European Project Cluster on
Mixed-Criticality Systems

Salvador Trujillo§, Roman Obermaisser‡, Kim Grüttnert†, Francisco J. Cazorla‡ and Jon Perez∗

*IK4-IKERLAN, Mondragon, Spain, {strujillo, jmperez}@ikerlan.es
†University of Siegen, Germany, roman.obermaisser@uni-siegen.de
‡OFFIS – Institute for Information Technology, Oldenburg, Germany, kim.gruettner@offis.de
§Barcelona Supercomputing Center and IIIA-CSIC, Barcelona, Spain, francisco.cazorla@bsc.es

Abstract—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. Without appropriate preconditions, the integration of mixed-criticality subsystems can lead to a significant and potentially unacceptable increase of engineering and certification costs. There are several ongoing research initiatives studying mixed-criticality integration in multicore processors. Key challenges are 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. This paper provides a summary of the challenges to be addressed in the design and development of future mixed-criticality systems and the way in which some current European Projects on the topic address those challenges.

I. INTRODUCTION TO MIXED-CRITICALITY SYSTEMS

In many domains such as automotive, avionics and industrial control, the economic success depends on the ability to design, implement, qualify and certify advanced real-time embedded systems within bounded effort and costs. Strong by-design evidence is needed to build solid arguments of correctness that can satisfy certification bodies. Timing correctness as a means to guaranteed performance is one of the key dimensions of interest to qualification and certification.

In those application domains there is also a trend toward an integrated approach under which different functions, possibly attributed to different criticality levels, share the same hardware, and therefore enable the standardization and modular encapsulation of service interfaces. This is for example the purpose of the Integrated Modular Avionics (IMA) paradigm in avionics, the IMA for Space initiative taken by the European Space Agency and the architectural guidelines in the AUTOSAR initiative. The integration of multiple functions with different criticality and certification assurance levels on a shared computing platform constitutes a mixed-criticality system (MCS). Mixed-criticality systems range from lowest assurance requirements up to the highest criticality levels (e.g., DAL A in RTCA DO-178B or SIL4 in EN ISO/IEC 61508 and ISO 26162).

The adoption of multicore and manycore processors is an obvious facilitator to integrated architecture approaches, and therefore a direct contributor to achieving three advantages: reducing SWaP costs, increasing reliability and enabling advanced functionality. These benefits of multicores have extended their use in embedded systems with estimations [1] that (1) the deployment of 45% in industrial applications by 2015; and (2) up to 95% of multicores will combine cores of mixed-criticality levels. In contrast, the latest versions of processors in industrial applications employ multiple cores, but typically, only one core is used nowadays when highly critical tasks are involved.

II. CHALLENGES IN MIXED-CRITICALITY SYSTEMS

The grand challenge of the integration of mixed-criticality systems in different domains comes with a number of specific challenges. Many of them are shared across the different projects running on the topic.

A. Timing

In the time domain, 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. Physical resources can be virtualized into partitions to encapsulate resources temporally (e.g. latency, jitter, duration of availability during a scheduled access, etc) and spatially (e.g., prevent a function from altering the code or private data of another partition). Resource partitioning provides a means to achieve composability in the time dimension, which in turn enables incremental verification. This enables ascertainment of the timing behavior without considering all possible interactions that may occur among applications, containing verification costs. Resources partitioning requires different solutions at chip and cluster level and require different solutions for communication and computation resources.

B. Certification

Certification is key to enable exploitation of results in certain application domains such as railways or energy. Several projects are already working on certification in the context of mixed-criticality systems such as CERTAINTY or MultiPARTES (safety concept based on multicore partitioning over hypervisors). DREAMS will investigate novel challenges related to modular safety cases to be prebuilt and composable. PROXIMA aims at delivering evidence and arguments on its probabilistic approach usable in the certification and safety processes of several industrial domains. Overall, there is a shift in scope from individual systems to families of systems. In this context, the goal is to attain product-line certification.
C. 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. In mixed-criticality systems, isolation of partitions needs to address these extra-functional properties. For example, a low-criticality service must not affect the security, reliability or energy integrity of services with higher criticality. Furthermore, integrated resource management has to consider the criticality of services when reallocating resources (e.g., degraded service mode upon low energy). CONTREX will further analyze power, temperature, and reliability properties to include and control power and temperature segregation of compute resources and partitions on the same MPPSoC.

