LIST OF CONVENTIONAL CATHODES 15
TABLE 2: LIST OF CONVENTIONAL ELECTROLYTES. 16
TABLE 3: NON-EXHAUSTIVE LIST OF VARIOUS INCIDENTS/ACCIDENTS INVOLVING LITHIUM BATTERIES IN FRANCE. 18
TABLE 4: LIST OF SYSTEM CONSTRAINTS....33
TABLE 5: UCA MATRIX....44
TABLE 6: UCA CLASSIFICATION....46
TABLE 7: DUAL-MOTOR TESTS....89

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

1 INTRODUCTION

1.1. Project Context

Work package 3 of the ALBATROS project aims to support the safe integration of novel fuels and energy systems into future aircraft architectures. As aviation transitions toward more sustainable technologies, such as hydrogen storage and large-scale lithium battery systems, it is critical to understand and mitigate the associated risks. These technologies introduce new failure modes and operational challenges that require thorough investigation to ensure safety, reliability, and regulatory compliance.

This deliverable builds upon the initial assessment presented in Deliverable D3.1, which included an analysis of measures aimed at improving the survivability of passengers and crew in future aircraft. It focuses on identifying potential risks associated with emerging energy systems and outlines the planned investigations to assess and mitigate these risks. Therefore, this document serves as a foundation for subsequent analyses and demonstrations, particularly those presented in Deliverable D3.3, which will detail the outcomes of the mitigation strategies and validation efforts.

1.2. Research Objectives

The primary objectives of this deliverable are:

1. Risk Identification: To systematically identify potential failure modes and hazards associated with hydrogen storage systems and large lithium battery installations in aircraft.
2. Preliminary Risk Assessment: To outline the scope and nature of risks that require further investigation, including operational, environmental, and safety-related concerns.
3. Mitigation Planning: To propose initial mitigation strategies and define the parameters for future testing and validation.
4. Framework Establishment: To establish a structured approach for the assessment of risks and mitigation effectiveness, which will be applied in future deliverables.

1.3. Approach

The approach taken in this deliverable reflects the differing maturity levels and operational contexts of battery-electric and hydrogen-powered aircraft technologies.

1.3.1. Battery-Electric Aircraft

Battery-electric aircraft, such as the certified Pipistrel Velis Electro, are already in commercial operation. As such, the focus of the risk assessment is on:

- Scaling and Continuous Improvement: Evaluating risks associated with scaling up battery systems for larger aircraft and longer missions.
- Field Data Analysis: Leveraging operational data from existing aircraft to identify emerging risks and validate mitigation strategies.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

- Prototype Testing: Conducting targeted tests on new battery configurations and integration concepts to assess safety and reliability.

1.3.2. Hydrogen-Electric Powered Aircraft

Hydrogen aircraft remain in the research and development phase, with no certified platforms currently in operation. Therefore, the approach is more conceptual and safety-focused:

- System-Theoretic Process Analysis (STPA): Applying STPA to identify potential hazards and unsafe control actions in hydrogen aircraft systems.
- Conceptual Risk Mapping: Exploring risks associated with hydrogen storage, distribution, and propulsion under various operational scenarios.
- Design Safety Assessment: Evaluating safety implications of different hydrogen system architectures and integration strategies.
- Scenario-Based Analysis: Defining representative use cases to guide future experimental validation and demonstration activities.

This bifurcated approach ensures that both technologies are assessed appropriately according to their development stage, enabling targeted and effective risk mitigation strategies to be developed in subsequent phases of the ALBATROS project.

1.4. Structure of the Document

Given the two distinctive different approaches for battery electric aircraft and hydrogen powered aircraft, the document is structured in two parts accordingly where:

- The first part focusses on the risks and mitigations associated with battery propulsion:
  - Starting with a cell level analysis of 18650 cylindrical cell thermal runaway simulation
  - Characterisations of battery risks along the lifetime of an aircraft, such as risks related to environmental conditions and the use of dissimilar battery modules in a system.
  - Post impact conditions on the battery system, including a drop test of a battery module.
- The second part of the report goes into a detailed STPA safety assessment method of a hybrid hydrogen-electric aircraft, including:
  - STPA methodology including the model control structure, identification of all loss scenarios, and a list of all defined critical parameters for monitoring.
  - A study into the influence of hydrogen fuel cell system component placement on the survivability.
  - Test of a Fuel cell powertrain component failure design improvement.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

2 SURVIVABILITY OF UAM: BATTERY FIRE MODELLING

2.1. Industrial Research Objectives

Lithium-ion (Li-ion) battery technology is one of the favorite candidates for a new electrified aircraft. These batteries are prone to thermal runaway (TR), which causes the release of toxic gases and fumes that not only risk igniting in a deflagration, but also rapidly progressing to detonation.

The objectives of T3.2 are therefore to address relevant aeronautical scenarios related to faulty Li-ion batteries in order to develop a simulation methodology (by coupling ONERA's fluid CEDRE solver with ONERA's material degradation MoDeTheC solver), to characterize and model this thermal runaway phenomenon. To this end, the actions to be implemented within ONERA's HEAT (High Energy and AeroThermal issues) unit are listed below:

- Develop a method to couple a Navier-Stokes solver with a material degradation solver in order to better understand and anticipate the phenomenon of thermal runaway.

2.1.1. Scope of the Study

A Li-ion battery is a rechargeable energy storage device based on the reversible transit of Li^+ ions between the anode and cathode. Compared to other energy storage technologies, Li-ion batteries are characterized by higher specific energy, energy density, and energy efficiency, as well as a longer lifetime.

Due to these characteristics, Li-ion technology is expected to play a crucial role in the transition to carbon-neutral storage solutions. Currently, Li-ion cells successfully address issues related to the storage and management of energy generated by solar and wind technologies.

Energy storage devices based on Li-ion technology come in a variety of cell formats, which have been developed to meet a wide range of needs depending on the amount of energy to be stored: pouch, prismatic, cylindrical, and coin-shaped.

2.1.1.1. The Risk of Fire in Batteries

Today, this technology has reached such maturity that it is at the heart of the development of modern electric vehicles. For aerospace applications, the energy/power levels required are high. It is therefore necessary to integrate the cells into modules or packs and connect them to the electrical network via a battery management system (BMS), in order to meet performance and safety requirements. This in turn requires an assembly offering high mechanical strength at the cell level, which is why we focus on prismatic and cylindrical cells.

2.1.2. Types of Battery Thermal Runaway

In the event of a single cell failure, heat can spread from one cell to another, triggering thermal runaway (TR) in adjacent cells, which multiplies the problem of heat generation and fire by the size of the system. In this regard, three characteristic runaway scales can be identified. Each of these is used depending on the

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

order of magnitude of the stored energy required. As this order of magnitude increases, the most critical incidents (larger fires and explosions) are likely to occur:

- **Cell level**, with a characteristic dimension of a few cubic centimeters, which corresponds to an energy scale of the order of W · h.
- **Module level**, with a characteristic size dimension of between 0.1 − 1.0 cubic meters (up to 10 000 cell units), which corresponds to an energy scale of the order of KW · h.
- **Container level**, which are filled with several hundred modules, reaching characteristic dimensions of several cubic meters, corresponding to an energy scale of the order of M W · h.

The origin of failures in large batteries is often attributed to a defect at the smallest scale, which spreads from one scale to another due to different heat transfer mechanisms. Therefore, lithium-ion batteries are prone to the phenomenon of *thermal runaway (TR)*. For this reason, in order to avoid failures as much as possible, improving production processes (quality control), certification regulations, and maintenance methods/processes has become an imperative goal.

So, TR is the phenomenon whereby the lithium-ion cell enters a state of self-heating accompanied by the production of hot, flammable, and toxic gases, which can lead to fires and/or explosions.

2.1.3. Components of a 18650 Battery

The 18650 format is a cylindrical cell with a diameter of 18 mm and a length of 65 mm. This format is widely used in industry and will be taken as the subject of study. A battery can therefore consist of one or more cells. A cell is typically composed of the following elements, (Fig. 1)

- **Cathode** : This positive electrode consists of a current collector (usually aluminum) coated with the active cathode material. The chemical compounds are in the form of a metal salt that includes Li and related metal alloys such as : M n, F e, Co, N i, Al to O (see Table 1).
- **Anode** : Like the cathode, the anode consists of a thin metal current collector (usually a copper foil) covered with an active material. The most common are Li x C 6 .

	Chemical composition	Energy density $[WH\,.L^{-1}]$	Specific energy $[WH\,.L^{-1}]$
LPF	$Li\ Fe\ P\ O_4$	2200	320
NMC	$Li\left(Ni_x\ Mn_y\ C_z\right)O_2$	2800 – 3700	620 – 760
LCO	$Li\ Co\ O_2$	3300	650
NCA	$Li\left(Ni_x\ Co_y\ Al_z\right)O_2$	3700	760
LMO	$Li\ Mn_2\ O_4$	2100	480
LMNO	$Li\left(Ni_x\ Mn_y\ \right)O_4$	2600	570

Table 1: List of conventional cathodes .

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

- **Electrolyte** : acts as an ion carrier. The selection of alkyl carbonate solutions is a good compromise that offers stability in terms of reactions with electrodes, good conductivity for Li+, and low overall toxicity when handled (see Table 2).

	Designation	Reduced chemistry	Boiling point $[°K]$
EC	Ethylene Carbonate	$C_3\ H_4\ O_3$	521.15
DMC	Dimethyl Carbonate	$C_3\ H_6\ O_3$	363.15
DEC	Diethyl Carbonate	$C_5\ H_{10}\ O_3$	399.15
EMC	Ethyl Methyl Carbonate	$C_4\ H_8\ O_3$	380.15
PC	Propylene Carbonate	$L\ C_4\ H_6\ O_3$	515.15
$Li\ P\ F_6$	Lithium Hexafluorophosphate	$Li\ P\ F_6$	----------

Table 2: List of conventional electrolytes.

- **Separator** : micro-perforated insulating layer(s) that simultaneously allow Li + -ions to migrate from one electrode to another and prevent internal short circuits caused by direct contact between the anode and cathode.
- **Solid electrolyte interphase (SEI)** : is an interface that protects the anode and prevents any further reaction of the electrolyte, while being permeable to migrating ions.
- **Binders** : the active ingredient is mixed with a liquid polymer-based mixture called «binder». It has two main functions :
    - it sticks the active material to the current collector and
    - it must be as transparent as possible during charging and discharging, which means that it must not react with the migrating lithium.

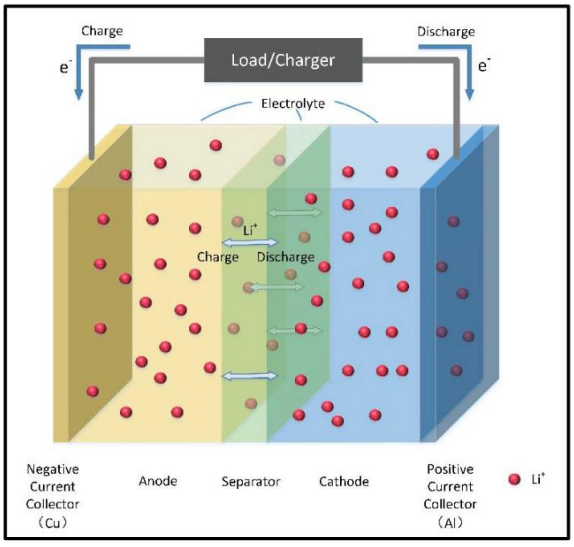


Figure 1: Schematic representation of how a lithium-ion battery works.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

2.1.4. The Triggers of Thermal Runaway

There are three phenomena classified as *abuse*, which can lead, either alone or in combination, to battery ET. These are mechanical, electrical, and/or thermal abuse (the latter being the direct cause of TR). The links between the different types of abuse and TR are shown in Fig. 2.

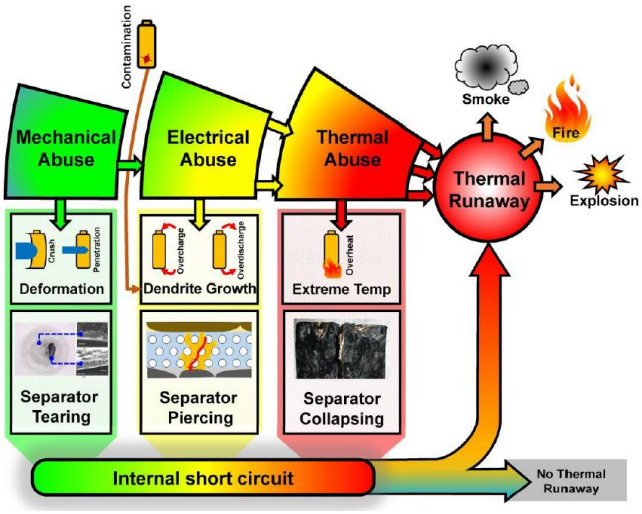


Figure 2: Propagation and attenuation of thermal runaway.

The type of abuse with which the best repeatability and control can be ensured when studying TR is thermal abuse, i.e., overheating, which can be caused by:

- exposure of the battery to an external heat flow for a given period of time, causing a significant rise or increase in the temperature of the internal components,
- internal electrical malfunctions, or
- mechanical incidents.

These scenarios lead to the release of high-energy gases resulting from the pyrolytic degradation of the battery's internal components. It therefore seems appropriate to break down the process leading to the TR of 18650 cells into three stages, associated with key temperatures:

1. Degradation phenomenon inside the cell up to a temperature of 398.15 °K
2. Opening of the cell and gas ejection between 398.15 °K and 453.15 °K
3. Important reaction kinetics in terms of degradation and flame generation from 453.15°K. This last stage initiates the onset of thermal runaway at a temperature T_0 which depends on the composition of the cell.

During these steps, the sources of species are identified as the anode, cathode, electrolyte, binders, and SEI :

- Firstly, SEIs break down by producing CO_2 and C_4H_4
- As the anode lithiates, i.e., degrades due to lithium, the binders are reduced, producing H_2, light hydrocarbons $C_1 - C_4$, CO and CO_2 , and
- Finally, the cathode releases O_2 which oxidizes the electrolyte, producing mainly CO_2 and H_2O

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

2.2. State of the Art

This chapter describes the current state of research on battery fires and explosions, both experimental and numerical. The aim here is first to identify what is currently being done internationally and then to specify ONERA's position and capabilities, as well as the expected progress through the implementation of the project.

2.2.1. Accidentology Surrounding Li-ion Technology

In France, the ARIA database (for Analysis, Research, and Information on Accidents) records incidents, accidents, or near misses involving lithium-ion batteries. The eMARS (Major Accident Reporting System) database in the European Union and the ZEMA (Zentrale Melde- und Auswertestelle für Störfälle und Störungen) database in Germany also track these types of incidents.

Date	Incident	Cause
05/1999	Explosion at a recycling facility in Rogerville	Fire at the facility causing explosions due to lithium coming into contact with water used to extinguish the fire
01/2000	Fire in an electric battery factory in Bordeaux	Short circuit during a sudden discharge of a battery
09/2007	Fire at an electrical equipment manufacturing plant in Poitiers	Short circuit in a marine lithium battery during assembly
05/2009	Fire at a car manufacturing plant in Aniche	Overheating short circuit in a lithium battery in a vehicle under manufacture that was being charged overnight
06/2016	Fire at an automotive factory in Fontenay-le Comte	Defective lithium battery
05/2017	Fire at a parcel center in Moissy-Cramayel	Battery crash
07/2017	Fire at an industrial testing center in Verneuil-en-Halatte	Battery short-circuit test
08/2019	Battery fire at a battery production plant in Chasseneuil-du-Poitou	Insulation fault
11/2019	Fire at a lithium-ion battery research company in Bernin	Electric arc during voltage measurement on a battery at the end of production
03/2021	Explosion of a shed resulting in the death of the owner in Berny-Rivière	Explosion of Li-ion batteries in an electric cart

Table 3: Non-exhaustive list of various incidents/accidents involving lithium batteries in France.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

2.2.2. Studies on Thermal Runaway

Even though the failure rate of Li-ion cells is very low, estimated at 1 in 40 million, the widespread use of this technology around the world and its massive adoption mean that many incidents have been recorded. For this reason, numerous studies have been devoted to reproducing Li-ion accidents, both experimentally and numerically. Compilations of results are available from the following sources [1] [2] [3], which are essential for feeding simulation frameworks with operating conditions and geometries of interest.

Access to operating conditions is essential and can be complex for such safety processes. Gas release after cell opening is studied in [4] [5] [6] [7], with particular attention to the opening process in [8]. Cell fire is characterized in [9] [10] [11] [12], leading to documentation of its impact on the heat propagation process in larger batteries [13] [14] [15] [16].

More rarely, explosions caused by vent gases are beginning to be documented, paving the way for high-fidelity simulations of these critical events [17] [18] [19].

Once the operating conditions have been selected, scenarios using simulation can be proposed, for example by calculating the influence of TR on the cell structure [20] [21], or by reproducing internal processes [22] [23]. In this respect, the use of computational fluid dynamics (CFD) becomes essential for observing and predicting TR-induced flows, including gas release, fires, and explosions. In recent studies, CFD has been applied to the study of cellular gas release [24] [25] and cellular fire [26], demonstrating the feasibility and potential of these simulations. Applications to heat propagation for cooling system design are also discussed by [27] [28] [29].

2.2.3. Methodology of the Study

The role of the ONERA in the T3.2 of the Albatros project is to treat relevant aeronautical scenarios related to failing Li-ion batteries to propose a multi-physics numerical strategy for the CFD simulation, in order to better understand and model the thermal runaway (TR) phenomenon.

Taking experimental [6] [7] [18] [19] and numerical [25] [30] [31] [32] references as a starting point, a critical path of activities that can enable the development and realization of coupled (fluid and solid) thermal runaway modelling can be proposed as follows :

- Reduced kinetic scheme for 18650 Li-ion cell (24 species and 93 reactions)
- 0D isochore reactor (Cantera)
- 1D premixed laminar flame (Cantera)
- 2D axisymmetric configuration (fluid domain - CEDRE)
  - Shock propagation in under-expanded jets
  - Jet flame of Li-ion vent gases (forced ignition)
- 3D Battery-Thermal-Runaway test bed (fluid domain -CEDRE)
  - Non-reactive under-expanded jet
- 2D axisymmetric porous media undergoing pyrolysis
- 2D axisymmetric configuration : porous media + fluid (non-reactive/reactive)

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

2.2.4. From Detailed Kinetic to Analytically Reduced Chemistry

If we assume that the cell behaves like a closed reactor, it is then possible to link the degradation of components to simplified reactions producing gases. Among the mechanisms of gas production, the destruction of the electrolyte plays a decisive role when it can be easily vaporized at the usual temperatures reached inside a faulty cell. Once in gaseous form :

- a fraction of the electrolyte may react inside the cell in the presence of oxygen released by the cathode and the SEI, then
- the vapours and liquid from the electrolyte may also be carried away when exposed to the open air, mixed with the products of other decomposition reactions.

In the event of a fire, electrolyte species burn along with other products generated by the decomposition of other internal cell parts ; these mixtures can influence flame dynamics. In this sense, to simplify the study of electrolyte oxidation and fires, it is proposed to reduce these phenomena to two «elementary» problems in CANTERA (a suite of open source tools for problems related to chemical kinetics, thermodynamics, and transport processes):

A. oxidation of electrolytic species in isochoric reactors 0D, and
B. 1D premixed flames of mixtures of electrolytic species with common release gases.

2.2.5. Numerical Simulation in CEDRE

The first numerical case study carried out as part of the ALBATROS project is an axisymmetric 2D simulation; this configuration is taken from the work published in 2021 by Kim [25].

Next, a 3D numerical study based on the «Thermal Runaway Bed» developed as part of Cellier's thesis [32] is presented. This case allows us to compare (with respect to experimental and numerical results) the characterization of the first venting (sub-expanded jet)

2.2.5.1. Axisymmetric 2D configuration: internal pyrolysis of the 18650 cell

This configuration will be used to characterize the flow of the second venting. The discretized calculation domain is shown in Figure 3.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

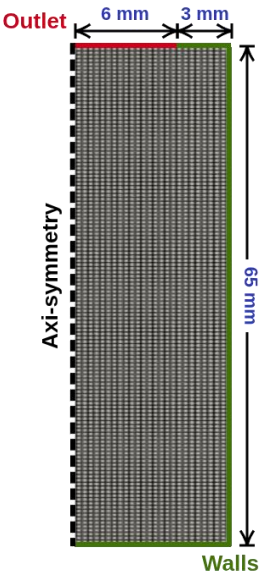


Figure 3: 2D axisymmetric mesh of the 18650 cell for MODETHEC (3225 cellules).

2.2.5.2. Axisymmetric 2D configuration

Such configuration (Figure 4) will be used to :

- characterize the more critical conditions of the first venting, i.e., non-reactive supersonic jet ; and the second venting, i.e., reactive sub-expanded jet ;
- test the reduced chemical kinetic model in a more practical setting, and
- validate a compressible and reactive CFD simulation model, then couple it to a Li-ion battery model that follows an internal pyrolysis process in the MoDeTheC solver.

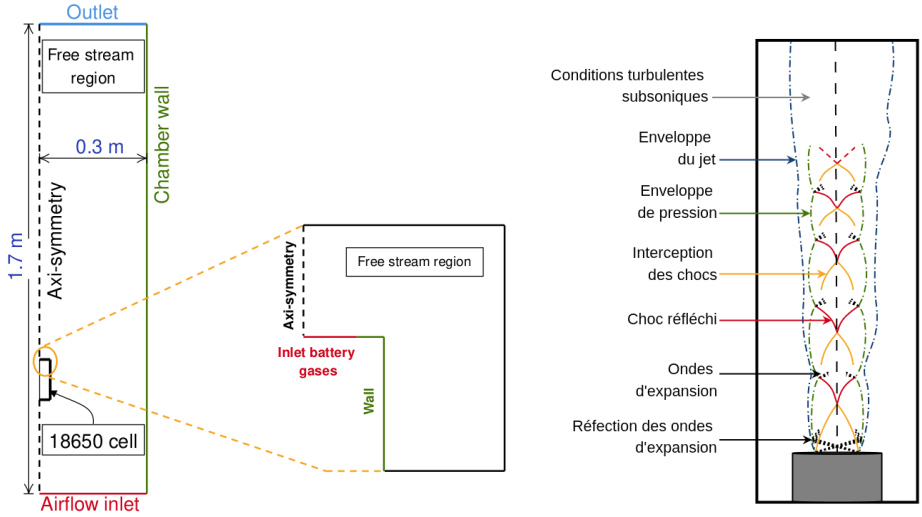


Figure 4: Left: Diagram of the discretized calculation domain for simulating the first and second degassing. Right: Diagram of the structure of a moderately under-expanded jet.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

2.2.5.3. 3D configuration : Thermal Runaway Bed (TRB) test

This configuration (Figure 5) is placed at the cell level and is designed to reproduce the first TR venting (opening with the formation of a supersonic jet).

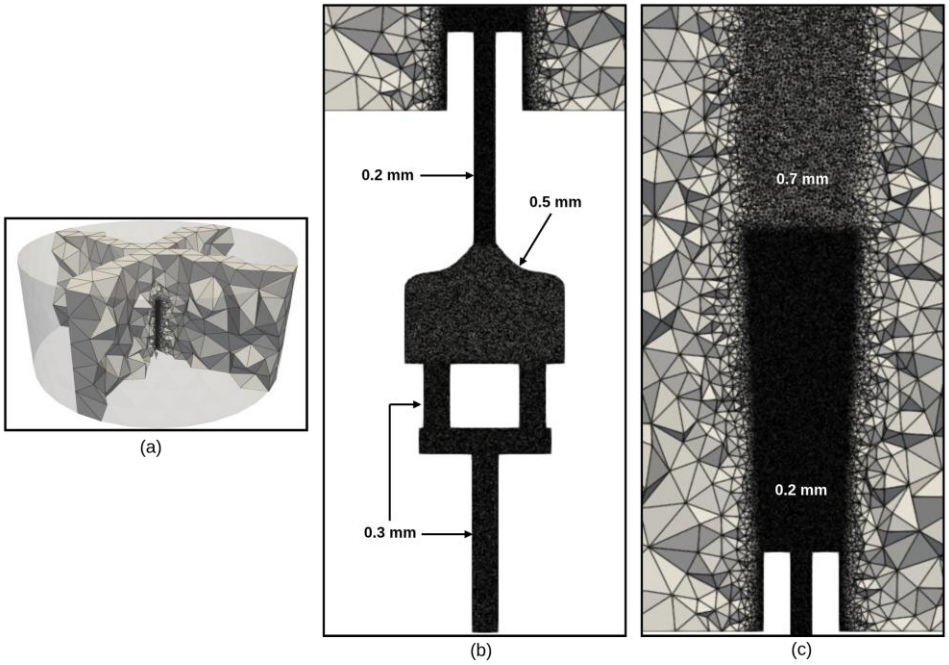


Figure 5: Simplified TRB test bench mesh with refinement criteria used: a) overview of the mesh through the sections, b) zoom on a section of the mesh inside the inyector, c) refinement criteria inside the jet region for shock wave capture.

