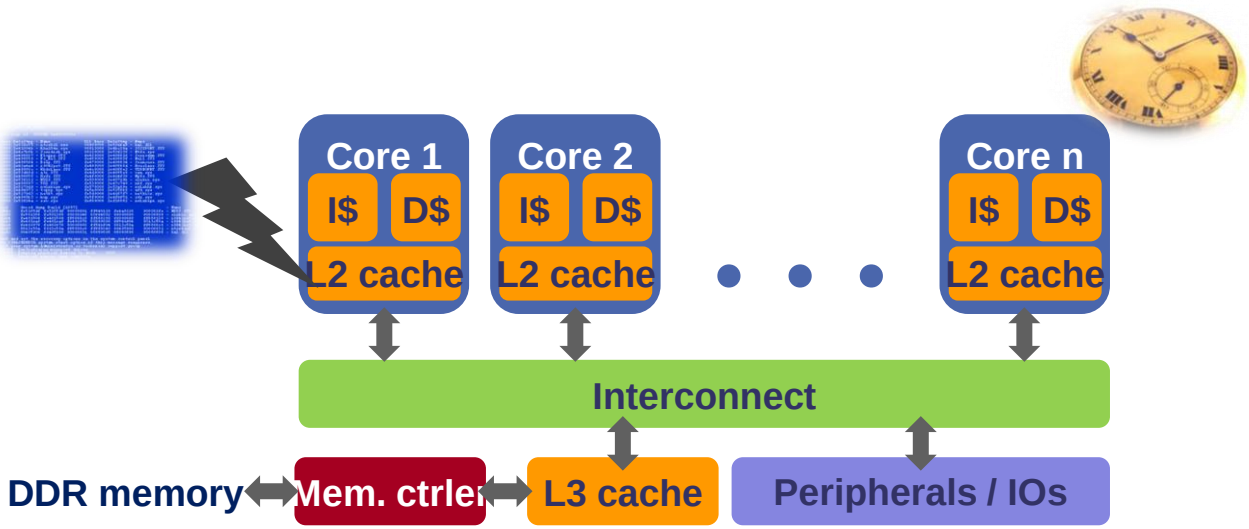
Reliable and Predictable MPSoC for Critical Embedded Systems

Arnaud Grasset – arnaud.grasset@thalesgroup.com

Multi-processor SoC for Critical Embedded Systems

- To fulfil ↗ performance requirements and support ↗ functionalities
- But high dependability requirements and hard real-time systems



- The shift to multi-core processors involves a re-examination of system development methods

THALES

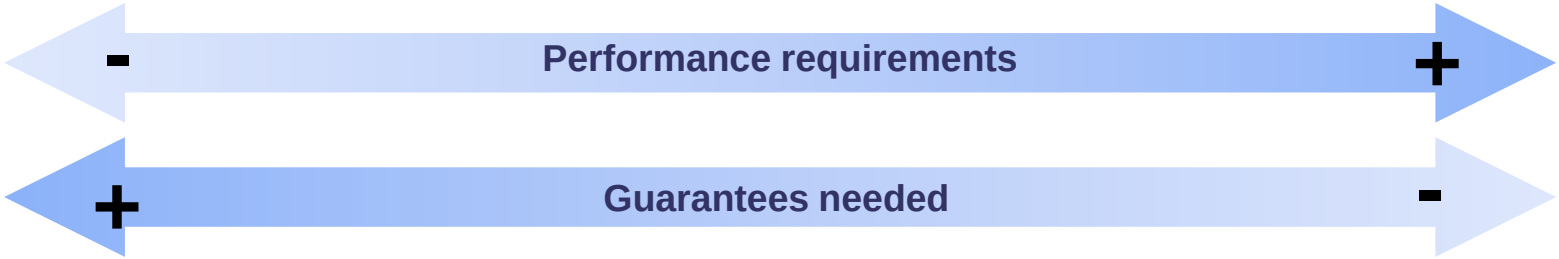
Contents

THALES

Mission critical and safety critical systems

Strong requirements on timing, fault tolerance/reliability, temperature, etc.

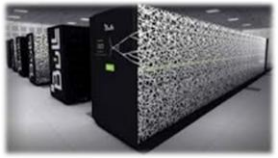
Strong requirements on performance, power, etc.



Safety critical

Mission critical

Soft real-time



Non real-time

Certified systems

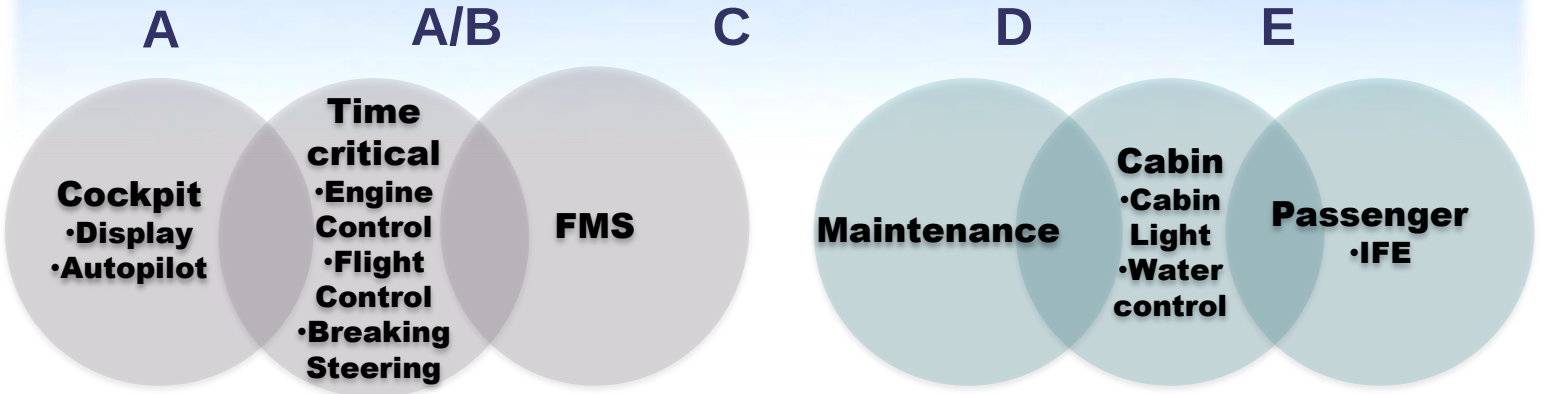
Less-certification requirements

Not critical

THALES

Diversity of applications, environments and severity levels

Design Assurance Level (DAL):



Aerospace safety process driven from the safety requirements

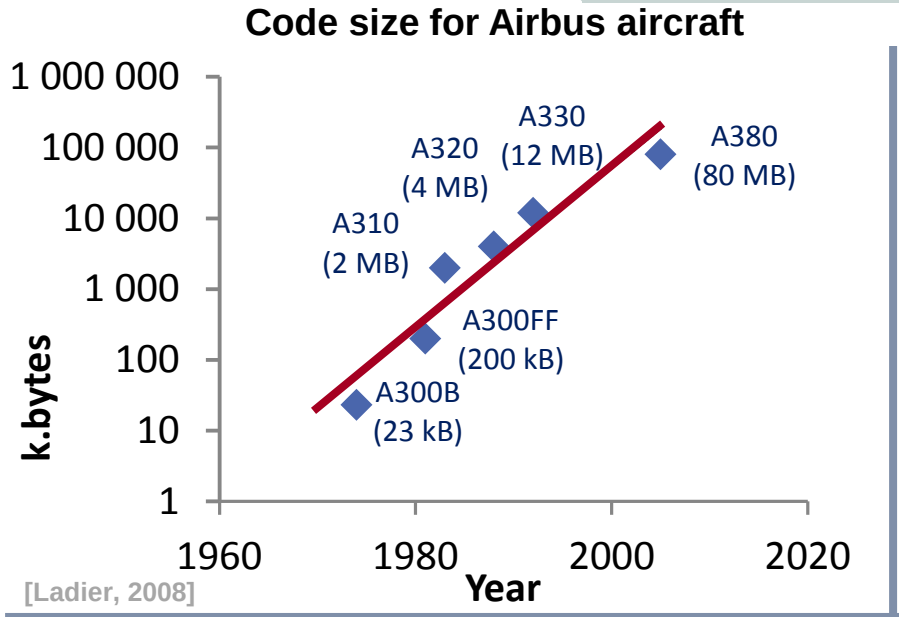
THALES

The example of cockpit evolution

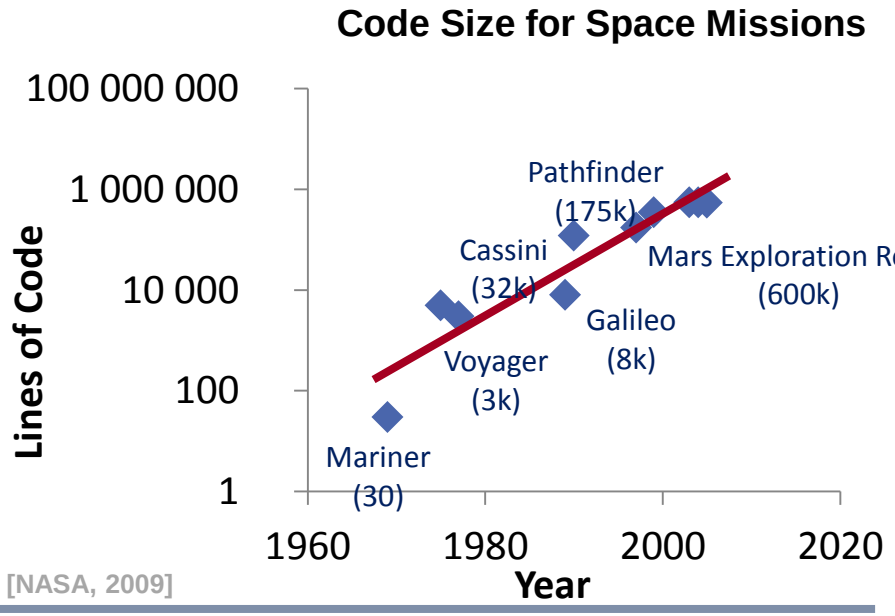
Performance growing needs for improved safety and maintenance!
(growing automation, anti-collision systems, improvement of passengers comfort …)

D342 | Concorde | A310 | A320 | A340 | A380 | A350 | Future

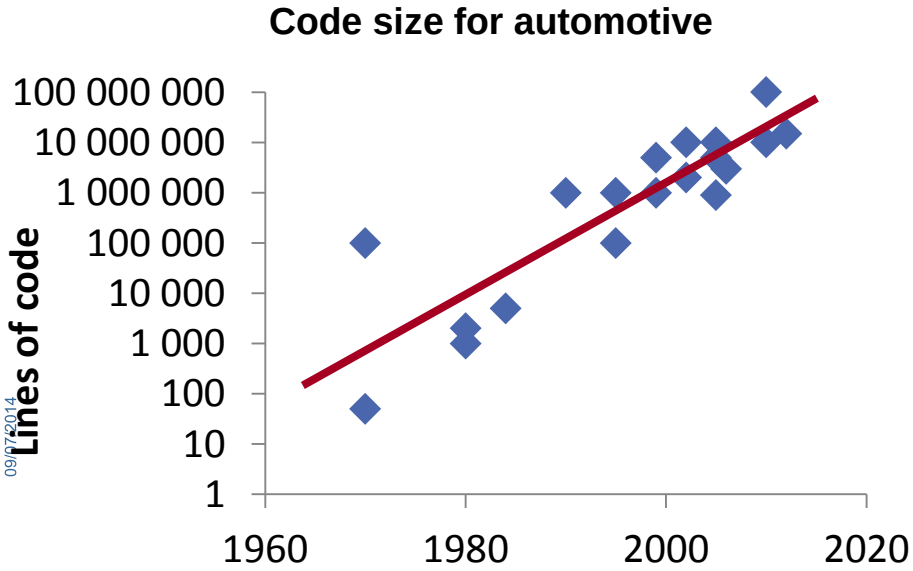
Mission Critical Systems: high-perf. requirements



[Ladier, 2008]



[NASA, 2009]



[Goto, 2013]

[Davey, 2013]

Code size evolution for critical embedded systems

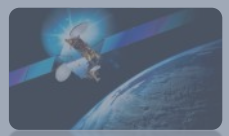
THALES

The critical embedded systems markets

Long lifetimes and relatively low market volume


50 years


25 years


15 years

10 years

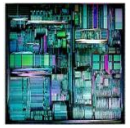
3 years 2 years

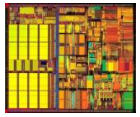
And also management of component obsolescence

1977 1987 2012 2025

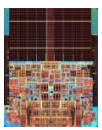
Technology process: 800nm 600nm 350nm 250nm 180nm 130nm 90nm 65nm 45nm 28nm 22nm 16nm 11nm 8nm

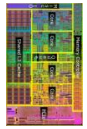

80486


Pentium Pro


Pentium III


Pentium 4


Core 2 Duo


Core i5

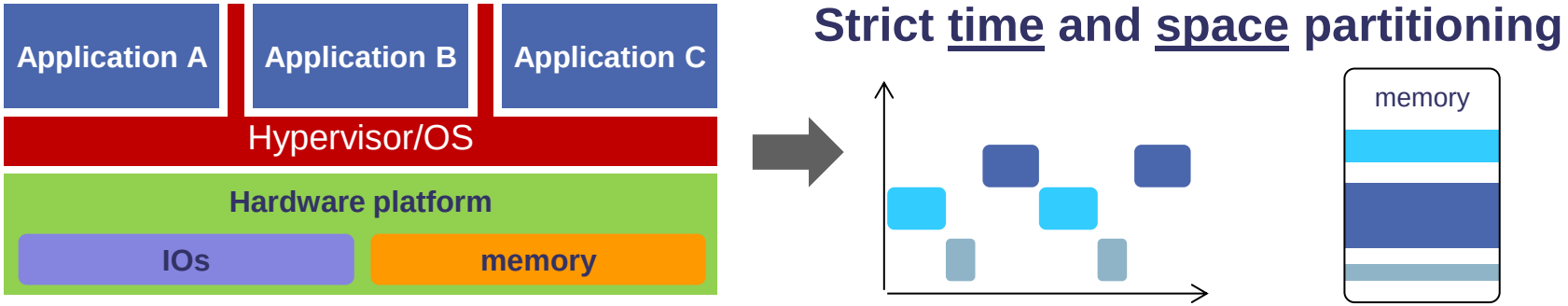
THALES

Multi-processor platforms in critical embedded systems

Modular platforms running multiple independent applications

- Higher levels of integration for size, weight and power reduction (fuel savings, simplified maintenance, …)
- e.g. IMA (Integrated Modular Avionics) for civil aircrafts (ARINC 653), AUTOSAR for automotive, IMA for Space (IMA-SP), …

Composability and incremental certification



THALES

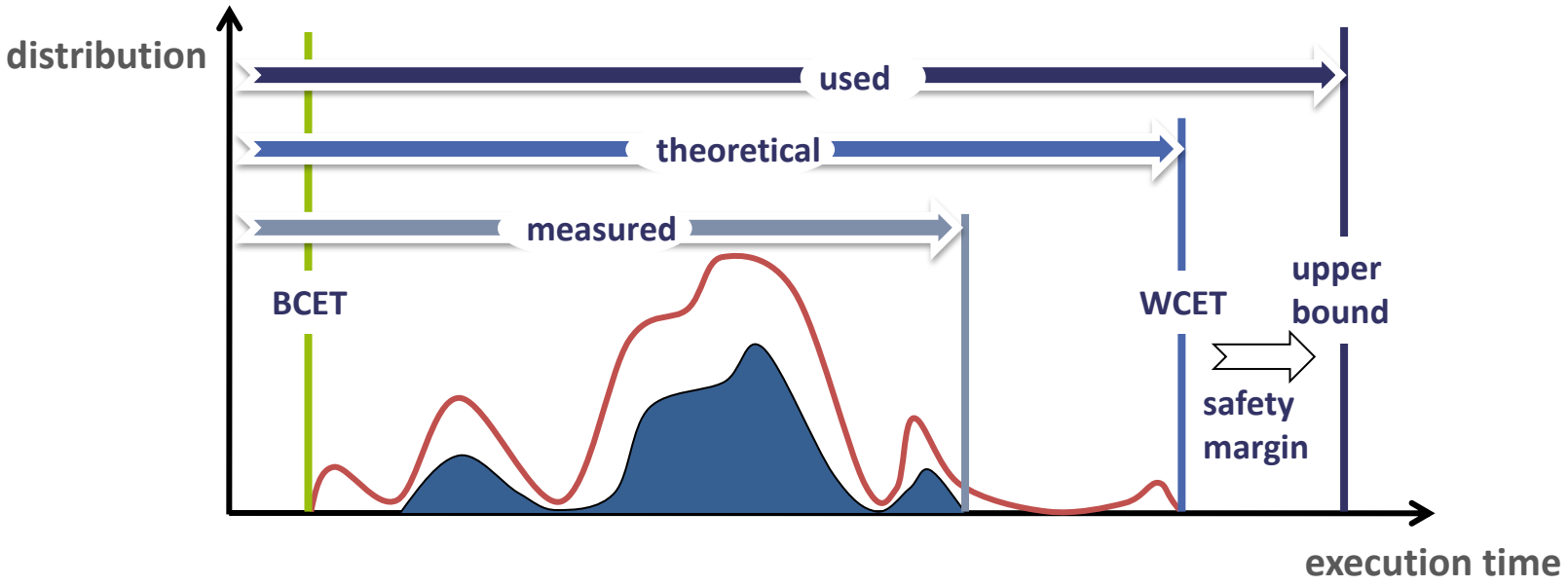
Contents

THALES

Predictability of complex architectures

Temporal behavior as important as logical function in ES

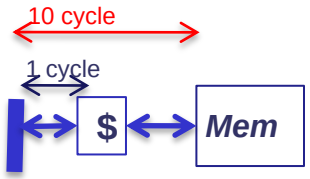
- Absolute guarantees on the timing (DO-178B)



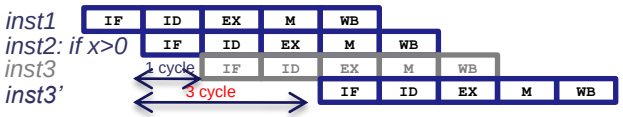
Design of commodity processors for average performance !

Shift to multi-core architectures

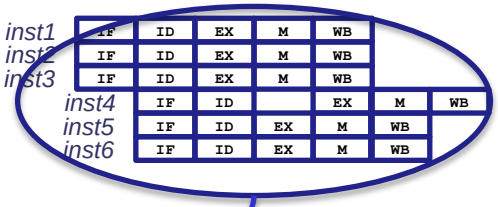
Cache



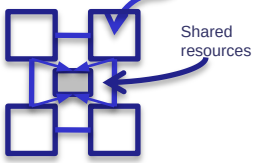
Pipelines



Superscalar Out of Order



Multicore

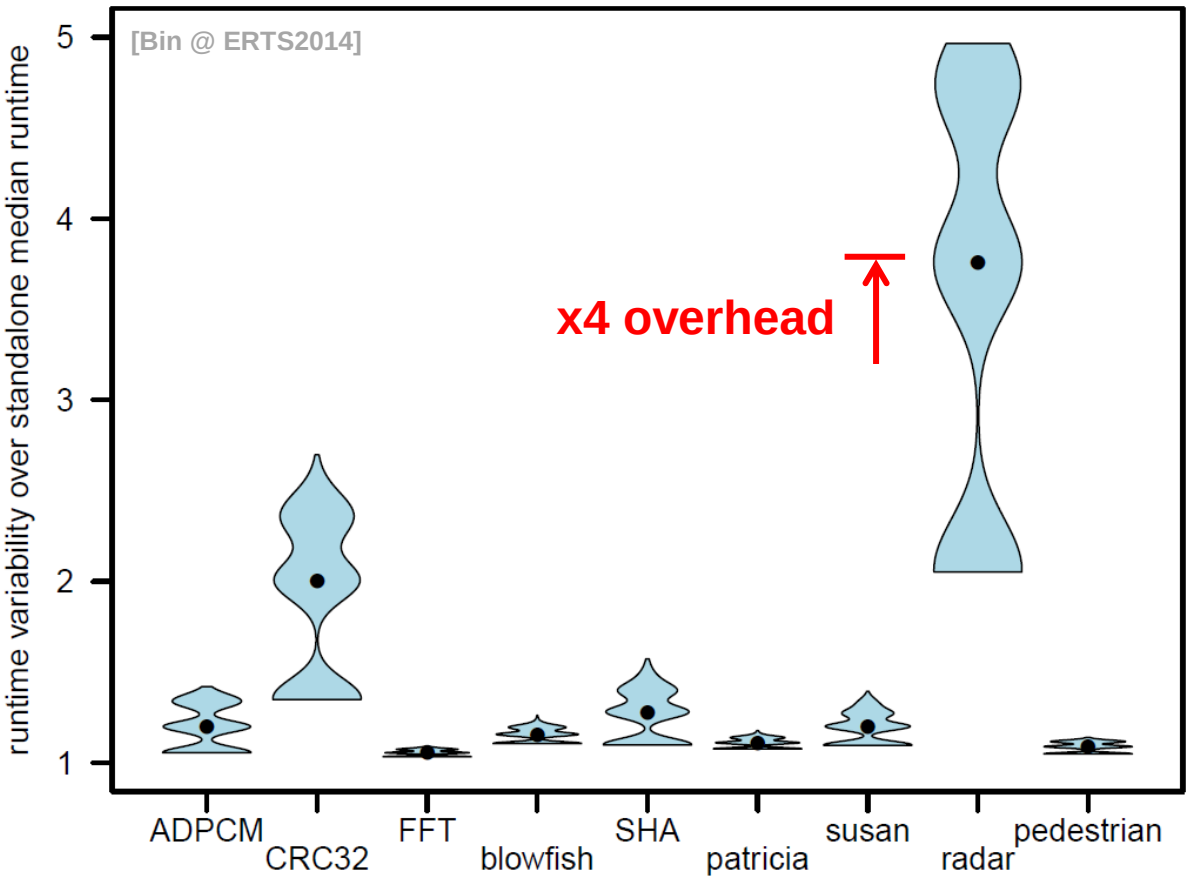


Difficulties in certification: WCET analysis, deterministic behavior, complexity of architectures, thermal constraints

THALES

Measurement of runtime variability

- Freescale P4080 platform
- 1 reference applications + 7 benchmarks stressing the shared memory path
- 600 iterations

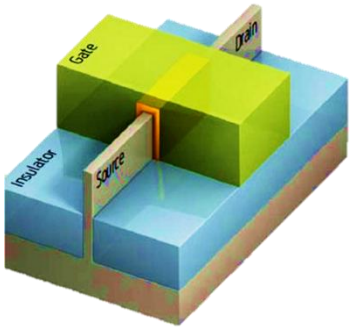


Safety margins to guarantee proper operating are no longer sustainable

THALES

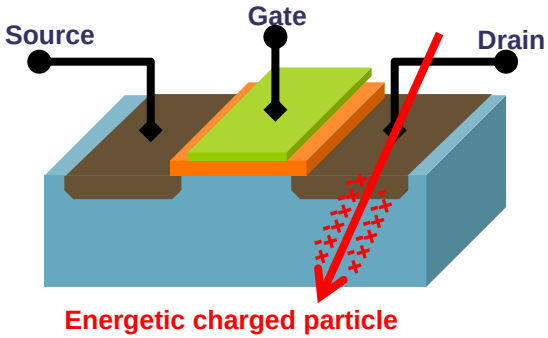
Technology scaling brings new challenges!

New technological process and process variability



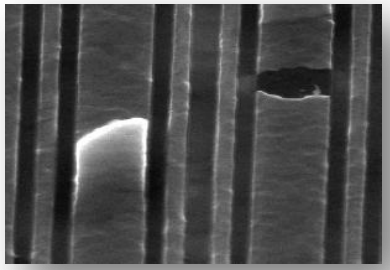
- New technologies: FD-SOI, FinFET, 3D integration, …
- Extensive process variations
- Infant mortality and intermittent faults

Increased susceptibility to environment



- Soft errors (SEU, MBU), EMC increased sensitivity
- Transient faults

Increased aging of devices



[IAlam, 2007]

- Early wear-out effects: BTI, TDDB, HCI, electromigration, …
- Permanent faults

Reduced lifetime/reliability of electronic components with the shrinking technology size

THALES

Impact on critical embedded systems

Harsh environmental conditions

- Extreme conditions of space environment
- High vibrations
- High level of radiations
- High temperature
- 24/7 ON time

Stringent dependability requirements

- High reliability
  - Failure rate as low as 10^{-9} failure per hour
- Critical ES life expectancy far exceeds that of their components lifetime
- Revision of qualification procedures

THALES

Impact on certification and timing predictability

Critical safety = predictability + reliability

(timing and behavior)

Timing predictability of error detection & recovery mechanisms (checkpointing, roll back, etc…)?

Significant impact of hard faults in prediction structures and caches on performance

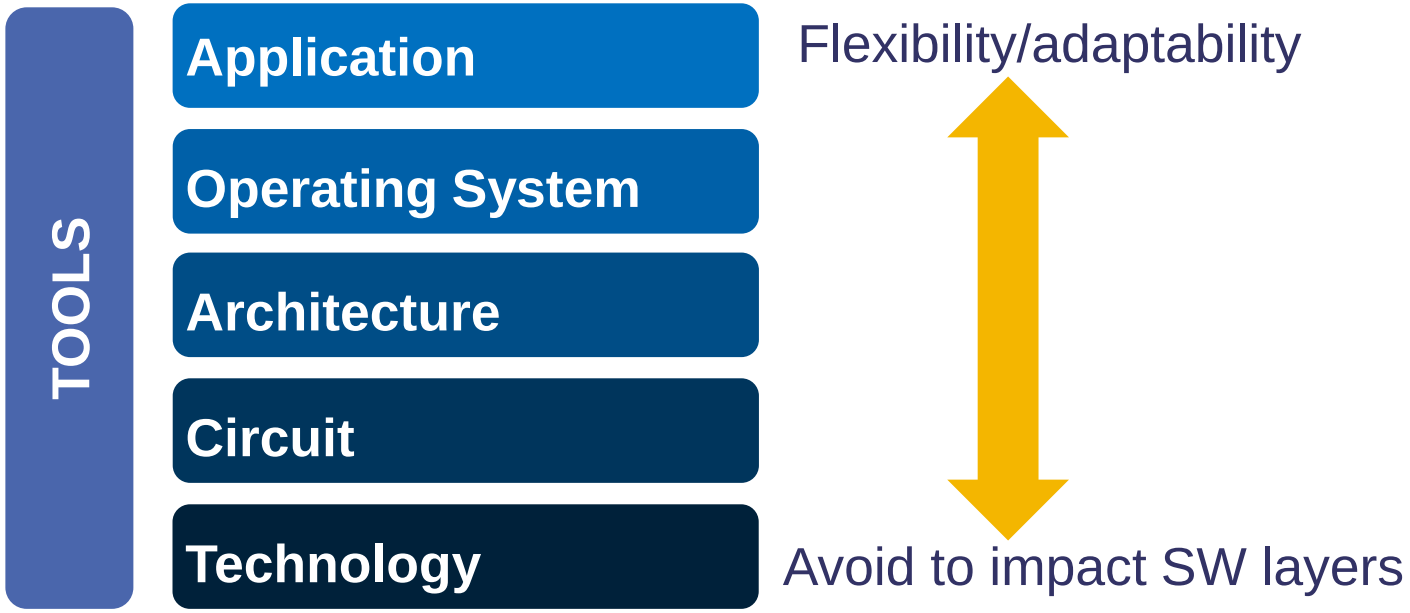
Guarantees on temporal and spatial isolation still valid in presence of faults

Contents

THALES

The need of new system design approaches

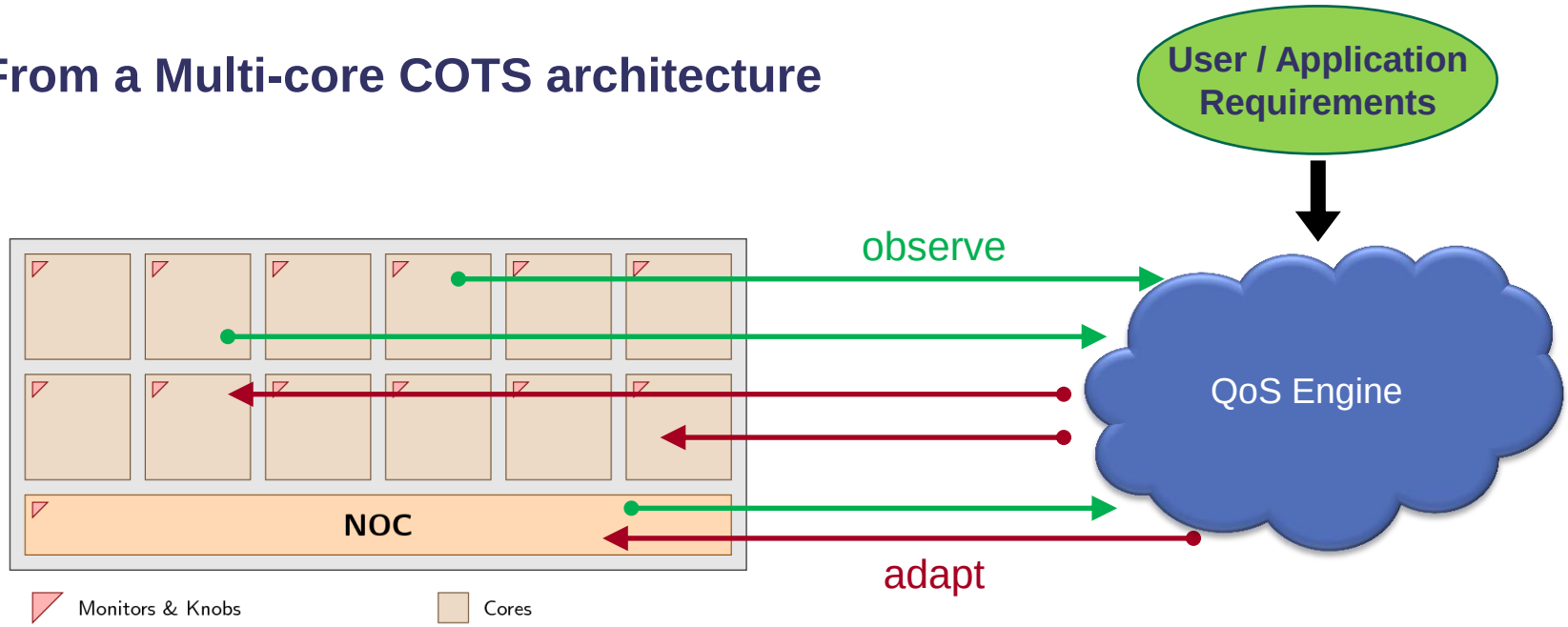
- **Challenge for future technologies: building "dependable" systems on top of unreliable components**
  - which will degrade and even fail during normal lifetime of the chip
  - while providing guarantees on reliability, timing …



THALES

Enabling COTS to mission critical

- **From a Multi-core COTS architecture**



- **Lightweight Mission Critical enablers for COTS Architecture:**
  - **Monitor** the system at various level (bandwidth, workload, temperature) to measure health and behavior
  - Know the application **requirements**
  - Control and adapt the behavior through **Knobs** (clock gating, migration) to tune the system to match the application requirements
  - Driven by **QoS Engine** to enforce application requirements

THALES

Service Level Agreement

- **Service Level Agreement between the application and the OS**

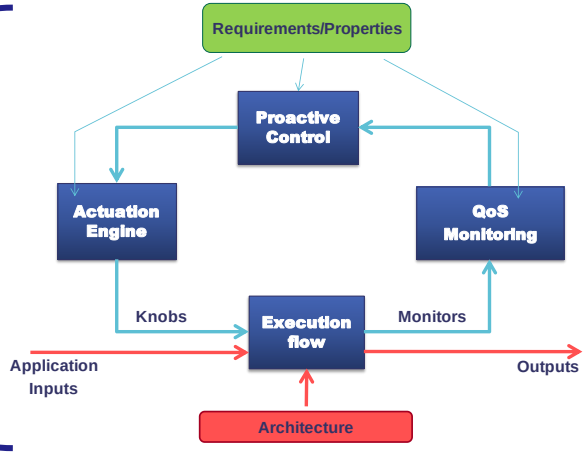
APPLICATIONS

QoS RUNTIME

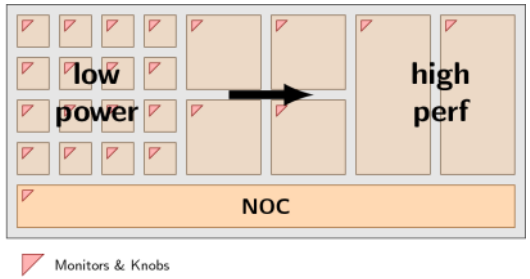
SLA

QoS OPERATING SYSTEM

QoS ARCHITECTURE



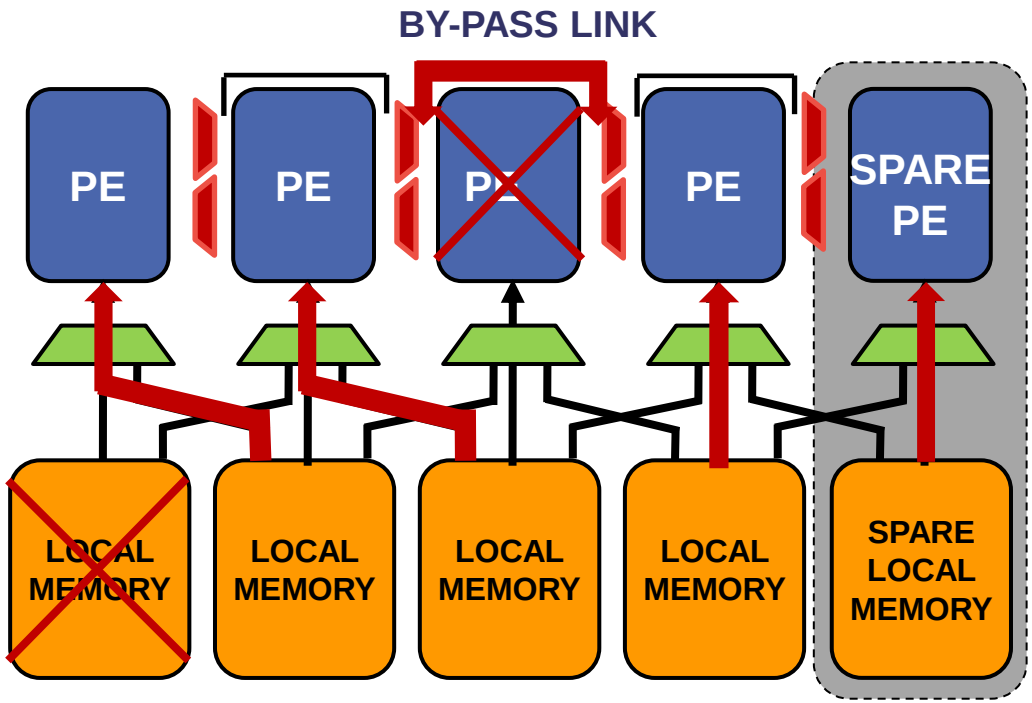
+ QoS



THALES

Example of HW fault-tolerance for SIMD architectures

- Exploiting the homogeneity of the PEs, a single spare element can replace any faulty PE avoiding Dual or Triple Modular Redundancy.
- By-Pass links allow the interconnection network to skip the faulty PEs replaced by the spare PEs

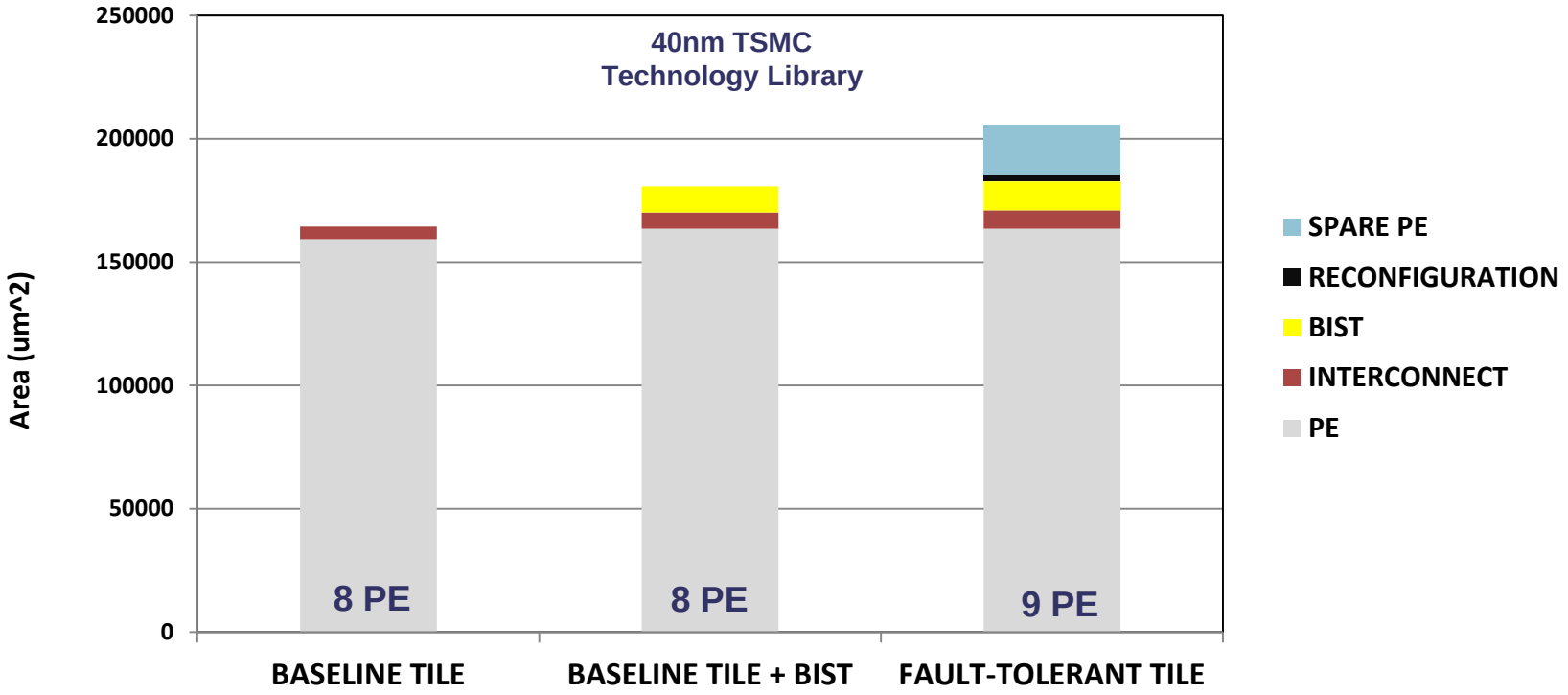


LOW RECONFIGURATION LATENCY AND SCALABILITY PRESERVED

AFFORDABLE AREA OVERHEAD

THALES

Experimental results: area overhead



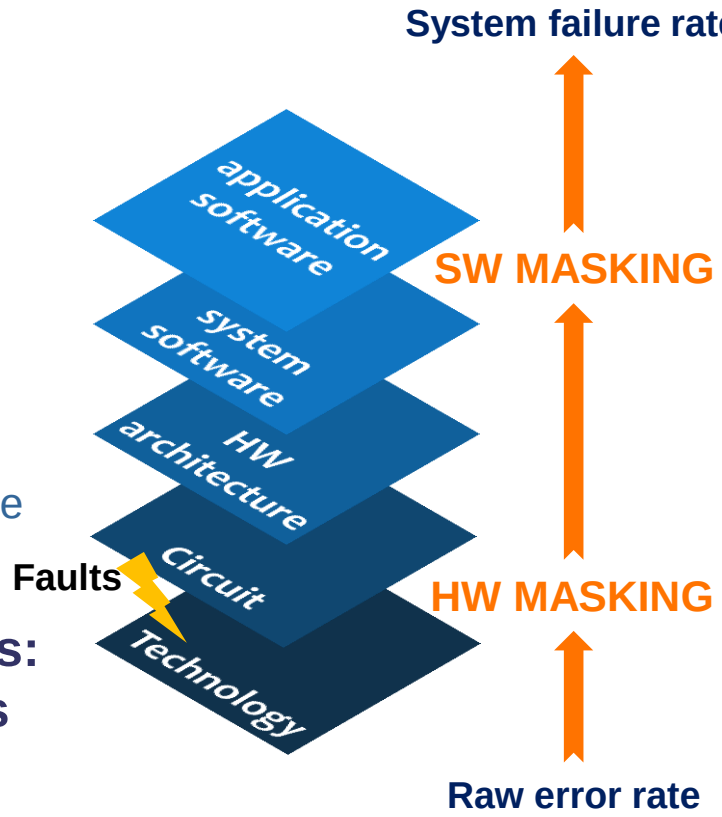
- The **Built-In-Self-Test (BIST)** scheme requires a **9.8% of area overhead** with respect to the baseline tile
- The **fault-tolerant tile** is able to integrate BIST, reconfiguration schemes and spare PE with **a 25% of total area overhead**