D. 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. To support certification a pure component model is not sufficient. Requirements need to become connected with the component model in a traceable way. To bridge the gap between the specification and implementation, proof obligations for the implementation model need should derive from the requirements of the specification model in a formal way. These requirements should be able to represent and combine functional and extra-functional aspects, like timing, power and temperature, including their interdependencies. Analysis of these aspects is a very challenging task. State-of-the-art model-checking techniques in the multi-physical domain suffer from complexity problem and non-decidability. Even validation through simulation is not straightforward, because efficient simulation techniques and new coverage-metrics to limit the number of simulation runs are required. For exploring the vast design-space of multi-physical mixed criticality systems, new design-space exploration techniques are needed to support the designer in the refinement process. Tool support is crucial, and yet only partial available.

III. Projects overview

Europe is facing a once in a lifetime challenge with the advent of multicore and the potential to integrate in a single platform systems with different levels of dependability and security, known as mixed-criticality systems integration.

There are currently several EU-funded research projects, some running and others about to start, introduced next:

A. DREAMS

Based on the strong foundation in European and national initiatives, DREAMS (Distributed RReal-time Architecture for Mixed Criticality Systems) will establish a European reference architecture for mixed-criticality systems by consolidating and extending platform technologies and development methods. DREAMS will leverage multi-core platforms for a hierarchical system perspective of mixed-criticality applications combining the chip- and cluster-level. DREAMS will deliver architectural concepts, meta-models, virtualization technologies, model-driven development methods, tools, adaptation strategies and validation, verification and certification methods for the seamless integration of mixed-criticality to establish security, safety, real-time performance as well as data, energy and system integrity. The objective of DREAMS is a cross-domain architecture supporting multiple application domains (e.g., avionics, wind power, healthcare).

B. PROXIMA

Continuing the PROARTIS STREP FP7 Project probabilistic approach to reduce timing verification and validation cost of MCS, PROXIMA (Probabilistic real-time mixed-criticality multi-core and many-core systems) pursues the development of probabilistically time analyzable (PTA) techniques and tools for multicore/manycore platforms. PROXIMA will selectively introduce randomization in the timing behavior of certain hardware and software resources as a way to facilitate the use probabilities to predict the overall timing behavior of the software and its likelihood of timing failure. To that end (1) PROXIMA will develop a tool chain including a multicore PTA-compliant processor implemented on FPGA and commercial Operating System and Timing analysis tool; (2) will develop four case studies, one in the main industrial scenarios studied in the project (Avionics, Space, Railway and Automotive) on the PTA-conformant platform; and (3) PROXIMA will also study the applicability of PTA Techniques to analyzing the timing behavior of COTS multicore processors.

C. CONTREX

CONTREX (Design of embedded mixed-criticality CON- Trol systems under consideration of EXtra-functional properties) will complement R&D activities in the area of predictable computing platforms, allowing for segregation of applications with different criticalities, with analysis and segregation techniques for the extra-functional properties real-time, power, temperature and reliability. These properties risk becoming major cost roadblocks when 1) scaling up the number of applications per platform and the number of cores per chip, 2) moving to battery powered devices or 3) switching to smaller technology nodes. CONTREX will enable energy efficient and cost aware design through analysis and optimization of real-time capability, power, temperature and reliability with regard to application demands at different criticality levels. The CONTREX results integrate into existing model-based design methods customizable for different application domains and target platforms.

D. MultiPARTES

MultiPARTES (Multi-cores Partitioning for Trusted Embedded Systems) aims at supporting mixed-criticality integration for embedded systems based on virtualization techniques for heterogeneous multicore processors. The starting point is XratuM, an open source cost-effective hypervisor developed specifically for real-time embedded systems increasingly used

---

1The description of the PROXIMA project provided in this paper comes from the PROXIMA Description of Work contributed by all its partners.
by the aerospace industry. Based on this approach, MULTIPARTES is developing a model-driven methodology to offer a rapid and cost-effective development of mixed-criticality systems integrating critical and non-critical applications on shared system resources. Road to certification is being assessed together with certification bodies. Temporal isolation by means of the hypervisor is a critical challenge in the project.

