THALES

A look at Computer Architectures for Mission-Critical Embedded Systems

MPSoC'19 – July 8 - 12, 2019 – Hakone, Japan

Arnaud Grasset – arnaud.grasset@thalesgroup.com

Embedded systems in mission-critical applications

Space

- Altitude and orbit control
- Communication payload
- Radar processing
- Scientific instruments

Avionics

- Cockpit display
- Autopilot
- Engine Control
- Flight Management System
- Breaking Steering
- Maintenance
- Cabin Light
- Passenger IFE

Railway

- Advanced train control and rail signaling systems
- Train Protection and Warning System
- Supervision systems
- Traffic management

Smart cities

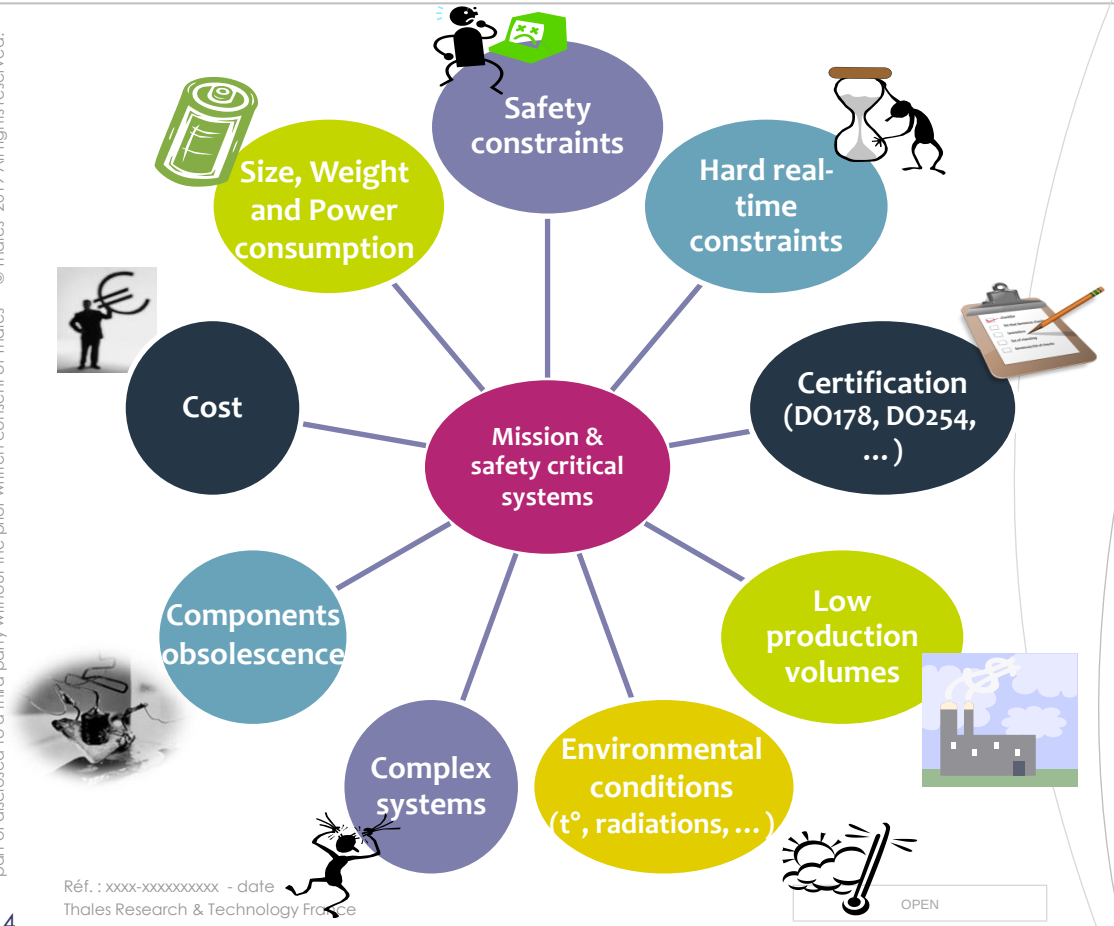
- Smart grids
- Intelligent transportation
- Intelligent buildings
- Tele-surveillance systems

A wide range of applications that play a vital role in our societies and economies