2.2.5.4. Coupled simulation

Using the numerical tool CWIPI [33] [34] [35], communication and synchronization have been established between the MODETHEC simulation of internal battery degradation caused by pyrolysis, and the CEDRE 2D axisymmetric reactive simulation.

This configuration was chosen to offer a combined study approach using CFD software and software describing the internal degradation of a cell with a porous medium model undergoing pyrolysis.

2.2.6. Conclusion

This chapter summarizes the essence of the scientific report, highlighting the methodology implemented to address the challenges presented in chemical kinetics modelling, numerical simulations, validation efforts, and safety insights related to Li-ion battery fires in the European ALBATROS project context.

A rigorous modelling framework for battery fire scenarios has been proposed, which enhance predictive capabilities crucial for safety assessments and regulatory compliance. Future perspectives include coupling more detailed turbulent combustion models and extending simulations to large battery packs for electric vehicles or energy storage systems.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

3 CHARACTERISATION OF BATTERY RISKS

Chapter 3 Characterisation of battery risks describes the tests that will be performed related to the characterisation of battery risks all along the lifecycle of an aircraft. This includes environmental risks (e.g. vibrations, temperature, etc.) and operational risks, focusing on having an aircraft using battery packs with different SOH in parallel, including an analysis of the consequences and mitigations.

3.1. Cell Heat Generation and Calorimetry Tests

Measuring heat generation during normal cycling allows the validation of thermal management models, quantifying the onset of thermal runaway allows for better BMS safety mechanism design.

This test justifies design features (insulation and venting) and informs emergency response planning (fire suppression capacity needed). It also ties into thermal runaway prevention by informing on excessive temperature avoidance during fast charge/discharge.

Single cells or a small cell stack are placed in a calorimeter which is then cycled through charging and discharging at various rates while recording the heat generated. In the second part the cell is induced into thermal runaway and the T_onset, time is recorded. These tests are done at different SoC to see how the stored energy affects the outcome.

The calorimetry results support the risk characterization of use case 5 from Albatros Deliverable D1.1 by quantifying the following parameters:

- Single cell trigger conditions to understand safe operating range for battery cells and when they become a fire hazard which requires the emergency response as described in D1.1.
- Thermal runaway behaviour with respect to amount/volume of gases being released, temperature of the venting gasses, and amount of fire suppression capacity needed.
- Fast-charging and discharging limits to ensure internal cell temperatures do not exceed the limit.

3.2. Parallel Battery Packs with Dissimilar State of Health

The two battery packs connected in parallel on the Pipistrel Velis Electro should exhibit similar ageing characteristics. This expectation arises from the fact that both packs are subjected to nearly identical electrical loads, thermal cycles, and operational conditions. The uniformity in their environment and usage patterns suggest that their SOH should degrade at a comparable rate.

However, it cannot entirely be excluded that one pack might age faster than the other. Various factors, such as manufacturing differences or defects, and variations in material properties could contribute to a divergence in ageing rates. This potential disparity could lead to a significant difference in SOH between the two packs over time.

This study will investigate what could happen if battery packs with significant differences in SOH would be mixed, either by dissimilar ageing or by replacement of one of the packs with fresh cells. In addition, other scenarios of mixed batteries will be analysed, such as combining packs which use different cell chemistries.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

The main purpose of this study is to understand the effect of differently aged packs, and if this brings any safety risks due to unexpected electrical behaviour between the two packs and how this could be detected.

3.3. Extreme Temperature Performance Tests

In flight, the battery can be subjected to frigid temperatures at altitude as well as elevated temperatures on ground/or due to high current operations. The BMS electronics must remain reliable to monitor and protect the cells under these conditions likewise the compression pads must continue exerting the optimal pressure on cells.

The test verifies the designs compliance with aviation requirements for temperature resilience and ensures that neither severe winter cold nor internal heat will compromise the battery system; in essence the electronics keep functioning preventing overcharge and thermal runaway and the protective pads maintain their spring force.



Figure 6: Electronics in temperature chamber

The test articles in question will be put inside an environmental chamber, the chamber cycles through the operational temperature extremes (-40°C & 60°C) to represent the coldest startup and hottest operating conditions the aircraft might experience. The test articles will be held at these temperatures for specified durations while monitoring their functionality and structural integrity. The electronics will be cycled as well at these extreme temperatures to verify they continue to operate within specifications without erratic behaviour or failure. Finally, other materials likely to be used in a battery pack that may experience material property change or degradation will be tested as well.

Successful passage of this test indicates there is alignment with guidance by RTCA DO-160G's non-operational cold soak and maximum rated temperature.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

4 POST IMPACT CONDITIONS OF LARGE BATTERY SYSTEMS

Chapter 4 Post impact conditions of large battery systems include all tests directly related to the hazards associated with potential crash scenarios of aircraft utilising large battery systems. The scope includes a study on supporting battery cells within a module to minimise damage due to a sudden impact, module level strength assessment, and testing of materials to contain a thermal runaway in case cells do get punctured in case of a crash.

4.1. Cell Level Drop Test

A sudden impact, such as a collision or drop, can lead to internal cell damage, short circuits, or even thermal runaway. Therefore, understanding how to support battery cells within a battery module to minimise such damage is essential for improving safety, reliability, and longevity of the battery system.

For this test a setup has been developed to gradually increase the impact energy applied on a battery cell. The tested cells will then be assessed based on a non-destructive assessment method (e.g. cell electrical characterisation or CT scan) to establish whether the cells have internal damage, potentially reducing capacity and increasing hazards, or if it is safe if they would continue to be used on an aircraft.

Three different support brackets will be tested where the battery cells will be exposed to different levels of impact energy. The difference between the brackets is the support area: bracket 1 provides a total of 12% support compared from two supports, each covering 6% of the length of the cell. Brackets 2 and 3 support 54% and 78% respectively, as can be seen in Figure 7.

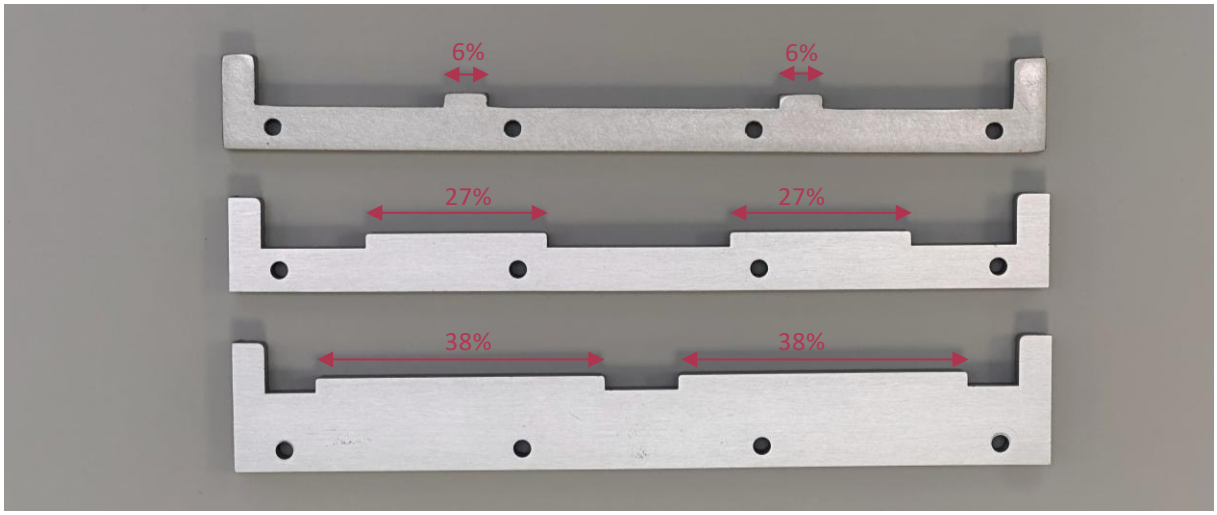


Figure 7: Brackets used for the drop test indicating the cell support area

The main objective is to understand if a severe impact scenario like this could result in hidden risks, causing increased probability of failure were the batteries continued to be used after a significant impact event. In addition, mechanical failure inside the battery cell could result in a thermal runaway which would pose an immediate hazard to the occupants during evacuation. Depending on whether any cells go into thermal runaway during the test, this might be included in the analysis of the results.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

4.2. Module Level Drop Test

In a hard landing or crash, a battery may experience high-G jolts or be flung against structures, if the structure were to be split open or cells to be crushed it could lead to fuel spillage (flammable electrolyte) or an instantaneous battery fire.

This test verifies that the battery enclosure can withstand sudden shocks or impacts without immediate catastrophic failure, in essence a level of crashworthiness is demonstrated. Practically this means that cell leakage or fire ignition is prevented for at least several minutes post impact which is essential for first responders to respond in time. The insights from different impact orientations also guide design reinforcements.

The test article will be dropped from a designated height (typical procedures indicate a height of about 1m onto concrete or steel). It (test article) will be dropped multiple times to cover different angles e.g. on a corner, edge, or bottom to challenge the enclosure weakest points. High speed cameras and sensors will be used to observe the impact and the resulting deformation, additionally after each drop the battery is inspected for damage leakage or thermal runaway indicators I.e. cracked housing exposed cells or wiring, electrolyte spillage, smoke or unusual heat. The packs electrical isolation is also measured to ensure it has not shorted internally.

The test criteria demands that the battery should not rupture or catch fire from impact, successful passage of this test aligns with RTCA DO-311A/DO-160G's mechanical abuse criteria which include drop impacts as part of the qualification for aviation batteries.

4.3. Thermal Runaway Containment

A lithium-ion cell in thermal runaway can reach over 800 °C, vent toxic flammable gas and eject shrapnel, with the potential to propagate to neighbouring cells and engulf an entire pack. This is considered a catastrophic failure mode in aviation safety.

The containment test validates that the battery design can withstand such an event without compromising aircraft safety. In practical terms this means that the test if successful indicates that, if a cell fails internally or due to external damage, the fire and byproducts remain confined to the battery enclosure.

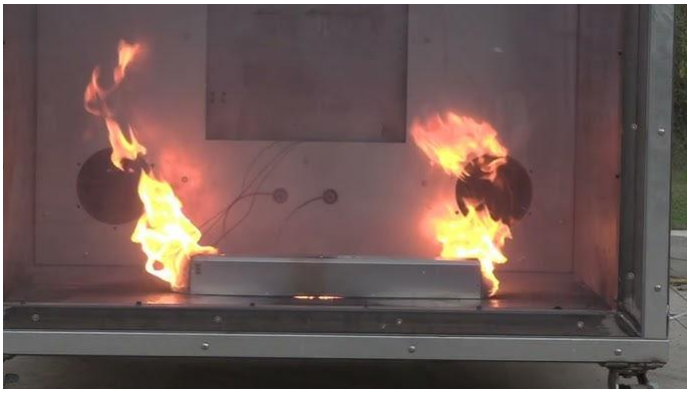


Figure 8: Battery thermal runaway containment test

One cell or more of a battery module will be intentionally triggered using a controlled heat source or overcharge while the module is sealed inside a prototype containment enclosure. Multiple enclosure materials are tested to compare their performance. During and after the test,

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

monitoring will be done to ascertain whether any flames or ejecta escape the battery enclosure through any means except via the designated venting paths.

Successful passage of this test indicates that there is protection for passengers and critical systems from direct flame exposure and enough time for the crew and first responders to react, this also aligns with RTCA DO-311A's focus on thermal event management without affecting surrounding systems.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

5 HYDROGEN-ELECTRIC POWERED AIRCRAFT

This chapter investigates strategies for mitigating risks in hydrogen-electric powered aircraft. Because this architecture is significantly more complex and distinct from conventional designs, a novel STPA-based safety analysis is applied to assess the observability of failure modes in hydrogen-electric powertrain integrations and to identify the critical parameters required for effective in-flight health monitoring. Another area for mitigating risk involves examining how the placement of hydrogen fuel-cell components within the aircraft affects overall survivability. Ending this section with a design improvement concept, the work reports on the construction of a physical dual-motor test rig and its experimental evaluation under varied operating scenarios to verify gains in redundancy and propulsion-system safety.

5.1. System Theoretic Process Analysis

Hybrid hydrogen–electric powertrains integrate cryogenic hydrogen storage and conditioning, fuel cells, high-voltage power electronics, batteries, and advanced control software—all tightly coupled with airworthiness-critical systems such as thermal management and ventilation. This multi-domain integration (software–electrical–mechanical–human) significantly enlarges the scale of hazardous scenarios compared with conventional kerosene-based architectures.

Conventional safety assessment methods excel at component-level failure reasoning but can underrepresent events that emerge from control interactions across subsystems, software behaviors, and operational context, especially in novel architectures with limited operational data. To address this, we apply System-Theoretic Process Analysis (STPA) to a hybrid hydrogen–electric aircraft powertrain. STPA frames safety as a control problem and systematically identifies unsafe control actions, causal factors, and constraints across the system, including human operators, automation, and procedures. This enables us to prioritize safety-critical parameters for health monitoring that reflect both component-level degradation and system-level interaction risks.

5.1.1. The STPA Methodology

System Theoretic Process Analysis or STPA is a safety assessment method developed by Dr. Nancy Leveson at the Massachusetts Institute of Technology. It is a systematic approach to identifying and mitigating safety risks in complex systems while focusing on the interactions between systems or components rather than just the components themselves. The STPA methodology is based on the STAMP Model which states that accidents are caused by inadequate control. It addresses the question of how inadequate control in a design is found. Hence the STPA considers that accidents can be caused by unsafe interactions of system's components without the individual component failing. The STPA Process consists of the following four central steps:

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

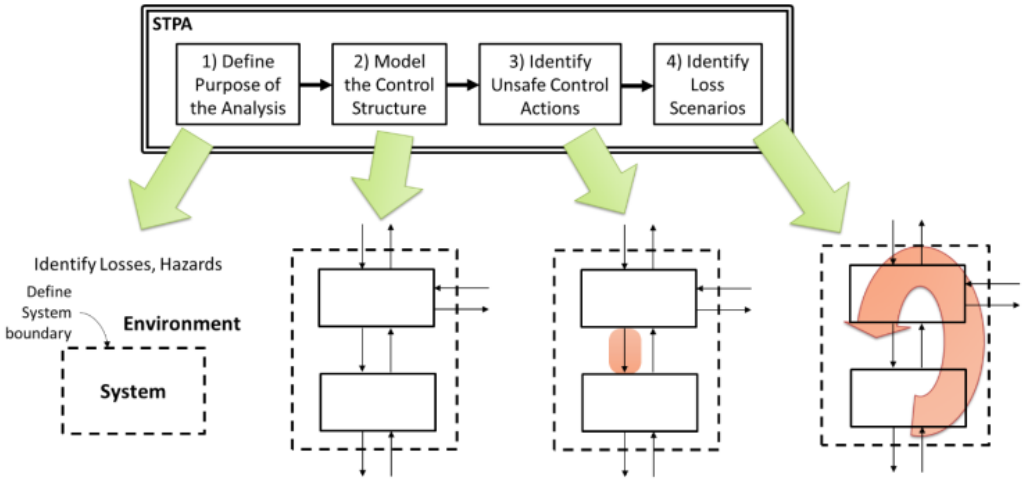


Figure 9: The four steps of STPA [36].

The first step of the STPA involves the definition of the purpose of the analysis and includes the following sub steps:

- Definition of system-boundary and context
- Definition of losses to be prevented
- Identification of system-level hazards
- Identification of system-level constraints

The control structures are modelled as part of the second step of STPA. A Control Structure is a hierarchical system model that is usually composed of several feedback control loops.

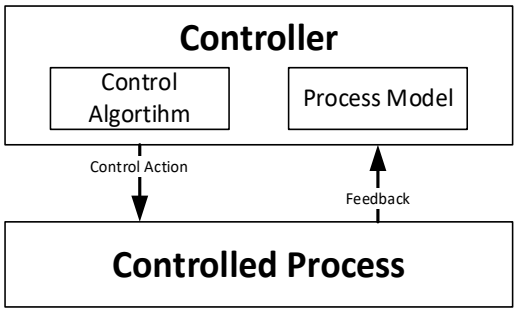


Figure 10: Basic Control Loop [36].

The Control and Feedback flows are modelled between controllers and controlled processes and at least one Control Action - CA is allocated to every control flow. During the conduction of the third step of the STPA, Unsafe Control Actions – UCA are identified. They describe the undesired behavior of the system that is to be prevented. Four categories of UCA's are defined to describe the way a CA can be unsafe:

1. Not Providing the CA causes Hazard	2. Providing the CA causes hazard	3. CA came too early, too late, out of order	4. CA was stopped too soon or applied too long

The undesired behavior is assessed in the fourth step by determining how it could occur. The causal factors that can lead to the UCA's are identified. Every UCA can be caused by several different scenarios that need

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

to be assessed to define suitable mitigation strategies. Central questions to be answered when analyzing the individual control loops for causal scenarios are:

1. Why would UCA occur?
2. Why would the CA be improperly executed or not executed, leading to hazards?

The STPA Handbook offers further, more detailed information on the STPA process including detailed definitions and process descriptions, especially for the fourth step, the scenario definition [36].

5.1.1.1. The Aircraft

To perform a comprehensive assessment from which the risks can be identified, a scope was defined to create an accurate system boundary and assumptions regarding the system to be assessed were made. As a reference system architecture, the concept from the UNIFIER 19 project [37] was chosen. It is a hydrogen electric powered aircraft concept, that was modified to fit the ALBATROS task requirements.

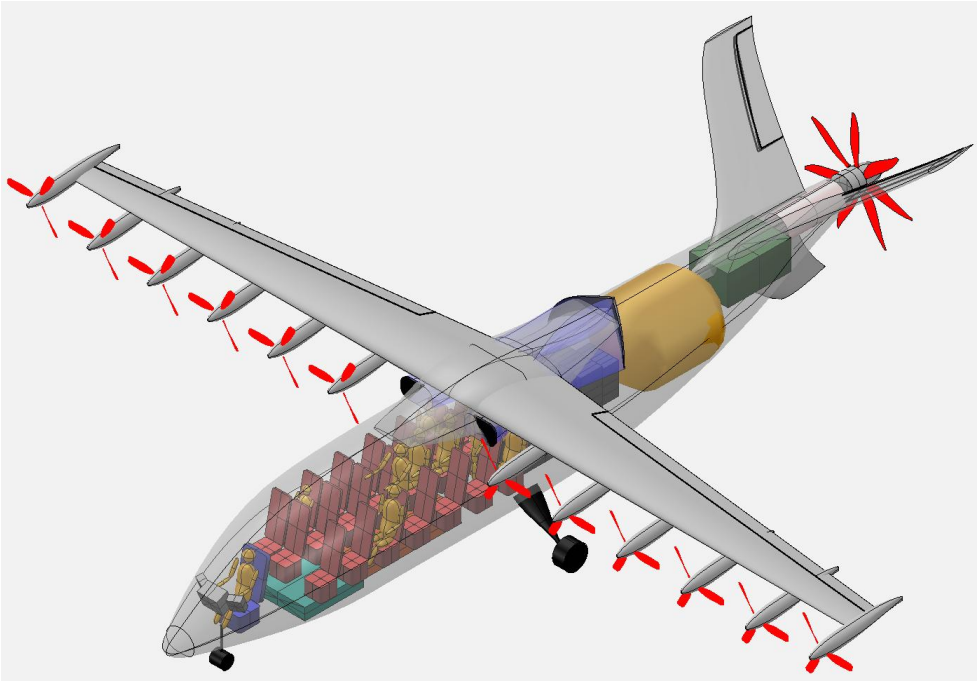


Figure 11: Unifier 19 Concept [37].

The aircraft's Electric Propulsion System (EPS) is primarily powered by the Fuel Cell (FC) System, with supplementary power provided by the battery system. The battery system compensates for any lags in power delivery and peak power demands. The fuel cell power is sized to meet the required cruise power, and the battery provides the additional power needed during take-off and climb. Other than this, the battery role is for voltage balancing. The respective controllers of the systems are monitored and managed by a PMCU (Power Management Control Unit). The PMCU oversees the state of health and performance of all systems, dynamically adjusting power generation, consumption and distribution to ensure reliable and efficient operation.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

It is assumed that the aircraft does not feature any in-flight charging or energy recuperation. The focus is on one direction of power flow – the power provision and not the charging of the batteries with external power or excess power from the FC system. The excess power of the FC system can be used up by a heater connected within the system's architecture. Another assumption that was made is that the hydrogen fuel delivered to the stack is already conditioned. Hence, the hydrogen conditioning within a balance of plant subsystem will not be an aspect of this risk identification.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

5.1.1.2. Defining the Purpose of the Analysis

Relevant stakeholders of the system include not only the manufacturer/producer, but also the aircraft operator, flight crew and passengers, certification authorities, the public and environment affected by the safe operation of the aircraft. Each of these stakeholders has an interest in ensuring that the operation of the propulsion system remains reliable, controllable, and compliant with applicable safety standards. The stakeholder losses describe a loss of this operation of the aircraft:

- L-[1] Loss of life or injury to passengers.
- L-[2] Structural damage to the aircraft.
- L-[3] Loss of hydrogen-electric powered flight.

Based on the system boundary, the system level hazards and sub-hazards that are linked to the stakeholder losses are listed below:

- H-[1] Aircraft does not have enough power for flight (L-[2], L-[3]).
  - H-[1.1] Fuel Cells not providing power needed for flight mission.
  - H-[1.2] Battery not providing compensating power needed for flight mission.
- H-[2] Incorrect power distribution in aircraft (L-[2], L-[3]).
- H-[3] Decrease of engine handling on aircraft(L-[2], L-[3]).
- H-[4] Violation of structural integrity of aircraft subsystems(L-[1], L-[2], L-[3]).
  - H-[4.1] Fuel Cells overheat/Membrane rupture.
  - H-[4.2] Pressure over limit in hydrogen tank.
  - H-[4.3] Battery in thermal runaway.
  - H-[4.4] Hydrogen fuel leak.

These hazards represent the unsafe states of the system that can consequently lead to the identified losses. By defining them at this early stage, the analysis ensures that subsequent steps of the STPA are explicitly linked to prevent outcomes that would be unacceptable to stakeholders.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

Based on the system level hazards, the high-level system requirements are defined as system level constraints.

Table 4: List of System Constraints.

ID	*System level Constraint*	*Connected hazard*
SC-1	Power must be provided	• H-[1] Aircraft does not have enough power for flight
SC-2	Fuel Cells must provide power for the mission	• H-[1.1] Fuel Cells not providing power needed for flight mission
SC-3	Battery must provide compensating power for the mission	• H-[1.2] Battery not providing compensating power needed for flight mission
SC-4	Power must be distributed accordingly	• H-[2] Incorrect Power Distribution in Aircraft
SC-5	Engine control must not decrease over a [TBD] safety threshold	• H-[3] Decrease of Engine Handling on Aircraft
SC-6	Structural integrity of aircraft must be maintained	• H-[4] Violation of Structural Integrity of Aircrafts Subsystems
SC-7	Fuel Cells must have pressure management and be maintained at a safe operating temperature and humidity	• H-[4.1] Fuel Cells Overheat/Membrane Rupture
SC-8	Pressure above the calculated/defined [TBD] limit must be vented	• H-[4.2] Pressure Over Limit in LH2 Tank
SC-9	Battery in TR must be contained for the [TBD] time of emergency landing and evacuation of the aircraft	• H-[4.3] Battery in Thermal Runaway
SC-10	H2 fuel leakage must be detected and vented out of cabin atmosphere	• H-[4.4] H2 Fuel Leaking

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Program, under Grant Agreement No. 101077071.

