Distributed REal-time Architecture for Mixed criticality Systems

Report of First Workshop on Roadmap
D 9.3.1

Project Acronym	DREAMS	**Grant Agreement Number**		FP7-ICT-2013.3.4-610640	
Document Version	1.0	**Date**	2014-07-24	**Deliverable No.**	9.3.1
Contact Person	Ankit Agrawal	**Organisation**		Technische Universität Kaiserslautern	
Phone	+49 (0)631 205 3674	**E-Mail**		agrawal@eit.uni-kl.de	

Contributors

Name	Partner
Ankit Agrawal	TUKL
Gerhard Fohler	TUKL
Roman Obermaisser	USIEGEN
Arjan Geven	TTT

Table of Contents

1 Introduction

This document is the deliverable D9.3.1 of the DREAMS project. It is the first deliverable of task *T9.3 –Mixed-criticality research and innovation roadmap* of work package *WP9 - Community building and standardization*. This deliverable *D9.3.1 – Report of first workshop on roadmap* presents the report of the first and second workshops organized towards developing the innovation roadmap for research and innovation in mixed-criticality systems.

1.1 Positioning of the Deliverable in the Project

The goal of work package WP9 is to steer and increase European research and technology awareness in the area of distributed mixed-criticality and embedded computing systems. Work package WP9 comprises of three tasks: T9.1, T9.1 and T9.3.

- Task *T9.1 – Community building* aims at building a sustainable community focusing on the results of the DREAMS project and other projects on mixed-criticality systems.
- Task *T9.2 – Standardization support* aims to provide support towards all standardization efforts emerging from all activities and results of the DREAMS project.
- Task *T9.3 - Innovation roadmap* aims to help align the academic and industrial research by developing a research and innovation roadmap on the topic of mixed criticality to achieve critical mass and facilitate breakthrough innovations in the medium and long- term.

This deliverable relates to task T9.3. Over the course of the project, T9.3 will provide two deliverables:

1. *D9.3.1- Report of first workshop on roadmap*
   This deliverable reports on the first and second workshops of partners in the consortium and stakeholders in the international research community to provide a roadmap for research and innovation on mixed critically to establish the state-of-the-art in the area and identify research challenges.
2. *D9.3.2 – White paper on mixed-criticality research and innovation*
   Deliverable D9.3.2 deliverable aims at providing a white paper for research in mixed-criticality beyond DREAMS. It will also serve to disseminate the achieved results in DREAMS to the community at large.

The confidentiality level of this deliverable is public (PU) and it will be published on DREAMS website, once approved by European Commission.

1.2 Objectives of the Deliverable

The objective of this deliverable is:

"To report on the completed activities (first workshop and second workshop) directed towards the preparation of the research and innovation roadmap on mixed-criticality".

1.3 Planned workshops & Timeline

Task T9.3 aims at developing a research and innovation roadmap in mixed criticality by harnessing the collaborative efforts of the researchers both in academic and industrial areas. To achieve this aim, we planned three workshops in the first phase of the task:

1. **First Workshop**: It was organized on 15 May 2014 as a part of HiPEAC Computing Systems Week (CSW) 2014 together with PROXIMA in Barcelona, Spain. We availed this opportunity to get the viewpoint on mixed criticality of wider the research community.
2. **Second Workshop**: It was organized on 2 July 2014 and directed towards the community comprising of the projects funded under EU FP7 program in the mixed criticality cluster (MCC) - DREAMS, PROXIMA and CONTREX. This workshop aimed at obtaining the viewpoints of the community that is central to the mixed criticality research in Europe.
3. **Third Workshop**: This workshop will be tentatively organized in Dec. 2014. It will be a scientific workshop specifically aimed at collaborating with international researchers towards developing an innovation roadmap for mixed criticality. The key outcomes of the first and second workshop will serve as the starting point for discussion in this workshop.

1.4 Contents of the Deliverable

In chapter 2, we provide a report on the first workshop. Further in chapter 3, we also provide the report on the second workshop. Each chapter (2,3) is organized into different sections, each providing information on the specific aspect of the workshop: organization and participation, aims of the workshop, overview of talks and the key outcomes. The program of the first and second workshop is provided towards the end of this document in the appendix A and B, respectively. Chapter 4 sheds light on the next step – third workshop, towards developing an innovation roadmap for mixed criticality. Finally, towards, the end of the document, in chapter 5, a short biography of each of the speakers in the first and second workshop is provided.

2 First Workshop

2.1 Organization

The first workshop organized was a one-day event held on 15 May 2014 at Universitat Politècnica de Catalunya (UPC) in Barcelona, Spain. It was a part of HiPEAC Computing Systems Week (CSW) 2014. HiPEAC CSW provided an ideal platform towards engaging wider scientific and industrial community in obtaining viewpoints towards identification of challenges in mixed criticality.

The workshop was titled: *"Challenges in Mixed Criticality and Real-time and Reliability in Networked Complex Embedded Systems"*. It comprised of four sessions:

1. S1 (Session 1): Mixed-Criticality in Avionics, Automotive and Space Domain
2. S2 (Session 2): Real-time Reliability and Cross Domain Challenges
3. S3 (Session 3): Resource Sharing and Partitioning in Multicores
4. S4 (Session 4): Certification, Models of Computation, and Software Development in Mixed-criticality Cyber-Physical Systems

A detailed program of the workshop is provided in Appendix A of this document.

The workshop was jointly organized by Gerhard Fohler (DREAMS – TUKL, Germany), Jaume Abella (PROXIMA - BSC, Spain) and Yanos Sazeides (UCY, Cyprus). Roman Obermaisser (DREAMS – USIEGEN, Germany) and Arjan Geven (DREAMS – TTT, Austria) also played an important role in setting the theme of the workshop. The detailed information (program, presentation slides etc.) is available on the webpage (http://rts.eit.uni-kl.de/hipeac-ws-0514/) especially created for disseminating the workshop content to the public at large.

2.2 Aims of the Workshop

The workshop aimed at:

1. Bringing together representatives from related initiatives (EU FP7 projects: DREAMS, PROXIMA)
2. Establishing relevant application areas and their specific demands, state-of-the-art, and research challenges
3. Providing special focus on understanding specific challenges from related application domains to, e.g., identify what these criticalities actually are and which problems should be solved

2.3 Participation

The number of speakers that gave the talks was 12. One speaker could not make it to the workshop. However, abstract and presentation slides were provided for the interested audience.

The workshop was well attended as the number of participants in each session ranged from 39[1] to 47[2]. It was strongly interactive in nature as it brought together representatives from related initiatives (HARPA, VeTeSS, CLERECO, PROARTIS, OMAC4S, RACE), and experts from both industrial applications and demands, as well researchers for state-of-the art and novel research directions. It achieved high cross dissemination by bringing together related, but not closely linked research communities, as well as, exposing the topics to the HiPEAC community at large.

[1] Source: HiPEAC - http://www.hipeac.net/add/res/104/481

[2] Source: HiPEAC - http://www.hipeac.net/add/res/104/480

2.4 Overview of Different Sessions

In this section, we provide a brief overview of each talk in the four sessions that were a part of the workshop.

2.4.1 Session 1: Mixed Criticality in Various Domains

2.4.1.1 Mixed-criticality Challenges on the Avionics Safety Critical Domain (Daniel Gracia Pérez, TRT, FR)

The avionics industry has for a long time lead the development of mixed-critical systems. With solutions such as the AFDX network standards and the Integrated Modular Avionics (IMA) computing infrastructure, applications with different criticality could be combined on a single computing device and the different off-chip communications ensured, independently of their criticality level. However, the higher computing and communications requirements, and the performance stagnation of single core processors, are forcing the avionics industry to more adapt new design/software/hardware solutions. Multi-cores are one of the most promising hardware solutions to serve as base of future IMA products. However, their integration with the software execution environments (operating system and hypervisors) and the communication solutions to ensure the safety requirements, as the time and space partitioning, while achieving the high performance requirements remains a problem.

This presentation describes current practices in the avionics domain to address the mixed-criticality systems with single-cores as computing resources, and the challenges that remain open in order to use multi-cores in future avionics solutions.

2.4.1.2 Mixed-Criticality in Automotive Domain: A Vehicle Control Platform as Safety Element out of context (Kai Höfig, Siemens AG, DE)

A vehicle control platform as safety element out of context – The major challenges for dependability assurance of (Automotive) CPS include to exchange dependability-related information across domains and complex value chains. Automated dependability assurance enables fast change impact analysis and supports dependability assurance for CPS integration in the field.

RACE project aims to tackle these challenges by providing a dynamic duplex control computer approach. Fault containment regions and a master slave mechanism provide a safe environment for safety critical functions such as steer-by-wire. As a safety element out of context, dependability related development artifacts become reusable.