THALES

Challenges of mission-critical embedded systems

Dependable systems



Availability

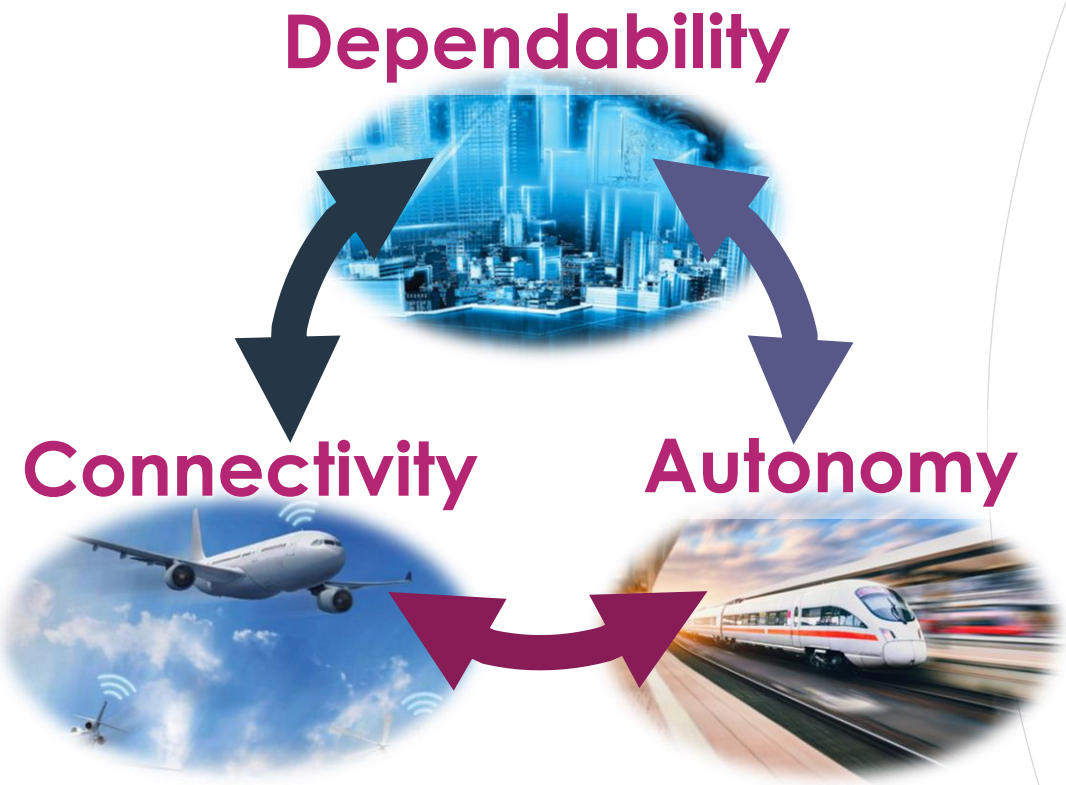
Reliability

Safety

Integrity

Maintainability

Future of critical embedded systems



Guaranteeing safety and reliability

Artificial intelligence and deep learning

More and more connected systems in the era of IoT

THALES

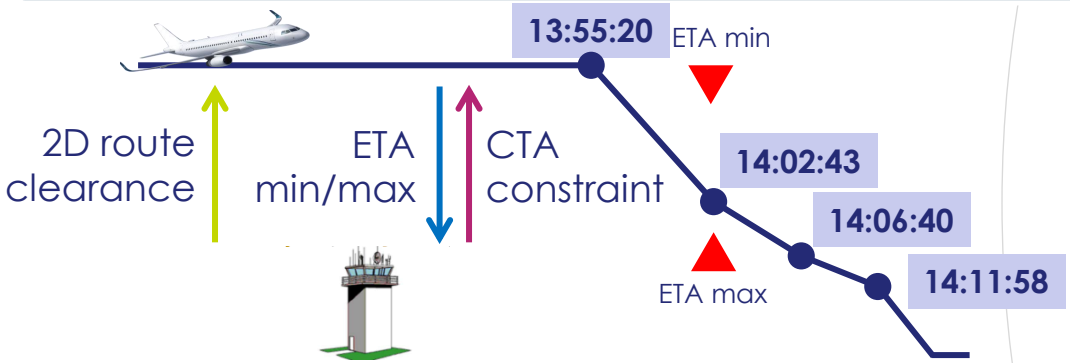
The example of cockpit evolution

Performance growing needs for improved **display** and **Human Machine Interface**