5.1.2. Model of the Control Structure

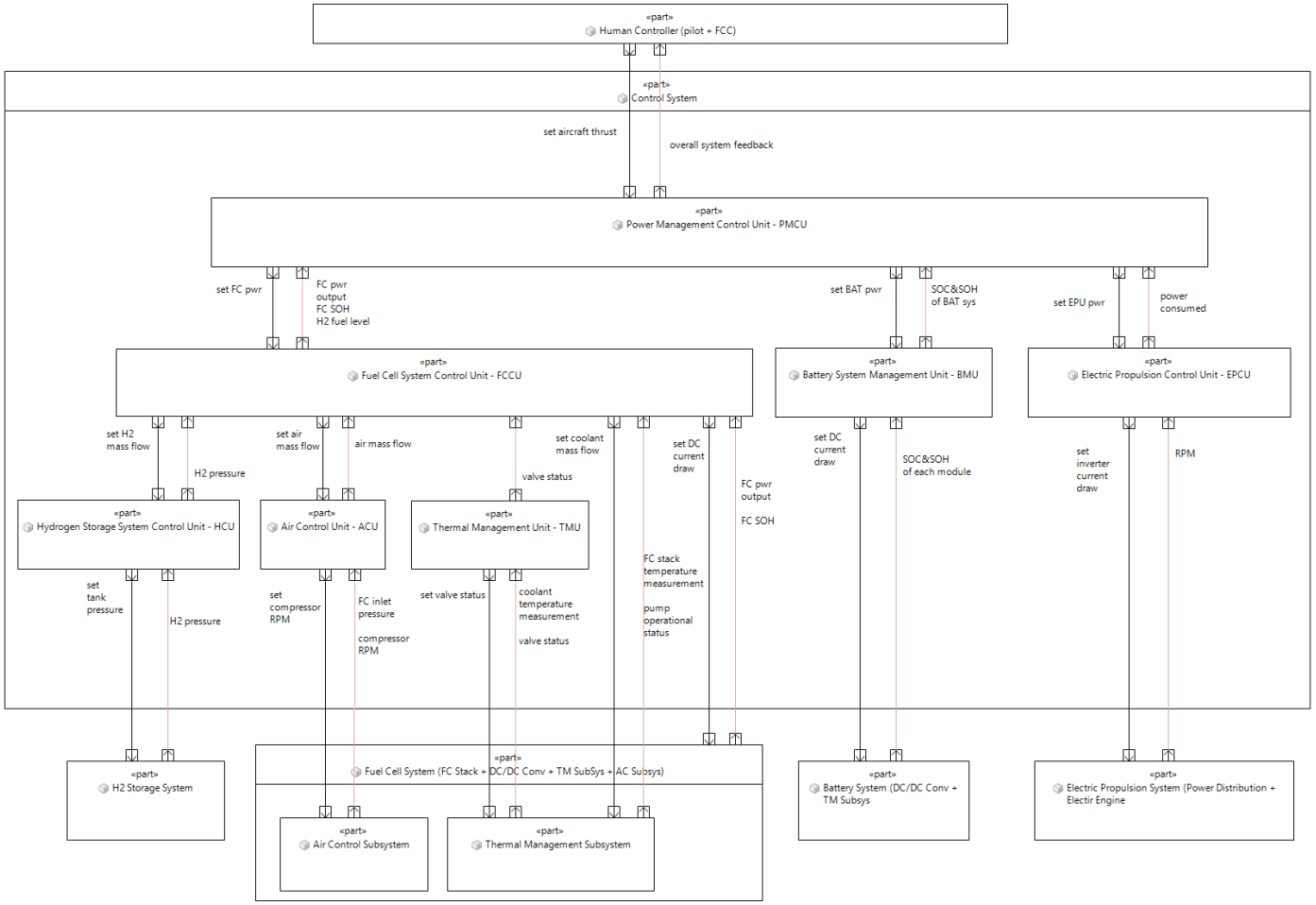


Figure 12: Control Structure.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

5.1.2.1. Elements of the Control Structure

Human Controller - HC

Consisting of the Pilot, Human Machine Interface (HMI) and Flight Control Computer (FCC). The HC represents the point of communication to the aircrafts systems. It provides the thrust command which afterwards, is processed by the FCC and given out as a control action in the form of power[kW].

Power Management Control Unit - PMCU

The PMCU monitors the different states of the subsystems and provides the command to increase or decrease the power consumption of the engines, electrical power generation of the Fuel Cells, and power provision from the battery. The PMCU is programmed to maintain the battery discharge rate to be as low as possible, as the primary source of electrical power is the FC System. The only instance that the battery provides electrical power is during cases where the Engines consume more power than available from the fuel cells. The PMCU has the authority to allocate power distribution and decide whether and to what extent the FCS and the BAT provide electrical power. The issued control action is based on readings from all the relevant systems.

Fuel Cell Control Unit - FCCU

The FCCU is controlling and monitoring the flow of the reactants in the Fuel Cells, by sending commands to different lower-level controllers and balance of plant subsystems. To control the Hydrogen flow, the FCCU provides a control action to the HCU. The air flow and pressure are controlled by valves and compressors via the ACU. The FCCU also is responsible for determining the duty cycle of the fuel cell DC/DC converter, that provides power to the HV bus. It sets the coolant mass flow rate and adjusts accordingly with the TMCU (see below).

Air Control Unit - ACU

The ACU is responsible for monitoring the compressor data, the FC inlet pressure and adjusting the compressor RPM parameter of an electric motor accordingly so the compressor delivers the requested flow rates.

Thermal Management Control Unit - TMCU

The Thermal Management Control Unit is responsible for controlling the valve's position to direct coolant circulation either through or around a radiator. The unit sets the valve position depending on the temperature of the coolant. If the coolant temperature is above a defined threshold, the coolant flow is directed through the radiator to reduce the temperature of the coolant.

Fuel Cell System - FCS

The FCS consists of cathode and anode cells, distribution lines and valves for the reactants flow and a DC/DC converter. Integrated within the FCS are the Air Control Subsystem and the Thermal Management Subsystem designed for maintaining the ideal conditions for operation and efficient power generation.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

Air Control Subsystem - ACS

Responsible for maintaining the required compressor RPM and inlet pressure within the FC system. The subsystem is assumed to have automatic humidity control of the air in order to keep an appropriate environment for the membrane and would be defined later on in the development of the project.

Thermal Management Subsystem - TMS

The Thermal Management subsystem contains coolant lines, valves, coolant pumps and sensors. The coolant pumps are responsible for regulating the coolant mass flow through the cooling circuit depending on the demanded mass flow rate by the FCCU. The demanded mass flow rate depends on the measured fuel cell stack temperature. The sensors of the TMS measure temperatures at different positions in the circuit including prior to the coolant entering the stack and the stack temperature itself.

Hydrogen Storage System Control Unit - HCU

The HCU monitors the pressure values in the hydrogen storage tank as well as the fuel lines that lead from the tank to the conditioning system. For clarification the Hydrogen conditioning (temperature, pressure and humidity) is not in the scope of this assessment so it will not be considered in this control structure.

Hydrogen Storage System - HSS

Consisting of the hydrogen tank and fuel lines. The system features multiple safety valves, pressure controllers, as well as pressure sensors.

Battery Management System - BMS

The BMS monitors the voltage and temperature of the cells. It also translates this information into State of Charge (SOC) and State of Health (SOH) values that are utilized in the PMCU's process model. The BMS has the authority of disconnecting and locking the battery system in the case of a serious failure, like an unexpected big discharge rate, or high temperatures in the Battery System. The BMS accepts PMCU requests and converts it to current draw from the battery system. It then controls the DC/DC converter through its current draw.

Battery System - BAT

Consisting of cells connected in parallel and series, voltage, current and temperature sensors, and a DC/DC converter.

Electric Propulsion Control Unit - EPCU

A control unit that computes and demands the required inverter current draw for a power setting demanded by the PMCU. The unit also monitors the performance of propulsion system data like RPM and torque and feeds monitoring data back to the PMCU.

Electric Propulsion Unit - EPU

EPU contains the subsystems that are primarily needed for thrust generation. The Inverters, the Motor and connected Propeller. In addition, at least two sensors to measure the output torque and the RPM of the

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

Motor are included in the EPU. It is controlled through the EPCU with an inverter current draw setting and feeds back the RPM and delivered Torque as measures of performance.

5.1.2.2. Identified Control Actions for Hydrogen-Electric Powertrain

Every Control Action (CA) is defined, and the according control loop is shown to clarify how the control and feedback flow in each individual case. All control loops combined make the control structure shown in Figure 12. The red areas represent the controlled processes and the blue areas represent controller and feedback provision entities.

- ***CA.1 Set Aircraft Thrust*** - The pilot, via the Human-Machine Interface and Flight Control Computer, provides a thrust command representing the desired power output of the propulsion system. This command serves as the primary input linking human intent to system-level power management and is expressed as a target thrust level.

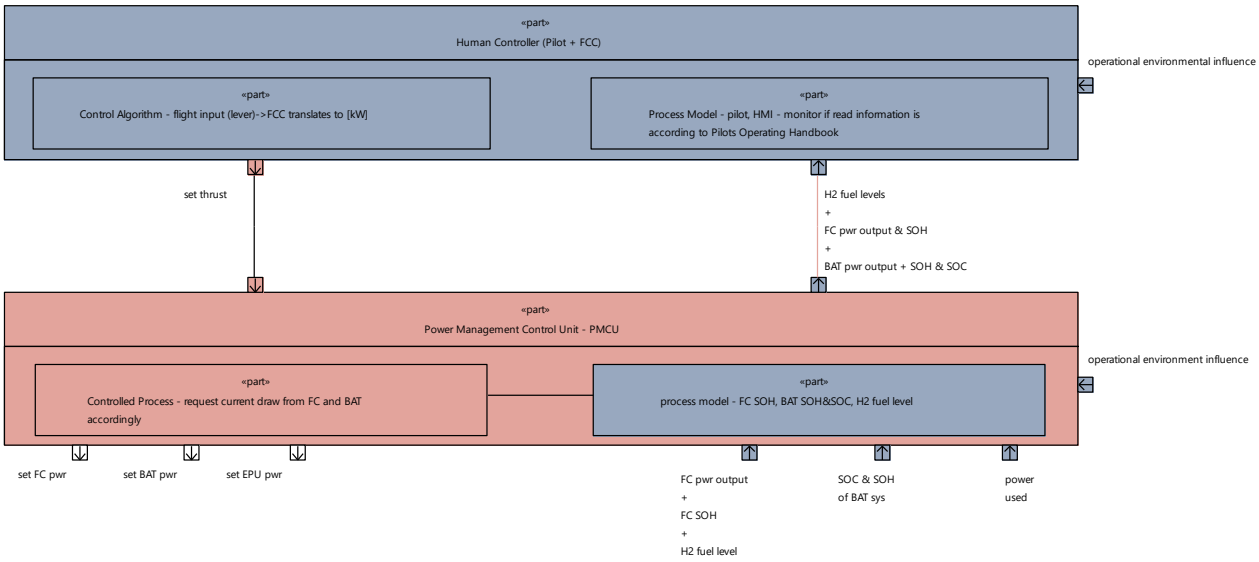


Figure 13: CA.1 Set Aircraft Thrust.

- ***CA.2 Set Fuel Cell Power*** - The PMCU issues commands regulating the electrical power output of the fuel cell system to match propulsion and auxiliary demands. It balances energy flows between the fuel cells, battery, and propulsion units, typically prioritizing fuel cell operation while maintaining minimal battery discharging except during peak load conditions.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

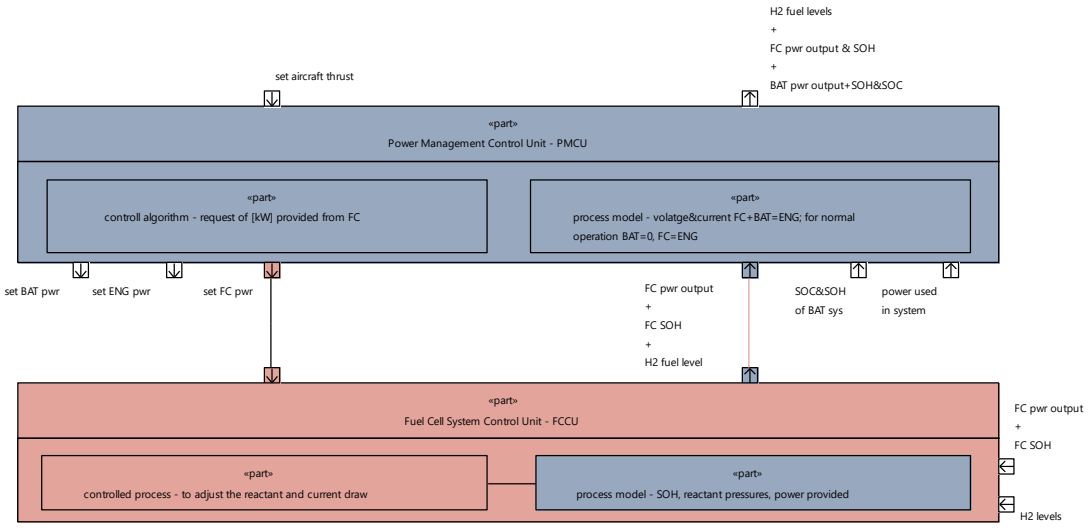


Figure 14: CA.2 Set Fuel Cell Power.

- ***CA.3 Set Air Mass Flow Rate*** - The FCCU determines and commands the airflow required by the fuel cell stack to sustain electrochemical reactions at the demanded power level. It regulates mass flow through compressors and valves to ensure appropriate oxygen supply, enabling efficient fuel cell performance and preventing conditions such as oxygen starvation.

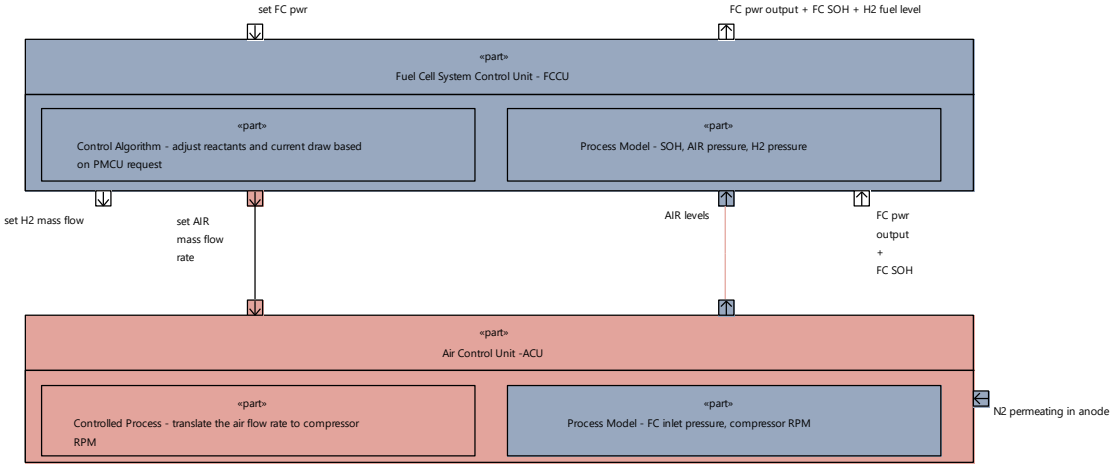


Figure 15: CA.3 Set Air Mass Flow Rate.

- ***CA.4 Set Air Pressure*** - The ACU modulates compressor speed and related components to achieve the pressure levels required at the fuel cell inlet. This action ensures stable stack operation by

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

maintaining airflow at the correct pressure for optimal reaction efficiency, durability, and system safety.

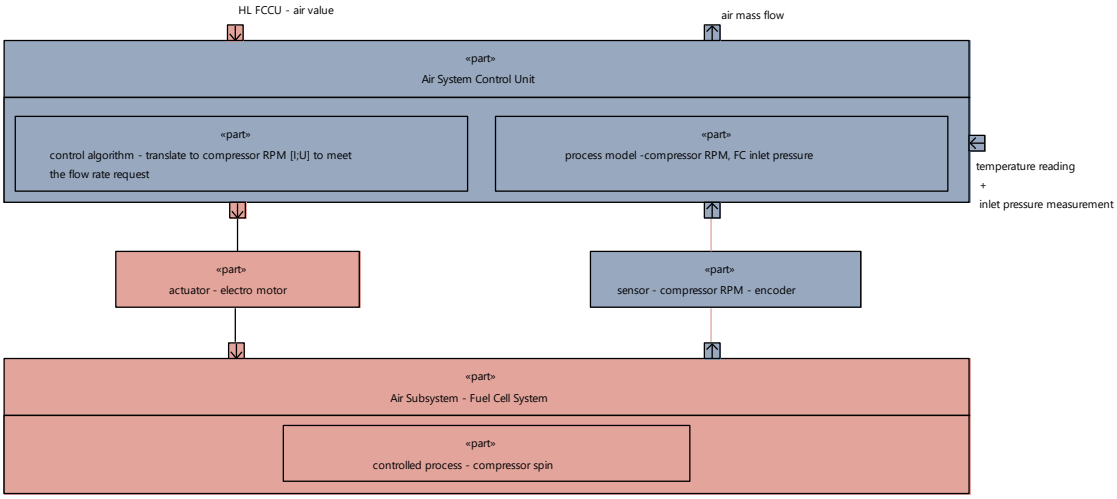


Figure 16: CA.4 Set Air Pressure.

- ***CA.5 Set DC/DC Current Draw*** - The FCCU sets the operating duty cycle of the fuel cell's DC/DC converter to control the current drawn from the stack. This governs the power delivered to the high-voltage bus, matching generation with demand and preventing overloading or underutilization of the fuel cells.

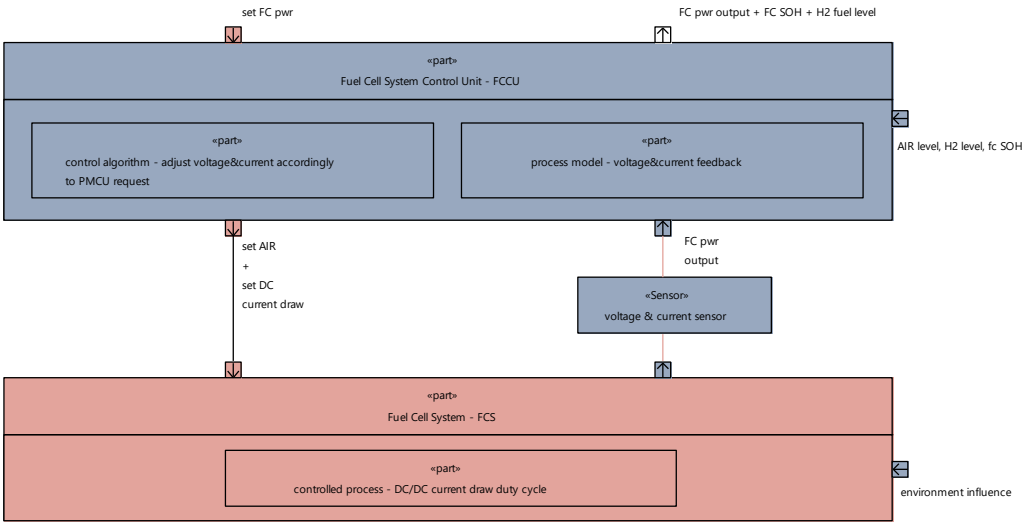


Figure 17: CA.5 Set DC/DC Current Draw.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

- ***CA.6 Set H2 Mass Flow Rate*** - The FCCU regulates hydrogen delivery to the fuel cell stack, typically through valves and flow controllers, in proportion to power demand. This ensures proper fuel utilization, maintains efficiency, and avoids unsafe conditions such as fuel starvation or excessive pressure within the system.

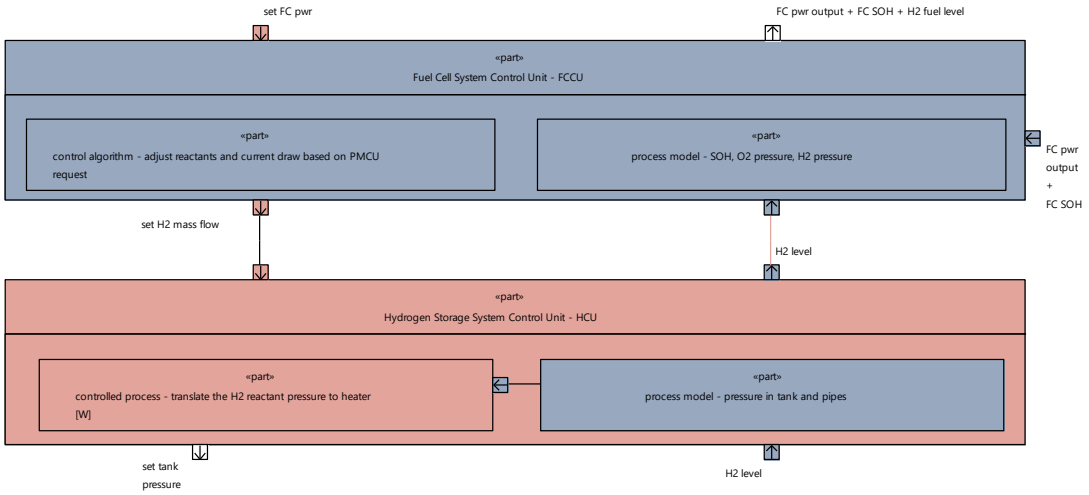


Figure 18: CA.6 Set H2 Mass Flow Rate.

- ***CA.7 Set Tank Pressure*** - The HCU monitors and adjusts hydrogen storage tank pressure, primarily by controlling the heater, managing valves and venting mechanisms. This action ensures that hydrogen is supplied to the conditioning and fuel cell system within safe pressure limits, preventing over-pressurization, leakage hazards, or supply interruptions.

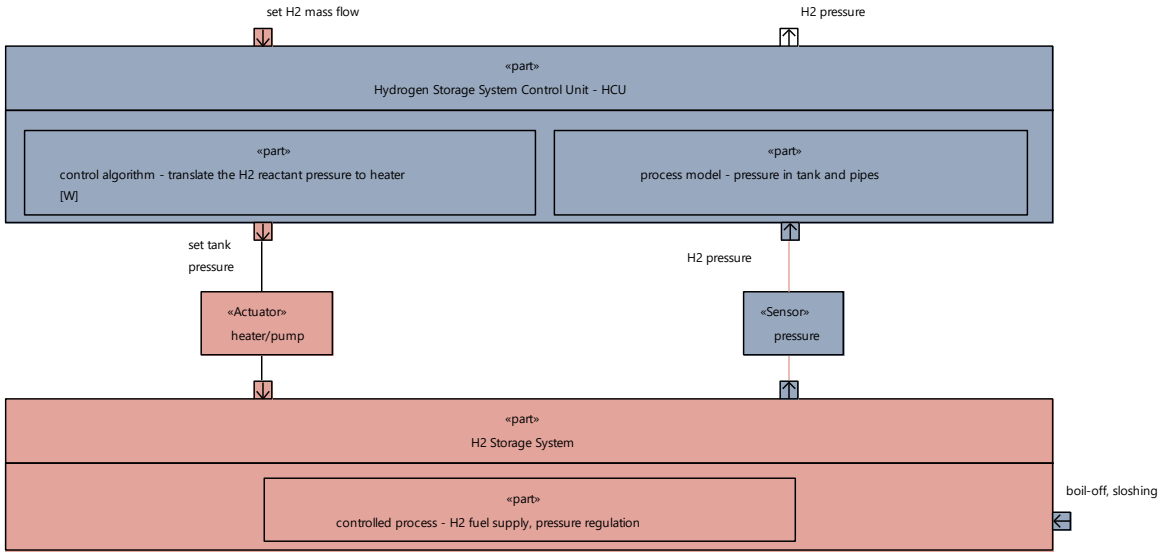


Figure 19: CA.7 Set Tank Pressure.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

- ***CA.8 Set inverter current draw*** – The EPCU sets the current draw of the inverter in the EPU, defining the RPM of the motor and subsequently the amount of thrust produced by the Unit.

