Ph.D. Proposal for C3S

Model-based High-level Integration of Heterogenous Components

Ludovic APVRILLE, Rabéa AMEUR-BOULIFA
Telecom ParisTech
Equipe LabSoC
450 routes des Chappes, F-06904 Sophia-Antipolis Cedex, France
Email: firstname.lastname@telecom-paristech.fr

October 26, 2018

1 Context and problematic

The design of embedded systems is complicated by the many different (safety and security) requirements and the presence of both hardware and software components provided by different partners [5]. Not only must we assure that the system will always behave safely and is protected against attackers, we must also consider the conformance to standards of the considered domain (e.g. ISO 26262). Difficulties discovered during an integration phase can impact product time-to-market or product quality which may in turn impact a costly maintenance e.g. product recalls.

Ideally, the inter working of components should be evaluated as soon as possible in the product development cycle. Components can be expressed at different level of abstractions and with different formalisms, e.g. embedded software defined with matlab models or with a C/C++/Java API, components specified with UML/SysML-like langages (e.g. ARCADIA/Capella), components provided as Hardware IPs or modeled as SystemC classes, components formally described (B method), etc. The (formally) verified integration of such components taking into account safety and security standards [7] is still an open issue.

One solution could be to capture all the components to be integrated using the same formalism. Thus, it has been shown keeping the entire modeling within a single toolkit minimizes the amount of rework at each change [6]. For that purpose, we could reuse our approach to designing safe and secure embedded systems: SysML-Sec [2] and its tool TTool [3]. Yet, the transformation of heterogeneous component models into a unique format is a fastidious task that would be difficult to automate. Thus, we think a better approach could be used, as explain below.

2 Objectives

The solution we intend to study in this Ph.D. is first **to define techniques for joining the semantics of components captured with heterogeneous models and at different level of abstractions**. To do so, we suggest gluing the (meta)models of these components via metamodel composition techniques, as proposed in [4], while taking into account constraints defined in current standards e.g. the gluing of the different components should take into account the evaluation of the safety of the intended function as described in ISO 26262. A second contribution is **to propose simulation and verification techniques that can applied on glued (meta)models**. This "glue" must be defined so as to minimize the transformation work while still allowing fast and accurate simulations and verifications that can be applied to safety, security and performance properties. In this second contribution, we intend to reuse existing simulation and verification techniques, such as the ones proposed by the TTool framework.

This work will obviously be driven from partners of the "C3S chaire". It will be based on our previous contributions with Automotive partners, e.g. the European FP7 project EVITA [8] and the VEDECOM institute [9] [1]. This work will also be performed in collaboration with the Ph.D. proposal entitled "Model-based Joint Analysis of Safety and Security" where the objective is to rely on faults and attacks trees in order to design an embedded architecture. The results of this thesis will be taken into account as one of the all possible models in which heterogeneous components can be captured. In particular, the security aspects defined in the first Ph.D. will be taken into account both in the gluing and verification objectives.

3 Expected work

To achieve the previously described methodological issues, the thesis should focus on the following stages:

1. Understand the methods currently in use for safe or secure systems within the partners of the "C3S chaire". More generally a first bibliography on model-driven approaches for designing embedded systems will be studied, with a focus on the semantics of the different models currently used to capture automotive components.

2. Learn how to perform simulations and verifications with TTool and SysML-Sec. You will practice with a case study provided by the Chaire committee.

3. A deep bibliographical study must then be done on modeling techniques for safe and secure embedded systems, including meta-model composition, as well as on standards for automotive systems.

4. Propose a methodology to glue meta-models of heterogeneous components with simulation and verification in mind. Describe the meta-model composition techniques, and the simulation and verification techniques that can be applied on composed meta-models, and test on toy examples.

5. Apply your techniques to case studies provided by the Chaire partners. Deduce a new design methodology that respect the current automotive standards. The main use case that we will consider will be based on autonomous vehicles. For instance, we could try to integrate together models of (advanced) sensors (LIDARS, smart cameras, etc.) with algorithms oriented components (data fusion, trajectory computation).

4 Skills

- Excellent skills in software engineering (principle of Model-Driven engineering) and embedded architectures (i.e. hardware/software architectures)
- Skills in safety and security are appreciated.
- No prior knowledge of UML is necessary.

5 How to apply?

Send the following elements - in **one pdf** file - by email to ludovic.apvrille@telecom-paristech.fr. Incomplete applications won't be taken into account. Selected candidates will be evaluated on technical skills and on their research capabilities (e.g. reviewing a paper).

- CV
- Cover letter
- Reference letters. At least one reference letter from your Master internship supervisor is necessary.
- Grades obtained during the master, and ranks.

References

[1] L. Apvrille, L. W. Li, and A. Bracquemond. Design and verification of secure autonomous vehicles. In *12th European ITS Congress*, Strasbourg, France, June 2017.

[2] L. Apvrille and Y. Roudier. SysML-Sec: A Model Driven Approach for Designing Safe and Secure Systems. In *3rd International Conference on Model-Driven Engineering and Software Development, Special session on Security and Privacy in Model Based Engineering*, France, February 2015. SCITEPRESS Digital Library.

[3] Ludovic Apvrille. Webpage of TTool. In *http://ttool.telecom-paristech.fr/*, 2015.

[4] Matthew Emerson and Janos Sztipanovits. Techniques for metamodel composition. 01 2006.

[5] Thomas A Henzinger and Joseph Sifakis. The embedded systems design challenge. In *International Symposium on Formal Methods*, pages 1–15. Springer, 2006.

[6] National Instruments. Best practices for embedded software testing of safety compliant systems. http://www.ni.com/white-paper/13671/en/, 2016.

[7] Erwin Schoitsch. Design for safety and security of complex embedded systems: A unified approach. In Janusz S. Kowalik, Janusz Gorski, and Anatoly Sachenko, editors, *Cyberspace Security and Defense: Research Issues*, pages 161–174, Dordrecht, 2005. Springer Netherlands.

[8] H. Schweppe, Y. Roudier, B. Weyl, L. Apvrille, and D. Scheuermann. C2x communication: Securing the last meter. In *The 4th IEEE International Symposium on Wireless Vehicular Communications: WIVEC2011*, San Francisco, USA, September 2011.

[9] VEDECOM. Institut français de recherche partenariale publique-privée et de formation dédié à la mobilité individuelle décarbonée et durable. http://www.vedecom.fr/.