Co-funded by the European Union

ALBATROS

Applying STPA to Hybrid Hydrogen-Electric Aircraft: Critical Parameter Identification for System Health Monitoring

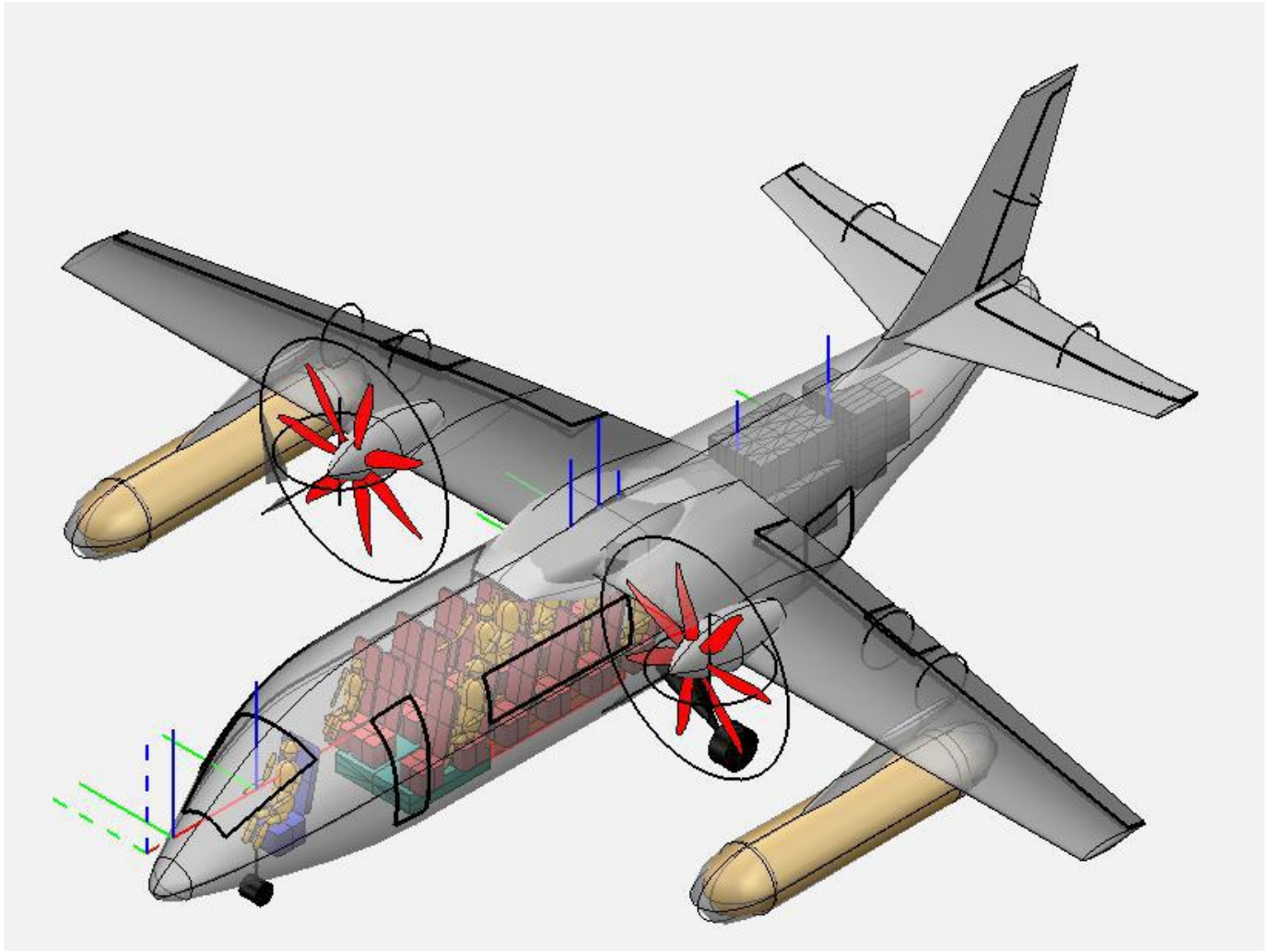
Pipistrel Vertical Solutions

Presenter: Nina Pavlovska

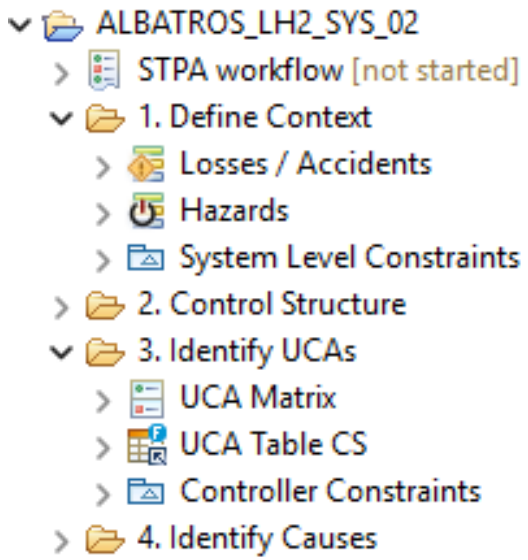


Reference Architecture: UNIFIER19 Aircraft Concept

- Hybrid hydrogen electric aircraft
- 29 passengers zero emmision air mobility
- Abstracted powertrain system:
  - Fuel Cell
  - High Voltage Batteries
  - Power Management
  - Electrical Propulsion Systems



STPA Execution



Task/Requirement	Checked	Related Artifacts	Checked By	Date of Check	Note
Define the Purpose of the Analysis	☐				
Identify Losses	☐	Losses / Accidents			Define Losses
Identify System-Level Hazards	☐	Hazards			Define Hazards and connect them to the Losses
Identify System Level Constraints	☐	System Level Constraints			Define SLC and connect them to the Hazards
Model the Control Structure	☐				
Identify Control Elements	☐				Define Controllers and Controlled Elements
Identify Control actions	☐				Define Control Connections and Control Actions
Identify Feedback	☐				Define Feedback Connections and Feedback

Defining the Purpose of the Analysis

Scope:

Powertrain monitoring and control during enroute flight phase.

Goal:

Identify critical parameters for operational health monitoring.

