THALES

Towards the Reliability Estimation of Embedded Computing Systems: a Cross-Layer Approach

ARNAUD GRASSET – MPSOC 2016 - JULY 11-15, 2016

arnaud.grasset@thalesgroup.com

Introduction

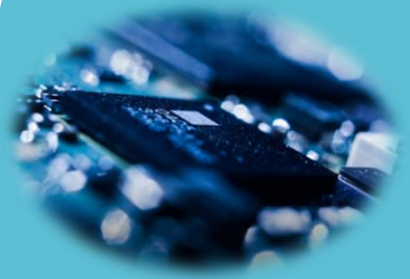
Decreasing lifetime/reliability of electronic components with new technology nodes

- New technologies and extensive process variations, increased susceptibility to environment, increased aging of devices

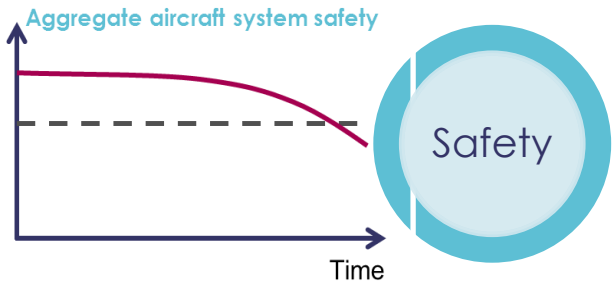
Specific technologies and IC are less and less affordable for mission-critical systems

- Need of fault-tolerance mechanisms to build dependable systems on top of unreliable components

Requires new approaches for reliability estimation!



Reliability Challenges for Critical Embedded Systems

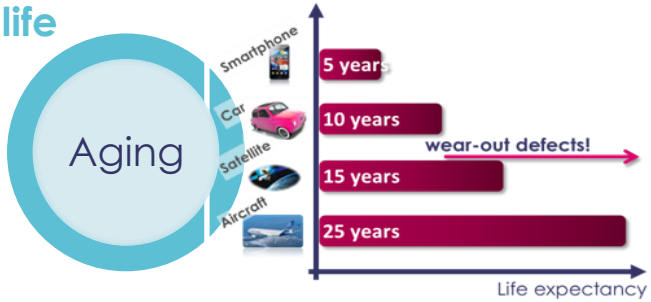


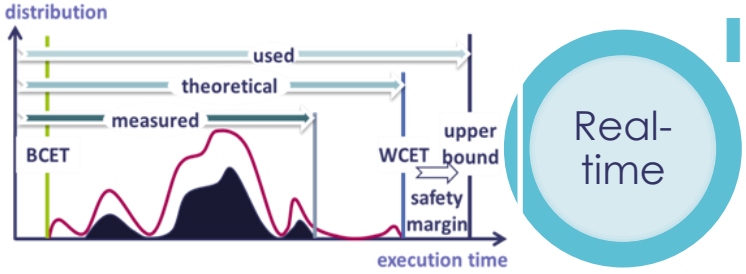
Operational reliability and safety impact

- Failure rate as low as 10^{-9} failure per hour
- Increasing soft-error failure rates
- Current practices based on the hypothesis of constant failure rates

Transistor aging and service life

- Preventive maintenance
- Components derating





Critical safety = predictability + reliability

- Predictability of error detection & recovery
- Impact of faults on timing

Réf. : TRT-Fr/STI/LSEC/AG,16/58 - 07/06/2016
Thales Research & Technology France
Template trtp version 8,0,0 / Template : 87204467-DOC-GRP-EN-002

THALES

New approaches to critical embedded system design

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 …

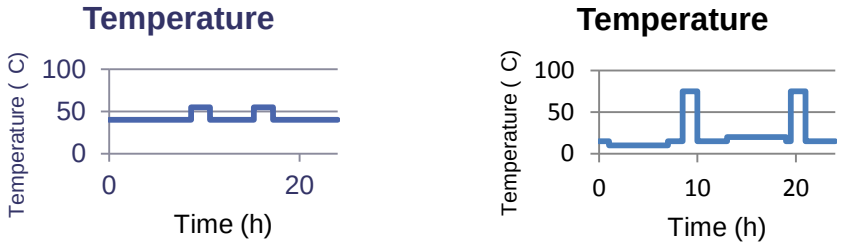
Need of methods and tools:

- To optimize HW and SW fault tolerance mechanisms (area, performance ,power and design efforts)
- To evaluate the impact of design choices on the reliability (e.g. processor selection and configuration)
- To avoid over-design due to excessive safety margins

