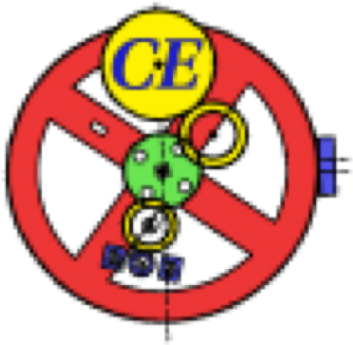
Computer Engineering Laboratory

Quantum and Computer Engineering Department

Said Hamdioui

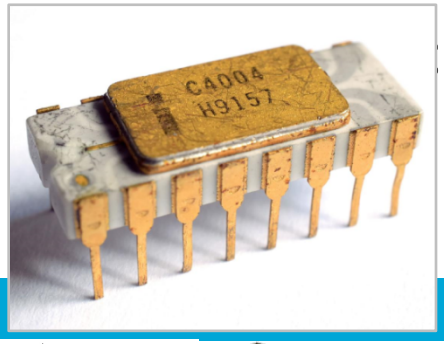


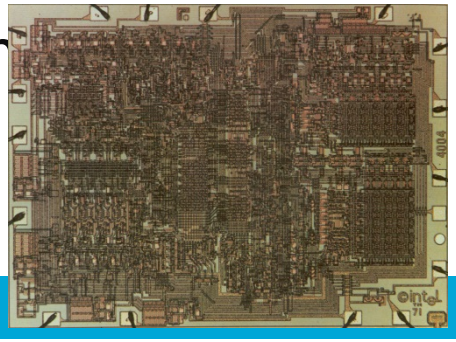
Delft University of Technology

Integrated Circuits

First commercialized IC

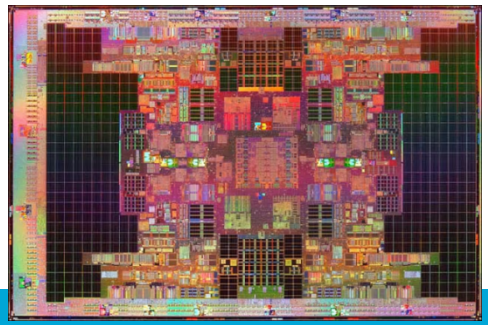
- Intel 4004 (1971-1978)
- Clock speed: 740 KHz
- Transistors: **2300**
- Pins: **16**
- Application: Arithmetic
- Min. feature size: **10 µm**



