Mixed-Criticality Cluster Portfolio Analysis

Haydn Thompson

Report from the Mixed Criticality Workshop

Held on 19th and 20th May 2015 in Milan, Italy

June 2015

Communications Networks, Content and Technology Directorate-General DG CONNECT
http://cordis.europa.eu/fp7/ict/embedded-systems-engineering/home_en.html

Executive Summary

The Mixed-Criticality Systems Workshop was held in Milan in May 2015 to bring together the mixed-criticality projects (CONTREX, PROXIMA and DREAMS). This portfolio analysis presents the outcomes of the workshop and also provides some insights and analysis into the achievements to date and the future prospects for the work. A key aim of the workshop was to try and move from very technical descriptions of the work, which can only be understood by experts in the field, to more general descriptions that can be digested by people with a technical background but also by the public at large. Here it is important to be able to justify the impact of the work to the general public who are ultimately paying for the research.

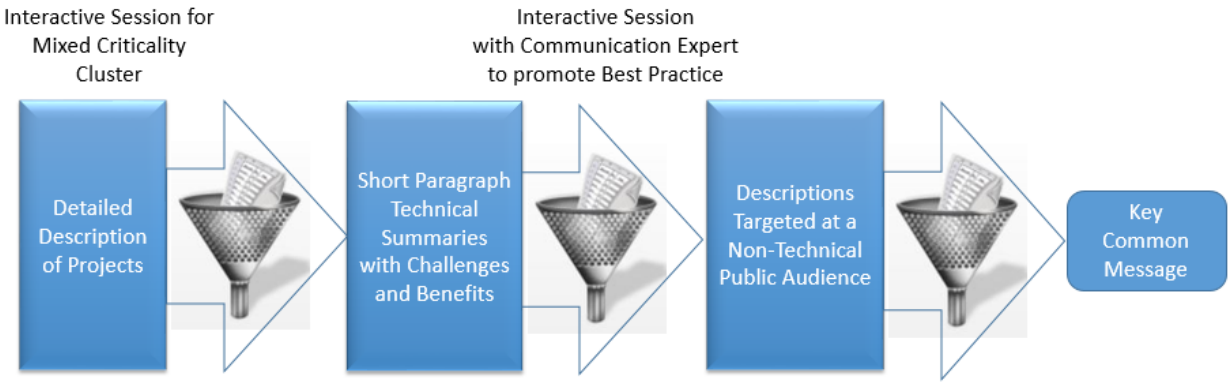

Fig. 1 Levels of Information Provided in the Report

This report is divided into sections. The sections are logically divided to present different levels of information:

- Highly detailed technical information for an expert audience
- Brief summary paragraphs for a general technical audience
- Brief description of projects and aims for a non-technical public audience, and
- An overall Common Message for the Mixed-Criticality Cluster

The intention of presenting the information in this way is to allow the material to be adapted and used for different target audiences. For ease of reading the report is presented in a “reverse order” starting with the brief descriptions targeted at the public, then short paragraphs targeted at technical people before providing more detailed overviews of the work and progress. In the final sections Best Practice for communications is described followed by the single common messages that were put forward in an interactive session.

The workshop itself was divided into highly technical sessions, briefing sessions and also a presentation was given by a Communications Expert on Best Practice for engaging with a non-technical audience. The workshop activities on communication highlighted how difficult it is to present information in a suitable and relevant way to the general public and non-technical audiences. Some useful tips were provided on how best to do this. An exercise was also run to try and establish a common message for the cluster. This led to a number of interesting proposals, however, many of these are still too obtuse for the general public. Based on the overall messages conveyed in the statements the author has presented a proposal for common message to disseminate to the public which is:

"Smarter and safer in an increasingly complex world"

However, a lot of work is needed to present a coherent and understandable message that can be used to engage with the wider public. The first steps to this have been made but a continued effort is required in order to promote and popularise the importance and need for research in mixed-criticality systems.

The projects have also come together to create a Mixed-Criticality Community. This brings together the 3 projects with other actors. Currently there are 6 projects, 69 organisations and 85 participants. Joint road mapping and joint dissemination is being performed and training has been provided for the next generation of engineers. Workshops are also being held to facilitate technology adoption. A first draft of an Innovation Roadmap has been produced highlighting research challenges. Looking to the future the projects will also make technology building blocks available. The three projects are working on a variety of use cases. These form a good basis for demonstrating the efficacies of the tools and methodologies developed. As the projects are addressing safety-critical applications the cluster is also jointly engaging with the certification authorities to ease the route to certification of future mixed-criticality systems.

Table of Contents

Overview of Mixed-Criticality Cluster

Mobility is central to Europe's citizens, we use cars, trains and aircraft for business and pleasure in our everyday lives. We want to know that these are safe. In the future adoption of multi-core processors with mixed-criticality functions will provide greater functionality giving us better and safer systems (e.g. assisted driving functionality), more options for entertainment – Internet surfing in the car, and greater connectivity and access to information.

Modern embedded applications already integrate a multitude of functionalities, with potentially different criticality levels, into a single system and this trend is expected to grow in the near future. Further, Europe is facing a once in a lifetime challenge with the advent of multi-core processors and the potential to integrate in a single platform systems with different levels of dependability and security, known as mixed-criticality systems integration. Without appropriate preconditions, the integration of mixed-criticality subsystems based on multi- and many-core processors can lead to a significant and potentially unacceptable increase of engineering and certification costs and runtime overheads. A mixed-criticality cluster has been established, which brings together the DREAMS, CONTREX and PROXIMA projects. The projects are performing joint road mapping and dissemination with the aim of creating a Mixed-Criticality Community.

Fig. 1 The Mixed-Criticality Cluster

The three projects that compose the Mixed-Criticality Cluster are shown in Fig. 1. The research being performed by each of these projects is addressing key aspects that need to be solved in order to allow Europe to create and develop new mixed-criticality applications.

CONTREX is working on techniques to allow different functionalities to be integrated onto multi-core platforms. Here the focus is on design and analysis of power consumption, temperature and timing constraints early in the design before hardware is available. Power consumption and thermal management is particularly important for applicitions that are battery powered, e.g. mobile devices.

PROXIMA is working on reliability, analysability and performance of multi-core sytems swith a concentration on development of a new technique for proving that time deadlines will be met. Traditional approaches cannot be used so the project is working on a new technique that uses probabilistic analysis. The project is working with the certification authorities to pave the way for early adoption of this technique in industry.
DREAMS is defining an architectural style for networked multi-core chips considering safety, security, real-time support and adaptivity. Here the aim is to quickly adapt functionality to different applications or “product lines” much as they do in the smart phone industry where different variants can be supplied with different functions. This product line approach based on a model driven methodology is targeted at promoting widespread adoption of the technology.

The projects are complementary addressing different aspects of mixed-criticality systems. There is only a very slight overlap between CONTREX and PROXIMA in the sense that they are both looking at timing analysis, the critical difference is that PROXIMA is developing a radical new approach to timing analysis which, if successful, will be a major change in the industry, whereas CONTREX is adopting a more traditional technique to timing analysis but in a holistic sense while at the same time also looking at power consumption and temperature and the interplay between the three.