Avionics and air traffic management systems

Escalating growth in air traffic and environmental constraints

Connection of aircraft and ground systems for real-time exchange of trajectory information



4D trajectory management: 3D plus time

Artificial intelligence for aerospace

Proliferation of Unmanned Air Vehicle

- Safe and secure integration of drones operations in urban areas and countryside

AI-enhanced training of pilots & air traffic controllers

- Tracks the eye movements, monitors heart rate and captures voice cadence
- Catches errors that would have previously gone unnoticed

Next steps: flying drone taxi, single pilot cockpit?

Connectivity in ground transportation systems

Boosting their capacity and efficiency

Real-time and fully secured exchange of information between the railway system and the train

Driving optimization

Updated schedule

Network reconfiguration

Smart infrastructure in the era of the Internet of Things

- New fibre optic sensor that not only detects trains, but can also provide data like vehicle speed and vehicle load

Autonomous train

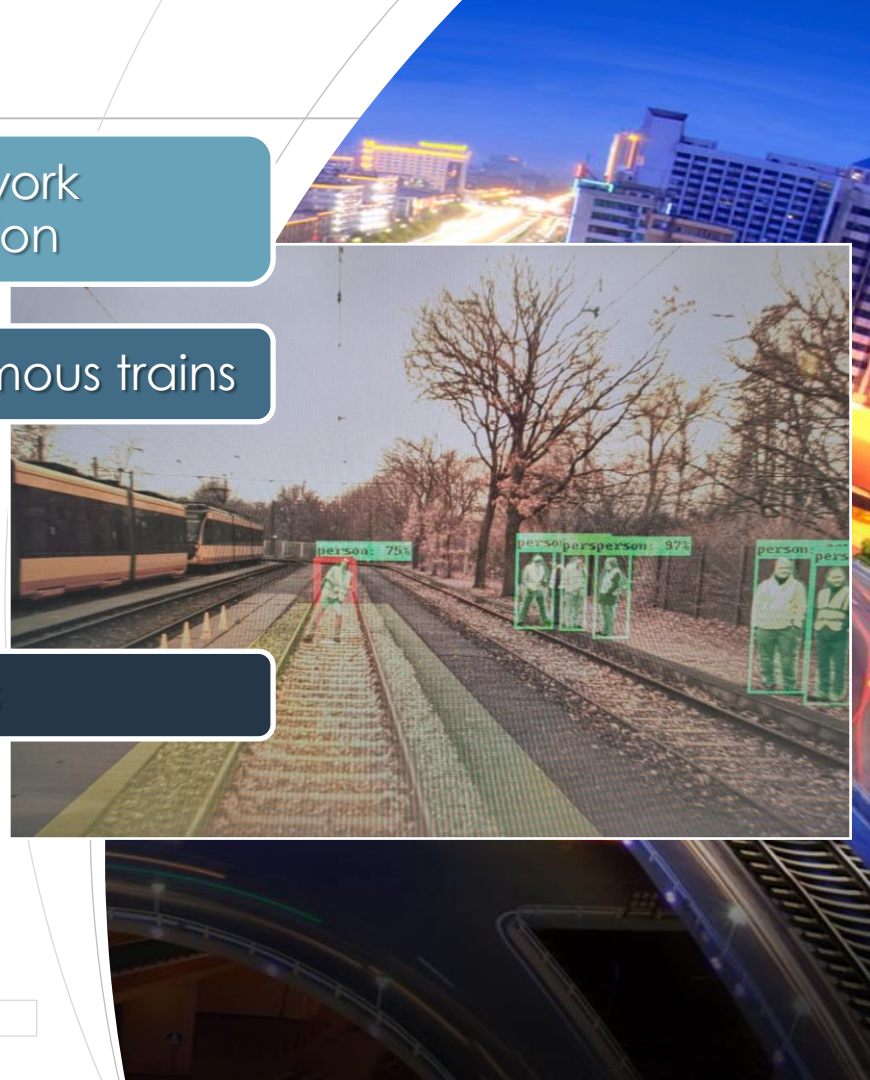
Reduction of infrastructure, increase network capacity, reduction of energy consumption

