COMPUTER AND CONTROL ENGINEERING

MUR DM 118 - Reliability and security of AI-based systems

Funded By	MINISTERO DELL'UNIVERSITA' E DELLA RICERCA [P.iva/CF:97429780584] Politecnico di TORINO [P.iva/CF:00518460019]
Supervisor	SANCHEZ SANCHEZ EDGAR ERNESTO - ernesto.sanchez@polito.it
Contact	
Context of the research activity	Artificial Intelligence (AI) based applications, and in particular unmanned vehicles (UVs) have been a subject of great interest during the last years. In fact, its complexity due to the hardware and software interaction is growing up continuously. In this context, an emerging set of problems regard the verification, testing, reliability, and security of such applications, and in particular, considering the computational elements involved in the artificial intelligence computations. During this project, the Ph.D. candidate will study from the hardware and software perspective how to improve the reliability and security aspects related to unmanned vehicles based on AI solutions. Progetto finanziato nell'ambito del PNRR - DM 118/2023 - CUP E14D23001780006
	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 UVs, 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. Different types of AI-based systems in UVs will be analyzed: the first one implements the A.I. algorithm supported by Open-Source devices or components-off-the-shelfs (COTS) such as systems that embeds high performance processor cores. On the other hand, the system application can be based on hardware accelerators that exploit, for example FPGA implementations. From the reliability point of view, there is a lack of metrics able to correctly assess how reliable an AI-based system is, in fact, a study and proposal of appropriate metrics is also required at this point. As a matter of fact, it will be necessary to gather the most suitable metrics or define a set of fault models oriented to better identify the device vulnerabilities during the development time.

Objectives	An additional effort to consider the system security of AI algorithms running on embedded systems is also required. Regarding security, the lack of metrics and experimental demonstrators make important to fulfill this gap by providing some indications about the main security criticalities and how to mitigate them in UVs 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. Proposed work plan The work plan is divided in three years as follows: • First year: 1. Study and identification of the most important works on design and verification of AI solutions used in unmanned vehicles. 2. Study and identification of the most relevant works related to security issues for AI solutions used in unmanned vehicles. 3. Design and implementation of the cases of study resorting to hardware accelerators, Open-Source devices, and COTS based on high performance processor cores. • Second year: 4. Fault model definition and experimentation, mainly resorting to the implemented cases of study. 5. Metrics definition for the reliability assessment of UVs. 6. Metrics definition for the security assessment of UVs. • Third year: 7. Mitigation strategies proposal. In a few words: the first three steps will leave the Ph.D. candidate with the appropriate background to perform the following activities. Steps 4 to 7 are particularly interesting from the research point of view, allowing the student to write papers and present them in the international conferences related to the different research areas faced during the Ph.D. During these research phases, the student will have the possibility to cooperate with international companies such as NVIDIA and STMicroelectronics, and foreign research groups in Lyon, Montpellier and other universities. Target publications: The main conferences where the Ph.D. student will possibly publish her/his works are: DATE: IEEE - Design, Automation & Test in Europe Conference ETS: IEEE European Test Symposium ITC: IEEE International Test Conference VTS: IEEE VLSI Test Symposium IOLTS: IEEE International Symposium on On-Line Testing and Robust System Design MTV: IEEE International workshop on Microprocessor/SoC Test, Security & Verification Additionally, the project research may be published in relevant international journals, such as: TCAD, TVLSI, ToC, IEEE Transactions on Vehicular Technology, IEEE Transactions on Reliability.
Skills and	Applicants should have good knowledge in the area of digital systems

competencies for the development of the activity	design and processor architectures. Good knowledge in security aspects of embedded systems. Good knowledge in programming languages such as Python, C and C++ is also required.