The projects are closely driven by industry. Some of the applications are very near term, e.g. the CONTREX application for telematics is developing a “black box” to record minor car crashes and damage by vandalism when the car is parked – here the concept has been demonstrated with real hardware and software and the industrial interest in this has been shown by Vodafone buying the SME that started the project with the intent of rolling out products in the near term. Tools are also being developed that will be available to industry to help them develop mixed-criticality systems within 2 to 3 years. Other outputs from the Mixed-Criticality Cluster such as a new approach to certification of multi-core and many core systems need time to become accepted but may be adopted in the 5 to 10 year timescale.

Expected Impact for Industry and European Citizens

The expected impact is that it will be possible to adopt multi-core processors in future safety-critical applications in a variety of sectors such as automotive, aerospace, rail, medical monitoring, etc. This means safer systems for European Citizens, with much more functionality, which will be lighter, more compact and consume less power (reducing CO_2 emissions).

Workshop - Tell me your story - Communicating achievements in Mixed-Criticality Systems

A workshop was held in Milan to address communicating the achievements of the mixed -criticality cluster. Here the aim was to gather and present information on the impact of the work being performed and provide coaching on how best to present this information to a non-technical audience. A communication expert, Sabine Appelhagen, gave an overview of Communication Best Practices in particular to address communication with non-technical audiences. Each project in the cluster gave a 5 minute presentation on their key achievements explained for a nontechnical audience.

CONTREX

The CONTREX project explained the concept of mixed-criticality through the use of an animation based video to explain the idea of running different criticality software on a quadrotor which is used to provide surveillance. It was highlighted that the flight control system and camera control software could be run on the same processing platform and the consequences of a flight control system failure could result in a crash potentially leading to injuries. The wider context of mixing such criticality was also highlighted with applications in cars, aircraft, mobile phones and telecoms networks. On the platform the camera system has a low level of criticality. This consumes considerable power and heats up significantly. When a temperature limit is reached there is a need to switch off the unit to cool down. The consequences of this shut down are not critical just a loss of video for a while. For safety-critical functionality the hardware costs and development costs are high. For the camera control the hardware and development costs are far lower. The aim is to integrate both systems into one multi-core device using one powerful computer instead of two which results in lower power and cost. If the two systems are integrated then it is not possible to turn off the flight control when the camera overheats. CONTREX is thus developing tools to predict and control the temperature of electronic systems so that it is possible to keep the safety relevant parts going.

PROXIMA

PROXIMA is addressing development techniques for future real-time systems such as cars, aircraft and autonomous vehicles. It was noted that cars of the future will be computers on wheels and there is a move from mechanical to mechatronic systems. In these electronics, informatics and mechanics are brought together. Overall complexity is increasing and the number of lines of software is growing rapidly with a typical car having 100 million lines of code. Hardware is also getting more complicated and multi-cores is a key technology for the future. Cars, aircraft, etc. will become complex computing systems providing infotainment and safety-critical functionality operating on

the same hardware. There is a need to guarantee safety. Fundamentally, the current approaches to proving this cannot be used. Casual modelling from one system state via an event to a new system state is not scalable as systems become more complex. To address this a new approach is being developed where randomisation is being injected into timing analysis and system timing properties are proved using probabilistic and statistical modelling. The achievements of the project have been to investigate randomised behaviour on hardware. The project has also looked at software based techniques for use on COTs hardware employing real-time operating systems which is producing promising results.

DREAMS

In mixed-criticality systems there is a pressing requirement to reduce the number of computers and cables while adding more functions. Increasingly there is a need to integrate functions at different levels of safety. The trend is towards multi-core platforms due to limited scalability of uniprocessors and networked multi-core chips will be used in many domains in the future such as aerospace. The key achievements of DREAMS include definition of an architectural style, development of modelling methods to express properties, and development of techniques to provide security against attacks and to deal with unknown environmental conditions. A model driven development methodology has been produced and work has also investigated tools certification of mixed-criticality product lines. The project is looking at the feasibility of the approaches in real world scenarios promoting widespread adoption. The benefits are reduced development cost and time to market. Another aim is to achieve economies of scale by exploiting the approaches over larger markets. By consolidation of virtualisation solutions, in the future it is expected to be able to provide flexibility, adaptability and energy efficiency through integrated resource management, and also higher reliability, security and safety.

The feedback from this session from the communication expert was that although the attempts at communicating the project results were good they were more directed at a first year engineering student rather than a public audience. In particular, too much information was provided which made it difficult for a lay person to follow.

Problems Being Addressed, Benefits of Proposed Work and How the Projects Address Them

In this section the author has extracted the key messages in bullet point form for each of the projects to highlight the "Why?, What?, How?" for each of the projects in the cluster. This information allows the problems being addressed, the key benefits of performing the work and how the projects are addressing them to be quickly summarised.

CONTREX

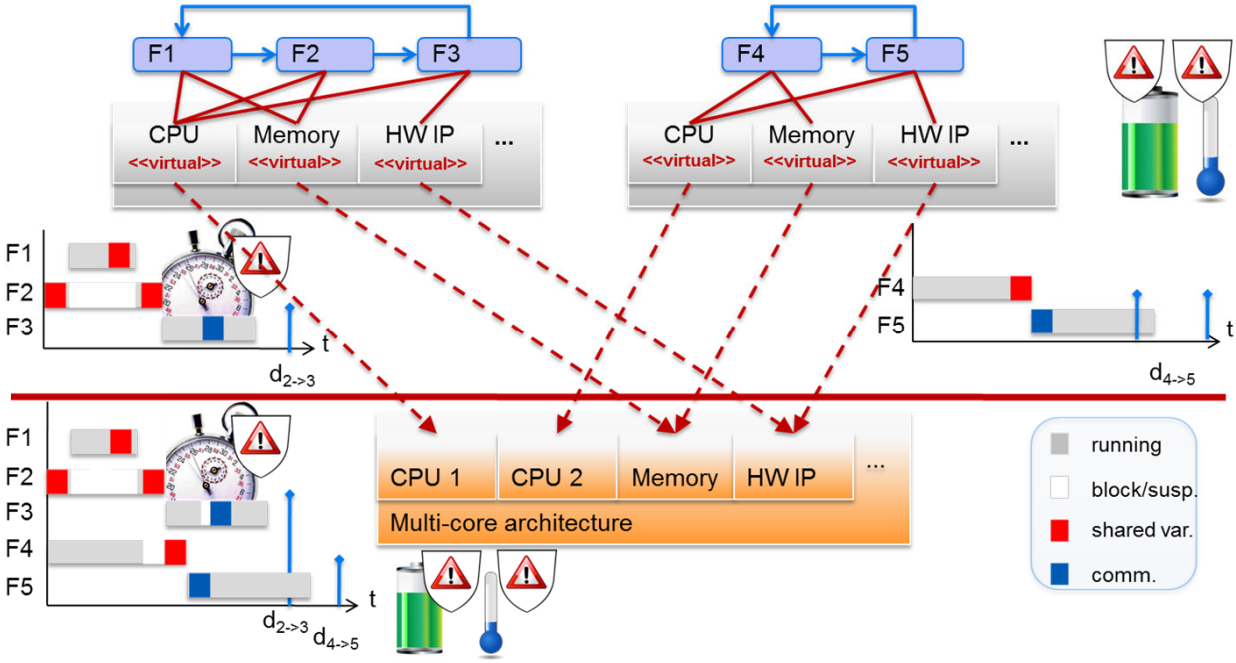

Fig. 2 Overview of CONTREX Project - Timing, Power and Temperature Analysis

Problem/Benefits

- Currently many systems are developed in isolation with physical segregation of safety-critical and non safety-critical functionality
- Many applications are limited by battery power, e.g. mobile phone
- Combining high and low criticality applications on multi-core processors reduces cost and power
- Sharing of resources, however, presents problems, i.e. we do not want to turn off critical functions if a non-critical function is causing device overheating
- Tools are required to analyse and develop new mixed-criticality applications

