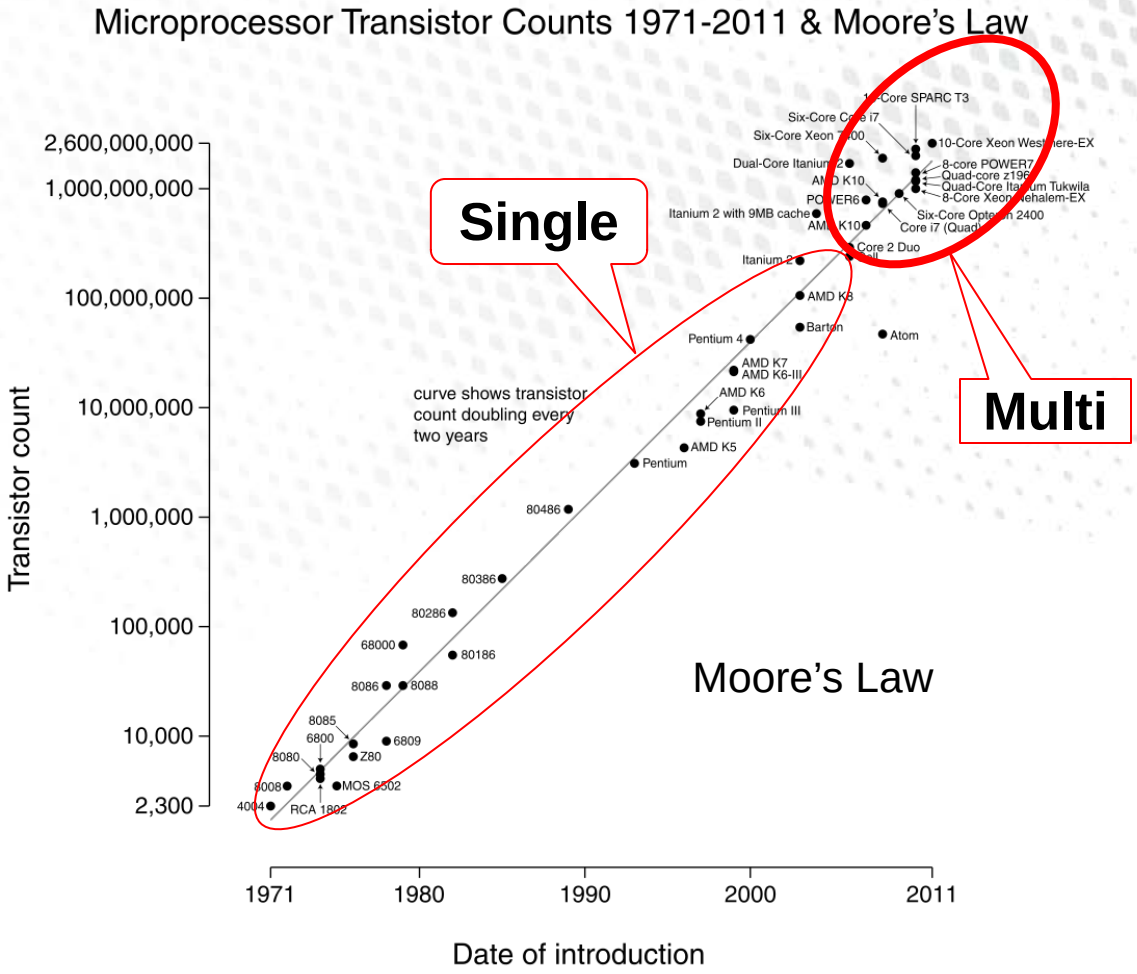
Open Architecture Platforms for Avionics Applications:
Challenges in Safety Critical Systems and possible solutions

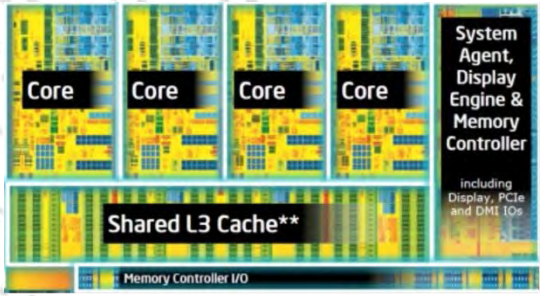
First TCRTS Workshop on Certifiable Multicore Avionics Systems (CMAS)
Seattle/WA, USA, 13.04.2015

Bernd Koppenhoefer

AIRBUS DEFENCE & SPACE

COTS HW Evolution - Single-Core → Multi-Core





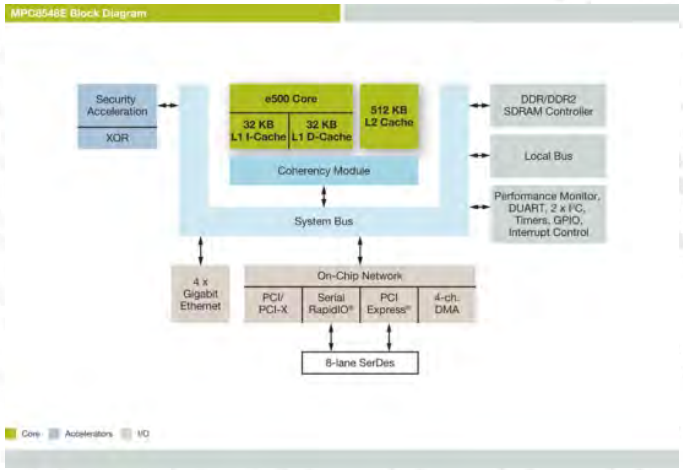
Intel Core I7

Source: Wikipedia, Die freie Enzyklopädie, 17.02.2015, https://de.wikipedia.org/wiki/Datei:Transistor_Count_and_Moore%27s_Law_-_2011.svg

