Ph.D. proposal:

Definition and implementation of an agile method for designing and verifying communicating embedded systems

Ludovic APVRILLE, Bastien SULTAN
Telecom Paris
LabSoC team
450 routes des Chappes, F-06904 Sophia-Antipolis Cedex, France
Email: firstname.lastname@telecom-paris.fr

February 7, 2025

1 Context and problematics

In recent years, there has been a significant trend towards integrating embedded systems with networks using various wired and wireless protocols. While traditional techniques for designing embedded systems evolved gradually before the era of connected systems, the widespread interconnection of these systems has introduced new design challenges.

One of the key challenges arises from the common practice of simulating embedded systems directly from design models. Among the well-known simulators, the SystemC initiative and its simulation engine are frequently cited [1]. Other initiatives also include TTool-Diplodocus [5]. While these simulators effectively account for hardware and software aspects, they inherently lack support for protocol stacks and communication technologies beyond those typically found in System-on-Chip (SoC) architectures.

Addressing this limitation represents the first major challenge of this research.

A second challenge stems from the increasing complexity introduced by connectivity. As embedded systems become more complex, agile methodologies are likely to be employed to structure the design process into well-defined stages. However, verification remains a crucial step, particularly for critical embedded systems, where it is known to be costly and, in some cases, infeasible within reasonable time constraints: the well-know problem of combinatory explosion. Therefore, agile modeling and verification methods are essential. One promising approach is incremental verification, which has already been explored in the literature [3]. However, optimizing incremental verification for mixed, communicating, and critical embedded systems remains an open research problem. Addressing this issue constitutes the second challenge of this thesis.

These challenges will be addressed in the scope of a collaborative research project with Prove&Run.

2 Objective

The objective of this Ph.D. thesis is to define, implement, and evaluate a novel agile modeling and verification method to enhance the design of networked embedded systems.

As a starting point, [3] proposes leveraging graph analysis techniques to capture logical dependencies between system elements. This approach should be extended to include the logical dependencies inherent in networked systems. Building on this foundation, extended models for the Diplodocus environment will be developed [4], incorporating support for network-based communications. Since networked systems are exposed to different attack vectors compared to standalone embedded systems, security extensions for Diplodocus [6] will also be explored. All contributions related to this objective will be implemented as extensions of the TTool-Diplodocus graphical user interface [2] and simulator [5].

The second objective focuses on the incremental modeling and verification of the proposed models. This will build upon existing techniques developed by the research team [7, 3], as well as insights from a broader state-of-the-art review. A new incremental modeling and verification technique tailored to the extended models will be designed, implemented, and evaluated, addressing both safety and security aspects. The approach will integrate an enhanced mutation-based verification strategy and novel verification algorithms. Additionally, emerging methodologies such as artificial intelligence may be explored to further improve modeling and verification efficiency.

3 Expected work

In order to address the aforementioned challenges, we propose the following steps:

1. Analyze existing methods for designing and verifying embedded systems and communication protocols.

2. Acquire expertise in simulation and formal verification using the TTool framework, including its existing capabilities for incremental verification. Initial models for the SolidCloud project will be developed within this framework.

3. Develop a novel method, along with the necessary supporting technologies, to address the identified challenges. Implement the corresponding updates in TTool.

4. Apply the proposed techniques to case studies provided by the SolidCloud project and benchmark the results against state-of-the-art approaches.

5. Publish findings in A-rank conferences and journals.

4 Required Skills

- Strong background in computer engineering is mandatory.
- Prior knowledge of embedded systems (hardware and software) is highly recommended.
- Experience in modeling and verification is preferred.
- Familiarity with UML/SysML is not required.

5 How to apply?

Do send all the required information—**in a unique pdf file**—by email to:
ludovic.apvrille@telecom-paris.fr and to bastien.sultan@telecom-paris.fr

Incomplete applications will not be processed. Candidates will be selected upon technical aspects (maths, computer engineering) and on their ability to pursue scientific research (for instance: reviewing a research paper).

- CV.
- Cover letter clearly stating your interest for our lab and for the topic of the Ph.D.
- Recommendation letters.
- Master's grades.

References

[1] Ieee standard for standard systemc® language reference manual. *IEEE Std 1666-2023 (Revision of IEEE Std 1666-2011)*, pages 1–618, 2023.

[2] Ludovic Apvrille. TTool for DIPLODOCUS: an environment for design space exploration. In *Proceedings of the 8th International Conference on New Technologies in Distributed Systems*, pages 28–29. ACM, 2008.

[3] Sophie Coudert, Ludovic Apvrille, Bastien Sultan, Oana Hotescu, and Pierre de Saqui-Sannes. Incremental and formal verification of sysml models. *SN Computer Science*, 5(6):714, Jul 2024.

[4] Andrea Enrici, Ludovic Apvrille, and Renaud Pacalet. A model-driven engineering methodology to design parallel and distributed embedded systems. *ACM Trans. Des. Autom. Electron. Syst.*, 22(2):34:1–34:25, January 2017.

[5] D. Knorreck, L. Apvrille, and R. Pacalet. Fast simulation techniques for design space exploration. In *47th International Conference Objects, Models, Components, Patterns*, volume 33, pages 308–327, Zurich, Switzerland, June 2009.

[6] Bastien Sultan, Ludovic Apvrille, Philippe Jaillon, and Sophie Coudert. W-sec: A model-based formal method for assessing the impacts of security countermeasures. In Luís Ferreira Pires, Slimane Hammoudi, and Edwin Seidewitz, editors, *Model-Driven Engineering and Software Development*, pages 203–229, Cham, 2023. Springer Nature Switzerland.

[7] Bastien Sultan, Léon Frénot, Ludovic Apvrille, Philippe Jaillon, and Sophie Coudert. Amulet: A mutation language enabling automatic enrichment of sysml models. *ACM Trans. Embed. Comput. Syst.*, sep 2023. Just Accepted.