“Smarter and safer in an increasingly complex world”

European Mixed-Criticality Cluster

Roman Obermaisser (Univ. Siegen)
Kim Grüttner (OFFIS)
Francisco J. Cazorla (BSC)
Arjan Geven (TTTech)

Motivation

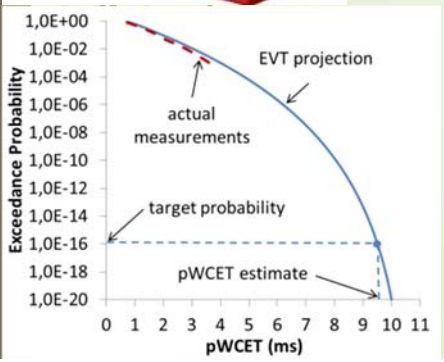
- Modern embedded applications already integrate mixed-criticality functionalities
- This trend is expected to continue with the advent of multicores.
  - ✓ Multicore benefits: higher degree of integration of systems with different levels of dependability and security, known as mixed-criticality.
  - ✗ Without appropriate preconditions, the integration of mixed-criticality multi-core processors can lead to a significant (potentially unacceptable) increase of engineering and certification costs.
- Grand challenge for EU industries in the integration of mixed-criticality systems in different domains having multicores and manycores as hardware computing platform

Derivate Challenges

- Timing: enabling integrated mixed-criticality multicore systems are mechanisms for temporal and spatial partitioning, which establish fault containment and the absence of unintended side effects between functions
- Certification: Key to enable exploitation of results in certain application domains such as railways or energy
- Extra-functional properties: timeliness, energy efficiency of battery-operated devices, dependable operation in safety-relevant scenarios, short time-to-market and low cost in addition to increasing requirements with respect to functionality.
- Development methods: with explicit support for modelling mixed-criticality

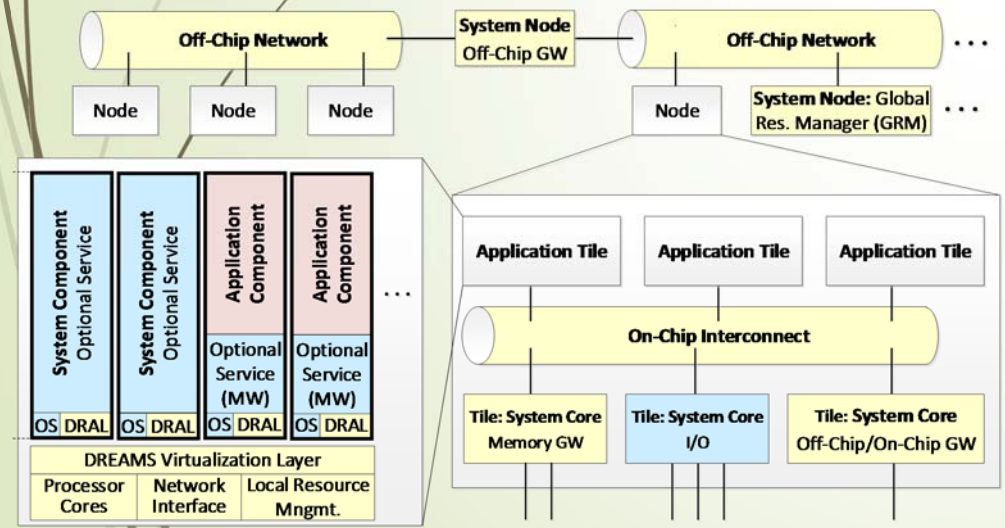
PROXIMA

- Provides industry ready software timing analysis using probabilistic analysis for multi-core real-time embedded systems
  - Improves standard measurement-based timing analysis on deterministic systems which find difficulties scaling to complex HW/SW
- Enable cost-effective verification of SW timing including WCET
- Industrial benefits
  - ✓ More performance using multi/many-core hardware in critical systems
  - ✓ Lower mixed-criticality integration costs with time-composable software
  - ✓ Cost-effective software timing analysis (WCET)
  - ✓ Certification arguments for DO-178B and safety standards



