PROXIMA DREAMS Contrex

EUROPEAN MIXED-CRITICALITY CLUSTER

TACKLING FUTURE CHALLENGES IN THE DESIGN AND DEVELOPMENT OF MIXED-CRITICALITY MULTICORE SYSTEMS

EDITORS

Francisco J. Cazorla, IIIA-CSIC and Barcelona Supercomputing Center
Roman Obermaisser, University of Siegen – DREAMS Project
Kim Grüttner, OFFIS e.V. – CONTREX Project

GRAPHIC DESIGN

Albert López, Barcelona Supercomputing Center
Cristian Opi, Barcelona Supercomputing Center
Núria Masdéu, Barcelona Supercomputing Center

CONTACT

Barcelona Supercomputing Center - Dissemination
email: dissemination@bsc.es
phone: +34 93 413 77 16

BSC Barcelona Supercomputing Center
Centro Nacional de Supercomputación

Barcelona, November 2016.

EUROPEAN MIXED-CRITICALITY CLUSTER

TACKLING FUTURE CHALLENGES IN THE DESIGN AND DEVELOPMENT OF MIXED-CRITICALITY MULTICORE SYSTEMS

MIXED-CRITICALITY SYSTEMS CLUSTER

Modern embedded applications already integrate a multitude of functionalities with potentially different criticality levels into a single system and this trend is expected to grow in the near future. Further, Europe is facing a once in a lifetime challenge with the advent of multicore and the potential to integrate in a single platform system with different levels of dependability and security, known as mixed-criticality systems integration. Without appropriate preconditions, the integration of mixed-criticality subsystems based on multi- and many-core processors can lead to a significant and potentially unacceptable increase of engineering and certification costs.

The EU FP7 projects CONTREX, DREAMS and PROXIMA collaborate in a European Mixed-Criticality Cluster (MCC) and closely work together in terms of identification of future challenges in the design and development of mixed-criticality multicore systems, joint dissemination activities and, where possible, exploring techniques to attach those challenges.

MIXED-CRITICALITY CLUSTER

Contrex DREAMS PROXIMA

SEVENTH FRAMEWORK PROGRAMME

Some of the key challenges to be tackled include the combination of software virtualization and hardware segregation and the extension of partitioning mechanisms jointly addressing significant extra-functional requirements (e.g., time, energy and power budgets, adaptivity, reliability, safety, security, volume, weight, etc.) along with development and certification methodology.

Timing

The foundations for enabling integrated mixed-criticality multicores systems are mechanisms for temporal and spatial partitioning, which establish fault containment and the absence of unintended side effects between functions.

Certification

Certification is key to enable exploitation of results in certain application domains such as railways or energy.

Extra-functional properties

The specific properties that must be satisfied by embedded systems include timeliness, energy efficiency of battery-operated devices, dependable operation in safety-relevant scenarios, short time-to-market and low cost in addition to increasing requirements with respect to functionality.

Development methods

State-of-the-art model-based design methods still lack of explicit support for modelling mixed-criticality of applications. Support for spatial and temporal segregation properties at the resource allocation or platform view and for the static or dynamic application to computation, memory and communication resource mapping is required.

MCC PROJECTS IN A NUTSHELL

PROXIMA (01/10/2013 - 30/09/2016) 🌐 www.proxima-project.eu

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

PROXIMA is supporting the use of multi-core platforms in mixed criticality systems by providing increased confidence in, and lower cost of, performing software timing analysis. PROXIMA enhances timing measurement techniques, increasing confidence on multi-core timing bounds and reducing the overheads.

To achieve this, PROXIMA uses statistical techniques to predict the overall timing behavior of the software and its likelihood of timing failure. To facilitate this, PROXIMA selectively introduces randomization in the timing behavior of certain hardware/software resources.

PROXIMA has been applied to both customized hardware and COTS technologies on industrial case studies. PROXIMA has introduced a number of different analysis methods and tools and demonstrated the approach in industrial contexts. The project has had a very significant academic impact and it has further generated a large number of exploitable technologies, some of which are being applied in industry and taken to a commercial level.

