ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

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

Titolo: *Development of SW/HW techniques for AI-enhanced Control-Flow-Integrity on Edge*

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. This requires a very fast processing of these traces using custom accelerators.

2. RESEARCH ACTIVITY (Attività di ricerca)

The research activity will concentrate on the development of AI methodologies for security analysis on edge and the development of custom neuromorphic accelerators. The research will focus on ROP and IDS attacks from one side and from the other on the development of deep learning approaches to detect those attacks.

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) Control flow integrity techniques for risc-v processors; iii) deep learning algorithm implementation on custom neuromorphic accelerators. The research activity will be done in the context the EdgeAI project and aligned with PNRR objectives.