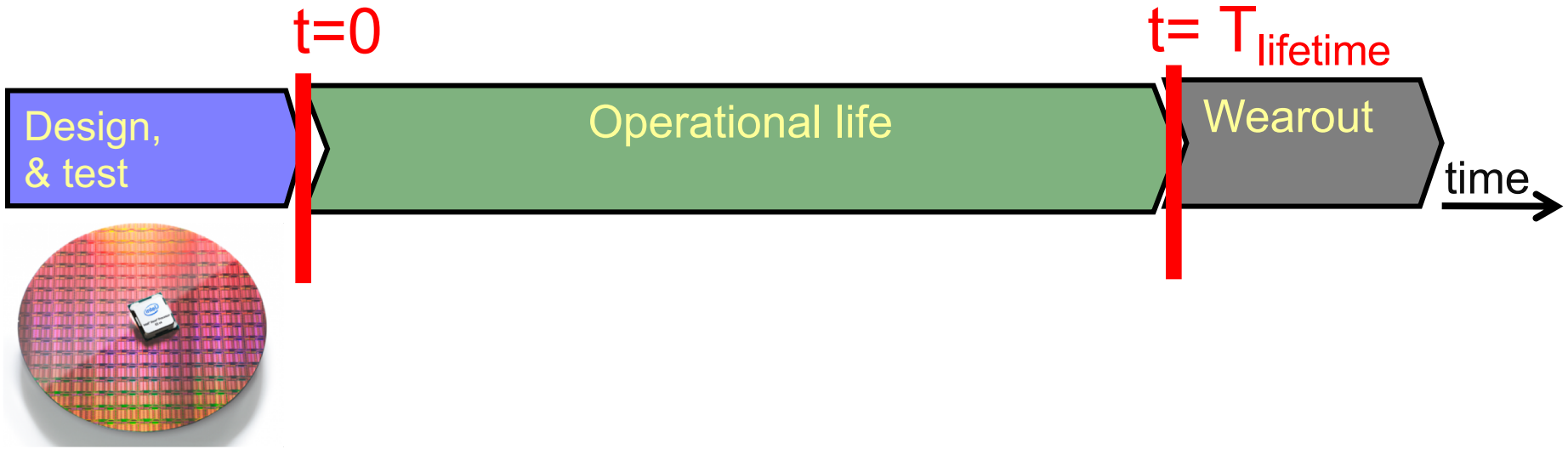


Itanium processor

- Intel 2001-2017
- Clock speed: 733MHz to 2.66GHz
- Transistors: >**2B** (2010/65nm)
- Pins: **1248**
- Application: Servers
- Min. feature size: **130nm- 32nm**
- 64bit architecture
- **21.5mmx32.5mm** die

