4 How will tool support be provided?

New industrial tools for development, deployment and verification are being provided during PROXIMA to support the PTA techniques.

ANALYSIS TOOLS

Rapita Verification Suite (RVS) from Rapita Systems Ltd is an industrial tool suite reducing the cost of timing analysis, measurement, optimization and verification of software in critical real-time systems.

PROXIMA is developing an enhanced version of RVS with the probabilistic worst case execution time analysis features of PROXIMA to support the new PTA-compliant hardware and software architectures to provide automated test and timing analysis solutions. RVS supports a number of multicore COTS platforms including P4080, LEON, AURIX and the enhancements from PROXIMA will enable even more accurate and reliable software timing analysis.

HARDWARE

The Next Generation Microprocessor (NGMP) is a quad-processor device that is currently in development at Cobham Gaisler under a contract from the European Space Agency. The changes made in PROXIMA to modify the processor support the time-randomization for PTA compliance in hardware will be immediately available for transfer to the NGMP.

Cobham Gaisler provides an IP library consisting of the LEON microprocessors and peripheral units. Companies, both in the space and consumer electronics markets, license this IP library to develop their own system-on-chip designs. The hardware modifications made to support the time-randomization for PTA compliance will be available as part of this IP library. Availability of PTA compliant hardware building blocks can allow quicker adoption of the developed technologies

OPERATING SYSTEMS AND DEVELOPMENT ENVIRONMENT

PikeOS incorporates the latest paravirtualization technology, making PikeOS a unique combination of real-time operating system and hypervisor. PikeOS directly solves issues like hardware convergence, legacy software migration, IP protection and how to use Linux in secure and safety-critical environments.

Within the PROXIMA project PikeOS is being enhanced to use the PTA results in the worst case execution time computation of its native and ARINC 653 guest OS services. This will allow achieve higher levels of time composability and be certifiable to the highest level of criticality.

SYSGO is extending the Eclipse-based IDE and graphical configuration tool “CODEO” to use PTA results in the worst case execution time computation of PikeOS services, helping the integrator to set a valid configuration in a mixed criticality context that aims to use available powerful hardware features.

5 What impact is PROXIMA expected to have?

As well as a significant impact within the project partners, PROXIMA will have a wider scientific, economic and societal impact in Europe, changing the way that we think about critical real-time software.

The overall technical objective of the PROXIMA project is to achieve an industrial implementation of probabilistic analysis techniques to enable the use of modern COTS multicore hardware for real-time applications. This will make the use of high-performance hardware possible for critical systems, allowing the highly complex needs of the future reliable software systems to be achieved at lower cost and with improved size, weight and power performance.

The strong industrial focus of the project including end users (Airbus, Astrium, Ikerlan) with OS, tool and hardware suppliers (SYSGO, Rapita Systems Ltd., Cobham Gaisler, Infineon) provides a motivated and strong route to commercialization of the leading research being done within the project. 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 embrace new multicore technologies as they become 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 critical real-time systems without techniques like those developed in PROXIMA, and the project partners aim to be the leading suppliers of PROXIMA technologies.

PROXIMA
www.proxima-project.eu

Coordinator: Dr Francisco J. Cazorla francisco.cazorla@bsc.es
Barcelona Supercomputing Centre, Computer Architecture Operating Systems Group,
c/ Jordi Girona 29, 2a Pl. Ed. Nexus, 08034 Barcelona, Spain
PROXIMA is a funded Framework 7 programme of the European Commission
Project ref: 611085
Start Date: 1/10/2013 **End Date:** 30/9/2016
Project Cost: 6,794,887 Euro **Project Funding:** 4,650,000 Euro

PROXIMA

Probabilistic real-time control of
mixed-criticality multicore and manycore systems

PROXIMA Use Cases

The PROXIMA project is working to enable the use of modern multicore and manycore systems in critical real-time embedded systems. Its aims are to enable incremental development of real-time software on multicore processors and increase the performance of applications on complex multicore processors by using advanced probabilistic timing analysis based on time-randomization of software and hardware features.

