POLITECNICO
DI TORINO

Dipartimento di
Automatica e Informatica

PhD in Computer and Control Engineering

XXX cycle

Supervisor

prof. Massimo Violante

Multi-Core Systems for Mixed Criticality Applications

PhD Candidate: *Stefano Esposito*

1. Introduction

A mixed-criticality application is composed of safety- or mission-critical modules and non-critical modules.

In a strictly regulated industry such as civil avionics, when two applications share hardware, they should always be certified at the level of the most critical one. To avoid such an increase in development effort, the industries usually implement applications at different assurance levels on different computers, thus increasing the number of on-board equipment (OBE).

In my thesis, I propose solutions enabling use of multi-processor systems-on-chip (MPSoCs) for mixed-criticality applications.

2. Issues and Solutions

Spatial Isolation: non-critical applications should never be able to corrupt resources used by a critical application.

Solution: Use type-1 hypervisors to enforce resource partitioning.

Temporal Isolation: non-critical applications should never be able to increase the execution time of a critical application.

Solution: Use a statistical approach to profile performance metrics and then use performance counters (PCs) to detect deviations and react.

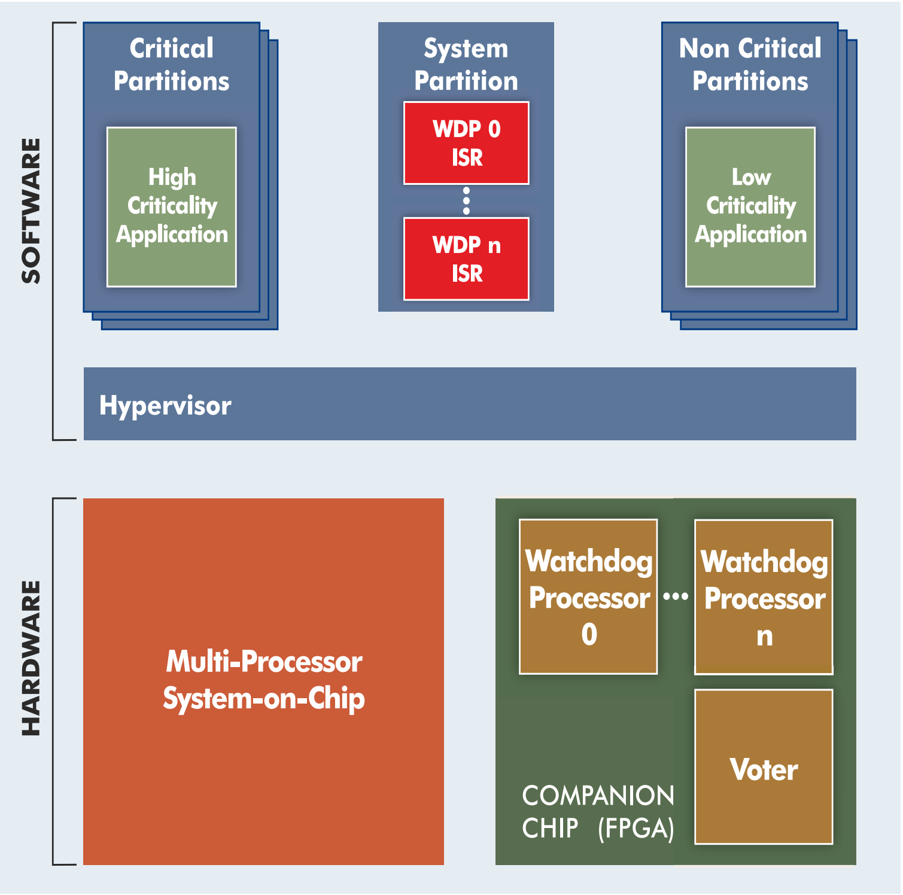

Figure 1. Block diagram of the proposed reference architecture.

The reference architecture depicted above, allows resource partitioning and integration of several applications on a single MPSoC, with the limit of the total number of applications being equal to the total number of processing cores available in the target MPSoC. A module integrated in the Hypevisor, allows monitoring of PCs and reaction to anomalies in an application-dependant way.

