Model-Based Dependability Analysis of Unmanned Aerial Vehicles - A Case Study

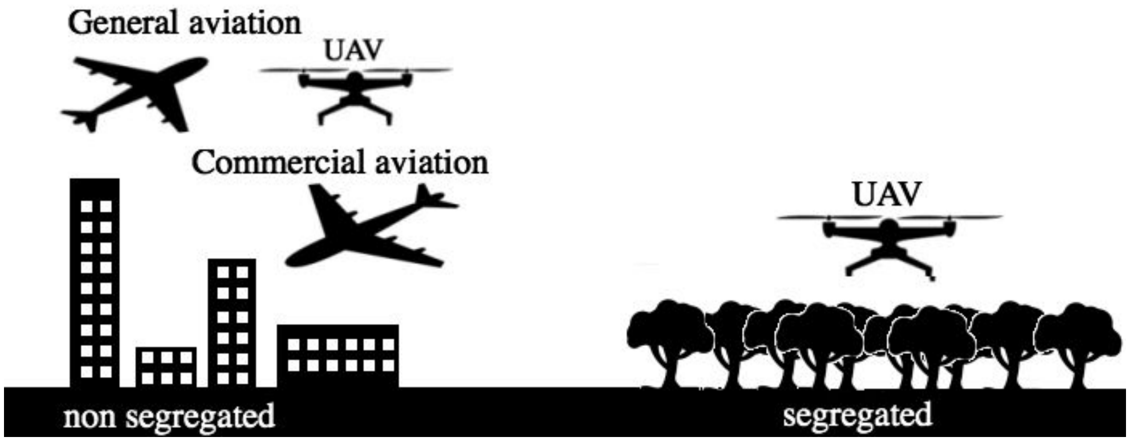
Matheus Franco*, Rosana Braga*, André L. de Oliveira**, **Catherine Dezan*****, Jean-Philippe Diguet***, Kalinka Branco*

*University of São Paulo (Brazil),
**Federal University of Juiz de Fora (Brazil),
***Lab-STICC (France)

June 25th, SSIV 2018

Introduction

- UAVs - demand the verification of dependability properties in different levels of abstraction in order to achieve certification and to be released for operation (in compliance with DO-178C and SAE ARP 4754A aerospace standards).



Introduction

- **Dependability analysis:** it is the identification, early on the design, of potential **threats** to system **reliability**, **availability**, **integrity** and **safety**;

- Variation in the **Usage Context** might raise:
  - Different **hazards** with different causes;
  - Different **risk** that the same hazard may pose for the overall safety;
  - Different **component faults** might occur and contribute to the occurrence of hazards, and;
  - Different **safety requirements** (functional and non-functional) may be allocated to eliminate or minimise the hazard effects.

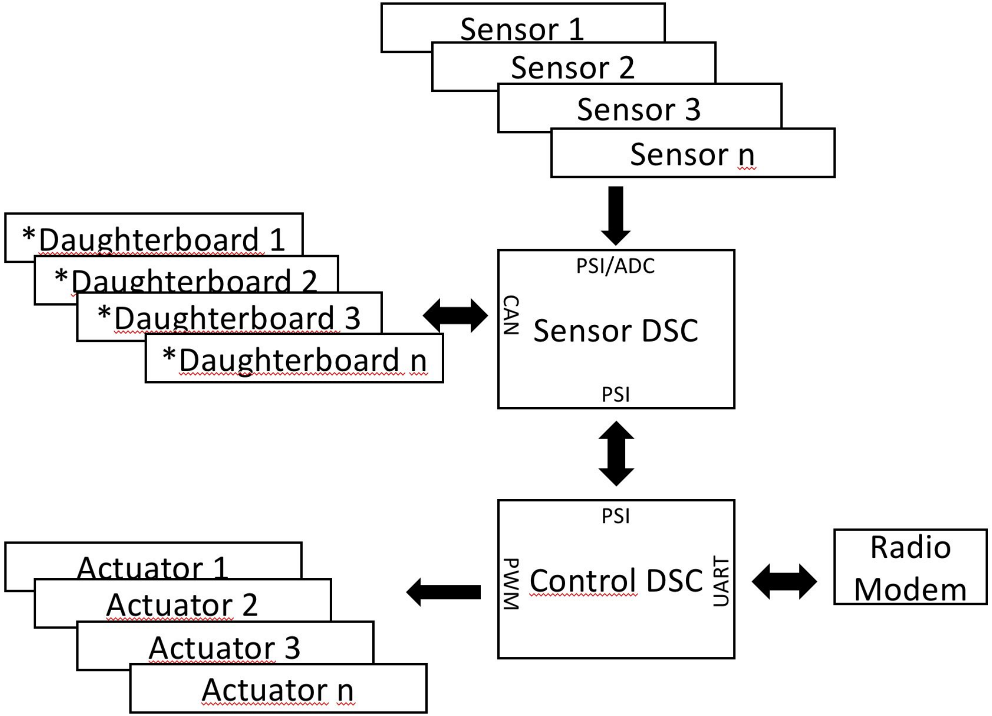
Introduction

- There is a lack of systematic guidance to support engineers in performing dependability analysis in the autonomous UAV domain;

- We provide a systematic and context-aware model-based approach to support dependability analysis and automated generation of artefacts required for safety-certification of UAVs.

