PhD thesis offer (CIFRE)

Timed contracts for Correct-by-Construction system design

Company:	MITSUBISHI ELECTRIC R&D CENTRE EUROPE 1 allée de Beaulieu, CS 10806, 35708 Rennes Cedex 7, France Web site: http://www.mitsubishielectric-rce.eu/
Contract type:	3 years determined term period (CDD), September 2015
Reference:	FM_PhD_201509
Research theme:	Formal methods, systems and services

Scientific environment:

Mitsubishi Electric R&D Centre Europe is the European research laboratory of Mitsubishi Electric group. Mitsubishi Electric builds a wide range of products, from most common ones (fridges, air-conditioning, etc.) to most specialized safety critical ones (nuclear power plant or train control systems, satellites, power electronic systems, elevators, etc.). COM division of Mitsubishi Electric R&D Centre Europe works on formal methods, amongst other topics, to improve product quality and reduce production costs while taking into account the whole development process (people qualification, properties to ensure, usability vs. provability ratio, integration into classical development process, etc.).

This PhD proposal is in partnership with INRIA Rennes.

Established in 1967, INRIA is the only French public research body fully dedicated to computational sciences. Combining computer sciences with mathematics, INRIA's 3,500 researchers strive to invent the digital technologies of the future. Educated at leading international universities, they creatively integrate basic research with applied research and dedicate themselves to solving real problems, collaborating with the main players in public and private research in France and abroad and transferring the fruits of their work to innovative companies. The researchers at INRIA published over 4,450 articles in 2012. They are behind over 250 active patents and 112 start-ups. The 180 project teams are distributed in eight research centers located throughout France.

TEA (Time, Event and Architectures) is a new INRIA project-team created in 2015 at INRIA-Rennes and IRISA. TEA investigates time and quantitative reasoning in embedded system design, and to put it to practice by revisiting analysis and synthesis techniques for real-time system design with the compositionality gained from that formalization. In this aim, TEA seeks applications to verification, synthesis techniques, and to virtual integration: to accurately simulate a system based on models of its physical and digital components by using formal analysis.

Context of the PhD:

To meet commercial pressure, engineers need to develop systems in shorter time. On the contrary, to meet greater customer expectations or simply safety or regulatory constraints, the requirements on overall system quality are higher. Introduction of software has added a lot of flexibility to system design, allowing fulfilling partially the previous needs. However, industrial systems are more and more complex, being built from not only specific parts but also COTS (Components of the Shelf), mixing physical and software parts, etc. For example a factory automation system is made of pre-made computing modules called PLC (Programmable Logic Controller), connected to actuators and detectors and interconnected to each other. Each PLC module should be programmed in such a way that the overall production chain makes a coherent action (e.g. peek a piece of equipment by a robot, put it on a machine, after machine processing, put back the piece of equipment on a trolley, etc.), while fulfilling global safety and time requirements. Moreover, to face rapid requirement changes and to be more efficient, more iterative system building are needed, where some properties of a system or sub-system are assumed but might be changed in future version of the architecture and design.

This increased complexity of system building makes the current approach more and more difficult. A possible solution would be to use a suitable method and tools that ensure Correct-by-Construction system architecture, design and implementation. In other words, the properties to fulfil are intrinsically weaved into the system during its construction. In this perspective, a promising way is the notion of "contracts". At any point of the system, e.g. module or component interface, one describes the expectations of both sides of the interface: the provider of the interface describes the provided service under needed requirements – pre-conditions – while the caller of the interface promise to fulfil those requirements with the guarantee to obtain the provided service – post-conditions. Such a contract can be both written by the end-user and generated by the development environment.

Formal Methods also offer promising solutions to several of above issues by ensuring exhaustive verification of some properties.

While being considered for a long time, the recent progresses on computer efficiency as well as on algorithmic aspects make the formal methods more and more practical to ensure Correct-by-Construction system building even if end-users are not formal methods specialists.

However the full potential of formal approaches can only be reached if the Mathematics is hidden behind tools and graphical user interfaces.

Research proposal:

The goal of this PhD proposal is to investigate contractual approach to cyber-physical system design and design a compositional framework to modularly specify non-functional constraints of system components, such as physical, thermal, power and time constraint. We want to demonstrate the use of that framework by defining a methodology and developing functionalities to ensure design correctness by construction. In particular, we are interested in the verification of global requirements: end-to-end latency, power demand, system throughput, real-time schedulability; or in exercising simulation: validation of scenarios, faults injection.

