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



Critical Embedded Systems

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



- 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

Global Risk Time:	10000	🚽 🚺 Ha	azards - I	HiP-H	×>		×
Description:		Name:	erro_angulo	_longitudinal_du	plo		LLiD
Hazards	simples	SIL:				0	105
erro_angulo_lateral erro_angulo_longitu	_duplo dinal_simples]
erro_angulo_longitu erro_pwm erro_navigation	dinal_duplo	Gauses	Enilune Eur		De	Add	
		Value-Syster	m.LongitudinalChar	inel.dErad AND \	/alue-Sys	Edit	
Optimisation Paramete Maximum Generations	ers s:					Delete	
Objective	Goal						
None Selected	\sim						
None Selected	~	<			>		
None Selected				Cancel	Save and Close]	
			Course and Oliver	7			

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

lobal Risk Time: 10000	🛃 Hazards - HiP-H — 🔲 🗙
scription.	Name: erro_angulo_longitudinal_duplo
azards erro_angulo_lateral_simples erro_angulo_lateral_duplo erro_angulo_longitudinal_simples erro_angulo_longitudinal_duplo erro_anym	
erro_navigation	Failure Expression Pr Add Value-System LongitudinalChannel dErad AND Value-Sys. Edit
ptimisation Parameters aximum Generations: bjective Goal	Delete
one Selected	
une selected	

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

Blobal Risk Time:	10000	🚽 📣 Ha	zards - H	HiP-H			×
escription:		Name:	erro_angulo	_longitudinal_dup	lo		LliD
Hazards erro_angulo_lateral_sir erro_angulo_lateral_du erro_angulo_lonoitudin	mples iplo al simples	SIL:				\$	10 5
erro_angulo_longitudin erro_pwm erro_navigation	al_duplo	Value-System	Failure Exp	ression nel.dErad AND V	Pr	Add	
Optimisation Parameters Aaximum Generations:	0.000					Edit	
None Selected							
None Selected	~	<			>		
tone beleeted	-			Cancel	Save and Close		

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

Name: Description:	Value-Sistema.LongitudinalChannel.dTabs	2
Svetem (2
Severity:		
📣 Caus	se - HiP-HOPS Fa — 🛛	×
bability:		
ure Expression.	(Value-U_holdPID OR VFailure1) or (Value-dyrW OR VFailure1) or (Value-U_holdPID OR VFailure8) or (Value-dt_trim OR VFailure4) or (Value-XYZm OR VFailure19) or (Value-thata_m OR VFailure3) or (Value-Manual OR VFailure21) or (Value-dt_FF_gain OR VFailure31)	و اہ

Inputs:

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

Component Fault Modeling

Name: Description:	P-HOPS Failur — — X	
System Ou Severity:	e - HiP-HOPS Fa	×
Probability: Failure Expression:	(Vfailure-U_c OR VFailure1) or (Value-dyNP OR VFailure13) or (Value-U_holdPID OR VFailure8) or (Value-dT_trim OR VFailure4) or (Value-XYZm OR VFailure19) or (Value-thata_m OR VFailure15) or (Value-Manual OR VFailure21) or (Value-dT_FF_gain OR VFailure31)	P S
	Cancel Save and Close	

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

Name:	Value-Sistema.Lo	ongitudinalChannel.	dTabs			iD
Description:				^ >	Π	5
System (utport?			More.		+
Severity:						
🔨 Caus	e - HiP-HO	PS Fa				X
- Cuu		1 o i am		0 - 30 6.		
bability:						
ure Expression	(Vfailure-U_c OR VFail	ure1) or (Value-dy /Failure8) or (Value	NP OR VFailure	13) or	^	
	(Value-XYZm OR VFail	lure19) or (Value-t	hata_m OR VFa	ilure15) or		
	(Value-XYZm OR VFail (Value-Manual OR VFa	lure19) or (Value-t ilure21) or (Value-	hata_m OR VFa dT_FF_gain OR	ilure15) or VFailure31)		
	(Value-XYZm OR VFail (Value-Manual OR VFa	lure19) or (Value-t ilure21) or (Value-	hata_m OR VFa dT_FF_gain OR	ilure15) or VFailure31)		
	(Value-XYZm OR VFail (Value-Manual OR VFa	lure19) or (Value-t ilure21) or (Value-	hata_m OR VFa dT_FF_gain OR	ilure15) or VFailure31)		
	(Value-VZm 0R VFa (Value-Manual 0R VFa	lure19) or (Value-t ilure21) or (Value-	hata_m OR VFa dT_FF_gain OR	ilure4) or VFailure31)		
	(Value-XYZm OR VFa (Value-Manual OR VFa	lure19) or (Value-t ilure21) or (Value-	dT_FF_gain OR	allure4) or ilure15) or VFailure31)		
	(Value-XYZm OR VFa (Value-Manual OR VFa	ure19) or (Value-t ilure21) or (Value-	hata_m OR VFa dT_FF_gain OR	ulure1) or VFailure31)		
	(Value-XYZm OR VFa (Value-Manual OR VFa	ure19) or (Value-t ilure21) or (Value-	hata_m OR VFa dT_FF_gain OR	ulure1) or VFailure31)		
	(Value-XYZm OR VFa (Value-Manual OR VFa	ure19) or (Value-t ilure21) or (Value-	hata_m OR VFa	Ulure15) or VFailure31)		

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;
- ComputePSIDotL1OutputFeed backController;
- 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)

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.

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.

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.



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	Ι.
SC ³	Value double longitudinal angle	Value-LongCh. dErad AND Value-LongCh dTabs	Hzdous	В	
SUC	Value doubleValue-LongCh.longitudinaldErad ANDangleValue-LongCh.dTabs		Major	С	
SC	Value lateral channel	Value-LateralCh. dArad AND Value-LateralCh.dRad	Hzdous	В	į
SUC	Value lateral channelValue-LateralCh. dArad AND Value-LateralCh.dRad		Hzdous	В	\
SC	Value PWM signals	Value-PWMGen .pwmSign OR Late-PWMGen. pwmSign	Hzdous	В	
SUC	Value PWM signals	Value-PWMGen .pwmSign OR Late-PWMGen. pwmSign	Major	С	

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

EI FaultTrees

- - □ 🛆 AND (3301)
 - Value-System.LongitudinalChannel.dErad (3209)
 System.LongitudinalChannel.VFailure5 (532)
 System.LongitudinalChannel.VFailure6 (533)
 System.LongitudinalChannel.VFailure7 (534)
 System.LongitudinalChannel.VFailure8 (535)
 System.LongitudinalChannel.VFailure9 (536)
 System.LongitudinalChannel.VFailure10 (537)
 System.LongitudinalChannel.VFailure11 (538)
 - System.LongitudinalChannel.VFailure6 (533)
 - O System.LongitudinalChannel.VFailure8 (535)
 - System.LongitudinalChannel.VFailure11 (538)
 - System.LongitudinalChannel.VFailure15 (542)

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.