**PhD student position at Laboratory VERIMAG and INRIA POP-ART Project**
**Grenoble, France**

# Topic: High-confidence design of cyber-physical systems

**Context.** High-confidence design of cyber-physical systems poses a great challenge, because they must meet various requirements (such as intelligent and autonomous behavior, adaptability and resilience) to cope with unexpected errors in their components and possible configuration changes. To model and reason about the interactions between computer systems and physical processes, hybrid system that combine continuous and discrete dynamics are an appropriate mathematical model. In addition to the problem of undecidability, several features of hybrid systems (such as infinite state space and the lack of analytical solutions of systems described by differential equations) make these systems particularly difficult to analyze by exact methods, and it is often necessary to resort to approximate methods. Existing methods and tools for the formal analysis of hybrid systems, because of their high complexity, allow verifying verify practical systems only partially. Their scalability remains a major issue.

**Objectives of the thesis.** The thesis aims to develop an *approach based on contracts* for hybrid systems, to reduce the size of the systems to verify and leverage the scalability of formal analysis of cyber-physical systems. The definition and verification of contracts will be based on the approach of "assume-guarantee". This approach has been well studied for discrete systems and extended to continuous dynamical systems with simple continuous dynamics. In this thesis we intend to propose assume-guarantee rules for complex hybrid systems (described with differential equations) that can be used to define and implement contract operations. These assume-guarantee rules can be verified by set-valued analysis of the input /output relation, and for this problem the existing infrastructure for reachability analysis of continuous and hybrid systems can be used.

The originality of the approach adopted in this thesis lies in the combination of these two approaches to achieve an efficient method of formal design. This approach will be applied to several case studies, including cyber-physical systems from medical applications. Contacts have been established with the Research and Innovation group VISEO who shows an interest in this approach to design and verification. Collaboration will be formalized this theme during the thesis.

The thesis will be co-supervised by **Gregor Goessler** (INRIA Rhone-Alpes) and **Thao Dang** (VERIMAG), who are experts in the theory of hybrid systems and in the design based on contracts respectively.

**Requirements.**
The successful candidate should have a Master in Computer Science, Electrical Engineering, Applied Mathematics. Programming experience (with C, C++) is required. Knowledge of dynamical systems, formal verification and related areas is a plus.

**Contacts.**

- Gregor Goessler, POP-ART Project, INRIA Rhône-Alpes, Email:gregor.goessler@inria.fr
- Thao Dang, CNRS/VERIMAG. Email: thao.dang@imag.fr