Fully Funded PhD Thesis: **Safe Contract-Based Design of Cyber-Physical Systems (with scholarship from AGIR Grenoble Innovation Recherche)**

VERIMAG/INRIA, Grenoble, France

Context

Anti-lock breaking systems, temperature regulation in buildings, and drug infusion pumps are examples of cyber-physical systems (CPS) where software interacts with physical processes so as to ensure a desired safe and efficient behavior. CPS are usually subject to safety and reliability requirements. Depending on the application, their failure may have unacceptable consequences. It is therefore crucial to ensure their correctness at design time.

Goals

This thesis focuses on contract-based design of safe CPS. The contract of a component formally specifies the hypotheses the component makes on its environment, and its commitments (or expected behavior) in case the hypotheses are verified.

In order to reason about interactions between software and physical processes one has to use *hybrid* models combining continuous and discrete dynamics. In addition to the problem of undecidability, several characteristics of hybrid systems such as their infinite state space and the lack of analytic solutions for systems described by differential equations, make these systems particularly hard to analyze using exact methods; often one has to use approximations. Existing methods and tools for formal analysis of hybrid systems do not scale well and only allow, in practice, for partial analysis of systems due to their high complexity.

The first goal of this thesis is to develop a contract-based design approach for hybrid systems, in order to overcome the current limitations of formal analysis. The definition and verification of contracts rely on *assume/guarantee* reasoning that has been extensively studied for discrete systems and extended to systems with simple continuous dynamics [AH01]. The first goal of this thesis is to propose assume/guarantee rules for complex hybrid systems that can be used to define and implement operations on contracts. These rules should then be implemented as set-based analyses on the input/output relation, using existing platforms for reachability analysis of hybrid systems such as [DT11, DT12]. The proposed approach will be applied to several case studies of medical devices.

Working Context

The thesis will be co-advised by Thao Dang (Verimag) and Gregor Goessler (INRIA). The PhD student will be hosted by the Verimag laboratory, near Grenoble in the French Alps. The work will be performed in collaboration with Vasiliki Sfyrla (VISEO group), who will provide several case studies.

Required Skills

Candidates should have good background in theoretical computer science and continuous mathematics. Good programming skills are a plus.

Application

Interested candidates should send a cover letter and curriculum vita to Thao.Dang@imag.fr and Gregor.Goessler@inria.fr

References

[AH01] L. de Alfaro and T. A. Henzinger. Interface theories for component-based design. In *Proceedings of the First International Workshop on Embedded Software*, EMSOFT '01, pages 148–165, London, UK, UK, 2001. Springer-Verlag.

[DT12] T. Dang and R. Testylier. Reachability analysis for polynomial dynamical systems using the Bernstein expansion. *Reliable Computing Journal*, Special issue: Bernstein Polynomials in Reliable Computing, ISSN 1573-1340, December 2012.

[DT11] T. Dang and R. Testylier. Hybridization Domain Construction using Curvature Estimation. *Hybrid Systems: Computation and Control HSCC'2011*, pages 123-132, ACM, 2011.