Proposition de recherche doctorale

Formal certification of real-time implementations

Mots clés :

- **Directeur de thèse** : Dumitru POTOP-BUTUCARU
- **Co-encadrant(s)** :
- **Unité de recherche** : INRIA-Paris
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Research context: 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 startups. The 180 project teams are distributed in eight research centers located throughout France. The AOSTE research team (http://www.inria.fr/en/teams/aoste) promotes the use of synchronous formalisms for the high-level modeling, the full formal design, and the distributed real-time implementation of embedded software. The team builds upon prior work by its members on the SyncCharts, Esterel, and SynDEx formalisms, which included extensive algorithmic studies on dedicated modeling, compilation, analysis, and optimization techniques. Our main expertise is in the fields of formal semantics of synchronous reactive systems, and optimized mapping (i.e. distribution and scheduling) between application algorithms and physical architectures descriptions. The position is funded by the ITEA3 Assume collaborative project (https://itea3.org/project/assume.html). Assume proposes a set of methods and tools for the synthesis of correct and efficient parallel software. The common denominator of these techniques is formalization and full automation. The technical focus is placed on formal compiler verification and on correct real-time implementation for parallel applications. In both cases, hardware modeling is recognized as a major issue and dedicated specific attention. Work will be done in collaboration with the GALLIUM research team (http://www.inria.fr/en/teams/gallium). Topic description: To this day, the design and implementation of industrial real-time systems has remained to a large extent a craft, involving significant manual phases. Automation is only possible when design needs are formalized and standardized, to allow cost-effective tool building. But automation can no longer be avoided, as the complexity of systems steadily increases in both specification size (number of tasks, processors, etc.) and complexity of the objects involved (dependent tasks, multiple modes and criticalities, novel processing elements and communication media...). Fortunately, the standardization of specification languages (Simulink, Scade...) and of implementation platforms (AUTOSAR, ARINC653...) is today advanced enough that fully automated implementation is attainable for industrially significant classes of systems. The AOSTE team actively develops (among other tools) the Lopht real-time systems compiler [2,3] which allows fully automated multi-processor implementation of embedded control specifications with complex functional and non-functional properties. Lopht target s systems using static (off-line) or time-triggered real-time scheduling. Such systems are used in safety-critical systems (avionics, automotive, rail), such as those considered by the Assume project. The objective of this PhD thesis is to formally prove the correctness of (part of) the automatic code generation technology of Lopht. The main focus of our work will be on the formal verification of compilation techniques ensuring the respect of non-functional requirements, and in particular real-time requirements such as release dates, deadlines and periods. The result will be an extension of the CompCert methodology [1] to the embedded system level, taking into account non-functional requirements.

Résumé du projet de recherche (Langue 2)

The difficulty of this endeavor comes from the fact that proving the real-time correctness of a system necessarily involves detailed semantic knowledge on all system components and its implementation process. Structurally, a real-time system consists of three layers, with a specialized "basic software" layer (drivers/middleware/OS) providing the interface between the application layer and the physical architecture on which it runs. The real-time implementation chain mitigates, from the time domain perspective, the interactions between these three layers. For example, the semantics of the application running in the presence of the underlying architecture can be analyzed to compute worst-case execution time (WCET) bounds. The real-time operating system, approximated by a scheduling mechanism and driven by additional real-time constraints, maps the application on the architecture, introducing further timing overheads that must be taken into account. The PhD student will start by formally modeling the application software (which has a coarser, task-level grain, as opposed to existing representations used in compiler certification) and the execution platform (hardware and basic software). We will consider execution platforms identified as representative by the Assume project (Kalray MPPA 256 and simple multi-cores on the hardware side, bare metal and ARINC 653-based on the software side). Using the resulting models, the PhD student will then incrementally prove the compilation algorithms of Lopht. He/she will start with the real-time scheduling algorithm, with optimizations switched off. The PhD student will then consider various optimizations and also code generation algorithms such as the synthesis of communication and synchronization. The work will combine program proof and translation validation techniques, using the Coq proof assistant for specifications and proofs.

Informations complémentaires (Langue 1)

The work will take place in the European ITEA3 Assume collaborative project (https://itea3.org/project/assume.html).

Informations complémentaires (Langue 2)

Prerequisites: MSc degree in Computer Science or Computer Engineering, or equivalent. Good academic record. Previous exposure to formal modeling and/or verification techniques, concurrency theory, real-time systems, or compilation is considered a plus. Location: The successful candidate will join the AOSTE Research Group at INRIA Paris: http://www.inria.fr/centre/paris-rocquencourt http://www.inria.fr/en/teams/aoste References: [1] X. Leroy. Formal verification of a realistic compiler. Communications of the ACM, 52(7):107-115, 2009. [2] D. Potop-Butucaru, R. de Simone, Y. Sorel, and J.-P. Talpin: Clock- driven distributed real-time implementation of endochronous synchronous specifications. In Proceedings EMSOFT'09, Grenoble, France. [3] T. Carle. Efficient compilation of embedded control specifications with complex functional and non-functional properties. PhD thesis. http://www.theses.fr/2014PA066392 .