2.4.1.3 Mixed-Criticality in Space Domain: OMACS4S - Open Modular Architecture for Space (Hans Jürgen Herpel, Airbus, DE)

Today’s spacecraft avionics architecture is characterized by a broad variety of processing modules, operating systems and interfaces for exchanging data between different processing modules. The software that implements most of the satellite functionality has to deal with this fact and is one of the reasons why software has become one of the major cost drivers in satellite projects. Similar problems have triggered developments in other industrial domains like AUTOSAR in the automotive area or Integrated Modular Architecture (IMA) in the aerospace industry. All these initiatives are based on the definition of standards for computing platforms and the interfaces between these platforms.

The goals of the Open Modular Avionics Architecture for Space Applications (OMAC4S) initiative started by Airbus Defence and Space, Fraunhofer FOKUS, STI, SYSGO and TTTech are to outline a solution based on open standards that helps to reduce complexity and costs for space avionics significantly, as: the software has to deal with a much smaller spectrum of computing platforms and the usage of standards will allow to combine solutions from different vendors either hardware or software.

The main characteristics of the envisaged system architecture are listed below:

- Network centric approach (Satellite Deterministic Network based on Time Triggered Ethernet),
- Using passive backplane based on the industrial standard: PICMG CPCI-S.0

• Various CPU boards with different performance (single core to eight core CPU) and qualification level,

e.g. radiation hard CPUs and radiation tolerant COTS CPUs in dual or triple redundant configuration

• Full support for time and secure space partitioning

• Provision of a software framework that provides all basic services of a typical on-board software

This initiative is partly funded by the German national space agency (DLR) through the project On-Board Computer System Architecture (OBC-SA, FKZ 50RM1210).

2.4.2 Session 2: Real-time and Reliability

2.4.2.1 CLERECO: Cross Layer Early Reliability Evaluation for the Computing Continuum (Giorgio Di Natale, LIRMM, FR)

Advanced multifunctional computing systems based on future technologies hold the promise of a significant increase of the computational capability that will offer end-users ever improving services and functionalities. Reliability of electronic systems will become an ever-increasing challenge for information and communication technology and must be guaranteed without penalizing or slowing down the characteristics of the final products. CLERECO research project recognizes the importance of accurately evaluating the reliability of systems early in the process to be one of the most important and challenging tasks toward this goal. Being able to precisely evaluate the reliability of a system means being able to carefully plan for specific countermeasures rather than resorting to worst-case approaches. CLERECO project will be fundamental in the development of scaled systems for the next decade. The proposed CLERECO framework for efficient reliability evaluation and therefore efficient exploitation of reliability oriented design approaches starting with the earliest phases of the design process will enable circuit integration to continue at exponential rates. It will enable the design and manufacture of future systems for the computing continuum at a minimum cost contrary to existing worst-case design solutions for reliability. The applications of such chips will play a major role in our society and can be seen through the prism of future computing systems ranging from avionics, automobile, smartphones, mobile systems, Personal Computers and future servers utilized in the settings of Data Centers, Grid Computing, Cloud Computing and other types of HPC systems.

2.4.2.2 Timely Error Detection in light-lockstep Safety Critical Systems (Carles Hernández, Barcelona Supercomputing Center, ES)

Safety-critical systems rely on features such as lockstep execution for error detection, and reset and re-execution for error correction. In particular, light lockstep is an attractive choice since it does not require redesigning cores but, instead, comparing the off-core activities (i.e. addresses requested and data/addresses written). While this approach suffices to guarantee functional correctness of the system, as needed for certification against safety standards (e.g., ISO 26262), it fails to provide any timing guarantee as the time elapsed since the error occurs until lockstep detects it can be inordinately large. This talk introduces Live (Lightly Verbose), an approach to guarantee timely detection of errors at low cost in the context of light lockstep systems.

2.4.2.3 Worst Case Execution Time Estimation and Permanent Faults (Damien Hardy, University of Rennes I / IRISA, FR)

Semiconductor technology evolution suggests that permanent failure rates will increase dramatically with scaling. While well known approaches such as error correcting codes exist to recover from failures and provide fault-free chips, they will not be affordable anymore in the future due to their non-scalable cost. Consequently, other approaches like fine grain disabling will become economically necessary. All static worst-case execution time (WCET) estimation methods assume fault-free architectures. Their result is not safe anymore when using fine grain disabling of hardware components, which degrades performance. This talk, first, briefly describes a method that statically calculates a probabilistic WCET bound in the presence of permanent faults in instruction caches.

Then, it will explore the cache parameters as a first step in the exploration of the design tradeoffs for supporting faulty caches.

2.4.2.4 Modelling the Performance Implications of Permanent Faults in Caches (George Klokkaris, University of Cyprus, CY)

Current technology trends suggest that future processors will need to remain functionally correct in the presence of time-zero and time-dependent permanent faults, in order to sustain scaling benefits, limit field returns, and reduce down-time. One of the key obstacles towards such a development is the lack of tractable off-line (design-time) methods that can accurately assess the performance of processors with parametric and aging-induced permanent faults. This talk presents analytical techniques that can be used off-line to rapidly measure the performance distribution expected from the execution of a program in a population of processors that experience random permanent faults – at time zero and in the field – in cache arrays.

2.4.2.5 Management of Mixed Criticality and Reliability at Run-time: the HARPA Approach (William Fornaciari, Politecnico di Milano, IT)

The talk will address some of the crucial issues and showstoppers in the design of embedded applications exploiting multi-core platforms. One of the main goals is to guarantee Quality of Service (QoS) of the applications execution while fulfilling a number of not purely functional figures of merit such as energy, power, thermal, reliability, cost, etc. In high end embedded systems and HPC such a problem is exacerbated, since frequently there is a mixed workload and most of the optimizations carried out at design time can became no longer valid in a very short operating time. The goal of this talk is to present the methodology that is going to be developed during the HARPA (Harnessing Performance Variability) project whose goal is to ensure dependable performance by exploiting run-time adaptation at several abstraction levels, ranging from the modelling of silicon properties up to the allocation of the resources at the operating system level. During the talk, it will also be shortly presented the first project deliverable, named Barbeque (BBQ), which is an open source tool (http://bosp.dei.polimi.it/) running in user space, capable to provide run run-time management of multi-core architectures also in the presence of mixed workloads.

2.4.3 Session 3: Resource Sharing and Partitioning in Multicores

2.4.3.1 Reflections on Partitioning and Resource Sharing in MCS (Tullio Vardanega, University of Padua, IT)

This presentation discusses how the understanding of “sufficient isolation” catered for by partitioning solutions conceived for single-CPU processor systems does not hold for multicore processors. The discussion first recalls the premises and motivations of time-and-space partitioning and projects them on the hardware architecture of multicore processors. Then it touches on the correlation between the pursuit of (symmetric and asymmetric) guarantees of sufficient isolation and the notion of levels of criticality. Finally, it brings the sharing of logical resources into the picture, showing how complex that seemingly simple problem becomes in the face of real parallelism.

2.4.3.2 Resource Sharing and Partitioning in Multicores (Francisco Cazorla, Barcelona Supercomputing Center, ES)

This presentation introduces the problem of contention in Hardware Shared Resources in the context of real time systems. The high-level discussion covers stateless and statefull resources as well as some techniques in the literature on the topic.

2.4.4 Session 4: Certification, MoC and Software Development in CPS

2.4.4.1 Mixed-Criticality: Modular Certification (Jon Pérez, Ikerlan, ES)

In order to pave the way towards the competitive development and certification of mixed-criticality solutions, different challenges need to be addressed such as:

- Solutions that support complexity management, increase re-usability, reduce product cost and reduce product overall certification cost & time.

- Solutions to reduce overall cost required for the certification, validation and verification of mixed-criticality solutions
- Cross-Domain compatibility and support among certification standards (e.g. IEC-61508)
- Etc.

Modular certification addresses previously described challenges and supports the competitive development and certification of mixed-criticality systems.

2.4.4.2 Mixed-Criticality: Integration of Different Models of Computation (Roman Obermaisser, University of Siegen, DE)

Mixed-criticality architectures with support for modular certification make the integration of application subsystems with different safety assurance levels both, technically and economically feasible. Strict segregation of these subsystems is a key requirement to avoid fault propagation and unintended side-effects due to integration. Also, mixed-criticality architectures must deal with the heterogeneity of subsystems that differ not only in their criticality, but also in the underlying computational models and the timing requirements. Non safety-critical subsystems often demand adaptability and support for dynamic system structures, while certification standards impose static configurations for safety-critical subsystems. Several aspects such as time and space partitioning, heterogeneous computational models and adaptability were individually addressed at different integration levels including distributed systems, the chip-level and software execution environments. However, a holistic architecture for the seamless mixed-criticality integration encompassing distributed systems, multi-core chips, operating systems and hypervisors is an open research problem. This presentation describes the state-of-the-art of mixed-criticality systems and discusses the ongoing research within the European project DREAMS on a hierarchical mixed-criticality platform with support for strict segregation of subsystems and support for heterogeneous models of computation.