What is CONTREX doing to support this?

- The aim is to consider timing, energy management, temperature, etc. at the design phase so that different criticality functionality can be implemented on a multi-core platform reducing cost and power consumption
- Modelling techniques and a toolset are being produced that goes from design to simulation, to co-simulation with hardware
- Models for power and temperature are being incorporated into the simulation and analysis tools
- Addressing real world applications
  - Quadrotor for surveillance
  - Flight control for remote piloted vehicles
  - Automotive black box crash detection
  - Telecoms unit

PROXIMA

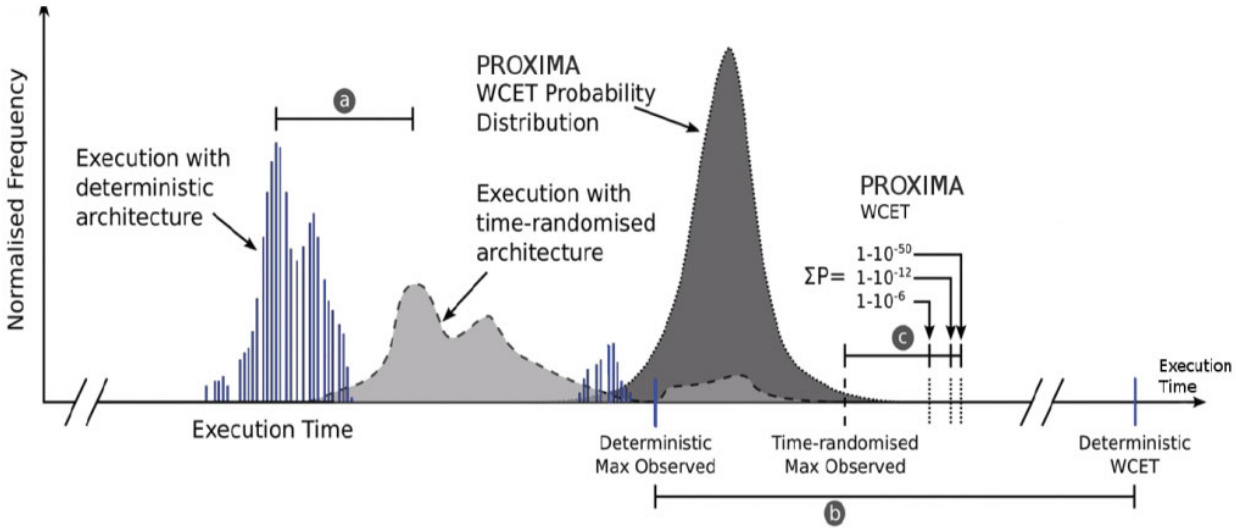

Fig. 3 Overview of PROXIMA Project – Probabilistic Timing Analysis

Problem/Benefits

- Electronics, informatics and mechanics are being brought together (mechatronics) in increasingly complex applications, e.g. aircraft, autonomous vehicles, etc.
- The number of lines of software is increasing rapidly (typical car 100 million lines of code) and so there is a move towards complex multi-core hardware
- These will mix non safety-critical, e.g. infotainment, and safety-critical functionality on the same processor - there is a need to certify such mixed systems and guarantee safety
- The problem is that it is impossible to use traditional timing analysis methods for certification based on casual modelling for multi-core devices

What is PROXIMA doing to support this?

- PROXIMA is developing a novel approach using randomisation in timing analysis
- Probabilistic and statistical modelling is used to provide timing guarantees allowing systems implemented on FPGAs and multi-core processors to be certified
- This has been shown to work theoretically and is currently being implemented and refined on real industrial hardware platforms
- PROXIMA is engaged with the certification authorities to gain acceptance of the concept and also with relevant industrial sectors
  - Aerospace
  - Space
  - Rail
  - (Automotive – yet to engage)

