ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

DIPARTIMENTO
DI INGEGNERIA
DELL'ENERGIA ELETTRICA
E DELL'INFORMAZIONE
"GUGLIELMO MARCONI"

Titolo: *Hardware-in-the-Loop framework for development of Secure AI applications on edge Devices*

1. TOPIC

Edge devices for industrial applications such as plant control and monitoring are part of critical infrastructures but at the same time they are connected to computer networks to support remote access, updates and reconfiguration. The software running on these systems must be reliable and secure. For this reason, security is a key design criteria for both SW and HW. New approaches are looking at usage of AI algorithms to detect intrusions identifiable as control-flow diversions. These techniques are often based on processing traces of execution online. Techniques for developing HW/SW support require the availability of a Hardware-in-the-loop infrastructure.

2. RESEARCH ACTIVITY (Attività di ricerca)

The research activity will concentrate on the development of a HiL framework for designing HW/SW strategies to extract the data needed to analyze execution flow and detect intrusions. The research will focus on ROP and IDS attacks from one side and from the other on the development of HiL framework to detect those attacks on RISC-V based SoCs based on deep learning algorithms on edge.

3. ACTIVITY PLAN

The researcher will acquire or consolidate, in parallel with the research activity, the knowledge of: i) security issues and attack models of edge devices; ii) Hardware-in-the-loop based on FPGA prototypes; iii) techniques to profile algorithms and methodologies based on deep learning algorithms for intrusion detection implemented on custom neuromorphic accelerators. The research activity will be done in the context the EdgeAI project and aligned with PNRR objectives.