2.4.4.3 Co-existence of Closed Subsystems and Open Subsystem with Emerging Behaviour and Dynamic Resource Allocation (Michael Zolda, University of Hertfordshire, UK)

This talk outlines the research activities on software development of cyber-physical systems (CPS). The software coordination language is extended to include facilities that allow one to describe concurrency aspects of CPS together with mixed criticality properties and mixed timing regimes, i.e., those with some real-time constraints and some average-case performance requirements. This coordination language will reduce the complexity of concurrent programming, as all concurrency is expressed at the level of the coordination level. At the same time extra-functional requirements are expressed at the coordination language level as well. The particular challenges imposed by the open-world assumption about things that were easier in the closed-world case: real-time and timing analysis, safety, certification, security, etc. need to be addressed.

To ensure the conservation of the required timing properties, the speaker presents system architecture with an execution layer and operating system that can support the conservation of required timing properties by means of isolation and criticality-aware scheduling. Resource managers on the different subsystems will provide the emerging property of dynamic adaptation to accommodate changing operation contexts of the system.

Based on the recent research on performance optimization, it is proposed to use system-wide resource-property aggregation in programming large-scale smart cyber-physical systems. System-wide resource-property aggregation is a novel concept that allows the aggregation of extra-functional properties and functional properties in a single constraint framework, which makes it possible to find solutions for various resource constraints up to observable parameters. Properties can be aggregated for multiple CPS services. Rather than abstracting away from the hardware platform, a hardware-characteristic description layer that allows for more precise timing analysis of the application software for both real-time and average-case performance constraints will be developed. To support the openness of CPS, security signatures to confirm compatibility of merging services are used.

2.5 Key Outcomes

2.5.1 Challenge 1: Use of static analysis and formal methods for determination of WCET in COTS multicores

Use of static and formal analysis and formal methods in COTS multicore is a challenge as information about network-on-chip (NoC) latency, memory latency etc. is not provided by COTS multicore suppliers, which results in treating these components as black boxes. Certification authorities encourage use of static analysis and formal methods. In such a case, one can directly tick the required box provided in the checklist and move forward in the certification process. If except static analysis and formal methods, any other approach (like measurement based etc.) is used for timing analysis, extensive documentary evidence needs to be provided that is both time-consuming and costly.

2.5.2 Challenge 2: Resource sharing and partitioning in COTS multicores

Sharing of resources leads to the problem of execution time of a task executing on a core being affected by the execution history of tasks running on other cores. This results in a challenge of how to provide execution history independent access-latency bounds for task running on a core without being concerned about the execution history of tasks running on other cores.

2.5.3 Challenge 3: Non-availability of standards for multicore platforms

Standards like ARINC 653 etc. are not defined for multicore platforms. In this regard, certification of such platforms is a challenge, as no guidelines exist. A suggestion that was given based on previous experiences of the researcher related to certification was: “Do not be stifled by the current standards towards providing temporal and spatial partitioning as most of them were designed for mono-cores. If you have a solution for multicores and if it breaks the present standards, do not worry. But be ready to provide a proof for your solution”

2.5.4 Challenge 4: Common understanding of mixed criticality in the community

The term “mixed criticality” has been used with different meaning by different researchers over the years. Graydon and Bate [GB13] also mentioned this problem in their 2013 paper. It is a challenge to establish a common notion of mixed criticality in the community.

2.5.5 Challenge 5: Mixed criticality - Certification in a composable manner

Plug and play kind of support is desired to add new ECUs to a car when it arrives at the workshop for servicing. It is desirable to update the software in a car without going through whole certification process again. This requires an incremental certification process. Ideally, no certification is the best possible way, as it will result in faster time to market of the latest automotive software. The rationale is that car manufacturers want to sell functionalities to the consumers throughout the lifetime of the automobile, to generate additional revenues. This may warrant addition of ECUs and/or installing/updating of software. This scenario highlights the motivation for plug-and play solutions desired by car manufacturers: Say a consumer buys a car and then returns it to the car manufacturer after 1 year (to buy latest model etc.). From a car manufacturer perspective, the car runs for 1 year and then the manufacturer gets back the car. So, the software is 1 year old. However, the software was developed 3 years before. Thus, it results in software being 4 years old.

In addition, if the instruction timing of the already certified hardware platform changes (say due to silicon revision), one has to go through the process of certification again. This is to make sure that the previous timing analysis still holds. Aircraft manufacturers need to provide support and maintenance for their airplane models for typically 20 years and more. As the hardware platforms may change (updated (say) due to silicon bugs etc.) it is desirable to not go through the complete certification process for the software of the hardware timing changes in order to save time, effort and money.

2.5.6 Challenge 6: Hierarchical Mixed-Criticality Systems and Internet of Things

Many mixed-criticality systems encompass multiple integration levels ranging from multi-core processors managed by operating systems with time and space partitioning to multi-cluster distributed systems. Mixed-criticality systems encompassing clusters of networked multi-core chips will be required to satisfy resource requirements exceeding the resources of a single node computer. In addition, failure rates low enough to meet the reliability requirements of ultra-dependable systems can only be achieved by utilizing fault-tolerance strategies that enable the continued operation of the system in the presence of node failures. In addition, future mixed-criticality systems will involve mobile networking, connectivity to the Internet and the need for exploiting cloud computing services. It is a significant challenge to provide real-time guarantees, temporal and spatial partitioning, reliability and security in hierarchical systems ranging from multi-core chips to the Internet of Things.

2.5.7 Challenge 7: Mixed-Criticality – Heterogeneity

Mixed-criticality systems consist of heterogeneous application subsystems that differ not only in their criticality, but also exhibit dissimilar requirements in terms of timing (e.g., firm, soft, hard, non real-time) and different models of computation (e.g., dataflow, time-triggered messaging, distributed shared memory). Also, subsystems can have contradicting requirements for the underlying platform such as different tradeoffs between predictability, certifiability and performance in processors cores, hypervisors, operating systems and networks. Research challenges include the support for different models of computation in development methodologies and distributed execution platforms for mixed-criticality systems.

3 Second Workshop

3.1 Organization and Participation

The second workshop – *Mixed Criticality Cluster Workshop* was a 1-day workshop held on 2 July 2014 at the facilities of the Spanish Government, Rue du Trône 62 in Brussels, Belgium. The date was specially chosen to be one day after the mixed-criticality cluster (MCC) project reviews at the European Commission (EC) to save travelling expenses and time, and to have maximum participation from all the three projects in MCC cluster.

The second workshop was jointly organized by the three projects sponsored under the EU FP7 program – DREAMS, PROXIMA and CONTREX, that form a part of the MCC cluster. The people responsible for the organization were the co-ordinators of the before-mentioned projects - Roman Obermaisser (DREAMS – USIEGEN, Germany), Francisco Cazorla (PROXIMA – BSC, Spain), and Kim Grüttner (CONTREX - OFFIS, Germany).

The workshop comprised of 6 technical sessions, 1 session on mixed-criticality community platform – www.mixedcriticalityforum.org and 1 session dedicated to panel discussion focusing on joint exploitation of projects results. The brief summary of each talk in the technical sessions is provided in section 3.3. The detailed program is available in Appendix B of this document. The slides of the technical sessions are available in the public domain through a website hosted by TUKL – http://rts.eit.uni-kl.de/mcc-0714/

The workshop was a closed event i.e. only open to members of the three projects and the related people (Project Officers, Reviewers etc.). The number of participants was around 50. In all, there were 14 different speakers for the 6 technical sessions from the three projects in the MCC cluster.

3.2 Aims of the Workshop

This is workshop specifically aimed at

1. Obtaining the viewpoints of the members of the MCC cluster community that is central to the mixed criticality research in Europe.
2. Providing a platform for closer understanding of the three projects amongst the members of the MCC cluster community

3.3 Overview of Different Sessions

3.3.1 Session 1: Welcome and Overview

At the start of the session, Roman Obermaisser welcomed the participants from the MCC cluster to the workshop. Later, he provided an overview of the DREAMS project. It was followed by the overview of PROXIMA and CONTREX projects, provided by Francisco Cazorla and Sven Rosinger, respectively.