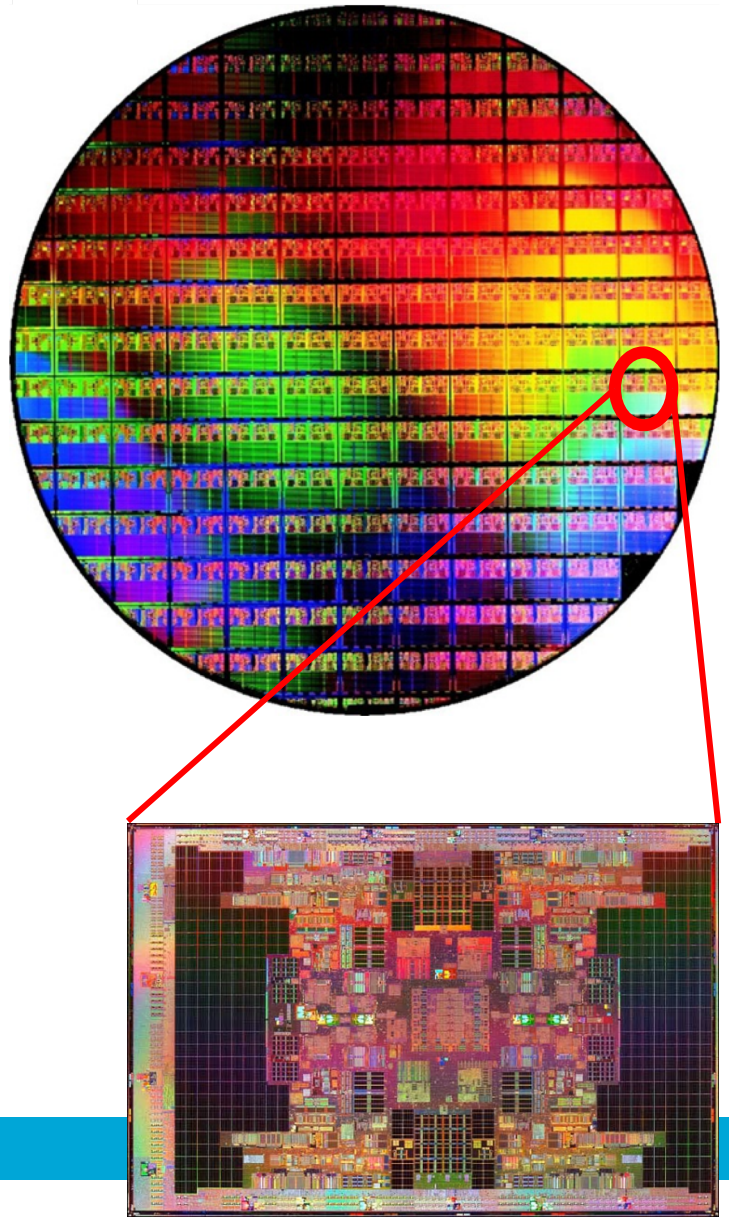


HW Dependability: Test & Reliability



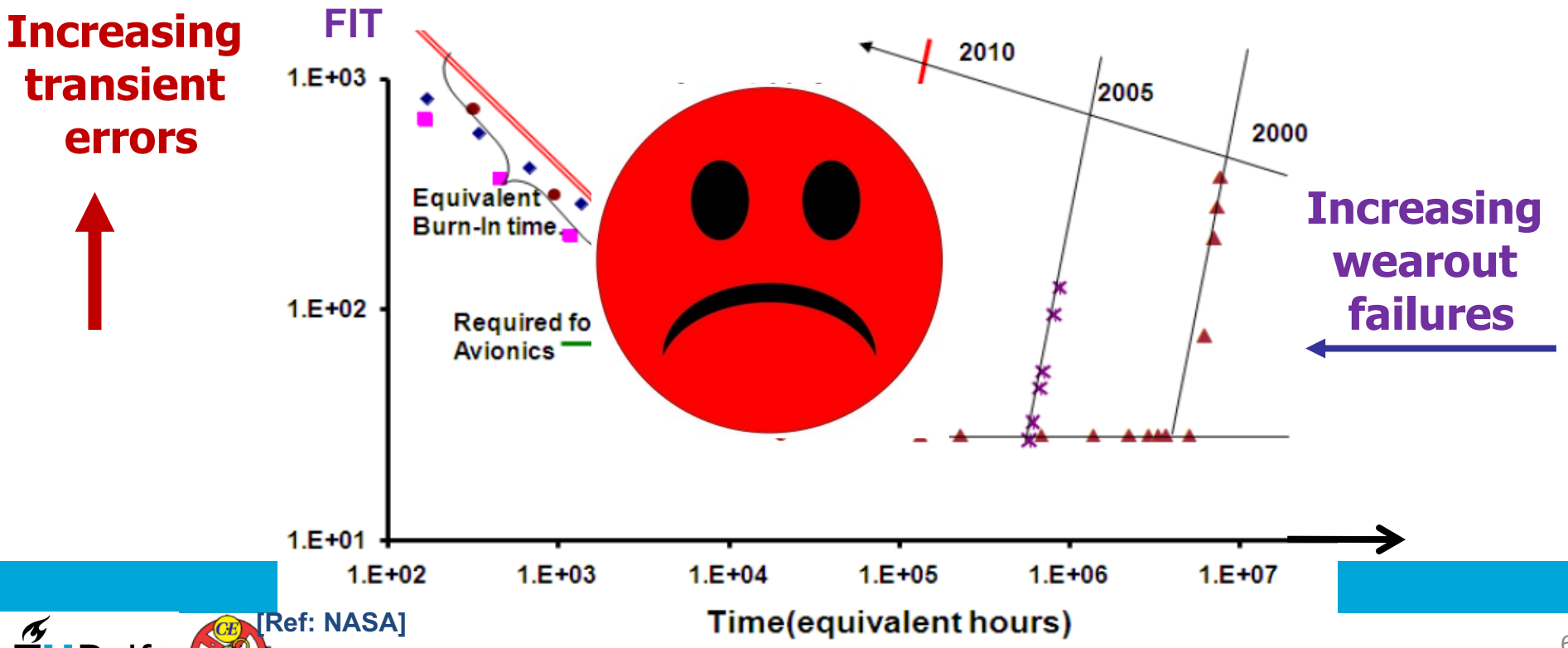
HW Dependability: Test & Reliability

- Wafer test: case 1
  - Assume chip is 8 bit **adder**
  - Test machine: 1 GHz
  - Required test time: $2^{16}*10^{-9}$= **65,5 us**
- Wafer test: case 2
  - Assume chip is 32 bit **adder**
  - Test machine: 1 GHz
  - Required test time: $2^{64}*10^{-9}$= **585 years!**
  - **NOT practical**
- Challenges
  - Deep understanding of failure mechanisms
  - High quality and efficient solutions
  - Strongly application dependent