IV. DREAMS PROJECT

The objective of the European FP7 project DREAMS is to develop a cross-domain architecture and design tools for networked complex systems where application subsystems of different criticality, executing on networked multi-core chips, are supported.

In many mixed-criticality systems, platforms encompassing networked multi-core chips will be required. In addition to requirements exceeding the resources of a single chip, today's technology does not support the manufacturing of electronic devices with failure rates low enough to meet the reliability requirements of ultra-dependable systems. Since component failure rates are usually in the order of $10^{-5}$ to $10^{-6}$, ultra-dependable applications require the system as a whole to be more reliable than any one of its components. This can only be achieved by utilizing fault-tolerance strategies that enable the continued operation of the system in the presence of component failures.

Therefore, DREAMS will develop a mixed-criticality architecture based on system perspective of networked multi-core chips. The goal is to develop a hierarchical platform including both on-chip resources (e.g., processing cores, memory, Network-on-a-Chip (NoC)) and off-chip resources such as computer network. This system perspective will be established by virtualization (e.g., secure and timely end-to-end channels with different on-chip and off-chip segments), platform models and tools and integrated resource management resulting in higher flexibility, adaptability and energy efficiency.

The architecture will allow fine-grained mixed-criticality integration using multiple partitions within each core of the networked multi-core chips. Each partition can have a separate criticality level, including the highest criticality levels for certification.

The architectural definition will be cross-domain and provide a methodology approach towards the design and development of certifiable mixed-criticality embedded systems based on model-driven engineering. The methodology will support cross-domain certification standards such as IEC-61508 and product family technologies that enable the seamless development of optimized product variants (safety, price, power-consumption, etc.) based on previously developed components. The technical objectives of the project are as follows:

1) Architectural Style and Modelling Methods based on Waistline Structure of Platform Services: Core architectural services will provide a stable foundation for the safe and secure composition of mixed-criticality systems out of components. The core architectural services will include time services, integrated resource management services, communication and execution services for time and space partitioning.

2) Virtualization Technologies at Cluster and Chip Level: Software virtualization and hardware segregation will be combined to provide partitioning addressing significant extra functional requirements (e.g., time, reliability, safety, security, etc.). Gateways will support end-to-end channels over hierarchical, heterogeneous and mixed-criticality networks.

3) Adaptation Strategies for Mixed-Criticality Systems: Integrated resource management for mixed-criticality systems will perform monitoring and runtime control of virtualization technologies recognizing system wide, high-level constraints, such as end-to-end deadlines and reliability.

4) Development Methodology and Tools based on Model-Driven Engineering: The development methods and tools will support the development process ranging from modelling and design to the validation of mixed-criticality systems.

5) Certification and Mixed-criticality Product Lines: A modular safety-case for mixed-criticality systems will be defined along with certification support for mixed-criticality product lines.

6) Demonstrators: Three demonstrators encompassing avionic, industrial, and healthcare mixed-criticality applications will show the feasibility and benefits of the DREAMS architecture in real-world scenarios.

The DREAMS project will consolidate and extend the architectural concepts, virtualization technologies and development methods from previous and ongoing EU projects. Projects such as GENESYS, parMERASA, CERTAINTY, VIRTICAL, MULTIPARTES, RECOMP, and ACROSS have developed solutions that contribute to the overall objective of mixed-criticality integration. DREAMS will analyze the scope of these projects and identify areas of overlap, strengths and weaknesses of the produced results. The technical integration of a selected subset of results from these earlier projects is planned, to combine them with the new development work carried out in DREAMS.

The DREAMS project will also promote widespread adoption and perform community building. A community infrastructure will be established and populated (e.g., website and repository), training materials will be made available, standardization activities will be performed and a European innovation roadmap for research in mixed-criticality systems will be defined.