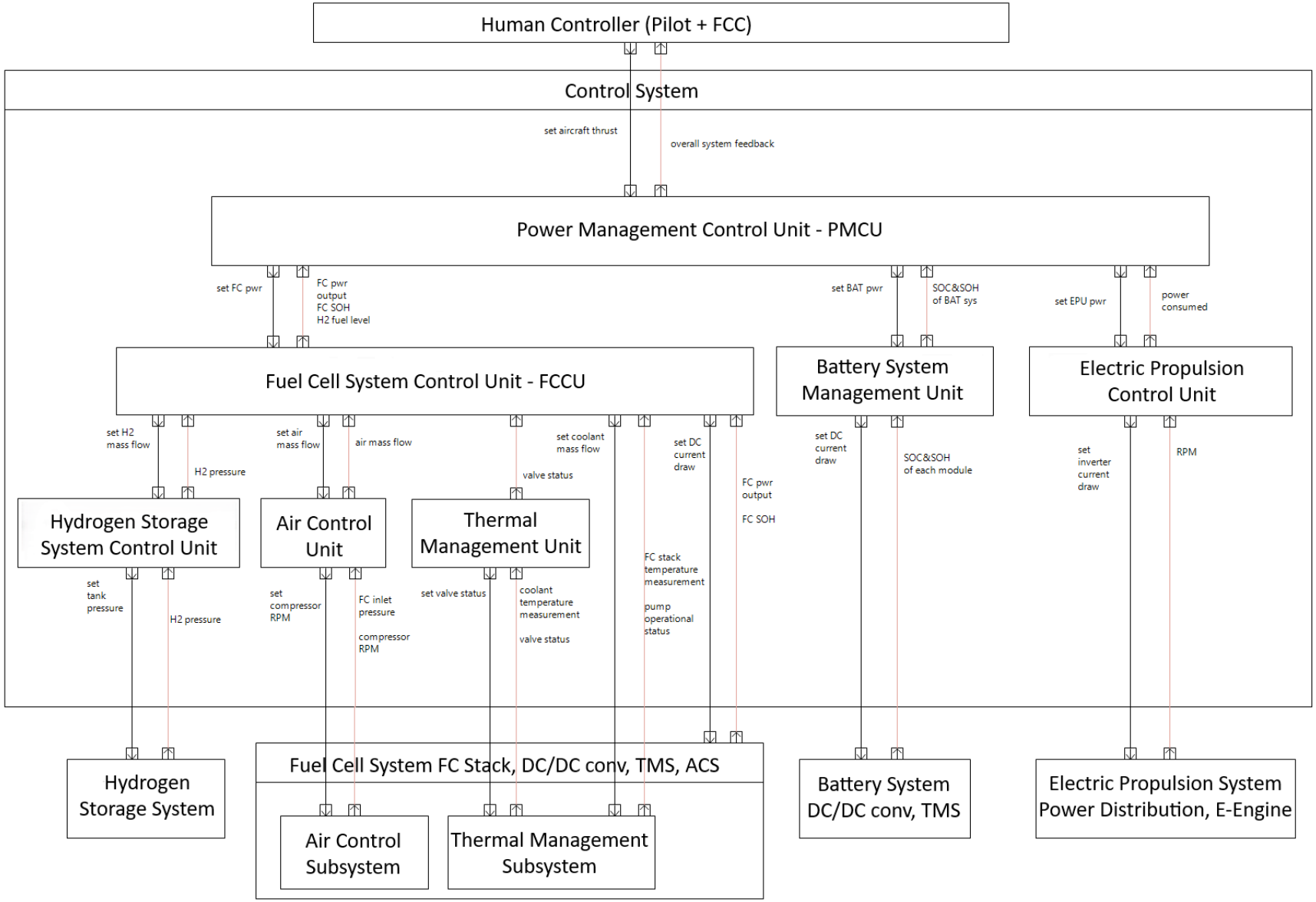
Losses to Stakeholder

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

Defining the Purpose of the Analysis

System Hazards	System Constraints
H-[1] Aircraft doesn't have enough power for flight L-[2], L-[3]	SC-[1] Power must be provided
H-[2] Incorrect electrical power distribution L-[2], L-[3]	SC-[2] Power must be distributed accordingly
H-[3] Decreased engine handling on aircraft L-[2], L-[3]	SC-[3] Engine control must not decrease over a [TBD] threshold
H-[4] Violation of structural integrity of aircraft subsystems L-[1], L-[2], L-[3]	SC-[4] Structural integrity of aircraft must be maintained