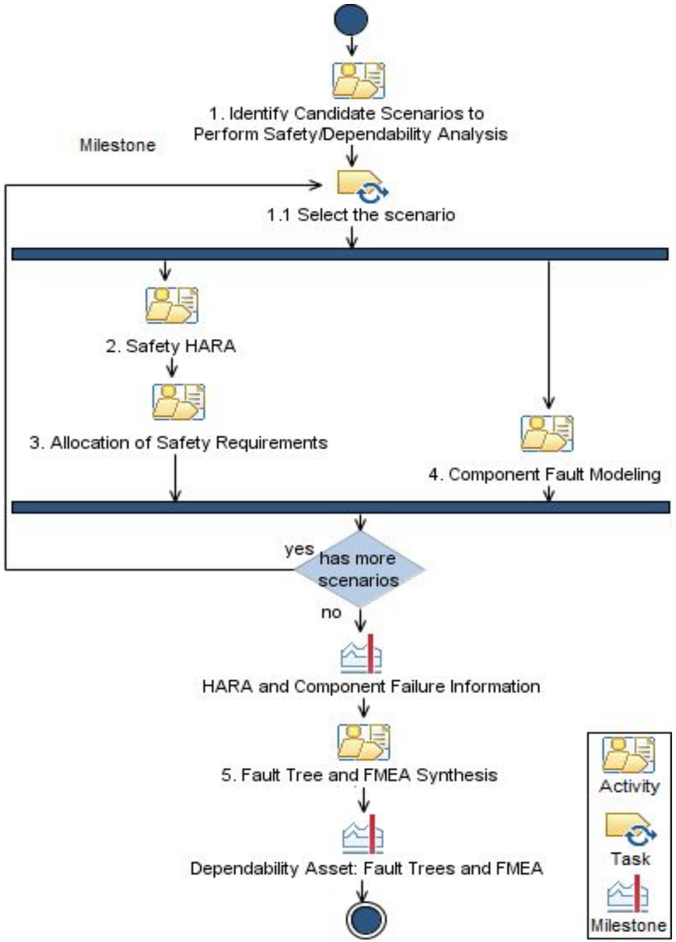
- This approach was applied in the SLUGS autopilot with the support of HiP-HOPS tool.

SLUGS Autopilot



* Optional

- Santa Cruz Low-Cost UAV GNC Subsystem (SLUGS);
- Open source;
- Open hardware;
- Developed in MATLAB/Simulink