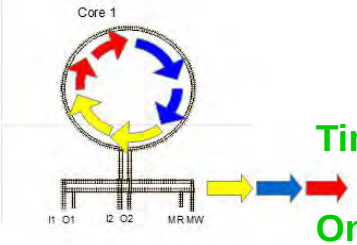
AIRBUS DEFENCE & SPACE

Challenge From Single-Core to Multi-Core

MPC8548



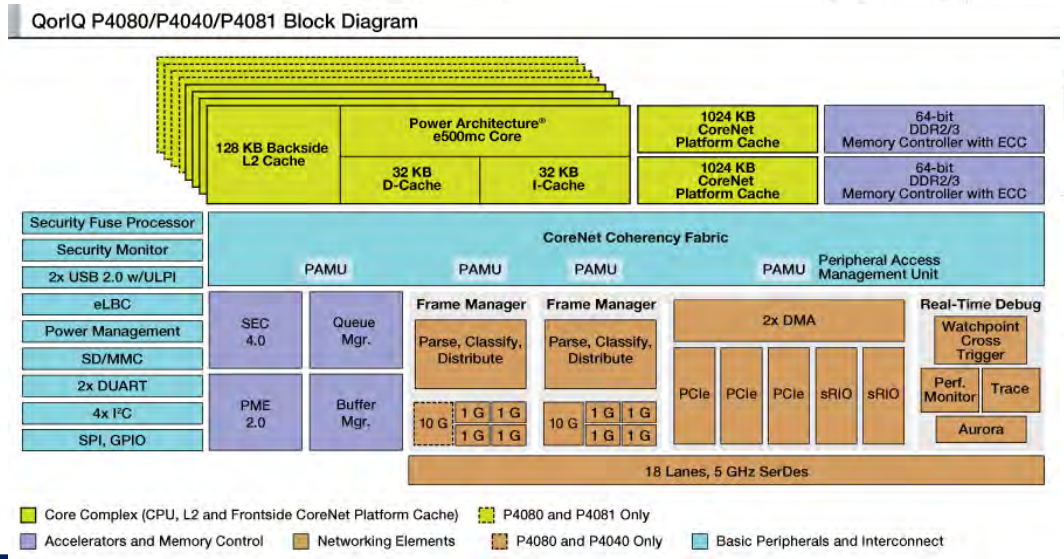
Proven - predictable



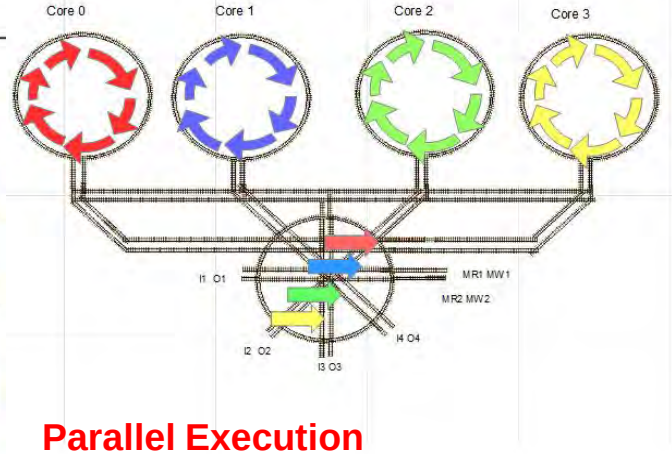
Time Partitioning

Only one SW is running at a given time

P4080



Is this still predictable ?