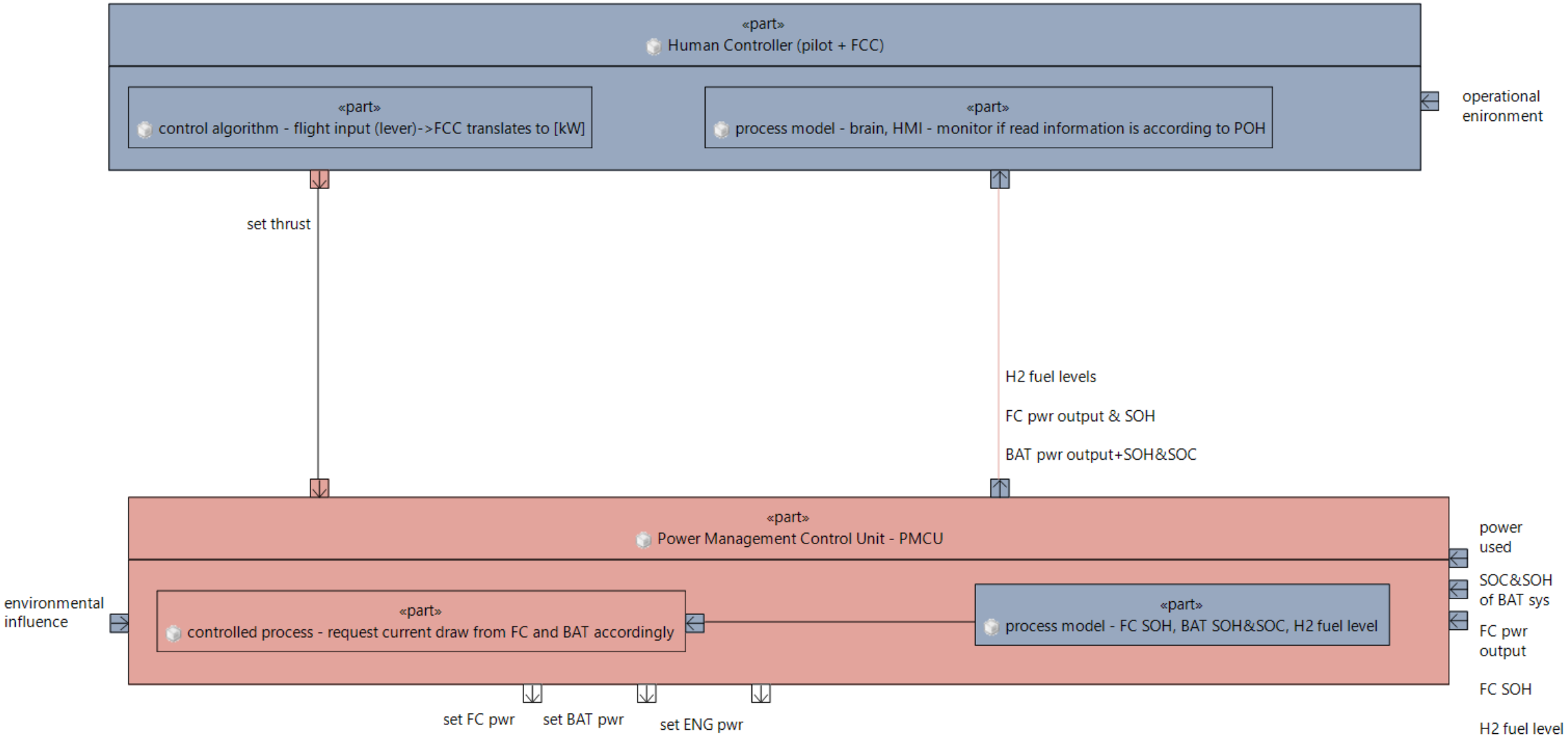
Modeling the Control Structure



Examples of Identified UCA and CC

Control Action	Unsafe Control Action	Hazard	Classification	Controller Constraints
HC -> PMCU				
[CA.1] set aircraft thrust	[UCA.1.1] Human controller doesn't 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 trust 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
PMCU -> FCCU				
[CA.2] set FC power	[UCA.2.1] PMCU doesn't 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
FCCU -> ACU				
ACU -> FCS				
FCCU -> FCS				
FCCU -> HCU				
HCU -> H2S				
[CA.7] set tank pressure	[UCA.7.1] HCU doesn't set tank pressure to match the required H2 flow during the opertion 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 operatioin 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