3.3.2 Session 2: Certification

3.3.2.1 Towards Modular Certification of Mixed-criticality Systems (Jon Pérez, Ikerlan, ES; DREAMS)

In order to pave the way towards the competitive development and certification of mixed-criticality solutions, different challenges need to be addressed such as:

- Solutions that support complexity management, increase re-usability, reduce product cost and reduce product overall certification cost & time.
- Solutions to reduce overall cost required for the certification, validation and verification of mixed-criticality solutions
- Cross-Domain compatibility and support among certification standards (e.g. IEC-61508)

- Propose strategies for the certification of product families (mixed-criticality) compliant with the standard (IEC-61508)
- Provide cross-domain patterns, e.g. Diagnosis strategy, I/O sever, communication server, etc
- Modular safety cases for hypervisor, COTS multicore processor and network

Modular certification addresses previously described challenges and supports the competitive development and certification of mixed-criticality product families.

3.3.2.2 Certification Approach in PROXIMA (Mikel Azkarate-askasua, Ikerlan, ES; Jon Pérez, Ikerlan, ES; PROXIMA)

Certification has become a legislative, customer and, above all, an economic and competitive need. This presentation describes the certification approach envisioned in PROXIMA analyzing the fitting of the project outcomes within current certification standards. The approach previews two paths assuring the collaboration between IP projects and cross-domain links to maximize the industrial readiness and impact of PROXIMA project. The first path will consist on a per-domain analysis and the second path on the elaboration and discussion of a Safety Concept that will be reviewed by an external certification authority.

3.3.3 Session 3: Scheduling and Timing Analysis

3.3.3.1 Resource Management for Mixed Criticality Systems – The DREAMS Approach (Gerhard Fohler, TUKL, DE; DREAMS)

Methods to ensure temporal correctness have profound impact on the resource usage of real-time systems. Many approaches focus on worst case situations. The resulting resource over dimensioning is acceptable in safety critical applications, but not in areas with varying resource demands and cost constraints, such as video processing. In systems dealing with applications of mixed criticality, the issue of handling both safety-critical as well as performance-oriented applications becomes paramount.

This presentation revisits the inspiration for the resource management approach and its development throughout a number of projects and application areas. It then highlights the novel issues in mixed criticality systems including safety-critical application and sketches the DREAMS approach and challenges for resource management in such systems.

3.3.3.2 Probabilistic Timing Analysis for Multi-cores (Mark Pearce, RAPITA, UK; Enrico Mezzetti, University of Padua, IT; PROXIMA)

The presentation gives a high level overview of Probabilistic Timing Analysis (PTA), focusing mainly on Measurement Based PTA (MBPTA), the refinement and industrialization of which is a key objective of the PROXIMA project. The conditions that must be met in order to undertake MBPTA are discussed as are some of the typical methodologies that have been used to undertake the analysis. Finally, some of the key challenges from the area of multi-core systems are discussed along with an indication of the direction future work is taking.

3.3.4 Session 4: MCS Platforms

3.3.4.1 TSP and Heterogeneous Models of Computation at Chip-level (Hamidreza Ahmadian, University of Siegen, DE; DREAMS)

In mixed-criticality systems, functions of different certification assurance levels are integrated on a shared distributed computing platform. To be able to guarantee these functions belonging to different assurance levels, certain requirements are imposed on the MCS platform in DREAMS. This presentation lists these requirements and focuses on two of them: time and space partitioning, and heterogeneous models of computation. It then explains the proposed solution in DREAMS.

3.3.4.2 Memory Interleaving (Marcello Coppola, ST, FR; DREAMS)

Embedded multi-core systems are getting more complex due to the integration of many applications and OSes, partly because of the energy efficiency, which is one of the key success factors. This implies a mix of application of different time-criticalities sharing hardware resources. With respect to real-time systems, providing predictable timing of the I/O subsystems with reduced variability in performance is a key challenge. The presentation talks about the work in progress that aims to tackle the before-mentioned challenge.

3.3.4.3 Chip-Level Platform for Probabilistic WCET Guarantees (Jaume Abella, BSC, ES; PROXIMA)

The advent of probabilistic timing analysis (PTA) and specially its measurement-based version (MBPTA) opens the door to obtaining tight and trustworthy WCET estimates with little burden for the end user. However, MBPTA places a number of requirements on the hardware. This talk describes those requirements, either upper-bounding or randomizing the timing behavior of hardware resources, and reviews how they are satisfied for multicore processors. This talk, then, points out how to satisfy them in the context of mixed-criticality manycores where heterogeneous guarantees are needed and hardware resources are massively shared.

3.3.5 Session 5: Model-driven Development

3.3.5.1 Modeling of Distributed Embedded Mixed-critical Systems (Julio Medina, Universidad de Cantabria, ES; CONTREX)

Modelling is now mature enough to tackle the modeling of current real-time systems. However, modeling needs the answers to the right questions in order to be help in the design of real-time systems. This talk sheds the light in this direction with the main message being “Modelling needs Questionnaires”.

3.3.5.2 Development Process for Mixed-Criticality-Systems and Modeling of Networked Multicore Systems[3] (Simon Barner, fortiss GmbH, DE; DREAMS)

DREAMS develops a hierarchical mixed-criticality architecture based on networked multi-core chips that includes both on-chip resources (e.g., processing cores, memory, Network-on-a-Chip (NoC)), off-chip resources such as computer networks, and software virtualization layers (e.g., hypervisors). This talk presents the development process that enables the design and implementation of mixed-criticality systems based on the DREAMS architecture and the corresponding resource adaptation strategies, and sketches the integration of safety, timing and security-aware development life-cycles. In particular, the talk presents how the AutoFOCUS3 (AF3) toolset (http://af3.fortiss.org/) will be extended in the scope of the project with a dedicated model of the DREAMS platform, and how the approaches enables the platform-independent description of mixed-criticality applications. Furthermore, it provides an overview of the view-points supported by AF3 (requirements view-point, logical architecture, technical architecture, and deployment view).

3.3.5.3 Variability Modeling (Øystein Haugen, SINTEF, NO; DREAMS)

The talk presents what variability modeling is – emphasizing that there are several different approaches to modeling variability and that there is no single approach that is the best for all occasions and that a mixture of the approaches are often preferable.

Then the talk presents the domain-specific language BVR (Base Variability Resolution) which is based on the legacy of CVL (Common Variability Language) a standardization drive within OMG. In BVR the variability model is a separate model referring to a corresponding base model in any language. A few examples are shown.

Finally, the talk presents how variability modeling and their resolutions can be applied in DREAMS to generate configurations, explore the architectural possibilities and provide optimal suites of test configurations. The SINTEF Tool Bundle for BVR is introduced and it is explained how this tooling will be adapted and enhanced in DREAMS.

[3] The talk was given by Dr. Christian Buckl (fortiss GmbH, DE) on behalf of Simon Barner (fortiss GmbH, DE).

3.3.6 Session 6: Extra-functional Properties

3.3.6.1 Analysis of Extra-functional Properties: Power, Temperature, and Degradation in MCS (Sven Rosinger, OFFIS, DE; CONTREX)

When safety-, mission-, and non-critical services are executed on generic HW/SW platforms several of the platforms extra-functional properties need to be considered in order to guarantee a safe coexistency of these services. Among timing, the platforms power consumption, its temperature and reliability as well as the coupling in between these properties is one of the main topics of the CONTREX project.

This presentation motivates the modelling of execution platforms extra-functional properties and incrementally describes an estimation and optimization flow to consider extra-functional properties during the design and in the design space exploration. The presentation concludes with a use case to which the flow will be applied.

3.3.6.2 Security in MCS (Thomas Koller, University of Siegen, DE; DREAMS)

In mixed criticality systems, the safety aspects cover unintended faults. Beside these unintended faults, there are faults which can be caused intentionally by a malicious attacker. By taking security aspects into account, protection against such intentional malicious faults can be provided. To analyze the security risks associated with a system and examine the potential threats and vulnerabilities, threat models need to be developed. This presentation introduces an approach to create threat models. It also presents the threat models for the different core services of the DREAMS architecture, such as for time synchronization, resource management, etc. The threats to the system, which are identified in the threat model, can be circumvented by providing appropriate security services. Identification of security threats, security services and mechanisms to protect against the identified threats are summarized in this presentation.

3.3.7 Session 7: Community Platform (Arjan Geven, TTTech, AT; DREAMS)

The talk focused on introducing the platform for the mixed criticality community – www.mixedcriticalityforum.org , that would act as a central place for aggregation of research and information related to the mixed-criticality. The website will be publicly accessible and registered members will be allowed to upload content as well. Currently, the website is in beta mode. It will be officially up and running in some time.