Parallel Execution

We can not predict the exact timing

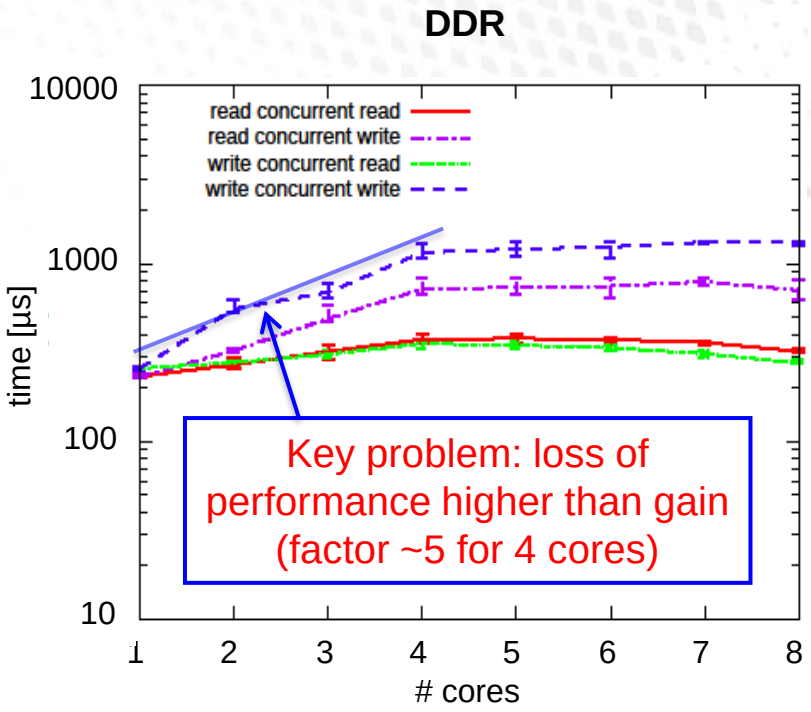
Source: *www.freescale.com*

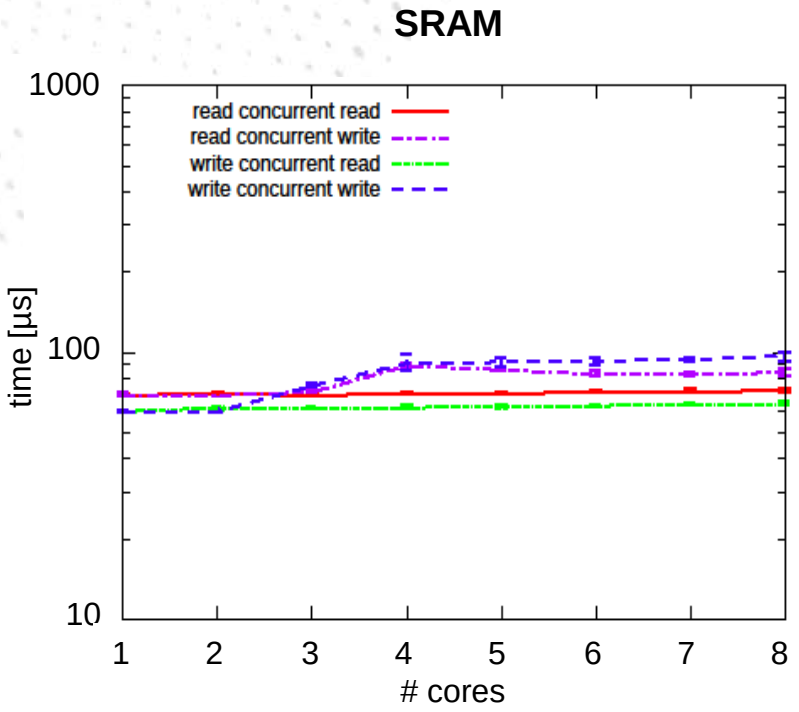
AIRBUS DEFENCE & SPACE

Example Freescale P4080 Evaluation Results

Source: "Leveraging Multi-Core Computing Architectures in Avionics", Jan Nowotsch, Michael Paulitsch
Ninth European Dependable Computing Conference, 2012, DOI 10.1109/EDCC.2012.27

- Maximum interference of one core by other cores test setup for DDR vs. SRAM (Level 3 Cache)
- Concurrent access to memory regions (4kB regions, 64B gap, 1 to 8 cores, …)





AIRBUS DEFENCE & SPACE

Multi-Core Processor (MCP) Research
… what is going on in Europe?

Selection of EU research projects on MCPs in Safety-critical Applications*)

*) *Automotive, **Avionics**, Industrial Manufacturing and Logistics, Internet of Things, Space*

• ACROSS:	EU funding;	04/2010 to 09/2013;	16 Partner;	Total Budget	16 M€
• RECOMP:	EU funding;	04/2010 to 03/2013;	41 Partner;	Total Budget	26 M€
• ARAMIS:	National (German) funding;	12/2011 to 11/2014;		Total Budget	37 M€
• EMC²:	EU funding;	04/2014 to 03/2017;	98 Partner;	Total Budget	100 M€

Other Multi-Core Activities:

- MCFA (Multi-Cores for Avionics Working Group); since September 2011:

  "AUSTIN, Texas--Freescale Semiconductor (NYSE:FSL) has formed a working group with top North American and European commercial avionics manufacturers to define their information requirements for advanced Freescale multicore processors being used in commercial avionics applications."

  http://www.businesswire.com/news/home/20110914005110/en/Freescale-Collaborates-Avionics-Manufacturers-Facilitate-Certification-Systems

