SS 03 - Automation, Critical Infrastructure and Sensing Systems Networks

Principal Organizer: Tiago Cruz (tjcruz@dei.uc.pt)
Affiliation: Universidade de Coimbra, CISUC, DEI, Portugal

Organizer 1: Leandros Maglaras (l.maglaras@napier.ac.uk)
Affiliation: Edinburgh Napier University, United Kingdom

Organizer 2: Paulo Simões (psimoes@dei.uc.pt)
Affiliation: Universidade de Coimbra, CISUC, DEI, Portugal

Over the past decades, automation infrastructures encompassing sensor and actuator networks have become increasingly pervasive, being found at the core of consumer and industrial applications alike, as it is the case for Industrial Automation and Control Systems (IACS), whose application scenarios range from simple process control to complex Critical Infrastructure monitoring and control tasks. Recently, such domains have been experiencing significant progress because of trends such as the rise of 5G connectivity, accessible Low Power WAN technologies and the emergence of the Industrial Internet-of-Things (IoT) paradigm. In many cases this constitutes a significant departure from the self-contained premises model, deployed on physically constrained areas under the responsibility of a single operator – instead, there has been an evolution towards the adoption of federated or overlayed multi-tenant architectures, crossing the access, edge or cloud domains and requiring the involvement of telecommunications, automation, and computing infrastructure providers. But regardless of their size or scope, such systems have one thing in common: a set of requirements in terms of security and safety, which ultimately define their criticality. Accidental or malicious disturbances might disrupt the nature of the involved control processes and applications, whose impact may range from a minor inconvenience to major, life-threatening incidents, especially in the case of critical infrastructures or applications. Necessarily, each context has its own specific issues and challenges: for instance, vehicular networks constitute a good example of a self-contained scenario with a wide range of security and safety implications, which is significantly different from massively distributed systems such as smart grids. With many of the latter quickly unfolding into increasingly larger scale (as it is the case for smart grids, which have pushed infrastructure components such as smart meters and inverters up to the consumer's doorstep), it is becoming increasingly difficult to ensure reliable, secure, and continuous operation in face of an increasingly diversified threat landscape.

This calls for the development of new tools and techniques, able to address the needs of critical infrastructure, automation and sensor networks, encompassing aspects such as security, automation protocols, fieldbuses, communication technologies and associated computing infrastructures, among others. This Special Session, realized under the auspices of the P2020 POWER and Smart5Grid Projects is aimed at representing the latest advances in the aforementioned domains.

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

- Consumer sensor applications.
- Industrial IoT safety and security applications.
- Algorithms and techniques for anomaly detection, for safety and security.
- Automation technologies such as SCADA systems for civilian and military uses.
- 5G and edge-computing for distributed automation environments.
- Virtualization and multi-tenancy for communications and computing infrastructures.
- Machine-to-Machine (M2M) communications and network infrastructure security for IACS.
- Security (auditing, protection, reaction) for IACS.
- Data-driven technologies and machine-learning approaches for IACS-based scenarios.
- Forensics and auditing techniques for IACS.
- Risk and interdependency modeling for IACS.
- Threat lifecycle and profiling analysis for IACS.

Important dates:

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

WFCS 2023
Website: wfcs23.unipv.it

IEEE Advancing Technology for Humanity | IES | Università di Pavia | Facoltà di Ingegneria Università di Pavia | inIT | TH OWL