YOGITECH

# Simplifying SIL3 MCU safety architectures in automotive applications according to IEC61508 norm

**Silvano Motto – CEO Yogitech**
**Stefano Lorenzini – Design Engineering Manager Yogitech**

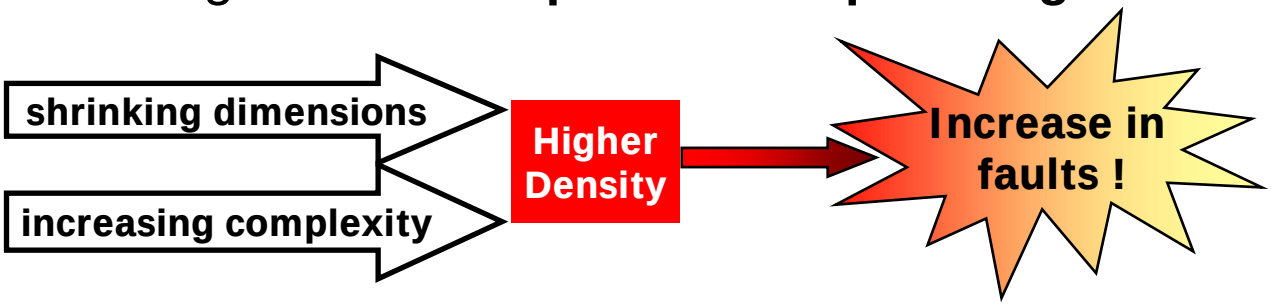
*Automotive Electronics and Electrical Systems Forum 2008, 6th May*

# Outline

- Background
- From black to white-box approach: the fRMethodology
- The faultRobust IPs
- A comprehensive approach
- Conclusions

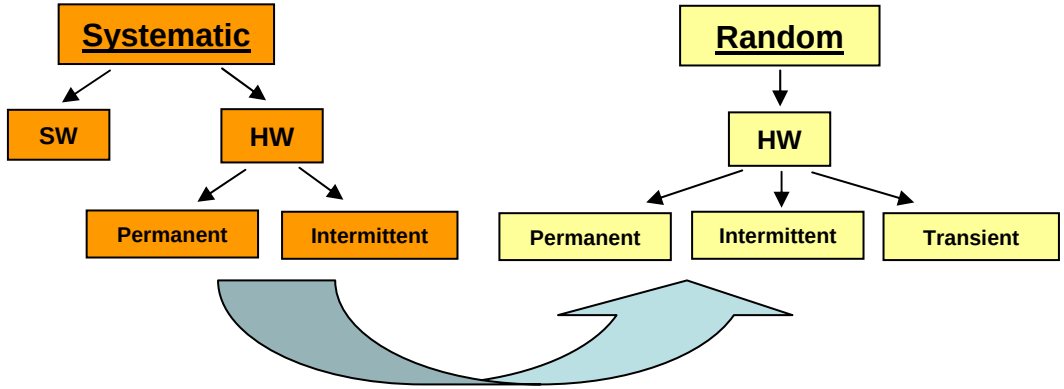
# Background (1)

New technologies allow **deeper and deeper integration**




| Fault model | Unit | Sources | Trend |
|---|---|---|---|
| Permanent | ≤ $10^{-5}$ FIT/gate | Telcordia Pauli, VDI SN29500 | ↔ |
| Transient (memories) | $10^{-2}$÷ $10^{-4}$ FIT/bit | ITRS 2006 | ↔ ↑ |
| Transient (registers) | $10^{-3}$÷ $10^{-5}$ FIT/reg | Kopetz, Mitra | ↑ |
| Transient (glue logic) | $10^{-7}$÷ $10^{-9}$ FIT/gate | Kopetz, Mitra | ↑ |

FIT = Failure In Time, number of failures in $10^9$ hours




**Fault robustness** is more and more a top priority concern

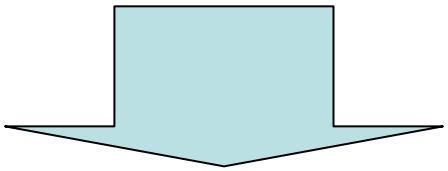
safety-critical automotive applications are looking **today** for next generation solutions and methodologies addressing fault robustness; IEC61508 and in future ISO26262 are more and more popular as reference norms

YOGITECH faultRobust

# Background (2)

**Modern MCUs:**

- Complex CPU with big memories and many peripherals
- Mix of commodity and safety-critical functions
- Complex interconnection scenarios



**A comprehensive approach for safety-integrity is needed:**

- reducing system costs and complexity
- saving CPU performance
- allowing reuse and flexibility
- easing system ‘safety’ engineering
- easing system certification

YOGITECH faultRobust

# Yogitech faultRobust technology


**fRMethodology**

A systematic procedure addressing IEC61508 requirements in the design of VLSI components for safety-critical applications

**fRIPs**

HW modules implementing ad-hoc diagnostic for basic elements like CPU, MEM, BUS and Peripherals aimed to reach appropriate Safety Integrity Level at VLSI component level



YOGITECH
faultRobust

# The fRMethodology

- Allowing a safety oriented design exploration at System-on-Chip level (white-box approach)

- Using well established methodologies (FMEA, Fault Injection, etc.) embedded in a standard System-on-Chip design&verification flow

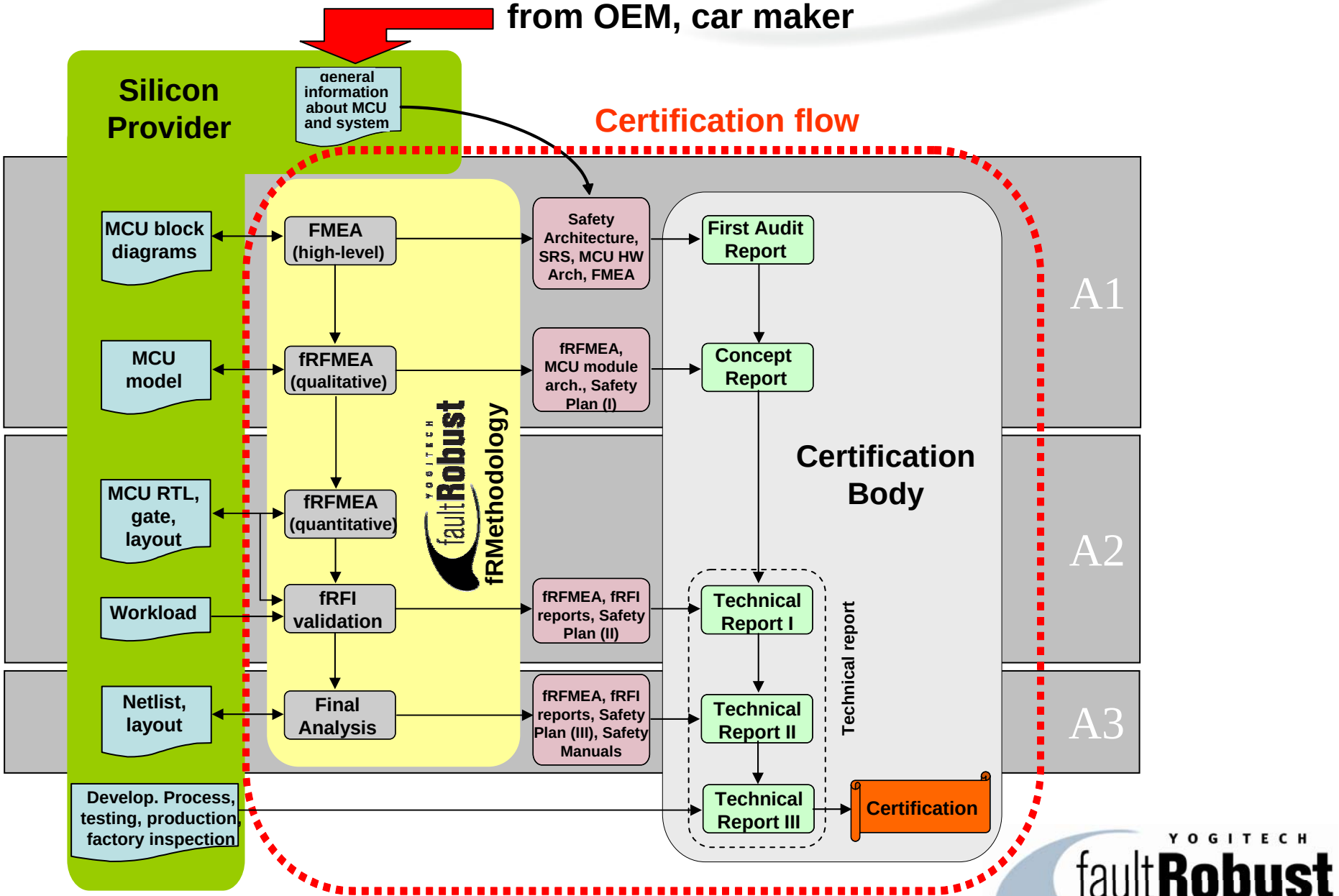
- Computing and validating metrics and parameters required for IEC61508 certification: Safe Failure Fraction, Diagnostic Coverage, Failure Rate and βIC