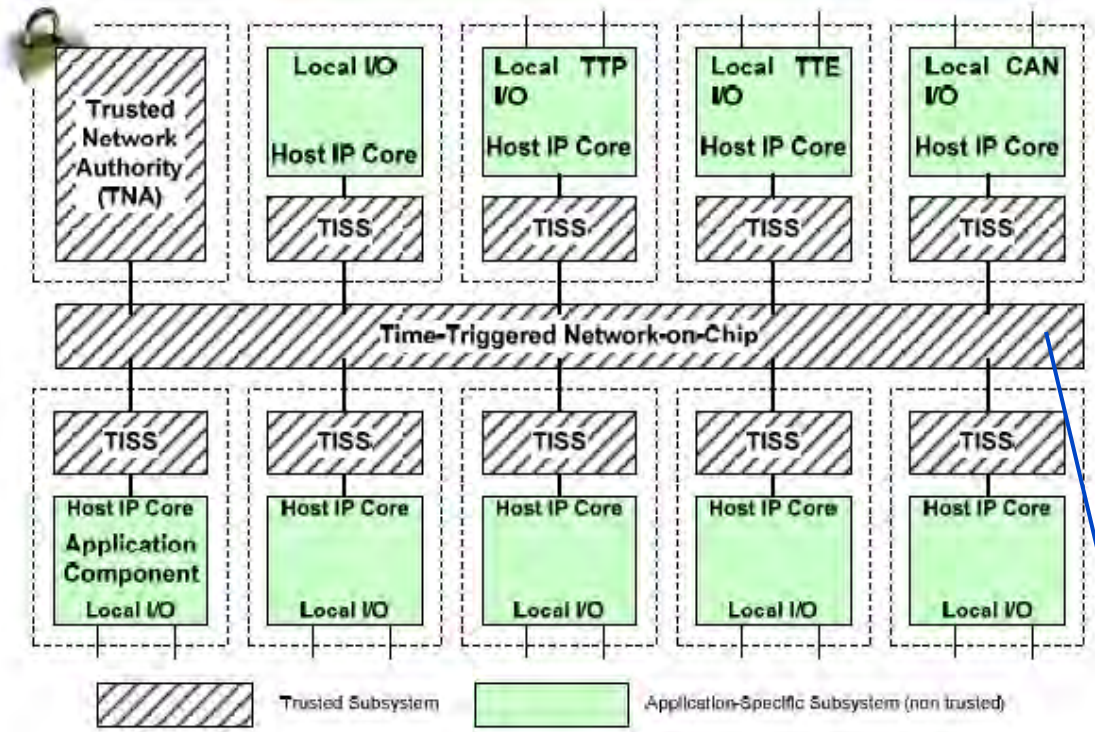
AIRBUS DEFENCE & SPACE

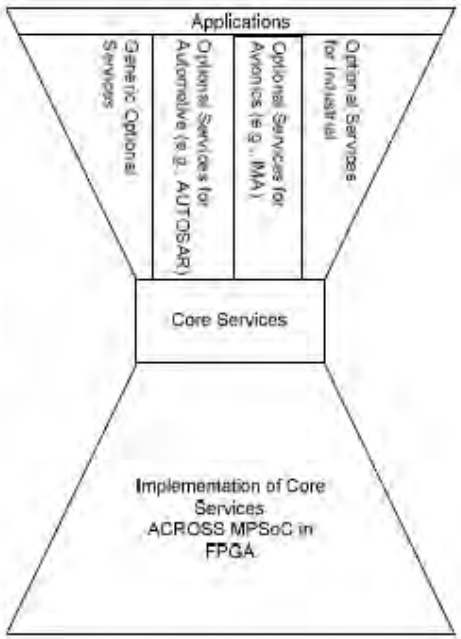
ACROSS

- Proposed a new “Cross Reference Architecture” for safety-critical Multi-Core Processors
- Based on deterministic communication services between cores
- Developed a FPGA-based implementation (@ Altera Stratix IV)
  → Generic Multi-Processor System on Chip Architecture
- Avionics domain: Demonstration of efficiency of new architecture
  with safety-critical application „Situation Awareness for Helicopters“

- Unfortunately, no commercial chip manufacturer wants to implement the new architecture

ACROSS Generic Multi-Processor System on Chip Architecture





non-standardized solution based on fragment switches.

- Component based design approach (as is best practice in aerospace industry)
- Computation services segregated from communication services (trusted network)
- Maximized segregation of functions/services (ideally: one function per processing node)

AIRBUS DEFENCE & SPACE

RECOMP

(Reduced Certification Costs for trusted Multi-Core Platforms)

- Investigated of several COTS Multi-Core Processor Architectures wrt. avionics certification
- Developed a Matrix with chip-internal interference channels
- Result:
  Usage of COTS Multi-Core processor is only possible with restrictions and mitigations