DREAMS

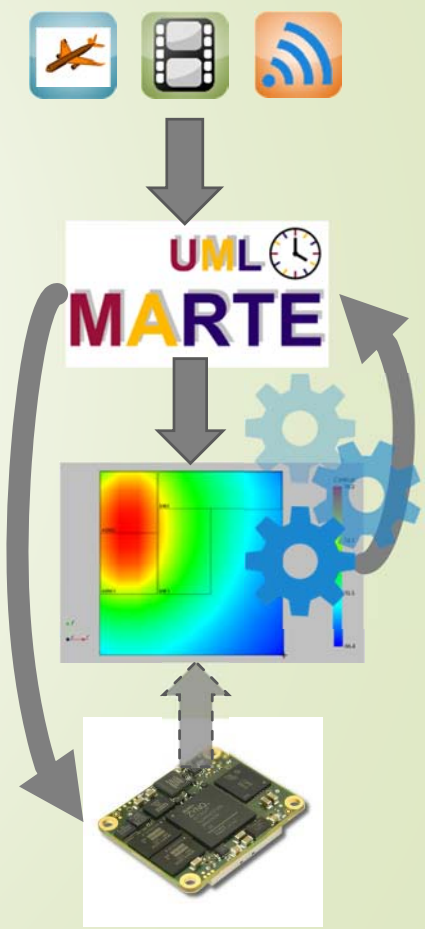
- Mixed-criticality architecture based on networked multi-core chips
  1. Architectural style, safety concepts, development methodology and tools based on MDE
  2. Virtualization technologies and adaptation strategies for mixed-criticality systems
  3. Demonstrators showing feasibility of DREAMS architecture in real-world scenarios
  4. Community building for widespread adoption



- Impact
  - Reduced cost and time-to-market
  - Exploitation of economies of scale
  - Higher reliability, security and safety due to virtualization
  - Higher flexibility and adaptability due to integrated resource management
  - System perspective of mixed-criticality systems combining chip and network level

CONTREX

- Provides tools for power and temperature specification, analysis and management in combined multi-core real-time and high-performance embedded systems
  - UML/MARTE modelling and analysis framework for extra-functional properties
  - Power and temperature aware simulation / virtual platform
  - Run-Time resource manager
- Enables energy efficient and cost-effective design of highly integrated systems
- Industrial benefits
  - ✓ Combined real-time and high-performance computing on multi/many-core hardware
  - ✓ Cost-effective integration testing based on virtual platforms
  - ✓ Support for energy constrained (e.g. battery powered) critical systems

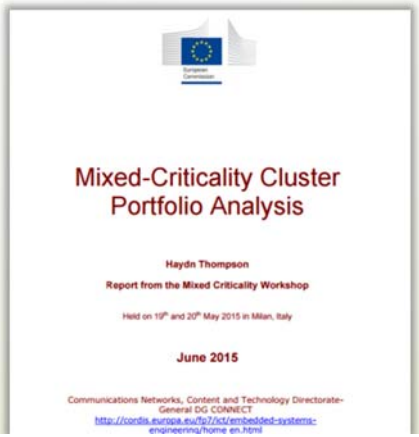


Joint Dissemination Impact

- Joint publications
- Joint workshops
- Joint meetings
- Joint booths at fairs and events

Joint Publications

- Trujillo, S., Obermaisser, R., Grüttner, K., Cazorla, F.J. and Perez, J., **European Project Cluster on Mixed-Criticality Systems**, 3PMCES Workshop (Performance, Power and Predictability of Many-Core Embedded Systems) at DATE, At Dresden, Germany
- Thompson, H., **Mixed-Criticality Cluster Portfolio Analysis**, Report from the Mixed Criticality Workshop, June 2015
- 14th June 2016 -The Advanced Computing and CPS collaboration workshop organized by HiPEAC in Brussels, jo**int MCC/PROXIMA, DREAMS and CONTREX pitches**
- 22th November 2016 – Cazorla, F.J., S., Obermaisser, R., Grüttner, **European Mixed Criticality-Cluster – Tackling future challenges in the design and development of Mixed-Criticality Multicore Systems,** Selected success stories for MCC Workshop, 22 November, 2016, Barcelona



Joint Workshops

- Joint workshops 2014
  - 2-Day MCS Workshop, January 22+23, 2014, Vienna (HIPEAC)
  - 1-Day Cluster Workshop, July 2nd, 2014, Brussels (PROXIMA)
- Joint workshops 2015
  - 1-Day MCS Workshop, January 19, 2015, Amsterdam (HIPEAC)
  - 1-Day Cluster Workshop, May 20, 2015, Milan (CONTREX)
- Joint workshops 2016
  - 1-Day MCS Workshop, January 18, 2016, Prague (HIPEAC)
  - 1-Day IMPAC Workshop, March 18, 2016, Dresden (DATE)
  - 1-Day Cluster Workshop, 22 November, 2016, Barcelona (PROXIMA)
- New MCS Workshop accepted in HiPEAC 2017