- TÜV SÜD approved

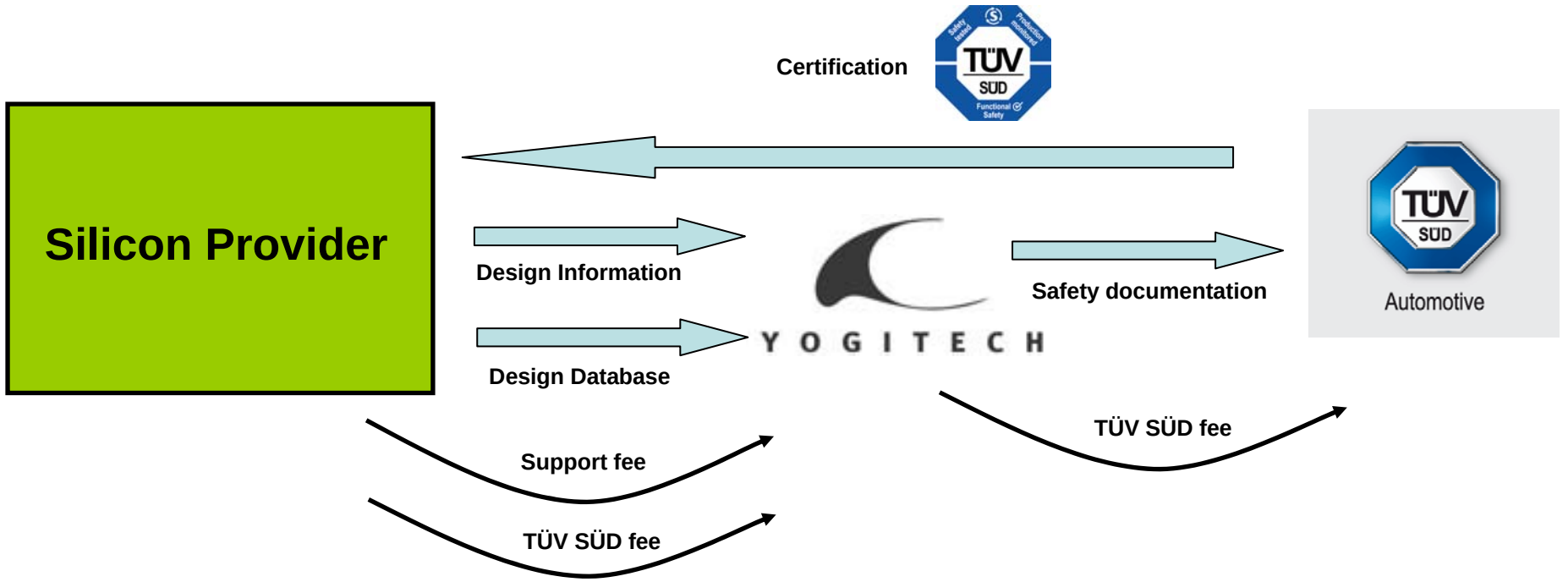


YOGITECH faultRobust

# Certifying with fRMethodology



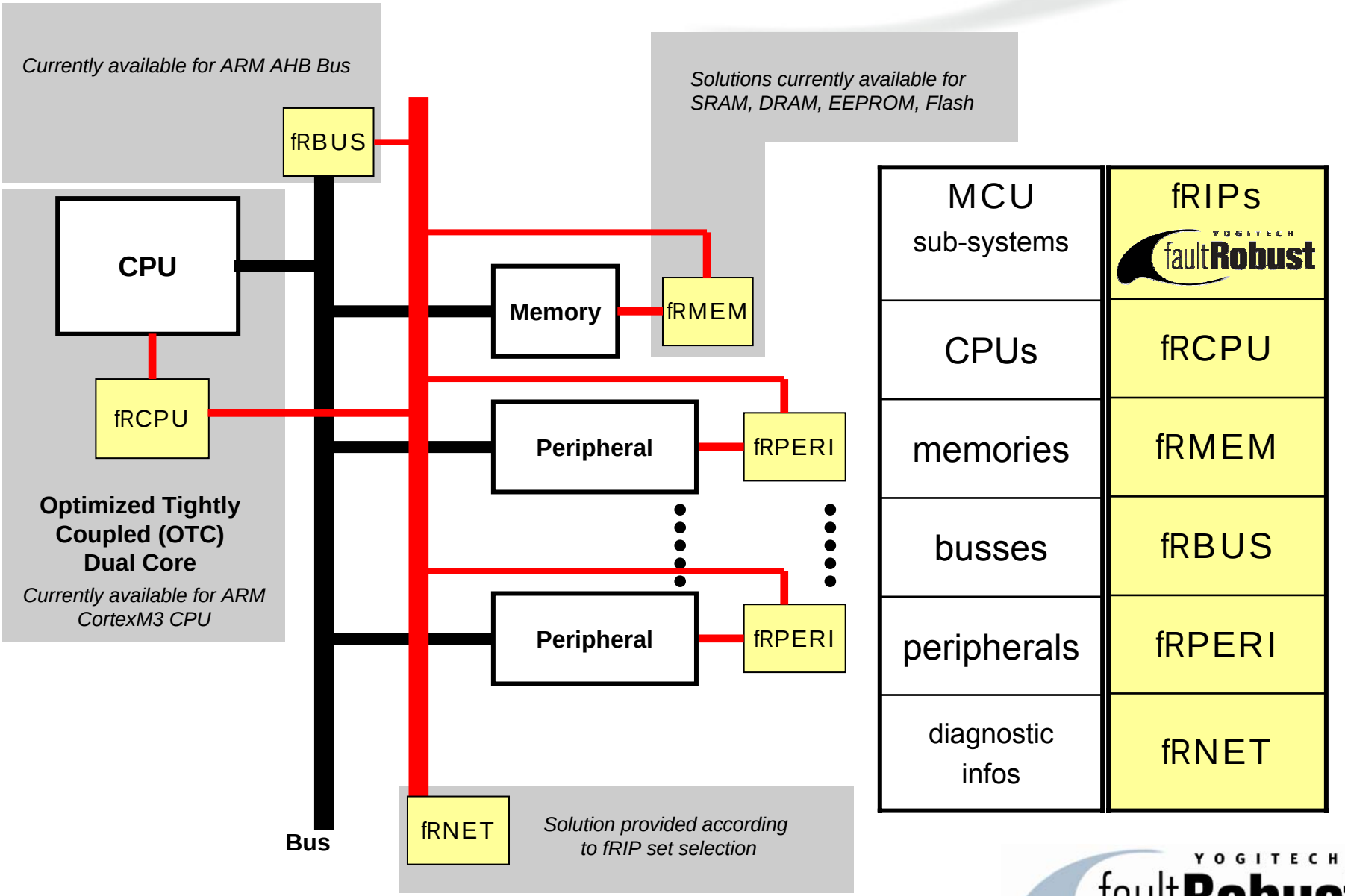
# fRMethodology: Business Model






YOGITECH faultRobust

# The faultRobust IPs



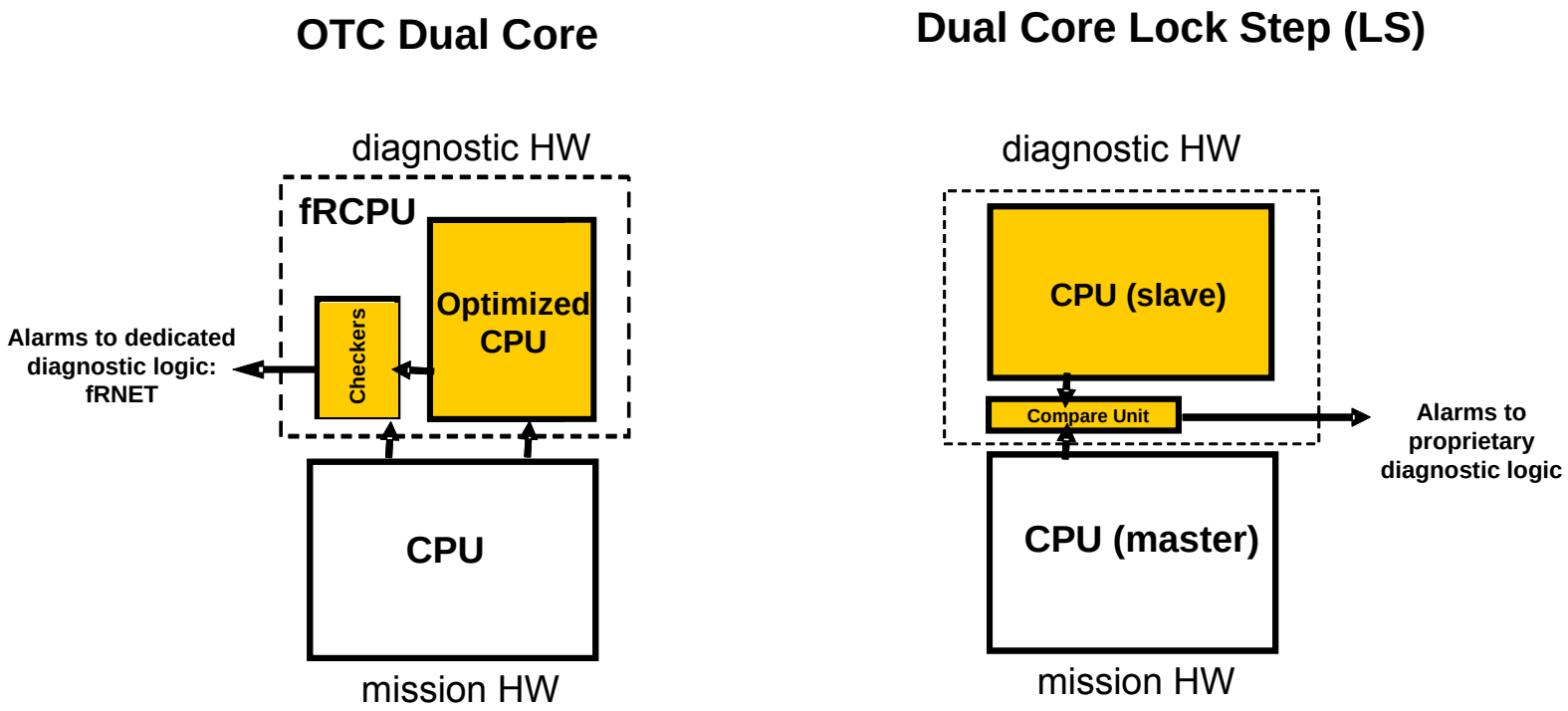

YOGITECH faultRobust

# Common features of IPs

- **Architectural + functional diversity**
  - common-cause failures intrinsically reduced
  - $\beta_{IC} \leq 25\%$ achieved without additional layout/HW measures
- **Functional safety guaranteed for the complete subsystem**
  - Safe Failure Fraction calculated at subsystem level
  - Self-checking circuitry included in each fRIP
- **Delivering detailed diagnostic information, e.g.:**
  - type of error
    - load/store fault, register fault, memory bit flip, bus matrix fault
  - context information
    - last instruction executed without errors, address of faulty location, bus slave addressed during the fault, etc…
- **All fRIPs delivered certified by TÜV SÜD**
  - each fRIP is delivered with HW/SW Safety Manuals

YOGITECH faultRobust

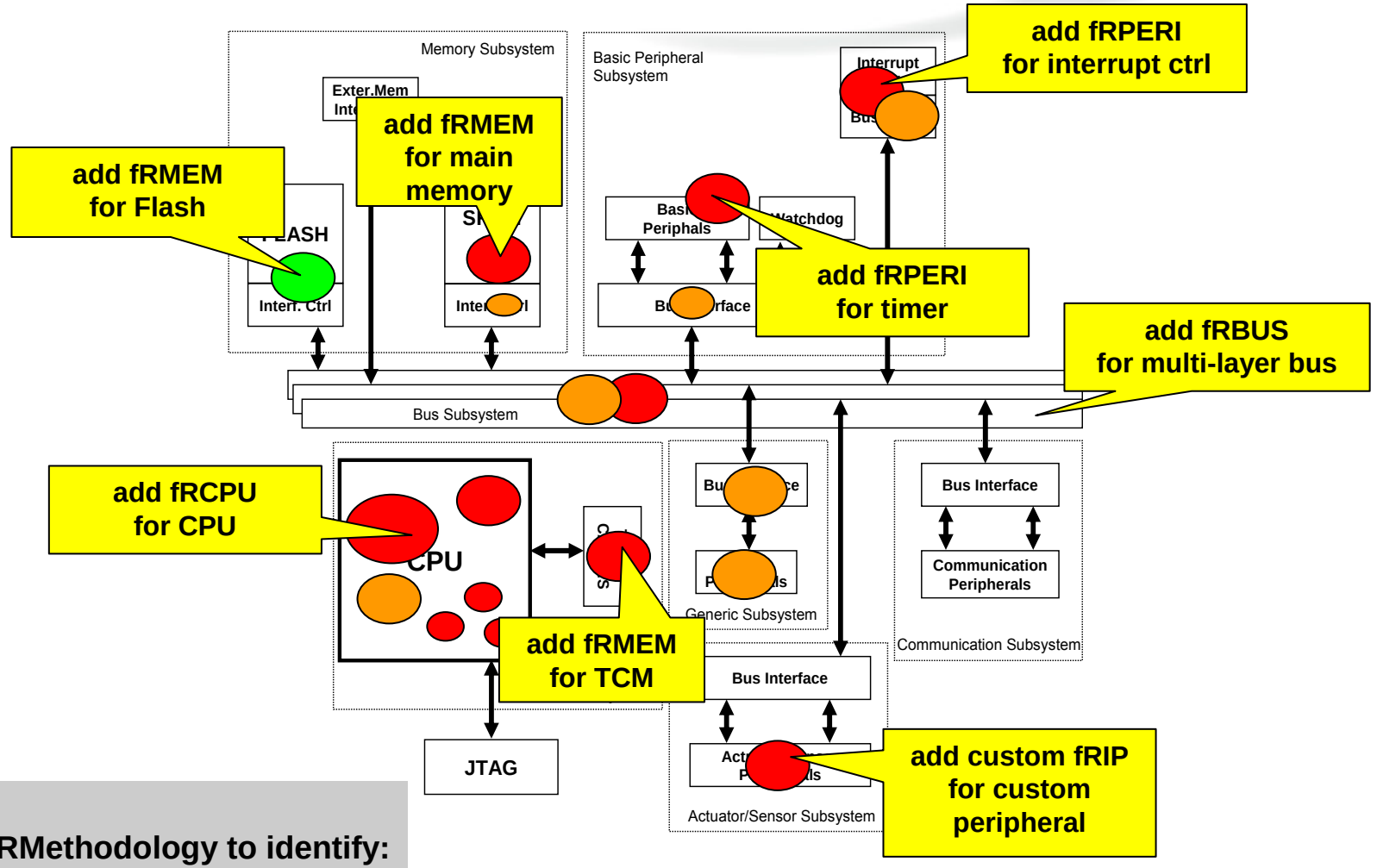
# OTC Dual Core block diagram




- OTC dual core's diagnostic cost is 1/5 if compared with LS dual core's diagnostic cost

- OTC dual core requires 85% less SW test if compared with LS dual core

