Ph.D. position

Transforming Model-Based Design: An Agile Method for Ensuring Safety and Security in Critical Systems

Ludovic Apvrille (ludovic.apvrille@telecom-paris.fr),
Pierre de Saqui-Sannes (pierre.de-saqui-sannes@isae-supaero.fr)

April 2023

1 Context and problematics

Model-Based Systems Engineering, commonly known as *MBSE*, is one of the drivers of the evolution of document-based systems engineering towards a systems engineering approach where a set of models serves as a reference throughout the system's life cycle. An increasing number of industrial projects are implementing an MBSE approach, where model evolution is a central element [Sultan et al., 2017]. Evolution involves creating a model m_1 and applying a mutation $\rightsquigarrow$ to produce a new model m_2: $m_1 \rightsquigarrow m_2$. For example, a mutation may involve adding a new component to the model (such as a component provided by a third party) or modifying the behavior of an existing component. Adding redundancy to a critical system involves duplicating a computation, which includes adding a new processor and an existing task to that processor. Another example is adding encryption to a network to improve the confidentiality of data transmitted over that network. Frequent and small mutations correspond to an agile approach.

One of the expected benefits of using MBSE is the ability to formally verify models to detect design errors early in the system's life cycle [de Saqui-Sannes et al., 2021]. Formal verification of a system involves defining a set of properties P and proving these properties on the model using simulation techniques or mathematical proofs, such as with model checkers. These proofs can be very computationally expensive and time-consuming. Moreover, in the context of an agile approach that involves frequent mutations to a model, proofs must be carried out at every stage, increasing their cost throughout the development cycle.

Initial work has been done in the direction of formally defining model mutations, either to better frame (formally) these mutations [Sultan et al., 2017], or to propose improved verification from models used in MBSE. For example, the work proposed in [Xie et al., 2022] illustrates a compositional proof approach (but not incremental) from SysML models. This composition is applied to safety properties. [Bougacha et al., 2022] proposes to rely on Event-B to frame the refinement of SysML models, and thus develop models correctly by construction. This framing heavily limits the possible mutations (which must be refinements) and does not support security.

The team proposing this thesis topic has already partially addressed this problem by relying on dependency graphs and the evolution of these graphs when a mutation is made to a model [Apvrille et al., 2022]. Yet, current work enables proof simplification only for reachability properties.

2 Contributions

The thesis will address the problem previously stated by reusing proofs made at modeling stage n for proofs to be made at stage $n + 1$.

More formally, let P be a set of properties that have been proven on a model m_1. We consider m_2 to be a model obtained after mutating $m_1 : m_1 \rightsquigarrow m_2$. The thesis will establish formal definitions $\mathcal{D}$ and algorithms $\mathcal{A}$ to best reuse the results of the proof of P on m_1. $\mathcal{A}$ must thus be able to compute the minimal set of properties P' to be proven on m_2 to ensure that the properties in P remain true on m_2.

Once these definitions and algorithms are established, they will need to be adapted to the SysML language and implemented in the free and open-source software TTool [TTool, 2022]. Finally, these works will need to be applied to both safety and security properties for different types of critical systems, particularly for aeronautical systems (e.g., real-time networks).

Thus, this thesis will propose a new framework for the design of safe and secure critical systems, supporting agile development methods.

3 Expected work

The Ph.D. is financed for 36 months, and will follow the following working plan:

1. **State of the art** on model mutations and incremental verification techniques.
2. **Proposal of an incremental verification approach** for the SysML language: definitions and algorithms.
3. **Prototyping in the TTool tool** of this approach and **performance study** to evaluate the complexity for random systems.
4. **Evaluation of the approach** on the development cycle of **critical systems** from the aeronautical, industry 4.0, or telecommunications domains. This evaluation will concern mutations corresponding to both functional safety and security aspects.
5. **Publication of the results** in at least one A-rank conference (e.g., MODELS) and in at least one international journal.

4 Administrative aspects

- Ph.D. scholarship: 50% by Télécom Paris and 50% by ISAE-SUPAERO.
- Ph.D director: Prof. Ludovic Apvrille (Télécom Paris)
- Co-director : Prof. Pierre de Saqui-Sannes (ISAE-SUPAERO)
- Co-supervisors: Dr Oana Hotescu (ISAE-SUPAERO), Dr Sophie Coudert (Télécom Paris)
- Duration: 36 months (18 months at Télécom Paris Sophia-Antipolis, 18 months at ISAE-SUPAERO Toulouse)
- Starting: September 2023

5 Profile and required skills

- Master's degree, engineer or equivalent in computer science
- Pre-requisites: the candidate should have taken courses in the field of system design (particularly embedded systems) and should have knowledge of the basis of formal methods.
- Programming languages skills: C/C++, Java
- Good level of spoken and written English

6 To apply

- Contact: Ludovic Apvrille (ludovic.apvrille@telecom-paris.fr), Pierre de Saqui-Sannes (pierre.de-saqui-sannes@isae-supaero.fr)
- Documents to include in the application: resume, cover letter, grades transcripts, recommendation letter(s).

References

[Apvrille et al., 2022] Apvrille, L., de Saqui-Sannes, P., Hotescu, O., and Calvino, A. T. (2022). SysML Models Verification Relying on Dependency Graphs. In *10th International Conference on Model-Driven Engineering and Software Development*, Vienna, Austria.

[Bougacha et al., 2022] Bougacha, R., Laleau, R., Collart-Dutilleul, S., and Ben Ayed, R. (2022). Extending SysML with Refinement and Decomposition Mechanisms to Generate Event-B Specifications. In *TASE 2022: Theoretical Aspects of Software Engineering*, volume 13299 of *Lecture Notes in Computer Science*, pages 256–273. Springer.

[de Saqui-Sannes et al., 2021] de Saqui-Sannes, P., Apvrille, L., and Vingerhoeds, R. (2021). Checking SysML Models Against Safety and Security Properties. *Journal of Aerospace Information Systems*, pages 1 – 13.

[Sultan et al., 2017] Sultan, B., Dagnat, F., and Fontaine, C. (2017). A methodology to assess vulnerabilities and countermeasures impact on the missions of a naval system. In *Computer Security*, pages 63–76. Springer.

[TTool, 2022] TTool (2022). https://ttool.telecom-paris.fr/. *Retrieved May 11, 2022*.

[Xie et al., 2022] Xie, J., Tan, W., Yang, Z., Li, S., Xing, L., and Huang, Z. (2022). Sysml-based compositional verification and safety analysis for safety-critical cyber-physical systems. *Connection Science*, 34(1):911–941.