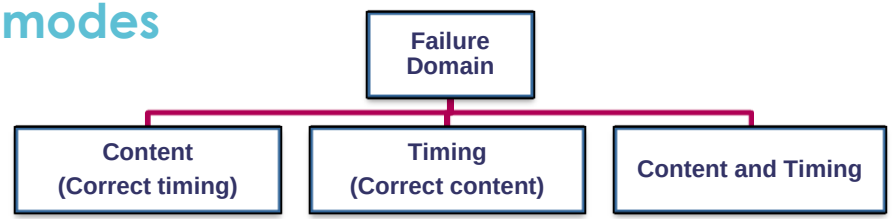
Reliability assessment is a critical point to support new methodologies

Challenges of Reliability Evaluation

Dependency on the environment, the mission profile, the location of the equipment in the system



Need to consider different failure modes



Faults propagation and masking of errors

Standard reliability evaluation approaches: massive and time-consuming simulations and/or fault injection campaigns

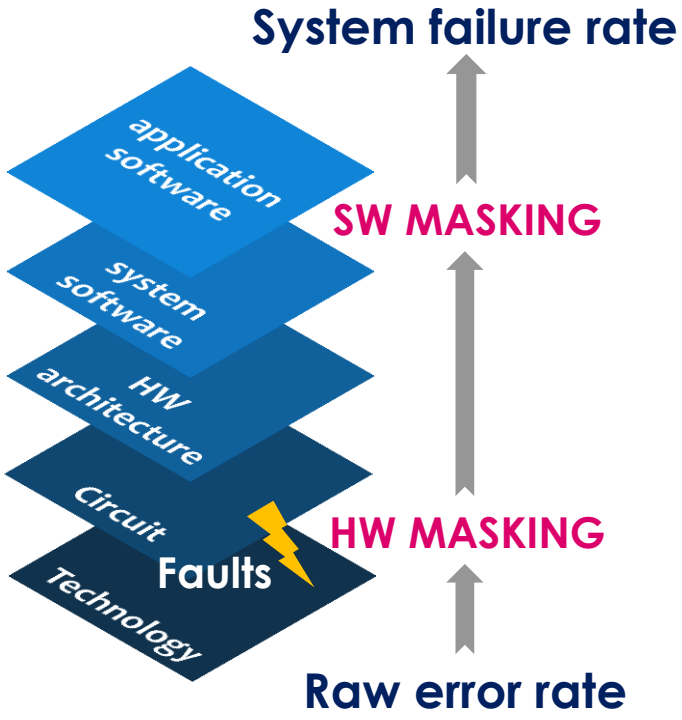
Cross-Layer Early Reliability Estimation

The CLERECO FP7 Collaboration Project

- http://www.clereco.eu

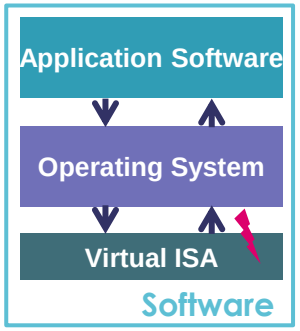
Cross-layer estimation:

- Reliability is evaluated at system level
- Considering the hardware structure as well as the software stack (application, OS, …)