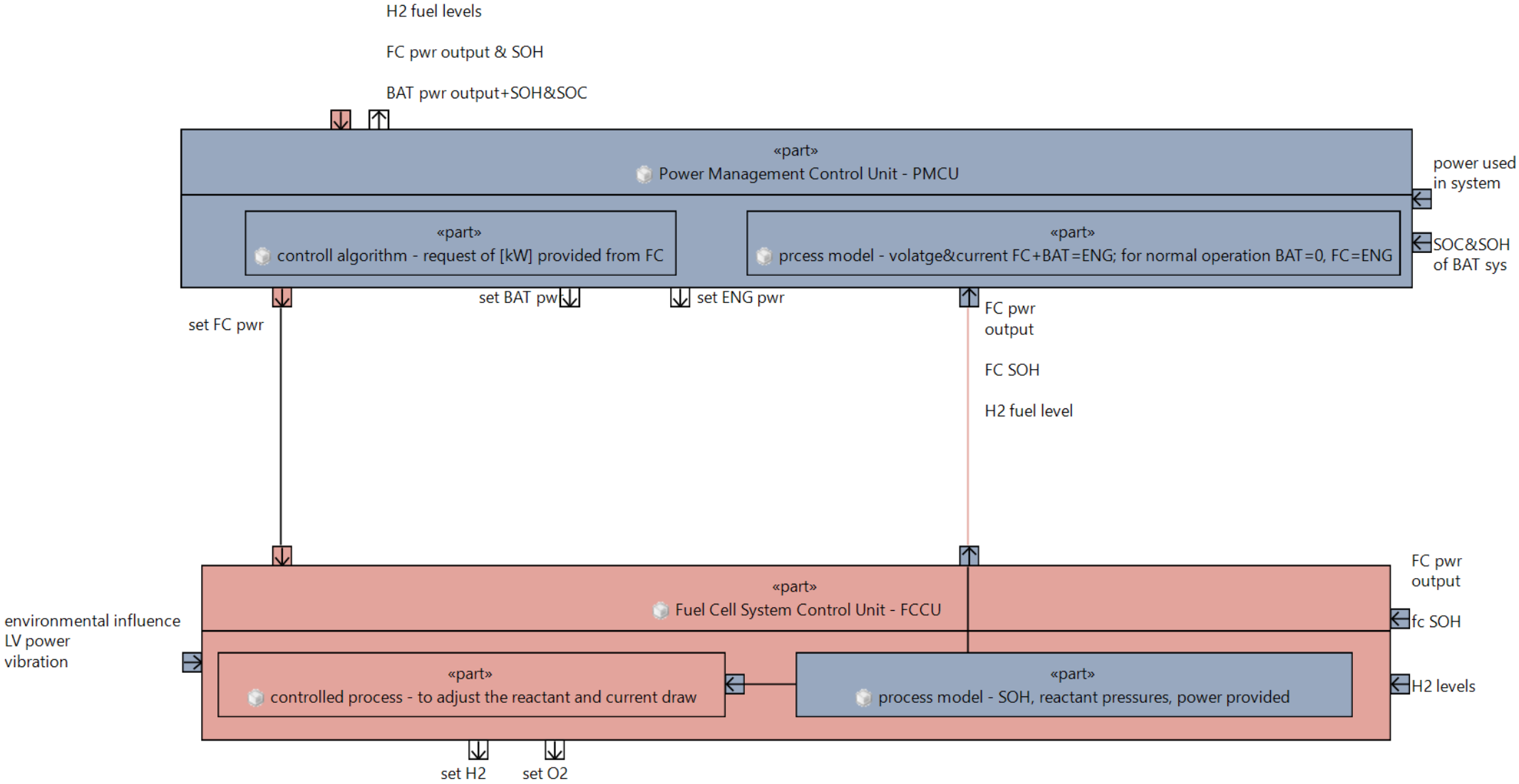
Example Control Loop CA.1



Example Causal Scenarios for UCA 1.1

- UCA1.1 Human controller doesn't set required trust to maintain flight during the mission
- Human interaction and operational factors
  - Set thrust is in response to aircraft conditions or ATC instructions.
  - Misinterpreted aircraft status due to incorrect or missing information on the flight display.
  - Received outdated or incomplete system information
- Controller and SW issues
  - FCC Incorrect translation of thrust commands into power request
  - PMCU incorrectly perceives aircraft state
  - Delayed feedback, processing overload
- Communication and Equipment failures
- Consequences: Aircraft doesn’t have enough power for flight
- Mitigations: Redundant control inputs, communication monitoring, FCC/PMCU fault detection, fault-tolerant displays, and verification of commanded versus delivered thrust

