19th IEEE International Conference on Factory Communication Systems (WFCS)

26-28 April 2023, Pavia, Italy

SS 01 - Advances in Security and Safety of Industrial Networked Infrastructures

Principal Organizer: Lucia Seno (lucia.seno@ieiit.cnr.it)
Affiliation: CNR-IEIIT, Padova, Italy

Organizer 1: Hans-Peter Bernhard (hans-peter.bernhard@silicon-austria.com)
Affiliation: Silicon Austria Labs & Johannes Kepler University, Linz, Austria

Organizer 2: Marco Ehrlich (marco.ehrlich@th-owl.de)
Affiliation: Institute Industrial IT, Lemgo, Germany

Organizer 3: Wolfgang Kastner (k@auto.tuwien.ac.at)
Affiliation: TU-Wien, Vienna, Austria

The increasing connectivity of industrial networked infrastructures, the exploitation, in this domain, of wired/wireless technologies and hardware/software components/paradigms typical of the IT domain, as well as the drive towards the seamless integration of OT and IT networks, on one side have improved automation, adaptability, and efficiency of industrial systems (in a broad sense), on the other have extended their attack surface, making them critically exposed to cyber-menaces. Cyber-attacks to industrial systems are rising as more sophisticated attack methodologies are developed, e.g., leveraging artificial intelligence and complex attack vectors, threatening, beside company assets, also equipment and personal safety. Advanced protection, detection, and mitigation/response measures, tailored on the specifics of industrial systems (latency/reliability requirements, no downtimes, heterogeneity of hardware/software components, etc.), also leveraging novel emerging technological/architectural trends in the industrial communication domain, are mandatorily needed. Security and safety in this domain are complementary views of the same issue, given that a lack of security may translate in a lack of safety and typical measures in one context may impact and/or increase opportunities for the other. This Special Session aims at bringing together researchers and practitioners from Academia and Industry to share and debate recent advances and promising directions in security and safety of industrial networked infrastructures.

The SS focuses on (but is not limited to):

- Security and safety of industrial networks, IIoT, and wireless/mobile networks for the industrial scenario and embedded systems.
- Security and safety of industrial systems and Cyber-Physical Systems (CPSs).
- Secure and dependable design of industrial networks and systems.
- Threat/vulnerability and risk analysis in industrial networks and systems.
- Authentication, authorization, and accounting in industrial networks and systems.
- Attack modelling and response in the industrial scenario.
- Monitoring, detection, and mitigation of threats in industrial networks and systems.
- Formal specification/enforcement/verification of security and safety properties in industrial networks and systems.
- Policy-based management for the industrial scenario.
- Artificial intelligence for security and safety of industrial network and systems.
- Distributed ledger and blockchain technologies for industrial applications.
- Security of and through next-generation networks/architectures in the industrial scenario (edge/fog/cloud computing, SDN/NFV, SaaS, etc.).
- Hardware and physical layer security.
- Security/safety vs. performance analyses, evaluation of (industrial) firewalls, IDSs, etc.
- Case studies, engineering practices and proof-of-concepts for safe and secure application domains (smart grids, transportation, health, etc.).

Important dates:

Deadline: February 3rd, 2023
Notifications: February 28th, 2023
Final versions: March 15th, 2023

WFCS 2023
Website: wfcs23.unipv.it