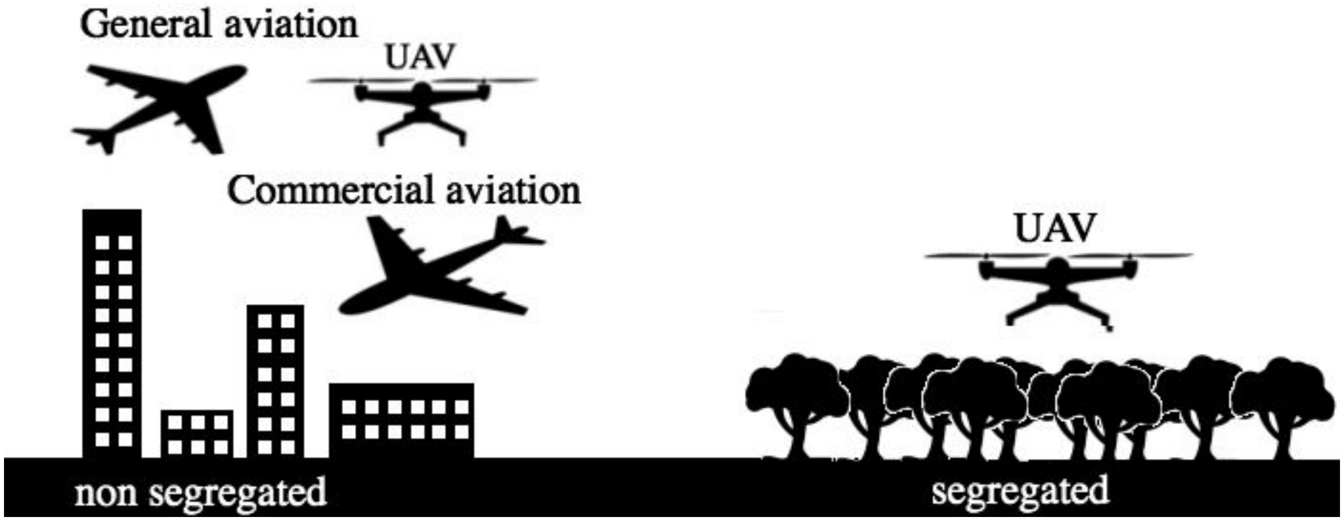


DePendable- ASE

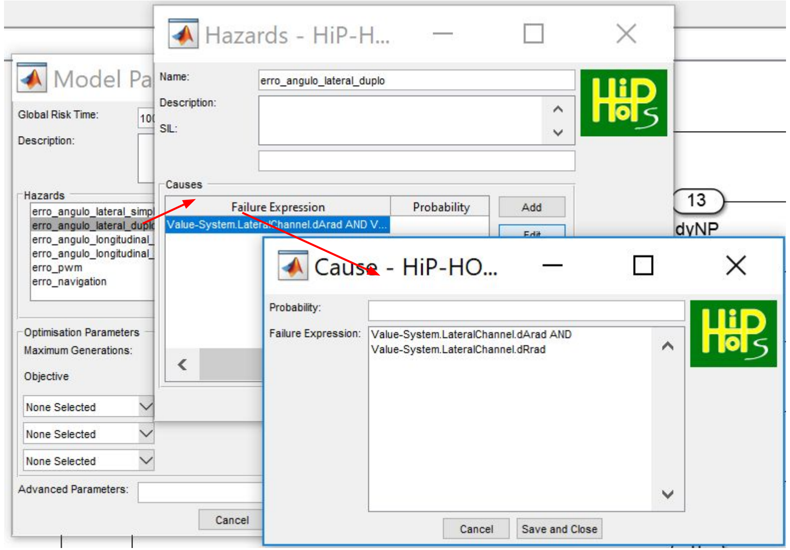
- Analysis of interactions among **design choices** and **usage contexts**;
- Scoping the autonomous system **dependability analysis** to a set of targeted **scenarios;**
- Allocation of **Safety Requirements;**
- Component **Fault Modeling**

Identify Candidate Scenarios

- Controlled and Uncontrolled airspaces



HARA



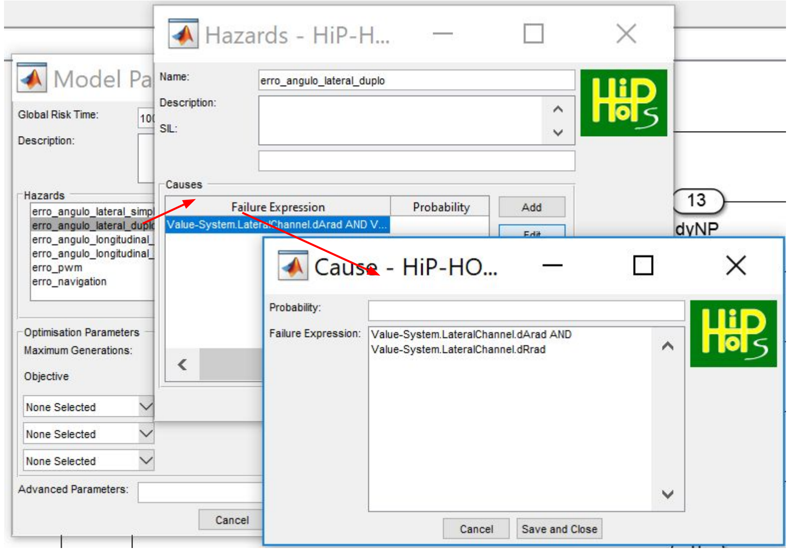
Inputs:

- The selected usage scenario.

Purpose:

- After choosing a scenario, HARA can be performed. Combinations among component failures leading to system-level failures (hazards) are identified;
- Hazards can be specified via logical expressions involving potential safety-related failures in system architectural components.

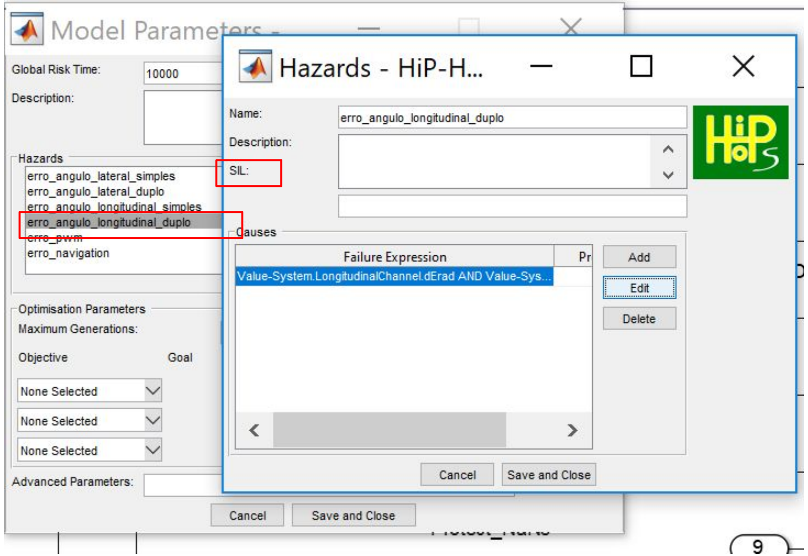
HARA



Output:

- A list of context-specific hazards and the classification of the risk that they pose for the overall safety.