Evolution from automatic to truly autonomous trains

Locate → **Detect, monitor, and identify** → **Take decisions**

Trains may be equipped with new sensors

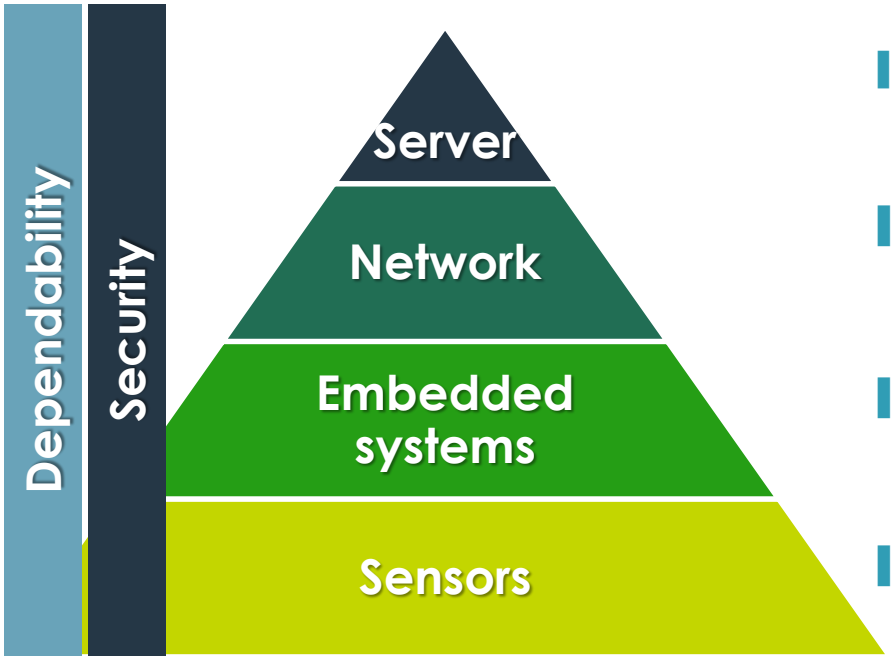
- Radar, lidar, cameras, satellite and inertial measurement systems…



Innovative space applications: the Stratobus™ concept

Autonomous, multi-mission stratospheric airship, midway between a drone and a satellite

From sensor to server



- Artificial Intelligence to optimize the management and supervision of air traffic and trains
- Increasing connectivity of embedded systems ➔ need to secure them
- Need of AI on the edge to take autonomous decision
- The integration of new sensors offers new capabilities

Réf. : xxxx-xxxxxxxxx - date
Thales Research & Technology France
Template trtp version 8,0,3 / template : 87211168-GRP-EN-004

OPEN

THALES

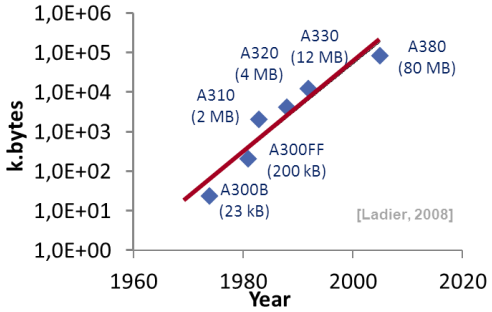
THALES

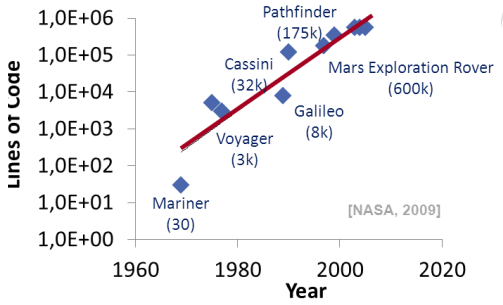
Evolution of Computer Architectures for Critical ES

Use of complex COTS in mission-critical systems

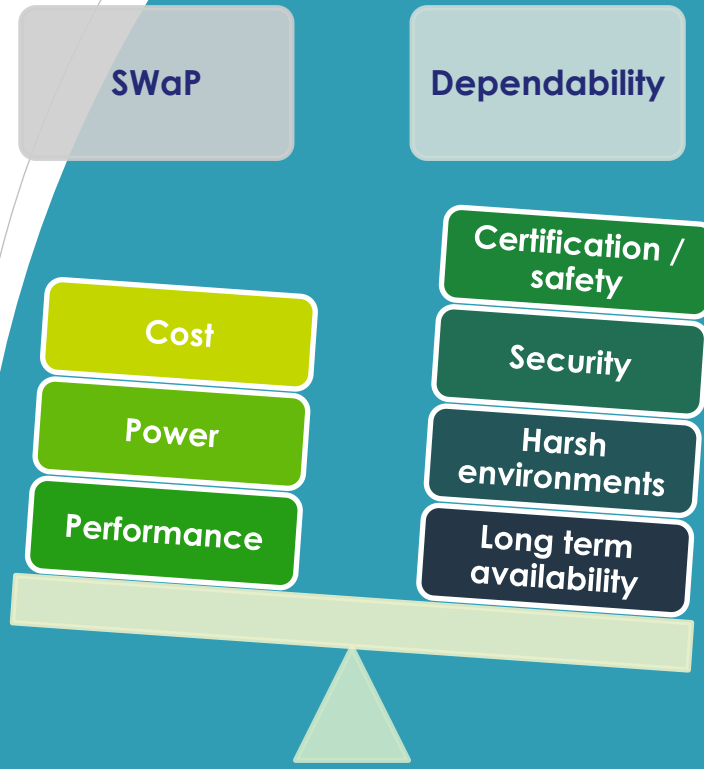
Huge processing power, and low cost allowed by mainstream markets

COTS becomes more and more complex



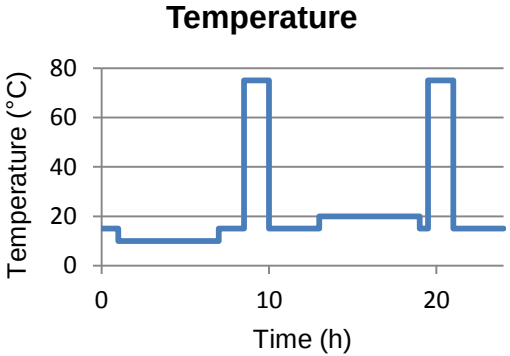


Power and performance overhead due to safety and reliability margins



Reliability challenges for critical embedded systems

How to build dependable system on top of "unreliable" parts?

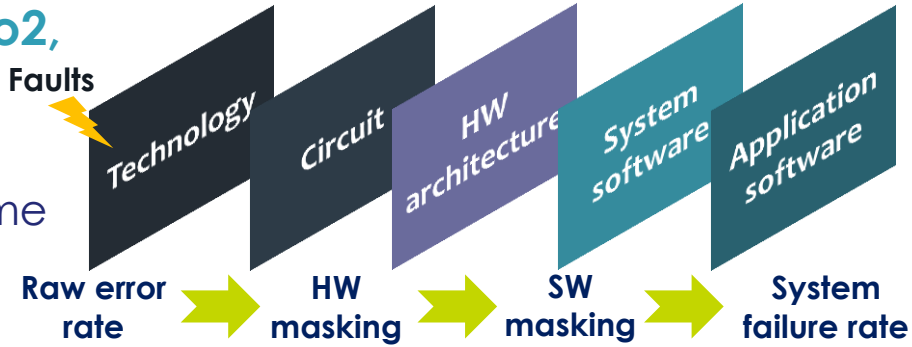


Derating of Embedded Processor to prolong useful life period requires:

- Good knowledge of mission profile
- Understanding of wear-out mechanisms

HW/SW fault tolerance (2-out-of-3, 2oo2, 1oo1)

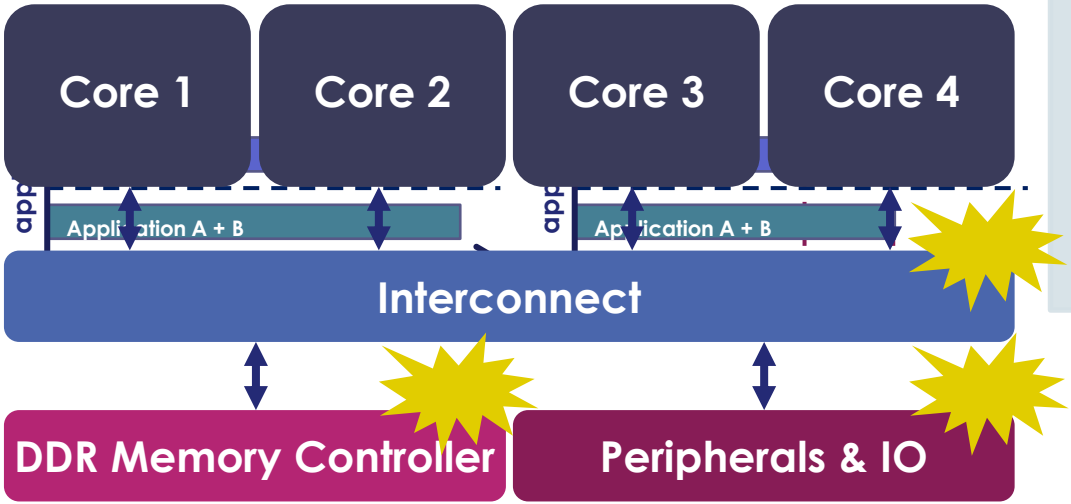
- Evaluation of SW and Architectural Vulnerability Factor early in the design time
- Reduction of overdesign



Rethinking partitioning in multi-cores processors

Safety certification requires spatial isolation and temporal isolation

Time composability is not ensured on multi-cores due to insufficient hardware segregation for shared resources



Application

- Scheduling of communications and IOs
- Impact on the application development process

OS/hypervisor

- Control of data transfers
- Impact on the performance

Secured platform for embedded systems

Basic security features

- MILS architecture based on PikeOS hypervisor

- Root of Trust/Chain of Trust with Secure Boot + TPM/HSM modules

Security vulnerabilities of undocumented subsystems

- E.g: The Intel Management Engine

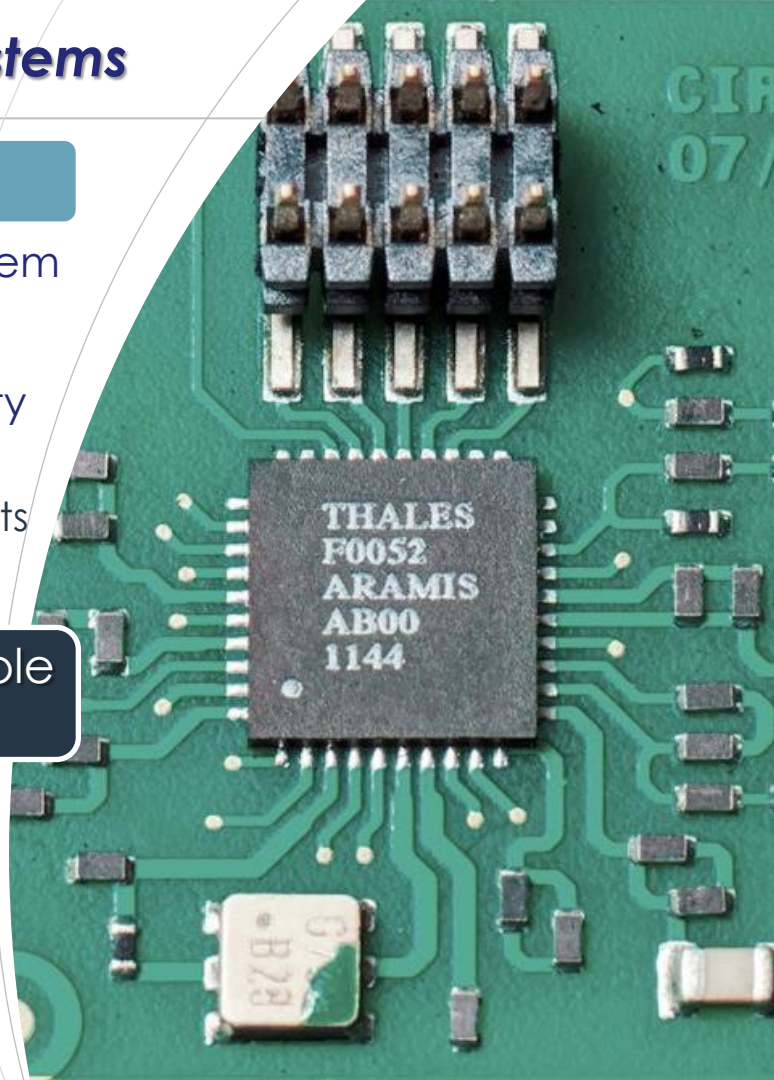
Use of custom SoCs for mission-critical systems