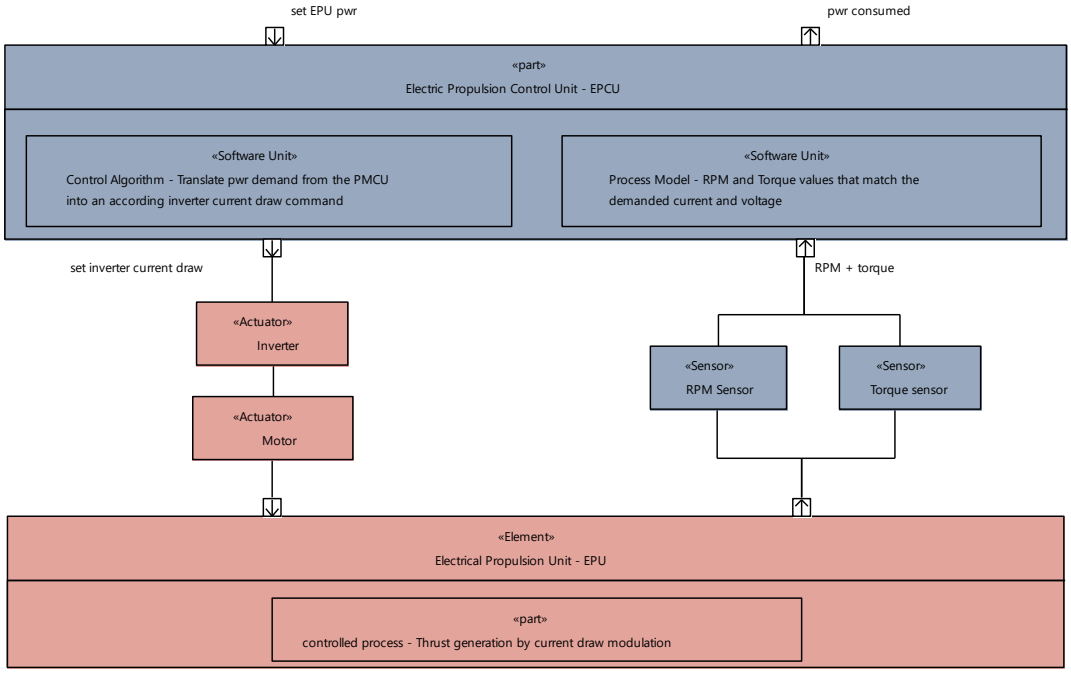


Figure 20: CA.8 Set inverter current draw.

- ***CA.9 Set BAT DC current draw*** – The BMU sets the level of the current that is to be drawn from the Battery based on the difference between the commanded and actual power.

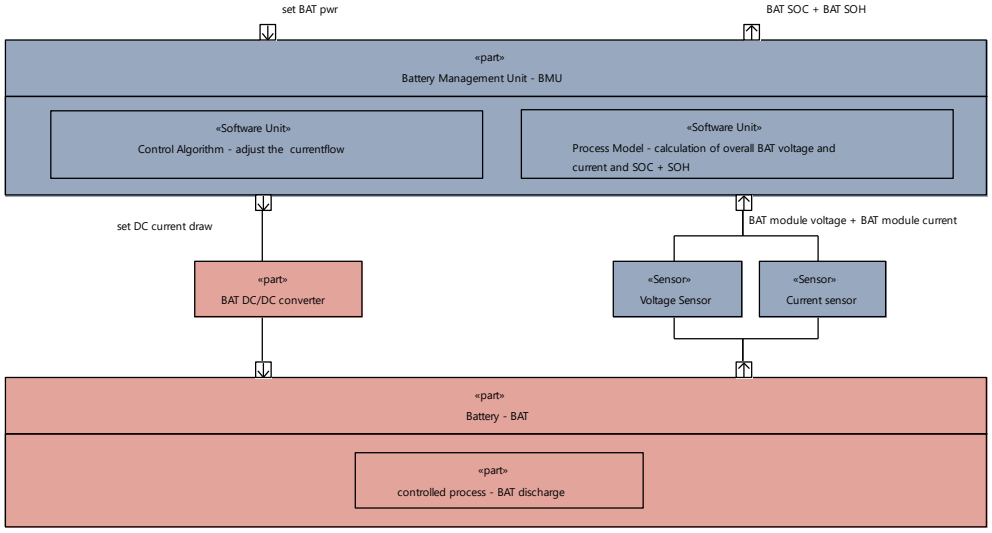


Figure 21: CA.9 Set BAT DC current draw.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

- ***CA.10 Set required BAT power*** – The PMCU sets the power that is required from the BAT. The amount of BAT power that is required depends on the amount delivered by the FCS; the amount consumed by the EPU und the requested thrust/power by the Human Controller.

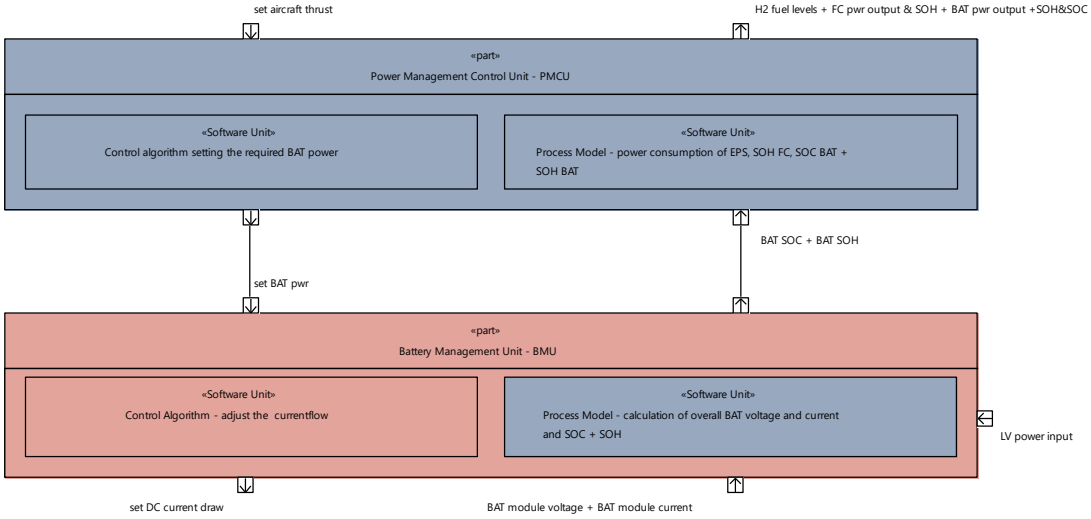


Figure 22: CA.10 Set required BAT power.

- ***CA.11 Set EPU power*** – The amount of power the PMCU requires, depends on the aircraft thrust setting issued by the Human Controller and the available power from the two electrical power sources FCS and BAT.

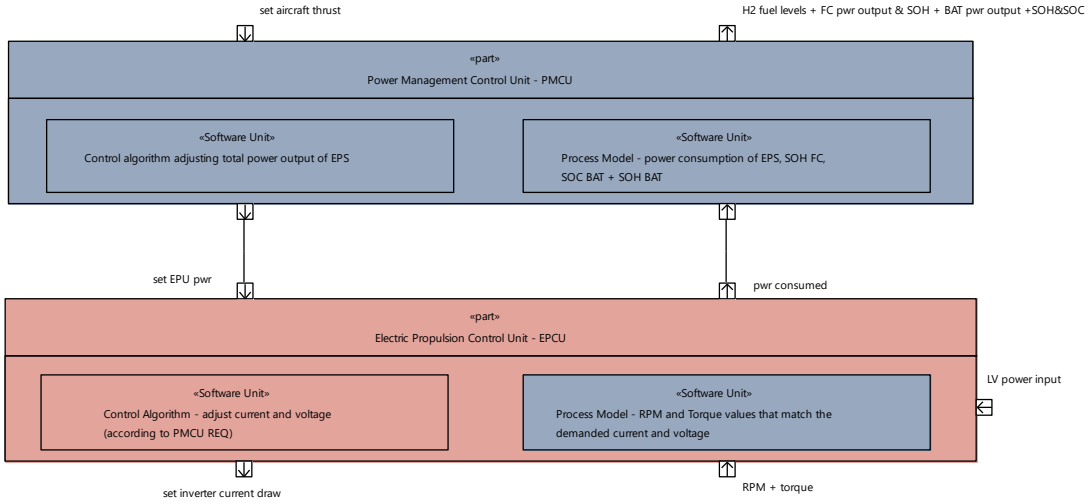


Figure 23: CA.11 Set EPU power.

- ***CA.12 Set coolant mass flow*** – The FCCU sets the coolant mass flow rate through the coolant circuit depending on the measured coolant and stack temperatures. If the temperature increases, a higher coolant mass flow rate is needed to provide more capacity for the cooling of the FC stack.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

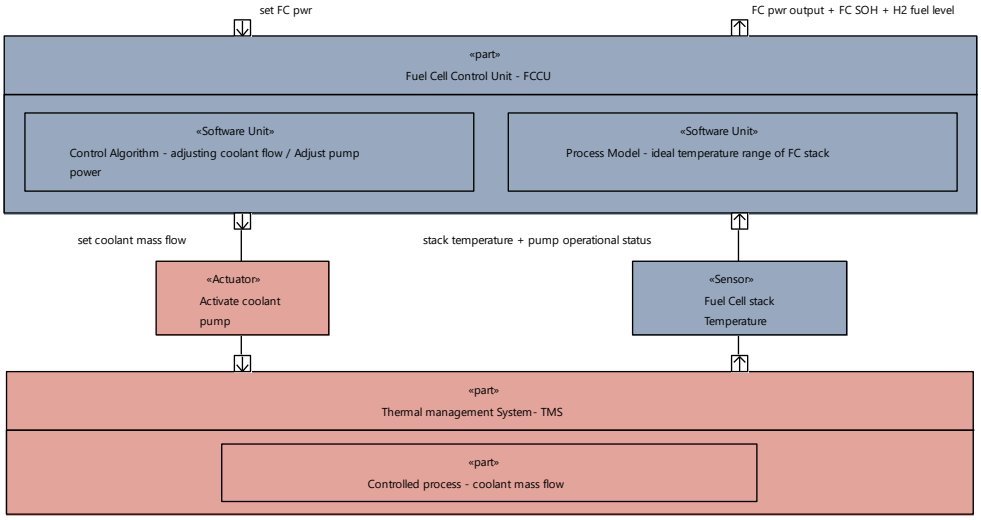


Figure 24: CA.12 Set coolant mass flow.

- ***CA.13 Set position of mixing valve*** – Depending on the temperature of the coolant after it leaves the FC stack, the TMCU adjusts the mixing valve accordingly. If the temperature is above a defined limit value, the mixing valve is set so that the coolant is channeled through the radiator to reduce its temperature and thus dissipate heat. If the temperature is below the defined limit, the coolant flow is channeled around the radiator.

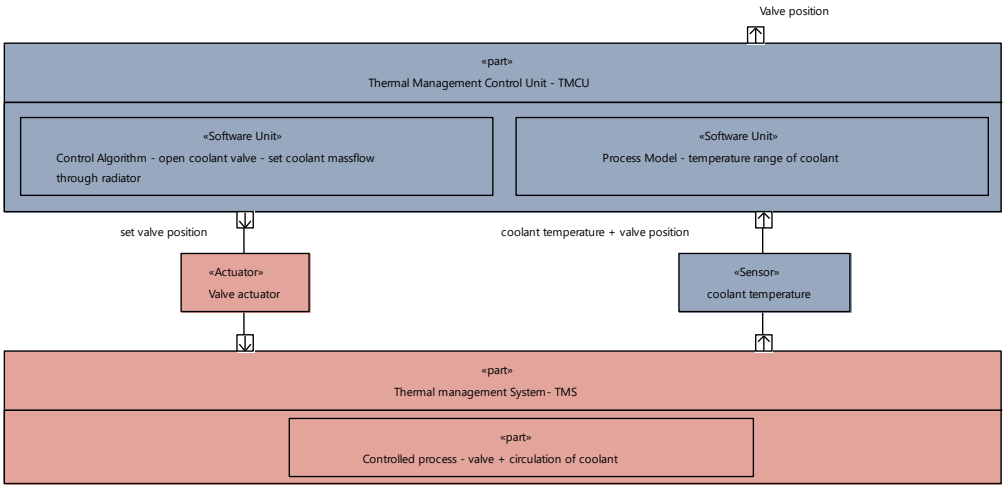


Figure 25: CA.13 Set position of mixing valve.

5.1.3. Identifying Unsafe Control Actions

By examining the control structure, potential Unsafe Control Actions (UCAs) were identified. The UCAs could occur if a command or control action is executed incorrectly or outside its intended context. Each previously identified control action was evaluated to determine how it might, under certain conditions, contribute to a hazardous system state. The assessment focuses on whether a control action was not provided, and the

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

hazard was caused, or providing of the control action caused the hazard. The guidewords “provided too early/late” and “applied for too long/short” (as per STPA Handbook) were not considered in this exercise, as the system consists of electronic controllers where such timing deviations are not relevant in the same manner as in mechanical systems. This systematic evaluation highlights unsafe interactions within the system and forms the basis for identifying causal scenarios in the following steps of the analysis.

Table 5: UCA Matrix.

Control Action	*Not Providing Causes Hazard*	*Providing Causes Hazard*
[CA.1] set aircraft thrust	[UCA.1.1] Human controller does not set required thrust to maintain flight during the mission	[UCA.1.2] Human controller sets more than required thrust for the flight mission
[CA.2] set FC power	[UCA.2.1] PMCU does not set required FC power to meet the engine consumption during the flight mission	[UCA.2.2] PMCU sets higher than required FC power production for the flight mission
[CA.3] set air mass flow rate	[UCA.3.1] FCCU does not set required air mass flow rate during operation creating a delta in reactants	[UCA.3.2] FCCU sets air mass flow rate higher than required for power production and cratering a delta in reactants
[CA.4] set air pressure	[UCA.4.1] ACU does not adjust air pressure to match the required air flow during operation creating a delta in reactants pressures	[UCA.4.2] ACU adjusts air pressure higher than the required air flow during operation creating a delta in reactants pressures
[CA.5] set DC/DC current draw value	[UCA.5.1] FCCU does not set required FC DC/DC current draw value during current consumption in the engines	[UCA.5.2] FCCU sets DC/DC current draw value that does not match the engine consumption
[CA.6] set H2 mass flow rate	[UCA.6.1] FCCU does not set required H2 mass flow rate during operation creating a delta in reactants	[UCA.6.2] FCCU sets H2 reactants value that is not required for the power production creating delta in reactants
[CA.7] set tank pressure	[UCA.7.1] HCU does not set tank pressure to match the required H2 flow during the operation creating a delta in reactants pressures	[UCA.7.2] HCU sets tank pressure above limit for the required operation creating overpressure in the tank
[CA.8] set inverter current draw	[UCA.8.1] The EPCU does not provide a set inverter current draw command during flight	[UCA.8.2] The EPCU provides an inverter current draw command that does not match the requested power on the motor by the PMCU

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

[CA.9] set BAT DC current draw	[UCA.9.1] The BMU does not provide a DC current draw command while BAT power delivery is expected and commanded by the PMCU	[UCA.9.2] A BAT DC current draw command is provided by the BMU although no power delivery is demanded by the PMCU
[CA.10] set required BAT power	[UCA.10.1] The PMCU does not provide the BMU with a power requirement command in flight	[UCA.10.2] The PMCU provides a set BAT power command with the delivered BAT power greatly exceeding the commanded value
[CA.11] set EPU power	[UCA.11.1] The PMCU does not provide a set EPS power command while a thrust is demanded from the propulsion system with the aircraft in flight	[UCA.11.2] The PMCU provides an erroneous set EPS power command that does not match the for the flight phase required thrust
[CA.12] set coolant mass flow	[UCA.12.1] The FCCU does not provide a set coolant mass flow command with the airflow temperature through the radiator exceeding the stack temperature limits and the aircraft in flight	[UCA.12.3] The FCCU provides a set coolant mass flow command leading to a decrease of the stack temperature below the lower temperature limit of the FC with the aircraft in flight
	[UCA.12.2] The coolant pump actuator receives a set coolant mass flow command with the coolant mass flow not changing as expected in flight	
[CA.13] set position of mixing valve	[UCA.13.1] The TMCU does not provide a set valve position command with the coolant flowing around the radiator, the stack temperature exceeding the stack temperature limits and the aircraft in flight	[UCA.13.3] The TMCU provides a set valve position command leading to a decrease of the stack temperature below the lower temperature limit of the FC with the aircraft in flight
	[UCA.13.2] The valve actuator receives a set position of mixing valve command with the position of the mixing valve not changing to open and the coolant flowing around the radiator in flight	

The identified UCAs are traced to the according hazards that were determined for the defined system's operating condition and Controller Constraints are assigned.

To support prioritization and to align the analysis with industry practice, each identified UCA was further assessed for severity classification in accordance with ASTM F3230. This classification provides a structured

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

categorization of the potential impacts of unsafe control actions on the aircraft and its stakeholders. By assigning a severity level, the analysis highlights which UCAs have the most critical consequences and therefore require the greatest attention in subsequent design, verification, or mitigation activities.

The severity classification considers the potential system-level losses associated with each UCA, such as loss of life or injury (catastrophic), significant structural damage (hazardous/major), or partial degradation of system performance (minor). This approach ensures that the UCAs are not only identified but also weighted according to the seriousness of their possible outcomes. The result is a prioritized set of unsafe control actions that informs both the hazard analysis process and future safety requirements for the hybrid hydrogen–electric propulsion system.

Table 6: UCA Classification.

Unsafe Control Action	*Hazard*	*Class*	*Controller Constraints*
[UCA.1.1] Human controller does not set required trust to maintain flight during the mission	• H-[1] Aircraft does not have enough power for flight	HAZ	[CC-01] Human Controller must set accurate thrust for a maintained flight
[UCA.1.2] Human controller sets more than required thrust for the flight mission	• H-[2] Incorrect Power Distribution in Aircraft	MAJ	[CC-02] Human Controller must respect the performance capabilities of the powertrain
[UCA.2.1] PMCU does not set required FC power to meet the engine consumption during the flight mission	• H-[1.1] Fuel Cells Not providing power needed for flight mission • H-[2] Incorrect Power Distribution in Aircraft • H-[4] Violation of Structural Integrity of Aircrafts Subsystems	HAZ	[CC-03] PMCU must request FC power provision to match the consumption of the engines
[UCA.2.2] PMCU sets higher than required FC power production for the flight mission	• H-[2] Incorrect Power Distribution in Aircraft • H-[4] Violation of Structural Integrity of Aircrafts Subsystems	MAJ	[CC-04] PMCU must not exceed FC power production in the powertrain
[UCA.3.1] FCCU does not set required O2 mass flow rate during operation creating a delta in reactant pressures	• H-[4.1] Fuel Cells Overheat/Membrane Rupture	MAJ	[CC-05] FCCU must monitor the mass flow rate to meet the pressure differences

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

	• H-[1.1] Fuel Cells Not providing power needed for flight mission		
[UCA.3.2] FCCU sets O2 mass flow rate higher than required for the power production and creating a delta in reactant pressures	• H-[1.1] Fuel Cells Not providing power needed for flight mission • H-[4.1] Fuel Cells Overheat/Membrane Rupture	MAJ	[CC-06] FCCU must maintain the mass flow rate within limits to not exceed the pressure difference
[UCA.4.1] ACU does not adjust air pressure to match the required air flow during operation creating a delta in reactant pressures	• H-[1.1] Fuel Cells Not providing power needed for flight mission • H-[4.1] Fuel Cells Overheat/Membrane Rupture	MAJ	[CC-07] ACU must monitor the air flow to meet the pressure difference
[UCA.4.2] ACU adjusts air pressure higher than the required air flow during operation creating a delta in reactant pressures	• H-[4.1] Fuel Cells Overheat/Membrane Rupture • H-[1.1] Fuel Cells Not providing power needed for flight mission	MAJ	[CC-08] ACU must maintain air flow within limits of the pressure difference
[UCA.5.1] FCCU does not set required FC DC/DC current draw value during current consumption in the engines	• H-[1.1] Fuel Cells Not providing power needed for flight mission	MAJ	[CC-09] FCCU must adjust current draw according to the requested power from PMCU
[UCA.5.2] FCCU sets DC/DC current draw value that does not match the engine consumption	• H-[2] Incorrect Power Distribution in Aircraft	MAJ	[CC-10] FCCU must not set current beyond requested power from PMCU
[UCA.6.1] FCCU does not set required H2 mass flow rate during operation creating a delta in reactant pressures	• H-[4.1] Fuel Cells Overheat/Membrane Rupture • H-[1.1] Fuel Cells Not providing power needed for flight mission	MAJ	[CC-11] FCCU must monitor and align the H2 pressure to meet the pressure from the O2

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

[UCA.6.2] FCCU sets H2 reactant value that is not required for the power production creating delta in reactant pressures	• H-[4.4] H2 Fuel Leaking • H-[4.1] Fuel Cells Overheat/Membrane Rupture	MAJ	[CC-12] FCCU must maintain the H2 pressure to not exceed the pressure from O2
[UCA.7.1] HCU does not set tank pressure to match the required H2 flow during the operation creating a delta in reactant pressures	• H-[4.1] Fuel Cells Overheat/Membrane Rupture • H-[1.1] Fuel Cells Not providing power needed for flight mission	HAZ	[CC-13] HCU must adjust flow of H2 in accordance to FCCU request
[UCA.7.2] HCU sets tank pressure above limit for the required operation creating overpressure in the tank	• H-[4.2] Pressure Over Limit in LH2 Tank • H-[4.4] H2 Fuel Leaking • H-[1.1] Fuel Cells Not providing power needed for flight mission	CAT	• [CC-14] No single point of failure must lead to the UCA • [CC-15] HCU must respect the pressure limit of the tank and must have direct monitoring of pressures
[UCA.8.1] The EPCU does not provide a set inverter current draw command during flight	• [H-1.1] Fuel Cells Not providing power needed for flight mission • [H-3] Decrease of Engine Handling on Aircraft	CAT	• [CC-14] No single point of failure must lead to the UCA • [CC-16] When required by the PMCU, the EPCU shall provide a set inverter current draw command
[UCA.8.2] The EPCU provides an inverter current draw command that does not match the requested power on the motor by the PMCU	• [H-3] Decrease of Engine Handling on Aircraft	MAJ	• [CC-17] When the PMCU requests power on the motor, the EPCU shall provide an inverter current draw command that exactly matches the requested power.
[UCA.9.1] The BMU does not provide a DC current draw command while BAT power delivery is expected and commanded by the PMCU	• [H-1.2] Battery Not providing compensating power needed for flight • [H-2] Incorrect Power Distribution in Aircraft	HAZ	• [CC-18] When the PMCU commands BAT power delivery, the BMU shall provide a DC current draw command to meet the power demand of the EPU.
[UCA.9.2] A BAT DC current draw command is provided by the BMU although no power	• [H-2] Incorrect Power Distribution in Aircraft	MAJ	• [CC-19] When no power delivery is demanded by the PMCU, the BMU

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

delivery is demanded by the PMCU			shall not provide a BAT DC current draw command
[UCA.10.1] The PMCU does not provide the BMU with a power requirement command in flight	• [H-2] Incorrect Power Distribution in Aircraft	HAZ	• [CC-20] The PMCU shall provide the BMU with a power requirement command to ensure adequate power management with the aircraft in flight
[UCA.10.2] The PMCU provides a set BAT power command with the delivered BAT power greatly exceeding the commanded value	• [H-2] Incorrect Power Distribution in Aircraft	MAJ	• [CC-21] When the PMCU provides a set BAT power command, the delivered BAT power shall not exceed the commanded value by [TBD] percent
[UCA.11.1] The PMCU does not provide a set EPU power command while a thrust is demanded from the HC with the aircraft in flight	• [H-1] Aircraft does Not have enough power for flight • [H-3] Decrease of Engine Handling on Aircraft	MAJ	• [CC-22] As soon as a thrust value is demanded by the HC, the PMCU shall provide a set EPS power command
[UCA.11.2] The PMCU provides an erroneous set EPS power command that does not match the for the flight phase required thrust	• [H-2] Incorrect Power Distribution in Aircraft • [H-3] Decrease of Engine Handling on Aircraft	HAZ	• [CC-23] When the PMCU provides a set EPS power command, it shall match the required thrust for the current flight phase
[UCA.12.1] The FCCU does not provide a set coolant mass flow command with the airflow temperature through the radiator exceeding the stack temperature limits and the aircraft in flight	• [H-1.1] Fuel Cells Not providing power needed for flight mission • [H-3] Decrease of Engine Handling on Aircraft • [H-4.1] Fuel Cells Overheat/Membrane Rupture	MAJ	• [CC-16] The FCCU shall provide a set coolant mass flow command as soon as the airflow temperature exceeds the stack temperature limits
[UCA.12.3] The FCCU provides a set coolant mass flow command leading to a decrease of the stack temperature below the lower temperature limit of the FC with the aircraft in flight	• [H-1.1] Fuel Cells Not providing power needed for flight mission • [H-3] Decrease of Engine Handling on Aircraft	MIN	• [CC-17] The FCCU shall not provide a set coolant mass flow command with the airflow temperature below the lower stack temperature limit

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

[UCA.12.2] The coolant pump actuator receives a set coolant mass flow command with the coolant mass flow not changing as expected in flight	• [H-3] Decrease of Engine Handling on Aircraft • [H-4.1] Fuel Cells Overheat/Membrane Rupture	HAZ	• [CC-18] Upon reception of a set coolant mass flow command the actual coolant mass flow shall change as expected within a specified time period
[UCA.13.1] The TMCU does not provide a set valve status command to the valve actuator with the coolant flowing around the radiator and the coolant temperature exceeding the stack temperature limits in flight	• [H-1.1] Fuel Cells Not providing power needed for flight mission • [H-3] Decrease of Engine Handling on Aircraft • [H-4.1] Fuel Cells Overheat/Membrane Rupture	MAJ	• [CC-19] The TMCU shall provide a set valve status command to the valve actuator to redirect coolant flow when the coolant temperature exceeds the stack temperature limits
[UCA.13.2] The valve actuator receives a set position of mixing valve command with the position of the mixing valve not changing to open and the coolant flowing around the radiator in flight	• [H-1.1] Fuel Cells Not providing power needed for flight mission • [H-3] Decrease of Engine Handling on Aircraft • [H-4.1] Fuel Cells Overheat/Membrane Rupture	HAZ	• [CC-21] The valve actuator shall set the position of the mixing valve according to the received command within a specified time period
[UCA.13.3] The TMCU provides a set valve status command leading to a decrease of the coolant temperature below the lower temperature limit of the FC with the aircraft in flight	• [H-1.1] Fuel Cells Not providing power needed for flight mission • [H-3] Decrease of Engine Handling on Aircraft	MAJ	• [CC-20] The TMCU shall not provide a set valve status command that would cause the coolant temperature to decrease below the lower temperature limit of the FC

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

5.1.4. Identifying Loss Scenarios

This step focuses on understanding how combinations of controller behaviors, process dynamics, and system interactions could result in a UCA being triggered. By tracing the causal pathways, the analysis provides insight into the underlying mechanisms that cause hazardous states and identifies opportunities for implementing effective safety constraints or design mitigations.