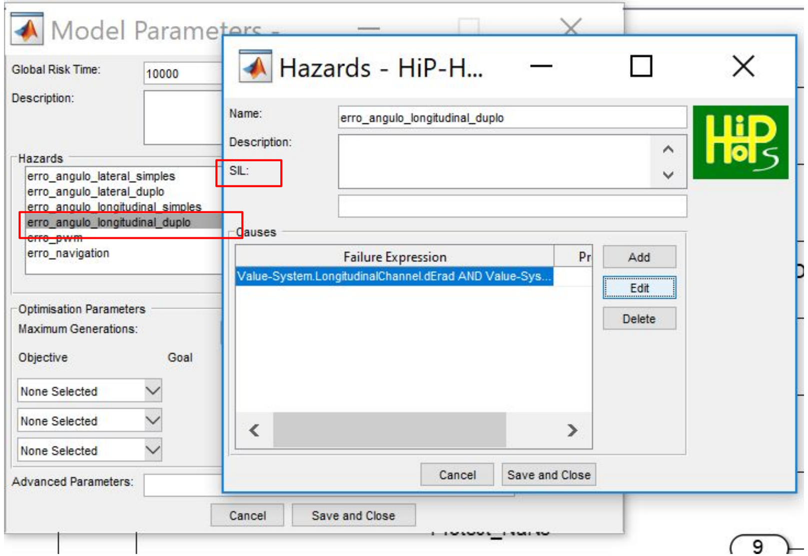
Allocation of Safety Requirements



Inputs : HARA results

- From the analysis of the HARA results, **functional safety requirements** and **Safety Integrity Levels** (SILs) are allocated aimed at eliminating or minimising the hazard effects on the overall safety.

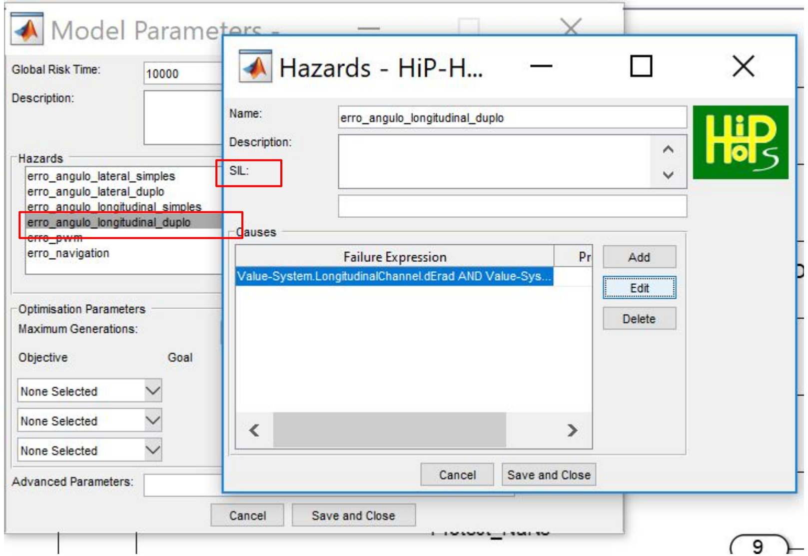
Allocation of Safety Requirements



Purpose:

- Safety Integrity Levels (SILs) are allocated to each identified hazard according to their risk classification defined during HARA;
- SILs allocated to system hazards can be further decomposed throughout contributing component failures and components.
- Allocation of functional safety requirements: aims at identifying system functions that can eliminate/minimising the impact of a hazard or a component failure in the overall safety.

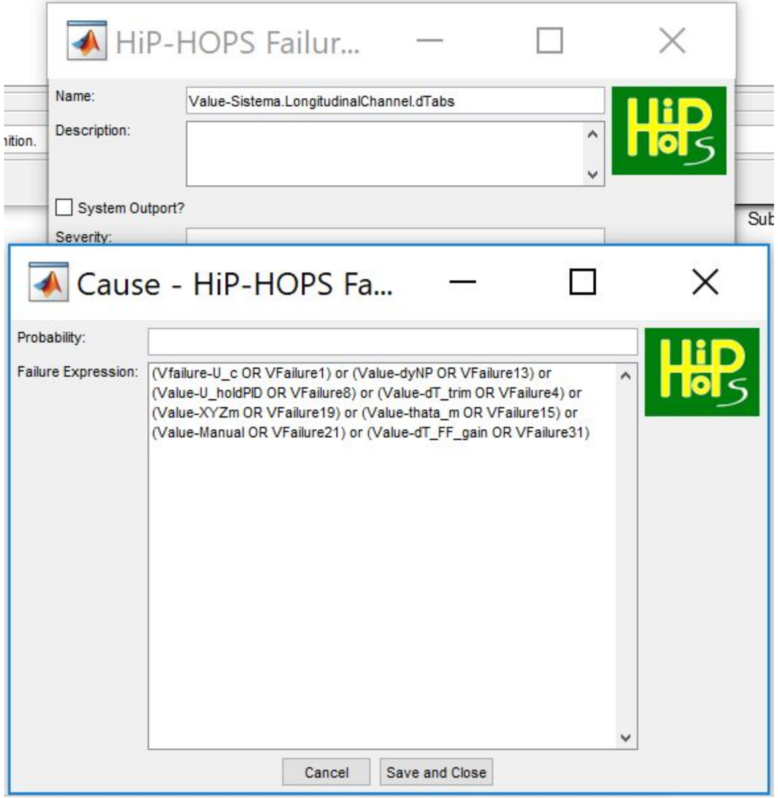
Allocation of System Safety Requirements



Output:

- A set of context-specific **functional safety requirements** and **SILs** to be allocated the mitigate the hazard effects on the overall safety.

