BORSA N. 3

DAUSY

Borsa di Ateneo
Tematica: *"Model based security and monitoring system for resilient industrial control systems"*

Research theme title:

Model based security and monitoring system for resilient industrial control systems

Contacts:

Prof. Federica Pascucci

e-mail: federica.pascucci@uniroma3.it

Curriculum of DAUSY:

C3 AS for Monitoring and Security

Hosting University/Research Centre

Università degli Studi Roma Tre

Department:

Dipartimento di Ingegneria

Via Vito Volterra, 62 – 00144 Roma – Italy

https://ingegneria.uniroma3.it

Prospective Supervisors:

Prof. Federica Pascucci (federica.pascucci@uniroma3.it)

Prof. Stefano Panzieri (stefano.panzieri@uniroma3.it)

Description:

Over the past decade, industrial control systems have experienced a massive integration with information technologies. Industrial networks have undergone numerous technical transformations to protect operational and production processes, leading today to a new industrial revolution. Nowadays, indeed, industrial control devices are one of the major targets for hackers due to their exposure to threats: the principle of "air gaps" (disconnecting the industrial control network from the operational networks) is not anymore feasible in a connected world. Despite the importance of protecting such systems, cybersecurity related issues have not been given due consideration.

The goal of this project is to improve the security and the resilience of cyber physical systems by exploiting early detection and risk analysis. The research project will fall in the cross-cutting edges among control engineering, cybersecurity, and machine learning. The application area will be focused on digital control systems operated over communication networks prone to cyber-attacks.

The research will focus on developing novel system analysis and design methodologies that jointly consider both the risk (i.e., impact and cascading effects) and detectability of attacks under uncertainties. It will exploit model-based approaches related to fault diagnosis and data-driven solutions such as machine learning. The developed methods shall support the design of anomaly detection and control algorithms for improving security and resilience. These algorithms will be validated by simulation and on experimental testbeds.

Specific Information:

Applicants must hold a master's degree, preferably in Engineering, with a good background in relevant areas of interest (i.e., Cybersecurity, Control Engineering, Computer Systems and Networks, Automation, and Machine Learning). Solid mathematical and coding skills are encouraged. Proficiency in both spoken and written English is required. The candidate should have the ability to work independently and to collaborate with teams. A positive attitude to problem solving for complex systems is strongly required.

References:

[1]. Sandberg, Henrik and Johansson, Karl H. and Gupta, Vijay, Secure Networked Control Systems (May 2022). Annual Review of Control, Robotics, and Autonomous Systems, Vol. 5, pp. 445-464, 2022.
[2]. R. Ferrari, A. M. H. Teixeira. "A Switching Multiplicative Watermarking Scheme for Detection of Stealthy Cyber-Attacks". IEEE Transactions on Automatic Control, 2020.

[3]. R. Taormina, S. Galelli, H. C. Douglas, N. O. Tippenhauer, E. Salomons, A. Ostfeld, A toolbox for assessing the impacts of cyber-physical attacks on water distribution systems. Environmental Modelling & Software, 2019.
[4]. M. H. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson. "A Secure Control Framework for Resource-Limited Adversaries". Automatica, vol. 51, pp. 135-148, Jan. 2015.
[5]. R. M. G. Ferrari, T. Parisini and M. M. Polycarpou, "Distributed Fault Diagnosis With Overlapping Decompositions: An Adaptive Approximation Approach," in IEEE Transactions on Automatic Control, vol. 54, no. 4, pp. 794-799, April 2009.

Type of scholarship:

Project funded by the Hosting Institution

Study and research period outside the Hosting Institution:

- Period length: up to 6 months;
- University of Coimbra – Centre for Informatics and Systems
- Polo II, Pinhal de Marrocos, 3030-290 Coimbra, Portugal
- https://www.uc.pt – https://www.cisuc.uc.pt/