PhD in Computer and Control Engineering

Research Title: Hardware-Based Neuromorphic Resilience to Faults and Attacks

Funded by	Ateneo Internazionalizzazione su fondi della Fondazione Compagnia di San Paolo

Supervisor	Stefano Di Carlo (Politecnico di Torino), stefano.dicarlo@polito.it Ramon Canal (UPC) rcanal@ac.upc.edu

Contact	https://www.testgroup.polito.it

Context of the research activity	This PhD project aims at the implementation of hardware coprocessors based on neuromorphic architectures for the identification of anomalies in microprocessor systems due to both failures (reliability) and intentional malicious interventions (security). The reliability and security of digital systems has long been analyzed in the context of separate disciplines and communities. Currently, with the pervasive use of these technologies, especially in the IoT sector, it is increasingly clear that the two aspects must be considered simultaneously with common and synergistic strategies. Specifically, while many of the applications of neural networks and AI in this sector are developed at the software level, this Ph.D. project is interested in investigating the integration of these features at the hardware level. Working at the hardware level allows to obtain more computing power, optimize computation, and provide the neural network with direct access to low-level information on the state of the system not normally accessible at the software levels. Results in this area could lead to the development of computing systems with resilience to failures and attacks that are currently unattainable. This research proposal is a collaboration between Politecnico di Torino and the Universitat Politècnica de Catalunya. Candidates are expected to spend half of their Ph.D. in Torino and the remaining time in Barcelona.

Objectives	This research proposal envisions three main objectives: 1) "Run-time monitoring infrastructure": through analysis and simulations on use cases in various application areas, the goal is to understand what types of monitoring systems need to be integrated at the circuit, architecture, and system level, and where to insert them, to provide an adequate level of observability to monitor the resilience of the system? How are the existing infrastructures for testing, debug, profiling of performances (performance monitoring counters) already able to provide information on the resilience of the system? In a system made up of heterogeneous computational blocks (microprocessors, accelerators for AI, crypto cores), are there already intrinsically resilient elements? 2) “resilience infrastructure”: this objective represents the heart of the PhD proposal. The aim is the pursuit resilience, through a series of learning-based approaches that analyze the behavior of systems based on the data provided by the run-time monitoring infrastructure and are able to identify anomalies and recovery strategies in such a way that systems can continue to provide the required functionality despite malfunctioning components, environmental disturbances, and malicious behaviors. 3) “Prototyping and emulation”: this objective aims to develop the tools necessary for the evaluation, prototyping and experimentation of the concepts developed during the doctorate. To achieve this, a fully automated flow is required, capable of collecting data, training, and testing learning models, and validating their predictions. The main challenge in this case is to be able to emulate the occurrence of selected classes of hardware / software anomalies and to observe the behavior of the system. The AI-based resilience system will be prototyped. This will require the development of specific coprocessors capable of accelerating the onerous activities of learning and detecting anomalies and the integration of this new hardware into the functioning of the operating system. To this end, the use

	of FPGA-based reconfigurable systems will be heavily used. Specifically, the goal is to integrate the developed concepts within the RISC-V microprocessor architecture. RISC-V is an open microprocessor architecture selected by the European Community as the reference architecture for the "European processor Initiative" (EPI) which aims to develop a European microprocessor. It is therefore in the European context a point of reference for those who deal with hardware architectures supported by the European Community in numerous calls of its research programs

Skills and competencies for the development of the activity	Hardware design and FPGA prototyping with emphasis on accelerators for neural networks, programming skills in Python and C.