V. PROXIMA PROJECT

PROXIMA focuses mainly on the challenges of Timing and Certification as defined in Section II. The PROXIMA thesis is that the temporal behavior of mixed-criticality Critical Real-Time Embedded Systems (CRTES) executing on multicore and manycore platforms can be analyzed effectively via probabilistic timing analysis techniques. The objective of probabilistic timing analysis is to provide WCET estimations and end-to-end worst-case response times (WCRT) which can be determined to be “safe enough” with respect to application

2For more information visit http://www.dreams-project.eu/

3For more information visit http://www.proxima-project.eu/
time constraints, so that they keep the overall failure rate of the application below the specific threshold of acceptability (e.g., $10^{-9}$ per hour) for that application. Probabilistic and statistical approaches are a natural fit to mixed-criticality systems where applications at different criticality levels have different, domain-specific requirements in terms of acceptable timing failure rates, for example, failure rates of $10^{-7}$ per hour for low criticality and $10^{-9}$ per hour for high criticality applications.

PROXIMA defines new hardware and software architectural paradigms based on the concept of randomization, ensuring that the risks of temporal pathological cases are reduced to quantifiably small levels. On top of this, 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 temporal analysis, bringing the probabilistic approach to a state of technological readiness, and priming multiple European industry sectors in its use via a number of case studies.

The PROXIMA project builds on the scientific and technical foundation laid down by the precursor PROARTIS project. PROARTIS has shown how to obtain statistical independence by construction on single core processors as well as on simple multicore processors. PROARTIS has also demonstrated how a time-composable operating system can be developed that transparently operates in support of PTA-conformance and exposes extra-functional properties under existing segregation and availability requirements taken from the automotive, avionics, and telecom munications domain and evaluate its effectiveness based on three industrial demonstrators pursuing feedback to the industrial state-of-the-art in mixed-criticality system design through a holistic design approach that considers extra-functional constraints as first-class citizens. It will represent and expose extra-functional properties under existing segregation and certification techniques (both in the design phase and during system operation), and finally include these properties into local (on the device/network node) and global (information exchange using cloud infrastructure) scheduling and control decisions.

PROXIMA will go far beyond PROARTIS for multicore systems by considering COTS technology at both FPGA and RTOS level to address the disruption caused to the tightness and robustness of PTA bounds by non-PTA-conformant components. PROXIMA will also investigate how the principles of PTA extend to manycore systems and propose the PTA-conformant design of new manycore processors. Furthermore, where the PROARTIS solutions were assessed against avionics needs, PROXIMA will cover a wider cross-section of the CRTES industrial domains including in addition, space, railways, and automotive.

Tool suppliers together with industry leaders in PROXIMA (Rapita Systems Ltd, SYSGO, Aeroflex Gaisler AB, AIRBUS Operations SAS, Astrium Satellites, IK4-IKERLAN and Infineon Technologies UK Ltd) will address the first challenge by taking the prototype results demonstrated in PROARTIS and turning them into industry-qualified products that can be used in industrial size projects. The research partners in PROXIMA (Barcelona Supercomputer Center, University of Padua, INRIA and University of York) will address the first challenge by extending the application below the specific threshold of acceptability (e.g., $10^{-9}$ per hour) for that application. Probabilistic and statistical techniques, the challenges posed in analyzing the timing behavior of complex applications of mixed-criticality levels, composed of tasks, allocated and scheduled on multicore and manycore processors. (By comparison, PROARTIS only considered execution times of single applications running non-pre-emptably).

PROXIMA will go far beyond PROARTIS for multicore systems by considering COTS technology at both FPGA and RTOS level to address the disruption caused to the tightness and robustness of PTA bounds by non-PTA-conformant components. PROXIMA will also investigate how the principles of PTA extend to manycore systems and propose the PTA-conformant design of new manycore processors. Furthermore, where the PROARTIS solutions were assessed against avionics needs, PROXIMA will cover a wider cross-section of the CRTES industrial domains including in addition, space, railways, and automotive.

Tool suppliers together with industry leaders in PROXIMA (Rapita Systems Ltd, SYSGO, Aeroflex Gaisler AB, AIRBUS Operations SAS, Astrium Satellites, IK4-IKERLAN and Infineon Technologies UK Ltd) will address the first challenge by taking the prototype results demonstrated in PROARTIS and turning them into industry-qualified products that can be used in industrial size projects. The research partners in PROXIMA (Barcelona Supercomputer Center, University of Padua, INRIA and University of York) will address the first challenge by extending the application below the specific threshold of acceptability (e.g., $10^{-9}$ per hour) for that application. Probabilistic and statistical techniques, the challenges posed in analyzing the timing behavior of complex applications of mixed-criticality levels, composed of tasks, allocated and scheduled on multicore and manycore processors. (By comparison, PROARTIS only considered execution times of single applications running non-pre-emptably).