Coordinator: Francisco J. Cazorla (Barcelona Supercomputing Center) ✉ francisco.cazorla@bsc.es

DREAMS (01/10/2013 - 30/09/2017) 🌐 www.dreams-project.eu

Distributed REal-time Architecture for Mixed Criticality Systems

The goal of DREAMS is to establish a mixed-criticality architecture based on networked multi-core chips. DREAMS will provide a hierarchical platform including both on-chip resources (e.g., processing cores, memory, NoCs) and off-chip resources. A fine-grained mixed-criticality integration will be supported using multiple partitions within each processor core where each partition can have a separate criticality level, including the highest criticality levels for certification. The detailed objectives are as follows:

- Architectural style and modelling methods
- Virtualization for security, safety, real-time performance, integrity in networked multi-core chips
- Adaptation strategies for mixed-criticality systems
- Development methodology and tools based on model-driven engineering
- Certification and mixed-criticality product lines
- Feasibility of DREAMS architecture in real-world scenarios
- Promoting widespread adoption and community building

Coordinator: Prof. Roman Obermaisser (University of Siegen) ✉ roman.obermaisser@uni-siegen.de

CONTREX (01/10/2013 – 30/09/2016) 🌐 contrex.offis.de

Design of embedded mixed-criticality CONTRol systems under consideration of EXtra-functional properties

CONTREX challenges to guarantee timing, power, temperature, and reliability requirements by controlling (shared) resource usage and access on the execution platform. CONTREX considers extra-functional constraints from the beginning, represent extra-functional properties in executable prototypes and include these properties into local and global scheduling and control decisions. Thus the CONTREX project targets the following objectives:

- A meta-model for the design and analysis of mixed-critical systems
- Deployment and mapping of control applications to platforms abiding extra-functional properties
- Development of a service-based power and temperature model for multi-core execution platforms
- Implementation of local and distributed power and temperature monitoring and control techniques
- Demonstration of a seamless integration of mixed criticalities under consideration
- Feedback to standard and certification bodies in the area of model-based mixed-critical system design

Coordinator: Kim Grüttner (OFFIS e.V.) ✉ kim.gruettner@offis.de

Multi-core Consultancy (Barcelona Supercomputing Center – Rapita Systems ltd)

Description

Multicores are becoming the standard computing-platform for real-time industry. Yet multicores bring difficulties to software timing analysis. In particular, contention in the access to hardware shared resources is challenging for timing analysis, including the measurement-based timing analysis extensively used in industry.

BSC and Rapita have entered into a partnership and framework agreement to support the provision of consultancy to examining timing analysis of multicores. BSC's expertise in multicore contention analysis and its micro-benchmark technology to expose pathological timing behavior together with RapiTime, part of the widely-used Verification Suite (RVS) will be used to analyze the timing behavior of multicore processors and will be the basis of this consultancy.

Impact

This technology is ready for exploitation in different real-time domains with a small tailoring effort required to adapt it to the specific multicore processor in consideration. It can be shown to interested customers. At the time of speaking, several confidential aerospace customers have been identified which are identified in this technology.

✉ Contact information: ianb@rapitasystems.com, francisco.cazorla@bsc.es

LEOPARD: A LEON multicore processor for Measurement-based Timing Analysis (Barcelona Supercomputing Center – Cobham Gaisler)

Description

BSC and CG have jointly developed LEOPARD, a 4-core LEON-based processor that is suitable for measurement-based timing analysis within the scope of PROXIMA. The developed processor architecture uses randomization techniques to make timing behavior of jittery resources to naturally be exposed on the platform by making several runs of the same program and consequently, releasing end-users from the burden of designing complex testing campaigns that in most of the cases cannot guarantee that the worst possible situations have been observed. LEOPARD is especially suited for the SPACE domain, where the Leon processors are widely used, and its capabilities has been satisfactorily evaluated with use cases from the European Space Agency and Airbus Defense and Space.

