PROBABILISTIC REAL-TIME CONTROL OF MIXED-CRITICALITY MULTICORE AND MANYCORE SYSTEMS

PROXIMA

Key innovation

In the next decade, EU industries developing Critical Real-Time Embedded Systems (CRTES), safety-, mission- or business-critical, will face a once-in-a-life-time disruptive challenge caused by the transition to multicore and manycore platforms. The opportunity therefore arises to integrate multiple applications onto the same hardware platform accruing significant advantages in performance, production costs, and reliability. Yet a serious threat rises relating to a key problem in CRTES; the need to ensure that timing constraints will be satisfied during operation. With the advent of multicore and manycore platforms, the complexilyt of interactions between cores and software applications rises to make incremental analysis much harder and software timing analysis far more costly, complex and risky.

PROXIMA asserts that the timing behaviour of mixed-criticality CRTES executing on multicore and manycore platforms can be analysed effectively via innovative probabilistic techniques. PROXIMA defines new hardware and software architectural paradigms based on the concept of timing randomisation. It extends this approach across the whole execution stack underneath the application to ensure that the risks of pathological timing overruns are reduced to quantifiably low levels. PROXIMA builds a comprehensive suite of probabilistic analysis methods integrated into commercial design, development, and verification tools, complemented by appropriate arguments for certification. PROXIMA provides a complete infrastructure; harnessing the full potential of new processor resources, demonstrating and supporting effective timing analysis, bringing the probabilistic approach to a state of technological readiness, and priming four EU industry sectors in its use.

Technical approach

As computing hardware becomes more complex, incorporating features such as multilevel caches and multicore and manycore hardware architectures, the challenges of providing trustworthy timing analysis become harder because of the rising complexity of the hardware and software interactions. The principle of probabilistic timing analysis (PTA) is that (if specific conditions are met) we can look at the timing behaviour and provide a probability distribution of an upper bound of its timing properties.

The project introduces time-randomization to complex hardware and software. For example, the use of a random replacement cache instead of a conventional LRU cache means that although at the low level you cannot determine absolute behaviour, at the application level you can have a solid,

Contract number
611085

Project coordinator
Dr Francisco J. Cazorla

Contact person
Francisco J. Cazorla
Barcelona Supercomputing Centre
Computer Architecture Operating Systems Group
c/ Jordi Girona 29, 2a Pl. Ed. Nexus
08034 Barcelona, Spain
Tel: +34 93 413 71 73
francisco.cazorla@bsc.es

Project website
www.proxima-project.eu

Community contribution to the project
4,650,000 Euro

Project start date
1st October 2013

Duration
36 months

mathematically sound, predictable emergent behaviour. Similarly for multicore and manycore architectures, randomized arbitration on access to shared hardware resources can be provided. Software-only techniques that employ compiler and operating system (OS) support are applied on COTS hardware, using techniques such as linker-supported memory allocation and object placement.

Incremental software qualification rests on composability, and timing composability is supremely difficult to achieve without resorting to potentially uneconomic overprovisioning. The Real-Time OS, as the place of mediation between the application and the processor hardware, has a most useful role to play in the quest for effective timing composability. While being neutral to the model of computation in place at the application end, the RTOS should use every opportunity, by design and operation, to ensure that the response time incurred by the application software on access to platform resources is provably free of dependence on execution history, which is known to break timing composability. PROXIMA will pursue this goal in the challenging context of modern, performance-aggressive multicore and manycore processor platforms.

Worst case execution time analysis tools to support these architectures are being developed, to enable automated test and timing analysis solutions. We use existing RapiTime technology with PROXIMA extensions to measure and predict the worst case execution time bounds and a distribution of execution times showing the probability of timing failure.

Demonstration and Use

The PROXIMA technology will be trialled and demonstrated in four key industries: aerospace, rail, automotive and space. Four different demonstrable platforms will be produced: a multicore FPGA, two COTS multicore processors, and a manycore simulator. These platforms will be used to support the evaluation of the industrial benefits on industrial applications provided by all the industrial partners and the members of the industrial advisory board.

The strong industrial focus of the project including end users (Airbus, Astrium, Ikerlan) with OS, tool and hardware suppliers (SYSGO, Rapita, Aeroflex Gaisler, Infineon) provides a solid and strong route to commercialization of the leading research being done within the project.

Scientific, Economic and societal Impact

There are many challenging scientific issues to address in this field of research which will have a direct industrial impact. The European critical embedded real-time industry will benefit by being able to embrace new multicore technologies becoming commonplace without compromising safety and reliability, leading to an increase in available processing power with lower size/weight/power. In 10 years, we cannot imagine multicore platforms being used efficiently in CRTES without techniques like PROXIMA, and the project partners aim to be the leading supplier of probabilistic timing analysis solutions.

Project partners	**Country**
Barcelona Supercomputing Center	Spain
Rapita Systems Ltd	United Kingdom
SYSGO SAS	France
Universita degli Studi di Padova	Italy
Institut National De Recherche en Informatique et en Automatique (INRIA)	France
Cobham	Sweden
Airbus Operations SAS	France
University of York	United Kingdom
Airbus Defence and Space	France
IKERLAN S.Coop.	Spain
Infineon Technologies UK Ltd	United Kingdom

Key Features

- Enable complex multicore platforms to be used in critical real-time systems
- Industrialization of research for use in Aero/Auto/Space/Rail markets
- Reduce size/weight/power through use of multi/many cores
- Reduce verification and certification costs of real-time software