The proposed framework will be applied and validated to the case for factory automation. A factory automation system is best characterized by global, environmental, requirements (plant size, power delivery, throughput), which have to be met by the assembly of components, each contributing by assumptions on the environment, and by promises on their contribution by the satisfaction of a contract to a common requirement.

An anonymised, industrially realistic, case study will be designed in the frame of the PhD to support and validate the method and tools developed in the context of the project.

Our primary research topic will be materialized by the design of a DSL to formalize the data-flow network of plants together with contracts pertained to the required and guaranteed resources: mechanical, electrical, temporal …

The nature of these constraints in the frame of factory automation advocates their linear approximation, when applicable (e.g. real-time) or, more generally (continuous constraints) to make them amenable to abstracted reasoning within SAT-SMT verification technologies (Z3, dReal), to favor efficient decision over specification details.

The natures of factory automation architectures strongly suggest data-flow networks as a main modeling concept, possibly adjoined with automata to describe mode of operations. Building our framework hence relies on a large corpus of related works in data-flow network theory, scheduling theory, contract theory and SAT-SMT verification.

In the iterative process of a contract-based design methodology, all contracts in an entire system under design may not be consistent at all times. Contracts are used in two ways:

- Top-down, to ensure that the contract of a component is fulfilled under the pre-conditions assumed about its parent environment
- Bottom-up, to check parent properties provided that the component post-conditions are fulfilled.

A meet-in-the-middle design process iterates design validation by modularly checking either of the above. It is sustained until the entire system architecture is eventually validated. If it cannot, a counter-example is produced to help identify the faulty interaction between components.

Once contracts are formally verified, they must be compiled in a form that is natural enough to be understood by domain experts for validation. The same approach to validation may apply to other than system-level level requirements (throughput, etc.) either component-level (third-party equipment) or systems-of-systems (a plant).

Ultimately, validated contracts can serve the production of traceability documents as well as the documentation of the architecture and design.

Then, at design-level, the purpose of contracts is to closely specify component implementations. Arguably, it hence needs to relate with secured system-level properties by the use of abstraction-refinement mechanisms: e.g. “gluing” invariants, as well as automated inference techniques.

Combining the two points of views, one of the research axes would be to provide to the user an environment where he can put contracts at various points of the system and use them to prove (i) that stated properties are indeed fulfilled under sub-module contract assumption, the environment inferring missing contracts along the module hierarchy, and (ii) that sub-module contracts can be proved using knowledge of component internal design or assumption about external sub-systems (physical process, legacy software, operating system, etc.). The proposed approach should be fully automatic in order to be usable in an industrial environment. In case the contract cannot be fulfilled, the environment should pinpoint the issue and proposes solution (e.g. relaxing constraints on the sub-module and strengthening constraints on another one for example). In case of architectural or design changes, the environment should help rapidly determine if the old and new constraints are still fulfilled or not.

Organization / supervisors:

The thesis is within the scope of a CIFRE collaboration with INRIA. Most of the work will be conducted in INRIA under the supervision of TEA project team. The work will make use of the facilities available on the campus of INRIA. The position includes regular visits to Mitsubishi Electric R&D Center Europe in Rennes very close to INRIA Rennes.

Supervisors:
Jean-Pierre Talpin (INRIA)
David Mentré and Benoît Boyer (Mitsubishi Electric R&D Centre Europe)

Essential qualifications / personal profile:

- Recently graduated Engineer or University Master with a background in formal methods or Mathematics
- Fluent English
- Excellent communication skills
- Motivation and dynamism to work in a research environment
- Open-mindedness, capacity to work in a multicultural and international environment

Please send CV and motivation letter by email (indicating in object: your name + reference of the offer) **to both following contacts**:

jobs@fr.merce.mee.com.

Jean-Pierre.Talpin@inria.fr

Deadline to apply: 15 July 2015

References:

"A Tutorial on Satisfiability Modulo Theories" L. de Moura, B. Dutertre, N. Shankar. International Conference on Computer Aided Verification, LNCS 4590, Springer, 2007.
http://yices.csl.sri.com/papers/cav2007.pdf

"Contracts for System Design". A. Benveniste et al. INRIA Rsearch report n°8147, 2012.
http://people.rennes.inria.fr/Albert.Benveniste/pub/RR-8147.pdf