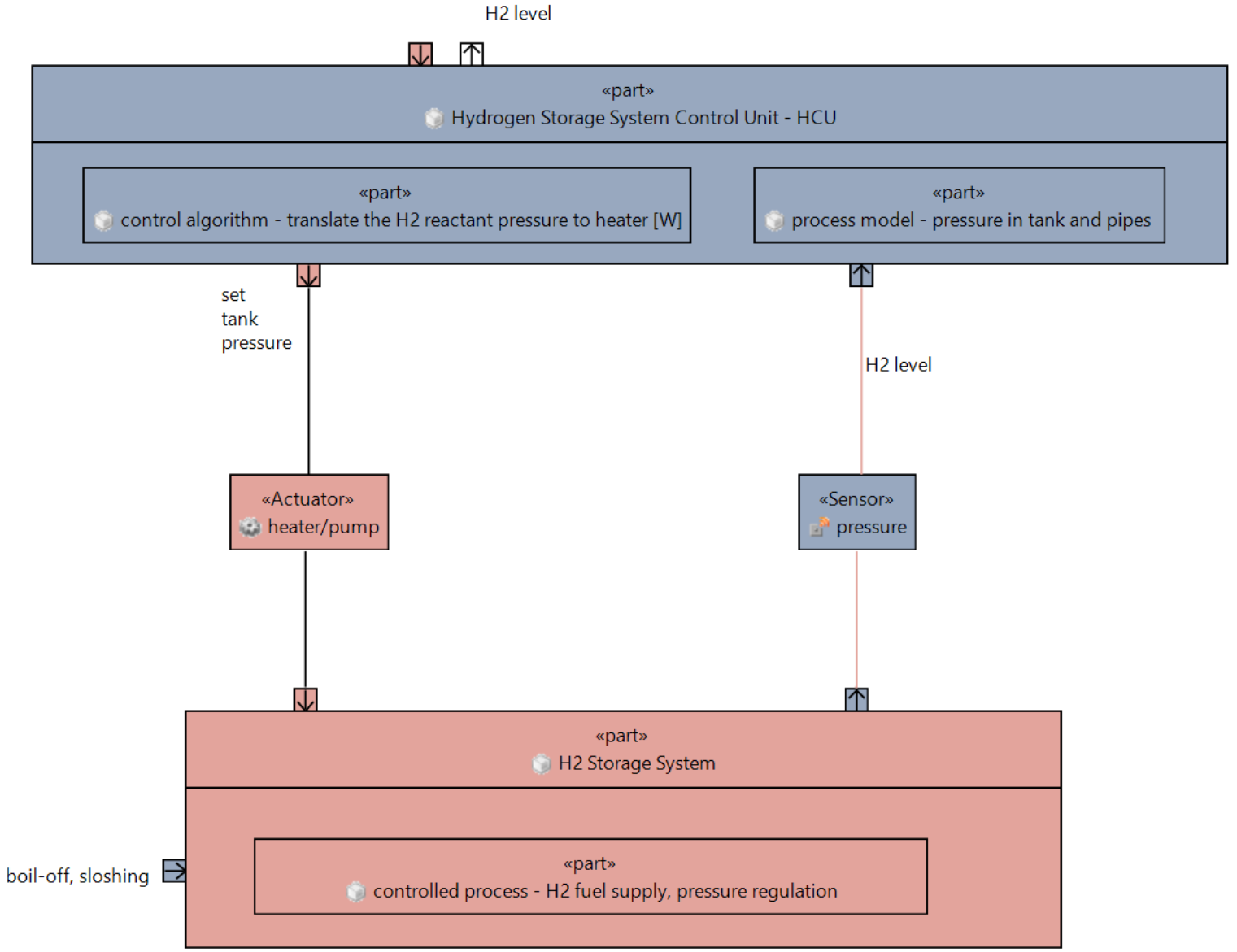
Example Control Loop CA.2



Example Causal Scenarios for UCA 2.1

- UCA 2.1 PMCU doesn't set required FC power to meet the engine consumption during the flight mission
- Controller and algorithm issues
  - Incorrect algorithm estimations and inaccurately processed system state
  - High voltage system information interference
- Communication and interface issues
- Feedback and system state awareness issues
- Consequences: Incorrect power distribution, insufficient power available for flight, and potential structural integrity concerns due to operation outside intended limits
- Mitigations: Algorithm validation, communication monitoring, controller fault detection, redundant communication paths, and real-time verification of power demand versus power delivery.

Example Control Loop CA.7



Example Causal Scenarios for UCA 7.2

- UCA 7.2 HCU sets tank pressure above limit for the required operation creating overpressure in the tank
- Incorrect calculation of the pressure required to support the requested power demand.
- Commanded excessive heating or pressure increase.
- Feedback and sensor issues
- Communication and interface failures
- Heater responds unexpectedly due to a fault or electrical disturbance.
- Tank pressure regulation system fails to respond to commands
- Consequences tank overpressure, hydrogen leakage, loss of propulsion power, and potential compromise of system integrity
- Mitigations: pressure sensors with voting logic, pressure limit monitoring, safety relief valves, fail-safe venting mechanisms, and independent verification of tank pressure.