3.3.8 Session 8: Panel Discussion on Impact and Joint Exploitation

The moderator of the panel discussion was Alfons Crespo (UPV, ES; DREAMS), who first introduced the five panel members and then initiated the discussion. The five panel members were:

- Arjan Geven (TTTech, AT; DREAMS)
- Marcello Copolla (ST, FR; DREAMS)
- Ian Bruster (RPT, UK; PROXIMA)
- Adam Morawiec (ECSI, FR; CONTREX)
- Kim Grüttner (OFFIS, DE; CONTREX)

The discussion centered around two major points:

- Exploitation of results of R&D projects
  - One of the means of exploitation of results is through spinoffs and startups.
  - Non-technical gap between having an idea and for it to be commercially productive
    - In academia, the taxpayer’s money is used to fund researchers and scientists to come up with a great idea that could possibly last for 20 years.
    - But, in a company, it’s customer’s money. Now, the focus is to generate good ideas that are valuable to someone, quite likely in a shorter timeframe.
    - 2-3 years of timeframe for adoption of an idea is a very short timeframe. More time is needed for an idea to be commercially viable and successful.

    - Timeframe for exploitation also depends on the market domain targeted
        - Slow turnaround time in conservative domains like avionics.
        - Fast turnaround time in consumer domain.
    - Measurement of impact
        - Measure the impact of the elements that make up the project and not of the project itself.
- Joint Exploitation of results amongst R&D projects
    - Need a common theme between projects so that joint exploitation is meaningful and mutually beneficial.
    - Together, all projects are directed towards enabling technologies for the future.
    - Existing Standards and Certification processes do not provide guidelines for using of many/multi-core architectures in mixed-criticality systems.
    - Since, any of the solutions that enable use of multi-cores in mixed-criticality systems will eventually have to pass the certification process, synergy amongst the projects in this direction could be mutually beneficial.
    - A starting point could be pooling of requirements for mixed-criticality systems from the projects and then dividing them according to the use-cases (avionics, wind power, automotive, healthcare etc.) they support.
    - Then, a solution and a working demonstrator together with the combined efforts will be needed to convince the committees behind the concerned standards and certification, to change the respective documentation. The combined efforts are especially needed for any proposed change. This is because, if the presented approach/solution has the backing of the larger community then, it’s more likely that it will be accepted by the concerned standards and certification agencies.
    - Requirements from other domains like Healthcare, IoT move into automotive domain. EU, being quite strong in automotive domain, it is beneficial to follow the requirements in other fields which then helps in exploitation in the automotive field.

3.3.9 Session 9: Workshop Closure

In the closing remarks, Roman Obermaisser thanked all the participants and speakers who made the workshop a successful event.

3.4 Key Outcomes

3.4.1 Challenge 1: Opening of Conservative Standards

Standards in domains like avionics, automotive etc. are quite conservative for the main focus is on safety. Use of multicore-systems in mixed criticality systems warrants the modification of current standards in before-mentioned domains. Instead of focusing on modification of domain-specific standards (say) for use of multicores in mixed-criticality systems, it is more meaningful to change a single standard that could in turn have a ripple effect on domain-specific standards (DO178C/254, ECSS-E-ST-40C-80C). IEC 61508 is a widespread standard that traverses across various domains. This approach has the benefit of saving efforts, time and money. This is because directing efforts towards standard in each of the domain is quite expensive and time consuming.

3.4.2 Challenge 2: Certification for Mixed-criticality Systems

The objective of certification for mixed-criticality systems is to pave the way for the competitive development of the MC product families. Current efforts in this direction are geared towards composable certification by determining the strategy/rules for composability of the building blocks, supporting scalability.

3.4.3 Challenge 3: Modeling needs questionnaires

Modeling is quite mature and can be quite useful in the design and development of mixed-criticality systems. However, one needs to choose meaningful parameters to model the system and abstract the rest of the system. This requires asking the right questions in order to determine the useful parameters for modeling.

3.4.4 Challenge 4: Security in Mixed-criticality Systems

With the emergence of Internet of Things (IoT), threats to systems in traditionally conservative domains like avionics may increase. The security aspect needs to be considered in mixed-criticality systems from the design phase itself, in order for these systems to be safe.

3.4.5 Challenge 5: Guaranteeing reliability requirements in Mixed-criticality Systems

With regards to reliability and execution of tasks, there is a difference between safety-critical systems and mixed-criticality systems. Scheduling of tasks in mixed-criticality systems affects not only timing but also extra-functional properties like temperature, degradation etc.. This is better explained by an example: Consider a case where there are 5 tasks in a safety-critical system having a combined utilization of 0.7. Now, say the same 5 tasks alongwith 2 lower criticality tasks with a combined utilization of 0.9 are executed on a mixed-criticality system. In this case, the execution of lower criticality tasks leads to increase in silicon temperature, resulting in greater degradation than the case of safety-critical systems. Thus, the execution of lower criticality tasks in a mixed-criticality system needs to be monitored at runtime in order to make sure that the reliability constraints are met throughout the lifetime of the system, which is challenge.

4 Next Step – Third Workshop

The third workshop will be tentatively organized in Dec. 2014. It will be a scientific workshop specifically aimed towards developing of the research and innovation roadmap for mixed criticality by harnessing the collaborative efforts of the researchers from both academic and industrial areas. The outcomes (challenges, messages etc.) of the first and second workshop will serve towards laying the groundwork for active discussion amongst the participants in the third workshop.

5 Short Biography of the Speakers in the two Workshops

5.1 Jaume Abella

Jaume Abella is a senior PhD. Researcher in the CAOS group at BSC and member of HIPEAC. He received his MS (2002) and PhD (2005) degrees from the UPC. He worked at the Intel Barcelona Research Center (2005-2009) in the design and modelling of circuits and microarchitectures for fault-tolerance and low power, and memory hierarchies. He joined the BSC in 2009 where he is in charge of hardware designs for FP7 PROARTIS and PROXIMA, and BSC tasks in ARTEMIS VeTeSS. Jaume is also involved in two ESA-BSC bilateral projects and FP7 parMERASA. He has authored more than 15 patents and 60 papers in top conferences and journals. He is (has been) co-advisor of ten MS and PhD students.

5.2 Mikel Azkarate-askasua

Mikel Azkarate-Askasua is a researcher at IKR since 2008. He is currently working on the development of dependable traction systems for railway domain (up to SIL2). He holds a Master in Embedded Systems by the Ecole Nationale Supérieure d'Electronique, Informatique et de Radiocommunications de Bordeaux, Industrial Electronics Technical Engineering by Mondragon University and doctoral studies in Computer Science at Technische Universität Wien (TU Wien) in the field of safety-critical embedded systems (System On Chip). He has previously worked as grant holder at IKR and Technische Universiteit Delft (Holland).

5.3 Francisco Cazorla

Francisco J. Cazorla is a researcher in the National Spanish Research Council (CSIC). He is currently the leader of the group on Interaction between the Operating System and the Computer Architecture at BSC (www.bsc.es/caos). He is also an associated researcher in the Computer Architecture Department at the UPC.

He received his BS degree in 1999 by the University of Las Palmas de Gran Canaria, and his MS degree in 2001 by the same university (he was awarded best student record in Computer Science in 2001). He also has a PhD (2005) by the Universitat Politecnica de Catalunya(UPC).

He has worked in industry-funded projects with several companies and public-funded projects:

- **Public-funded projects**
  - SARC EU FP6 STREP Project
  - MERASA EU FP7 STREP Project
  - PROARTIS EU FP7 STREP Project
  - parMERASA EU FP7 STREP Project
  - VeTeSS EU FP7 ARTEMIS Project(2011 -)
- **Industry-funded:**
  - **Intel** (2004 - 2005). High performance fetch for MT processors. The main objective of this project was o increase the resource utilization in MT (SMT) processors by an smare resource allocation policy of proecesso reosurces.
  - **IBM** (2005 -). In this project IBM and BSC intend to pursue a Research Collaboration to enable BSC to analyze, understand and evaluate the behavior of SMT/CMP processor architectures, including but not limited to IBM's POWER5, POWER6 and POWER7 processors.
  - **Sun Microsystems:** (2007 - 2009). In this project BSC and Sun microsystems Inc. collaborate in the area of Chip Multithreading (CMT) systems. As CMT systems we use boards based on the UltraSPARC T1 and T2 processors. In particular the project

focuses on (1) Task scheduling of low-layer network-type of applications, such as IP Forwarding and (2) Analyzing the virtualization capabilities on the UltraSPARC T1 and T2 processors.