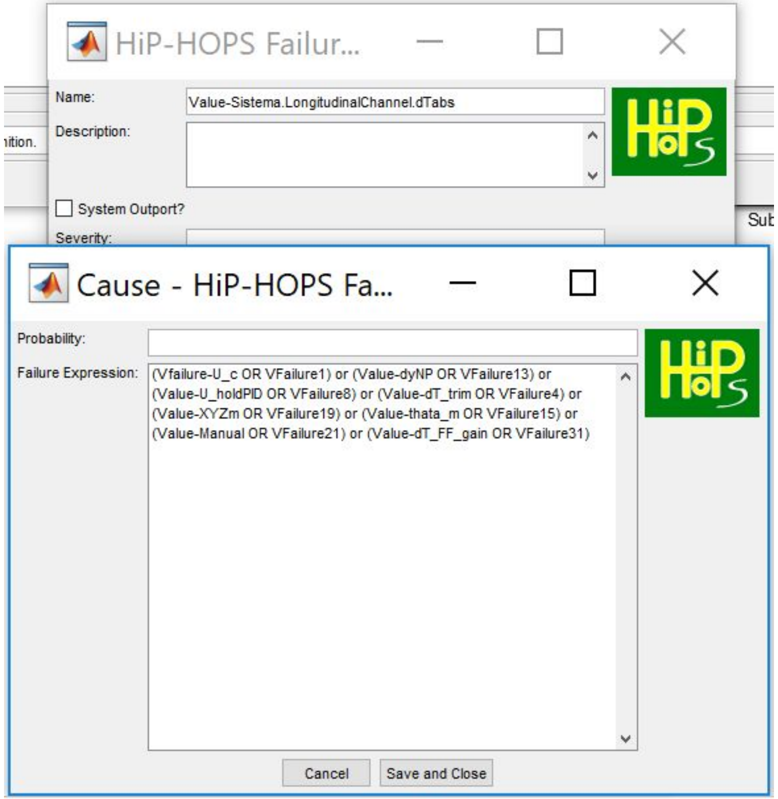
Component Fault Modeling



Inputs:

- HARA results;
- The system architecture model; and
- The targeted scenario.

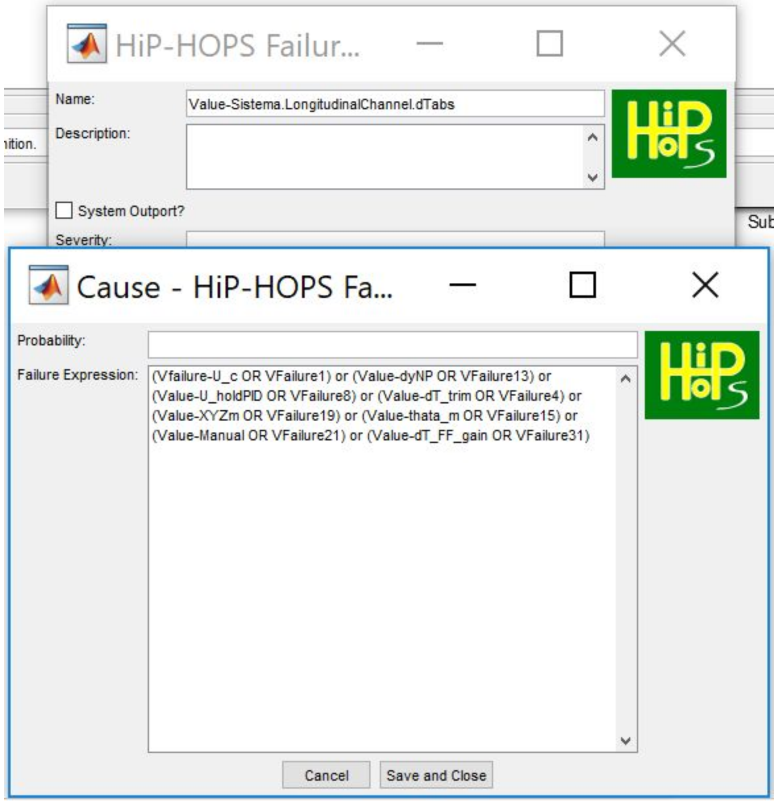
Component Fault Modeling



Purpose:

- From the analysis of the potential hazards that can be raised in a particular scenario, assumptions about how architectural components can fail and contribute to each identified hazard can be made;
- The failure behaviour associated with each component is specified by: stating what can go wrong with the component, and how it responds to failures elsewhere in the architecture.

Component Fault Modeling



Outputs:

- At the end, a set of component failure data showing how components can contribute to the occurrence of hazards in each scenario is delivered.

