

www.thalesgroup.com

Reliability Challenges of Critical Embedded Systems

A System-Provider Perspective

Arnaud Grasset
arnaud.grasset@thalesgroup.com

Research & Technology

THALES

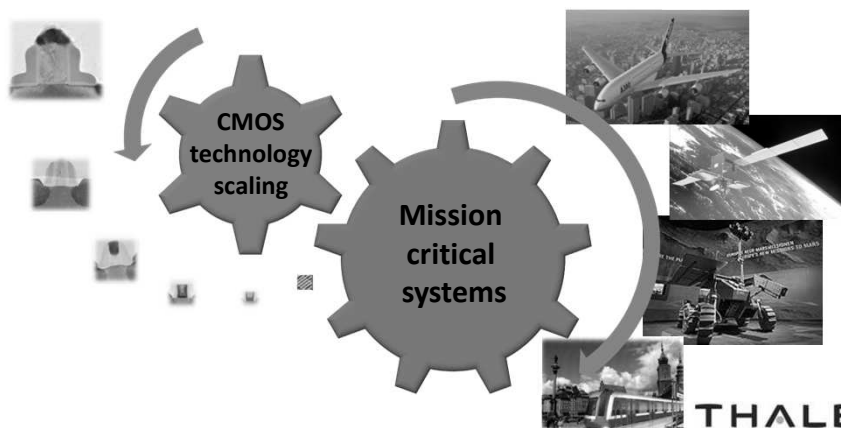
MPSiC 2015 - July 13-17, 2015

2 / 18

Introduction

Increasing complexity of mission-critical systems fueled by semiconductor technology evolutions

But the decreasing reliability of processors requires new approaches

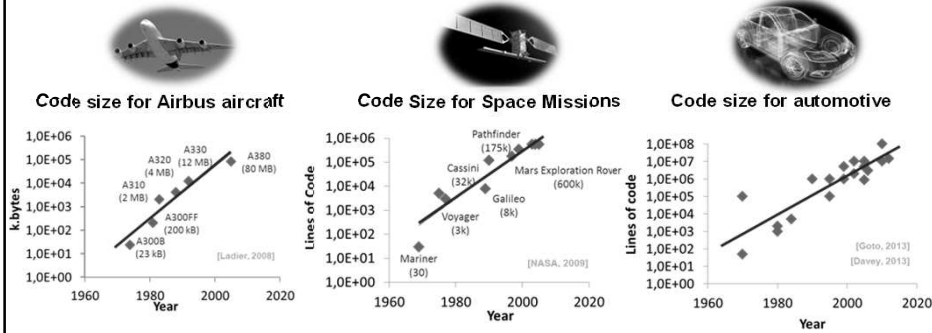


THALES

MPSiC 2015 - July 13-17, 2015

This document is not for production, modified, copied, published, translated or in any way disseminated without the prior written permission of Thales or THALES 2015 All rights reserved. Revision 7.0.

Code size evolution for critical embedded systems



Low-power low-performance processor not sufficient anymore for mission-critical systems

MPSiC 2015 - July 13-17, 2015

This document is not for sale, reproduction, modification, distribution, or any other use without the prior written consent of Thales. © 2015 Thales. All rights reserved. Version 7.1.0



- | | | | | | |
|--|---|---|--|---|--|
| <p>Flight Deck</p> <ul style="list-style-type: none"> CDS Control & Display System (1) HUD Head-Up Display OANS On board Airport Navigation System (1) BPI Brake Pressure Indicator | <p>Navigation & Flight Control</p> <ul style="list-style-type: none"> SFCS Slats & Flaps Control System (4) FCU Flight Control Unit (1) SNS Stand-by Navigation System DRA Digital Radio Altimeter RGU Ring Gyro Unit AU Accelerometer Units | <p>Cabin systems</p> <ul style="list-style-type: none"> In-Flight Entertainment TopSeries i-5000 video on demand on seats | <p>Avionics</p> <ul style="list-style-type: none"> IMA Integrated Modular Avionics (1) AFDX E/S Aircraft Full Duplex End-System (1) | <p>Utilities</p> <ul style="list-style-type: none"> DSMS Doors & Slides Management System (4) BSCF Braking & Steering System (3) | <p>Electrical Systems</p> <ul style="list-style-type: none"> EPGS Electrical Power Generation System (2) |
|--|---|---|--|---|--|



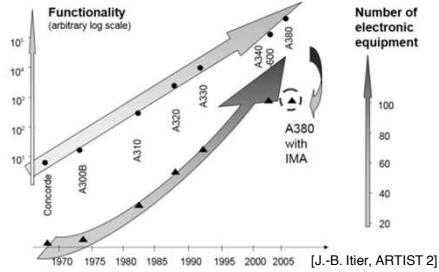
Diversity of applications, environments and severity levels

(1) In partnership with Diehl Aerospace
 (2) Developed by Aerotec, a JV with Goodrich
 (3) Supplied to Messier Bugatti
 (4) Delivered by Diehl Aerospace

Avionics bay



Motivations for IMA



➔ Avionics systems have transitioned from federated architectures to integrated architectures



MPS&C 2015 - July 13-17, 2015

This document is not for production, modified copies, callings, translations or material reproduction are prohibited without the prior written permission of Thales. © THALES 2015 All rights reserved. Version 7.1.0



THALES

MPS&C 2015 - July 13-17, 2015

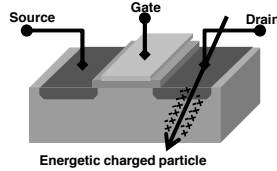
This document is not for production, modified copies, callings, translations or material reproduction are prohibited without the prior written permission of Thales. © THALES 2015 All rights reserved. Version 7.1.0

Technology scaling brings new challenges!

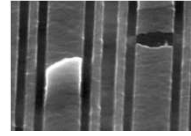
New technological process and process variability



Increased susceptibility to environment



Increased aging of devices



[IAIam, 2007]

- ◆ New technologies: FD-SOI, FinFET, 3D integration, ...
- ◆ Extensive process variations
- ◆ Infant mortality and intermittent faults
- ◆ Soft errors (SEU, MBU), EMC increased sensitivity
- ◆ Transient faults
- ◆ Early wear-out effects: BTI, TDDB, HCI, electromigration, ...
- ◆ Permanent faults

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

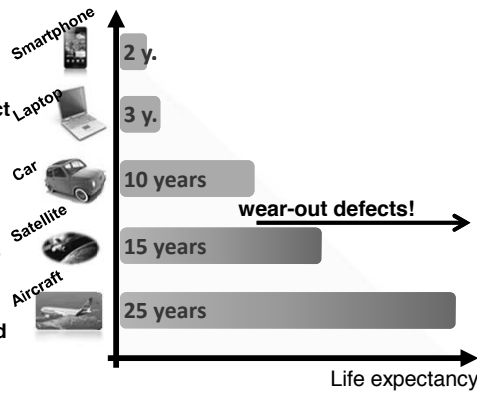
THALES

MPSiC 2015 - July 13-17, 2015

This document is not for production, modified, adapted, copied, retransmitted or used in any way without prior written permission of Thales. ©THALES 2015 All rights reserved. Rev. version 7.1.0

Transistor aging and service life guarantee

- ◆ Critical embedded systems life expectancy far exceeds that of their components lifetime
- ◆ Need of preventive maintenance → impact on cost and business model
- ◆ Will exacerbate the problem of the components obsolescence
- ◆ Degradation of SWaP expected for higher level of redundancy if strong degradation
- ◆ Reduction of the operating domains could limit the use of advanced component



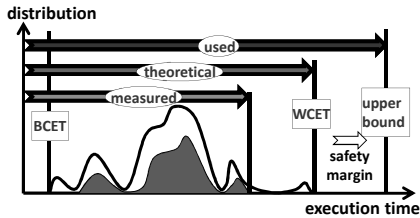
➔ Long-term reliability is a concern for products with long lifetimes

THALES

MPSiC 2015 - July 13-17, 2015

This document is not for production, modified, adapted, copied, retransmitted or used in any way without prior written permission of Thales. ©THALES 2015 All rights reserved. Rev. version 7.1.0

Critical safety = predictability + reliability



- ◆ Timing predictability of error detection & recovery mechanisms?
- ◆ Impact of hard faults in prediction structures and caches
- ◆ Guarantees on temporal and spatial isolation valid in presence of faults?

➔ Need of absolute guarantees on the timing (DO-178B)

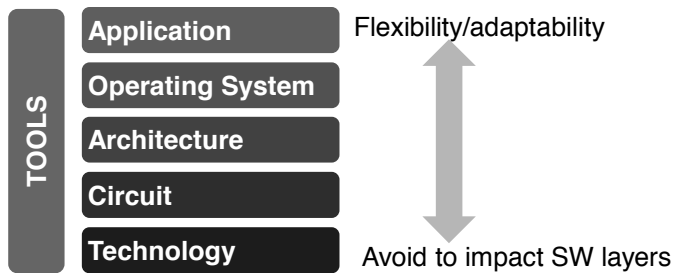


MPSiC 2015 - July 13-17, 2015

This document is not to be reproduced, modified, copied, distributed or used in any way without prior written permission of Thales. © THALES 2015. All rights reserved. Revision 7.1.0

◆ 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 ...



➔ Reliability assessment is a critical point to support new methodologies

MPSiC 2015 - July 13-17, 2015

This document is not to be reproduced, modified, copied, distributed or used in any way without prior written permission of Thales. © THALES 2015. All rights reserved. Revision 7.1.0



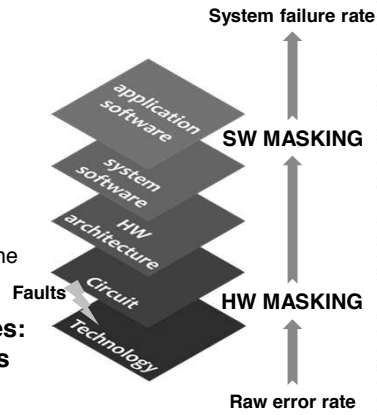
◆ The CLERECO FP7 Collaboration Project

- <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



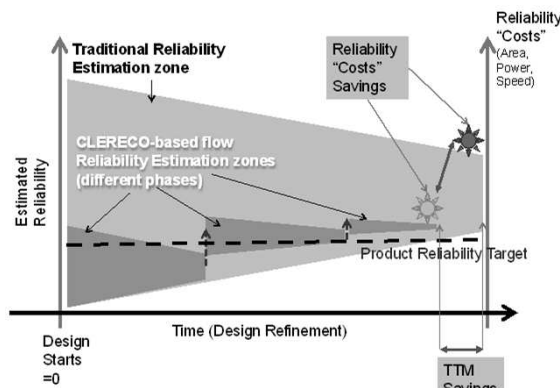
THALES

MPSiC 2015 - July 13-17, 2015

This document is not for production, modified, copied, distributed or used in any way without the prior written permission of THALES. © THALES 2015. All rights reserved. Rev. version 7.1.0.

◆ 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

MPSiC 2015 - July 13-17, 2015

This document is not for production, modified, copied, distributed or used in any way without the prior written permission of THALES. © THALES 2015. All rights reserved. Rev. version 7.1.0.

The CLERECO methodology in a nutshell

Software fault-injection

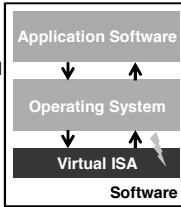
- ◆ At the intermediate code level in the LLVM framework
- ◆ Using a SW fault model defined at the ISA level

Micro-architectural simulator fault injection

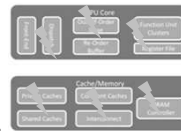
- ◆ Best trade-off between simulation time & accuracy
- ◆ Use of gem5 and MARSSx86 simulators
- ◆ Fault injection in all the major parts of the processor

Technology characterization

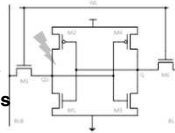
- ◆ Evaluation of raw error rates for different technologies and different operating conditions
- ◆ Resorting to Spice simulations



application + OS characterization

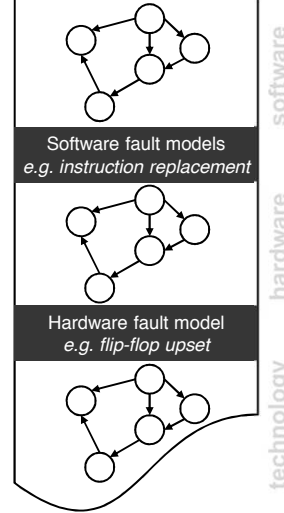


SW fault rates



raw error rates

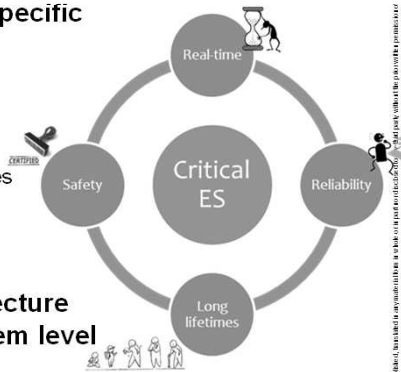
System model based on Bayesian network



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



THALES