- **European Space Agency** (2010 -). More information at http://microelectronics.esa.int/ngmp/ngmp.htm

Francisco has led several bilateral projects with industry: IBM, Sun Microsystems (now Oracle) and the European Space Agency. He also currently leads the PROARTIS FP7 STREP EU project. He has three submitted patents on the area of hard-real time systems. His research area focuses on multithreaded architectures for both high-performance and real-time systems on which he is co-advising ten PhD theses. He has co-authored over 70 papers in international refereed conferences. He spent five months as a student intern in IBM‘s T.J. Watson in New York in 2004. He is member of HIPEAC and the ARTIST Networks of Excellence.

Francisco J. Cazorla has been selected as one of the 100 Spanish ‘leaders of the future&rsquo according to the May 2009 issue of the Capital Magazine. This issue seeks for the 100 young Spanish citizens that will most influence Spain‘s future in all innovation areas. (www.capital.es). He has also been awarded by the Massachusetts Institute of Technology (MIT), as one of the 10 Spanish young innovators under 35 years, whose technical work has been successfully applied in recent years or has a great potential for development in the coming decades.

5.4 Gerhard Fohler

Gerhard Fohler has been holding the Chair for Real-time Systems at TU Kaiserslautern since 2006. He received his Dipl. Ing. and Ph.D. degrees with honors from the TU Vienna, Prof. Hermann Kopetz, then was with the University of Massachusetts at Amherst, USA as postdoctoral researcher. Before joining TU Kaiserslautern, he was with MDH Sweden where he was promoted to full professor.

His research is based on issues in the field of real-time, embedded systems, with emphasis on adaptive real-time systems. Recently, it has been including related issues in real-time and control, real-time networking, real-time media processing, and wireless sensor networks.

He has been involved in a number of EU projects, coordinator and partner, and was core partner of the EU IST Networks-of-Excellence ARTIST.

He is Chairman of the Technical Committee on Real-time Systems of Euromicro, which is responsible for ECRTS, the prime European conference on real-time systems, member of the executive board of the real-time and embedded committees of the IEEE, where he chairs the sub-committee on conference afairs. He was program chair of the leading real-time conferences, and is associate editor of Springer's Real-time System Journal.

He has been serving as expert reviewer for the EU IST embedded systems unit and other funding agencies. He is Senior Member of the IEEE.

5.5 William Fornaciari

William Fornaciari is Associate Professor at POLIMI. He published six books and over 170 papers, collecting 5 best paper awards, one certification of appreciation from IEEE and holds 3 international patents on low power design. Since 1993 he is member of program committees and chair of international conferences in the field of computer architectures, EDA and system-level design. Since 1997 he has been involved in 12 EU-funded international projects and he has been part of the pool of experts of the Call For Tender No. 964-2005 – WING – Watching IST INnovation and knowledge, studying the impact of FP5 and FP6 expenditures. Recently, he participated to the projects MULTICUBE for design space exploration and the IP WASP on Wireless Sensor Networks. In FP7 he has been WP leader for the IP COMPLEX projects and Project Technical Manager of 2PARMA (ranked as success story the EU) and he also participates to the Artemis SMECY project on smart multi-core embedded systems. Currently, he is work package leader of the CONTREX IP project on mixed criticalities and Project Coordinator of the HARPA STREP project on embedded and HPC technologies to ensure dependable performance. He was for around 20 years with the CEFRIEL Technology Transfer Center of POLIMI, gaining significant experience in cooperating with international companies for the development of leading edge products: industrial exploitation of research ideas is one of his main attitudes. His main research interests cover multi-many core architectures, NoC, low power design, software power estimation, run time resource management, wireless sensor networks, thermal management, and EDA-based design methodologies. He is co-author of the first Italian book on embedded systems and he acted as project reviewer for EC-funded projects and invited speaker during EU consultation/information workshops and international conferences.

In 2013, he co-founded the startup Intelligence Behind Things Solutions (www.ibtsolutions.it) whose focus is the design of embedded applications including cyber-physical-systems.

5.6 Damien Hardy

Damien Hardy received a PhD degree in computer science from the University of Rennes I in 2010. After being a postdoctoral researcher at the University of Cyprus, he is since 2012 an Assistant Professor at University of Rennes I. His research interests include timing analysis of real-time software (worst-case execution times estimation), performance analysis and reliability.

5.7 Øystein Haugen

Øystein Haugen is Senior Researcher at SINTEF and part-time Associate Professor at University of Oslo. Over the last 5 years he has advocated, initiated and organized work on standardizing a Common Variability Language in OMG (Object Management Group).

Earlier he has been responsible in the International Telecom Union for the standard Z.120 on Message Sequence Charts (2000), and then responsible for Sequence Diagrams in UML 2 (since 2000). He has worked in several European projects relating to and experimenting with product lines such as FAMILIES, MoSiS, CESAR, VERDE and VARIES.

His main interests lie in language design and how proper languages may persuade its users to make good systems. Automation is the key and thus precision in the language definitions without sacrificing practical usability. He and his research companions have worked on tooling for language support and for testing product lines.

5.8 Carles Hernández

Carles Hernández is researcher at the Barcelona Supercomputing Center. He received the M.S. degree in telecommunications, M.S. in Computer Engineering, and PhD in computer sciences from Universitat Politècnica de València, in 2006, 2008, and 2012, respectively. His area of expertise include network-on chip and reliable digital circuits design. He is currently involved in parMERASA and PROXIMA FP7 projects, and in VeTeSS ARTEMIS project.

5.9 Hans Jürgen Herpel

Dr. Hans Jürgen Herpel has more than 20 years of experience in the field of embedded systems. This includes the implementation and design of hardware (boards, FPGAs, ASICs) and software for embedded system as well as the definition and implementation of a design methodology for these systems. The field of application ranges from automotive, public transport, aeronautics to space-borne systems. Currently, he is working as study manager and R&D coordinator for satellite software projects at Airbus Defence and Space, Friedrichshafen.

5.10 Kai Höfig

Kai Höfig received his PhD at the University of Kaiserslautern. He combined safety and timing properties to improve the certification of safety-critical embedded systems. Now he works for Siemens Corporate Technology as a consultant for model-based reliability and safety analysis. He continues to work with safety-critical systems and supports certification activities in various domains.

5.11 Thomas Koller

Thomas Koller is a research assistant at the University of Siegen, Germany. He studied Applied Computer Science with the main subject Electrical Engineering at the University of Siegen and received his diploma in 2013 with a thesis on “QoS evaluation of mobile operating systems considering Multi-Service-Testing” at the Qualigon GmbH. In 2013 he started to work as research assistant at the chair for Data Communications Systems at the University of Siegen in order to continue his postgraduate studies and receive a PhD. He is currently involved in the DREAMS project and woks on security engineering for mixed-criticality systems.

5.12 George Klokkaris

George Klokkaris is a graduate student at the University of Cyprus. He likes to work on problems related to Computer Architecture and Fault Tolerance.

5.13 Giorgio Di Natale

Giorgio Di Natale received the PhD in Computer Engineering from the Politecnico di Torino (Italy) in 2003. Currently, he is a researcher for the French National Research Center (CNRS) at the LIRMM laboratory in Montpellier. His research interests include test, reliability, and fault tolerance of digital and secure circuits. He serves the European group of the Test Technology Technical Council of the IEEE Computer Society as Chair.

5.14 Roman Obermaisser

Prof. Dr. Roman Obermaisser is full professor at the Division for Embedded Systems of University of Siegen. Currently, he is also involved with the DREAMS EU FP7 project as the project coordinator. He has studied computer sciences at Vienna University of Technology, and received the Master's degree in 2001. In February 2004, Roman Obermaisser has finished his doctoral studies in Computer Science with Prof. Hermann Kopetz at Vienna University of Technology as research advisor. In July 2009, Roman Obermaisser has received the habilitation ("Venia docendi") certificate for Technical Computer Science. His research work focuses on system architectures for distributed embedded real-time systems. He wrote a book on an integrated time-triggered architecture published by Springer-Verlag, USA. He is the author of several journal papers and conference publications. He has also participated in numerous EU research projects (e.g. DECOS, NextTTA) and was the coordinator of the European research projects GENESYS and ACROSS.

5.15 Mark A Pearce

Mark Pearce is a Senior Software Engineer at Rapita Systems Ltd, a company specializing in real-time software timing analysis. He obtained his degree in Microelectronics and Microprocessor Applications in 1986 from the University of Newcastle Upon Tyne, and later studied for an MBA at Henley Management College which focused on the development of an extension to the SEI's CMMI model to suit application to complex competitive systems engineering programmes. He has over 30 years of industrial experience, primarily working on complex embedded real-time systems integration projects within the Aerospace, Defence, Telecommunications and Healthcare industries. A large proportion of his industrial experience has also involved working within international collaborative programmes of work.