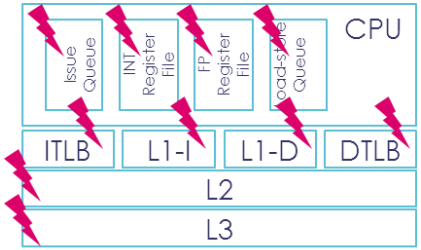
The CLERECO Methodology in a Nutshell

Software fault-injection



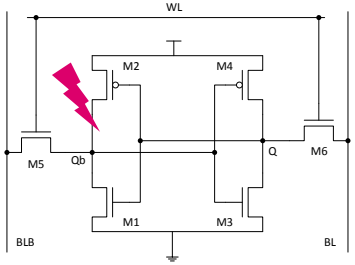
Application + OS characterization

Micro-architectural simulator fault injection



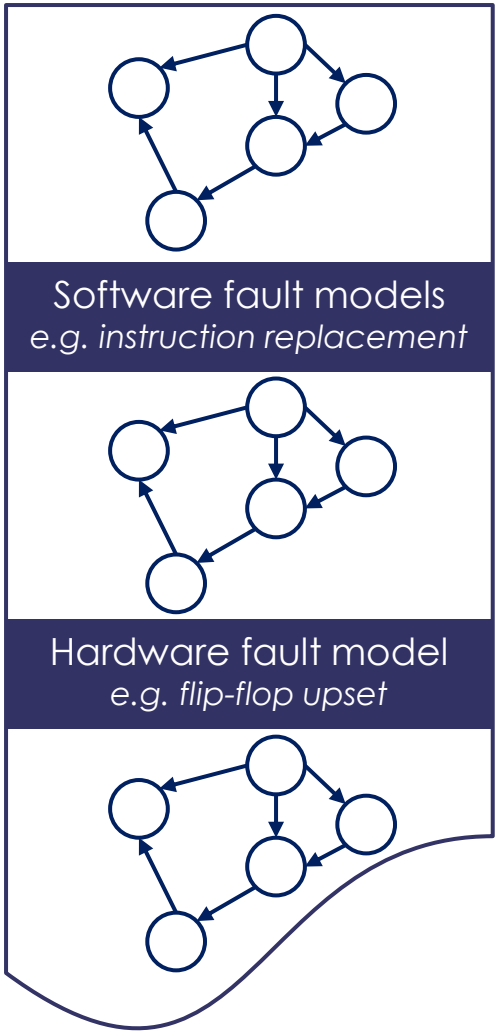
SW fault rates

Technology characterization



Raw error rates

System model based on Bayesian network



Micro-Architecture Reliability Analysis

Analysis of complex functional modules

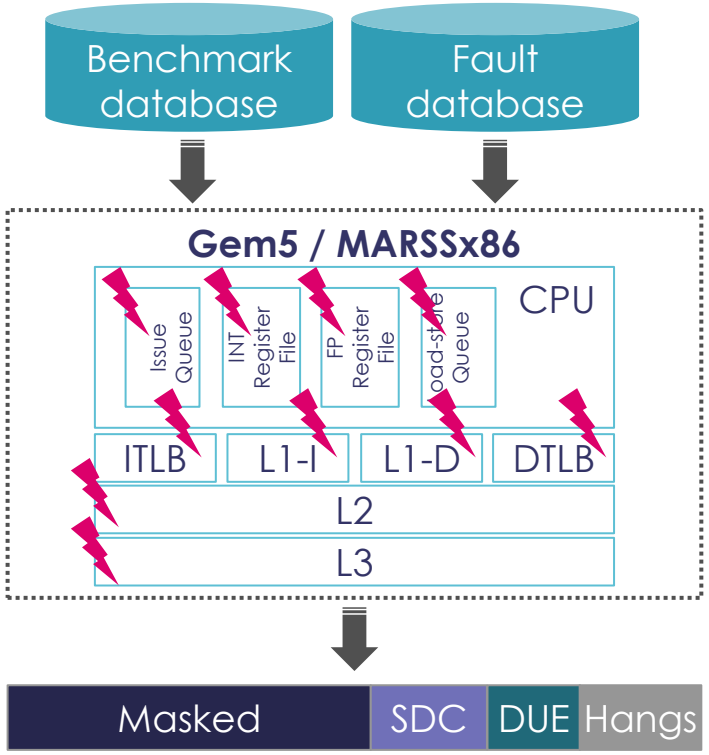
- CPU, GPU, NN accelerator

Fault injection at micro-architectural level

- Accurate models of storage components
- Simple implementation of control logic blocks

Tools based on Gem5 and MARSSx86 simulators for CPU characterization

- Characterization of x86 and ARM architectures
- Comparison of ISA and of simulators



M. Kaliorakis, S. Tselonis, A. Chatzidimitriou, N. Foutris and D. Gizopoulos, "Differential Fault Injection on Microarchitectural Simulators," 2015 IEEE International Symposium on Workload Characterization (IISWC), Atlanta, GA, 2015, pp. 172-182.