This brochure describes the intended use cases of the PROXIMA project and answers the following questions:

1. What is PROXIMA?
2. Who are the PROXIMA partners?
3. How are the findings from PROXIMA being applied?
4. How will tool support be provided?
5. What impact is PROXIMA expected to have?

1 What is PROXIMA?

PROXIMA is a research project that will increase software performance in critical real-time embedded systems using advanced multi/manycore processors with cache memory.

PROXIMA will use probabilistic timing analysis (PTA) techniques to enable software components to be developed for complex multicore hardware in critical systems. Software components can be developed individually to a high safety standard and then composed into a larger system containing multiple components on a multicore or manycore architecture.

The project introduces time-randomization to complex hardware and software; this allows systems to be analysed using PTA techniques. For example, the use of a random replacement cache instead of an LRU cache means that although at the low level you cannot determine absolute behaviour, at the level of the application you can have a solid, mathematically sound, predictable emergent timing behaviour. Similarly for multicore and manycore architectures, randomized access to shared resources can be introduced. Software-only randomization techniques through compiler and operating system support are used on COTS hardware. The new PTA techniques can then be used to determine worst case execution times with lower effort and more accuracy.

Achieving credible timing analysis, incremental development and time-composable software is becoming harder because of the complexity of understanding interactions between cores, applications and hardware features. PROXIMA provides a novel method for the design, verification and integration of software components that will change the way that we work with critical software in the European Aerospace, Automotive, Rail and Space industries.

2 Who are the PROXIMA partners?

The PROXIMA project is driven by the industrial focus of the project partners, including high profile industrial leaders in the EU.

The industrial partners will provide suitable systems for evaluation and testing of the PROXIMA technology from their respective sectors: Airbus (avionics), Infineon UK (automotive), Airbus Defence and Space (space), IKERLAN (rail). Rapita Systems Ltd will support the multicore and manycore architectures with its RapiTime timing analysis tool, SYSGO will provide PikeOS operating system support for the timing analysis techniques, and Cobham Gaisler will provide a hardware architecture implementation. The research partners (Barcelona Supercomputing Centre, University of Padua, INRIA and the University of York) will contribute their in-depth understanding in the areas of statistics, simulation, operating systems, scheduling, worst case execution time, real-time systems software, and multicore architectures.

An Industrial advisory board (IAB) made up of high profile key industrial end users from across the EU reinforces the project's industrial focus, and provides additional avenues for the dissemination and exploitation of results. The IAB has a particular focus on automotive, including several automotive OEMs and Tier 1 suppliers.

PROXIMA Consortium

PROXIMA Industrial Advisory Board

3 How are the findings from PROXIMA being applied?

Avionics

Mixed-criticality software in avionics is common, whether on computers hosting a single aircraft system, such as a flight control system, a data concentrator and gateway function; or Integrated Modular Avionics computers that host multiple aircraft systems that can have different criticalities.

Software timing analysis of these systems is hard, and becomes harder as hardware becomes more complex and less specific to avionics needs. Probabilistic timing analysis will help in reducing analysis effort especially for multiprocessors, reduce the amount of knowledge necessary for conducting an analysis, and provide a range of confidence levels that can be adjusted to the criticality of each avionics computer system.

USE CASE: FLIGHT SYSTEMS

The avionics case study that will be used in PROXIMA will involve the integration of different applications on two multicore platforms and associated system software stacks. Applications will be based on relevant extracts from existing avionics applications running on an ARINC-653 compliant RTOS. The applications listed are:

- Primary Flight Control Software extracts (DAL-A);
- Extracts from the IO Multiplexer (IOM) Gateway function (DAL-A);
- Flight Control Data Concentrator (FCDC) IMA application (DAL-B);
- Weight and Balance Backup (WBBC) IMA application (DAL-B).