5.1.4.1. Causal Scenarios for UCA 1.1

UCA1.1: Human controller does not set required thrust to maintain flight during the mission.

Why the UCA occurred?
Failure of thrust lever causing the UCA
Pilot does not set required thrust based on environmental conditions/ ATC communication causing the UCA
Pilot sets required thrust, but the FCC does not translate to power request due to control algorithm error causing the UCA
Pilot due to human error incorrectly reads the information on the flight display causing the UCA
Flight display provides incorrect information due to screen error providing the pilot misleading information causing the inadequate control algorithm and UCA
PMCU system state feedback gets delayed due to overloading causing the UCA
PMCU processed the system states, but did not forward them to the pilot causing the UCA

Why was the CA improperly/not executed?
Pilot set the thrust, but it was not registered due to communication issue/interference from the lever to the FCC/PMCU causing the UCA
FCC/PMCU non-responsive failure causing the UCA

5.1.4.2. Causal Scenarios for UCA 1.2

UCA 1.2: Human controller sets thrust that is not required when flight phase is near ending.

Why the UCA occurred?
Pilot set the thrust, but it was registered differently in by the FCC due to communication issue/interference from the lever to the FCC/PMCU causing the UCA
PMCU reacts regardless of the pilots input increasing the power request due to improper processing of parameter causing the UCA
PMCU due to software error increases the power request without the pilot's request causing the UCA

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

Why was the CA improperly/not executed?
Pilot set the thrust, but it was registered differently in by the FCC due to communication issue/interference from the lever to the FCC/PMCU causing the UCA
PMCU reacts regardless of the pilots input increasing the power request due to improper processing of parameter causing the UCA
PMCU due to software error increases the power request without the pilot's request causing the UCA

5.1.4.3. Causal Scenarios for UCA 2.1

UCA 2.1: PMCU does not set required FC power to meet the engine consumption during the flight mission.

Why the UCA occurred?
Complete PMCU failure causing the UCA
PMCU has an error in algorithm and does not request a set amount of power [kW] to be provided from the FC causing the UCA
PMCU incorrectly processes the voltage and current levels in the HV system (BAT+ENG) determining no FC power request causing the UCA
PMCU did not receive feedback from the FC and H2 system changes causing the UCA
PMCU received incorrect information from the FCCU Process model due to communication interference/problems causing the UCA
PMCU received incorrect feedback from FCCU due to incorrectly processed state of FC system causing the UCA

Why was the CA improperly/not executed?
PMCU sent the command, but it was not received by the FCCU algorithm, due to communication interference/problem causing the UCA
PMCU sent the command, but FCCU control algorithm did not respond due to overloading/interference/no LV/error causing the UCA

5.1.4.4. Causal Scenarios for UCA 2.2

UCA 2.2: PMCU sets FC power that is not required for the operation.

Why the UCA occurred?
PMCU has an error in algorithm and does not request needed amount of power [kW] to be provided from the FC causing the UCA

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

PMCU incorrectly processes the voltage and current levels in the HV system (BAT+ENG) determining no FC power request causing the UCA
PMCU did not receive feedback from the FC and H2 system changes causing the UCA
PMCU received incorrect information from the FCCU Process model due to communication interference/problems causing the UCA
PMCU received incorrect feedback from FCCU due to incorrectly processed state of FC system causing the UCA
PMCU received incorrect feedback from other control units due to incorrectly processed states of Battery and Engines causing the UCA

Why was the CA improperly/not executed?
PMCU sent the command, but it was not received by the FCCU algorithm, due to communication interference/problem causing the UCA

5.1.4.5. Causal Scenarios for UCA 3.1

UCA 3.1: FCCU sets less than required air mass flow rate during operation creating a delta in reactants.

Why the UCA occurred?
FCCU does not adjust the air mass flow according to the power request from the fuel cells due to error or update causing the UCA
FCCU does not process reactants pressures correctly (flawed process model - did not understand the feedback) causing the UCA
FCCU incorrectly processes the pressures in the FC due to an error or update causing UCA
FCCU received incorrect feedback due to environmental effects/influence causing wrong processing and algorithm
Unsafe input form PMCU causing UCA
FCCU received no feedback from ACU to trigger a parallel reaction for CA, causing UCA
ACU slow processing leads to delay in feedback to FCCU causing UCA
ACU slow processing leads to delay in feedback to FCCU causing UCA

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

Why was the CA improperly/not executed?
Control command sent but not received by ACU due to loss of communication between controllers causing UCA
ACU nonresponsive causing UCA
CA sent, but ACU acted improperly due to calibration issue/updates causing UCA

5.1.4.6. Causal Scenario for UCA 3.2

UCA 3.2: FCCU sets air mass flow rate that is not required for the power production and creating a delta in reactants.

Why the UCA occurred?
FCCU adjusts the air value without a power request from the fuel cells due to error or update causing the UCA
FCCU incorrectly processes the pressures in the FC due to an error or update causing UCA
FCCU received incorrect feedback due to not calibrated causing wrong processing and algorithm
FCCU received incorrect feedback due to environmental effects/influence causing wrong processing and algorithm
FCCU received delayed feedback on the pressures in the FC due to interference/damaged communication causing the UCA

Why was the CA improperly/not executed?
FCCU CA was received incorrectly by ACU because of environmental effects and interference causing UCA
ACU responds inadvertently due to surge in LV causing UCA (acts when it is not supposed to)

5.1.4.7. Causal Scenarios for UCA 4.1

UCA 4.1: ACU does not adjust air pressure to match the required air flow during operation creating a delta in reactants pressures.

Why the UCA occurred?
PID loop does not correct compressor RPM to match required flow rate causing UCA
ACU incorrectly processes the inlet pressure/compressor RPM due to update/error causing UCA
ACU received incorrect inlet pressure reading from the sensor causing UCA
ACU received no feedback from sensor due to communication loss causing UCA

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

ACU received no feedback due to sensor failure causing UCA

Why was the CA improperly/not executed?
Compressor actuator - electric motor - nonresponsive causing UCA
Compressor actuator did not receive command due to communication loss/ issue causing UCA
Compressor unable to spin due to blockage/ice causing UCA
Compressor blades failure - not functioning as expected causing UCA

5.1.4.8. Causal Scenario for UCA 4.2

UCA 4.2: ACU adjusts air pressure higher than the required air flow during operation creating a delta in reactants pressures.

Why the UCA occurred?
ACU received improper control input from FCCU causing UCA
PID loop does not correct compressor RPM to match required flow rate causing UCA
ACU incorrectly processes inlet pressure/RPM data causing UCA
ACU receives incorrect feedback due to sensor +/- error causing UCA
ACU receives incorrect feedback due to external interference causing UCA
ACU receives delayed feedback causing UCA
ACU process model unable to read correct values due to an update/ error in codes causing UCA
ACU receives incorrect feedback due to encoder not calibrated/failure causing UCA

Why was the CA improperly/not executed?
Compressor actuator acts incorrectly due to external influence/non calibrated / failure causing UCA
Compressor actuator receives incorrect signal due to communication interference causing UCA
Compressor responds incorrectly due to blockage/debris/ice causing UCA
Compressor responds inadvertently due to a surge in LV system causing UCA
Compressor responds inadvertently due to a pressure surge in the air system causing UCA

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

5.1.4.9. Causal Scenarios for UCA 5.1

UCA 5.1: FCCU does not set required FC DC/DC current draw value during current consumption in the engines.

Why the UCA occurred?
FCCU receives input from PMCU with no request for value of current draw causing UCA
FCCU does not adjust the current and voltage according to PMCU request due to an error/update causing UCA

Why was the CA improperly/not executed?
FCCU sent signal but due to communication path mistake, the signal was not received causing UCA
FCCU sent signal, due to interference in the communication path information was received incorrectly causing UCA
FCCU DC/DC nonresponsive to signal requesting required voltage and current value setting for correct current draw duty cycle causing UCA
FCCU DC/DC has inadequate duty cycle algorithm due to error or update causing UCA

5.1.4.10. Causal Scenarios for UCA 5.2

UCA 5.2: FCCU sets DC/DC current draw that does not match the engine consumption.

Why the UCA occurred?
FCCU received unsafe input from PMCU, higher current draw duty cycle request than needed for the operation of the engines causing UCA
FCCU inadequately adjusts higher or less the voltage and current value for the DC/DC causing UCA
FCCU incorrectly processes feedback for voltage and current values set on the DC/DC causing UCA
FCCU receives delayed feedback from the sensors causing UCA
FCCU receives incorrect feedback due to measurement error on sensors causing UCA
FCCU receives incorrect feedback due to interference in the communication path to the process model causing UCA

Why was the CA improperly/not executed?
FCCU sent signal, but due to interference, DC/DC duty cycle received it incorrectly causing UCA
FCCU DC/DC nonresponsive to controls, stays on previously set duty cycle causing UCA

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

FCCU DC/DC algorithm acted incorrectly to signal and did not execute the requested duty cycle due to error/update causing UCA
FCCU requests no change to duty cycle, due to interference DC/DC changes set duty cycle, acting when not expected causing UCA

5.1.4.11. Causal Scenarios for UCA 6.1

UCA 6.1: FCCU does not set required H2 value during operation creating a delta in reactants.

Why the UCA occurred?
FCCU does not adjust the value needed of reactants to match the current draw set for the DC/DC (inadequate control algorithm) causing the UCA
FCCU does not process the SOH and reactants' pressures correctly causing the UCA
Unsafe control input was received by FCCU from PMCU causing the UCA (*unsafe input which will be assessed in other scenarios)
FCCU received no feedback from HCU to trigger a change in control causing the UCA
Slower HCU process model leading to delay in feedback to the FCCU causing the UCA
HCU processed pressure in tank and pipes incorrectly (Incorrect HCU process model) giving incorrect feedback to FCCU causing the UCA

Why was the CA improperly/not executed?
Control action sent but not received by HCU (loss of communication between FCCU and HCU) causing the UCA
HCU nonresponsive causing the UCA
CA sent, but HCU acted improperly due to calibration or update causing UCA

5.1.4.12. Causal Scenarios for UCA 6.2

UCA 6.2: FCCU sets reactants value, that is not required for the power production creating a delta in reactants.

Why the UCA occurred?
FCCU incorrectly adjusts H2 reactant value compared to air and current draw (inadequate control algorithm) causing the UCA
FCCU incorrectly processes the H2 pressure compared to the air pressure (flawed process model) causing the UCA

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

FCCU has unsafe control input form PMCU causing the UCA
FCCU did not receive feedback on H2 flow causing the UCA
Feedback on H2 flow was delayed due slow HCU process model causing the UCA
Feedback incorrect due to an error/flaw in process model of HCU causing the UCA

Why was the CA improperly/not executed?
FCCU sent a corrective control action for the operation, but the command was not received by the HCU (communication issue) causing the UCA
FCCU sent a corrective control action, but HCU is nonresponsive causing the UCA
FCCU had not sent any control action, HCU responds anyway due to an error/interference causing the UCA

5.1.4.13. Causal Scenarios for UCA 7.1

UCA 7.1: HCU does not set the required tank pressure for operation creating a delta in reactants' pressure in the fuel cells.

Why the UCA occurred?
HCU does not translate the required power for the heater (inadequate control algorithm) to meet the needed H2 pressure causing the UCA
HCU incorrectly processes the pressure of the tank, (higher than actual - has flawed process model) due to an error or update causing the UCA
HCU received incorrect reading from the sensor causing UCA
HCU received no pressure reading due to path issue from the sensor to the controller causing UCA
Sensor sent no pressure reading to HCU due path issue between the controlled process and sensor itself causing UCA

Why was the CA improperly/not executed?
Heater is nonresponsive causing UCA
Heater received no command due to issue in the path from the controller causing UCA
Tank pressure limit set wrong not allowing the requested tank pressure to be achieved causing UCA

5.1.4.14. Causal Scenarios for UCA 7.2

UCA 7.2: HCU sets tank pressure above limit for the required operation creating overpressure in the tank.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

Why the UCA occurred?
HCU incorrectly translates the required power/time for the actuator (inadequate control algorithm) creating higher pressure than needed causing the UCA
HCU incorrectly processing/reading the pressure in tanks, less than actual (flawed process model) causing the UCA
Feedback from pressure sensor not received causing the UCA
Feedback from pressure sensor delayed causing the UCA
Improper pressure feedback(output) - lower than actual - due to systematic +/- error sent to controller causing the UCA
Improper pressure feedback - lower - due to influence from environment, or common +/- error received by sensor causing the UCA

Why was the CA improperly/not executed?
Heater due to error or a voltage spike in the system reacted incorrectly when it was not supposed to, causing the UCA
Tank pressure regulation (controlled process) nonresponsive to commands causing the UCA
Control action correctly executed, but tank pressure regulation system unable to react correctly to the boil off causing the UCA
HCU has inadequate control input from the FCCU (* unsafe input will be assessed in other scenarios)

5.1.4.15. Causal Scenarios for UCA 8.1

UCA 8.1: The EPCU does not provide a set inverter current draw command during flight.

Why the UCA occurred?
Due to incorrectly processed data in the control Algorithm the EPCU assumes that the current draw is already set properly leading to the UCA.
Due to incorrectly processed data in the control Algorithm, the EPCU assumes that the requested current draw cannot be achieved and therefore no command is issued leading to the UCA.
The EPCU does not receive a set EPU power command from the PMCU leading to the occurrence of UCA.
Failure of the EPCU due to a total loss of LV power provision resulting in UCA

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR. ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

Why was the CA improperly/not executed?
The EPCU receives no feedback RPM or Torque data from the EPU causing the UCA.
The EPCU receives incorrect RPM and Torque values that indicate an overspeed condition of the EPU and the UCA is triggered.

5.1.4.16. Causal Scenarios for UCA 8.2

UCA 8.2: The EPCU provides an inverter current draw command that does not match the requested power on the motor in flight.

Why the UCA occurred?
The EPCU provides the command, but it is not received by the EPU indicating a fault in transmission that leads to the UCA.
The EPCU is exposed to external electromagnetic radiation that affects the control algorithm and hence triggers the UCA.

Why was the CA improperly/not executed?
The EPCU receives incorrect torque feedback from the EPU causing the UCA.
The EPCU receives incorrect RPM feedback from the EPU causing the UCA.
The process model of the EPCU processes RPM and Torque sensor feedback data inaccurately and therefore a current draw is commanded to the EPU by the control algorithm that does not match the demand causing the UCA.

5.1.4.17. Causal Scenarios for UCA 9.1

UCA 9.1: The BMU does not provide a DC current draw command while BAT power delivery is expected and commanded by the PMCU.

Why the UCA occurred?
Due to a total loss of LV power supply the BMU fails and causes the UCA.
The BMU fails to issue a DC current draw command due to a software error leading to a failure of the control algorithm and therefore the occurrence of the UCA.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

Why was the CA improperly/not executed?
The BMU is not receiving any feedback from the BAT and the UCA is triggered.
The BMU is receiving incorrect Voltage and Current data leading to an inaccurate SOH calculation and therefore an indication of a defective battery that causes the UCA.
The BMU is receiving incorrect Voltage and Current data leading to an inaccurate SOC calculation and therefor an indication of a depleted battery that causes the UCA.
The process model of the BMU incorrectly determines overall BAT voltage and current based on individual module sensor feedback leading to the UCA.

5.1.4.18. Causal Scenarios for UCA 9.2

UCA 9.2: A BAT DC current draw command is provided by the BMU although no power delivery is demanded by the PMCU.

Why the UCA occurred?
The control algorithm assumes an EPU power setting command from the PMCU due to electromagnetic interferences that was not issued and therefore causes the UCA.
Due to a programming error in the Control Algorithm of the BMU a PMCU power delivery command is incorrectly processed and the UCA is caused.

5.1.4.19. Causal Scenarios for UCA 10.1

UCA 10.1: The PMCU does not provide the BMS with a power requirement command in flight.

Why the UCA occurred?
Complete PMCU failure causing the UCA.
PMCU has an error in the control algorithm and does not issue a set required BAT power command causing the UCA
The PMCU incorrectly processes the voltage and current levels in the HV system determining that no additional BAT power is needed causing the UCA.

Why was the CA improperly/not executed?
Incorrect SOH information makes the PMCU assume a defective battery resulting in the UCA.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

Incorrect SOC information makes the PMCU assume a depleted battery resulting in the UCA.
Incorrect feedback from other controllers (FCCU+EPCU) makes the PMCU assume no BAT power is needed causing the UCA.

5.1.4.20. Causal Scenarios for UCA 10.2

UCA 10.2: The PMCU provides a set BAT power setting command with the delivered BAT power greatly exceeding the commanded value.

Why the UCA occurred?
The control algorithm of the BMU incorrectly processes the BAT Power setting command and causes the UCA.

Why was the CA improperly/not executed?
The BMU processes voltage and current data of individual BAT modules incorrectly and therefore feeds lower than actual power consumption values back to the PMCU causing the UCA.

5.1.4.21. Causal Scenarios for UCA 11.1

UCA 11.1: The PMCU does not provide a set EPU power command while a thrust is demanded from the HC with the aircraft in flight.

Why the UCA occurred?
Complete PMCU failure causing the UCA
PMCU has an error in the control algorithm and does not issue a set EPU power command causing the UCA
PMCU incorrectly processes the voltage and current levels in the HV system (FC+BAT) leading it to assume no sufficient availability of power causing the UCA.
The process model of the PMCU is not able to adequately process the feedback data from the EPCU resulting in no control output.

Why was the CA improperly/not executed?
PMCU does not receive any feedback from other controllers (BMU+FCCU) causing the UCA

5.1.4.22. Causal Scenarios for UCA 11.2

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

UCA 11.2: The PMCU provides an erroneous set EPU power command that does not match the power for the flight phase required thrust.

Why the UCA occurred?
The PMCU is exposed to external electromagnetic radiation that affects the control algorithm and hence triggers the UCA.
The process model of the PMCU is not able to adequately process the feedback data from the EPCU resulting in inadequate control output and hence the UCA.

Why was the CA improperly/not executed?
PMCU does not receive power consumption feedback from the EPCU and hence assumes the EPU is not in operation - causing an increase in power output.

5.1.4.23. Causal Scenarios for UCA 12.1

UCA 12.1: The FCCU does not provide a set coolant mass flow command with the airflow temperature through the radiator exceeding the stack temperature limits and the aircraft in flight.

Why the UCA occurred?
Due to incorrectly processed temperature data, the FCCU does not issue a set coolant mass flow command leading to the UCA.
Due to a total loss of LV electrical power, the FCCU is not able to issue any command causing the UCA.
The FCCU provides a valid set coolant mass flow command but the command is not received by the TMS due to a failure in transmission and the coolant pump is not activated leading to the UCA.

Why was the CA improperly/not executed?
The process model of the FCCU is flawed and expects an ideal operating temperature range that does not represent the ideal range of the stack causing the UCA.
The FCCU does not receive any temperature values from the TMS with the stack temperature sensors working properly due to a failure in transmission therefore the UCA is caused
The FCCU receives incorrect temperature values that indicate a temperature at or below the stack temperature limits due to a malfunction in the temperature sensor with the actual temperature exceeding the limits.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR. ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

5.1.4.24. Causal Scenarios for UCA 12.2

UCA 12.2: The FCCU provides a set coolant mass flow command leading to a decrease of the stack temperature below the lower temperature limit of the FC with the aircraft in flight.

Why the UCA occurred?
Due to an inconsistency in the code of the control algorithm resulting in inadequately processed temperature sensor data, the FCCU issues a set coolant mass flow command with the stack temperature already in the ideal operating temperature range leading to the UCA.
External electromagnetic influences affect the control algorithm of the FCCU and a set coolant mass flow command is triggered although it was not intended.

Why was the CA improperly/not executed?
External electromagnetic influences affect the stack temperature sensors and a set coolant mass flow command is triggered although it was not needed or intended.
The process model of the FCCU is flawed and assumes that the measured temperature exceeds the stack temperature limits with the actual temperature being in range or below causing the UCA.
The FCCU receives incorrect temperature values that indicate a temperature above the stack temperature limits with the actual temperature being in range or below causing the UCA.

5.1.4.25. Causal Scenarios for UCA 13.1

UCA 13.1: The TMCU does not provide a set valve status command to the valve actuator with the coolant flowing around the radiator and the coolant temperature exceeding the stack temperature limits in flight.

Why the UCA occurred?
Due to an inconsistency in the code of the control algorithm resulting in inadequately processed temperature sensor data, the TMCU does not issue an open coolant valve command leading to the UCA.
Due to a total loss of LV electrical power, the TMCU is not able to issue any command and the UCA is caused.
The actuator receives the command but is not able to open the valve due to a mechanical blockage and the UCA is caused

Why was the CA improperly/not executed?
The Process Model of the TMCU does not receive any sensor data with the sensors functioning properly and the UCA is caused

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

Due to an error in the temperature sensor array, the Process Model assumes the coolant temperature to be in range with the actual coolant temperature exceeding the ideal operating temperature range causing the UCA
The Process Model of the TMCU is programmed for a temperature range that does not represent the actual ideal temperature range of the coolant and therefore the stack and the UCA is caused

5.1.4.26. Causal Scenarios for UCA 13.2

UCA 13.2: The TMCU provides a set valve status command leading to a decrease of the coolant temperature below the lower temperature limit of the FC with the aircraft in flight.

Why the UCA occurred?
The TMCU processes temperature sensor data incorrectly and therefore issues a set valve command with the coolant temperature already in the desired temperature range causing the UCA.
External electromagnetic influences affect the processing of sensor readings in the control algorithm of the TMCU and a set valve status command is triggered although it was not intended.

Why was the CA improperly/not executed?
External electromagnetic influences affect the coolant temperature sensors and a set valve status command is triggered although it was not needed or intended.
The process model of the TMCU is flawed and assumes that the measured temperature exceeds the coolant temperature limits with the actual temperature being in range or below causing the UCA.
The TMCU receives incorrect temperature values that indicate a temperature above the coolant temperature limits with the actual temperature being in range or below causing the UCA.

5.1.4.27. Causal Scenarios for UCA 14

UCA 14: The coolant pump actuator receives a set coolant mass flow command with the coolant mass flow not changing as expected in flight.

Why the UCA occurred?
An internal error in the coolant pump due to a motor failure leads to a total loss of coolant flow causing the UCA
A blockage of the coolant pump due to foreign matter in the coolant flow causing the UCA
The coolant pump actuator does not translate the set coolant mass flow command into an according pump RPM due to a software error causing the UCA

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

A total loss of power in the TMS leads to the actuator being unable to set a pump voltage and therefore causing the UCA
Due to external electromagnetic influences the actuator reacts with a RPM output that does not match the requested rotational speed leading to a coolant mass flow rate that does not match the requested causing the UCA

5.1.4.28. Causal Scenarios for UCA 15

UCA 15: The valve actuator receives a set position of mixing valve command with the position of the mixing valve not changing to open and the coolant flowing around the radiator in flight.