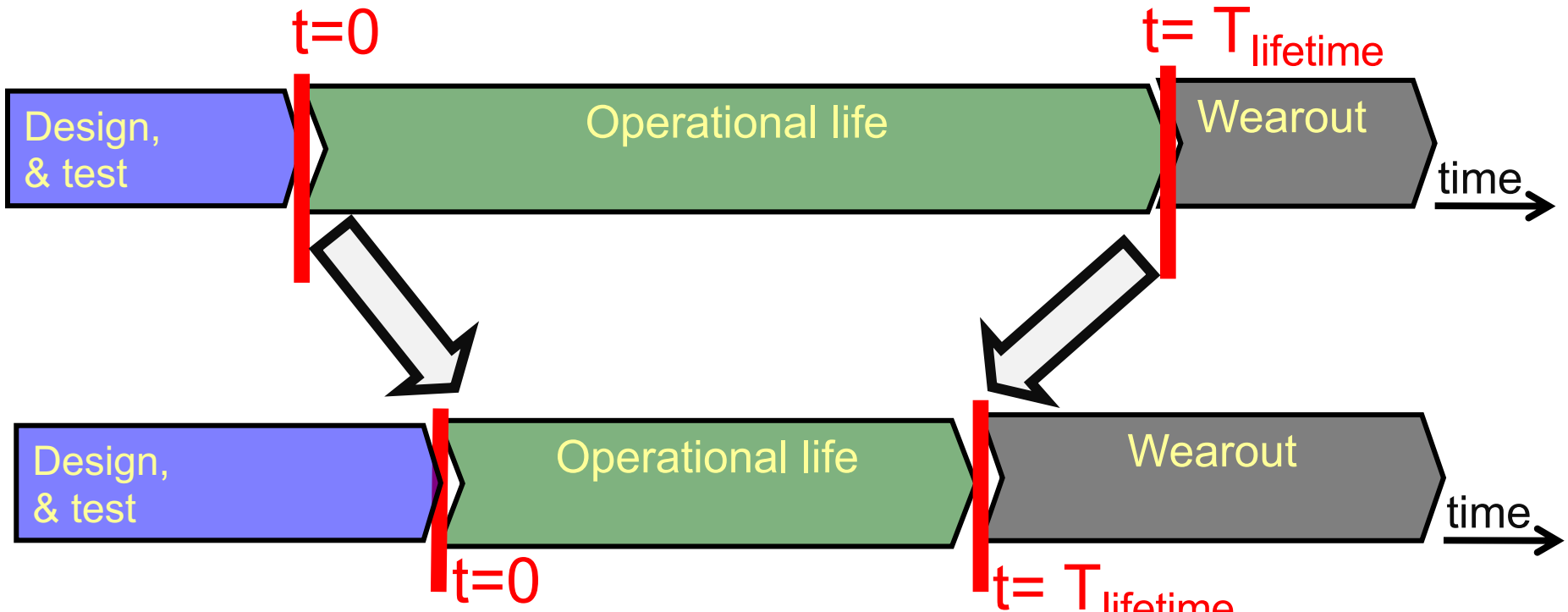
HW Dependability: Test & Reliability

HW Dependability: Test & Reliability



[Ref: NASA]

HW Dependability: Test & Reliability



Shorten TTM &
Extend lifetime &
Reduce failure rate

Technology trends & business pressure are redefining the Design, Test & Reliability paradigms

HW Dependability: Test & Reliability

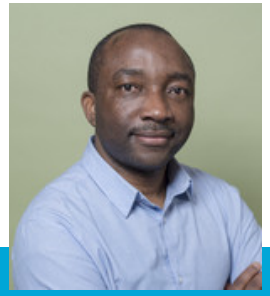
FinFET memories | **STT-MRAM** | **ReRAM**

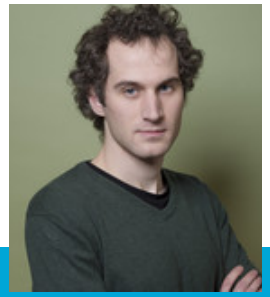
Device-Aware Test: A New Test Approach Towards DPPB Level

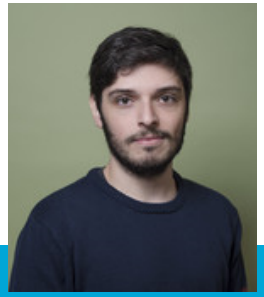
Moritz Fieback[1] Lizhou Wu[1] Guilherme Cardoso Medeiros[1] Hassen Aziza[2]
Siddharth Rao[3] Erik Jan Marinissen[3] Mottaqiallah Taouil[1,4] Said Hamdioui[1,4]
[1]Computer Engineering Laboratory, Delft University of Technology, Mekelweg 4, 2628CD, Delft, The Netherlands
[2]IM2NP, UMR CNRS 7334, Aix-Marseille Université, 38 rue Joliot Curie, F-13451, Marseille, France
[3]IMEC, Kapeldreef 75, B-3001, Leuven, Belgium
[4]CognitiveIC, Van der Burghweg 1, 2628CS, Delft, The Netherlands
Email: S.Hamdioui@tudelft.nl