DREAMS

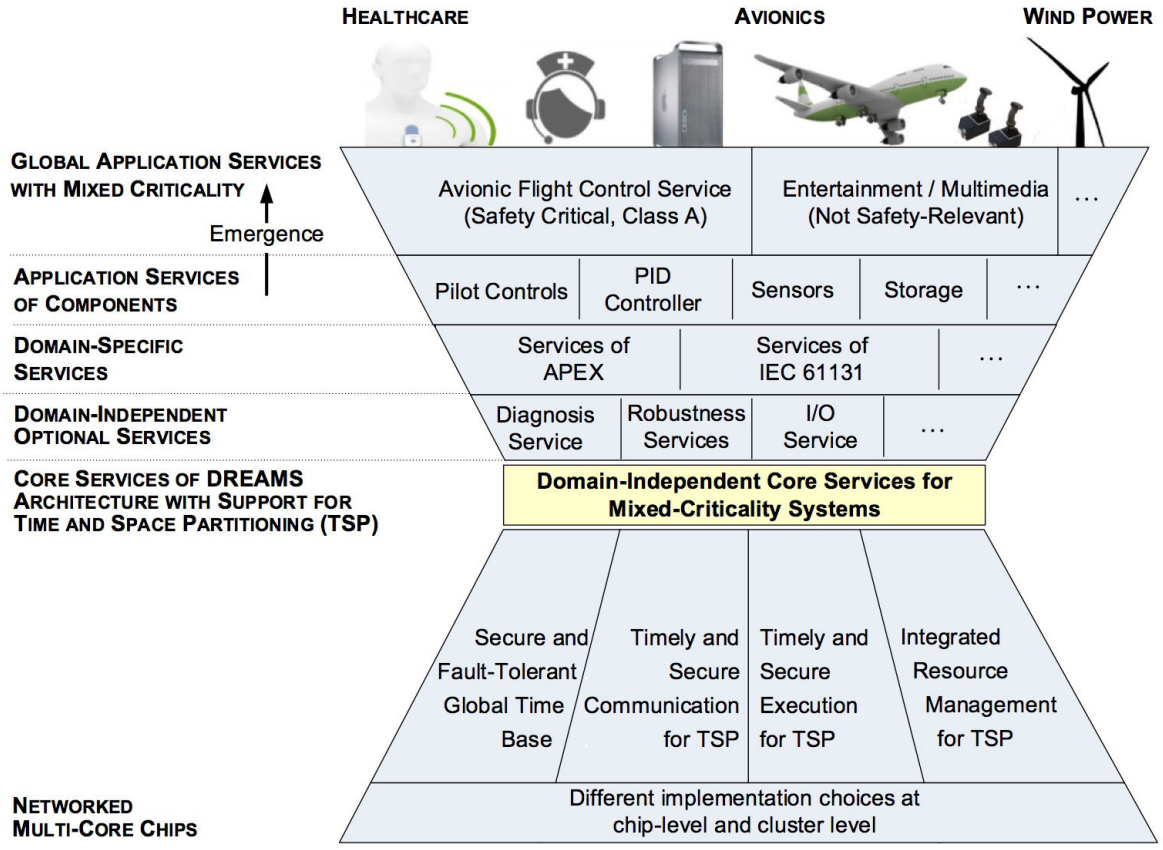

Fig. 4 Overview of DREAMS Project – Definition of DREAMS Architecture

Problem/Benefits

- There is a pressing requirement in many applications, e.g. aircraft, to reduce the number of computers and cables (reducing weight) while adding more functionality
- Traditional uniprocessors are no longer scalable so industry is moving to networked multi-core processors
- There is a need to reduce development cost and time to market for such systems
- There is a need to provide flexibility, adaptability and energy efficiency through integrated resource management
- There is a need to provide higher reliability, security and safety
- Economies of scale are needed so that companies can exploit over larger markets

What is DREAMS Doing to Support This?

- Definition of an architectural style for multi-cores and networks of multi-cores
- Development of a model driven development methodology and tools certification for mixed-criticality product lines
- Development of modelling methods and tools to provide performance benefits, security against attacks and to deal with unknown environmental conditions.
- The project is addressing real world scenarios promoting widespread adoption
  - Avionics
  - Wind Turbines
  - Video Streaming

Aim of the Mixed-Criticality Cluster

The mixed-criticality cluster has been formed to bring together the three projects to create critical mass to address key challenges. These are to:

1) Address extra-functional requirements in design and development, e.g., time, energy and power budgets, adaptivity, reliability, safety, security, volume, weight, etc.
2) Develop a certification methodology for mixed-criticality systems

To achieve these two key aims the following areas are being addressed through a combination of software virtualisation and hardware segregation, and via development of a supporting certification methodology.

- **Extra-functional properties:** In order to produce optimal implementations on multi-core devices it is necessary to ensure that a number of specific properties are satisfied. These extra-functional properties include timeliness, energy efficiency for battery-operated devices and dependable operation in safety-relevant scenarios. There is also a need for short time-to-market and low cost while at the same time adding increasing levels of functionality.
- **Timing Analysis:** The traditional approaches to timing analysis cannot be used for the increasingly complex multi-core and many core devices being developed. At a fundamental level new approaches need to be developed for temporal and spatial partitioning, which establish fault containment and the absence of unintended side effects between functions.
- **Certification:** Development of an approach to certification is crucial to allow multi-core devices to be used in safety-critical aerospace, rail and automotive applications.
- **Development methods:** State-of-the-art model-based design methods still lack of explicit support for modelling of mixed-criticality applications. Modelling and tool support is required to allow spatial and temporal segregation properties at the resource allocation or platform view, and for static or dynamic application to computation, memory and communication resource mapping.

The cluster is being led by DREAMS which has an aim to steer and increase the European R&D awareness in the area of distributed mixed-criticality and embedded computing systems via community building. Here the aim is to facilitate the exchange of ideas and also technological building blocks. In addition, efforts towards standardisation are being promoted. A further activity is development of a research and innovation roadmap for mixed-criticality systems.

A joint website has been established www.mixedcriticalityforum.org that provides a window on the projects and highlights the interactions between them. Additionally,

events are being organised to exchange information about technological results to the mixed-criticality community. These events also allow for collecting research problems, requirements and feedback on the work being undertaken. Here there is also engagement with other projects that are addressing mixed-criticality topics such as MultiPARTES, parMERASA and P-SOCRATES.

ARAMIS Project

The Mixed-Criticality Cluster is promoting links with other projects and supporting this a guest speaker, Olivier Sander, from ITIV KIT was invited to the Workshop to give an overview of work on the ARAMIS project which is addressing Automotive, Railway and Avionics Multi-core Systems. This is a German national project on multi-core technology. It was highlighted that systems are getting much more complex in aircraft and cars and there are no new innovations without the use of electronics. The degree of automation is increasing and a key enabling technology for this is embedded multi-cores. Single cores will not provide enough computing power in the future (the scaling according to Moore's Law is over). Multi-core processors are the future. It was also noted that systems are getting more and more connected. A challenge for industry is that there is a need to incorporate legacy code. This has been developed over many years at great cost and cannot be thrown away. There is also a move to allow customers to install their own apps provided by other companies on car hardware. A major challenge is that in multi-cores common resources are shared, e.g. memory, interconnect and peripherals. This leads to time interference, space interference and segregation issues. This can result in common cause failures and race conditions which are multi-core device specific as each has different connection architectures, etc.

ARAMIS is addressing these challenges together with safety, efficiency and comfort for automotive and rail applications. The consortium performing the work is large and includes the whole value chain (tier 1's, chip manufacturers and software providers) which in itself introduces problems as many of the partners are competitors. The project goals are to address architectures, safety, security, tooling and systems issues and produce working hardware and software for demonstrators. It was noted that virtualisation is a key technology.

Various roadmaps from the automotive, aerospace and rail industry have been analysed to try and produce a common viewpoint of what will be needed in the future. This highlighted that there is a need for research in design flows, design of fault tolerant multi-cores, definition of a common architecture, models, operating systems, middleware and application parallelisation. Overall there is a need to be deterministic at runtime and to be free from interference. Hardware security modules, security monitors and safety hardware are required. A knowledge base of hardware and software approaches for monitoring and redundancy in multi-cores is being compiled. A key enabling technology is virtualisation hardware support for peripherals and co-processors.

The project is also looking at tool chain integration and development of multi-core specific tools. Demonstrators are being created for a number of multi-core industrial use cases including an avionics use case for situational awareness and cabin management, a railway use case and four automotive use cases. Key drivers are safety and security.

In the automotive domain the main interest is in consolidation of architectures. The main aim is to have fewer units with more functionality. Multi-core virtualisation is seen as key to this. The car is divided into different functionalities, e.g., powertrain, chassis, etc. where the powertrain is classed as ASIL B (the highest level of criticality in automotive). In the future customers may want to download apps onto the automotive hardware so a laboratory and car demonstrator have been created for an infotainment system. Here the infotainment solution is integrated into the dashboard displays which also presents safety-critical information. An area is provided where Android apps can be downloaded.

Daimler have produced a demonstrator focused on GPU sharing. Here the aim is to do the rendering for the dashboard on a GPU with the aim for flexible display sharing and virtualisation of the instrument cluster.

