MITSUBISHI ELECTRIC
Changes for the Better

MITSUBISHI ELECTRIC R&D CENTRE EUROPE

1, ALLEE DE BEAULIEU, CS 10806
35708 RENNES CEDEX 7, FRANCE
TEL. (+33) 02.23.45.58.58 – FAX (+33) 02.23.45.58.59

for a greener tomorrow

PhD proposal M/F

A logical framework to verify requirements of hybrid system models

Ref BBY_PhD_201810

Industrial Partner: **MITSUBISHI ELECTRIC R&D CENTRE EUROPE (MERCE)**

1 allée de Beaulieu, CS 10806, 35708 Rennes Cedex 7, France

Site web: http://www.mitsubishielectric-rce.eu/

Academic Partner : **Centre de recherche Inria Rennes Bretagne Atlantique**
Equipe projet TEA
Campus universitaire de Beaulieu
35042 Rennes Cedex

Type of contrat: 3 years contract, from October 2018

Reference: BBY_PhD_201810

Research topic: A logical framework to verify requirements of hybrid system models

Subject proposed by: Benoît BOYER, co-advisor, MERCE

And Jean-Pierre TALPIN, advisor, INRIA

Thierry GAUTIER, co-advisor, INRIA

Context:

The main goal of this doctoral project is to build cyber-physical systems with a correct-by-construction approach in order to verify requirements against the two facets of the cyber and physical aspects of such designs. In particular the considered approach is based on components augmented with formal contracts so that component and contracts can be composed, abstracted or refined. The focus should be on proving properties at system-wide level by gathering individual properties proved at component level. This approach should be semantically grounded, be usable by regular engineers (i.e. not specialized in proofs) and tooled. As such, three main parts need to be developed:

1. A logical framework providing the theoretical foundation on which the semantics of the components and their interactions can be expressed and used to prove key properties. This logical framework should be accompanied by a methodology that prescribes how to use the framework to effectively build cyber-physical systems, i.e. model the continuous part and specify and implement the discrete part to ultimately verify key properties on their joint behaviour;
2. A user-level approach to describe formal specifications that is expressive, user friendly and can be translated into the above logical framework. In particular, a Simulink-like approach (dataflow oriented language) is considered to specify the system jointly with Parnas tables (e.g. NRL's SRC tools [1]) to specify contracts of the system's components;
3. A concrete implementation of the logical framework into a set of tools allowing to build and prove key properties (latency, timing, invariant …) of cyber physical systems.

Objectives:

The first part will build upon previous works that designed a component based approach for system design with an executable semantics of contracts [3] as well as formalized cyber-physical systems into components with a strong logical foundation grounded on differential logic dL and associated with an automatic composition theorem to prove properties from individual component contracts [2].

The doctoral project will be to merge the concepts on those works into a coherent framework and apply it to specify the semantics of a Simulink-like language of components allowing to equally specify and prove continuous and discrete components. In particular the logical framework will allow to verify the requirements seen as properties implied by the differential invariants of the analog model at the interface between the cyber and physical worlds. The contracts of such components will be based on guarded actions or (quantitative) logical propositions in separation logic. Ultimately, the implementation of the cyber (aka discrete) part should be amenable to an actual implementation as a set of tasks written in C language.

The second part should allow to capture and formalize requirements in simple terms of separation logic to support their formal verification in an industrial workflow of cyber-physical system design. The components of the CPS models under considerations are implemented in Simulink-like language augmented with formal contracts expressed in user-friendly form like Parnas tables. Requirements will be cured from possibly textual or informal specification into those Parnas tables.

The third part is to gather existing proof technology (Frama-C for C language, Keymaera X for dL, Liquid Haskell for liquid types, F* for dependent types, …) and organize them in such a way that industrially relevant properties can be indeed proved, i.e. verify the requirements against a refinement of the digital components (obtained by, e.g., static analysis or deductive verification). The use of proof technology should maximize proof automation. In case of errors, counter-examples should be proposed at user-level, i.e. at the same description level that the initial components contracts in Simulink-like language developed in the second part.

In order to support the adequacy of the doctoral project with actual industrial needs, Mitsubishi Electric R&D Centre Europe will provide a set of industrially relevant use cases from railway, automotive or factory automation domains.

Applications

The ideal candidate will have a strong background in mathematical logic, experience and interest in both program analysis, control theory and embedded system design. Depending on background and experience, he/she will engage either or both of the challenges posed by the verification of digital and analog requirements.

The successful applicant will be employed by the Industrial partner of the project Mitsubishi Electric R&D Centre Europe under a CIFRE grant and embedded with Inria project-team TEA at Inria, Rennes (Brittany, France).

Thank you to address CV and letter of motivation in PDF format by mail (by specifying in object: your name and the reference BBY_PhD_201810) to the following contact: jobs@fr.merce.mee.com

References

[1] Software cost reduction. Naval Research Laboratory: https://www.nrl.navy.mil/itd/chacs/5546/SCR

[2] "Compositional proofs in dynamic differential logic". S. Lunel, B. Boyer, J.-P. Talpin. International Conference on Applications of Concurrency to System Design (ACSD'17). Springer, 2017.

[3] “Mixing proved and unproved system parts through contracts to ensure correct-by-construction system design”. Antonin Butant, Master internship report, 2016.