PhD @ ISAE-SUPAERO, 3 years

Languages and tools for safety assessment of distributed and reconfigurable systems

Project CONCORDE (DGA/AID)

PhD supervisors:

ONERA : Tatiana Prosvirnova, Christel Seguin, Jérôme Morio
ISAE-SUPAERO : Jean-Charles Chaudemar

Contact: jean-charles.chaudemar@isae-supaero.fr; Tatiana.prosvirnova@onera.fr; Christel.seguin@onera.fr; Jerome.morio@onera.fr

Deadline for applying: December, 2023
Funding: French Defense Ministry (DGA/AID)
Scientific domain: safety, reliability, computer science, applied mathematics
Keywords: modelling, safety assessment, statistics

Context

The research activities of the department of Complex Systems Engineering at ISAE-SUPAERO mainly focus on developing the new assets of Model Based approaches at early-design phase. Similarly, the department ONERA/DTIS has an expertise in the methods and tools for certification, multidisciplinary design, autonomy, applied mathematics. These two departments are involved in the CONCORDE project aiming at dealing with the design of UAS under distinct and complementary aspects. This CONCORDE project offers new perspectives in order to enhance the methodologies used for the drone certification.

Description

The classic modelling formalisms used in safety, such as fault trees or block diagrams for reliability, are based on probabilistic Boolean algebras and have very handy graphical representations. But today, these formalisms have reached their limits. On the one hand they do not support accurate modelling of the dynamic aspects of systems (e.g. reconfigurations). On the other hand their structure usually aims at highlighting the combination on failure leading to a hazard. Such structures are far from the usual structures of design models (Model-Based Systems Engineering aka MBSE) and do not ease handling of complex systems. This is why the work on AltaRica, a high-level modelling language, dedicated to the safety analysis, began in the late 90s at LaBRI [1].

AltaRica is a modelling language based on automata, which makes it possible to represent the dynamic aspects of systems, such as reconfigurations. It is a compositional language. It is therefore possible to create component libraries and reuse them to create models. AltaRica is a text-based language. Its AltaRica DataFlow version [2] is used in several industrial modelling tools, such as SimfiaNeo developed by Airbus Protect and Cecilia developed by Satodev.

The new version of the AltaRica language, AltaRica 3.0 [3], enables the modelling of bidirectional flows between components, and also integrates new structural constructs derived from object-oriented and prototype-oriented programming languages. AltaRica 3.0 is supported by the OpenAltaRica platform (https://www.openaltarica.fr/), which integrates several processing tools.

Dependability models (and also AltaRica models) are used to calculate two main types of indicators:

- The failure scenarios that lead to the feared event;
- The probability of the undesired event.

These models are always a trade-off between the representativeness of the system model and the complexity of the computations that can be carried out through the model.

Nowadays, AltaRica models of reconfigurable systems represent systems with a finite and relatively limited number of components. The aim of this PhD thesis is to study the scaling of AltaRica models for large distributed and reconfigurable systems (e.g. UAS deployed in a system of systems context).

Work agenda

The roadmap of PhD thesis will focus on three research areas:

1) Representation of dependability models for large-scale reconfigurable systems (what is the right level of abstraction, how to develop the right modelling strategy to manage complexity, what are the right properties of modelling languages, how to model graphically, ...) ;
2) Computation of safety indicators (how to optimize the generation of critical failure scenarios, how to compute probabilistic indicators, experiments with guided stochastic simulation, etc.);
3) Analysis of the sensitivity of safety outcomes to different sources of uncertainty or lack of knowledge.

An application to a case study on UAVs will be carried out to validate the proposed approach.

Expected skills

The applicant holds a master degree in computer science or applied mathematics. In addition to the tasks about the setting out of a domain specific modelling language and method, the applicant will develop own method or high-level language. Fluency in English and soft skills are required abilities.

IT skills are as follows:

- languages: C, **Java, Python**, R

- modelling: **AltaRica**, safety, formal methods

References

[1] The AltaRica Formalism for Describing Concurrent Systems, André Arnold, Alain Griffault, Gérald Point, and Antoine Rauzy, in Fundamenta Informaticae. IOS Press. Vol. 34, pp 109–124, 2000

[2] The AltaRica Data-Flow Language in Use: Assessment of Production Availability of a MultiStates System, Marie Boiteau, Yves Dutuit, Antoine Rauzy, and Jean-Pierre Signoret, in Reliability Engineering and System Safety. Elsevier. Vol. 91, Num. 7, pp 747–755, July, 2006, doi: 10.1016/j.ress.2004.12.004

[3] AltaRica 3.0 in 10 Modeling Patterns, Michel Batteux, Tatiana Prosvirnova, and Antoine Rauzy, in International Journal of Critical Computer-Based Systems, Inderscience Publishers, Vol. 9, Num. 1–2, pp 133–165, 2019, doi: 10.1504/IJCCBS.2019.098809