BMW have produced a demonstrator addressing large-scale software integration using an embedded hypervisor. This is being applied to a powertrain application which is safety related. One partition is used for providing basic services and another one is used for running the powertrain.

Audi have a demonstrator for large-scale software integration. In this software components are being co-hosted on a shared AUTOSAR ECU platform. Notably here a speed up of 1.75 has been achieved through parallelisation of sequential tasks.

The AIRBUS avionics demonstrators are addressing situational awareness and cabin management. For aerospace weight is critical and the current computer modules are large and heavy. The driver in this application is to reduce SWAP (Size, Weight and Power) by putting everything into a single multi-core. A processor from the communications domain which has 8 PowerPC cores is being used. This consumes 30W but reduces the number of modules needed in an aircraft.

For the situational awareness demonstrator a multi-core module is being used to run radar applications for sensing obstacles and to steer aircraft. This application is driven by safety. A cabin management server has also been produced which allows different levels of functionality to be integrated. The intention is that in the future passengers will be able to bring their own devices and connect to system. This demonstrator is being driven by security.

In conclusion it was highlighted that the lessons learned and challenges of using multi-cores were far more complex than was expected in the beginning. No single multi-core architecture will meet the needs of all applications and there is a need for tailored multi-core applications. There is also a lack of available detailed information about what is going on inside a multi-core to allow certification. A positive step is that the certification authorities are now shifting their positon slightly from one where it was not possible to use multi-cores, to one where they were willing to discuss dual cores but not beyond this.

The Bigger Picture – Full Technical Achievements of Projects and Current Status

Each project also gave a more detailed overview of their work directed at a technical audience and to enable cross-fertilisation between projects. Here this is summarised giving the current status of each project within the cluster.

CONTREX

CONTREX is addressing segregation of applications with different criticalities. Analysis and segregation techniques for extra-functional properties, such as real-time, power, temperature and reliability are being developed. These properties risk becoming major cost roadblocks when:

- scaling up the number of applications per platform and the number of cores per chip,
- moving to battery powered devices or,
- 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 respect to application demands at different criticality levels. The CONTREX results integrate into existing model-based design methods and are customizable for different application domains and target platforms.

Overview, Status and Results (Kim Grüttner, OFFIS)

The motivation driving CONTREX is that currently many systems are developed in isolation. These systems can be compute and power intensive and in future will be integrated together onto a multi-core platform. This will require sharing of resources, space and time partitioning. In CONTREX although timing is being considered the focus is also on power consumption and temperature management. This is particularly important for battery driven systems. A key aim is to represent timing, power and temperature constraints early in development before hardware is available with the aim of analysing power efficiency and thermal management at design time. Power temperature and battery models are being used to model extra-functional properties. Requirements and “contracts” are being incorporated into a UML-MARTE meta model. It was noted that “criticality” is interpreted in different ways by different domains with associated classifications, e.g. D0-178B and IEC 61508. The research to date has shown that there are no standard power models and that the accuracy for models that

are available is not well documented. Getting information on processor platforms from SoC vendors is also difficult.

CONTREX UML/MARTE Modelling Methodology: Modelling mixed-criticality and Networks (Fernando Herrera, University of Cantabria)

A new CONTREX profile has been added to UML-MARTE. Extensions have been added for communications network modelling and mixed-criticality. Here it is possible to define applications with different levels of criticality. The interpretation of the levels depends on the domain, e.g. aerospace, automotive, rail, etc. (DO178B, ISO 26262 and IEC 61508). An approach to incorporating Worse Case Execution Time (WCET) has been produced and the methodology is being made available open source by the project.

Towards Joint-Analytical and Simulation-based Design Space Exploration Methodology for Mixed-Criticality Systems (Ingo Sander, KTH)

Analytical and simulation based design space exploration is being explored. The challenge is that the design space is very large. A new approach has been developed based on Adaptive Replica Search (ARS) to reduce the number of points that need to be considered. This reduces the time to find the Pareto set by selectively looking at the search space giving solutions in 20% of the time that other more general algorithms take. In this approach only solution points that are viable with respect to the constraints are considered. The KisTA and MOST exploration tools are being used on a voice activity detection example to demonstrate the concept. This has a hard constraint on throughput and the goal is to minimise the number of processers that are required. The next stage is to extend this to mixed-criticality systems with more objectives and provide a faster simulation tool.

Enabling Tools for Virtual Platform Integration (Franco Fummi, EDALab)

The aim of the virtual platform integration work is to provide better integration of tools and demonstrate effectiveness on the CONTREX use cases. Here there is a need for automatic configuration at the top level with the ability to include legacy RTL blocks. These are converted to SystemC. Functional and non-functional properties (temperature, power, reliability) are combined using the HIF Suite to integrate the tools. The thermal and power models are integrated into the virtual platform. Already this has been tried with a number of test benches showing that simulation time is reduced by using abstraction. Experimental results have also been produced for the CONTREX quadrotor and telecoms applications.

Run-Time Resource Management targeting Multi-/Many-core Architectures (William Fornaciari, Politecnico di Milano)

Run time resource management is required to match QoS requirements with resource availability. The work is targeting many core devices, multi-cores and GPGPUs. The approach being developed is suitable for both critical and best effort applications.

Deadlines are considered with respect to process variations and the needs to meet run time demands. This is targeted at platforms with a few to hundreds of processing elements. There is a need to deal with thermal management, systems reliability and fault tolerance. The BBQ-RTRM engine is being used running on top of Linux. With this tool it is possible to change the frequency or voltage of devices in the platform. The run time variability is tracked and then optimisation tools are used to provide system wide optimisation. The same framework can be used for design time and run time. The tool considers the application loop level and also the resources available. Currently this is being extended to many cores. Work with the Xilinx ZynQ board shows that it is possible to reduce temperature by using multi-cores while at the same time increasing the frame rate for a camera application.

Vodafone

A short presentation was also given by Vodafone who hosted the workshop. It was highlighted that every car maker is now looking at the service business opportunities and advantages of connected cars. Vodafone are particularly interested in telematics for the aftermarket in the insurance domain. This is being driven by insurance companies to avoid false claims, e.g. for whiplash, and also to gain a better understanding of drivers styles which may impact their insurance.

PROXIMA

PROXIMA leads on from the FP7 PROARTIS project. The aim is to use probabilistically time analysable (PTA) techniques and tools for multi-core/many core platforms. Randomization is selectively introduced into the timing behaviour of the hardware and software resources to facilitate the use of probabilities to predict the overall timing behaviour of the software and its likelihood of timing failure. PROXIMA is developing a tool chain including a multi-core PTA-compliant processor implemented on a FPGA and a commercial Operating System and Timing analysis tool. Four use cases from Avionics, Space, Rail and Automotive are being developed. A study on the feasibility of applying these techniques to COTS multi-core processors is also being performed.