5.16 Daniel Gracia Pérez

Daniel Gracia Pérez is a Research Engineer at THALES with a PhD on Computer Architecture from Paris XI University. Currently, he is also involved with the DREAMS project as the leader of the work package that deals with avionics demonstrator. Previously, he participated in the creation of the UNISIM project, while working at the French Alternative Energies and Atomic Energy Commission (CEA). He has participated in various French and European projects including ANR SoCLib (work package coordinator), ANR Hecosim (work package coordinator), CATRENE COMCASS, OPEES, and ITEA TWINS. His research interests include computer architecture, networks on chip design, simulation, genetic algorithms and neural networks.

5.17 Jon Pérez

Dr. Jon Pérez is a Researcher at IKERLAN research center. He is currently head of the embedded systems research line and works in the design and development of safety-critical embedded systems, for example SIL4 railway signaling (ERTMS/ETCS). He is a certified TÜV Functional Safety engineer for the design of hardware and software based on the IEC-61508 standard.

He has received a B. Eng in Industrial and Robotics at Mondragon University, a M.Sc. in Electronics & Electrical Engineering with distinction at the University of Glasgow and he finished his doctoral studies in Computer Science at TU Wien in the field of safety-critical embedded systems.

5.18 Sven Rosinger

Sven Rosinger received the B.Sc. and M.Sc. degrees in embedded systems and the Ph.D. degree in engineering from the Carl von Ossietzky Universität Oldenburg in 2005, 2006 and 2012. In 2006 he joined the OFFIS - Institute for Information Technology and has been involved in several national and european research projects. Currently he is the project manager of the european FP7 CONTREX project.

5.19 Tullio Vardanega

Tullio Vardanega currently is an associate professor at the Department of Mathematics of the University of Padua, Italy, which he joined in January 2002. He holds a master degree in Computer Science obtained at the University of Pisa, Italy, in 1986, and a PhD in Computer Science obtained at the Technical University of Delft, Netherlands, while working at European Space Agency Research and Technology Centre (ESA/ESTEC). After working as project leader in a software consultancy firm in Pisa from November 1986 to June 1991, he was with ESA/ESTEC from July 1991 to December 2001, holding responsibilities for research and technology transfer projects ranging from software engineering methods and tools to real-time systems theory and technology, for use in the production of the software embedded onboard satellite platforms and launcher avionics. At the University of Padua he joined the Department of Mathematics where he took on teaching and research responsibilities in the areas of high-integrity real-time systems, quality of service under real-time constraints and software engineering methods, including model-driven engineering and component-based development, and related processes. He has been running a score of research projects in the areas of his research interests on funding from international and national organizations. He has been a member of IEEE for the last 20 years. He is the Italian representative in ISO/IEC JTC1/SC22, the international standardization subcommittee for programming languages, their environments and system software interfaces, where he is especially active in WG9 (Ada) and

WG23 (Programming Language Vulnerabilities). Since 2004 he is president of Ada-Europe, a Europe-based not-for-profit organization that promotes the use and the knowledge of Ada in academic and research establishments.

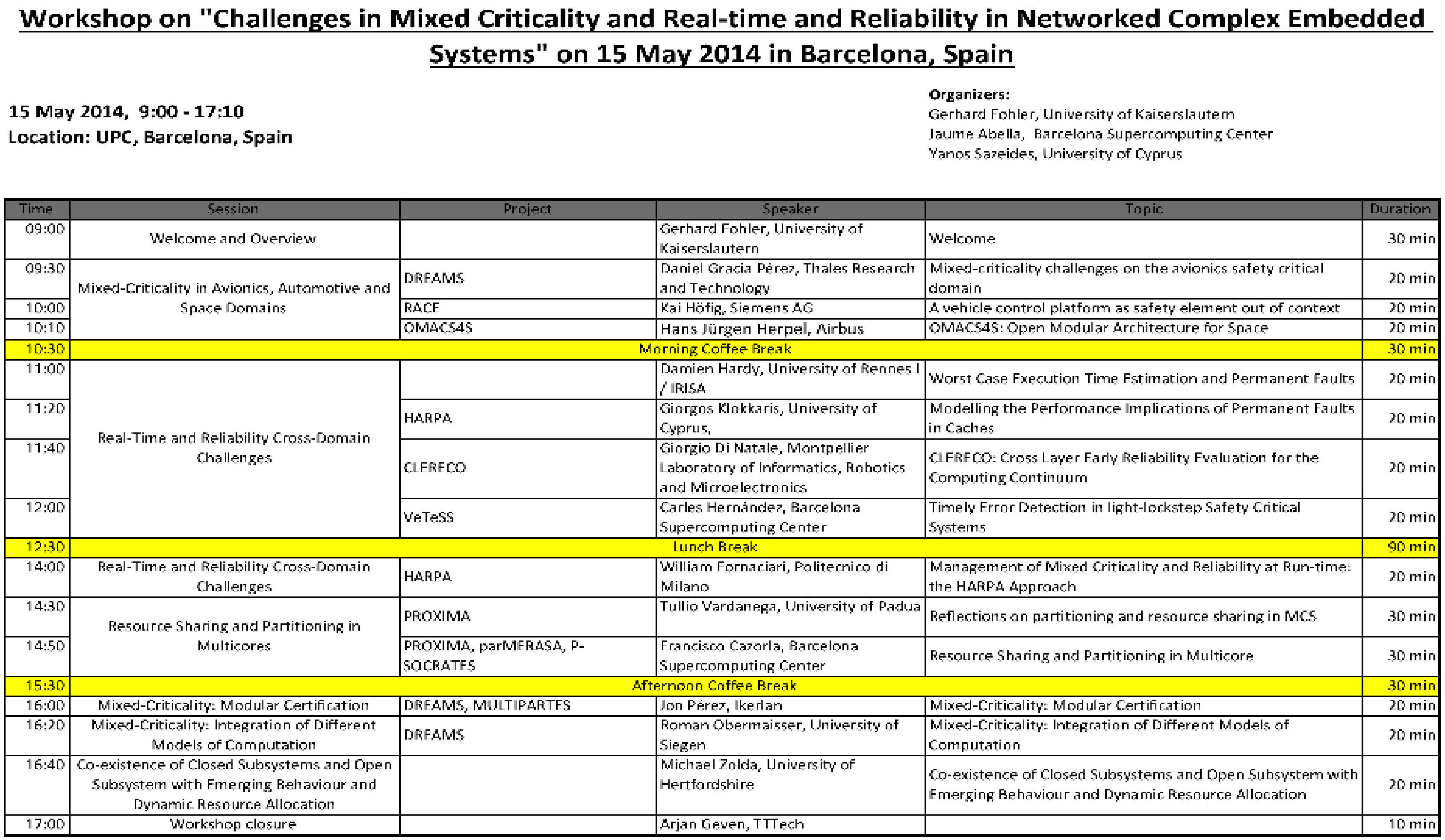
5.20 Michael Zolda

Dr. Michael Zolda is a research fellow at the University of Hertfordshire, UK. He received his doctoral degree from Vienna University of Technology in 2012. From 2007 to 2011 he worked on the FWF/DFG research project FORTAS-RT on execution time analysis of real-time systems. He has published multiple papers at acclaimed international conferences and workshops. Currently he is working on dependable stream processing systems within the EC/transnational research project CRAFTERS. He is also taking part in the European ICT COST Action TACLe (Timing Analysis on Code-Level).

6 Bibliography

[GB13] P. Graydon and I. Bate, "Safety Assurance Driven Problem Formulation for Mixed-Criticality Scheduling," *Proc. WMC, RTSS,* pp. 19-24, 2013.

