29TH INTERNATIONAL CONFERENCE ON EMERGING TECHNOLOGIES AND FACTORY AUTOMATION

ETFA 2024 PADOVA, ITALY SEPTEMBER 10TH-13TH 2024

Call for Papers
SS01 – AI-based Safe, Secure, and Sustainable (I)IoT

Organized and Chaired by

Muhammad Taimoor Khan[1], Dimitrios Serpanos[2], Howard Shrobe[3] , Kunio Uchiyama[4]

[1] University of Greenwich, UK, m.khan@gre.ac.uk
[2] ISI Athena, ECE, University of Patras, Greece, serpanos@ece.upatras.gr
[3] MIT CSAIL, USA, hes@csail.mit.edu
[4] AI Chip Design Centre, Japan, kunio.uchiyama@aist.go.jp

FOCUS. Computing constitutes a fundamental component of the emerging initiatives like Society 5.0, Industry 5.0, Healthcare 5.0, and Agriculture 5.0 (aka X 5.0), which combine cyber and physical spaces (i.e., processes) and requires control and monitoring techniques for their operation and management. In X 5.0, people, things, devices, and systems are connected in cyberspace and operate exploiting automated methods, including machine learning (ML) and artificial intelligence (AI). Such operation and management bring new value to industry and society in ways not previously possible. Typical cyber physical systems (CPS) are based on (I)IoT (Industrial - Internet of Things) and (I)CPS (Industrial - Cyber Physical Systems) and have applications in all critical infrastructure domains with strict real-time requirements, such as healthcare, electric grid, transportation, to name a few. Intentional or accidental errors/failures/attacks to these systems have highly severe consequences. Therefore, novel design methodologies are required to ensure that design of real-time cyber physical systems and applications in the emerging Society 5.0 are free of vulnerabilities, threats and attacks. Since the physical part of CPS involves several processes, typically, it is challenging to ensure that the design is free from all known vulnerabilities. It is necessary to develop run-time monitoring and analysis techniques that can help to detect run-time incidents by observing the processes and their data. Furthermore, adequate modelling of CPS physical processes and corresponding cyber and physical attacks is fundamental to systematically model, analyse and verify real-time security of CPS. Importantly, since AI and machine learning have demonstrated their success in many application areas including cyber security, this special session focuses on investigating AI, machine learning and formal methods-based techniques to develop safe, secure, privacy and law-aware real-time cyber physical systems, digital twins and smart cities at all levels, from hardware components to applications.

TOPICS. Topics of interest include, but are not limited to:

- Design-time and run-time safety, security, privacy and law in modern systems, e.g., X 5.0, Digital Twins, ICPS, and IIoT.
- Data-driven (AI and Machine Learning or model)-based
  - Safety, security, privacy and law in cyber-physical systems (CPS), networks and communication
  - Prevention, detection and mitigation techniques for real-time CPS (RT-CPS) applications against cyber, non-cyber and cyber-non-cyber threats
  - Hardware design for safe, secure, privacy and law-aware RT-CPS
  - Vulnerability analysis of RT-CPS applications
  - Attack modeling and performance analysis of RT-CPS
- Formal methods (FM)-based safety and security of critical systems at design-time and run-time
- Safety, security and privacy of citizens in X 5.0 including manmade and natural cyber and non-cyber threats, pandemics and disasters
- Methodologies and tools for analysis, compliance and enforcement of law and regulations for safety, security and/or privacy
- Methodologies and tools for compliance testing and standardization
- CAD tools for AI-based cyber-physical systems (CPS)
- CAD tools for safe, secure, privacy, and law-aware RT-CPS
- Case studies for AI and machine learning-based RT-CPS
- Case studies for digital law compliance and regulations in RT-CPS
- Benchmarks for security, safety, privacy and or/law in RT-CPS
- Challenges in modelling, analysis, safety, security, privacy and law of RT-CPS

AIM

The aim of the Special Session is to bring together security, safety, privacy and law researchers and practitioners from the industry and academia and provide them with a platform to report on recent advances and developments in the newly emerging areas of Society 5.0 (i.e., their underlying infrastructure that includes modern IIoT and ICPS), their design-time and run-time safety, security and privacy employing AI, ML and FM based techniques.

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