THALES

Cross-layer Early Reliability Estimation

Clereco
Cross-Layer Early Reliability Evaluation for the Computing cOntinuum

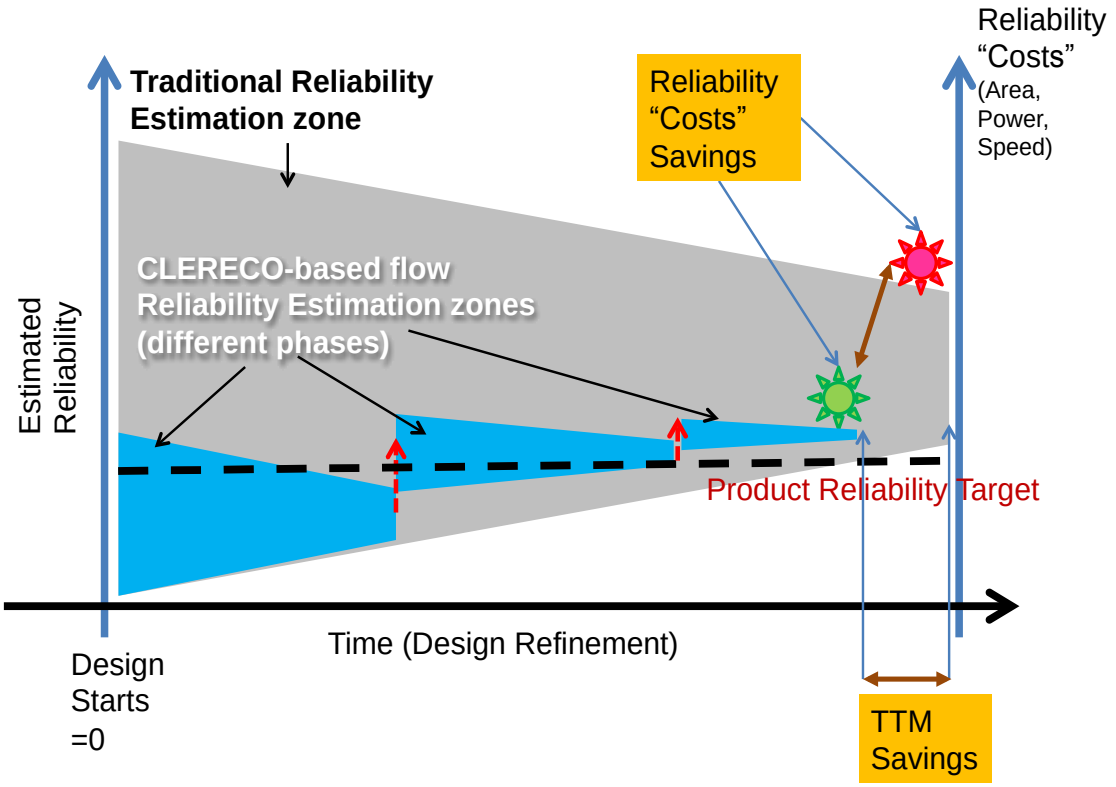
- **The CLERECO FP7 Collaboration Project**
  - http://www.clereco.eu
- **Cross-layer estimation:**
  - Reliability is evaluated at system level
  - Considering the hardware structure as well as the software stack (application, OS, …)
- **Standard reliability evaluation approaches: massive and time-consuming simulations and/or fault injection campaigns**



THALES

Cross-layer Early Reliability Estimation

- **EARLY: reliability evaluation performed in every phase of the design cycle even when only high-level specifications are available**
  - Reduction of area and design effort (dedicated to reliability)
  - Reduction of performance and energy lost for reliability



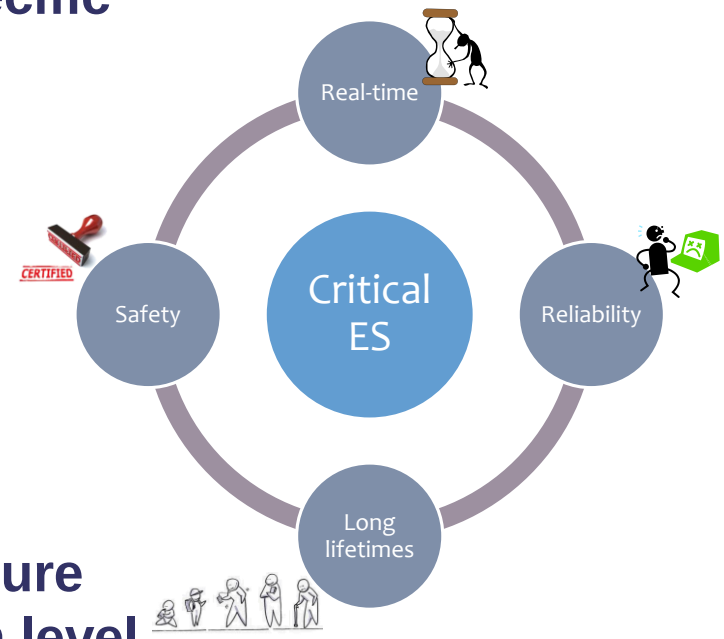
THALES

Contents

THALES

Conclusions

- **Critical Embedded Systems have specific and diverse requirements**
- **Strongly impacted by:**
  - the ↗ complexity of processor architectures
  - the ↘ reliability of CMOS technologies
- **Mitigation techniques at the architecture level and/or at the application/system level**
- **How to design complex systems with predictable and deterministic behavior?**



THALES

Q & A

THALES