Call for Papers
SS09 – Industrial Cybersecurity Methods and Technologies

Organized and Chaired by

Paulo C. Bartolomeu[1], Amjad Gawanmeh[2], Stefano Marrone[3]
[1] University of Aveiro (Portugal), bartolomeu@ua.pt
[2] University of Dubai (UAE), agawanmeh@ud.ac.ae
[3] University of Campania "Luigi Vanvitelli" (Italy), stefano.marrone@unicampania.it

FOCUS

Industrial cybersecurity has become a key research topic in recent years due to the massive connectivity brought by the Internet of Things and the rise of cyberattacks against industrial assets. While fostering contemporary applications and use cases, ubiquitous Internet access has also exposed legacy operational technologies to new and challenging security threats that must be addressed. This Special Session focuses on novel security, safety, and privacy-enhancing technologies for current and future industrial applications.

TOPICS

- ❖ Security, safety, or privacy-enhancing technologies in industrial systems
- ❖ Modeling of cybersecurity threats
- ❖ Applications of Artificial Intelligence in cybersecurity of industrial systems
- ❖ Applications of distributed ledger technologies/blockchains in Industry 4.0
- ❖ Self-sovereign identity for M2M and decentralized device-to-device communication
- ❖ Hardware advances for securing Industrial devices and networks
- ❖ Quantitative evaluation and/or interconnections among non-functional aspects (e.g., reliability vs. safety, security vs. performance)
- ❖ Run-time methods and technologies for Complex Event Detection systems
- ❖ Software engineering methods and techniques for high dependable control systems
- ❖ Security and privacy issues in CPS for industry systems
- ❖ Cyber-Physical Attacks and Countermeasures
- ❖ Real-time Threat Detection and Response for CPS and industry systems
- ❖ Case studies / lessons learned of security, safety, or privacy assessments of industrial systems

AIM

This Special Session aims at bringing together professionals from industry and academia to share cutting-edge concepts, recent developments, research results, and practical achievements in the design for and assurance of cybersecurity in industrial settings.

SOLICITED PAPERS

♦ Original Research (Regular) ♦ Surveys ♦ Industry practice ♦ Work-in-progress
The working language of the conference is English, For submission rules, please refer to the Author's Instruction on the conference website.

PAPER ACCEPTANCE

Accepted, registered, and presented papers will be copyrighted by IEEE and published in the conference proceedings. The proceedings will be available in the IEEE Xplore® Digital Library. The final manuscript must be accompanied by a registration form and a registration fee payment proof and it is mandatory that at least one author attends and presents the paper at the conference. Failure to adhere to these guidelines may result in paper exclusion from post-conference distribution via IEEEXplore by the ETFA 2024 Organizing Committee. All conference attendees must pay the conference registration fee and cover their own personal expenses for travel and accommodations.

AUTHOR'S SCHEDULE 2024

❖**Regular and special sessions papers**

Submission deadline	**April 28th**
Acceptance notification	May 31st
Deadline for final manuscripts	July 1st

❖**Work-in-progress/ Industry practice papers**

Submission deadline	**May 26th**
Acceptance notification	June 17th
Deadline for final manuscripts	July 1st

IEEE · IEEE Industrial Electronics Society · Consiglio Nazionale delle Ricerche · Istituto di Elettronica e di Ingegneria dell'Informazione e delle Telecomunicazioni · Università degli Studi di Padova · Dipartimento di Ingegneria dell'Informazione

www.ieee-etfa.org
etfa2024@dei.unipd.it