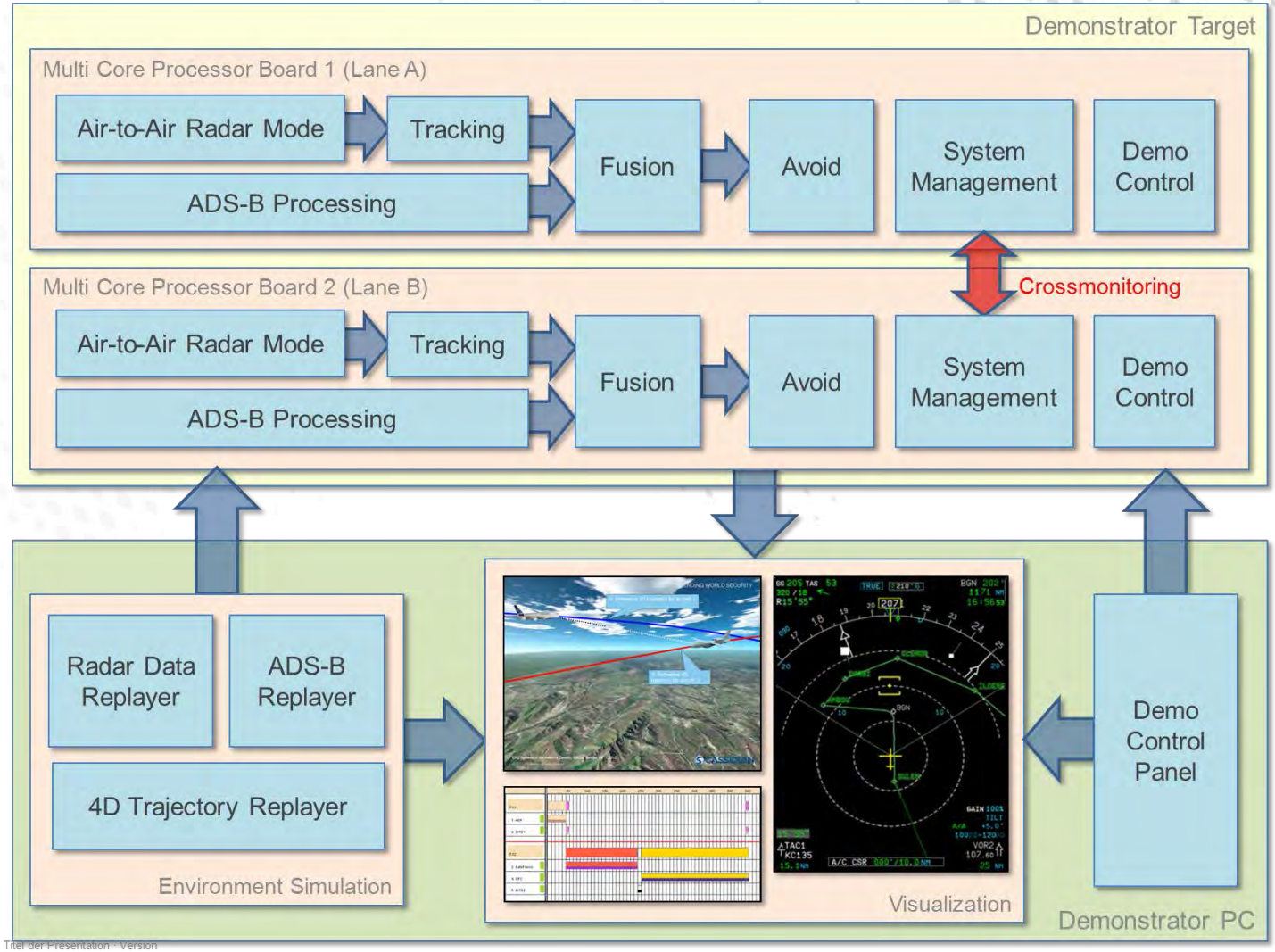
Resource	Identified Problem	Problem condition	Problem mechanism description	Solution category	Specific solution	Final comment
Shared cache	Cache line eviction	Cache is shared by cores	Application executed on one core causing the cache replacement mechanism to replace lines belonging to application from other cores	Application-specific spatial separation of cache entries	Cache partitioning	Feasible solution when HW supports this, which is not common
					Cache way partitioning	Promising candidate, needs HW support
					Cache line locking	Usable if HW supports it, possible performance impact
					Cache colouring	Feasible if application allows this; depends on architecture's memory space mapping, performance impact
				Pseudorandom replacement policy - enables statistical predictability		Interesting research direction as hard analysis seems to incur heavy penalties due to asynchronous execution. Requires significant research. Difficult to certify.
				Write-through		Feasible if HW supports it, reduces performance depending on application

AIRBUS DEFENCE & SPACE

ARAMIS

- Investigated the implementation of chip-internal monitoring
- Complete functionality integrated in a single Multi-Core Chip (Freescale P4080)
- Avionics domain: Demonstration of efficiency of monitoring with an sample safety-critical radar application “Sense & Avoid”
  - Application ported from a implementation using 8 DSPs to 4 Cores of P4080
  - Bandwidth monitoring guarantees calculation-integrity