***Abstract*—This paper proposes a new test approach that goes beyond cell-aware test, i.e., device-aware test. The approach consists of three steps: defect modeling, fault modeling, and test/DfT development. The defect modeling does not assume that**

Testing defects in logic and memory chips underwent a long evolution process. For logic, early test methods were mainly functional and did not use any fault models. However, the increasing cost of such test approaches has led to the


Innocent Agbo


Daniël Kraak


Guilherme C. Medeiros

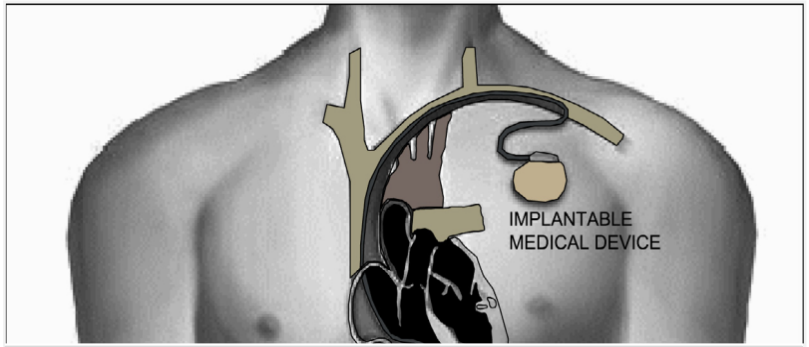

Lizhou Wu


Moritz Fieback


Felipe A. da Silva

HW Dependability: Security- Attacks

IC data



IC functionality

IC design

IC functionality

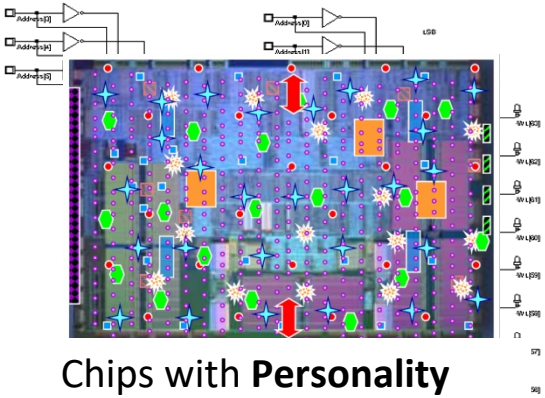
Costs the global economy over **US$400 billion** a year!

90 % of companies insufficiently prepared for attacks!

HW Dependability: Security

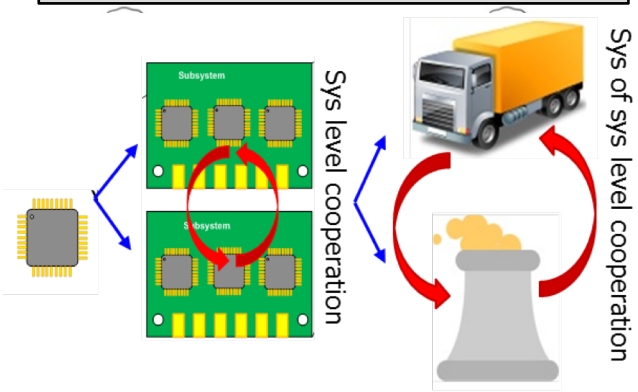
HW Attacks

Design-for-Security



Chips with **Personality**

Secure architectures



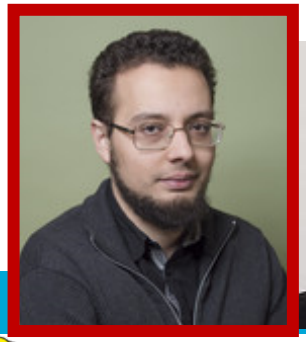
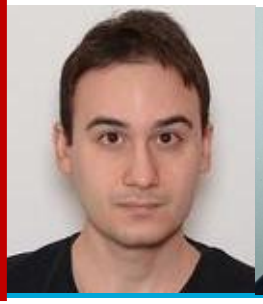
intrinsic ID

