Layer 0 - Specifications

November 9, 2021

Abstract

The European working group RESSAC was tasked with applying the Overarching Properties to a small prototype project that embodied hardware, software, and system considerations. This has helped to refine the criteria for the Overarching Properties, developed representative processes and activities compliant with the criteria, and is developing evidence for evaluation against the Overarching Properties and their criteria. The prototype defines a micro UAV, called µXAV. It is composed of 4 main sub-systems: the physical body, an Electrical propulsion system (EPS), a Hydraulic Braking System (HBS) and a Mission Management System (MMS). This allows deploying different Development Assurance Processes.

1 Introduction

In Europe, the avionics industry decided to support the FAA (Federal Aviation Administration) initiative on Development Assurance Process by setting up a research project named RESSAC (Re-Engineering the standards for Avionics Certification).

Further, they describe the specification of the Overarching Properties, their associated criteria, and the activities of the RESSAC project to demonstrate the use of the Overarching Properties.

2 The three overarching properties

The three "Overarching Properties" that must be present in any safety critical system independent of domain. These Overarching Properties are:

2.1 Intent

The defined intended behavior is correct and complete with respect to the desired behavior.

2.2 Correctness

The implementation is correct with respect to its defined intended behavior, under foreseeable operating conditions.

2.3 Acceptability

Any part of the implementation that is not required by the defined intended behavior has no unacceptable safety impact.

They have to be simultaneously satisfied at the end of the development process. The OP's are assumed to be applied at each development step of the development process, when identified input and output artefacts are available. They are the high level goals, the intent core of development assurance to be applied to this development step. The safety assessment process itself is out of scope of the Overarching Properties.

3 Layer 0 - Architectural Specification

The OPs do not refer to the architecture. The complete development of the µXAV systems includes several abstraction layers.

Layer 0 - Architectural Specification describes the physical and informational architecture that connects the three systems embedded in the air vehicle µXAV see Fig. 1.

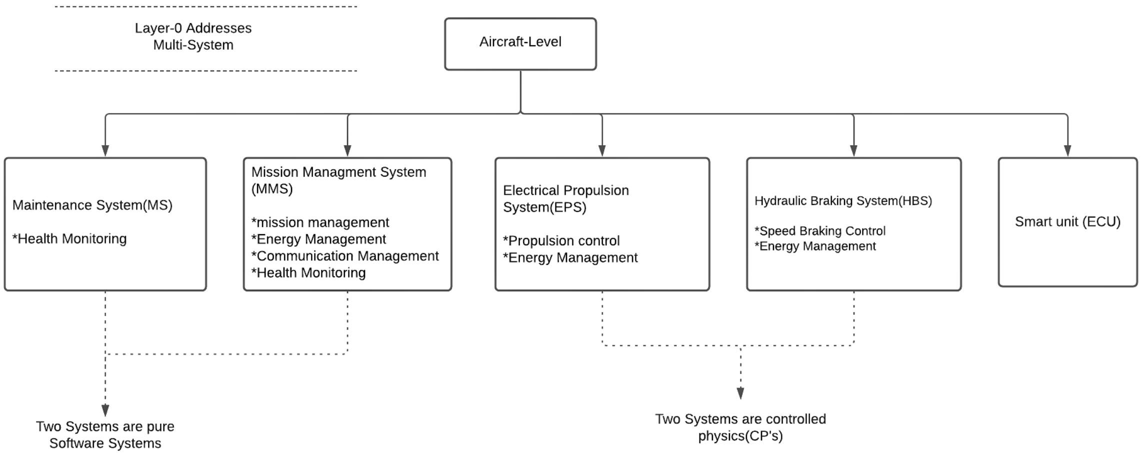
Layer-0 Addresses Multi-System
Aircraft-Level
Maintenance System(MS)
*Health Monitoring
Mission Managment System (MMS)
*mission management
*Energy Management
*Communication Management
*Health Monitoring
Electrical Propulsion System(EPS)
*Propulsion control
*Energy Management
Hydraulic Braking System(HBS)
*Speed Braking Control
*Energy Management
Smart unit (ECU)
Two Systems are pure Software Systems
Two Systems are controlled physics(CP's)

Figure 1: Systems embedded in uXAV

These are the input of the PASA (Preliminary Air-vehicle level Safety Assessment), mapping of functions to systems and for functional specifications.

