DAUSY

Research theme title:

Security for Industrial Internet of Things

Contacts:

Prof. Federica Pascucci

e-mail: federica.pascucci@uniroma3.it

Dr. Graziana Cavone

e-mail: graziana.cavone@uniroma3.it

Curriculum of DAUSY:

C3 AS for Monitoring and Security

Hosting University/Research Centre

University Roma Tre, Rome, Italy

Department of Civil, Computer Science, and Aeronautical Technologies Engineering

Via della Vasca Navale 79/81, Rome – Italy

https://ingegneriacivileinformaticatecnologieaeronautiche.uniroma3.it/

Supervisors:

Prof. Federica Pascucci
(https://www.uniroma3.it/persone/R0x2Y3hpRUdiZWM4VzI4OGZWQzZMOURSaGp3UEh5c09xbjViN3dwUHJRbz0=/)

Dr. Graziana Cavone
(https://www.uniroma3.it/en/persone/R0JTU1pTOHZzY0lwTkhWaDBoUXp2UVQzL1A3Y0Ivdy9JZjlQdWtuaG9CUT0=/)

Description:

Over the past decade, the paradigm of the Internet of Things has made its way in the Industrial sector, leading to the broader concept of Industrial Internet of Things (IIoT) [1]. In fact, in the industrial world we are assisting to the advent of the digital and smart manufacturing, which aim at integrating Operational Technology (OT) with Information Technology (IT) domains. Basically, the IIoT, which is one of the pillars of digital manufacturing, regards the connection of all the industrial assets, including machines and control systems, with the information systems and the business processes. This can positively impact the productivity of the industrial systems affecting all the industrial value chain. Nevertheless, the IIoT connectivity can lead to security issues in the industrial environment, and in particular, in the Industrial Control Systems (ICS) framework. In fact, in 2022 ICS have experienced a large increase in ransomware attacks by an increasing number of ransomware groups that target industries. This aspect becomes further critical when considering the human-centric approach of the industry of the future, where the human well-being is prioritized, and the operators strictly collaborate or cooperate with digital technologies. In this context, the principle of the "air gap", i.e., the disconnection of the industrial control network from external networks, is no longer viable to guarantee security. Thus, it becomes urgent the definition and implementation of novel methodologies.

The main research question to be addressed is: "Can we improve the safety of the IIoT and ICS in the context of human-centric industry?"

The goal of the PhD project is to improve the security and resilience of IIoT and in particular of ICS in the context of a human-centric industry, by leveraging early threat detection and risk analysis. The PhD project cuts across the disciplines of control engineering, information security and machine learning [2 - 4]. The application area will be focused on distributed industrial control systems composed of remote sensors and actuators (according to the IIoT paradigm) [5].

The research will focus on the development of new system design and analysis methodologies that jointly consider both the risk (i.e., impact and cascading effects) and the detectability of attacks under conditions of uncertainty. It will leverage model-based approaches to fault diagnosis and data-driven solutions such as machine learning [6]. The developed methods will support the design of anomaly detection and control algorithms to improve security and resilience. These algorithms will be validated by simulation and on experimental testbeds (prototypes) [7].

Specific Information:

Applicants must hold a master’s degree, preferably in Engineering, with a good background in relevant areas of interest (e.g., cyber-physical systems, human-centered design, industrial control systems, and distributed control). Solid mathematical and coding skills are encouraged. Proficiency in both spoken and written English is required. The candidate should be highly motivated and interested in undertaking innovative and challenging research activities involving both theoretical analysis and experimental validation.

References:

[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag and M. Gidlund, Industrial Internet of Things: Challenges, Opportunities, and Directions, min IEEE Transactions on Industrial Informatics, vol. 14, no. 11, pp. 4724-4734, Nov. 2018.

[2]. Bernieri, G., Conti, M., & Turrin, F. (2019, November). Kingfisher: An industrial security framework based on variational autoencoders. In Proceedings of the 1st Workshop on Machine Learning on Edge in Sensor Systems (pp. 7-12).

[3]. Bernieri, G., Conti, M., & Turrin, F. (2019, July). Evaluation of machine learning algorithms for anomaly detection in industrial networks. In 2019 IEEE International Symposium on Measurements & Networking (M&N) (pp. 1-6). IEEE.

[4] Baldoni, S., Battisti, F., Carli, M., & Pascucci, F. (2021). On the Use of Fibonacci Sequences for Detecting Injection Attacks in Cyber Physical Systems. IEEE Access, 9, 41787-41798.

[5]. Ding, D., Han, Q. L., Wang, Z., & Ge, X. (2019). A survey on model-based distributed control and filtering for industrial cyber-physical systems. IEEE Transactions on Industrial Informatics, 15(5), 2483-2499.

[6] Albaba, B. M., & Yildiz, Y. (2019). Modeling cyber-physical human systems via an interplay between reinforcement learning and game theory. Annual Reviews in Control, 48, 1-21.

[7] Conti, M., Donadel, D., & Turrin, F. (2021). A survey on industrial control system testbeds and datasets for security research. IEEE Communications Surveys & Tutorials, 23(4), 2248-2294.

Type of scholarship:

Project funded by PNRR DM118.

Study and research period outside the Hosting Institution:

Possible study and research period abroad:

- period length: 6 months;
- Hosting institution:
  - To be defined.