riscure
Challenge your security

UNIQIC

Nederlands Forensisch Instituut
Ministerie van Veiligheid en Justitie

LIRMM



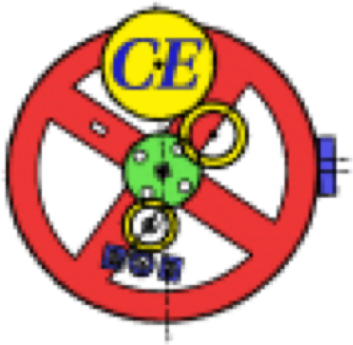
M. Taouil

T. Cagil Koylu | S. Masoumian | A. Aljuffri | C. Reinbrecht | **F. Smailbegovic**

Computer Engineering Laboratory

Quantum and Computer Engineering Department

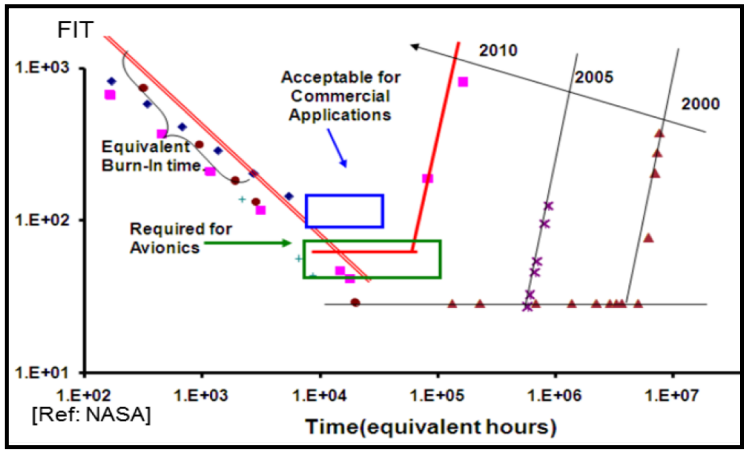
Said Hamdioui



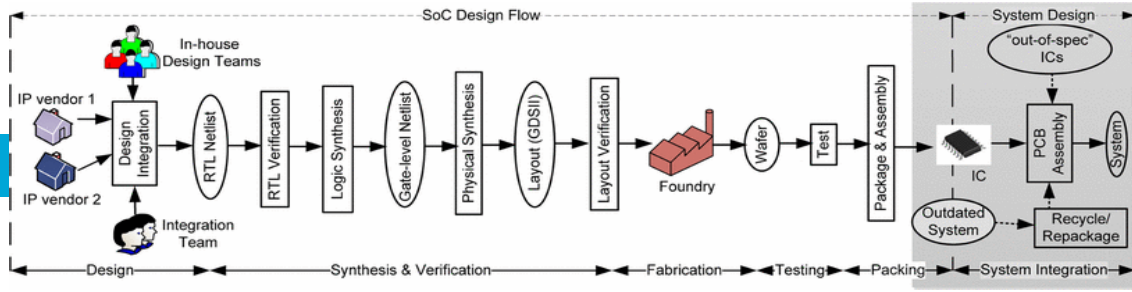
Delft University of Technology

Hardware/technology challenges

- Constant filed scaling
  - Reduced **reliability**
  - High leakage High cost,
  - Low yield,
  - TTV & TTM => **Test & diagnosis**



- **Globalization of IC supply chain**
  - Insert malicious circuits & chip/system vulnerabilities
  - Attacks: data (asset), design (IP), functionality (tempering)
  - User privacy and data protection (cloud)
  - **Security**



Hardware dependability research

- **Test and Reliability**
  - Fault modeling & Test generation
  - Design for testability
  - Reliability modelling and mitigation
  - STT-MRAM, ReRAM, FinFET SRAMs, 3D ICs

- **Hardware security**
  - Design for security
  - Secure hardware
  - PUF technology
  - HW driven solutions

Collaborators

Projects