2019-01509 - PhD Position F/M Adaptive Fault-Tolerant safety-critical systems on multicore Architectures

Type de contrat : CEO de la fonction publique
Niveau de diplôme exigé : Bac + 5 ou équivalent
Fonction : Doctorant

A propos du centre ou de la direction fonctionnelle

The Inria Rennes - Bretagne Atlantique Center is one of Inria's eight centers and has more than thirty research teams working on recognized projects in the field of digital sciences. It is at the heart of a rich R&D and innovation ecosystem: highly innovative PMEs, large industrial groups, competitiveness clusters, research and higher education players, laboratories of excellence, technological research institute, etc.

Mission confiée

Context

The embedded systems in safety-critical domain industries must provide guarantees on safety and reliability, especially for critical applications, ensuring both fault tolerance and hard real-time constraints. On top of the system hard timing requirements, natural and technical sources from the environment can cause faults that impact the system functionality [1]. Examples of such systems can be found in: i) the avionics domain, e.g. the fly-by-wire system requires compliance with the Design Assurance Level (DAL) standard, while it operates in high altitude and is exposed to radiation [2], ii) the space domain, e.g. the navigation system that operates under extreme particle and high-energy electromagnetic radiation [2], and iii) the automotive domain, e.g. the automatic braking system suffers from alpha particles, high temperature peaks and electromagnetic interferences [3]. These systems also face exponential growth in performance requirements [4], which has led the processor manufacturing industry towards multicore and manycore architectures. While such architectures can successfully meet the demands for the majority of computing systems, the same cannot be stated for safety-critical systems [5] that require timing guarantees. No established approach exists yet to achieve safety certification on multicore architectures [6], especially due to two main scientific challenges: non-deterministic timing behaviour and fault susceptibility.

The first challenge comes from the sharing of resources among cores in multicore and manycore architectures, e.g. the interconnection network on chip, memories and controllers. Parallel execution of applications on the same platform leads to potential concurrent accesses to the shared resources. These concurrent accesses introduce interferences and timing delays highly affecting the application’s timing behaviour in a non-deterministic way. To preserve a deterministic timing behaviour, either spatial and temporal isolation is enforced or Worst Case Execution Time (WCET) bounds are over-estimated. In both cases, the result is a sub-optimal use of resources. The former solution over-provisions the resources to the critical applications [14]. The latter solution has to consider the worst-case during WCET estimations: at every access to a shared resource by a core, it is assumed that the remaining cores access the same resource at the same time. Consequently, the WCET estimations are overly pessimistic. The additional processing capacity provided by the multicore is negated by the WCET pessimism [5]. To reduce the impact of the WCET pessimism, run-time approaches are expected to achieve significantly higher gains than design-time ones, because they can take advantage of the real information during execution [7].

The second challenge is that a multicore platform is susceptible to faults due to the nature of electronic systems. In electronic systems, the variation on the threshold voltage depends on the transistor width, whereas voids or small cracks in the wiring lead to close or open circuit problems. The current and voltage activity and the hot spots are inevitable during the system operation, but they create sources of faults, such as circuit aging-wearout and electromagnetic interferences [8]. With the reduction of the transistors size, e.g. 6/5nm technology is expected in 2021 [10], the multicores are becoming more and more sensitive to the operating and the environmental conditions [9]. To improve the multicore reliability, either radiation-hardened processors are used or the software and/or hardware are replicated. The former solution develops processors that are significantly slower than the regular ones [11], while it requires a hard-to-find design expertise that combines digital and
analogue electronics with semiconductor physics. The latter solution is costly as it usually implies high performance and area overhead [12]. To avoid the system overdesigning, while dealing with the fault, resource and application changes occurring during the system operational life, the means to provide reliability must be adaptive [13].

The goal of this thesis is the exploration and the development of run-time adaptation to establish safety and reliability in many/multi-core platforms exploring the trade-offs between (un)predictability, (un)safety and system performance. More precisely, to achieve run-time adaptation, it is required to design low cost monitors, to observe the execution and the occurring faults, and run-time control mechanisms, to adequately adapt the system. The adaptation schemes will include different fault tolerant hardware/software approaches and potential reconfigurations of the system in order to provide guarantees with respect to timing and safety requirements and a near-optimal design for the application trade-offs. To achieve low cost run-time mechanisms, several design options must be analysed during the design phase in order to provide as much as possible information to the run-time mechanisms, so as to act with low overhead. The analysis will focus on the most important design metrics, such as the gain in the quality of service, the overhead of the techniques for fault tolerance and for the predictability guarantee (with respect to time and energy consumption), the better utilization of the resources and the percentage of faults detected/corrected.

Bibliography


Principales activités

Main activities:
- Study existing work on run-time adaptation approaches for safety and fault tolerance.
- Analyse the trade-offs and constraints wrt the application requirements (quality of service, fault tolerance, predictability) and cost (performance, area, energy consumption)
- Propose novel solutions and methodologies for run-time adaptation.
- Implement the proposed solutions to a multicore architecture. At the core level, the core IP (e.g. RISC-V) will be extended to provide the required monitoring and adaptation means and at the system level, the multicore architecture will be extended to support the proposed run-time adaptation mechanisms.

Additional activities:
- Present the results at conferences and workshops.

Compétences
Working experience in the areas

- Strong knowledge of computer and system architecture
- Strong programming skills (C/C++, Hardware Description Languages, High Level Synthesis)
- Working experience in the areas of Worst Case Execution Time and fault tolerance is an advantage

Languages and skills:

- Very good communication skills in oral and written English.
- Open-mindedness, strong integration skills and team spirit.

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage