



Y O G I T E C H

HiPEAC Innovation Event
Edinburgh, 4th May 2010

Riccardo Mariani

YOGITECH snapshot

- Semiconductor IP Design&Verification Company, founded in August 2000, headquartered in Pisa
- Ownweship: Managers (60%), Toscana Venture Fund (25%) and business angels (15%)
- 20 people
- Background on VLSI Design&Verification, expertise on fault tolerance from nuclear physics and satellite applications
-  Technology applied to safety-critical market fields
- Revenues: average 2004-2008: €2m
- Revenue split: 40% Europe, 48% Japan, 12% USA

- Main Customers



Mission

- Nowadays, many safety-critical systems depend on **electronic devices** operating correctly
 - For example, a microcontroller for braking systems or a microcontroller in a pacemaker
- International norms such as IEC 61508 and ISO 26262 define measures to be adopted to guarantee **functional safety**
 - Those measures are rated according “safety integrity levels” (for example SIL3 or ASILD)
- The ultra-deep integration allowed by modern semiconductor technologies bring the safety risk **INSIDE** those complex devices
- Our mission:
to guarantee functional safety of **integrated circuits**

faultRobust technology



fRMethodology

A white-box approach to perform functional safety assessment and safety-oriented design exploration of integrated circuits according IEC 61508 and ISO 26262