PROXIMA goals and technical achievements of the project (Francisco J Cazorla, BSC)

The drivers from the aerospace, automotive, space and rail domains were highlighted indicating that there is a need for increased computation power. This could be achieved with single cores but a great number would be needed to meet requirements. A multi-core approach thus would be better. There is a need to address reliability, analysability, performance, and in particular, time determinism. The traditional approach used for this, which relies on transition from one system state to a new system state, is not possible as this is based on a causal approach. To address this issue PROXIMA is investigating a probabilistic model using randomised timing behaviour. Here a measurement based approach is being used to capture the probability distribution of Worse Case Execution Time (WCET) with a given level of confidence. The measurement based approach imposes some restrictions on the underlying platform. Crucially it cannot be applied

blindly to any COTS platform. The platform needs to be compliant. The analysis and deployment phases need control of inputs. A grey box approach is used considering sources of execution time variability. The WCET is deterministically upper bounded and time randomised. The hardware platform must be designed such that deterministic events have the same or higher upper bounded latency and probabilistic events have a distribution that matches or upper bounds that at deployment. Notably it is only necessary to do this when necessary, not for all hardware resources. The project is working with LEON3+FPGA, AURIX (3 core) and P4080 boards using PikeOS and RTEMS. A customised FPGA and industrial tool chain is being used for COTS FPGA default hardware. Already the project has developed hardware randomisation for FPGAs and also SW randomisation. In the future the project will address many core architectures.

Randomisation Injection: From HW randomisation for customized HW to SW randomisation in COTS platforms (Jaume Abella, BSC)

Hardware and software randomisation have been developed for the COTS AURIX and P4080 platforms which are used by industry. This covers random placement and replacement, fixed latency FPU operations and randomised arbitration for the bus and memory. Here the timing of individual components can be adapted but with limited modification. A key aim is to keep the overhead of the technique low. Interfaces have been developed to provide tracing allowing matching of timing analysis requirements. Random placement and replacement in caches is achieved using a random hash function. It should be noted that there are overheads in randomisation with currently 70% logic occupancy. This issue is being worked on. For software randomisation the project has successfully ported the code to a SparcV8 working on top of RTEMS-SMP proving the feasibility of the approach. The aim is to evaluate this with benchmarks. Additionally, some work is investigating software randomisation for self-modifying code on an AURIX platform. The aim is to make this transparent to the tool chain.

Path coverage under MBPTA: technique and initial steps towards its implementation in RVS commercial tool (Tullio Vardanega, University of Padova and Mark Pearce, Rapita Systems)

A key finding is that probabilistic bounds can potentially result in tighter bounds. The hardware overheads for the approach are considered acceptable. The approach is based on measurement, not static analysis. By taking measurements it is possible to get information about the past but not the future so it is necessary to learn from observations what is valid in the future. Extended Path Coverage developed in the previous PROARTIS project is being used to address path coverage. Although branches in code would be considered to be a problem in the approach the branches are probabilistically equalized with respect to timing behaviour. The original approach proposed was not acceptable to the certification authorities so a new approach called EPC based on MBPTA exploiting Control Flow Graph (CFG) knowledge over measurements has been developed. Here probabilistic padding is added to each block based on a probability distribution. This assumes that loop bounds are measured or

given. This approach is still competitive compared with other approaches even if a 20% industrial margin is added to the timings. Industrialisation for this is on-going but it is necessary to persuade tool providers that the approach is viable.

Certification aspects in PROXIMA (Mikel Azkarate-Askasua, IK4-IKERLAN)

The aim of this work is to pave the way for early adoption in industry by engaging with the certification authorities to foster standards and best practices. Another aim is to promote cross domain interactions. The DREAMS and PROXIMA projects have a common certification team which is talking to the certification authorities and also with end users from the railway, avionics and space sectors. Additionally, there is a desire to engage with the automotive sector, however, a link is yet to be made. Cross domain requirements have been elaborated and a rail safety concept has been proposed up to SIL4 using a traction system example. This utilises a quad core FPGA and an 8-core COTS processor. The feedback from the certification authorities is that is the approach needs to be supported with mathematical rigour and authority base.

DREAMS

The aim of DREAMS is to establish a European reference architecture for mixed-criticality systems by consolidating and extending platform technologies and development methods. DREAMS is considering multi-core platforms from a hierarchical system perspective for mixed-criticality applications combining both the chip- and cluster-level. A cross-domain architecture will be defined that supports multiple application domains, e.g., avionics, wind power, healthcare. DREAMS will deliver architectural concepts, meta-models, virtualization technologies, model-driven development methods, tools, adaptation strategies, and validation and verification to meet certification needs. The objective is to provide seamless integration of mixed-criticality to establish security, safety, real-time performance as well as data, energy and system integrity for future systems.

Overview, Status and Results (Roman Obermaisser, University of Siegen)

DREAMS is concentrating on a mixed-criticality architecture for networked multi-core chips with safety, security, real-time support and adaptivity. It is using a model driven methodology for mixed-criticality which is being evaluated with demonstrators. The project has performed requirements analysis, established a definition for architectural style and has produced a first version of the models with associated virtualisation and development methods. The models and virtualisation techniques are being demonstrated in use cases. A system model of a mixed-criticality system with fault and threat assumptions is being used with specification of architectural services and supporting certification strategy. Safety, security and timing are being considered.

Meta models have been created for the application and platform considering architectural, logical, technical and deployment viewpoints. A temporal viewpoint is provided that includes extra functional viewpoints of safety, security and power. A

variability viewpoint has also been created for product lines with associated model editors and toolsets. Gateways are used to bridge between nodes. Gateway tiles have been defined and partition tiles are used for running applications. The DREAMS arbitration layer provides communication and scheduling services for core services and communication services. At the chip level a hardware local resource scheduler is used that provides guarantees for rate constrained and time-triggered communications. The MEMGuard has been extended for bandwidth regulation. Real-time scheduling heuristics and I/O scheduling have also been included. The DREAMS abstraction layer (DRAL) has been created for system and partition management, monitoring and configuration, inter-partition communication, time management and scheduling. At the cluster level there is a gateway to wireless and wired gateways. For communication, segregation between different traffic classes is used. Cluster level safety and security services are provided. An analysis of the state-of-the-art in the area of scheduling has been performed and a compromise between online and offline solutions is being developed. Design space exploration is enabled by use of multi-objective evolutionary algorithms and variability modelling.

Certification validation and verification is being addressed through use of a modular safety case based on modular safety arguments considering the impact of one product on certification and also its impact on other products. A simulation framework is required for the chip, hypervisor and clusters. Several simulation tools have been provided that allow co-simulation to simulate end-to-end interactions.

Three demonstrators are being produced. One is addressing an avionics subsystem for flight management. Here timing isolation, fault management and performance are being considered. Another application is investigating a wind turbine application and a third is considering safety-critical health monitoring for the medical sector combined with an entertainment system.

Development Methodology (Simon Barner, FORTISS)

There is a need for tool support and to enable this the process has been split into different roles.

- System Architect
- Application Developer
- System Integrator

Offline resource allocation is used taking the input application and platform models to create a platform specific model. A DREAMS Meta Model has been defined giving architectural, logical and technical viewpoints. There is a temporal viewpoint and extra functional property viewpoints for safety, security and power. There is also a variability viewpoint for product lines. A number of model editors and toolsets have been developed. The technical viewpoint describes the hierarchical structure. It is also possible to describe non-functional properties such as failure rates and power estimations.