Why the UCA occurred?
A blockage of the coolant valve due to foreign matter in the coolant flow causing the UCA
The valve actuator does not translate the set position of mixing valve command into an electric valve actuator voltage due to an inconsistency in the internal code causing the UCA
A total loss of power in the TMS leads to the actuator being unable to set a valve status and therefore causing the UCA
The valve moves in the opposite direction as commanded due to an inconsistency in the software of the control algorithm
Due to external electromagnetic influences the actuator reacts with a voltage output to the electric valve actuator that does not match the requested valve position and therefore causing the UCA

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

5.1.5. STPA Outcomes

Our STPA surfaced a few hazardous scenarios of great concern for a hybrid hydrogen electric powertrain: hydrogen tank over-pressure, loss of inverter current command, fuel cell power falling short under demand, unavailability of battery assistance during transients of power, fuel cell thermal limits' exceedance due to cooling and improper reactants' balancing. Each scenario is based on specific unsafe control actions (UCAs), with traceable causal factors and controller constraints. Collectively, these scenarios span across hydrogen storage & conditioning, electrical powertrain, thermal management, and control unit software interactions, and they all translate into prioritized health-monitoring parameters, sets up thresholds, and plausibility checks that can be implemented early and refined with testing.

The exercise pointed out the importance of carefully and clearly defining the system boundary definition, as this significantly influences the completeness of the analysis. Additionally, distinguishing between mission phases and flight phases proved essential for structuring the assessment in a meaningful way. Many critical parameters can be identified with defining different scopes of the analysis once the development has progressed enough. One key parameter that could be assessed in the future would be humidity control and monitoring of the inlets of the cells.

A key lesson learned was the necessity of a solid understanding of controller logic and internal mechanisms in order to accurately define the potential hazards and triggers to the identified losses and correctly define control actions. Without sufficient technical insight into how a controller operates, it becomes difficult to judge whether a control action can be unsafe and under which conditions. This underlines the importance of cross-disciplinary collaboration and the involvement of subject matter experts throughout the process. Even though STPA can be conducted with general system knowledge, the quality and depth of results improve considerably when technical expertise is applied. This is particularly relevant for the next step in our approach of the exercise, where subject matter experts provide targeted mitigations for the identified scenarios to the respective UCAs.

STPA has strong potential as a method for future compliance demonstrations, particularly for high-complexity systems where conventional prescriptive approaches may not fully capture all interactions and emergent hazards. Its structured, top-down approach allows for a comprehensive evaluation of both functional and interaction-based risks. Overall, this assessment methodology provided valuable insights into potential hazards and causal pathways that may not be readily visible using the traditional safety assessment method. Beyond identifying specific risks, the process also fostered a deeper understanding of system interactions and emphasized the importance of early, structured hazard analysis in the design process.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

5.1.6. Critical Parameters for Hydrogen-Electrical Powertrain Health Monitoring During Flight.

Our analysis of the STPA defined critical parameters to monitor for all 7 controllers. The chosen parameters can be found below and are further explained in the chapter below.

- Air mass flow.
- Oxygen concentration.
- Pressure (cathode inlet, anode inlet, FC TMS coolant and tank).
- Cathode and anode differential pressure.
- Temperature (air, hydrogen and coolant).
- (Fuel Cell) cell voltage.
- System voltage and current.
- Hydrogen concentration.

The scenarios that could lead to unsafe control actions for the human operator mostly came down to the reliability of the system or algorithm implementation. We believe that redundant lower-level controllers and appropriate design assurance levels prevent all of the scenarios, leading to UCAs for human controller.

Next level of control units that we looked at is the FCC/Power management control unit. All the evaluated scenarios stem from incorrect or inaccurate communication or data processing, which is eliminated with appropriate Design Assurance Level (DAL) and code validation and reviews. All aircraft controllers that communicate through CAN bus are susceptible to communication errors and failures. While CAN modules on control units commonly come with error detection, additional bus monitoring units are highly encouraged. Other than that, this controller does not have any parameters to monitor.

The FCCU is the control unit that oversees the fuel cell system. It controls the air supply subsystem, the stack's thermal management subsystem and the electrical distribution subsystem on the stacks. Delivering an incorrect amount of oxygen will affect the fuel cell's performance so the air mass flow rate and oxygen concentration are among the critical parameters that need to be monitored. Another important parameter that's important for the health of the fuel cell stacks is cathode inlet pressure. Blockage on the air line could be detected with a pressure sensor at the inlet of the compressors. This is our next critical parameter to monitor. We assume that the compressors will have their own control units, that would detect blockage or debris in the compressor enclosure. If this is not the case, determining compressor health through continuous built-in tests is necessary. Following this we are also interested in the differential pressures between cathode and anode. Pressure is bound to the compressor speed, so directly controlling for pressure is hard/inefficient. We assume that the hydrogen supply will be able to react to the air side pressure changes and adjust the inlet pressure so that the differential pressure between the sides of the stack membrane is near zero. With this our next critical monitoring parameter is defined: differential pressure between anode and cathode.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

Thermal management (of PEM fuel cells in particular) is vital. The main temperature sensors that must be included in this subsystem are coolant temperature sensors. They allow us to easily monitor the thermal state of the fuel cell stacks at a high level. For the lower-level insight, local thermometers are recommended throughout the fuel cell stacks to be able to detect local hot spots and inconsistencies in stack's thermal performance. In order to transfer equal amount of heat, but at the same time achieve a lighter thermal management system, the temperature of the coolant must be increased. As this temperature is close to the boiling temperature at atmospheric pressure, and in case of a short-term spike in heat generation, this could result in boiling of the coolant. To keep the coolant far enough from boiling conditions, the system should be pressurized. To monitor and upkeep the pressure of the TMS and to be able to detect leakage, pressure sensors should be installed throughout the thermal management system. Cavitation of pumps is a common factor in a pump's lifespan. Detecting high-temperature low-pressure coolant on the pump inlet would allow operators to notice an issue as soon as it starts occurring.

High temperature has a negative impact on cell voltage. It can also be detected electrically, through a Cell Voltage Monitor (CVM). A cell voltage monitor is a device that measures voltages between subsequent cells. Voltage is one of the primary indicators of fuel cell's performance and health, so we believe a cell voltage monitor is a critical component of any fuel cell stack. The power distribution subsystem must be able to confirm how much power the system is providing. Current and voltage sensors are necessary for controlling power.

Lastly, our analysis determined that the most important parameter for the hydrogen storage control unit (dubbed HCU) to monitor is the tank pressure. High redundancy of the sensors is recommended. From the safety perspective, venting subsystem must always be available to avoid tank rupture. To avoid ice buildup on the valves and blockage of vent lines, we recommend temperature monitoring and heating elements.

Given that we operate in a hydrogen environment, with hydrogen as the fuel cell fuel, it is essential to deploy hydrogen concentration sensors at critical joints along the fuel piping. These sensors are vital for detecting potential leaks in areas where mechanical stress or imperfect sealing may occur. Early detection of a leak is crucial for preventing hazardous conditions.

It is not practical to prescribe a specific sensor type, as the selection is inherently driven by the unique requirements of each application and use case. Nevertheless, we recommend considering the sensor's output signal type during selection. Where feasible, opt for output types that offer greater resistance to electromagnetic interference (EMI), such as resistance-based sensors (RTD for temperature measurement) or current loop outputs.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

5.2. Influence of Fuel Cell System Component Placement on Survivability.

5.2.1. Intro to Survivability, Crashworthiness, and CREEP

Survivability in aviation refers to the ability of passengers and crew to withstand the consequence of an accident, not only during the moment of impact but also in the critical minutes that follow. Crashworthiness, a central concept in survivability, is defined as the ability of the aircraft and its systems to protect occupants during and after a crash. In conventional aviation, the fuel system and fuselage design play decisive roles in survivability. For hydrogen-powered aircraft, new challenges arise due to the presence of cryogenic hydrogen tanks, and different ignition risks compared to kerosene.

5.2.1.1. CREEP

To analyze survivability systematically, investigators use the CREEP methodology. CREEP stands for Container, Restraint, Environment, Energy Absorption, and Post-crash factors. Each element must remain within human tolerance levels, if any one component fails, survivability is compromised.

After evaluation of many accidents over the years, some CREEP deficiencies that mainly occurred outside of a crash, were identified in “Redefining Creep” paper [38]. These were added the elements of CREEP where they fall under and marker with asterisks “*”.

5.2.1.1.1. Container

The most critical consideration for crashworthiness concerns the container, or the occupant compartment. The concept of container is a derivation of DeHaven’s first principle and deals with the occupiable space that surrounds the occupants of the aircraft. The aircraft structure “should possess sufficient strength to prevent intrusion of structure into occupied spaces during a survivable crash, thus maintaining a protective shell around all occupants” throughout the accident [39]. This protective shell is often referred to as survivable space or survivable volume.

Protection provided by the other four principles is of no value if the cabin volume is compromised. The following are the main elements of the Container:

- Survivable space must be maintained.
- Airframe hardening:
  - Prevent intrusion into aircraft.
  - Structure must maintain shape throughout crash.
  - Emergency egress locations hardened.
- Retention/Shedding of high mass items:
  - Heavy mass (LH2 tank, Cargo) must be secured to prevent detachment.
  - Ancillary equipment is all removable equipment carried inside the aircraft that could constitute a hazard if unrestrained during a crash:
    - Emergency Equipment (Oxygen bottles, Fire extinguisher, first aid kit...)
    - Survival Equipment (life jackets, locator beacons...)
    - Miscellaneous Equipment (navigation kits, luggage, toolboxes...)
    - Aircraft Subcomponents (batteries, radio and electronic equipment)
- Structurally designed to prevent plowing.
- Protection from high energy strikes*:

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

- Engine failure: While engine cases can be used to contain failed engine components, fuselage shielding may be required for turboprop or propeller driven aircraft.
- Bird/Wildlife strikes: Bird strikes can potentially penetrate the aircraft, causing injury to the crew on the flight deck. Modern aircraft structures and engines are specifically designed to be resistant to bird strikes.

5.2.1.1.2. Restraint

Restraining the occupants within the container is the next most important consideration. Restraints are those systems used to limit occupant flail and prevent striking the interior of the airplane around the survivable space of the aircraft throughout a crash event. These include seat belts, shoulder harness, airbags. The restraints should transfer the inertial loads from the occupants out through the body's strong skeletal structure rather than through soft tissue or vital organs.

The main elements of Restraint:

- Mitigate energy of occupants throughout crash.
- Limit occupant flail, even before the crash*:
  - Restrain occupants inside the aircraft.
  - Secure upper torso to prevent flail.
- Must maintain occupants tie-down chain:
  The Belts are attached to the seats, which are mounted to the aircraft structure.
- Loads must be transmitted to skeletal structure of occupant.

Head injuries due to impacts with the surrounding environment are very common for occupants, restrained only with lap belts. Restraining the upper torso by adding a shoulder harness can significantly reduce the displacement of the chest and head, thus greatly reducing the potential for injury from head and chest impacts and helps to maintain proper spinal alignment for strictly vertical impact forces.

5.2.1.1.3. Environment

Environment “refers to the space that any portion of his body may occupy during dynamic crash conditions” [39].This concerns the occupant’s immediate surroundings during and after a crash. Survivability depends on minimizing hazards within the “flail envelope”, the space a restrained occupant’s body may contact.

If the fuselage provides a protective shell around the occupants after a crash but the occupants receive fatal injuries inside this shell, survivability has not been improved.

The main elements of Environment:

- Delethalization of occupants’ surroundings:
  - Keep objects out of flail envelope when possible.
  - If not, add padding or design to be frangible.
- Environment free from toxic fumes. The effects of smoke exposure can be mitigated by having supplemental breathing devices available.
- Environment free from H_2 leakage. Other than the risk from easily igniting, H_2 can cause asphyxiation.
- Thermal environment in flight or on the ground before any crash*:
  - Extreme temperatures: Exposure to Fire.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

- Cryogenic temperatures due to H_2 leakage or liquid pools.

- High energy, high mass items striking occupants in flight without a crash*:
  - Projectiles withing the container:
    - Unrestrained passengers/lap-held infants.
    - Unrestrained cargo.

5.2.1.1.4. Energy Absorption

Energy Absorption refers to how the aircraft structure, systems, and terrain manage kinetic energy during a crash; Kinetic energy constitutes a significant source of energy at an aircraft's initial impact. The goal is to keep loads transmitted to passengers within human tolerance.

Energy absorbing systems include landing gear, aircraft structure, and crashworthy seats.

The landing gear absorbs the most energy in a vertical impact on a hard surface. The landing gear should be designed such that if it fails, it does not protrude into occupiable section, or into a region containing flammable fuel tank or lines. If this cannot be accomplished by location, the gear should be designed to break away under longitudinal impact conditions.

The fuselage structure must then be designed to absorb the remaining energy that is not absorbed by the landing gear or the seat system.

The structural configuration of the lower fuselage shell is an important factor in crashworthiness. This unoccupied structure should be designed to allow crushing or collapse and absorb energy during deformation.

Several factors influence the required energy absorption:

- Vertical vs longitudinal impact.
  - The energy due to longitudinal and lateral velocities is typically dissipated throughout the aircraft slide out.
  - Vertical velocities: energy is absorbed by the terrain, landing gears, aircraft structure and seats.
- Terrain:
  - Soft ground:
    - Vertical impact: absorbs more energy compared to hard surfaces.
    - Horizontal sliding: aircraft can plow into the ground and displace soil and collapse the structure.
  - Hard ground
    - Horizontal sliding: aircraft will dissipate the energy via the friction between the structure and surface.
- Descent angle and velocities:
  - Most survivable accidents involve descent angles less than 15 degrees and velocities in the range of those for take-offs and landings [40].
  - The vertical velocity component is a limiting factor for most aircraft.
- Impact attitude:

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

- A roll attitude can allow a wing to impact first, producing side accelerations and increasing the danger of fuel spillage by crushing the wing pod fuel tanks or breaking the wing through a fuel tank.
- Pitch attitude increases the likelihood of breaking the fuselage in the occupied areas.

- Materials:
  - A brittle structure will tear away, while a ductile structure, even though it crushes out of the way, will continue to resist loads and absorb energy during the extreme deformation.
  - Not only will unnecessary strength result in an unacceptable weight penalty but on impact high acceleration that degrades occupant survivability may be generated.
- Human tolerance:
  - Human tolerances to accelerations are the highest in the longitudinal direction which is considered eyeballs in or out. They are the lowest in the lateral direction which is considered eyeballs left or right. Some of the most common acceleration-based injuries in aviation are in the vertical direction or eyeballs up or down.
  - Human tolerances may vary based on individual factors

5.2.1.1.5. Post-crash Factors

The last component of CREEP is post-crash factors which include anything that can impact survivability after the crash is over.

One of the most important factors affecting survivability after a crash is the presence of a post-crash fire. Other considerations include water impact, exposure to the elements, availability of medical care, and prompt rescue operations [41].

The Post-Crash Factors can be summarized as:

- Post-Crash fire
  - Respiratory injury due to inhalation of hot gases.
  - Thermal injury.
  - Toxic gases.
  - Smoke: The hazards of smoke may be physical (blocking vision) and physiological (irritation of eyes and respiratory tract, toxicity).
  - Emergency egresses are critical to reduce risk of post-crash fire.
  - H_2flame is invisible and has low radiant heat, so one will know/feel the fire too late.
- Over or under the water egress: Emergency exists should be operable in all aircraft attitude.
- Occupants of high-wing, multiengine aircraft seem to have significantly less chance of surviving a ditching than do occupants of other types of fixed wing aircraft.
- Exposure to the elements after egress
  - Weather/Local Environment.
  - Wildlife.
  - Availability and use of flotations systems:
    - Personal floatation for warm water.
    - Rafts are necessary for cold water immersion.
- Quick access to medical care.
- Prompt rescue operations.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

- Internal Material Choice: Interior materials and insulation can slow the spread of smaller fires and give occupants time to evacuate the aircraft safely or to be rescued by other personnel. However, if not carefully selected, they could release smoke and toxic gases during combustion.

5.2.1.2. Crashworthiness Demonstration Strategy for LH_2 Tank Integration [42]

This study looked at the crashworthiness of single aisle and wide body aircraft of non-integral LH_2tank mounted in the aft of the fuselage. Several interesting points come from this study; they will be listed briefly next.



Figure 26: DLR study, Aft fuselage LH2 tanks (light blue color). [42]

The study investigated what it takes to have crashworthy LH_2 tank integration. They took inspiration from CREEP methodology and Crash Resistant Fuel System used in military aircraft and helicopters.

The main recommendations for a crash resistant LH_2 System are:

- Spatial Arrangement:
  - Installation area relative to crash zone (tank overloading) and cabin area (mass retention).
    - Crash zones are parts of the aircraft where the structure is expected to deform in a crash to protect occupants/components above it. For example, the subfloor under the passenger is designed to deform to absorb energy and protects the floor above it and ultimately the occupants.
  - Spatial separation of energy storage and occupants (e.g. bulkheads, vents, fire walls).
- Surrounding structure (ultimate strength & failure behavior):
  - Resist ultimate inertia forces and provide proper failure behavior to prevent puncture and rupture.
- Energy storage (Frangible / deformable attachment):
  - Tank mount and surrounding airframe structure designed for mass retention and load attenuation. Mounting solutions should be capable of sustaining longitudinal crash load after first impact.
- Distribution system (Frangible /deformable cables & hoses):
  - Reinforced installation areas.
  - Self-sealing breakaway couplings and mounts.
  - Flexible / reinforced / extra-long cables and pipes.
- Energy storage (Impact and tear resistance):
  - Crashworthy tank design with impact, cut and tear resistance regarding true crash loads beyond CS-25.561.
- Ignition source control:
  - Crashworthy vent pipe to discharge boil-off.
  - Spatial separation of LH_2 and ignition sources, or by using ATEX approved equipment.
  - De energizing / shielding electrical sources.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

- LH_2 tank integration for leakage prevention:
  - Limit tank accelerations.
  - Prevent tank intrusion.
  - Limit tank deformation.
- Post crash factors:
  - Evacuation path vs hazards from H_2 (leakage, tank explosion, venting, cryogenic risk).

The study looked at 3 crash load cases:

- Fuselage section Vertical crash impact.
- Fuselage section Horizontal crash pulse.
- Airplane level Combined crash impact.

There are several factors affecting loads in crashes, these are: Vertical and longitudinal velocities, landing gear configuration, aircraft mass, payload, fuel states, pitch and roll and yaw angles, terrain (hard / soft, flat / sloped), obstacles in loss of landing gear and loss of engine situation.

The load cases were simulated for the forward LH_2 tank. Particularly they investigated various tank mounting designs, and the one that was favored is the Spokes and X-rods combination.

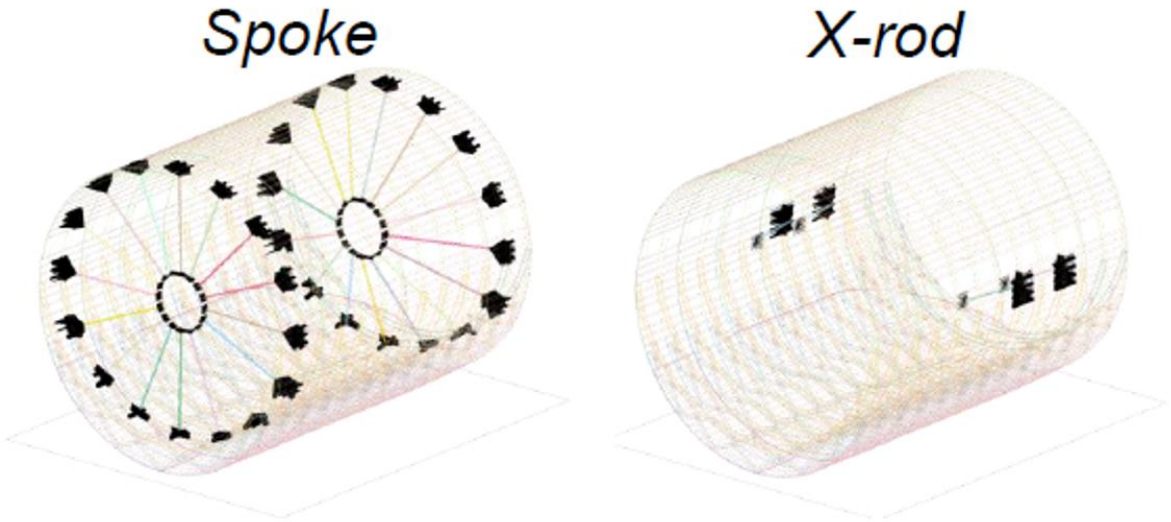


Figure 27: DLR study, tank mounting structure. Left: Spoke type, Right: X-rod type. [42]

The Spokes are the main tank mount structure and resist vertical crash loads. While the X-rods resist the horizontal loads.

In addition to this, they investigated tank crash structure design. The design consists of 3 elements, shown in the figure below:

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

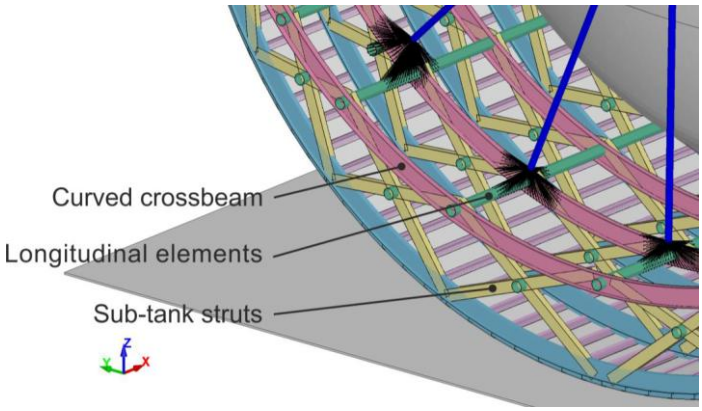


Figure 28: DLR study: LH2 tank crash structure. [42]

- Sub tank struts: absorb the kinetic energy during impact. They are positioned tangentially to the tank surface to minimize the risk of tank penetration.
- Curved crossbeam: withstands crushing loads from the struts and protect the tank.
- Longitudinal elements: stabilize the curved crossbeam and struts under vertical loads and transfer the inertia under horizontal loads.

The conclusion from this study is that although the fuselage section versus full aircraft simulation showed similar results, more distinct failures were identified for the whole aircraft and that's because the kinetic energy of the entire aircraft is at play vs fuselage alone during crash, so higher loads are present. This necessitates the evaluation of the whole aircraft for crashworthiness.

The other main finding is that for a maximum occupant survivability, two layers of crashworthiness need to be stipulated, the crashworthiness of tank integration (airframe structure and tank mount) providing the container function and the crashworthiness of the tank preventing Leak. In some cases, the loads on the aircraft exceed the fuselage capability and penetrate the structure; that is where a crashworthy tank plays a role. It complements the fuselage by providing additional capacity and prevents tank leakage in this extreme case.

Obviously, there are many other crash scenarios that need to be investigated in order to study the survivability of hydrogen concept aircraft such impact of sloped terrain, impact with nose down on a flat surface, break-up mechanisms of the rear section and the effect on the tank...

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

5.2.2. Influence of Hydrogen Component Placement on Survivability.

The location of various Hydrogen components in the aircraft play a significant role in terms of the hazards posed and probability of survival. This section will investigate various positions of the LH_2tank and Fuel Cell within the aircraft, and how these affect the survivability.

It was decided to use Concep C7-HARW from unifier 19 project [37], which is a European funded project under Clean Sky 2 JU.

The C7-HARW model is used for concept 1 and as a reference for the STPA analysis in section 2. OpenVSP [43] is an open-source parametric aircraft geometry tool; once a model is established, components can be easily repositioned to generate alternative aircraft concepts.

Guided by the crashworthiness criteria and recommendations presented earlier, four concept aircraft were designed. These will be presented below and analyzed in terms of survivability using CREEP methodology.

The color codes of the components concerned, used in all configurations, are shown for reference in Figure 30.

In general, for all configurations, there should be firewalls separating the LH_2tank and fuel cells from the cabin and luggage compartment respectively. Firewalls are fire-resistant bulkheads, that slow down the spread of flames and prevent leakage into other compartments.

Another separation is needed between the fuel cells and the LH_2tank. Since the FC is source of high voltage and could potentially be source of ignition. So, by separating them, we eliminate the possibility of any tank's leakage from getting ignited by the fuel cell.

Thus, the recommendation is to have 2 separate sealed compartments, one for the tank and another for the FC.