Custom SoCs and ASIC in Thales

- Low volume markets and small software ecosystem
- Not really powerful solutions
- For secured products or high availability/reliability products
  - E.g. custom rad-hard processor + rad-hard circuits (ASIC/FPGA)

Opportunity for an ecosystem providing trustable and dependable processors?

- End of Moore's law is coming…
- New solutions (e.g. open ISA)



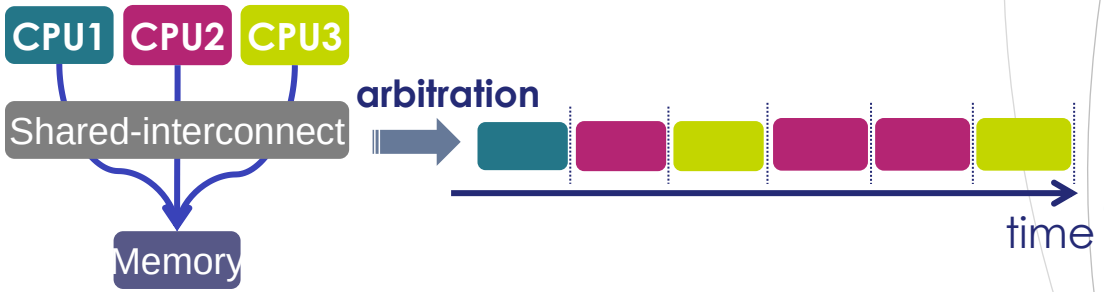
Time predictable SoC for hard real-time systems

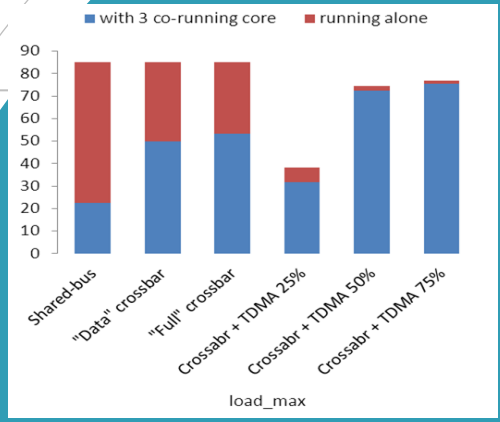
Proof-of-concept of an isolation mechanism at HW interconnect level

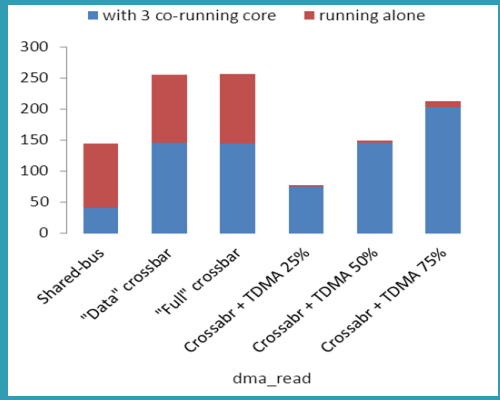
- TDMA arbitration policy to bound interferences
- Control access to shared-resources