3.1 Multi-system

Multi-system at aircraft-level is made of:

- Mission Management System (MMS): in charge of mission supervision.
- Electrical Propulsion System (EPS): powering propulsion, the computation resources and the switching resources of the drone.
- Hydraulic Braking System (HBS): is in charge of braking in flight emergency situations.

4 Layer 0 – Functional specifications

Layer 0 – Functional specifications describes the functions at air vehicle level. The layer0 functional specification supplements the layer0 operational specification. This is an input for the Mapping of functions to MMS (Mission Management System), EPS (Electrical Propulsion System), HBS (Hydraulic Breaking System), MS (Maintenance System) and (AFHA activity of the safety assessment process). Layer 1 - functional specifications refines the mapped layer0 functions.

4.1 Behaviour

Behaviour at air vehicle level is decomposed into three operational functions see Fig. 2.

- Payload Transport: It ensures the mission when the drone is operated in conditions compatible with mission completion.
- Emergency Landing: It takes over in any condition where mission completion is no longer possible, and has to be aborted.

- Health Monitoring: It operates in background on all digital resources. It provides the health status of the resources they depend on.

  The operational functions are supported by the functions:

- Communication: It ensures communication of the system with the external world: Ground Station (GS) and field operator. It also ensures communication between the systems, and within.
- Fault Tolerance: It ensures isolation and recovery in case of random or systematic failure. Failure detection is ensured by the operational functions.

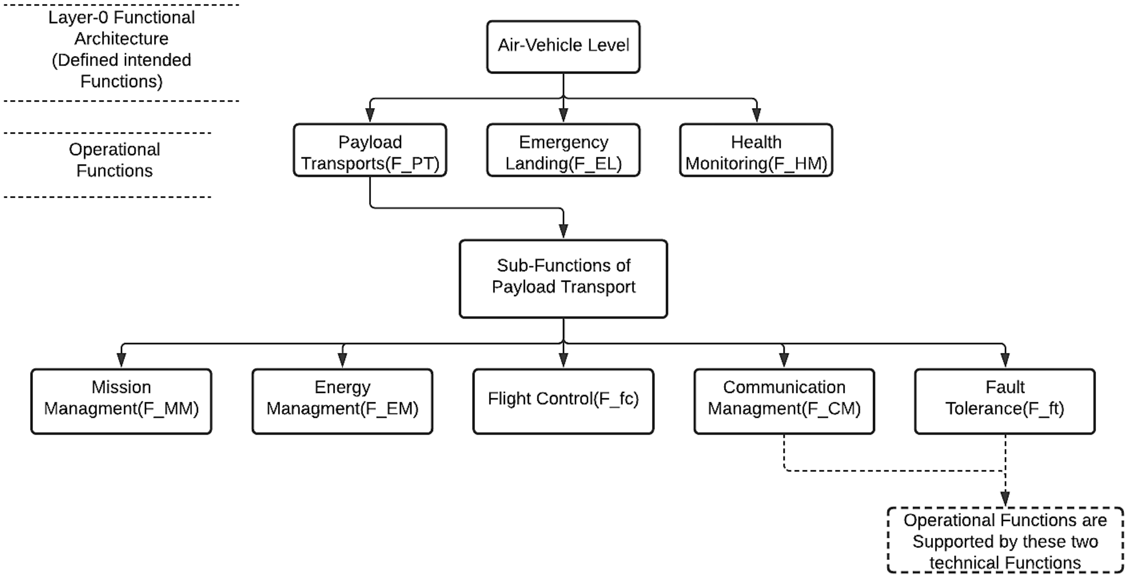

Figure 2: Defined Intended Function

5 Layer 0 – Operational specification

Layer 0 – Operational specification define a set of mission scenarios at air vehicle level. These scenarios are intended to contribute to the specification of layer 0 and layer 1 function to be used for multi-system level verification and validation.

µXAV is intended to perform 7/7-H24 autonomous or remotely controlled cargo transport missions. There are two ways of operating the drone: Without data link: "Autonomous" mode. With data link: "Remotely Piloted" mode. Operating procedures defines µXAV can be operated in autonomous mode without interactions with the ground station. Operational specification also defines the foreseeable operating conditions (i.e.: environmental conditions, human errors, failures and threats) and scenario specifications.

6 Safety-critical aspects

The RESSAC case study was designed to the safety-critical aspects. The initial activity of the safety assessment process is AFHA (Air Vehicle Level Functional Hazard Analysis).

