Case Study: Application of FBSE approach in the development of a novel hydrogen fuel cell powered aircraft

Jean Machado
Chief Systems and Safety Engineer
Cranfield Aerospace Solutions Ltd

Agenda

- Introduction
  - Case Study – Project Fresson
  - Regulatory Context
- System Development Process
  - Function Allocation
  - Methodology
  - Results
- Conclusion
  - What are we learning?
  - Next Steps

Introduction

Case Study – Project Fresson

- Project FRESSON 1a WHITE is a technology demonstrator programme that will fly an existing Britten-Norman BN-2B Islander aircraft modified to incorporate a Fuel-Cell Propulsion System (FCPS) in the starboard wing, whilst retaining the reciprocating engine in the port wing.

- The FCPS consists of the Hydrogen Fuel Cell System (HFCS), the Electric Propulsion Unit (EPU), and Propellor System. The HFCS and EPU are mounted in a new nacelle, using the same wing attachment points as the original engines. A new constant-speed variable-pitch propeller and pitch control unit will be installed.

Fig. 1 – Fresson 1a White Aircraft Configuration

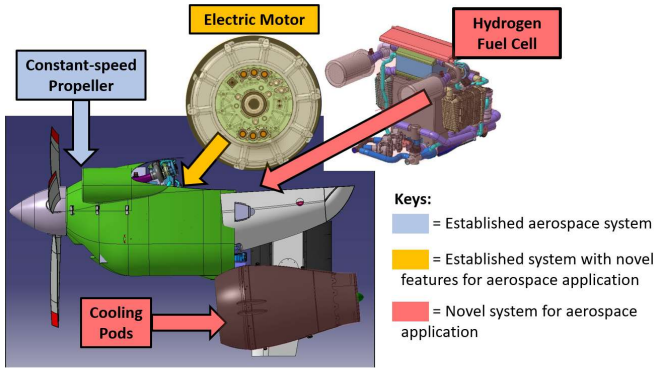

Fig. 2 – FCPS Concept

Introduction

Case Study

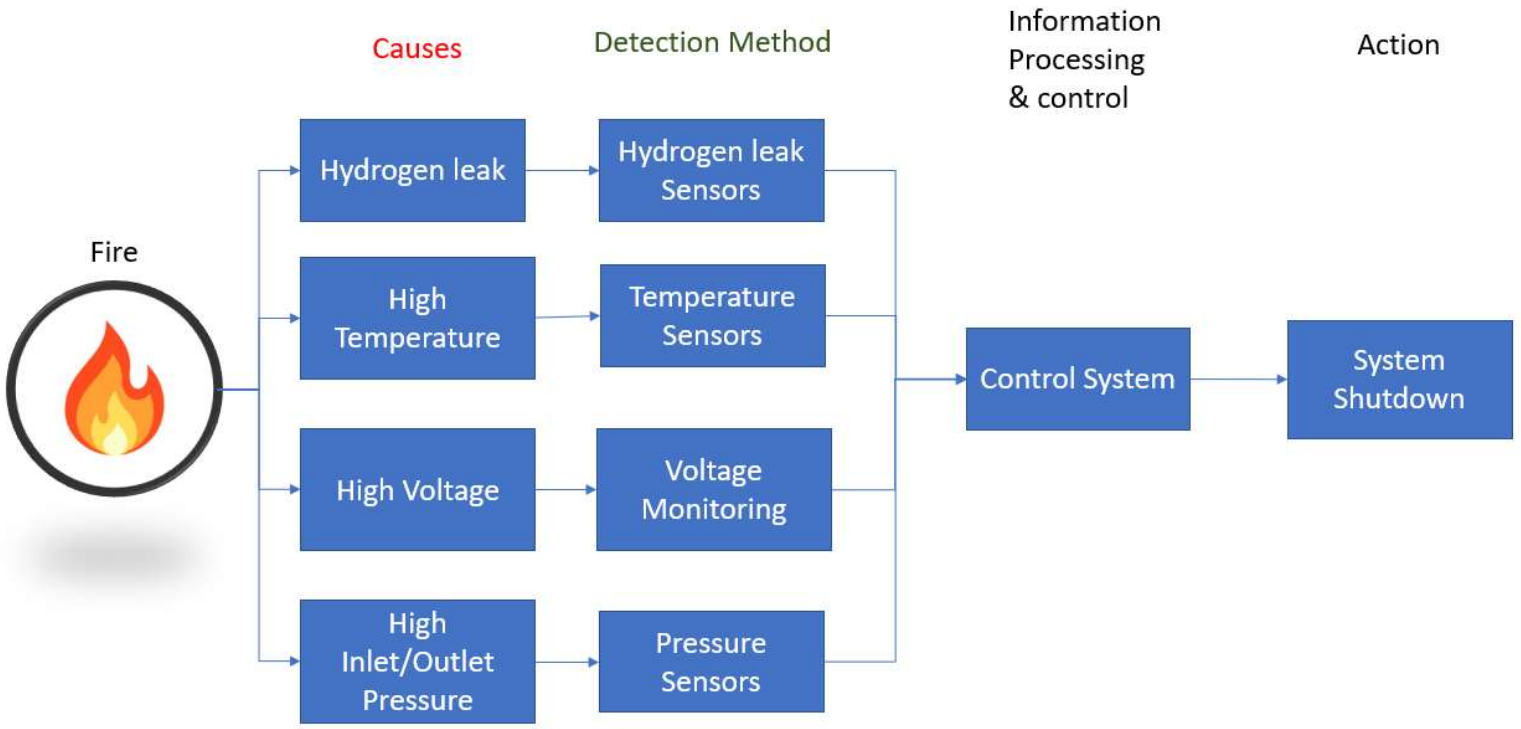

Figure 3 – Fire Hazard

Introduction

Regulatory Context

- **SC E-19, Issue 1 - Consultation paper on Electric / Hybrid Propulsion System**

  EHPS.350 EHPS Control System

  (b) Development Assurance

  Any software and Airborne Electronic Hardware, including programmable logic devices, must be designed and developed using a structured and methodical approach that provides a level of assurance, that is commensurate with the severity of the hazard associated with the failure or malfunction of the systems using this software or hardware, and is substantiated by a verification methodology acceptable to the Agency.