Impact

CG can offer their customers processor designs (and components) based on PROXIMA technology. CG is already advertising the availability of PROXIMA technology in its webpage. Furthermore, CG has plans to include PROXIMA technology in some of its future processor developments.

✉ Contact information: jan@gaisler.com, carles.hernandez@bsc.es

Knowledge Transfer Partnership for FBI-VICI Analysis (University of York)

Description

University of York has successfully received funding from Innovate UK to transfer the FBI-VICI analysis technology into Rolls-Royce for use on aircraft engines. Rolls-Royce are interested in adopting mixed-criticality systems as part of reducing their costs. In addition, Rolls-Royce are interested in using more advanced platforms and scheduling policies than they currently do. Analysis to understand the interference between tasks caused by both the software and the platform are essential to enabling this. The FBI-VICI analysis will be matured and transferred into the company to enable this.

Impact

This exploitation path offers UoY to create a product and license it to a large company within the aerospace market. For Rolls Royce, a solution to multi-core timing analysis would support their future needs on multi-core, allowing more processing capacity and a cost-effective mixed-criticality compute solution in their product.

✉ Contact information: iain.bate@york.ac.uk

Partnership to support testing tools (Rapita Systems Ltd and Sysgo)

Description

Based on the work done in PROXIMA, Rapita and Sysgo are actively strengthening their partnership to exploit the tracing capabilities and integration of RVS and PikeOS. There are at least two specific customers that are being targeted that will benefit from Rapita's RVS tool offering and its integration with PikeOS, providing timing analysis as well as code coverage and system/unit testing.

Impact

Rapita and Sysgo expect to be able to increase their business offerings and increase revenue, primarily in the aerospace industry. As key suppliers to aerospace in Europe, this offers EU Tier 1 suppliers an opportunity to reduce their testing cost.

✉ Contact information: ianb@rapitasystems.com, fva@sysgo.com

Probabilistic description to enrich model-based design to guarantee WCET estimations (INRIA, Rapita, Airbus, Sysgo)

Description

Based on the work done in PROXIMA, INRIA is today proposing a WCET estimation method for a direct integration in a (larger) model-based tool chain. French direct government funding (PIA LEOC Capacites, FUI Waruna, PIA BGLE Departs and FUI Ceos) is supporting INRIA technology transfer for the coming three years into the following:

- Waruna framework (Clearsy, Thales, RTaW, Artal) with expected integration of open source versions in Polar SYS. Rapita is included in this project as Inria sub-contracting.
- Capacites WCET estimation method on Kalray boards (Kalray, Airbus, Dassault Aviation, Airubs Helicopter, ARMINES, MBDA, OpenWide, Probayes, RTaW, Safran). Rapita is included in this project as Inria sub-contracting.
- Departs compositional approach (CS, ANSYS, Clearsy, RTaW, SNCF, Nexter) proposing compositional properties for WCET estimation.
- Ceos framework for mixed-criticality solutions for cyber-physical systems (Thales, ADS, EDF, Aeroport de Lyon, RTaW) uses probabilistic reasoning as the link between hard and soft real-time constraints necessary for the design of cyber-physical systems while satisfying timing constraints. Sysgo is included in the project as sub-contracting.

Impact

INRIA is transferring the technology through its industry partners (RTaW, ThalesRT, RPT, Sysgo) by including the WCET estimation methods to the main existing model-based tool chains. Such tool chains are used today by the main time critical embedded industry. INRIA's short-term target markets are: avionics, space, automotive and railways. Long-term targets are connected medical devices, assisted music and drones market. The creation of an InriaLab together with its industrial partners is the final step of this transfer.

