18th IEEE International Conference on Factory Communication Systems (WFCS)

27-29 April 2022, 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: Wolfgang Kastner (k@auto.tuwien.ac.at)
Affiliation: TU-Wien, Vienna, Austria

The increasing connectivity of industrial systems and the convergence of OT and IT, boosted by Industry 4.0, make the security of their communication infrastructures a major concern and a hot topic for both the industrial and academic communities. The need for remote monitoring and management, made painfully clear by the Covid19 pandemic, the interaction with emerging paradigms such as smart grid/transportation/buildings/communities/city, the adoption of popular technologies from the non-industrial world (wired/wireless networks, IoT, cloud computing, etc.) and the Internet-based access to large amounts of data for process optimization, all expose industrial systems to cyber-threats that may result in harm to people and damages to assets and the environment. Wireless communication, in particular, brings new attack and mitigation scenarios, driving novel research topics on security/safety of systems integrating 5G, WiFi 7 and beyond to support the flexibility of Industry 4.0.

Solutions are urgently needed, tailored to industrial networked infrastructures, also jointly addressing security and safety, given their interdependency in this scenario. This SS aims at bringing together researchers and practitioners to discuss recent advances, criticalities and future directions on the topic.

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

- Security of industrial networks, IoT, industrial IT and OT, embedded systems
- Security and safety of cyber-physical (production) systems
- Secure and dependable design of industrial networks and systems
- Secure deployment of wireless industrial communication and integration in existing communication structures
- Vulnerability and risk assessment in industrial communications and systems
- Monitoring, detection and mitigation of threats in industrial networks and systems
- Hazard and threat identification techniques, attack modeling and countermeasures in the industrial scenario
- Formal specification/enforcement/verification of security and safety properties in industrial systems
- Artificial intelligence and machine learning for security and safety of industrial communications and systems
- Distributed ledger and blockchain for industrial application
- Security of specific architectures and services (edge, fog, cloud, SDN, NFV-based, etc.) in the industrial scenario
- Security vs. determinism/performance analysis, evaluation of (industrial) firewalls, IDSs, etc.
- Policy-based security management for the industrial scenario
- Case studies, engineering practices and proof-of-concepts for safe and secure application domains (smart grids, cyber-physical production systems, transportation, buildings, etc.)

PAPER SUBMISSION: Up to 8 double-column pages, following the IEEE conferences template.

Website: wfcs22.unipv.it

IMPORTANT DATES (extended)**:**
Deadline: February 7th, 2022
Notifications: March 1st, 2022
Final versions: March 12th, 2022

Sponsored by IEEE IES Technical Committee on Factory Automation (TCFA) – Subcommittee FA6: Security in Industrial Communication and Embedded Systems