Since small leakage in any of these compartments is highly probable, the compartment needs to be continuously vented, to prevent hydrogen concentration from reaching its lower flammability limit. Another option would be to utilize the numerous H_2 sensors spread around the tank and FC to detect any tiny leak and then start ventilating the compartment. This can be complemented with the ALBATROS Operational System, like UC6 in D1.1 [44], where the onboard system via the sensors reading can detect H2 leakage for example and send an alert simultaneously to the pilots, and to the affected stakeholders for example the air navigation service providers, airlines and airport operators. This will make the stakeholders aware early on of the critical situation and prepare for an emergency. The ALBATROS Operational System is updated with any new information, and all the relevant users are informed.

Another requirement is to have a crashworthy vent pipe like the kerosene fuel system crashworthiness requirement. The idea is to allow certain movement of the vent pipe either by being flexible or longer than needed.

Connections between the tank/FC and piping should incorporate breakaway couplings (self-sealing valve), including at the firewall passthroughs. The system is designed to be segregated so that, in the event of crash damage or component separation, any potential leakage can be contained.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

The tank mounting structure needs to provide mass retention in all configurations. This becomes more critical and might require stronger attachments the closer the tank to the cabin is.

All configurations were designed so they meet the center of gravity safety margin as the original concept of unifier19.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

5.2.2.1. Configuration 1(C7-HARW): Mid-Fuselage.

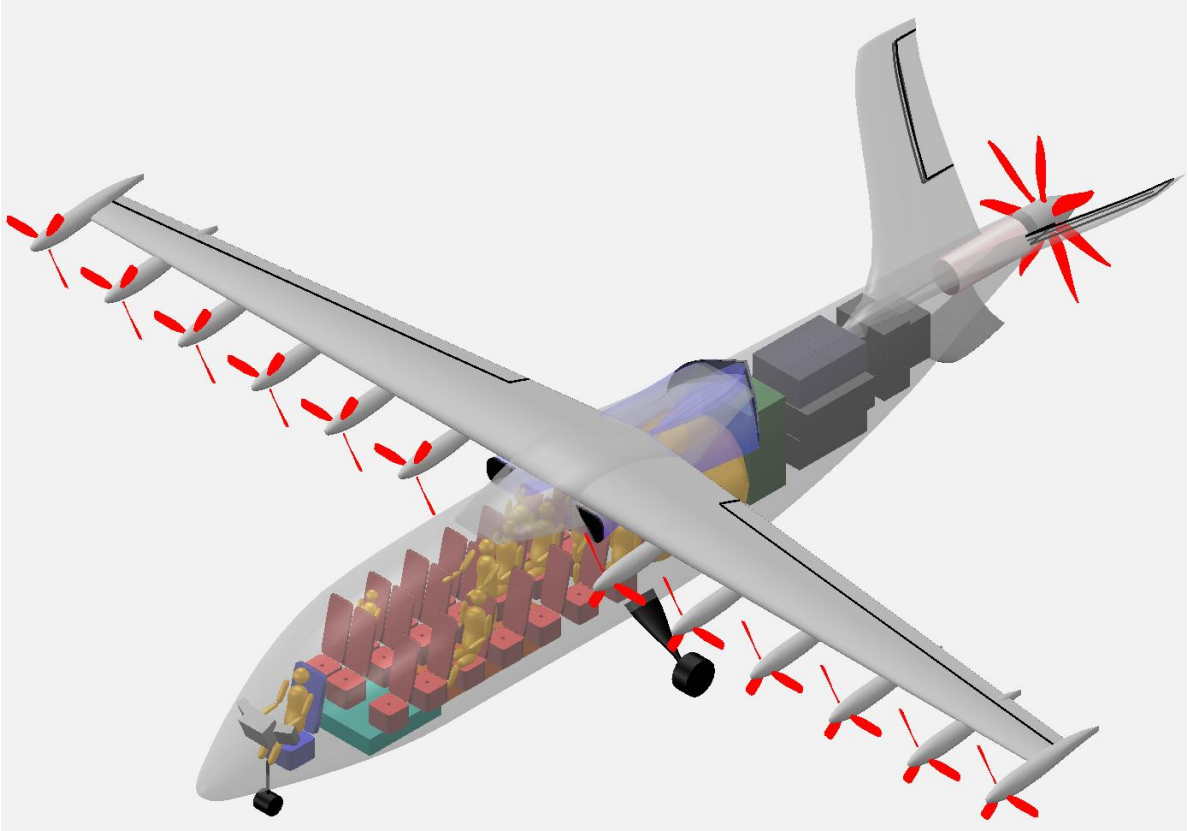


Figure 29: Configuration 1: Mid-Fuselage, Iso left view. [43]

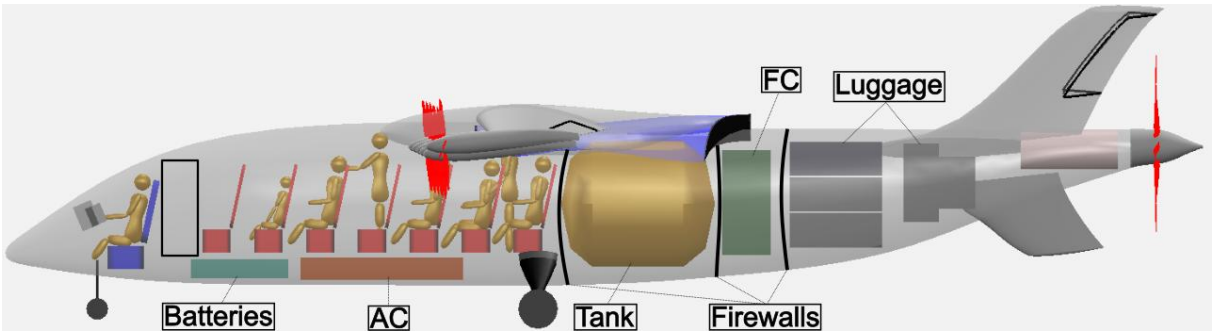


Figure 30: Configuration 1: Mid-Fuselage, Side view. [43]

In this configuration, the tank and the fuel cells are in the middle of fuselage between the cabin and luggage compartment. The tank, being a significant mass located directly behind the cabin, presents an additional safety risk. A robust mounting solution is required to ensure it remains secure and does not endanger passengers.

By placing the tank close to the fuel cell, this configuration shortens the piping and decreases the likelihood of leakage at joints or connections.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

However, in the event of a fire or leak, this configuration places the rear evacuation route in closer proximity to the H_2 hazards.

Thus, the recommendation is to have maximum separation between energy storage and cabin/evacuation path, separated via firewall, and robust tank mounts.

5.2.2.2. Configuration 2: Aft-Fuselage.

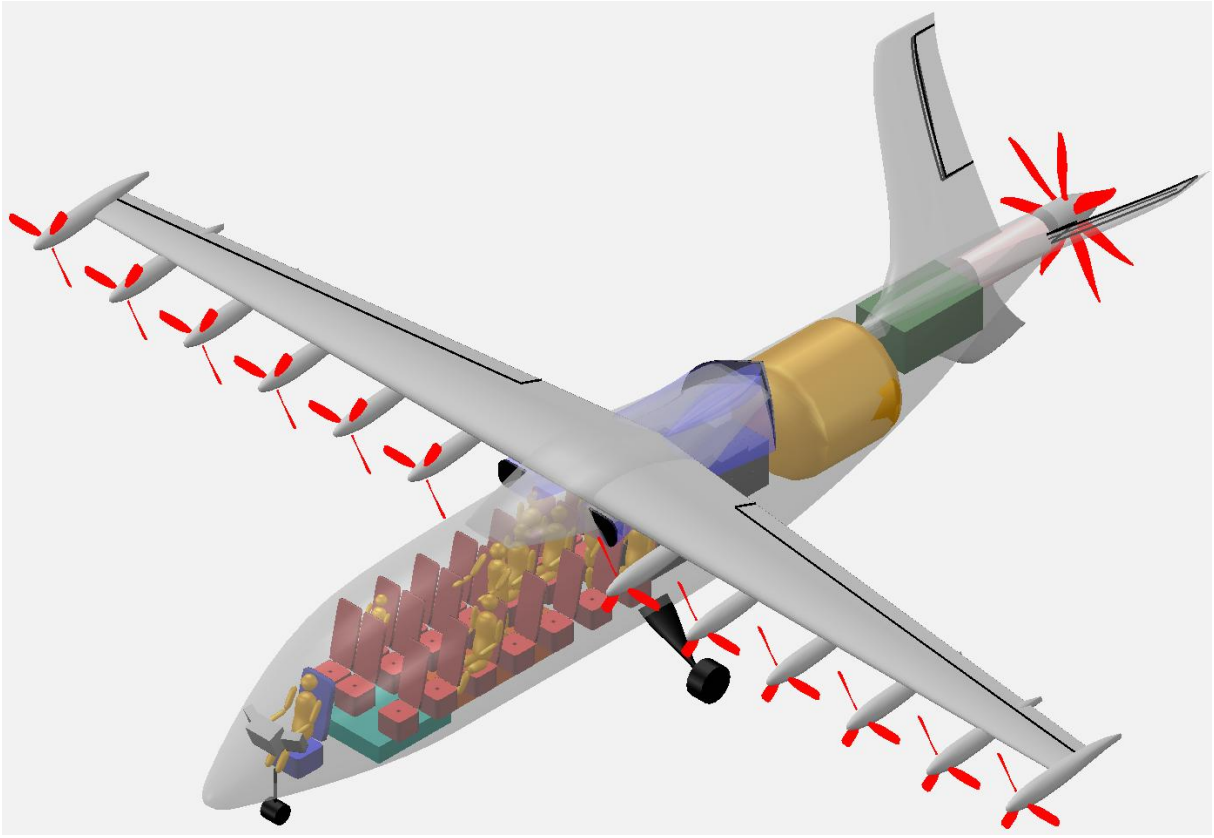


Figure 31: Configuration 2: Aft-Fuselage, Iso left view. [43]

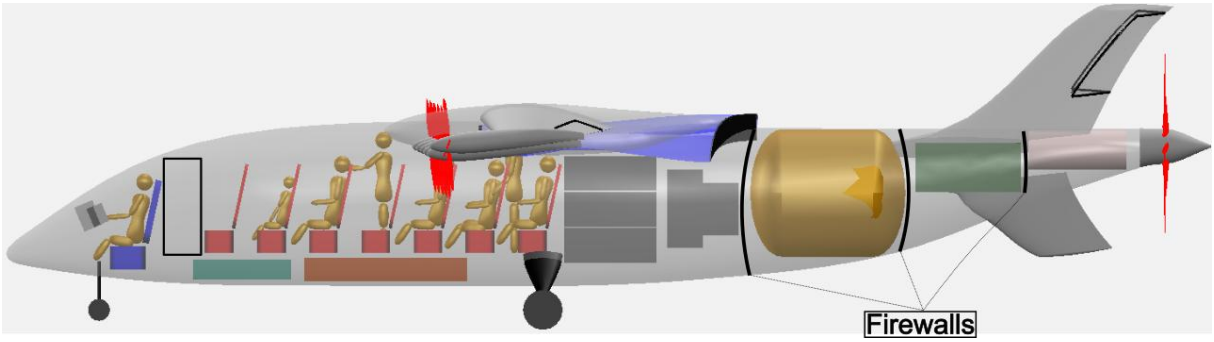


Figure 32: Configuration 2: Aft-Fuselage, Side view. [43]

In this configuration, the tank is separated from the cabin by the luggage compartment; so, there is good separation between fuel source and occupants.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

The tank is outside the crash zone, away from the landing gear, eliminating the risk of a landing gear collapsing and piercing the tank.

The tank and FC being further aft, result in an increase of high voltage (HV) wire length running towards the motors. Long HV cables can potentially act as ignition source if damaged in a crash or due wear.

This concept has the benefit that it preserves the front and rear egress in case of a leak or fire.

Although this section focuses on the placement of hydrogen powertrain components, it's important to note the unconventional positioning of the battery within the subfloor area. Traditionally, the subfloor is engineered to crumple and absorb impact energy, thereby safeguarding the cabin and its occupants. However, the battery, being a rigid structure, does not deform or dissipate energy in the same manner. This design choice can lead to increased acceleration forces on passengers during a collision and heighten the risk of thermal runaway due to its location within the crash zone. Additionally, any intrusion of the battery into the cabin space could compromise the integrity of the subfloor.

5.2.2.3. Configuration 3: Front-Fuselage.

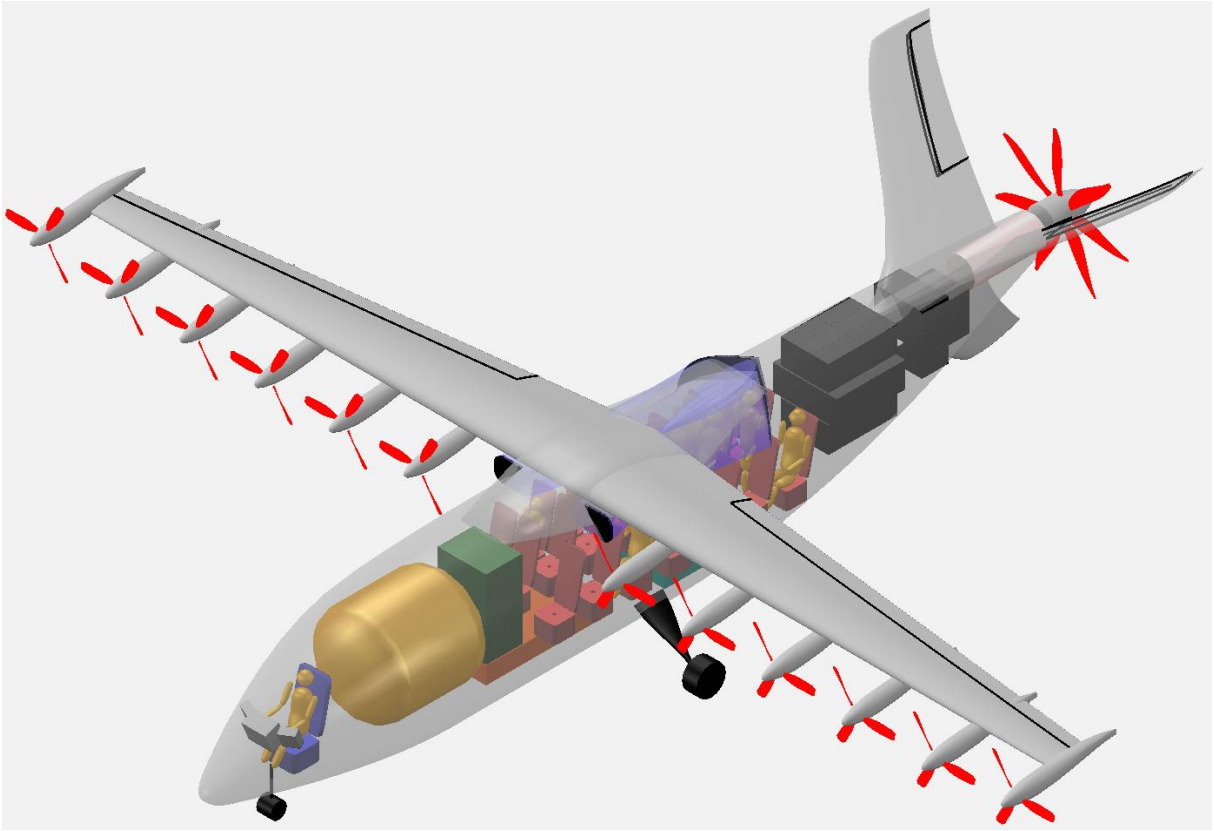


Figure 33: Configuration 3: Front-Fuselage, Iso left view. [43]

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

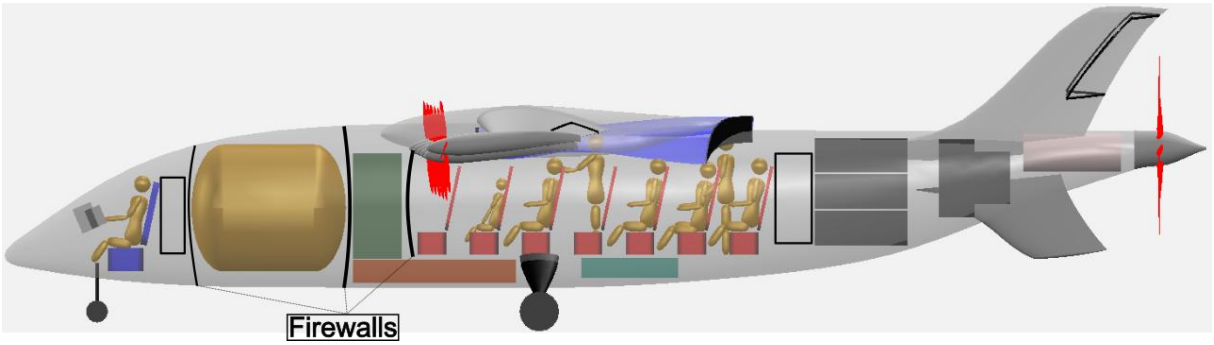


Figure 34: Configuration 3: Front-Fuselage, Side view. [43]

In this configuration, the LH2 tank and Fuel cells are in the front part of the fuselage between the pilot and passengers' cabin. So, the cockpit and cabin have separate exits. Like the first concept, this configuration suffers from lack of sufficient separation with the cabin compartment. And in this case, it is quite close to the cockpit, so, more critical mounting is required for mass retention.

Again, in case of a fire or a leak, this increases the H_2hazards proximity to the front evacuation pass.

Another drawback is that airplanes typically land into a headwind; therefore, in the event of a fire or fuel leak during a crash, smoke and flames may be carried toward the cabin, heightening the risk of burns or asphyxiation.

Furthermore, in a horizontal front impact with a wall, the front structure could crash and deform/pierce the tank resulting in an increased risk.

From all the configuration presented in this report, this has the most drawbacks and thus the least favorite.

5.2.2.4. Configuration 4: Pod-Wings.

In this concept, the LH2 tanks are located in Pods under the wings. Firstly, this results in a shorter fuselage as tank is no longer located within the fuselage. The pod wing concept offers some unique characteristics, first the fuel source is quite separated from the cabin, and any fire or leak from the tanks does not reach the passengers, but it might hinder their evacuation in some situations.

However, the hydrogen pipes are relatively long and traverse multiple sections of the aircraft to reach the fuel cells, which increases the risk of leakage. This risk can be mitigated by routing the fuel line outside the fuselage, thereby eliminating the potential hazard. If not, route the fuel pipe through an enclosed and ventilated shroud.

A unique risk of this configuration is the exposure to high-energy impacts, either from bird strikes or blade release. While bird strike hazards can be mitigated through an existing split-bird pod design, blade release poses a greater challenge since the open-rotor electric motors lack the protective nacelle found in conventional systems. To address this, the pod must be reinforced in the area facing the propellers, which inevitably increases weight.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

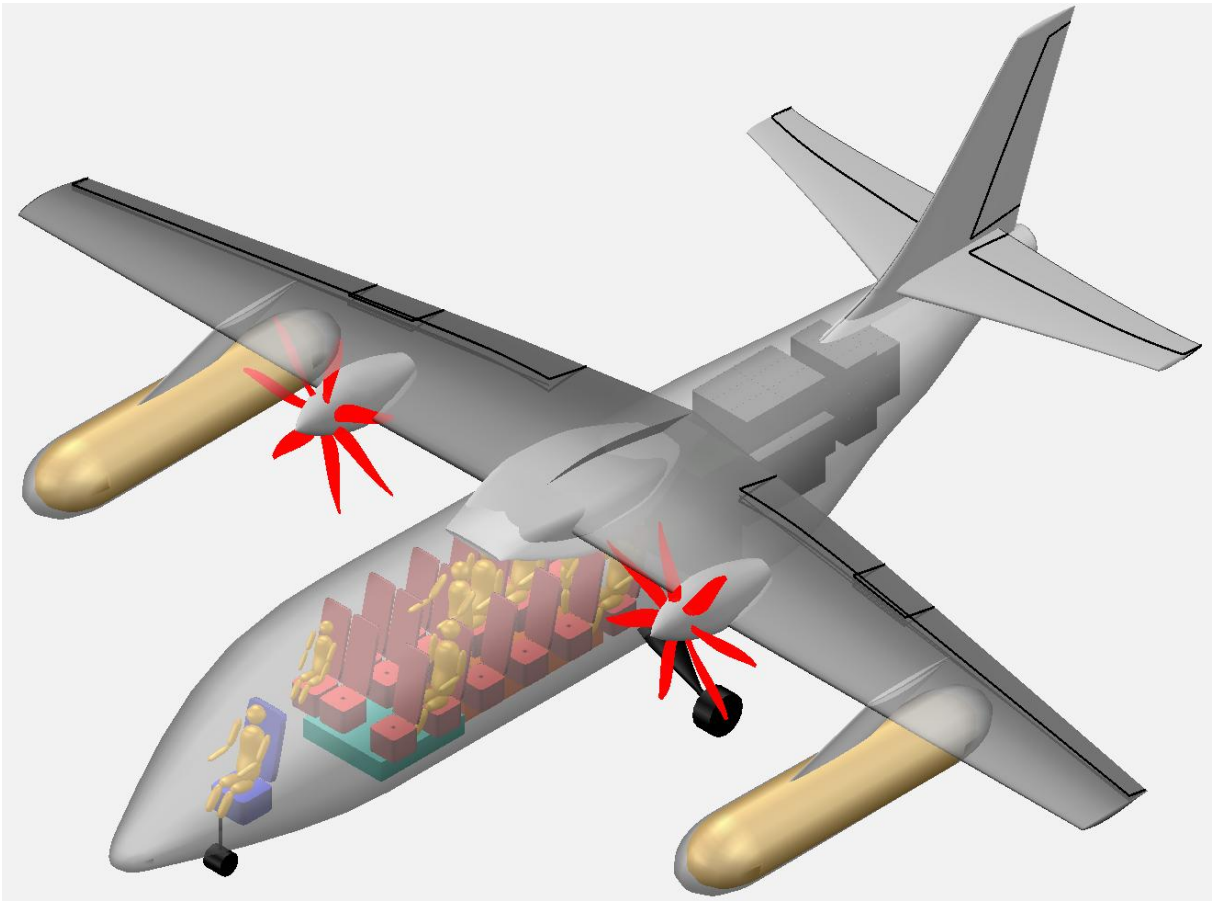


Figure 35: Configuration 4: Pod-Wings, Iso left view. [43]

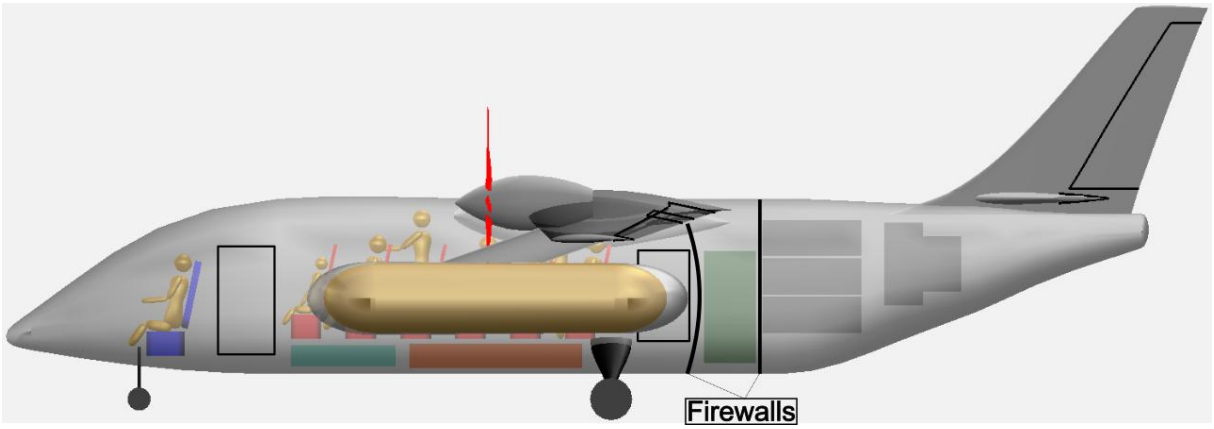


Figure 36: Configuration 4: Pod-Wings, Side view. [43]

Another advantage of this configuration is that the pod mounting can be designed as frangible, similar to a pylon engine, allowing it to detach upon direct impact. This reduces wing loads and lowers the risk of fire or leakage affecting passengers. Certainly, the tank's pressure relief valve, safety valve and burst disk are attached to the tank under the fairing. For the venting and fueling lines, these needs to have frangible

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

attachments and self-sealing valve under the fairing, so when the tank pod detaches, all lines connected to the tank are sealed.