ARAMIS „SENSE and AVOID“ Demonstrator



AIRBUS DEFENCE & SPACE

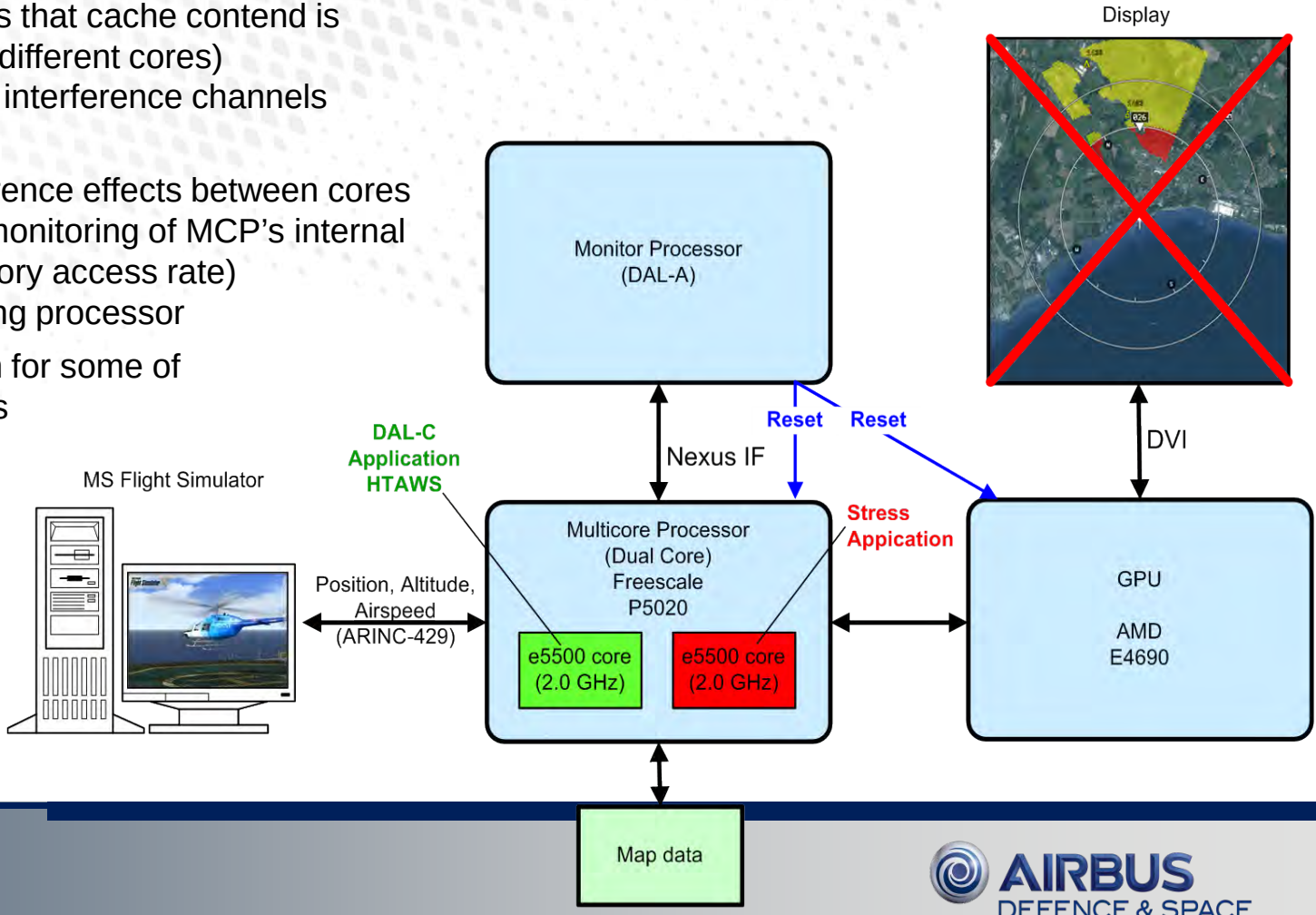
EMC^2 *(Embedded Multi-Core Systems for Mixed Criticality Applications in dynamic and changeable Real-time Environments)*

- Investigates alternatives to limitations in CAST-32
  - SW applications from one system
  - only two active MCP cores

- Avionics domain: Demonstration of an extended MCP-internal "Safety-net" based monitoring approach
  - Using a **H**elicopter **T**errain **AW**areness **S**ystem (HTAWS) implementation on a Freescale P5020

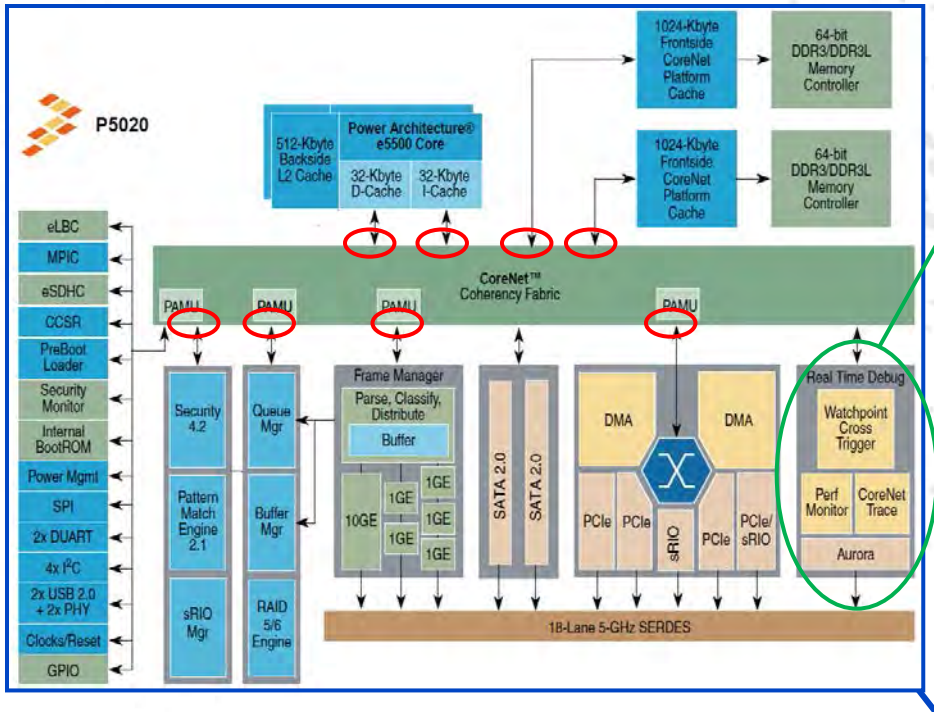
EMC² Planned Tasks @ Avionics Domain

1. Implement **HTAWS** at one e5500 core
   and a **Stress Application** at other e5500 core
2. Search for MCP specific features (e.g. coherency fabrics which ensures that cache contend is exchanged between different cores) which may introduce interference channels between cores.
3. Investigate, if interference effects between cores can be detected by monitoring of MCP's internal resources (e.g. memory access rate) via external monitoring processor
4. Implement mitigation for some of the detectable effects



AIRBUS DEFENCE & SPACE

EMC² MCP-internal Monitoring



Use **on-chip debug facilities**

to implement a **bandwidth and timing monitoring**

Display

Monitor Processor (DAL-A)