Appendix A: Program of First Workshop



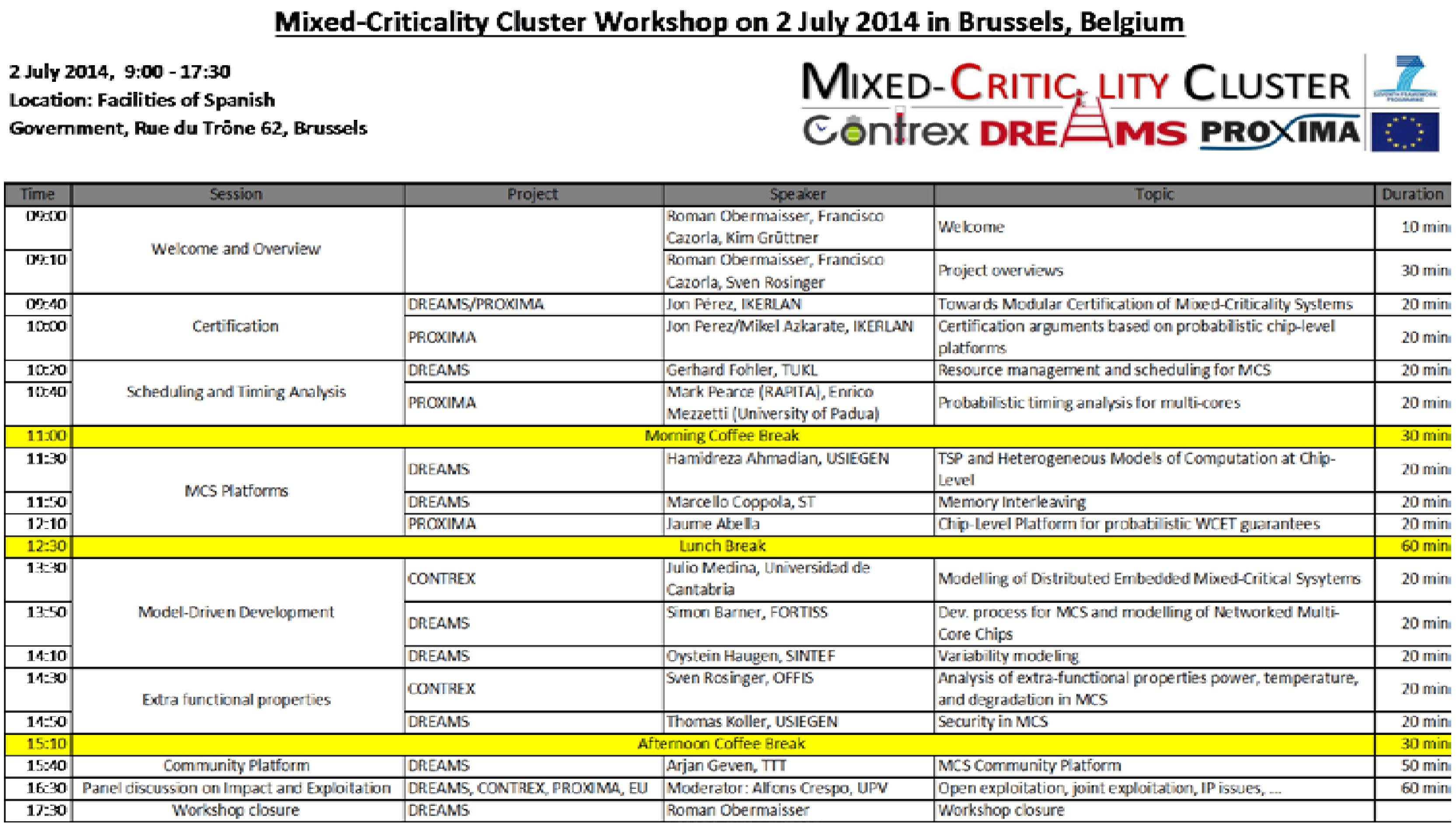
Workshop on "Challenges in Mixed Criticality and Real-time and Reliability in Networked Complex Embedded Systems" on 15 May 2014 in Barcelona, Spain

15 May 2014, 9:00 - 17:10
Location: UPC, Barcelona, Spain

Organizers:
Gerhard Fohler, University of Kaiserslautern
Jaume Abella, Barcelona Supercomputing Center
Yanos Sazeides, University of Cyprus

Time	Session	Project	Speaker	Topic	Duration
09:00	Welcome and Overview		Gerhard Fohler, University of Kaiserslautern	Welcome	30 min
09:30	Mixed-Criticality in Avionics, Automotive and Space Domains	DREAMS	Daniel Gracia Pérez, Thales Research and Technology	Mixed-criticality challenges on the avionics safety critical domain	20 min
10:00		RACE	Kai Höfig, Siemens AG	A vehicle control platform as safety element out of context	20 min
10:10		OMAC4S	Hans Jürgen Herpel, Airbus	OMAC4S: Open Modular Architecture for Space	20 min
10:30	Morning Coffee Break				30 min
11:00	Real-Time and Reliability Cross-Domain Challenges		Damien Hardy, University of Rennes I / IRISA	Worst Case Execution Time Estimation and Permanent Faults	20 min
11:20		HARPA	Giorgos Klokkaris, University of Cyprus,	Modelling the Performance Implications of Permanent Faults in Caches	20 min
11:40		CLERECO	Giorgio Di Natale, Montpellier Laboratory of Informatics, Robotics and Microelectronics	CLERECO: Cross Layer Early Reliability Evaluation for the Computing Continuum	20 min
12:00		VeTeSS	Carles Hernández, Barcelona Supercomputing Center	Timely Error Detection in light-lockstep Safety Critical Systems	20 min
12:30	Lunch Break				90 min
14:00	Real-Time and Reliability Cross-Domain Challenges	HARPA	William Fornaciari, Politecnico di Milano	Management of Mixed Criticality and Reliability at Run-time: the HARPA Approach	20 min
14:30	Resource Sharing and Partitioning in Multicores	PROXIMA	Tullio Vardanega, University of Padua	Reflections on partitioning and resource sharing in MCS	30 min
14:50		PROXIMA, parMERASA, P-SOCRATES	Francisco Cazorla, Barcelona Supercomputing Center	Resource Sharing and Partitioning in Multicore	30 min
15:30	Afternoon Coffee Break				30 min
16:00	Mixed-Criticality: Modular Certification	DREAMS, MULTIPARTES	Jon Pérez, Ikerlan	Mixed-Criticality: Modular Certification	20 min
16:20	Mixed-Criticality: Integration of Different Models of Computation	DREAMS	Roman Obermaisser, University of Siegen	Mixed-Criticality: Integration of Different Models of Computation	20 min
16:40	Co-existence of Closed Subsystems and Open Subsystem with Emerging Behaviour and Dynamic Resource Allocation		Michael Zolda, University of Hertfordshire	Co-existence of Closed Subsystems and Open Subsystem with Emerging Behaviour and Dynamic Resource Allocation	20 min
17:00	Workshop closure		Arjan Geven, TTTech		10 min

Appendix B: Program of Second Workshop



Mixed-Criticality Cluster Workshop on 2 July 2014 in Brussels, Belgium

2 July 2014, 9:00 - 17:30
Location: Facilities of Spanish
Government, Rue du Trône 62, Brussels

MIXED-CRITICALITY CLUSTER
Contrex DREAMS PROXIMA

Time	Session	Project	Speaker	Topic	Duration
09:00	Welcome and Overview		Roman Obermaisser, Francisco Cazorla, Kim Grüttner	Welcome	10 min
09:10			Roman Obermaisser, Francisco Cazorla, Sven Rosinger	Project overviews	30 min
09:40	Certification	DREAMS/PROXIMA	Jon Pérez, IKERLAN	Towards Modular Certification of Mixed-Criticality Systems	20 min
10:00		PROXIMA	Jon Perez/Mikel Azkarate, IKERLAN	Certification arguments based on probabilistic chip-level platforms	20 min
10:20	Scheduling and Timing Analysis	DREAMS	Gerhard Fohler, TUKL	Resource management and scheduling for MCS	20 min
10:40		PROXIMA	Mark Pearce (RAPITA), Enrico Mezzetti (University of Padua)	Probabilistic timing analysis for multi-cores	20 min
11:00	Morning Coffee Break				30 min
11:30	MCS Platforms	DREAMS	Hamidreza Ahmadian, USIEGEN	TSP and Heterogeneous Models of Computation at Chip-Level	20 min
11:50		DREAMS	Marcello Coppola, ST	Memory Interleaving	20 min
12:10		PROXIMA	Jaume Abella	Chip-Level Platform for probabilistic WCET guarantees	20 min
12:30	Lunch Break				60 min
13:30	Model-Driven Development	CONTREX	Julio Medina, Universidad de Cantabria	Modelling of Distributed Embedded Mixed-Critical Sysytems	20 min
13:50		DREAMS	Simon Barner, FORTISS	Dev. process for MCS and modelling of Networked Multi-Core Chips	20 min
14:10		DREAMS	Oystein Haugen, SINTEF	Variability modeling	20 min
14:30	Extra functional properties	CONTREX	Sven Rosinger, OFFIS	Analysis of extra-functional properties power, temperature, and degradation in MCS	20 min
14:50		DREAMS	Thomas Koller, USIEGEN	Security in MCS	20 min
15:10	Afternoon Coffee Break				30 min
15:40	Community Platform	DREAMS	Arjan Geven, TTT	MCS Community Platform	50 min
16:30	Panel discussion on Impact and Exploitation	DREAMS, CONTREX, PROXIMA, EU	Moderator: Alfons Crespo, UPV	Open exploitation, joint exploitation, IP issues, ...	60 min
17:30	Workshop closure	DREAMS	Roman Obermaisser	Workshop closure	