Research theme title:
Control and monitoring of secure and distributed Cyber-Physical Systems through the Digital Twin paradigm.

Description:
The Digital Twin (DT) paradigm is now widely used in various application domains (including industry, healthcare, smart city, agriculture, and so) to identify a tool, or a set of heterogeneous tools, able to model complex systems and monitor their status. The DT paradigm can be effectively used to model physical objects or, more in general, cyber-physical systems. Through the DT, it is possible to monitor the temporal evolution of real objects/systems, as well as predict this evolution by simulating the presence of specific inputs. Therefore, through the DT paradigm, it would be possible to formulate new methodologies and techniques for the control and monitoring of (complex and secure) Cyber-Physical Systems, even on a large scale.
Based on these considerations, the main goal of such a research project proposal is to conceive and investigate advanced and innovative methodologies for the control and monitoring the security level of distributed Cyber-Physical Systems (such as telecommunication infrastructures, industrial plant, etc.) based on the massive usage of DT paradigm. More specifically, this challenging objective can be achieved through the following main steps of the work:
Assuming that the distributed Cyber-Physical Systems may have heterogeneous devices and segments (e.g. sensing devices, robots, network segments, that are potentially used by different tenants), during the first step of the work, the PhD student will explore protocols and procedures through which collecting (in real-time, flexible and hierarchical manner) all the parameters that will feed the corresponding DT, useful to classify its security level. Subsequently, the work will consist in studying/formulating new methodologies and approaches able to operate on interconnected DTs, through which the operator (or more generally the infrastructure provider) will have the possibility to emulate the evolution of the network caused by specific modifications (e.g. introduction of a new agent, a list of events, the creation of a new slice, allocation of a new MEC server, admission of a new application, etc.), estimate the resulting network conditions expressed in terms of Key Performance Indexes (e.g., bandwidth, latency), Key Value Indicators (e.g., energy consumptions), and security (e.g., attack surface, vulnerabilities).

References:

- M. Sanz Rodrigo, D. Rivera, J. I. Moreno, M. Àlvarez-Campana and D. R. López, "Digital Twins for 5G Networks: A Modeling and Deployment Methodology," in *IEEE Access*, vol. 11, pp. 38112-38126, 2023, doi: 10.1109/ACCESS.2023.3267548.
- W. Xian, K. Yu, F. Han, L. Fang, D. He and Q. -L. Han, "Advanced Manufacturing in Industry 5.0: A Survey of Key Enabling Technologies and Future Trends," in *IEEE Transactions on Industrial Informatics*, doi: 10.1109/TII.2023.3274224.
- C. Alcaraz and J. Lopez, "Digital Twin: A Comprehensive Survey of Security Threats," in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1475-1503, thirdquarter 2022, doi: 10.1109/COMST.2022.3171465.

Contacts:

Prof. Giuseppe Piro, giuseppe.piro@poliba.it

Hosting University
Polytechnic of Bari, Italy

Type of scholarship:
DM 118/2023 – Project on PNRR (Italy's Recovery and Resilience Plan)