- **DAL (Development Assurance Level)**

  A Failure Condition can be caused by one or more Failures or Errors. Errors are mitigated by implementation of Development Assurance Process.

  The Development Assurance Level is the measure of rigor applied to the development process to limit, to a level acceptable for safety, the likelihood of Errors occurring during the development process of aircraft/system functions (FDAL) and items (IDAL) that have an adverse safety effect if they are exposed in service.

Introduction

Regulatory Context

- ARP4754 provides an accepted process for demonstrating regulatory compliance for highly integrated or complex systems.
- AC 23.1309E does not use Functional Development Assurance Levels (FDALs) and this adds complication when demonstrating compliance with the guidance of ARP 4754A.
- For the Fresson 1A White Demonstrator an interpretation of both ARP 4754A and AC 23.1309E has had to be made.

Classification of Failure condition	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Allowable Qualitative Probability	No Probability Requirement	Probable	Remote	Extremely Remote	Extremely Improbable
Class IV (Typically Commuter Category)	No Probability or SW and HW Development Assurance Levels Requirement	<1.0E-03 Note 1 P = D	<1.0E-05 Notes 1 and 4 P = C S = D	<1.0E-07 Note 4 P = B S = C	<1.0E-09 Note 3 P = A S = C
Class II (Typically MRE, STE, or MTE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	<1.0E-03 Note 1 P = D	<1.0E-05 Notes 1 and 4 P = C S = D	<1.0E-06 Note 4 P = C S = C	<1.0E-07 Note 3 P = C S = C

Note 1: Numerical values indicate an order of probability range and are provided here as a reference.