# Comprehensive approach




**Step 1**
**applying fRMethodology to identify:**

- very critical areas
- critical areas
- attention areas

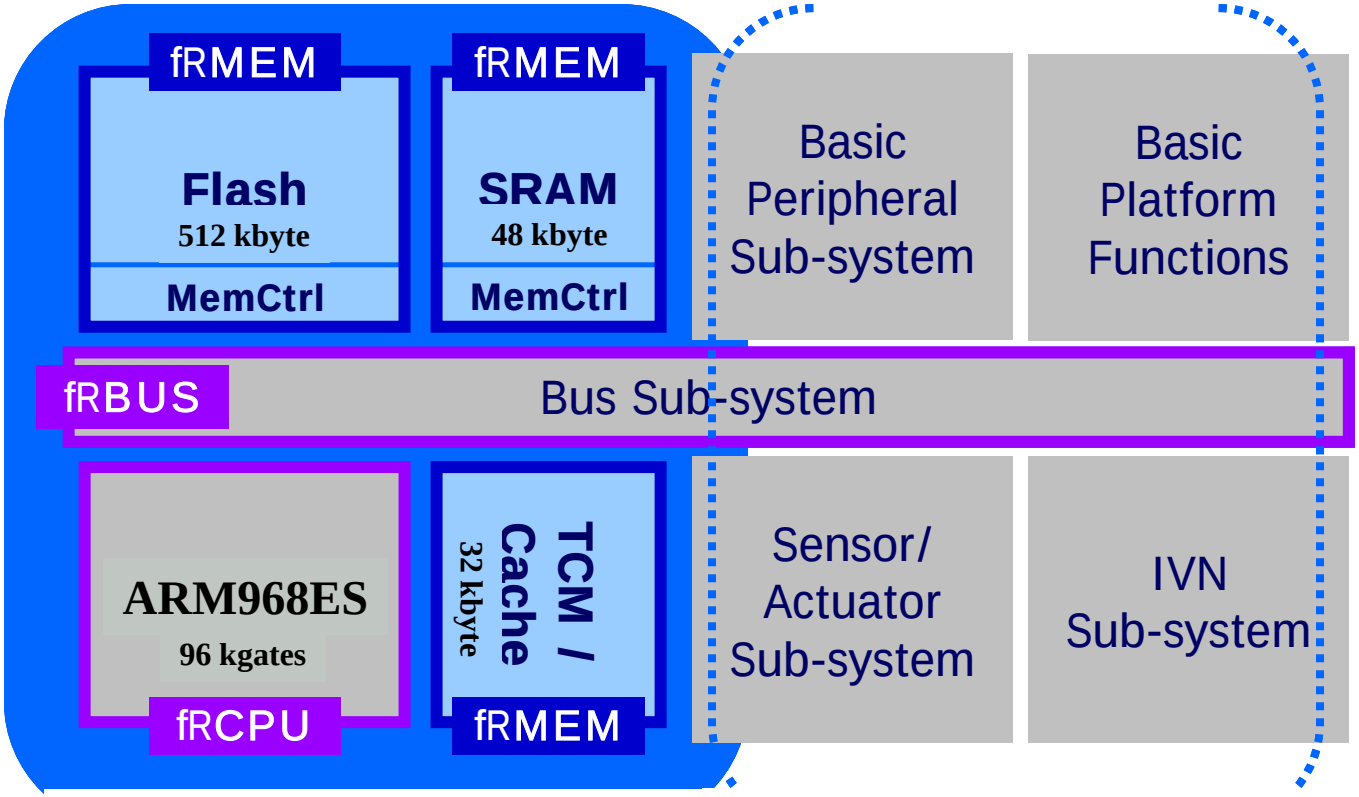
**Step 2**
**implementing ad-hoc diagnostics:**