To provide the logical viewpoint a language is used to describe the application architecture. State automata are used that can be annotated with additional information on criticality levels and memory consumption.

To establish safety compliance a design space exploration module is used with optimisation goals, such as safety and estimated energy consumption of the system. Temporal constraints can also be imposed. It is also possible to include redundancy to meet safety requirements. The variability specification is used to define optional features in a product line. The intention of this is to ease certification and be more cost efficient.

Resource Management (Gerhard Fohler, TU Kaiserslautern)

A high quality video streaming application was described with applications in consumer electronics such as mobile terminals where cents of manufacturing costs are important. In considering resource dimensioning the worst case situation for memory would result in a design which was too expensive. It is not possible to use buffering as the requirement is for live video. The usual approach is to adopt a best effort approach and try and do it as quickly as possible. This results in bad quality and bad resource use. There is a need to meet end-to-end requirements while considering battery life and also temperature. The challenge is to match demand with availability as there is no point in playing “catch up”. In order to meet a QoS band a Global Resource Manager is used with a centralised view of the system state which provides new configurations, scheduling tables, resources, budgets, etc. In the initial implementation this communicated with local resource managers that deal with resources at the local level. Now a hierarchical resource management architecture is being adopted as many of the changes can be done locally without involvement of higher levels.

Community Building (Arjan Geven, TTTech)

The aim of the community building exercise is to promote R&D awareness in distributed mixed-criticality and embedded computing systems. It also supports the mixed-criticality cluster community. A project website and forum website have been set up with general information. This will disseminate the Innovation Roadmap and a catalogue of technology building blocks. A workshop was held at HIPEAC in 2014. Training is also being provided to the community to facilitate technology adoption. One aim is to create awareness of mixed-criticality at an introductory level through organisation of academic courses and seminars. A first draft of an Innovation Roadmap has been defined highlighting research challenges considering what needs to be done in 5 years’ time. The community currently consists of 6 projects, 69 organisations and 85 participants.

Best Practices in Communication

The session was introduced by Peter Martin from the European Commission who highlighted the importance of communicating outside of the scientific community to politicians and also to the general public. The rise of term "digital" was outlined being now a policy item of Commission with the establishment of the Single European Digital Economy. There is very much a need to be able to clearly explain in non-technical terms how EU research money is being used to support Europe's industry.

Sabine Appelhagen (FitForCamera), a communication expert, gave a presentation on how to explain scientific results to a wide audience outside of the scientific community.

This highlighted that it was not uncommon for scientists to dress up information in order to sell research and gain funding. An example is NASA who have a team of people who colourise the grey scale pictures produced by the Hubble Space telescope in Baltimore, using romanticised paintings as an influence. This is designed to appeal to the "spiritual" side of people making the stars look how we would like to see them.

There are 5 Magic Rules for Communication

1) Understand your Audience
2) Find the perfect message to go
3) Visualise, visualise, visualise
4) Tell your story
5) Serve everything with the Magic Sauce

1 Understand Your Audience

It is important to understand your audience – both old and young. Media is totally audience driven and a lot of effort is placed on getting viewing figures and establishing the interest of audience. For instance TV producers get the previous night's viewing figures every morning. There is also a lot of effort in working out what is a successful format or not. In preparing a presentation or dissemination output it is important to select a representative for your target group. An example is that for an afternoon TV show a TV station created a profile for their target audience. This was a lady called Gudrun who would be ironing in front of TV when watching the programme, her husband was a long distance trucker and she had 3 children. Whenever a topic came up which was being considered for inclusion in the show the team asked themselves whether Gudrun would be interested in this. In trying to establish at what level to pitch the idea it is useful to visualise a specific person to represent the target audience, this may be your grandmother or son.

It is then necessary to ask the right questions and give the right answers. There is a well-known technique for doing this called the 4MAT system which has 4 key questions:

- Why? - Why should I listen to you?
- What?- What facts do I need to understand this?
- How? - How does this work and how can I use it in practice?
- What if? - What will happen and what can I make out of this?

It is also best to put yourselves in the target audience's shoes. An example of best practice here is that researchers are using an "Age Suit" which a researcher puts on which makes mobility, sight and hearing more difficult replicating the problems that elderly people encounter. This is used to establish what makes life easier for elderly people.

It is also important not to talk about the process but to talk about the results. If you ask what the time is you do not want a description of how a watch works. It is necessary to chunk down the information and serve it to the audience. It is important never to use foreign words or technical terms. Here it should be noted that even "processor" can be considered to be a technical term.

2 Find the Perfect Message to Go

Here it is necessary to think about "if the audience can only remember one thing from a presentation what would it be?". An example here is newspapers where the reader will typically jump from one headline to another. The headline needs to entice the reader to read further if they are interested. A good key message:

- is concrete
- is simple
- is unexpected (perhaps provocative)

The key aim is to start the "cinema in your head".

3 Visualise, Visualise, Visualise

Tests have shown that a human remembers 10% of things that they hear, 20% of things that they read, 30% of things that they see and 70-90% of things that they feel. This is because in order to remember things it is necessary to connect both sides of the brain. The left side of the brain deals with analytics, figures and letters. The right side of the brain deals with emotions, colours and feelings. Long term storage involves both sides of the brain. It is this important to make people see your idea as pictures make you remember. It is even better if you can make people feel to give the outcomes of your project a face, make it move or make it touchable. Here the example of Al Gore presenting the Inconvenient Truth was highlighted as being best practice. His approach was to use a visualisation very effectively to get over a message to adults and children about the increase in CO_2 emissions.

4 Tell Your Story

It is important to tell a story. The best stories have a good structure. Here the Attention, Interest, Desire and Action (AIDA) approach from marketing is useful:

- Attention - generate awareness
- Interest - satisfy curiosity in what you offer
- Desire - stimulate their desire and wishes
- Action - provoke activity

A good story delivers a solution to a problem. It is notable that humans want to avoid pain and want to seek pleasure. An example of an advert for a skin cancer check was shown using Dalmatians which got over its message in an audience friendly way. It was highlighted that a good story lets your audience go on a trip. It is important to make them believe that you know where you are going and make them want to follow you. A good example of this approach to storytelling is the “One minute physics” web site that explains complex physics ideas in one minute in an accessible manner.

A good story has a personal touch and sense of humour. Here a video was shown of a lady explaining a project on TED artificial intelligence. In this a computer was being trained to recognise pictures. Although this was able to recognise some pictures it still failed in a humorous way to identify others. The presenter also empathised with the audience highlighting the difficulties that they had in gaining funding for the work.

5 Serve Everything with the Magic Sauce

Finally, it is necessary to serve the message with enthusiasm and passion. It may also be necessary to dress it up.

Exercise to Establish a Common Message

The cluster partners, helped by the communication expert and the rapporteur performed an exercise to elaborate common key messages. The intention of this was to identify a common "story" on mixed-criticality systems for the whole cluster.