Note 2: The letters of the alphabet denote the typical SW and HW Development Assurance Levels for

Primary System (P) and
Secondary System (S).
For example, HW or SW Development Assurance Level A on Primary System is noted by P=A.

Note 3: At airplane function level, no single failure will result in a Catastrophic Failure Condition.

Note 4: Secondary System (S) may not be required to meet probability goals. If installed, S should meet stated criteria. (this implies that a single system implementing a Function may not be able to achieve the required Failure Condition through a single functional group).

Tab. 1 – AC 23.1309E, Class II Aeroplane Safety Objectives

Development Process

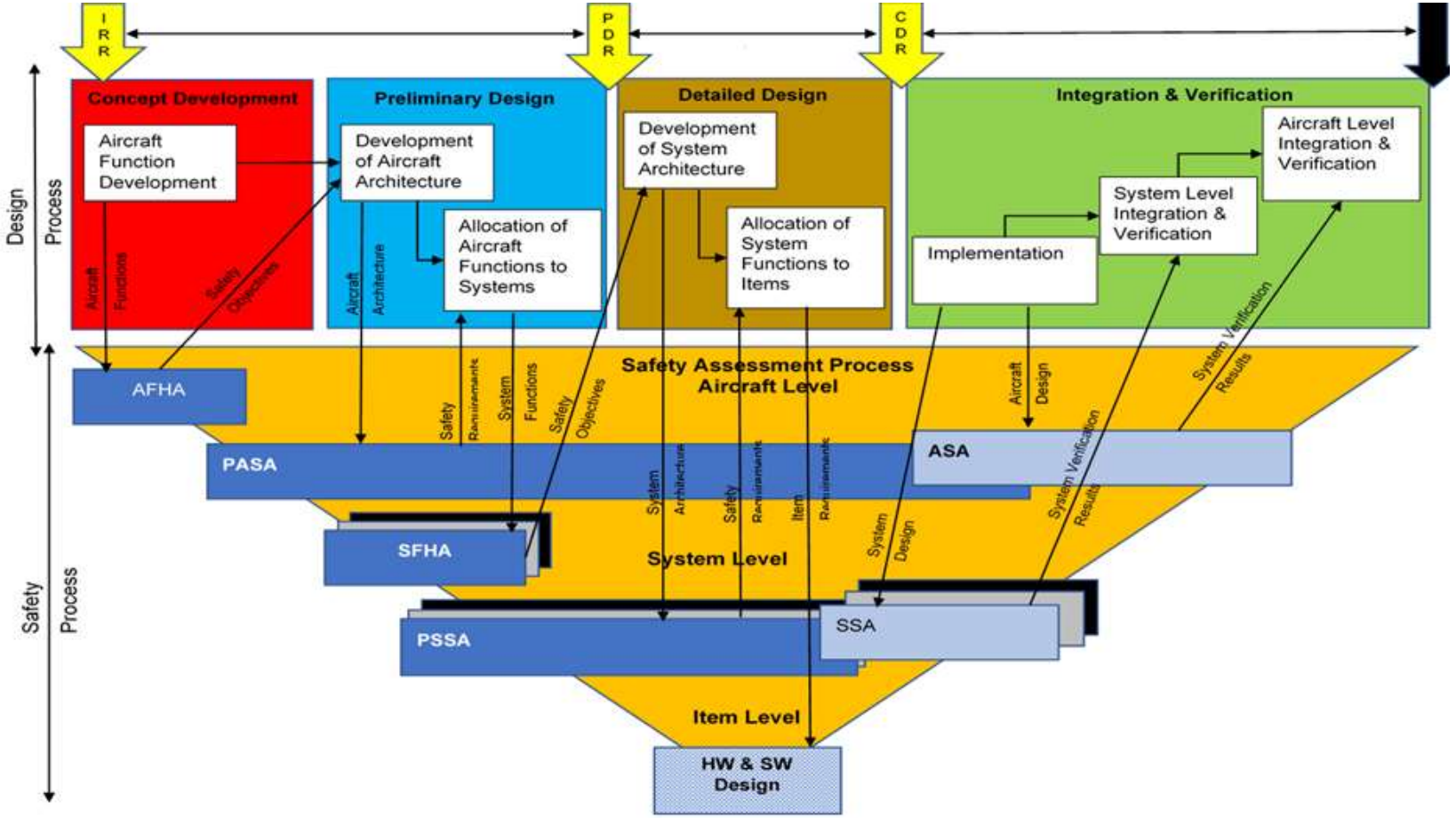

Fig. 4 - System Development Process

Function Allocation

It is important to notice that, although the process to perform the function allocation (select the list of aircraft/systems functions is essential to the development process) it is not described in the ARP4754 guidelines;

Therefore, it was applied system thinking to define a structured process to perform function allocation.

For this case study, it was selected the FBSE (Functions-Based System Engineering).

According to INCOSE (2015), “FBSE is an approach to Systems Engineering that focuses on the functional architecture of the system. The objective is to create a functional architecture for which system products and processes can be designed and to provide the foundation for defining the system architecture through the allocation of functions and sub-functions to hardware/software, databases, facilities and operations”.

Development Process

Methodology

- Identify system functions derived from Aircraft Level;
- Review system architecture to clarify system functions;
