Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Titolo: Security Risks and Solutions for Cyber-Physical Systems

(Finanziamento PNRR PE7-SERICS)

INTRODUCTION

A Cyber-Physical Systems (CPS) is embedded systems tightly interacting with the surrounding physical environment though sensors and actuators. CPS are pervasive in many applications, ranging from plant control in automotive, avionics, robotics, manufacturing and energy production systems, infrastructural and environmental monitoring. CPS have special characteristics that impose many design requirements: i) Because of the interaction with physical world, they must be able to react in real-time to physical stimuli; ii) Because of their pervasiveness, they are often embedded in physical equipment, thus they have to have a small footprint and low-energy consumption; ii) Due to the direct or indirect interaction with humans and critical infrastructures, CPS must be reliable and secure. At the same time, these security and reliability must be implemented with low or negligible impact on real-time guarantees and energy consumption. In this project, the research activity of the candidate student will focus on the latter aspect, taking into account the trade-off with the first two.

RESEARCH ACTIVITY

The research activity will be performed within the *“SEcurity and RIghts in the CyberSpace (SERICS)”* Extended Partnership PE7. In particular the research will study existing approaches to protect data and control flow integrity, analyze their robustness with respect also to malicious attacks and possible faults and aging conditions affecting the hardware implementing them, and propose new approaches for data and control flow security, accounting for low-power and real-time constraints.

ACTIVITY PLAN

The researcher will acquire or consolidate, in parallel with the research activity, the knowledge of CAD tools for electronic circuits and systems design and implementation (HSpice, Synopsys, etc) as well as cross-compiling toolchain for microcontroller and low-power embedded systems

The research will encompass the following phases:

1) Review of existing approaches to protect data and control flow integrity for different kinds of applications (wireless sensor networks, firewalls, economical transactions, AI systems, etc)
2) Selection of some representative approaches and evaluation of their robustness wrt to malicious attacks and faults/aging possibly affecting the adopted hardware and system software in the field
3) Development of innovative approaches, featuring higher robustness than those considered at point 2) above and/or lower costs