The solution for temporal isolation, has an offline phase, in which profiling data is analyzed to evaluate three thresholds: T_W or warning, T_D or detection, α or reaction. The on-line monitor reacts by switching to an hot stand-by spare if the measured metric is above T_D, and starts a counter when the metric is above $T_{W.}$ This counter is incremented each consecutive time the metric is above T_W and when the counter reaches α a graceful degradation is triggered.

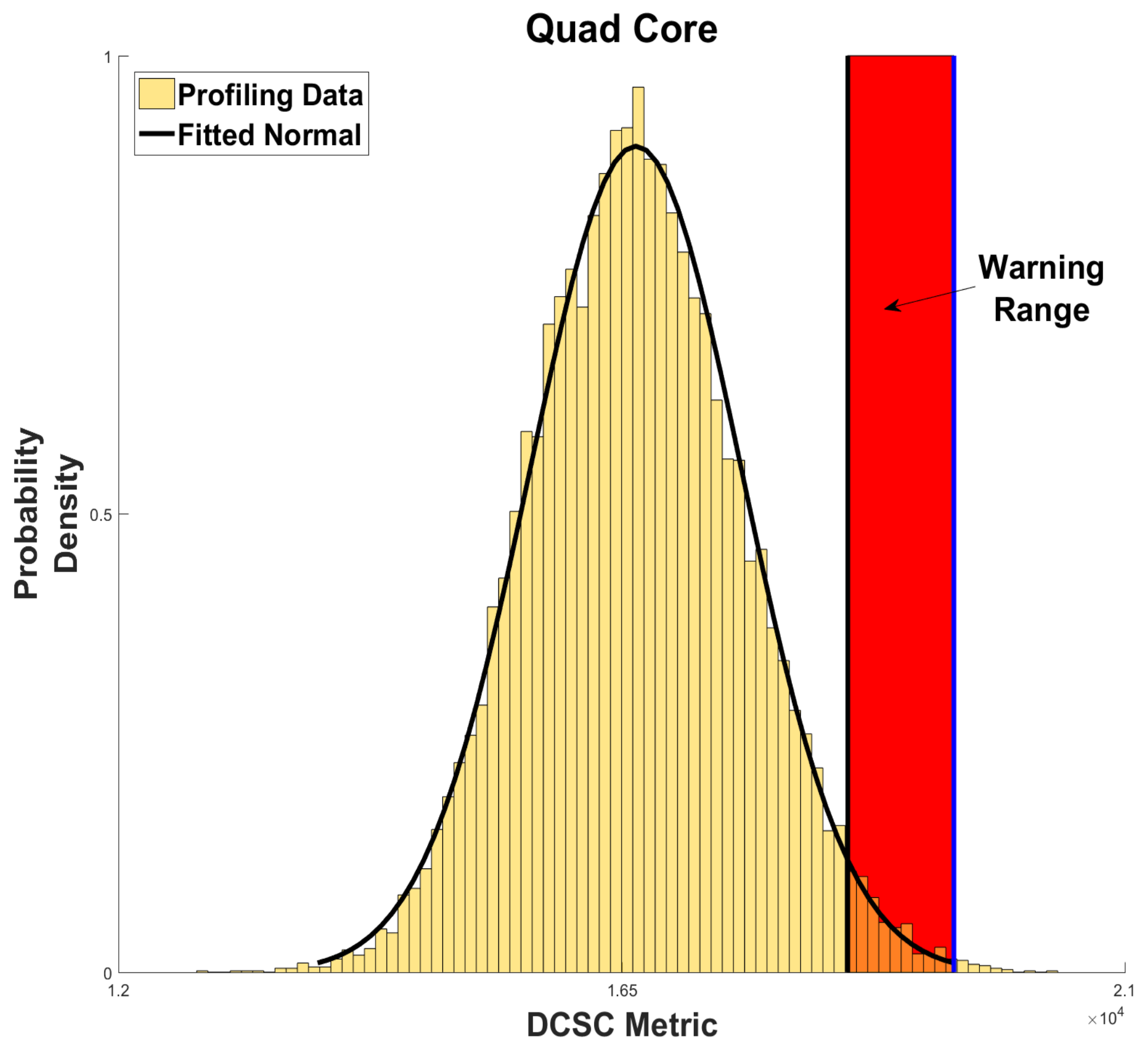

Figure 2. Example of temporal isolation solution application. The red region is delimited by T_W (left) and T_D (right). The profiling data is fitted to a Normal distribution in order to simplify threshold evaluation.