5.2.2.5. General Recommendation for All Configurations

There should be proper emergency escape provisions:

- Emergency exits must remain functional after deformation.
- Exits should be located as far as possible from fuel spillage areas and from major ignition sources.
- Emergency exits must be clearly marked both inside and outside the aircraft so that occupants and rescuers can find them promptly.
- Emergency exits must be equally divided between both sides of the aircraft to provide alternate means of escape if, for any reason, the exits on one side become blocked.
- Proper interior emergency lighting and emergency exit lights.
- Unimpeded access to some of the exits: Consideration should be given to equipment, such as seat backs, that could impede egress.

Ignition sources should be prevented or limited:

- There are two types of spark generation:
  - Friction spark: Friction sparks become possible ignition sources when portions of aircraft structure scrape along the ground. There are two ways to mitigate this:
    - For likely region of contact: use materials that have little to no-sparking tendency. Compared to other metal used in aircraft, Aluminum alloys are the least likely to cause ignition of spilled fuel. [45]
    - Shielding: Prevent flammable fluids from reaching potential ignition sources, for example by using baffles or sealed curtains.
  - Electrostatic sparks: It may be possible to reduce electrostatic charge by applying coatings to those parts of the aircraft likely to be separated in a crash.
- Electrical source: The aircraft electrical system is a potential fire ignition source because it is distributed extensively throughout the aircraft. Effective ways to reduce these ignition hazards:
  - De-energizing batteries, generators and inverters, before or during a crash.
  - Components should be located away from flammable sources, and in areas where anticipated impacts will be minimal.
  - Wires should be routed along the strongest structural members and attached via frangible attachments.
  - Non-sparking breakaway connectors should be used in areas where high forces are expected. [46]
  - All wire connectors must be shielded and of non-sparking type.
  - Use of ATEX approved equipment.
- Oil, Hydraulic fluid: can be easily ignited from a hot surface; by themselves, they constitute a low threat to aircraft occupants. But unfortunately, they function as ignition sources for other combustibles, especially spilled fuel. [47]
- Hot surface

A crash-fire prevention system should include an initiating system that senses the existence of crash-fire conditions and causes action to be taken to suppress the ignition sources.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

5.2.3. Conclusion

In conclusion, all 4 configurations are feasible. The following recommendations can be deduced:

Hydrogen fuel lines should be routed where there is less likely to be damage to the structure, route them through ventilated shroud, to prevent leakage going into other compartments.

Firewalls should be installed between LH_2 compartment and cabin, fuel cell compartment and luggage area.

The LH_2 and fuel cell compartments should be ventilated either constantly or based on measured H_2concentration.

H_2 sensors, and probably temperature and pressure sensors, should be spread around both compartments, and around fuel piping, in order to detect any leak early one and take all the precaution to prevent fire and explosion from occurring, by ventilating for example, shutting off some lines…

LH_2 tank and fuel cells should be positioned away from crash zones, and they may need to be designed as crashworthy so that survivability is achieved in all expected survival loads.

Furthermore, there should be proper emergency escape provisions, and elimination of ignition sources where possible, otherwise a good separation from the fuel source.

To continue the studies on survivability of hydrogen fuel cell aircraft, it is recommended to perform computational crash analysis on the structure, especially using the full aircraft, to obtain more reliable data on the deformation of the survivable volume that allows the prediction of potential damage to powertrain components during the crash.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

5.3. Fuel Cell Powertrain Components Failure Design Improvement

As hydrogen fuel cell powertrain uses electrical motors for its propulsion, one design improvement could be using dual-motor for a single propeller, this improves redundancy and safety. The section below describes the dual-motor setup along with the tests done to prove the working concepts.

5.3.1. Dual-Motor Tests

Hydrogen fuel cell powertrains paired with electric motors provide several advantages over conventional combustion-driven propellers. Beyond their higher efficiency, they also offer improved reliability and built-in redundancy. Since the FC generates electrical power for the electric motors to use, which is subsequently converted into thrust via a propeller, the propulsion architecture can be optimized for redundancy and distributed load-sharing rather than constrained by the limitations of a single prime engine.

Instead of relying on a single large motor to spin a propeller, the system can employ two smaller electric motors, mechanically coupled to a common propeller shaft. This setup introduces redundancy: if one motor fails, the other can continue operating at half total torque, allowing the mission to proceed safely. The concept can be extended further; each propeller can be powered by two motors, managed by two inverters, and supplied by two independent power sources. This mirrors the advantages of Distributed Electric Propulsion (DEP), where redundancy and fault tolerance are built into the design.

Such a dual-motor configuration is particularly valuable for the pusher motor, which provides cruise thrust and assist in takeoff in concepts 1, 2, and 3 in section 5.2.2. Even if one motor, or one inverter, or one power source (one of the fuel cell or a battery) fails, the pusher can still deliver at half its original thrust, ensuring mission continuation or enabling a safe emergency landing.

In the twin-engine architecture (concept 4), each nacelle can incorporate dual-motor system. In the event of a single motor or inverter failure, thrust can be redistributed across the remaining units, thereby eliminating the asymmetric thrust and yawing moment characteristic of conventional IC twin-engine aircraft. Unlike combustion-based systems, where the failure of one engine results in complete thrust loss on that side and significant yaw instability, the dual-motor electric configuration ensures balanced thrust distribution, eliminates the large yawing effect, and significantly improves overall safety margins.

To test this design improvement, it was decided to build a dual-motor setup and test it. The dual-motor consists of two EMRAX 268 MV electric motors. One motor is standard motor, while the other comes with extended shaft, where both outer cases of the outrunner motors are connected to the same shaft. The structure connecting the two motors and the mounting is designed in house. Figure 37 shows the various parts, along with the final assembly of the dual-motor.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.



Figure 37: Dual Motor assembly.

Each motor is connected to a Pipistrel developed 800V inverter, shown in Figure 39. Each inverter is connected to one power source consisting of two 400V batteries in series to provide the 800 Volts needed. The two-power sources are independent. Additionally, the motors and inverters are liquid cooled using a mixture of 50% Glycol and 50% water.

The dual motors are mounted to the test stand via two flat plates and between them load cells to measure the thrust and the torque.

Furthermore, via the inverters we measure the RPM, current and voltage, thus the electrical power. From RPM and torque we can calculate the shaft power and compare it to the electrical power to evaluate efficiency.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

A four-bladed propeller is used, which can handle the combined torque output of the dual-motor setup, achieving a higher RPM than a single motor can.



Figure 38. 4-Bladed propeller.



Figure 39. Test Rig assembly

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

Several tests were done on the dual-motor setup with the aim of proving the working concept and testing different scenarios that might be faced during a flight.

The tests are listed in Table 7.

Test No. & Title	Objectives
1. Dual motor at maximum rated prop RPM of 2300.	Find the maximum power, thrust, torque at the maximum propeller rated RPM of 2300.
2. Max RPM single motor	Find the maximum RPM and associated power, thrust and torque of a single motor.
3. Both running disengage one	To demonstrate that 2^{nd} motor can be disengaged in operation, and 1^{st} motor continues operating.
4. One running engage 2^{nd}.	To demonstrate that 2^{nd} motor can be engaged in operation.
5. Asymmetric power	To simulate a situation when the 2^{nd} motor produces less power.
6. Breaking	To simulate one motor breaking.
7. Single Dual Motor	To quantify the friction/losses from the 2^{nd} motor in the dual-motor setup compared to a single motor setup.
8. Single Motor	Used for comparison to answer the objective of test 8.

Table 7: Dual-Motor tests.

The inverter is controlled via CAN communication protocol using Dewesoft for data acquisition.

During all tests we increased and decreased the RPM gradually then ran the test at the desired RPM for at least a minute, to make sure motors can run without any error or temperature limitations.

Below is a more detailed description of the tests and findings.

1. The propeller is rated at 2300 RPM.
    a. Increase the RPM gradually to reach 2300, then adjust the torque of both motors so that they contribute equally.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

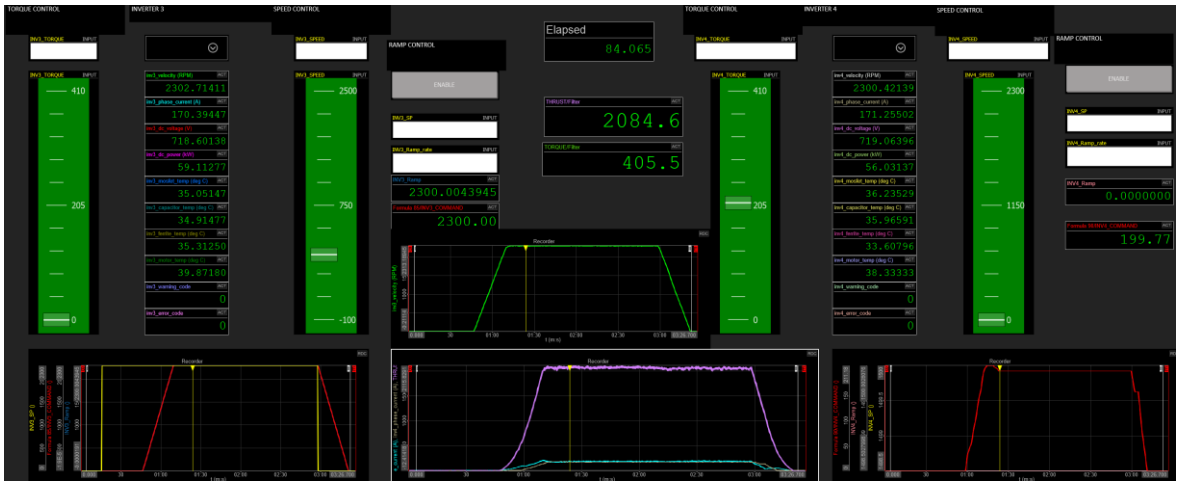


Figure 40: Dual motor test 1 @2300RPM.

2. With only on motor running, find the maximum reachable rpm.
    a. One motor could reach 2260 RPM, short of 2300, just for a brief moment as its temperature reaches 110°C and the inverter's protection kicks in and reduces the power.
3. In this test, we simulate a problem in flight on one of the motors, so it stops generating torque; this can be a result of a failure of either the motor or the inverter or one power source (FC or battery). After disengaging one of the motors, the second motor continues spinning, still generating certain thrust, also reduced, at a lower RPM.

    Thus, in this case, the flight can continue safely.
4. In this test, we simulate restarting/engaging second motor in flight. We start with one motor working at 2000 RPM and then engage the second one. The second motor starts contributing to the required torque for maintaining the RPM constant and thus relieving the first motor.
5. In this test we simulate asymmetric power. Starting with two motors contributing equal torque at 2300 RPM, we reduce the torque on one of the motors, the second motor tries to compensate by increasing its torque to keep the RPM constant. The system continues working without any issue.
6. In this test, we simulate a mechanical failure of one motor, thus resisting the rotating of the 2nd motor (applying negative torque). The 2nd motor continues rotating and outdo the resistance of the "broken" motor. The test continued until the resistive torque is equal to the positive one, and here both motors came to a stop.
7. Test 7 & 8: In the dual-motor setup, if one motor is supplied power and rotating at constant rpm, the unpowered motor(open-circuited) will be producing certain resistance, which is mainly due to bearing friction or windage, or any other mechanical loss due to coupling.

    The aim of this test is to find out how significant this resistance is. To do so, we compare the dual-motor with only one of the two motors powered with a standalone single motor. Both tests are run at a fixed RPM of 2000. The torque necessary to reach this rpm, is recorded and compared between the two tests.

    What these two tests showed is that the extra torque required to overcome the resistance of the 2nd motor is not significant, in the order of couple of Nm.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

5.3.2. Conclusion

The performed tests showed that the dual-motor concept worked as intended. It is a feasible and beneficial concept that could be implemented when redundancy and safety are of upmost importance. Even though this system is a bit heavier, mainly due to mounting the motors together, compared to a bigger motor with equal total torque, the benefits in terms of redundancy and safety might outweigh the extra mass. This concept could be most beneficial in aircraft where it is either the main pusher/puller engine, or in a twin engine configuration as it eliminates the large yawing moment resultant from one engine inoperable and could result in smaller vertical tail, if certification permits it.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

6 CONCLUSION

This deliverable establishes the foundation for understanding and addressing the safety implications associated with emerging battery-electric and hydrogen-electric propulsion technologies. By outlining the relevant hazards, framing the planned analyses, and defining the methodological approach for both technology pathways, the report provides a structured basis for the work that follows in subsequent project phases.

The distinction between the more mature battery-electric domain and the exploratory nature of hydrogen-electric propulsion has shaped the organisation of this document, resulting in a two-part structure that reflects the differing levels of operational experience, data availability, and technological readiness. This structure ensures that each technology is evaluated through an appropriate lens: empirical and improvement-oriented for batteries, conceptual and safety-driven for hydrogen systems.

The analyses presented here serve primarily as preparatory work for the detailed investigations, demonstrations, and validation activities to be delivered later in the project, in particular in D3.3. By identifying key risks early and defining the frameworks through which they will be assessed, this deliverable supports a coherent and transparent progression of the Albatros WP3 work package. It ensures that future experimental efforts will be grounded in a clear rationale and aligned with the project's overarching objectives of enabling safe, reliable, and certifiable integration of novel energy systems into future aircraft.

Overall, this report marks an essential step in the project's broader aim: to translate emerging propulsion concepts into practical, validated, and safety-informed solutions for the aviation sector. The methodologies, risk mappings, and planned investigations described here will guide the next stages of research and help ensure that the transition to sustainable aviation technologies is supported by rigorous and proactive safety assessment.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

7 REFERENCES

[1] X. Feng, M. Ouyang, X. Liu, L. Lu, Y. Xia and X. He, "Thermal runaway mechanism of lithium ion battery for electric vehicles : A review," *Energy Storage Materials,* no. 10, pp. 246-267, 2018.

[2] Y. Chen, Y. Kang, Y. Zhao, L. Wang, J. Liu, Y. Li, Z. Liang, X. He, X. Li, N. Tavajohi and B. Li, "A review of lithium-ion battery safety concerns : The issues, strategies, and testing standards," *Journal of Energy Chemistry,* vol. 59, pp. 83-99, 2021.

[3] L. Román-Ramírez and J. Marco, "Design of experiments applied to lithium-ion batteries : A literature review," *Applied Energy,* vol. 320, 2022.

[4] F. Larsson, P. Andersson and B.-E. Mellander, "Lithium-Ion Battery Aspects on Fires in Electrified Vehicles on the Basis of Experimental Abuse Tests," *Batteries,* vol. 2, no. 2, 2016.

[5] D. P. Finegan, E. Darcy, M. Keyser, B. Tjaden, T. M. M. Heenan, R. Jervis, J. J. Bailey, N. T. Vo, O. V. Magdysyuk, M. Drakopoulos, M. D. Michiel, A. Rack, G. Hinds, D. J. L. Brett and P. R. Shearing, "Identifying the Cause of Rupture of Li-Ion Batteries during Thermal Runaway," *Advanced Science,* vol. 5, 2017.

[6] A. W. Golubkov, D. Fuchs, J. Wagner, H. Wiltsche, C. Stangl, G. Fauler, G. Voitic, A. Thaler and V. Hacker, "Thermal-runaway experiments on consumer Li-ion batteries with metal-oxide and olivin-type cathodes," *RSC Advances,* no. 7, pp. 3633-3642, 2014.

[7] A. W. Golubkov, S. Scheikl, R. Planteu, G. Voitic, H. Wiltsche, C. Stangl, G. Fauler, A. Thaler and V. Hacker, "Thermal runaway of commercial 18650 Li-ion batteries with LFP and NCA cathodes – impact of state of charge and overcharge," *RSC Advances,* no. 70, pp. 57171-57186, 2015.

[8] F. A. Mier, M. J. Hargather and S. R. Ferreira, "Experimental Quantification of Vent Mechanism Flow Parameters in 18650 Format Lithium Ion Batteries," *Journal of Fluids Engineering,* 2019.

[9] Y. Fu, S. Lu, K. Li, C. Liu, X. Cheng and H. Zhang, "An experimental study on burning behaviors of 18650 lithium ion batteries using a cone calorimeter," *Journal of Power Sources,* 2015.

[10] X. Liu, S. I. Stoliarov, M. Denlinger, A. Masias and K. Snyder, "Comprehensive calorimetry of the thermally-induced failure of a lithium ion battery," *Journal of Power Sources,* vol. 280, pp. 516-525, 2015.

[11] F. Larsson, J. Anderson, P. Andersson and B.-E. Mellander, "Thermal Modelling of Cell-to-Cell Fire Propagation and Cascading Thermal Runaway Failure Effects for Lithium-Ion Battery Cells and Modules Using Fire Walls," *Journal of The Electrochemical Society,* vol. 163, no. 14, 2016.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

[12] A. García, J. Monsalve-Serrano, R. L. Sari and S. Martinez-Boggio, "An optical investigation of thermal runaway phenomenon under thermal abuse conditions," *Energy Conversion and Management,* vol. 246, 2021.

[13] H. Li, Q. Duan, C. Zhao, Z. Huang and Q. Wang, "Experimental investigation on the thermal runaway and its propagation in the large format battery module with Li(Ni1/3Co1/3Mn1/3)O2 as cathode," *Journal of Hazardous Materials,* vol. 375, pp. 241-254, 2019.

[14] S. Gao, L. Lu, M. Ouyang, Y. Duan, X. Zhu, C. Xu, B. Ng, N. Kamyab, R. E. White and P. T. Coman, "Experimental Study on Module-to-Module Thermal Runaway-Propagation in a Battery Pack," *Journal of The Electrochemical Society,* 2019.

[15] S. Shahid and M. Agelin-Chaab, "A review of thermal runaway prevention and mitigation strategies for lithium-ion batteries," *Energy Conversion and Management : X,* 2022.

[16] H. Wang, H. Xu, Z. Zhao, Q. Wang, C. Jin, Y. Li, J. Sheng, K. Li, Z. Du, C. Xu and X. Feng, "An experimental analysis on thermal runaway and its propagation in Cell-to-Pack lithium-ion batteries," *Applied Thermal Engineering,* vol. 211, 2022.

[17] DNV GL Energy Insights USA, Inc., "McMicken Battery Energy Storage System Event Technical Analysis and Recommendations," Chalfont, 2020.

[18] M. Henriksen, K. Vaagsaether, J. Lundberg, S. Forseth and D. Bjerketvedt, "Simulation of a premixed explosion of gas vented during Li-ion battery failure," *Fire Safety Journal,* vol. 126, 2021.

[19] M. Henriksen, K. Vaagsaether, J. Lundberg, S. Forseth and D. Bjerketvedt, "Numerical study of premixed gas explosion in a 1-m channel partly filled with 18650 cell-like cylinders with experiments," *Journal of Loss Prevention in the Process Industries,* 2022.

[20] W. Li, K. Crompton, C. Hacker and J. K. Ostanek, "Comparison of Current Interrupt Device and Vent Design for 18650 Format Lithium-ion Battery Caps," *Journal of Energy Storage,* vol. 32, 2020.

[21] W. Li, K. Crompton and J. K. Ostanek, "Comparison of current interrupt device and vent design for 18650 format lithium-ion battery caps : New findings," *Journal of Energy Storage,* vol. 46, 2022.

[22] G.-H. Kim, A. Pesaran and R. Spotnitz, "A three-dimensional thermal abuse model for lithium-ion cells," *Journal of Power Sources,* vol. 170, no. 2, pp. 476-489, 2007.

[23] Q. Wang, P. Ping, X. Zhao, G. Chu, J. Sun and C. Chen, "Thermal runaway caused fire and explosion of lithium ion battery," *Journal of Power Sources,* vol. 208, pp. 210-224, 2012.

[24] W. Li, V. L. Quiroga, K. R. Crompton and J. K. Ostanek, "High Resolution 3-D Simulations of Venting in 18650 Lithium-Ion Cells," *Frontiers in Energy Research,* vol. 9, 2021.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

[25] J. Kim, A. Mallarapu, D. P. Finegan and S. Santhanagopalan, "Modeling cell venting and gas-phase reactions in 18650 lithium ion batteries during thermal runaway," *Journal of Power Sources,* vol. 489, 2021.

[26] D. Kong, G. Wang, P. Ping and J. Wen, "A coupled conjugate heat transfer and CFD model for the thermal runaway evolution and jet fire of 18650 lithium-ion battery under thermal abuse," *eTransportation,* vol. 12, 2022.

[27] X. Li, F. He and L. Ma, "Thermal management of cylindrical batteries investigated using wind tunnel testing and computational fluid dynamics simulation," *Journal of Power Sources,* vol. 238, pp. 395-402, 2013.

[28] R. Srinivasan, M. E. Thomas, M. B. Airola, B. G. Carkhuff, L. J. Frizzell-Makowski, H. Alkandry, J. G. Reuster, H. N. Oguz, P. W. Green, J. L. Favors, L. J. Currano and P. A. Demirev, "Preventing Cell-to-Cell Propagation of Thermal Runaway in Lithium-Ion Batteries," *Journal of The Electrochemical Society,* vol. 167, no. 2, 2020.

[29] G. Wang, D. Kong, P. Ping, X. He, H. Lv, H. Zhao and W. Hong, "Modeling venting behavior of lithium-ion batteries during thermal runaway propagation by coupling CFD and thermal resistance network," *Applied Energy,* vol. 334, 2023.

[30] A. Cellier, F. Duchaine, T. Poinsot, G. Okyay, M. Leyko and M. Pallud, "An analytically reduced chemistry scheme for large eddy simulation of lithium-ion battery fires," *Combustion and Flame,* vol. 250, 2023.

[31] A. Cellier, F. Duchaine, T. Poinsot, E. Brodu, B. Boust, M. Bellenoue, G. Okyay, M. Leyko and M. Pallud, "Large eddy simulation of lithium-ion battery vent gases flame ignition and anchoring," *Proceedings of the Combustion Institute,* vol. 40, 2024.

[32] A. Cellier, "Simulation aux Grandes Echelles de Feux de Batteries Lithium-ion pour le Diagnostic de l'Emballement Thermique," *Theses,* 2023.

[33] A. Refloch, B. Courbet, A. Murrone, P. Villedieu, C. Laurent, P. Gilbank, J. Troyes, L. Tessé, G. Chaineray, J. Dargaud, E. Quémerais and F. Vuillot, "CEDRE Software," *Aerospacelab,* 2011.

[34] M. Moratilla-Vega, H. X. M. Angelino and G. Page, "An open-source coupled method for aeroacoustics modelling," *Computer Physics Communications,* vol. 278, 2022.

[35] E. Quémerais, "Coupling With Interpolation Parallel Interface," 2023.

[36] J. P. T. Nancz G. Leveson, STPA Handbook, 2018.

[37] "Unifier19," [Online]. Available: https://www.unifier19.eu/www.unifier19.eu/index.html.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.

[38] M. Knott, "Redefining Creep: A Comprehensive Analysis of Aviation Accident Survivability," Embry-Riddle Aeronautical University, Daytona Beach, Florida, USA, 2020.

[39] D. F. Shanahan, "Human Tolerance and Crash Survivability," in *North Atlantic Treaty Organization (NATO), Research and Technology Organization (RTO) Lecture Series,*, Madrid, Spain, 2004.

[40] D. L. Greer, J. S. Breeden, and T. L. Heid, "CRASHWORTHY DESIGN PRINCIPLES," General Dynamics/Convair, San Diego, CA, 1964.

[41] J. J. Lee, "The naval flight surgeon's pocket reference to aircraft mishap investigation," Norforlk, VA.

[42] Waimer, M., Schatrow, P., Wegener, E., "Crashworthiness aspects for LH2 tank integration in transport airplanes," in *Aerospace Structural Impact Dynamics International Conference 2025*, Seville, 2025.

[43] NASA, "OpenVSP," [Online]. Available: https://openvsp.org/.

[44] Choi, J. et al., "Initial concept and procedures forsharing of information on safety, crises and emergencies," 2024.

[45] Simula, Inc.; Command, U.S. Army Aviation Systems, "AIcraft Crash Survival Design Guide. Volume III: Aircraft Structural Crash Resistance," St. Louis, MO, 1989.

[46] Simula, Inc.; Command, U.S. Army Aviation Systems, "Aircraft crash survival design guide. Volume I: Design criteria and checklists," St. Louis, MO, 1989.

[47] Simula, Inc.; Command, U.S. Army Aviation Systems, "AIcraft Crash Survival Design Guide. Volume V: Aircraft Postcrash Survival," St. Louis, MO, 1980.

This document is the property of ALBATROS and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
ALBATROS has received funding from the Horizon Europe Research and Innovation Programme, under Grant Agreement No. 101077071.