Nexus IF

DVI

MS Flight Simulator

Position, Altitude, Airspeed (ARINC-429)

Multicore Processor (Dual Core) Freescale P5020

e5500 core (2.0 GHz)

e5500 core (2.0 GHz)

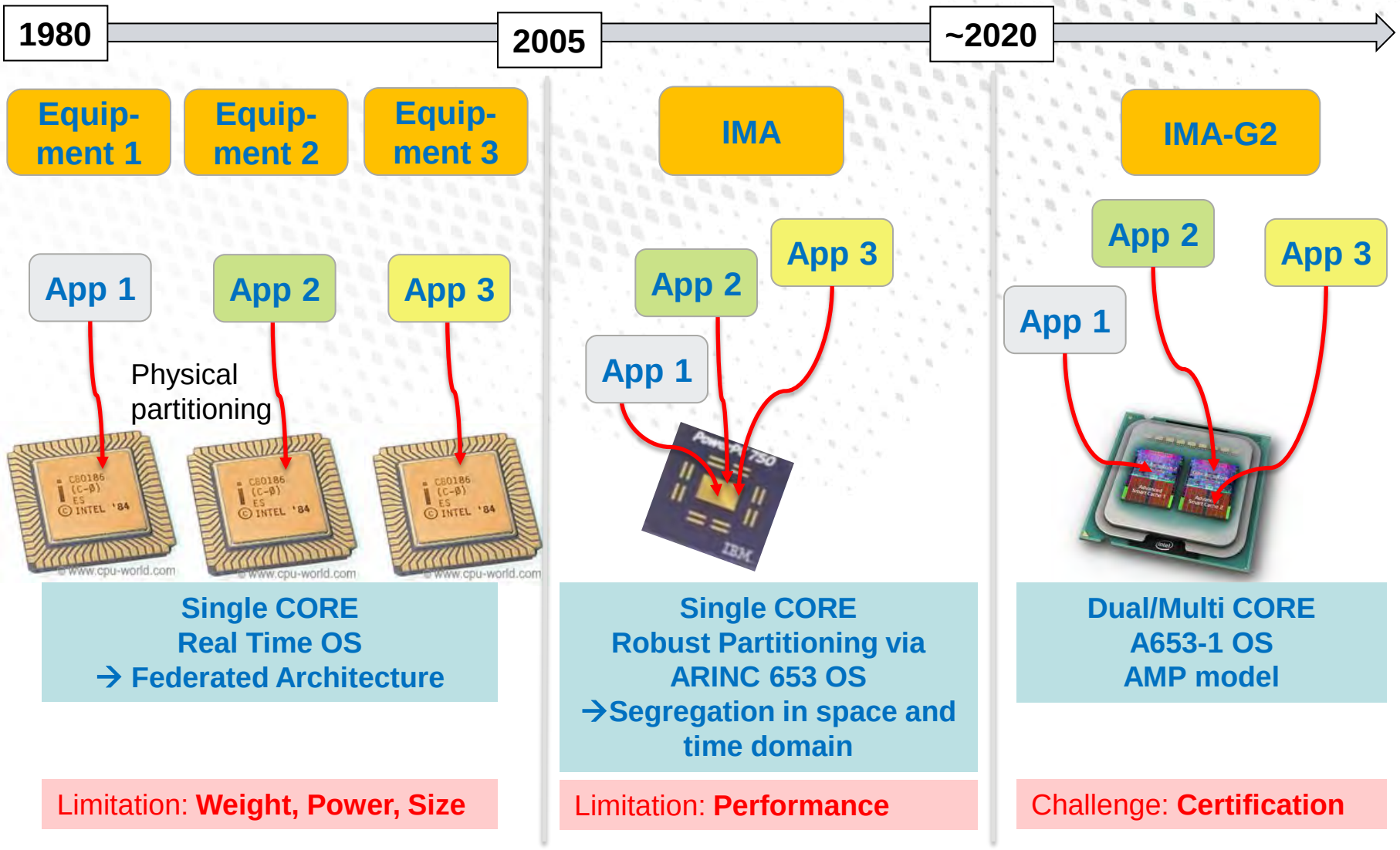
GPU

AMD E4690

Map data

AIRBUS DEFENCE & SPACE

Avionics System Evolution: From Single to Many Cores Processors



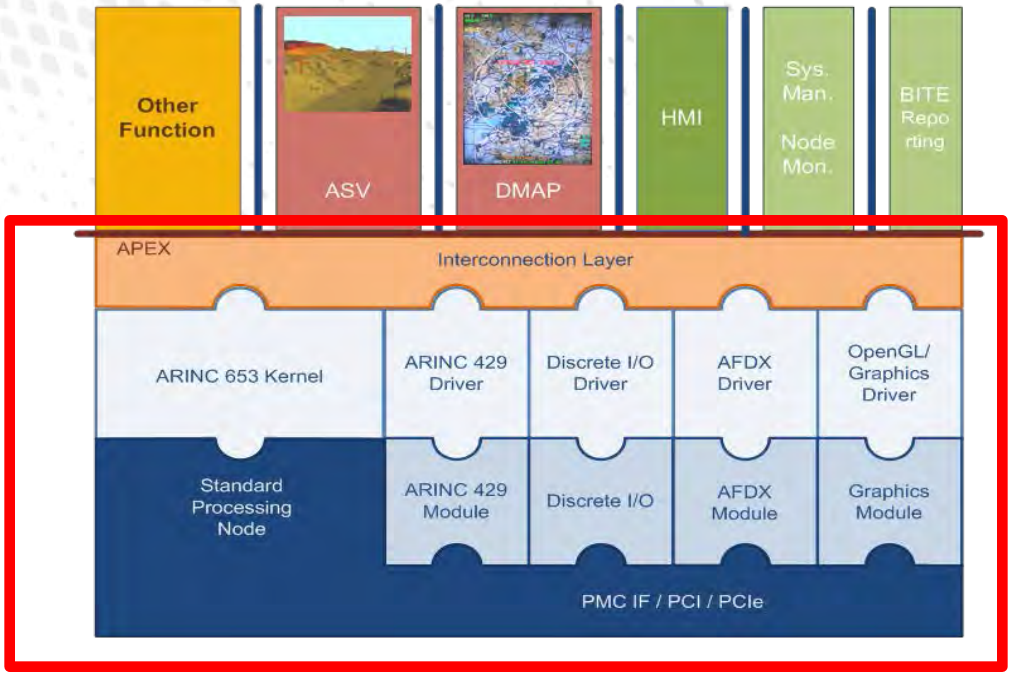
IMA: Integrated Modular Avionics

AMP (Asymmetric Multi-processing): *Each individual functional process is permanently allocated to a separate core and each core has its own operating system.*

AIRBUS DEFENCE & SPACE

Integrated Modular Avionics (IMA) / Open Architecture Computing Platform

- Computing platform without applications
- Small size & low weight
- Low power consumption
- High computing power
- Various I/O types
- Allows integration of different applications



CERTIFICATION - DO254 / DO178C - DO297 ??

AIRBUS DEFENCE & SPACE

IMA Certification Challenges

- Highly integrated, complex system
  - Higher risk for development errors and unintended effects
  - Development of a finite test suite it is not practical (or impossible)
  - Numerical methods for characterizing errors are not available
- Independence between functions, systems or items may be required to satisfy safety or regulatory requirements
- For catastrophic failure conditions
  - common cause events must be precluded
  - Independence must be shown by Common Cause Analysis

Guidance: ARP 4754A

- However, for economical reasons we want to integrate and certify (parts of) independent aircraft functions/systems in one computing platform

Guidance: DO297

DO297 suggestions wrt. shared resources

- Use partitioning
  - Resources may be shared by the method of access time (acc. to ARINC653)
- Problem: A shared resource has the potential to become a single point of failure

  Solution: Use robust SW partitioning
  - A SW partition must not contaminate the code, I/O or data storage areas of other partitions
  - A SW partition must not consume shared processor resources only during its allocated time
  - A SW partition shall only consume its allocation of shared I/O resources
  - Failures of SW unique to one SW partition must not cause adverse effects on other SW partitions

  Approved Method: Time and Space Partitioning

DO297 suggestions wrt. shared resources (2)

The objective of robust partitioning is to provide the same level of functional, if not physical, isolation and protection as on federated architectures *(DO297 2.3.3)*