Software Reliability Analysis

Analysis of complex software stack

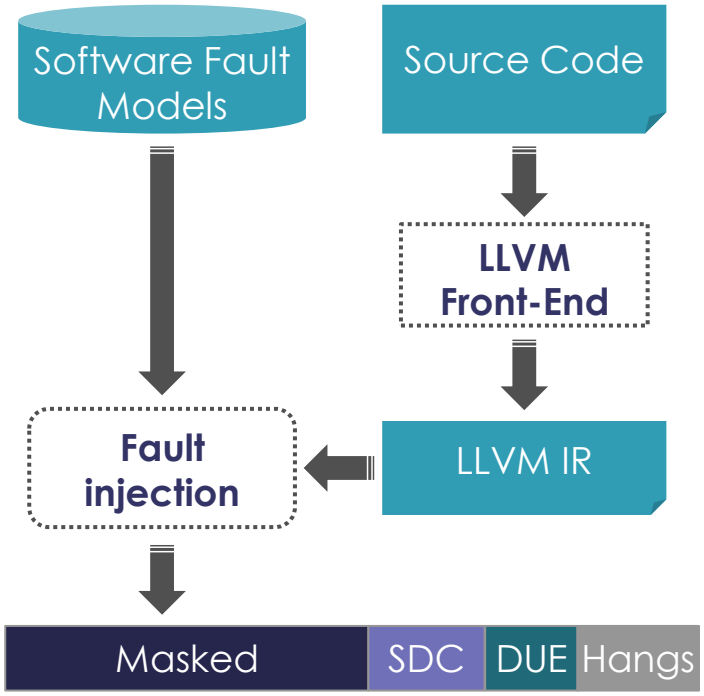
- Independently from the target HW
- FI less computation intensive at software layer than at architectural level

LLVM Intermediate Representation (IR)

- Independent from the source language and the target machine

Software Fault Models defined at the ISA level

- Data fault models, code faults models, system fault models
- Represent effects of real HW faults



M. Kooli, A. Bosio, P. Benoit and L. Torres, "Software testing and software fault injection," 2015 10th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS), 2015, pp. 1-6.

System Reliability Analysis

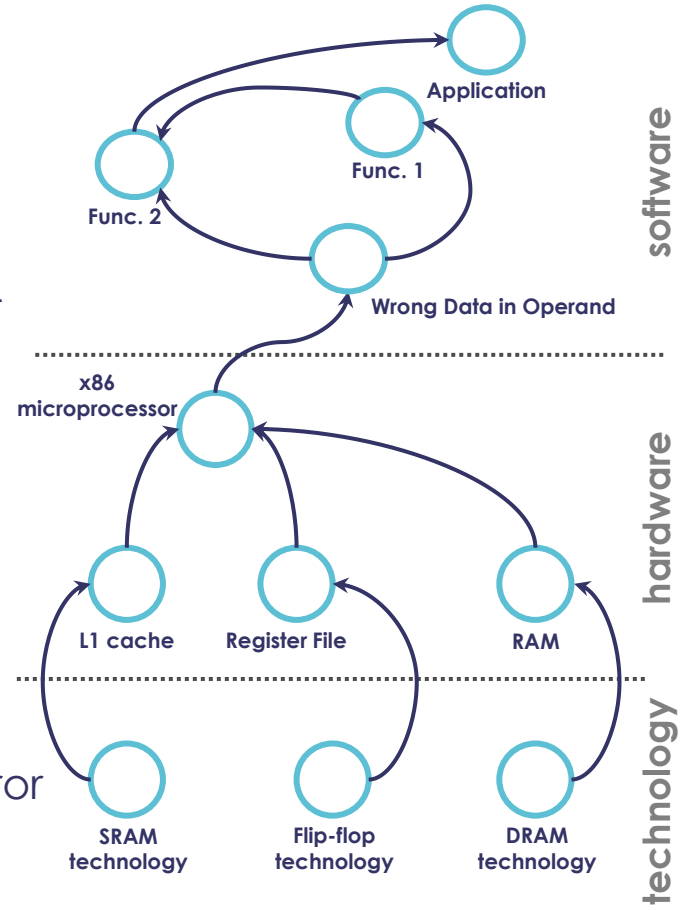
Use of Bayesian Network as a model for statistical reliability modelling

Nodes are associated to:

- Technologies with raw failure rates (with respect to the target fault model)
- Hardware resources
- Software fault models (i.e. probability of propagation from HW to SW)
- SW functions or portions of SW functions

Analysis of the interaction of the blocks

- A Conditional Probability Table (CPT) models error propagation or masking
- Predictive reasoning or diagnostic reasoning



A. Vallero et al., 2015. Cross-layer reliability evaluation, moving from the hardware architecture to the system level. Microprocess. Microsyst. 39, 8 (November 2015), 1204-1214.

Conclusion

Evolution of semiconductor technologies will impact the reliability of critical embedded systems

- Severely constrained by safety rules and standards

Early reliability estimation necessary to drive & optimize design

The CLERECO project addresses the problem of the early reliability estimation of computing systems

- Independent HW and SW analysis to reduce the complexity
- Enables a deep understanding of fault masking and propagation of errors