PROXIMA will go far beyond PROARTIS for multicore systems by considering COTS technology at both FPGA and RTOS level to address the disruption caused to the tightness and robustness of PTA bounds by non-PTA-conformant components. PROXIMA will also investigate how the principles of PTA extend to manycore systems and propose the PTA-conformant design of new manycore processors. Furthermore, where the PROARTIS solutions were assessed against avionics needs, PROXIMA will cover a wider cross-section of the CRTES industrial domains including in addition, space, railways, and automotive.

Tool suppliers together with industry leaders in PROXIMA (Rapita Systems Ltd, SYSGO, Aeroflex Gaisler AB, AIRBUS Operations SAS, Astrium Satellites, IK4-IKERLAN and Infineon Technologies UK Ltd) will address the first challenge by taking the prototype results demonstrated in PROARTIS and turning them into industry-qualified products that can be used in industrial size projects. The research partners in PROXIMA (Barcelona Supercomputer Center, University of Padua, INRIA and University of York) will address the first challenge by extending the application below the specific threshold of acceptability (e.g., $10^{-9}$ per hour) for that application. Probabilistic and statistical techniques, the challenges posed in analyzing the timing behavior of complex applications of mixed-criticality levels, composed of tasks, allocated and scheduled on multicore and manycore processors. (By comparison, PROARTIS only considered execution times of single applications running non-pre-emptably).

PROXIMA will go far beyond PROARTIS for multicore systems by considering COTS technology at both FPGA and RTOS level to address the disruption caused to the tightness and robustness of PTA bounds by non-PTA-conformant components. PROXIMA will also investigate how the principles of PTA extend to manycore systems and propose the PTA-conformant design of new manycore processors. Furthermore, where the PROARTIS solutions were assessed against avionics needs, PROXIMA will cover a wider cross-section of the CRTES industrial domains including in addition, space, railways, and automotive.

Tool suppliers together with industry leaders in PROXIMA (Rapita Systems Ltd, SYSGO, Aeroflex Gaisler AB, AIRBUS Operations SAS, Astrium Satellites, IK4-IKERLAN and Infineon Technologies UK Ltd) will address the first challenge by taking the prototype results demonstrated in PROARTIS and turning them into industry-qualified products that can be used in industrial size projects. The research partners in PROXIMA (Barcelona Supercomputer Center, University of Padua, INRIA and University of York) will address the first challenge by extending the application below the specific threshold of acceptability (e.g., $10^{-9}$ per hour) for that application. Probabilistic and statistical techniques, the challenges posed in analyzing the timing behavior of complex applications of mixed-criticality levels, composed of tasks, allocated and scheduled on multicore and manycore processors. (By comparison, PROARTIS only considered execution times of single applications running non-pre-emptably).

The solutions that PROXIMA will develop, centered on high Technology Readiness Level hardware and software components and timing analysis methods, will enable European industry to retain market leadership with the ability to develop cost-effective, high-performance, CRTES encompassing multiple applications with different criticality levels on multicore and manycore platforms. In product terms, this ability will bring about benefits in size, weight and power consumption, effectively doing more (hard real-time performance and average throughput) with less (processing resource and energy usage).

In development terms, PROXIMA technology will streamline the software development process, reducing the elapsed time, the effort and the costs entailed in the integration, verification, validation, and, where applicable, certification activities. This is expected to bring considerable benefits in terms of time-to-market and reduced development costs.

VI. CONTREX PROJECT

CONTREX will enable the cost-efficient and cost-sensitive design through analysis and optimization of power, temperature, and reliability regarding applications demands at different criticality levels running on the same multi-core networked computing platform. The CONTREX approach integrates into an existing model-based design methodology and open source environment, customizable for different application domains and target platforms. CONTREX will put its focus on the requirements taken from the automotive, avionics, and telecommunications domain and evaluate its effectiveness based on three industrial demonstrators pursuing feedback to the industrial design practice, standards, and certification procedures.