3. Validation

The proposed architecture was implemented in two demonstrators, the first on a Zynq (dual core with on-chip FPGA), the second on an Inventami board (quad core with FPGA on companion chip).

Spatial isolation was verified by means of HW and SW fault injection, results in table 1 and 2.

Tgt	NE	Det	F	Inj
RF	87.75%	12.25%	0	2000
Cfg	96.65%	3.35%	0	4000
Tot	93.68%	6.31%	0	6000

Table 1. HW F.I. results (NE: no effect, Det: detected, F: silent data corruption, Inj: injected faults. RF: register file, Cfg: MPSoC configuration bits)

NE	CA	NCA	F	Inj
88.80%	0	11.20%	0	10000

Table 2. SW F.I. results (NE: no effect, CA: error in the critical application, NCA: error in the non-critical application, F: silent data corruption, Inj: Injected faults). All faults were injected in a non-critical application.

Temporal isolation was verified by injecting bugs in non-critical applications to generate a potential performance overhead for the critical application.

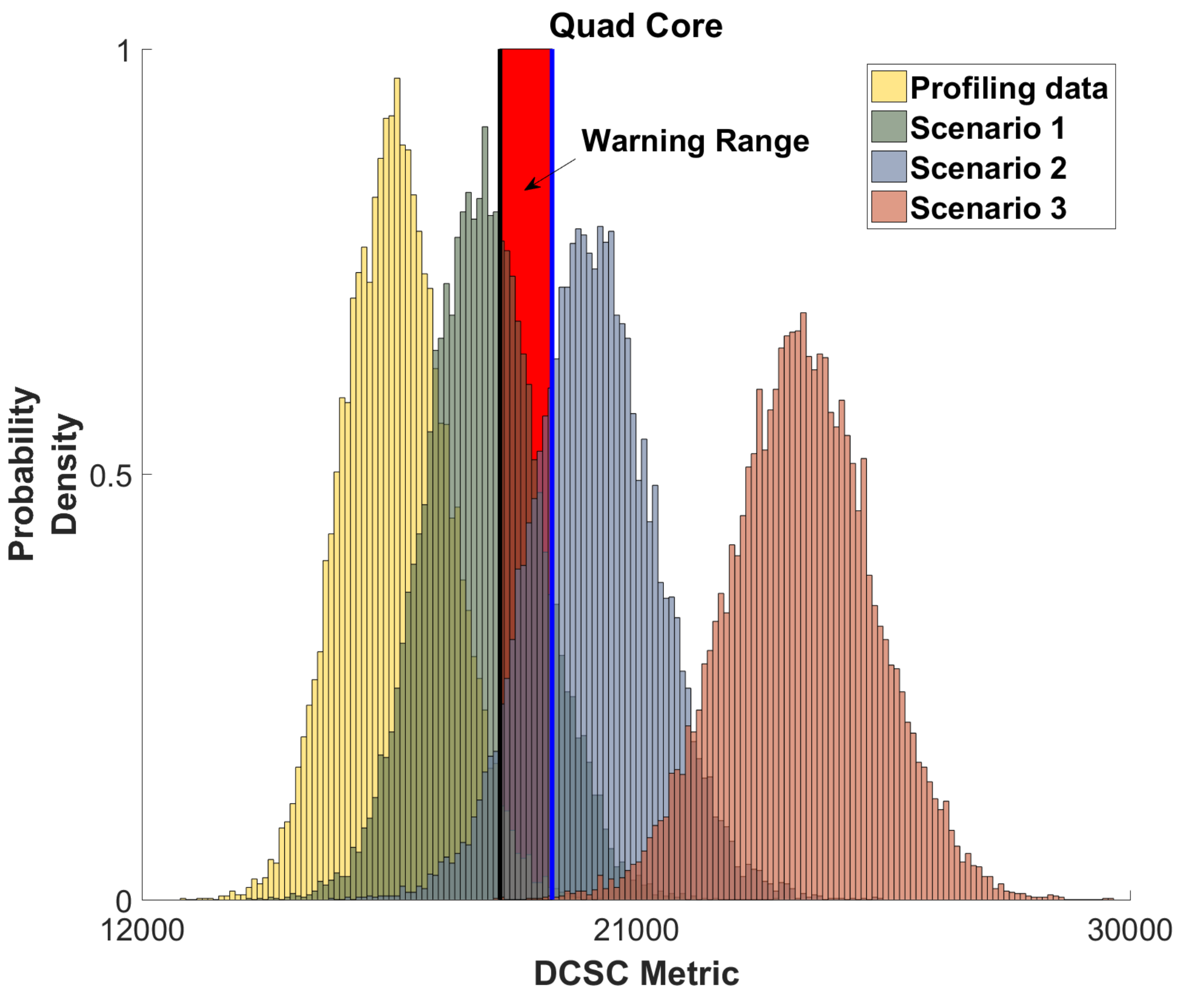

Figure 3. Measurements with no bugs, 1 bug, 2 bugs, 3 bugs (1 bug = 1 non-critical application abusing the shared bus).

4. References

1. Esposito, Stefano; Violante, Massimo; Sozzi, Marco; Terrone, Marco; Traversone, Massimo (2017) A Novel Method for Online Detection of Faults Affecting Execution-Time in Multicore-Based Systems. In: ACM TRANSACTIONS ON EMBEDDED COMPUTING SYSTEMS, vol. 16 n. 4, pp. 1-19. - ISSN 1539-9087
2. Esposito, Stefano; Violante, Massimo (2017) On the consolidation of mixed criticalities applications on multicore architectures. In: JOURNAL OF ELECTRONIC TESTING, pp. 1-12. - ISSN 0923-8174