Overview of certification process *(DO297 4.1)*

- Task 1: Module Acceptance
  - Verification of the partitioning of the Computing Platform
  - Without detailed knowledge of the applications
- Task 2: indiv. Application SW/HW Acceptance
- Task 3: IMA System Acceptance
- Task 4: Aircraft integration of IMA System (including validation and verification)
- Task 5:.. Change
- Task 6:.. Reuse

Incremental Certification

→ Certification of IMA is not an easy task

→ It gets even worse if State-of-the-art COTS MCPs are used

Alternatives @ usage of state-of-the-art COTS Processors

- Stay with single Core processors
  → Not really a long term solution
- Use deterministic MCPs
  → Where is the Chip Vendor / Market (see results of ACROSS project)
- Use core intrinsic Resources (Cache) only
  → It is not easy to find appropriate applications
  → Does not help at conflicts with external resources
- Gain in-service experience of COTS MCPs
  →How many hours do we need? In which configuration?
  →No good COTS candidates exist, see results of RECOMP project
- Use COTS MCPs with System Safety Net
  → Monitoring and mitigation on system level
  → Application specific
- Use COTS MCPs with HW Safety Net
  → Monitoring of the device function independent of the application on HW-level
  → Versatile approach. However: Further research required, see EMC^2 project

Wish List for Future Open Architecture Platform

Use MPC based platform with one Application (and one OS?) per core

- HW/SW Services provided for robust partitioning
- For higer DAL level use HW based safety net with external processor

Reduced verification cost by

- Incremental Verification
- Certification done in Final Configuration
- Update requires recertification and impact analysis

Summary

- Open Architectures may help to save cost for integration, certification and maintaining systems
- Powerful HW Platforms required
- Certification issues of state-of-the-art processors (MCPs) still not solved
- To overcome this limitations very detailed knowledge and additional measures necessary

Thank you for your attention!

Questions?

Info:

Bernd Koppenhoefer
Computing Platforms for Sensors
Phone.: +49 731 / 392 – 5354
Bernd.Koppenhoefer@cassidian.com

Dietmar Geiger
Computing Platforms for Sensors
Phone.: +49 731 / 392 – 4190
Dietmar Geiger@cassidian.com

AIRBUS DEFENCE & SPACE