RESEARCH MASTER THESIS

Department of Complex Systems Engineering

Supervisors :

Jean-Charles Chaudemar (jean-charles.chaudemar@isae-supaero.fr), Kevin Delmas (kevin.delmas@onera.fr)

Location : Toulouse, ISAE-SUPAERO

Duration : 5-6 months (flexible)

Start in : March, 2021

INTERNSHIP DESCRIPTION

Domain : MBSE – MBSA

Title : **TOWARDS A FRAMEWORK FOR EARLY SAFETY ASSESSMENT AND DESIGN**

Model-Based Systems Engineering approaches (MBSE) enables to organise people, products and processes around a methodology for the design of systems. MBSE outputs are part of the baseline for lots of technical engineering processes such as the safety process. For instance, the requirements and the design architecture are key elements in the safety activities. Moreover, providing experts with MBSE models to be relied on as repositories of reference models for the analysis and the justification. Examples of MBSE tools to be used in that design framework include TTool, Capella, Cameo Systems Modeler and Papyrus.

In particular, the safety view is paramount during the development of UAS to obtain flight authorisation. Demonstrating the safety of these systems is tied to the analysis of the contributions of various elements to the hazardous situations, such as mid-air and on-ground collision. For UAS, these contributors range from an erroneous execution of a task by the operator, to an on-board failure of critical components. To mitigate the effects of failures, drone manufacturers often rely on highly reconfigurable and autonomous architectures. The variety of the contributors to the risk and the innovative architecture proposed by the manufacturers challenge the current practices of safety assessment.
To handle both the variety of contributors and the complexity of the UAS architecture, work like [3] proposes to rely on Model-Base Safety Assessment (MBSA) that is to perform various analyses based on models built over a formal language like Altarica [1] and dedicated to specific types of contributors. These analyses can consider the impact of an erroneous application of a task in a procedure, or the propagation of a material failure (e.g., motor failure) in the architecture. Obviously, most of the hazardous scenarios are a combination of contributors of various kinds, for instance an erroneous application of an emergency procedure triggered by an on-board material failure. There is a need to formalise the relation between all these models to ensure the consistency of the overall analysis.

More precisely, the intern's tasks are as follows:

- To do a state-of-the-art for this research theme;
- To identify the key processes and data flows for safety analysis and design;
- To propose and build-up a modelling framework;

The intern has to show abilities to meet following issues :

- Can we trace the impact of failure requirements on UAS design and safety analysis?
- Can we assess a UAS design while meeting safety objectives? And how?

The framework and proposed assessments will be illustrated on a realistic fixed wing UAS operating in a sparsely populated area.

I. REFERENCES

[1] Pierre Bieber, Christian Bougnol, Charles Castel, Jean-Pierre Heckmann Christophe Kehren, Sylvain Metge, and Christel Seguin. *Safety assessment with Altarica*. In Building the Information Society, pages 505-510. Springer, 2004.

[2] Marco Bozzano, Alessandro Cimatti, Oleg Lisagor, Cristian Mattarei, Sergio Mover, Marco Roveri, and Stefano Tonetta. *Safety assessment of Altarica models via symbolic model checking*. Science of Computer Programming, 98:464-483, 2015.

[3] Kevin Delmas, Christel Seguin, and Pierre Bieber. *Tiered model-based safety assessment*. In International Symposium on Model-Based Safety and Assessment, pages 141-156. Springer, 2019.

[4] FAA. *Concept of operations* v1.0, 2018.

[5] JARUS. *Jarus guidelines on specific operations risk assessment*, 2017.

[6] F. Mhenni, J.-Y. Choley, and N. Nguyen. *An integrated design methodology for safety critical systems*. In 2016 Annual IEEE Systems Conference (SysCon), pages 1-6, 2016.

[7] Leveson N., M. S. Herring, B. D. Owens, M. Ingham, and K. A. Weiss. *Safety-driven model-based systems engineering methodology*. Technical report, MIT, 2007.

[8] Pant Vatsal, Demmou Hamid, and Chaudemar Jean-Charles. *Safety Analysis of Pilot-System Interaction*. In 12th International Conference on MOdeling, Optimization and SIMulation (MOSIM18), 2018.

[9] Pant Vatsal, Chaudemar Jean-Charles, and Demmou Hamid. *Using Systems Engineering to Model the Interaction of the Pilot, the Aircraft, and the Procedures*. In 5th International Symposium on Systems Engineering (ISSE 2019), 2019.

0 % Theoretical Research	**100 % Applied Research**	0 % Experimental Research

Possibility to go on a Ph.D.: o Yes o No

APPLICANT PROFILE

Knowledge and required level:

Systems engineering (requirements, process, concepts), safety analysis (fault tree analysis, functional hazard analysis, failure mode and effect analysis), safety assessment

Languages/Systems :

Applications should be sent by e-mail to the supervisor, enclosing CV, cover letter mandatorily, and master transcript optionally.