Politecnico di Torino

Finanziato dall'Unione europea NextGenerationEU

COMPUTER AND CONTROL ENGINEERING

Autonomous systems' reliability and security

Funded By	Ministero dell'Università e della Ricerca - MUR [P.iva/CF:96446770586]
Supervisor	SANCHEZ SANCHEZ EDGAR ERNESTO - ernesto.sanchez@polito.it
Contact	
Context of the research activity	Autonomous Systems (A. Sys.) have been a subject of great interest during the last years. In fact, autonomous devices have been investigated and proposed by very different actors: from the automotive industry to hospital UV disinfection robots; from automatic stacking systems to unmanned aerial vehicles. In order to support the software complexity, A.Sys. may include some microprocessor cores, different memory cores, and hardware accelerators in charge of performing the Deep Artificial Neural Network applications. An emerging problem is the verification, testing, reliability, and security of Autonomous Systems, and in particular, regarding the computational elements involved in the artificial intelligence computations. In general, these very complex systems are still lacking a holistic analysis and comprehension related to reliability and security. It is for example unclear, how to functionally verify the behavior of a DNN, or what may happen when the autonomous system is affected by a fault from both points of view: reliability and security. During this project, the Ph.D. candidate will study from the hardware and software perspective, how to improve the reliability and security of autonomous systems based on AI solutions.
Objectives	The Ph.D. proposal aims at studying the current design, verification and testing methodologies that try to guarantee a correct implementation of AI based systems in A.Sys. with particular interest on the available solutions to increase the systems reliability and security. During the initial phase, a set of benchmarks that will provide the suitable cases of study for the following research steps are defined. Two main types of AI systems in A.Sys. will be analyzed: the first one is based on hardware accelerators that exploit for example FPGA implementations; and the second one implements the A.I. algorithm supported by components-off-the-shelfs (COTS) such as systems that embeds high performance processor cores. From the reliability point of view, there is a lack of metrics able to correctly assess how reliable is an AI-based system, in fact, a study and proposal of appropriate metrics is also required at this point. As a matter of facts, it will be necessary to gather the most suitable or define a set of fault models oriented to better identify the device vulnerabilities during the development time. A first attempt to consider

	the system security of AI algorithms running on embedded systems is also required. Regarding security, the lack of metrics and experimental demonstration make important to fulfill this gap by providing some indications about the main security criticalities and how to mitigate them in an A.Sys. based on embedded systems. Finally, mitigation strategies based on self-test, error-recovery and earlier detection mechanisms will be developed for the autonomous systems studied. The final goal is to equip the AI hardware with self-test mechanisms to detect hardware errors, and possible thread intrusions thanks to the implementation of fault-tolerance and secure oriented mechanisms for increasing the reliability and security of the AI algorithm while maintaining the system accuracy.

Skills and competencies for the development of the activity	Applicants should have a good knowledge in the area of Artificial Intelligence, and in particular in topics related to Artificial Neural Networks. In addition, knowledge in processor architecture, processor-based systems, as well as in testing, and programming, is also welcomed, although not strictly required.