ScuDo
Scuola di Dottorato ~ Doctoral School
WHAT YOU ARE, TAKES YOU FAR

Doctoral Dissertation
Doctoral Program in Computer and Systems Engineering (XXXI cycle)

Network-on-Chip -based Multi-Processor System-on-Chip: Towards Mixed-Criticality System Certification

By

Serhiy Avramenko

******

Supervisor(s):
Prof. M. Violante

Doctoral Examination Committee:
Prof. A. Bosio, École Centrale de Lyon, France
Prof. M. Jenihhin, Tallinn University of Technology, Estonia
Prof. M. Ottavi, Università degli Studi di Roma Tor Vergata, Italy

Politecnico di Torino
2019

Abstract

The usage of single-core–based microprocessors is slowly disappearing, while multi-core–based devices becoming the only normally used nowadays. This is true also for the critical domains, like for instance avionics domain. However, the key point is that the multi-core microprocessors are de facto used as single-core devices as all-but-one executing cores are powered off. Meanwhile, the market offers more and more sophisticated solutions, proposing so called Multi-Processor System-on-Chip (MPSoC) device generation. These devices integrate tens or even hundreds of processing cores and peripherals on the same chip, connected through the network-on-chip (NoC) interconnection

The main obstacle for the usage of multi-core and MPSoC devices in the context of critical systems is the high certification effort required to ensure the proper level of dependability (and especially safety) for a system based on such kind of devices. Considering the commercial off-the-shelf (COTS) devices, these do not present any safety-dedicated features as the critical domains market size is relatively negligible. In fact, the high non-recurring engineering cost prevents the development of any COTS MPSoC specifically designed for the safety-critical applications.

This thesis presents a number of solutions to address the main dependability issues, preventing the usage of MPSoC-based systems in the context critical system. In particular the avionics domain is considered and the main focus is put upon the safety issues related to the usage of a shared interconnection, for what it concerns the temporal isolation between the software components. Although, the avionics domain is explicitly considered, the techniques presented are expected to be applicable for a generic safety-critical and even mission-critical domains, given that the required adaptation to the domain-specific peculiarities is done. As further contribution, this dissertation presents solutions to easier the dependability assessment of software components at executing core level.

Considering the executing core level, a proper fault tolerance against radiation induced soft errors was and remains crucial for the space applications. However, as the geometries keep shrinking and power saving techniques are becoming more and more aggressive, the issue of soft errors is no longer a space domain's prerogative. This thesis proposes an approach to rank a set of candidate software modules according to their intrinsic robustness to the soft errors. The main advantage of the proposed approach is that it's almost agnostic of the actual architectural details of the executing platform as it is based on software-level fault injections. The information collected during the proposed high-level analysis can also be used optimize the hardening phase.

As main contributions of this thesis, I address the main safety issues concerning the shared (NoC) interconnection of an MPSoC, both considering COTS and custom components. In particular, I focus on the temporal isolation of software components running on the same MPSoC. A typical safety-critical scenario is considered, where the software components have different levels of criticality (or severity of failure), i.e., mixed criticality scenario. As the main contribution, I propose a partitioning techniques to enable the usage of (NoC-based) MPSoC for the mixed criticality systems, both considering COTS and custom devices. For what it concerns the usage of COTS devices, where the main effort was spent, the proposed technique exploits the deterministic routing algorithm of the NoC. The proposed solution is suitable for a ample range of MPSoC devices as its requirements consider a fairly common MPSoC characteristics. The partitioning technique is intended to have a purely software implementation, as a module of a real-time operating system, which targets both the certification potential and reusability aspects. For what it concerns the custom NoC architectures, a set of simple solutions has been derived with the specific purpose of high certification potential.