Time is divided in multiple slots

- Slots statically allocated to each cores

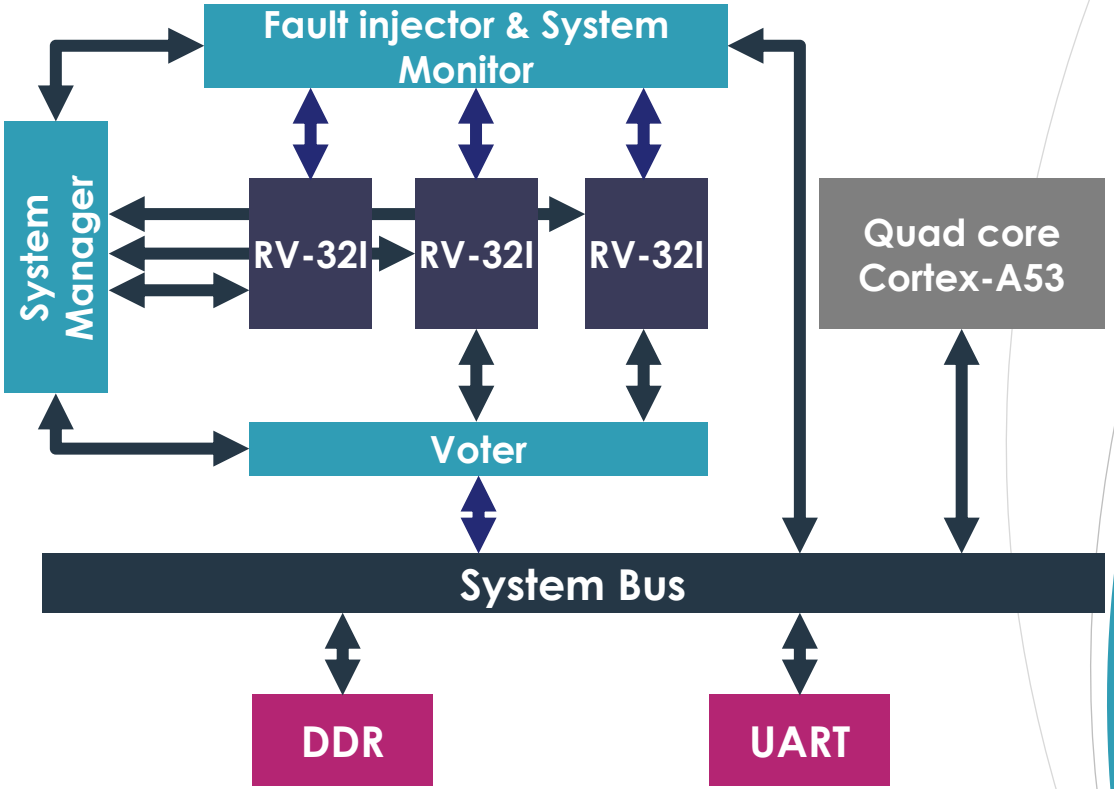






Interference measurement on a SoC demonstration platform

Demonstrator of a Triple-Modular-Redundancy RISC-V platform



Mitigates (SEU) with minimum impact on software

Based on an open source implementation of RISC-V ISA

Fault detection, isolation of the faulty core, recovery procedure to restore the state of the core

Implemented on a Xilinx UltraScale+ MPSoC device

Leveraging open-source hardware?

Increasing visibility and credibility of open-source projects

- RISC-V ecosystem
- NVIDIA Deep Learning accelerator (NVDLA)

RISC-V cores based on the RISC-V open ISA

- Openness for innovation and customization
  - Product differentiation by focusing on specific elements
  - Domain-specific solution

Software
large ecosystem compatible across implementations

Performance
State-of-the art processor

Safety
No black-box

Security
A fully auditable processor

SWaP
Exact fit between features and application needs

Sovereignty
European ecosystem from design to production of SoC

No vendor-locking
A SME business to develop custom version is being established

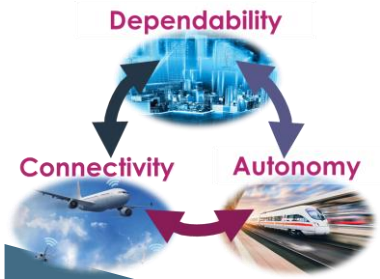
THALES

THALES

Conclusion

Conclusion

Tight requirements of mission critical ES



Autonomy & connectivity

Open source hardware?

THALES

A look at Computer Architectures for Mission-Critical Embedded Systems

MPSoC'19 – July 8 - 12, 2019 – Hakone, Japan

Arnaud Grasset – arnaud.grasset@thalesgroup.com