✉ Contact information: liliana.cucu@inria.fr

Mixed-Criticality networking architecture and implementation

Description

The DREAMS project has facilitated the design and implementation of a mixed-criticality distributed integrated modular architecture (DIMA) for safety-critical systems based on Deterministic Ethernet. The deterministic networking platform provides the communication facilities for applications that require non-critical (e.g. infotainment), time-critical (e.g. navigation) and safety-critical (e.g. control system) data paths. This way, all communication can be integrated on the same backbone.

Impact

Networking components: The developments in the DREAMS project have led to improvements to TTTech's deterministic Ethernet networking switches and end-systems including security features, gateway features and support for the DREAMS abstraction layer for improved ease-of-use. These features are crucial in the future deployment of TTEthernet technology in environments where both safety and security play a major role and are requested to be embedded in the different system layers by TTTech's customers.

Railway impact: The DIMA platform developed in DREAMS is used in several demonstrators in the project (healthcare, avionics) and has in particular also raised the interest in the railway domain. The need for fundamentally simplified electronic architectures and a common distributed/shared embedded computing and communication infrastructure for modular integration of all safety-, time- and mission-critical, and non-critical train functions is very high on the agenda for railway OEMs, so that future trains in the next decade will be equipped with DIMA platforms built on DREAMS networking technology. A first major step in this direction has been undertaken with the start of the European Safe4RAIL project in Oct 2016 with the participation of key architecture partners from DREAMS (TTTech, University of Siegen, and Ikerlan).

✉ Contact information: arjan.geven@tttech.com

Alstom Renovables España, S.L. – Manufacturer of wind turbines

Description

Alstom turbines are equipped with an industrial controller. This controller has several different missions that can globally be categorized in production optimization, product lifetime assurance and status notification. Seen from a product safety and integrity point of view these missions have a different level of criticality, thus having also different requirements on the controller unit itself. Moreover, also in the wind industry tendencies are moving towards SIL qualification for turbine integrity related functions which have a high impact on the controller design and certifications.

By using the DREAMS harmonized platform the (SIL) qualified functions can be managed and distributed in such way that the development cycle and certification process can be short.

Impact

Using the DREAMS harmonized platform Alstom can offer better time-to-market for customer demands for safety related functions, can meet with the latest safety requirements while increasing the repair time by improving the diagnosis functions.

✉ Contact information: anton-aart.trapman@power.alstom.com

Healthcare Platform for clinical diagnostic and therapy solutions

(STMicroelectronics –Marcello Coppola)

Description

Healthcare has emerged as one of the biggest and fastest growing industries around the world. The increase in the life expectancy and ageing of the world population has a direct impact towards the expenditure on long-term care. In order to keep the health care expenditure under certain levels, in particular for hospitals; it is important to introduce appropriate solutions that enable to establish a continuum of care that encompasses genetic and dietary predisposition, risk factors, asymptomatic and active diseases. Micro technology companies ease this process by implementing innovative products, strategies and road maps that improve the means of healthcare to address specific needs and the personalization of remote services. Within this context DREAMS has developed a healthcare platform (based on the STM Body Gateway devices) that eases the clinical diagnostic and therapy solutions while also addressing the multimedia services available in modern hospitals.

Impact

STM is collaborating with San Raffaele Hospital to develop innovative solutions that enable a continuous care while targeting new levels of efficiency in healthcare system. Furthermore, STM can offer their customers the Body Gateway (and other components) based on DREAMS technologies. Last but not least the different technologies used in the healthcare platform represent a concrete path toward a successful exploitation.

✉ Contact information: marcello.coppola@st.com, mdgramma@cs.teicrete.gr

VOSYSmonitor, a low latency monitor firmware for mixed-criticality systems

Description

In mixed critical systems, a key design requirement is the consolidation of software applications, with different levels of criticality, into a common hardware platform. To meet this requirement, Virtual Open Systems has designed and developed VOSYSmonitor, a low latency monitor firmware for ARMv8-A platforms; its implementation is carried on to be compliant with ISO-26262 certification. VOSYSmonitor enables the native concurrent execution of a General Purpose Operating System (GPOS) with virtualization extensions, such as Linux-KVM, along with a safety critical Real Time Operating System (RTOS) upon a common ARMv8-A hardware platform. It provides spatial and temporal isolation of each Operating System by using the hardware security extensions called TrustZone, thus ensuring that the safety critical RTOS is isolated from any GPOS illegal access.