- YOGITECH fRIP solutions
  ...or other solutions

YOGITECH faultRobust

# MCU safety concept example

## Platform protection approach




**Application indipendent**
Safety Integrity Level is achieved independently on the specific application

**Application dipendent**
Safety Integrity Level is achieved with the contribution of specific measures at ECU level (at HW and/or SW level)

**Concept Report obtained from TÜV SÜD by using fRMethodology**

*"...risk level SIL3 in compliance with IEC61508 is achievable by the planned safety concept..."*

YOGITECH faultRobust

# Key advantages areas

Comparison is given with reference to Dual Core LS

**MCU level**

- **Common-cause failures (CFF) intrinsically reduced**
- **Lower gate counts and easier scalability**
- **Lower power consumption**
- **Lower performance impact**
- **Smaller memory footprint**
- **No risk of undetected systematic HW faults**

**ECU level**

- **No need for external supervisor/watchdog**
- **Detailed diagnostic available and lower detection latency**
- **Simplified fail operational functionality**
- **Application SW easier to be certified (few CoU)**
- **Shorter MCU time-to-certification**
- **Reduced cost for MCU certification**
- **Fast product derivation (HW certification reusability)**

YOGITECH faultRobust

# Conclusions

- **Systematic methodology addressing IEC61508 requirements, easing safety certification.**
  - TÜV SÜD certified white box approach computing and validating metrics required for IEC61508
- **Achieving robustness reducing HW/SW costs**
  - using optimized HW fault supervisors
  - distributing the supervisors to the whole MCU
- **Guaranteeing compliance with IEC 61508**
  - developed under the supervision of TÜV SÜD
  - achieving SIL3
  - Solving $\beta_{IC}$ (common mode)
- **Being scalable and flexible**
  - implementing a portable and reusable architecture
- **Adding system-level benefits**
  - increasing availability by enhancing diagnostic capability
  - freeing CPU performance
  - allowing system makers to exploit new ideas
    - sophisticated safety concepts
    - next level of component integration



YOGITECH faultRobust

# YOGITECH

**YOGITECH SPA**
via Lenin 132/p
56017 San Martino Ulmiano
Pisa (Italia)