Extra-functional properties will limit the capabilities and realization of future mixed-criticality system with regard to overall energy consumption, mobility (due to limited battery capacities), waste heat discharge, and finally reliability and availability [2]. For this reason, CONTREX will extend the industrial state-of-the-art in mixed-criticality system design through a holistic design approach that considers extra-functional constraints as first-class citizens. It will represent and expose extra-functional properties under existing segregation and certification techniques (both in the design phase and during system operation), and finally include these properties into local (on the device/network node) and global (information exchange using cloud infrastructure) scheduling and control decisions.

For more information visit http://contrex.offis.de/
The main goal of the project is to enable cost-efficient design, modeling, analysis, simulation, and exploration of complex networked control systems with mixed-criticality on different levels of abstraction. The project targets a meet-in-the-middle approach for the integration of existing design environments, models, and analysis and simulation tools.

The project will extend the state-of-the-art in domain specific control system modeling (top-down) through:

- Separation of design decisions for control application, deployment and underlying hardware/software architecture at device level and
- Formalization, annotation, and refinement of constraints/contracts on extra-functional properties: time, power, and temperature.

State-of-the-art segregation techniques for shared computing resources (i.e. multi-core systems) cover functional correctness and timing, but ignore possible influence and feedback paths originating from parasitic extra-functional effects. Sharing the same computing platform, multiple applications can interfere indirectly through power/energy and temperature properties. Running a hard-real time application and non-timing critical application (best effort) on the same execution platform, the non-timing-critical application can have an extra-proportional contribution to the overall power consumption. The increased power consumption heats up the whole chip and requires to slow-down (e.g. dynamic voltage and frequency scaling) dedicated cores and the memory subsystem to keep the chip temperature within a rage allowing reliable operation. This dynamic reaction to control waste heat and reliability of the chip might have an influence on the core running the hard real-time task. This can be either directly through reducing the clock frequency of the core running the real-time application or indirectly through the effects in the memory subsystem. When designing such systems, all critical applications of the system need to be designed with the explicit awareness of possible mode switches due to control of extra-functional properties.

Integrating mixed-criticality applications on multi-core and especially mobile battery-powered computing platforms requires additional segregation along extra-functional dimensions, while keeping up classic temporal and special segregation properties. For this purpose, CONTREX will extend state-of-the-art in execution platform modeling and segregation for functional and extra-functional properties (bottom-up) through:

- Separation of physical hardware resources like processors, memories, communication channels (on- and off-chip) from services that enable a transparent virtualization of different underlying hard-ware/software platforms,
- Characterization, abstraction and explicit representation of timing, power, and temperature properties for specific hardware/software platforms, and
- Segregation along extra-functional dimensions.

The project will combine top-down (control system modeling) and bottom-up (execution platform modeling) approaches in an integrated design environment establishing a missing link through:

- Deployment and mapping of control applications to a network of virtualized hardware/software platforms and network infrastructure abiding extra-functional properties.
- Simulation infrastructure that scales from detailed sub-system to overall networked control system simulation including dynamicity of extra-functional properties.
- Support for the exploration of different deployment and mapping alternatives to obtain the most cost-efficient solution under the given extra-functional constraints.
- Cloud services for data acquisition and monitoring of extra-functional properties to obtain an overall health-state of the controlling system and the system under control including the coordination of global compensation actions at run-time.

Our economic goal is to improve energy efficiency by 20% and to reduce cost per system by 30% due to a more efficient use of the computing platform.

CONTREX will draw upon pre-existing results from the FP7 IP COMPLEX [3] and Thermator [4], establishing the basis for the estimation and analysis of SoC power and temperature. A strong background in safety-critical multicore applications builds on the ARTEMIS projects CHESS, nSafe-Cer and the FP7 project T-CREST.

VII. MultiPARTES Project\(^5\)

The MultiPARTES FP7 project aims at supporting mixed-criticality integration for embedded systems based on virtualization techniques for heterogeneous multicore processors.

The main objective of MultiPARTES is to provide execution environments and tools to support the development of mixed criticality applications over partitioned embedded platforms based on a multicore open source virtualization layer thereby shortening the time-to-market. This is being carried out through the definition, demonstration and validation of a complete engineering framework supporting the design and development of partitioned systems.