Impact

Although Virtual Open Systems is continuously adding advanced features to VOSYSmonitor, the component is ready for exploitation and supports already several ARMv8-A hardware platforms, such as Renesas R-CAR H3, NVidia Jetson TX1. In addition, thanks to a modular and scalable architecture, it is possible to port it on new ARMv8 targets with a minimal effort. VOSYSmonitor has been showcased to potential customers during international events such as Automotive Linux Summit 2016 in Tokyo, Renesas R-CAR consortium forum in 2016, and through face to face customers meetings. VOSYSmonitor is of interest in different market segments such as automotive, drones, industrial.

✉ Contact information: contact@virtualopensystems.com

UML-MARTE based modelling, analysis and simulation of a mixed-criticality avionics platform

Description

CONTREX provides an integrated design flow for system modelling, model-based analysis, simulation and Design Space Exploration (DSE), as well as an integrated toolset that automates many of the aforementioned activities. This way, it provides the necessary means for early assessment of system performance and efficient exploration of wide design spaces, thus enabling to find optimal configurations that minimize cost, size, weight and power consumption, without compromising safety and overall performance.

Impact

The CONTREX integrated flow has been assessed in its applicability to the tailoring of existing Flight Control Computer systems to future avionics solutions for light remotely piloted aircraft platforms, based on all-purpose commercial MPSoC platforms. A significant advance in knowledge about current techniques on analysis, modelling and design space exploration as well as a set of relevant evaluation figures have resulted from the work performed during CONTREX. Additionally, an avionics demonstrator platform has been developed to serve as prototype for future commercial avionics platforms.

✉ Contact information: mclomba@gmv.com, villar@teisa.unican.es

Insurance telematics for reduced cost of ownership

Description

Telematics boxes for vehicles mainly monitor the driver journey and his driving style. They typically include a sensing unit installed on the car for acceleration/orientation measurements, a GPS unit and a data processing and communication module. The main benefit up to now is to obtain a discount on the car insurance fee. At present, companies provide private and/or fleet vehicle drivers with a support service in case of accident. Vodafone Automotive in cooperation with the CONTREX automotive use case team extended such scenario to cover the following topics:

1. Enhanced and semi-automated accident classification and reporting, with a reconstruction of the crash dynamics.
2. Real-time analysis of driver behavior and crash severity.
3. Extraction of features on the driving style.
4. Extreme low energy requirements.
5. Recognition of low energy crashes.
6. Filtering of false positives.
7. Self-calibration of the device orientation.

Impact

It is now possible to analyze low energy crashes even when the engine is switched off for months. This is a totally new feature that is added to the Vodafone automotive product portfolio. This feature will be activated both on new products and 200k devices already on the field by the end of 2016. A complete new 1-2 years roadmap has been opened starting from CONTREX, to introduce the low energy events detection also at key-on. Improved crash management and advances in terms of power consumption, enable conceiving a black box for the motorbike. The Vodafone goal is to be the first player with a real product, with the possibility to multiply the number of customers by a factor of 2. Some members of the POLIMI team have created a startup in July 2017, to work with Vodafone Automotive on the development of a new product for the motorbike market. The algorithms for crash detection have been reused to develop a pilot product for the rally cross racing market in order to collect telemetry and crash information to be shown during a television live broadcast.

✉ Contact information: luca.ceva@vodafonetelematics.com, william.fornaciari@polimi.it

An experimentation platform for mixed-criticality avionics architectures for multi-rotor system

Description

The experimental platform consist of a commercial multi-rotor chassis with a custom designed mixed-criticality avionics hardware platform based on the Xilinx Zynq SoC. On the system, the safety-critical flight control and stabilizing algorithm and a non-critical video capturing and object-tracking algorithm are implemented. The system comes with an OVP-based virtual platform for functional and power validation of the integrated system based on a co-simulation with a flight simulator based on the CAMeLView tool.