Airbus expects from PROXIMA a way to analyse the timing of multicore mixed-criticality systems, enabling conformance with the objectives of robust partitioning and incremental qualification. Software-only time-randomization techniques are applicable to some COTS processors. Therefore, PROXIMA will be one of the very few viable timing verification techniques of tomorrow, filling a need that the avionics industry just cannot make go away.

Automotive

For many automotive applications, single core controllers are still sufficient for application needs. However, for performance driven applications, for example powertrain control (whether electric motor or internal combustion engine) the move to multicores is driven by the need to keep power dissipation low. While a faster uniprocessor is technically possible, this would usually exceed power dissipation limits for passive (rather than active) cooling. In addition, integration of previously separate single core applications onto a multicore ECU is increasingly common for cost reasons. Together these two factors account for the rising deployment of multicores into automobiles.

When moving to a multicore controller, if any component of the integrated applications has safety aspects, then the new automotive software safety standard ISO26262 must be achievable, requiring isolation and freedom from interference for the safety tasks.

USE CASE: ELECTRIC MOTOR CONTROL

The automotive case study involves the hardware and software from a control module for an electric motor in hybrid or fully electric vehicles. The Hybrid Kit for HybridPACK™2 is made up of two PCBs (Driver Board and Logic Board) mechanically and electrically suitable for use with an IGBT Module (Insulated-gate bipolar transistor), a DC-bus capacitor and a cooler. All these components build a complete main inverter for electric vehicle applications up to 80kW.

The software is basically a control loop, with additional interrupt servicing, running on a single core of the AURIX TC277 Microcontroller. In addition to the control routine, other tasks will be running on the other two cores of the TC277. The analysis of worst-case execution time of the main routine in the presence of these sources of temporal variability is the key outcome for the use case.

Space

In space software, validation is done incrementally such that the validation of one software component is not sensitive to the addition of another software component, but the current validation process cannot scale to multicore processors because of the lack of timing isolation necessary to deal with the inter-core interference.

The goal of the space case study is to ensure that the incremental validation process will still be possible when going to multicore using the PROXIMA technology.

USE CASE: PAYLOAD APPLICATION

The Space case study selected for PROXIMA will integrate a control application and an image processing application. Generally, these would be validated all together at the higher level of criticality. The objective of the case study is to show that the technology developed in PROXIMA can be used to deal with the timing interference caused by the other applications of different criticality running on the same hardware.

The study will provide a payload application combining requirements for the high processing performance of a multicore with mixed-criticality components: high criticality for the control application and low criticality for the processing application. The control application is robust to functional misbehaviour of the image processing application. However the temporal interference caused by a malfunction in the image processing application could affect the timing of the high criticality control application. On a multicore, this temporal isolation cannot be guaranteed only by design of the applications; it is also necessary that the hardware and OS have time composable properties to avoid the propagation of timing errors from low criticality to high criticality applications.

Railway

The number of functional and safety applications continues to increase in the railway domain, but the computation power of the single core processors/DSPs is limited. Adding new processors and their associated high speed communication buses leads to reliability and availability issues (e.g., material reliability, EMC, etc.) and to future scalability limitations.

The use of multicore processors under mixed-criticality constraints in conjunction with the industry ready PTA technology developed in PROXIMA project will contribute to the increase in reliability and availability of future generations of trains, which integrate different subsystems on a single chip.

USE CASE: ON-BOARD RAILWAY SIGNALING

The European Train Control System (ETCS) standard requires SIL-4 safety integrity for the on-board railway signaling applications according to the EN-50128 safety standard. The target of this safety-critical use case is to ensure that the speed of the train does not exceed the previously defined speed limits for the current track.

USE CASE: TRACTION POWER INVERTER CONTROL

The traction of the train is obtained by the control of power switches with strict real-time requirements with execution period below 1 millisecond. Within the period, the execution loop must capture electrical parameters (e.g., currents, voltages), execute the control algorithm and command the power switches accordingly.