- The system architecture model is enhanced with dependability information

Fault Trees and FMEA Synthesis

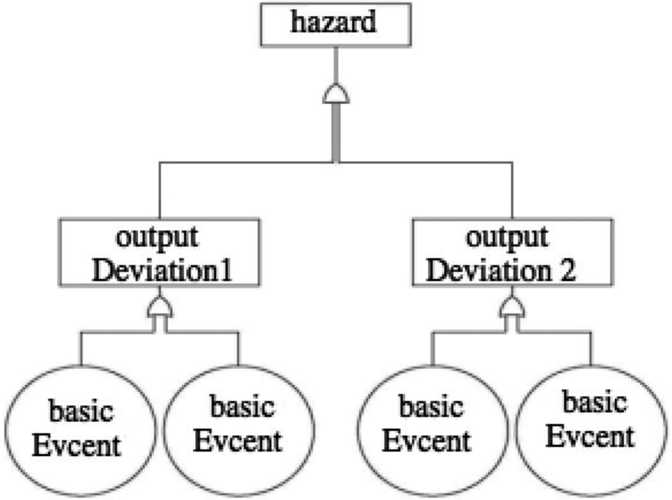
Inputs:

- The system architecture model enhanced with specific dependability information.

Purpose:

- Generating FTA and FMEA artefacts, which are evidence required by safety standards, e.g., ARP 4754A, from a system model enhanced with dependability information;
- In this step the system architecture model enhanced with dependability information are input to compositional analysis techniques, e.g. HiP-HOPS, to automatically generating fault trees and FMEA dependability artefacts.

Fault Trees and FMEA Synthesis

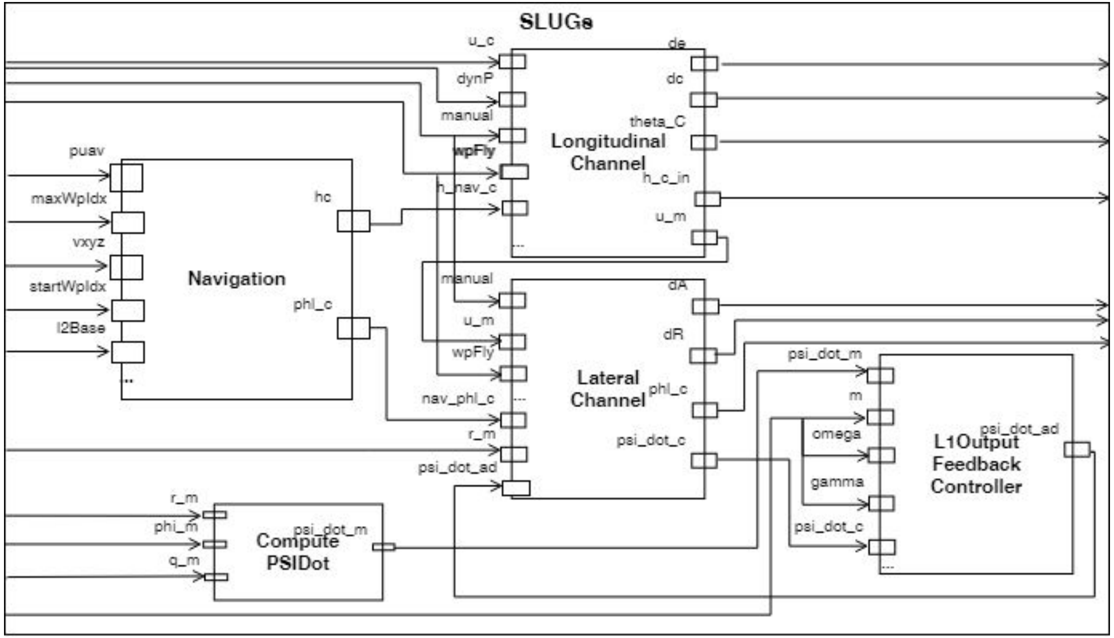


Outputs:

- FTAs and FMEA results used to demonstrate that the system architecture addresses the safety requirements.
- FTA illustrates how system-level failures (hazards) propagate throughout the system architecture;
- FMEA illustrates how each component contributes directly/indirectly to system failures.

A Study Case

SLUGS DEPENDABILITY ANALYSIS



SLUGS autopilot mainly comprises the following five subsystems : Navigation

- Longitudinal Channel ;
- Lateral Channel;
- ComputePSIDotL1OutputFeedbackController;
- Navigation;
- ComputePSIDot

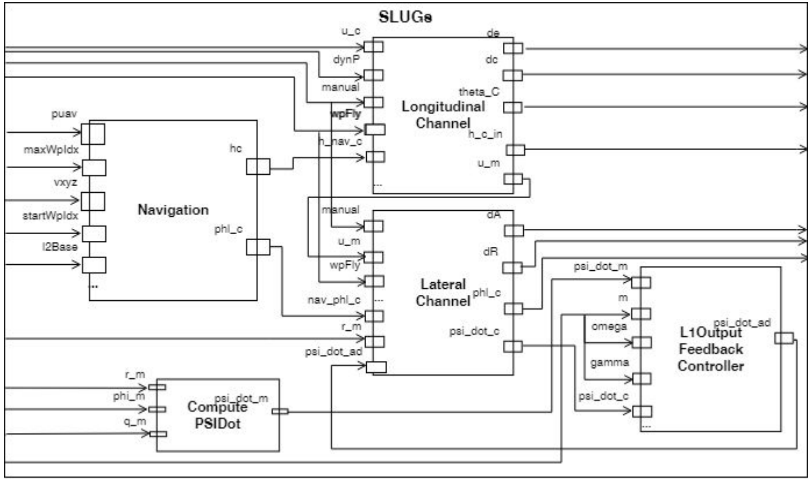
The application of DEPendable-ASE approach steps to SLUGS autopilot is detailed in the following.