Impact

The experimentation platform is fully extensible and can be used as a research vehicle or industrial pre-study for the assessment of future mixed-critical avionics platform. The CONTREX multi-rotor platform is used as demonstrator for different studies of mixed criticality systems in the EMC2 and SAFEPOWER project. The platform will be made fully available to the public within the SAFEPOWER project.

✉ Contact information: soeren.schreiner@offis.de, kim.gruettner@offis.de

A multiservice gateway as IoT enabling technology & Eclipse Kura IoT Platform

Description

The EUTH Minigateway is the prototype of a compact size multiservice gateway oriented to IoT and M2M application in the industrial and automotive domains. It is an industrial grade smart device targeting low cost and low power applications. It provides full support to the Kura framework for M2M platform integration and services applications. Kura IoT is a Java/OSGi-based framework for IoT gateways. It is an open-source Eclipse project and, currently the most downloaded project of the Eclipse IoT initiative. The prototype has been adopted in the CONTREX automotive use-case as a vehicle control unit in charge of controlling and monitoring the sensing devices in the vehicle, collecting/elaborating the data of vehicle crashes and storing data on the cloud.

Impact

The EUTH Minigateway prototype inspired a new family of low cost industrial grade gateways, called ReliaGate. It will be available for sale in the fourth quarter of 2016. The ESF (Everyware Software Framework) is a commercial, enterprise-ready edition of Eclipse Kura. ESF adds advanced security, diagnostics, provisioning, remote access and full integration with Everyware™ Cloud, Eurotech's IoT Integration Platform. The exploitation of R&D activities performed on Kura allowed developing a new version of ESF that will be available from the fourth quarter of 2016.

✉ Contact information: paolo.azzoni@eurotech.com

Virtual platform introduction for the development of telecommunication equipment

Description

Ethernet over Radio is part of a family of important bridging technologies that occupy a significant niche in telecom service linking and migration. Central functionalities like Automatic Transmit power Control and adaptive modulation can vary power and bitrate according to signal-to-noise ratio to provide both low-grade (e.g. POTS) and high-grade connections (e.g. emergency response). However, their highly dynamic behavior has made it difficult to capture and analyze power and thermal characteristics (an important factor in the commercial offering), leading to budget and time overruns. The CONTREX Virtual Platform has introduced a new simulation environment making it possible to obtain reliable, fine-grained traces of power and thermal evolution and iteratively perfecting these extra-functional characteristics before committing to the final platform in silicon. In addition, the simulation environment of the Virtual Platform is aiding the transition to more powerful multicore technologies used in the higher end of the wireless bridging product families.

Impact

The provision of the Virtual Platform is enabling Intecs to seek opportunities in emerging telecom markets that use adaptive transmission functionality, including Long-Term Evolution (LTE) base stations that offer wireless backhaul linking of traffic to the core network, but must offer lower power consumption to be competitive. In addition, Intecs is pursuing opportunities in the growing market for broadband introduction to Class C & D zones of Europe where fiber is considered uneconomical, but Ethernet over Radio can bridge from the core network to the street cabinet and permit reuse of the existing copper infrastructure with VDSL technologies.

✉ Contact information: silvia.mazzini@intecs.it, kim.gruettner@offis.de

Mixed-Criticality Cluster

Contrex DREAMS PROXIMA

WWW.PROXIMA-PROJECT.EU | WWW.DREAMS-PROJECT.EU | CONTREX.OFFIS.DE

THE PROXIMA, DREAMS AND CONTREX PROJECTS HAVE RECEIVED FUNDING FROM THE EUROPEAN COMMISSION'S SEVENTH FRAMEWORK PROGRAMME (FP7-ICT) UNDER GRANT AGREEMENT № 611085, 610640 AND 611146, RESPECTIVELY.