Critical Parameters for Health Monitoring

Fuel Cells Stack	Hydrogen System	Air System	DC/DC Converter	Thermal Management
• Cathode and Anode differential pressure • Temperature	• H2 Mass Flow • Hydrogen Concentration • Tank Pressure • Temperature	• Air mass flow • Air Humidity & Temperature • Oxygen concentration	• System & Cell Voltage • Current Draw	• Coolant Temperature • Coolant Mass Flow • Pressure



Consortium

STICHTING KONINKLIJK NEDERLANDS LUCHT- EN RUIMTEVAARTCENTRUM (NLR)
DEUTSCHES ZENTRUM FUR LUFT - UND RAUMFAHRT EV (DLR)
OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES (ONERA)
CENTRO ITALIANO RICERCHE AEROSPAZIALI (CIRA)
ROTTERDAM AIRPORT BV (RABV)
SCHIPHOL NEDERLAND B.V. (SNBV)
ATHENS INTERNATIONAL AIRPORT S.A. (AIA)
AEROPORTOS DE PORTUGAL SA (ANA)
AIRBUS OPERATIONS SL (AI-ES)
AIRBUS OPERATIONS GMBH (AI-DE)
ECOLE NATIONALE SUPERIEURE DES OFFICIERS DE SAPEURS-POMPIERS (ENSOSP)
PIPISTREL VERTICAL SOLUTIONS DOO PODJETJE ZA NAPREDNE LETALSKE RESITVE (PVS)
FERRONATS AIR TRAFFIC SERVICES SA (FATS)
STICHTING BEHEER JAA TRAINING ORGANISATION (JAA)
ILMATIETEEN LAITOS (FMI)
OULUN YLIOPISTO (OULU)
SOMNI CORPORATION B.V. (SOMNI)
AEGEAN AIRLINES AE (AEGEAN)
AIRBUS PROTECT GMBH (ACS)
EUROPEAN UNION AVIATION SAFETY AGENCY (EASA)
FACHHOCHSCHULE NORDWESTSCHWEIZ (FHNW)
DEEP BLUE SRL (DBL)

ALBATROS has received funding from the European Union's Horizon Europe research and innovation programme, under Grant Agreement No 101077071.
Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or CINEA.
Neither the European Union nor CINEA can be held responsible for them.