Scenarios for SLUGS Safety/Dependability Analysis

The following scenarios were considered in performing SLUGS autopilot HARA and component fault modelling:

- SLUGS operating in a controlled airspace usage context (SLUGS/Controlled), and SLUGS operating in an uncontrolled airspace (SLUGS/Uncontrolled)

Hazard Analysis and Risk Assessment



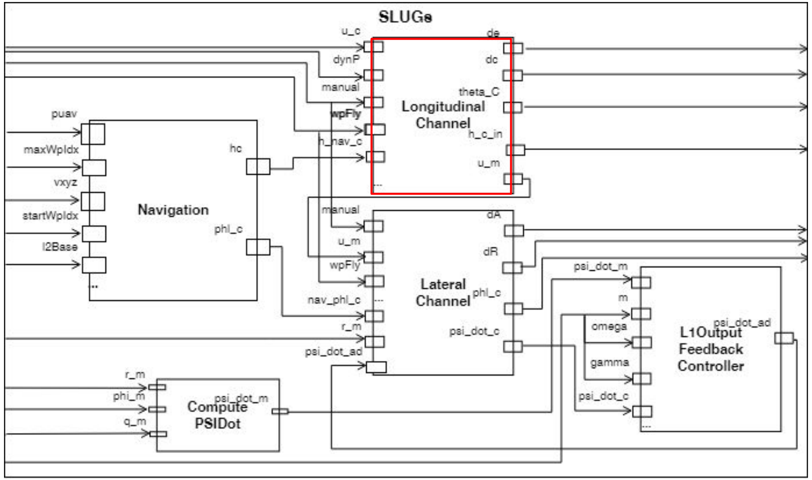
Value double longitudinal angle:

- Occur due the incorrect value of both dE and dC outputs from Longitudinal Channel component.

Value lateral channel:

- Occur due to incorrect value of dA and dR outputs from Lateral Channel component.

Hazard Analysis and Risk Assessment



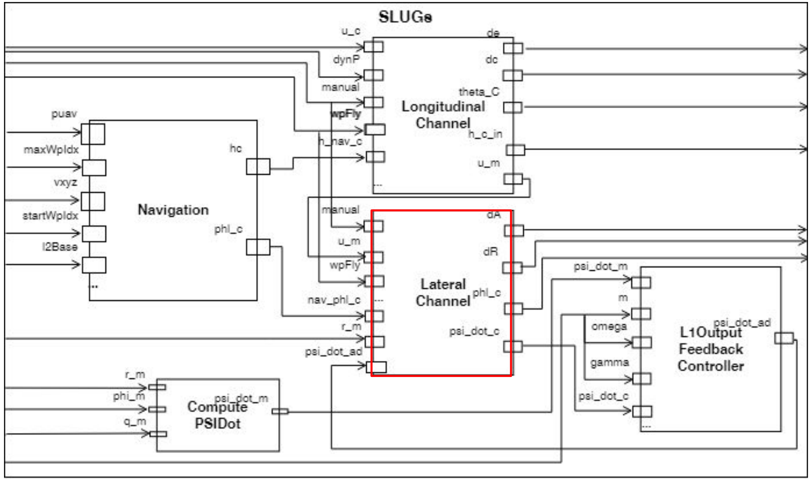
Value double longitudinal angle:

- Occur due the incorrect value of both dE and dC outputs from Longitudinal Channel component.

Value lateral channel:

- Occur due to incorrect value of dA and dR outputs from Lateral Channel component.

Hazard Analysis and Risk Assessment



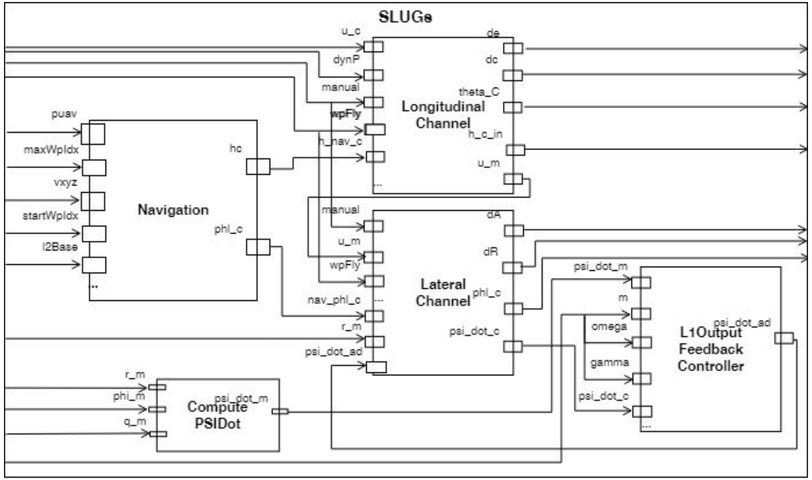
Value double longitudinal angle:

- Occur due the incorrect value of both dE and dC outputs from Longitudinal Channel component.

