RESEARCH MASTER THESIS

Department of Complex Systems Engineering

Supervisors:

Pierre de Saqui-Sannes

(Pierre.De-saqui-sannes@isae-supaero.fr)

Jean-Charles Chaudemar

(Jean-charles.Chaudemar@isae-supaero.fr)

Kevin Delmas (Kevin.DELMAS@ext.isae-supaero.fr)

Charles Mathou (charles.mathou@isae-supaero.fr)

Location : Toulouse, ISAE-SUPAERO

Duration : 5-6 months (flexible)

Start in : March, 2023

INTERNSHIP DESCRIPTION

Domain : MBSA – code generation

Title : **CODE GENERATION FOR SAFETY ASSESSMENT OF UAV PHYSICAL ARCHITECTURE**

The Safety Analysis (SA) of a system consists in the verification and validation of its safety properties. Such safety properties include the system's capacity to maintain an acceptable level of safety despite the occurrence and propagation of system faults (*e.g.* a UAV landing safely despite losing an engine). Within the Concorde project, research is carried out in order to streamline the usually complex processes of safety analysis and certification for UAVs, notably through the Model-Based Safety Analysis (MBSA) approach. This methodology uses models in order to facilitate simultaneous and unambiguous collaboration between various parties. It offers features to simplify and accelerate the SA processes.

The AltaRica DataFlow (ADF) language supports the MBSA approach, notably through the definition of custom components exhibiting user-defined behaviours. As ADF has no notion of inheritance or genericity, different projects often require rewriting largely identical components that differ only marginally. The Scala-based domain-specific language (DSL) ALPACAS provides the same Stochastic Guarded Transition System (SGTS) features as ADF, while also offering generic programming capabilities. However, ALPACAS is a "traditional" programming language editable via text only where ADF can be used both textually and visually thanks to the Cecilia Workshop.

The proposed internship consists in leveraging the existing ALPACAS DSL's generic programming features to automatically generate the code of various ADF components based on their logic description.

More precisely, the intern's tasks are:

- To do a state-of-the-art for the theme of safety analysis code generation;
- To familiarize themselves with the Scala 3 and ADF languages and the ALPACAS DSL;
- To provide a user-friendly mean of encoding an ADF component's logic into Scala 3;
- To generate the corresponding ADF code;
- To establish a formal proof of adequacy of the code generation;
- To illustrate the generation process on a sample UAV physical architecture

I. REFERENCES

[1] Buyse, M., Delmas, R., & Hamadi, Y. (2021). ALPACAS: a language for parametric assessment of critical architecture safety. In *35th European Conference on Object-Oriented Programming (ECOOP 2021)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik.

[2] Boiteau, M., Dutuit, Y., Rauzy, A., & Signoret, J. P. (2006). The AltaRica data-flow language in use: modeling of production availability of a multi-state system. *Reliability Engineering & System Safety*, *91*(7), 747-755.

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

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

APPLICANT PROFILE

Knowledge and required level:

Knowledge in computer science and programming languages (Scala 3 is a plus)

Notions of safety analysis

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