The key questions to be answered were:

1. Why should people be interested in it?
2. What is it?
3. How does it work?
4. What can it do for the audience?
5. Where will it go?

It was noted that participants tended to answer 1-4 in a single statement. Below the responses have been transcribed from the sheets produced by the participants and organised into three categories:

- Why should people be interested in it and what can it do?
- What is it?
- Proposed Message

Why should people be interested in it and what can it do?

- Because products will work better
- Apps of different criticalities can co-exist reducing cost and space requirements
- It makes things more safe and ready for the future
- Take a flight without having concerns when someone is connecting to the on-board systems
- A car packed with computers to allow it to drive autonomously cannot carry people because it is too heavy and full. Mixed-criticality systems will make these systems small and safe.
- Lower cost, cheaper products become accessible to people
- Jobs in Europe, safety, energy, efficiency and more advanced electronic systems
- Reduce the amount of computers in an airplane, car (lighter faster cheaper) by putting more functions together. However, these functions should never interfere with each other in order to be safe.
- Mixed-criticality systems have a huge potential, for example bringing Head-up Displays to car drivers, without extra costs by integrating computers together
- We all spend long hours and considerable money travelling to work, for business, and on vacations.
- It affects people's security and safety
- People wish to be able to use a wide range of services but the important ones must work when needed

- With mixed-criticality systems we want to make room for more, with more efficiency and provide guarantees for everyone

What is it?

- It is in lots of electronics devices surrounding you in everyday life
- Critical and non-critical systems working on the same computers
- It is in almost every single computer device
- Mixed-criticality systems will be the basis for the design of future computers and all aspects related to IT
- Allows us to run lots of things at the same time while being cheaper and more efficient. However, we do not want the brakes coming on when the radio playing.
- A way to build computers such that they are safe, more secure and even faster

Proposed Messages

- Needed for the future to steadily increase the level of comfort in vehicles
- To make things safe
- Increase the quality of life in areas of healthcare and transportation
- Mixed-criticality systems save energy, save natural resources and increase planet life
- More powerful computers help cars/airplanes understand the world around them and help you get there safer
- Mixed-criticality systems - a threat to society? Will wrong use of sharing of resources cost lives?
- Mixed-criticality systems will allow us to travel 10 times faster spending $1/10^{th}$ of the money
- Think about driving your car with your family and the engine stops because your bank account reaches 0
- You want more from less
- Low cost, safe and feature-full transportation for everyone
- Smart transport means providing functionality similar to smart phones and tablets
- Less electronic waste with more comfort and safety in cars, trains and planes
- You should not fiddle with your car radio when coming to an intersection
- Would you like to drive a safe car and not be stuck in a traffic jam – mixed-criticality allows you to do this

It was noted that safety is a concept that people do not generally understand. They just assume that systems are safe. The expectation is that flights are safe and not delayed. The public does not understand (or even wants to understand) the details of how something works but for them it must work when needed otherwise they get annoyed. Although the proposed messages give specific examples related to automotive and aircraft a more general overall message headline has been derived by the author which is:

“Smarter and safer in an increasingly complex world"

Concluding Remarks

The Mixed-Criticality Cluster comprising DREAMS, CONTREX and PROXIMA is addressing key aspects of mixed-criticality systems as shown below.

Aspect	Project Addressing	Synergy/Opportunity
Extra Functional Properties	• CONTREX is addressing timing but also other physical properties of system components such as power consumption, temperature and reliability. • PROXIMA is concentrated on timing analysis but there are relationships to power and temperature	The approaches to timing analysis being developed by PROXIMA could be combined with the power consumption, temperature and reliability techniques of CONTREX to provide an "optimised" system solution considering trade-offs and attainment of multiple objectives.
Modelling	• CONTREX is developing models for extra-functional properties, e.g. power and thermal.	The models being developed are designed to be modular to be integrated into tool chains. Thus it should be possible to integrate these into both PROXIMA and DREAMS.
Compositional Reasoning	• DREAMS, CONTREX and PROXIMA are all using compositional reasoning and system construction, but in slightly different ways.	Synergies between the three approaches exist and there is an opportunity to investigate the effectiveness of the three approaches for the use cases.
Probabilistic Timing Analysis	• PROXIMA is developing a probabilistic approach to timing analysis of multi-core and many-core architectures.	This development is more at a fundamental level of developing a new approach that can be used for system certification. The approach should be universal being applicable to FPGAs, multi-cores and many cores given the proviso that the platform is "compliant".
Hardware Design	• PROXIMA is developing adapted hardware to assist with Probabilistic Timing Analysis.	This work supports the adoption of probabilistic timing analysis by definition of a compliant platform. This could be exported to the other projects.
Cross-domain architectural style for mixed-criticality systems	• DREAMS has defined an architectural style that supports multiple integration levels, cluster, multi-core chip, and hypervisor for a mixed-criticality system.	The opportunity here is to use this for exploitation at a wider level in multiple sectors.
Embedded RTOS	• DREAMS is developing a RTOS to support partitioning • PROXIMA is developing a RTOS to support randomisation	There may be an opportunity to combine both approaches in the future into a single RTOS.

Table 1 Aspects Being Addressed by the Mixed-Criticality Systems Cluster, Synergies and Opportunities

The projects are complementary addressing different aspects of mixed-criticality systems addressing certification barriers, challenges of optimising performance and

managing the complexity of design for multi-core applications. The outcomes of the cluster should lead to the ability to design new mixed-criticality systems in a more time and cost effective way, providing better performance from systems and also with the ability to analyse and optimise a number of extra functional properties. Critically the new approach to timing analysis has the promise of allowing future systems based on multi-core devices to be certified in safety-critical applications.

There are many synergies between the projects and this leads to opportunities for future joint work or comparison of results. These opportunities are highlighted in the last column of Table 1. Notably there is a slight overlap in topics being addressed between CONTREX and PROXIMA in the sense that they are both looking at timing analysis. PROXIMA is developing a radical new approach to timing analysis which, if successful, will be a major change in the industry, whereas CONTREX is adopting a more traditional technique to timing analysis while also looking at the interplay with power consumption and temperature.

Already the projects are performing joint road mapping and joint dissemination. Training has been provided to students to educate the next generation of engineers. Workshops have been run to facilitate technology adoption. A first draft of an Innovation Roadmap has been produced highlighting research challenges considering what needs to be done in 5 years' time. The Mixed-Criticality Community is growing and currently there are 6 projects, 69 organisations and 85 participants. Looking to the future the projects will provide technology building blocks. The work on use cases will raise the profile of the work and demonstrate the efficacies of the tools and methodologies developed. The joint approach to certification authorities by the cluster will ease the route to certification for future mixed-criticality systems.

The workshop activities on communication highlighted how difficult it is to present information in a suitable and relevant way to the general public and non-technical audiences. Some useful tips were provided on how best to do this but there is still a lot of work needed to present a coherent and understandable message that can be used to engage with the wider public. The first steps to this have been made but a continued effort is required in order to promote and popularise the importance and need for research in mixed-criticality systems.