- Define the system boundaries and context to identify the internal and external interfaces;
- Decompose systems functions into sub-system / equipment functions;
- Allocate system functions to system requirements;
- Restart process considering alternative decompositions.

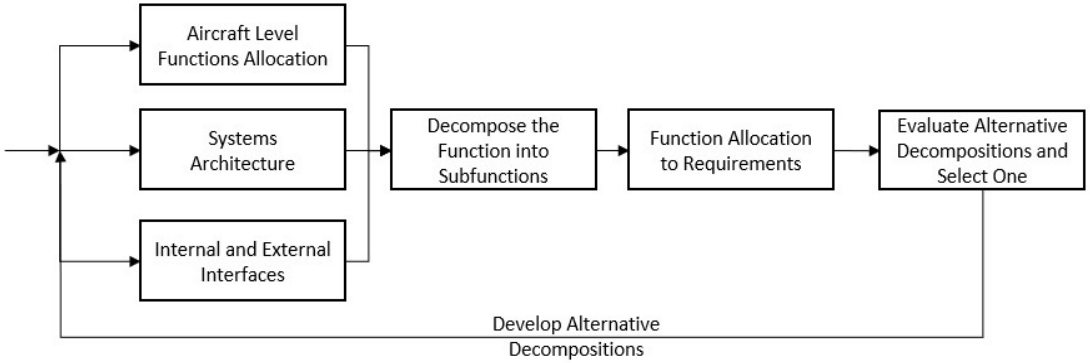

Fig. 5 - System Function Allocation Process

Results

First interaction identified that the first set of functions were not adequate to cover all requirements. Main issues:

- Number of functions without a requirements allocation, which indicates missing requirements or a function that is not needed;
- Number of requirements without a function, which could mean that it is missing a function or a requirement that it is not a user need.

Requirements	EPU	HFCS
First Iteration		
% allocated to functions	79%	45%
% not allocated to functions	10%	13%
Non-functional requirements	9%	10%
Unnecessary requirements	2%	32%
Second Iteration		
% allocated to functions	100%	100%

Tab. 2 – Results Summary

Conclusion

What are we learning?

System thinking and principles help to:

- Understand and manage the complexity and uncertainty of systems;
- Set guidelines to apply a structured process to design, develop, integrate, validate, verify and maintain the system;
- Ensure that the system meets the stakeholders needs and expectations, as well as the functional, operational and safety requirements.

Next Steps

- Airworthiness and Certification: Needs collaborative effort to define the certification requirements.
- Supplier Management: Need to establish process to help suppliers to comply with Aerospace standards.
- Improve Internal Process: It is necessary to create/develop new methods to address this new technology challenge.