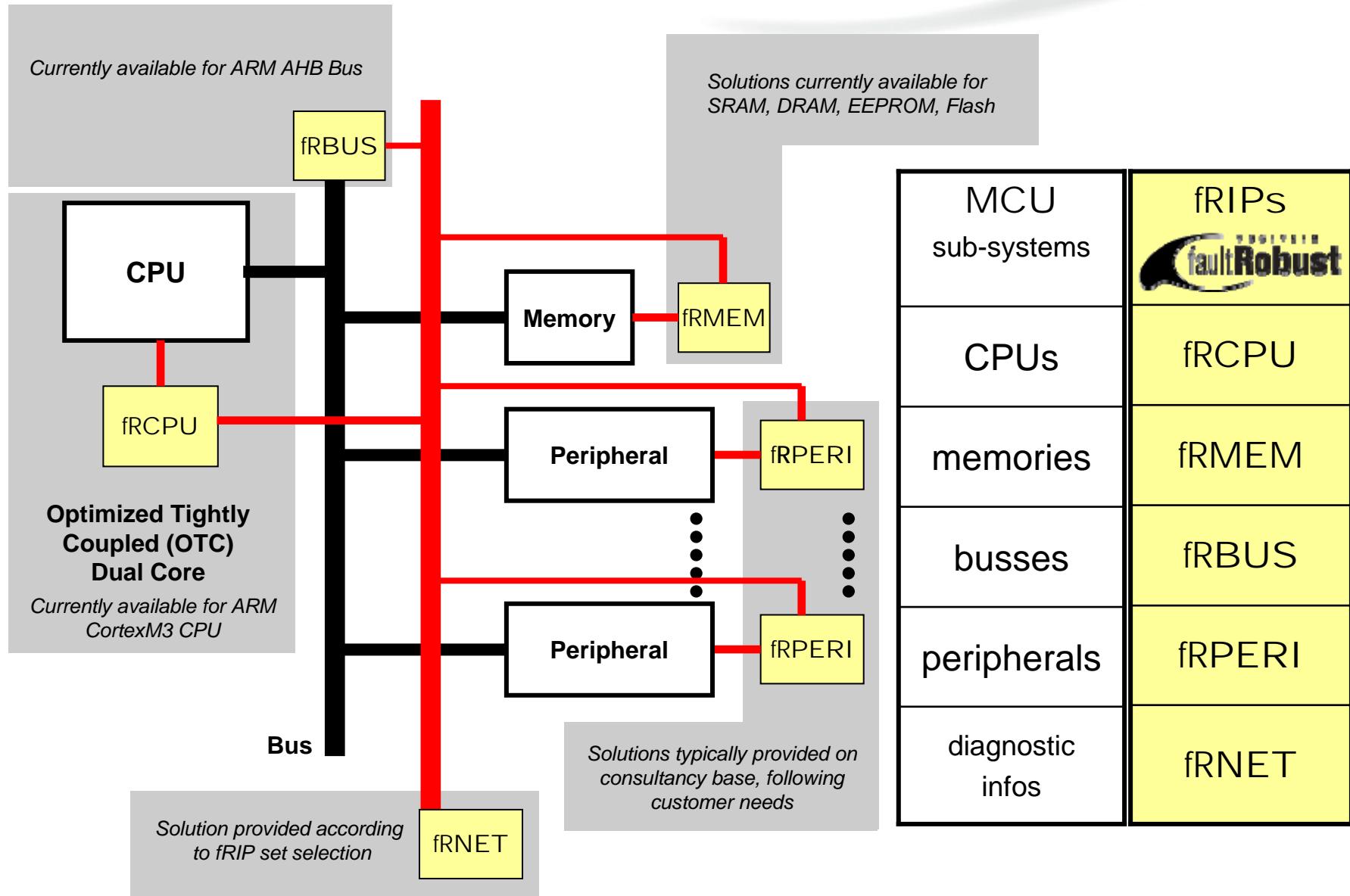
fRIPs

HW modules implementing safety mechanisms for basic units like CPU, MEM, BUS and Peripherals, aimed to reach appropriate Safety Integrity Level at integrated circuit level

fRM methodology

- fRM methodology is a “white-box” approach to do functional safety analysis and safety-oriented exploration of integrated circuits (e.g. microcontrollers, analogue-mixed ASIC, FPGA) in compliance with IEC 61508 and other domain-specific functional safety norms such as ISO 26262, EN 50128/9 etc...
 - splitting the component or system in elementary parts (“sensitive zones”)
 - computing their failure rates
 - using those failure rates to compute safety metrics
 - validating the results with fault injection
 - allowing sensitivity analyses of those metrics by changing architectural or technological parameters
 - delivering to customer numbers to compare different architectures

faultRobust IPs

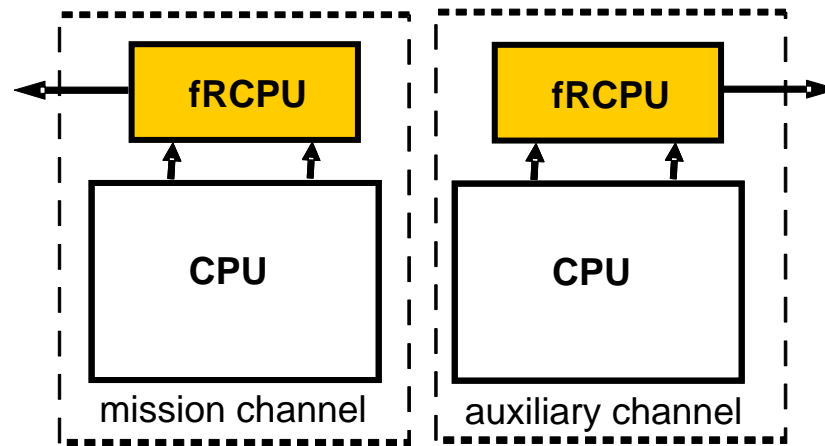


Common features of fRIPs

- Much **smaller** than a simple redundancy
 - e.g. fRCPU is 30%-40% of the CPU size
- Architectural + functional **diversity**
 - common-cause failures intrinsically reduced without the need of additional layout/HW measures
 - systematic failures detected by the diversity
- **Full functional safety** including the supervisor itself
 - fRIPs include circuitry to detect or support detection of latent faults
- Delivering **detailed diagnostic information**, e.g.:
 - type of error
 - load/store fault, register fault, memory bit flip, bus matrix fault etc...
 - context information
 - last instruction executed without errors, address of faulty location, bus slave addressed during the fault, etc...

Targeting multi-cores

- Using faultRobust IPs for **cost-optimized** safety-critical multi-cores:



- Two channels, each one supervised by one fRCPU
 - both actives in normal operation: in case of a fault in one of the two cores, tasks of one core can be mapped on the other core
 - or keeping one active in normal operation while the other (auxiliary channel) is switched on only if the first is failing

Adoption of faultRobust



Press Release

Toshiba announces implementation of new functional safety concept on MCU for SIL3 and ASILD level applications

ARM Cortex™-M3 MCU has been specified, designed and analyzed in accordance with functional safety norms IEC61508 and ISO26262

Düsseldorf, Germany, 18th January, 2010 – Toshiba Electronics Europe (TEE) has announced a microcontroller that can be certified to Safety Integrity Level 3 (SIL3) and Automotive SIL D (ASILD) while significantly reducing associated system cost and performance overheads.

....

TEE worked closely with Yogitech SpA, a company specialized in functional safety, and utilized Yogitech's fRMethodology based assessment flow and library of Intellectual Properties (fRIPs) in its solution.

.....

<http://www.toshiba-components.com/prpdf/5937E.pdf>



Y O G I T E C H

YOGITECH SPA

via Lenin 132/p

56017 San Martino Ulmiano

Pisa (Italia)