6.1 Air Vehicle Level Functional Hazard Analysis(AFHA)

AFHA determines the hazards and failure conditions for each level 0 function, as well as their severity. As an input, AFHA requires a complete list of aircraft functionalities.

In the AFHA, failure conditions are specified broadly in order to provide a scope that includes all detailed failure possibilities that can result in the top level functional effect.

After all failure condition effects have been identified, the failure condition classification activity begins and then the severity classification is determined. It is used as input of the Preliminary Air-vehicle level Safety Assessment (PASA), and it is necessary to the development process and to the assurance process.

6.2 Preliminary Air-vehicle level Safety Assessment (PASA)

The PASA process identifies the interactions and dependencies between the aircraft systems, assesses how their failures can lead to the aircraft level failure conditions identified by the AFHA, and determines whether the AFHA objectives can be met and also identifies aircraft level safety requirements. If the PASA evaluation determines that the safety considerations are not achievable, feedback is delivered early in the development process to revise the aircraft architecture and operations see Fig. 3.

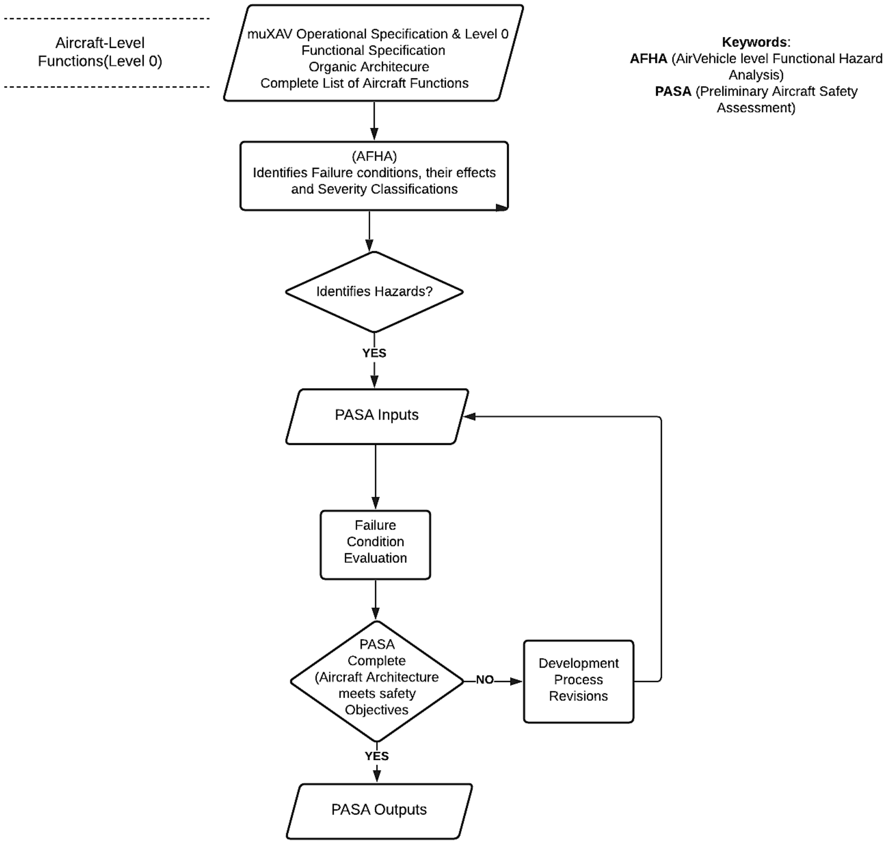
Aircraft-Level
Functions(Level 0)
muXAV Operational Specification & Level 0
Functional Specification
Organic Architecure
Complete List of Aircraft Functions
Keywords:
AFHA (AirVehicle level Functional Hazard Analysis)
PASA (Preliminary Aircraft Safety Assessment)
(AFHA)
Identifies Failure conditions, their effects and Severity Classifications
Identifies Hazards?
YES
PASA Inputs
Failure Condition Evaluation
PASA Complete (Aircraft Architecture meets safety Objectives
NO
Development Process Revisions
YES
PASA Outputs

Figure 3: Activity diagram of AFHA and PASA

The Aircraft-level failure conditions are evaluated to determine the contribution of the functional failures of the systems identified in the interdependence analysis which helped to meet the aircraft level safety requirements.

7 Reference

Ledinot. 2018. RESSAC Use Case - Layer0 UAV. https://github.com/AdaCore/RESSAC_Use_Case/tree/master/UseCaseData/Layer0_UAV. (2021).