Amsterdam, Jan 2015


Milan, May 2015


Dresden, March 2016

Prague, Jan 2016

Joint Meetings

- CONTREX-BSC/PROXIMA meeting
  - Barcelona in September 16-17, 2015 co-located with FDL.
  - One-day meeting among CONTREX and PROXIMA aimed at exploring the combination of the technologies of both projects.
- Cluster telephone conference meetings
  - MCC telcos organized by CONTREX, DREAMS and PROXIMA coordinators ca. every 2 months or when needed for the allignment of common activities
    - 2014: April, Sept, Nov
    - 2015: Jan, March, May, July, Sept, Nov
    - 2016: Mar, May, July, Sept

Joint booths

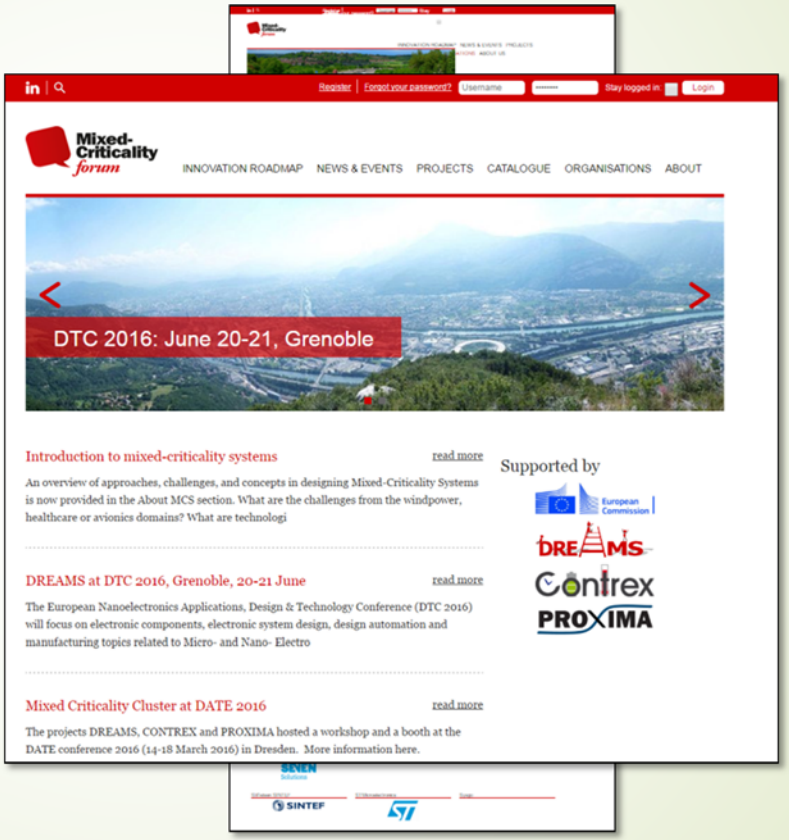
- Joint Booth (w. MultiPARTES) at DATE, March 2014, Dresden
- Joint Booth at ARTEMIS/ITEA Co-summit, March 2015, Berlin
- Joint Booth at DATE, March 2016, Dresden