Value lateral channel:

- Occur due to incorrect value of dA and dR outputs from Lateral Channel component.

Hazard Analysis and Risk Assessment



Risk assessment depends on the usage context (controlled or uncontrolled)

=> higher severity level for the controlled airspace (less tolerant because of the more significant damages)

HARA and Allocation of Safety Requirements

Usage Ctx	Hazard	Hzd Causes	Severity	DAL
SC [3]	Value double longitudinal angle	Value-LongCh. dErad AND Value-LongCh.dTabs	Hzdous	B
SUC	Value double longitudinal angle	Value-LongCh. dErad AND Value-LongCh.dTabs	Major	C
SC	Value lateral channel	Value-LateralCh. dArad AND Value-LateralCh.dRad	Hzdous	B
SUC	Value lateral channel	Value-LateralCh. dArad AND Value-LateralCh.dRad	Hzdous	B
SC	Value PWM signals	Value-PWMGen .pwmSign OR Late-PWMGen. pwmSign	Hzdous	B
SUC	Value PWM signals	Value-PWMGen .pwmSign OR Late-PWMGen. pwmSign	Major	C

Level A is the highest stringent integrity, and level E is the less stringent. Addressing higher stringent DALs demand the most stringent safety objectives, system engineering activities, and software artefacts, increasing the development costs.

Value double longitudinal angle:

- Hazard has a hazardous (B) severity with probability of occurrence of 10e-9 per hour of operation in a controlled airspace context (SC).

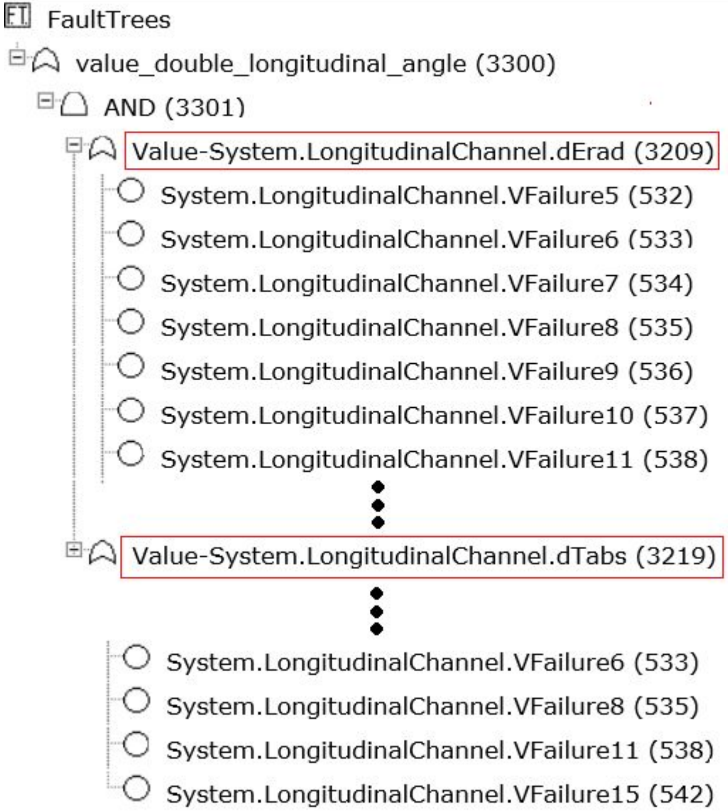
Component Fault Modelling

Component	Output Deviation	Failure Exp.
LongitudinalChannel	Value-dErad	VFailure1 OR (Value-uc OR Value-manual OR Value-dynp...)
	Value-dTabs	VFailure1 OR (Value-uc OR Value-manual OR Value-dynp...)

During the SLUGS autopilot component fault modelling, 29 failure expressions were added to 11 SLUGS model elements.

Example: an incorrect value of dErad output deviation can occur due to an internal failure or due to an incorrect value of one of the Longitudinal Channel input ports.

Fault Trees and FMEA



- The occurrence of LongitudinalChannel.dErad and LongitudinalChannel.dTabs component output deviations are top-level failures of incorrect value for double longitudinal angle fault tree.

Conclusion

- The application of the proposed approach reduced the effort, costs, and the **number of errors** in performing Hazard Analysis and Risk Assessment (HARA), component fault analysis/modelling, and enabled the automated generation of **FTA and FMEA** dependability artefacts required by the standards to achieve safety.

- The use of **Bayesian Networks (BN)** to improve the analysis of the relationships between **safety**/**security** in the unmanned aerial vehicles domain.