3. Esposito, Stefano; Violante, Massimo (2017) System-level architecture for mixed criticality applications on MPSoC: A space application. In: 4th IEEE International Workshop on Metrology for AeroSpace, MetroAeroSpace 2017, Padova (IT), 2017. pp. 479-483
4. Esposito, Stefano; Violante, Massimo (2016) Commercial Off-the-Shelf Components in Space Applications. In: Semiconductor Devices in Harsh Conditions / Kirsten Weide-Zaage, Malgorzata Chrzanowska-Jeske. CRC PRESS, pp. 3-20. ISBN 9781498743808
5. Stefano Esposito; Massimo Violante (2016) Mitigating Soft Errors in Processors Cores Embedded in System-on Programmable-Chips. In: FPGAs and Parallel Architectures for Aerospace Applications. Springer, pp. 219-238. ISBN 9783319143521
6. Esposito, Stefano; Avramenko, Serhiy; Violante, Massimo (2016) On the consolidation of mixed criticalities applications on multicore architectures. In: 2016 17th Latin-American Test Symposium (LATS), Foz-do-Iguacu (Brasile), 6-8 Aprile 2016. pp. 57-62
7. Esposito, Stefano; Violante, Massimo; Sozzi, Marco; Terrone, Marco; Traversone, Massimo (2016) Online Time Interference Detection in Mixed-Criticality Applications on Multicore Architectures using Performance Counters. In: 22nd IEEE International Symposium on On-Line Testing and Robust System Design, Sant Feliu de Guixols (Spagna), 4-6 July 2016.
8. Avramenko, Serhiy; Esposito, Stefano; Violante, Massimo; Sozzi, Marco; Traversone, Massimo; Binello, Marco; Terrone, Marco (2015) An Hybrid Architecture for consolidating mixed criticality applications on multicore systems. In: IEEE International On-Line Testing Symposium. pp. 26-29