DATE, March 2016, Dresden

Mixed-Criticality Forum

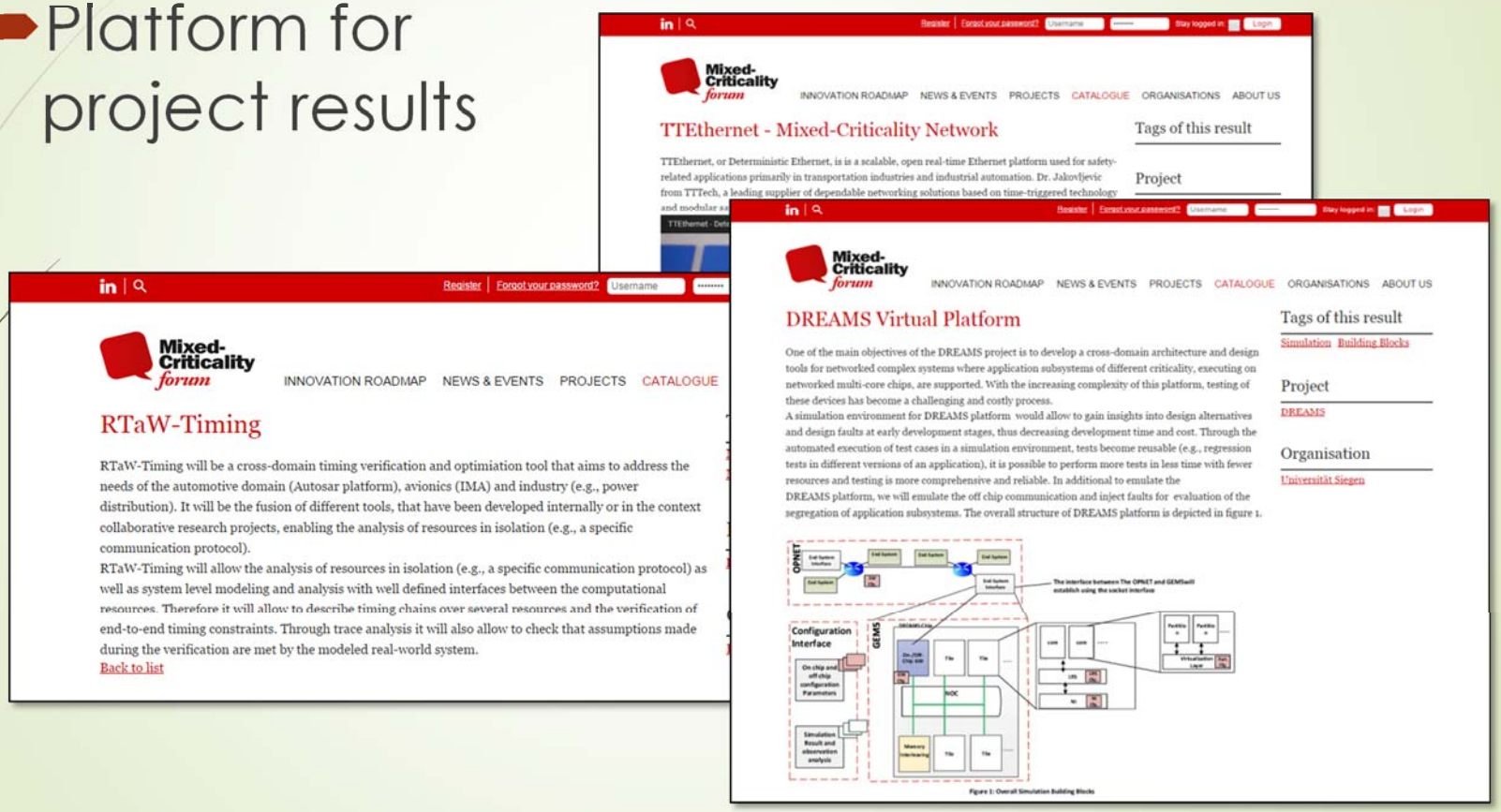
After ca. 24 months of mixed-criticality forum:

- 13 projects
- 83 organisations
- 125 participants



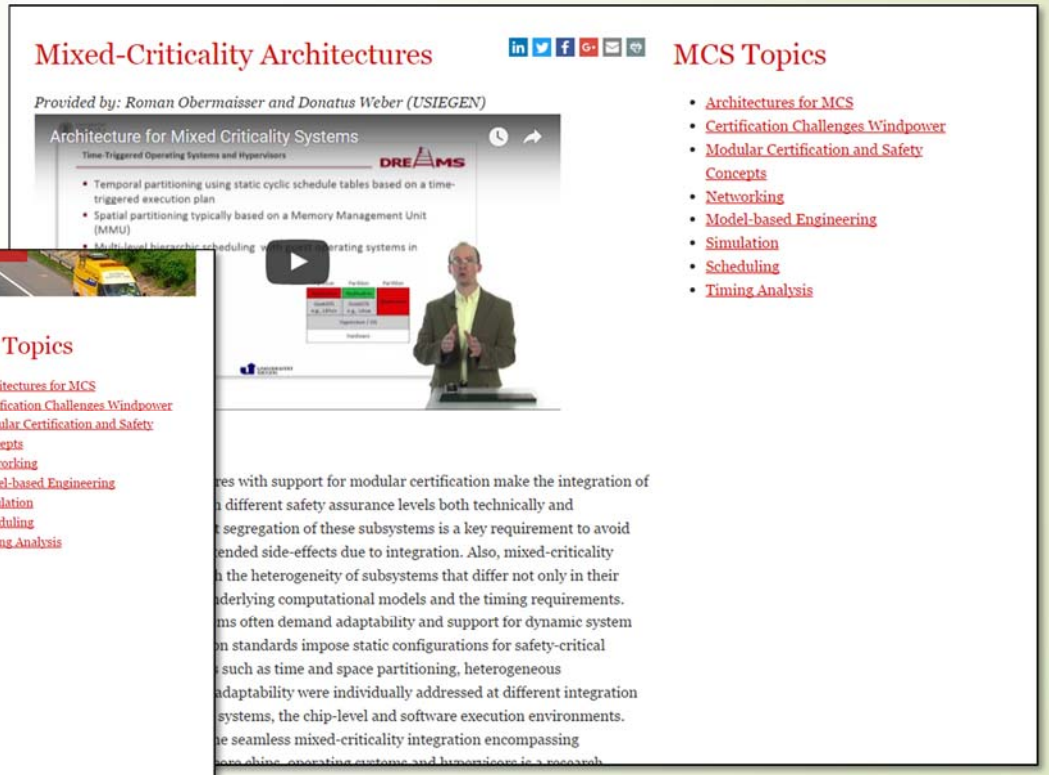
Mixed-Criticality Forum

- Platform for project results



Mixed-Criticality Forum

- What are Mixed-Criticality Systems



Mixed-Criticality Architectures

Provided by: Roman Obermaisser and Donatus Weber (USIEGEN)

res with support for modular certification make the integration of
different safety assurance levels both technically and
segregation of these subsystems is a key requirement to avoid
ended side-effects due to integration. Also, mixed-criticality
the heterogeneity of subsystems that differ not only in their
derlying computational models and the timing requirements.
ms often demand adaptability and support for dynamic system
n standards impose static configurations for safety-critical
such as time and space partitioning, heterogeneous
daptability were individually addressed at different integration
systems, the chip-level and software execution environments.
e seamless mixed-criticality integration encompassing

MCS Topics

- Architectures for MCS
- Certification Challenges Windpower
- Modular Certification and Safety Concepts
- Networking
- Model-based Engineering
- Simulation
- Scheduling
- Timing Analysis

Modular Certification and Safety Concepts for Mixed Criticality

Author: Imanol Martinez (IKERLAN)

Safety certification according to industrial standards poses many challenges as provide sufficient evidence to demonstrate that the resulting system is safe for its purpose.
A 'safety case' "represents an argument supporting the claim that the system is safe for a given application in a given environment". It provides I) arguments to demonstrate that safety properties are satisfied and risk has been mitigated, II) a notation mechanism that is often required as a piece of the certification process and III) interoperability among different standards and domains (e.g., avionic, automotive, railway).
A well partitioned safety case limits the impact of changes to a reduced area of the safety case and enables the reusability of these parts. Partitioning is a complexity management technique that subdivides the system into smaller parts (modules) that are independently generated and used to compose the system. On this basis, the implementation of modular safety cases potentially enables the reusability of predefined modules, reducing the overall complexity (simplification strategy) and supporting the limitation of change impacts to specific modules.
The modular safety case of a system component defines a set of minimum and reasonable arguments and evidences that the component should meet/provide in order to enable/support the development of mixed-criticality systems compliant with a domain specific safety standard. Different devices can fulfil this modular safety case using different strategies and solutions. Therefore a 'linking analysis' document must be provided for each

MCS Topics

- Architectures for MCS
- Certification Challenges Windpower
- Modular Certification and Safety Concepts
- Networking
- Model-based Engineering
- Simulation
- Scheduling
- Timing Analysis

Mixed-Criticality Cluster Outlook

- HIPEAC Workshop 2017
  - Organized by DREAMS, PROXIMA, CONTREX and SAFEPOWER projects
- Mixed-Criticality Forum
  - Publication of Draft MCS Roadmap
  - Publication of project results from the MCC projects

“Smarter and safer in an increasingly complex world”

European Mixed-Criticality Cluster

Roman Obermaisser (Univ. Siegen)
Kim Grüttner (OFFIS)
Francisco J. Cazorla (BSC)
Arjan Geven (TTTech)