A major outcome of the project is the MultiPARTES XtratuM, an open source hypervisor designed as a generic virtualization layer for heterogeneous multicore. MultiPARTES evaluates the developed technology through selected use cases from the offshore wind power, space, visual surveillance, and automotive domains. A promising solution is to incorporate mechanisms that establish multiple partitions with strict temporal and spatial separation between the individual partitions. In this approach, subsystems with different levels of criticality can be placed in different partitions and can be verified and validated in isolation.

There are four major outcomes from the project:

1) The definition of a methodology to enforce the development and production of new applications based on partitioned multicore systems. The methodology will be supported by a tool that allows the definition

\(^5\)For more information visit http://www.multipartes.eu/
of activities and its attributes (security level, criticality level, real-time constraints, operating system needs, hardware dependencies, etc.). Based on these attributes, the tool proposes a partitioning scheme to isolate activities in partitions, an allocation of partitions to cores, and a scheduling scheme to execute the partitions. The result is a set of configuration files that statically define the behavior of the virtualization layer.

2) An execution platform based on XtratuM [5] hypervisor specifically designed for embedded real-time systems. It provides spatial and temporal isolation of partitions and permits to execute partitions without a specific knowledge of its internals. Partitions can contain different execution environment as single thread (bare partitions), multi-thread (guest RTOS or GPOS) or multicore (multicore guest OS).

3) Execution environments. In the project several execution environment (guestOSs) have been ported: MPTAL (MultiPARTES Abstraction Layer) which is a simple runtime which offers services close to the ARINC-653 P4, ORK+ that provides an Ada environment based on Ravenscar profile [6], Partikle that is a POSIX RTOS [7] and a Linux environment.

4) A set of advanced HW virtualization features are being developed. In particular, memory hierarchies are being defined to enable spatial partitioning and avoid cache flushing side effects.

The certification process of safety critical real-time applications, by so-called Certification Authorities (CAs) is based on very conservative assumptions, which typically exceed what is required by the designers assurance levels. As a consequence, the system designer has to deal with mixed-criticality job sets: high criticality applications (jobs), which have to be certified by CAs, have two different worst case execution times (WCETs): designers WCET and a more pessimistic (longer) WCET of the CAs.

In many cases, the V-Model shape is employed since it covers the entire development progress including requirements engineering, specification, implementation and integration as well as validation and verification (e.g., testing). Therefore, it eases certification according to the mentioned safety standards. However, this needs to be adapted to the mixed-criticality realm.

Plentifuls of methods are being studied to be applied nowadays to engineer mixed criticality systems. More prominent are those related to Model-Driven Engineering (MDE) and Software Product Lines. There is as well a line of work based on Components. These techniques promote cross-industry reuse with reduced development cost, shorter time-to-market and higher reliability of mixed-criticality systems. The development process will leverage the reuse of software and hardware components, safety case reuse, multi-vendor tools interoperability and traceability, and prevent any side effects of component interaction.

A key goal of the project is for academia to listen industry, and for industry to explain openly its needs. An updated roadmap to adoption is expected as an output of the discussion. A key point is how to assure that techniques are certification ready and certification bodies are well aware of the last progress. In this regard, a hot topic is sufficient independence among involved subsystems. Other relevant trends as multicore advent, pressure from consumer electronics, and other topics will be covered.

VIII. CONCLUSION

Currently a number of related European research projects under both FP7 and ARTEMIS programs, namely, ACROSS, MultiPARTES, ARAMIS, CERTAINTY, VIRTUALCAL, parMERASA, RECOMP and PROARTIS have worked, along similar lines. They featured some works on both the practical and scientific perspectives, on topics such as reference architecture, methodology, tools, certification issues and industrial application, among others. Three new projects DREAMS, PROXIMA and CONTREX, which started in October 2013, will continue these research paths. This paper reviewed the status and developments of some of the projects running on the topic, paving the way for future collaboration in the topic to realize the mixed-criticality systems vision.

ACKNOWLEDGMENT

This work has been supported by the European Commissions funded projects DREAMS (610640), PROXIMA (611085), CONTREX (611146) and MultiPARTES (287702).

REFERENCES


