ETFA

26TH INTERNATIONAL CONFERENCE
ON EMERGING TECHNOLOGIES
AND FACTORY AUTOMATION

2021 VÄSTERÅS, SWEDEN
SEPTEMBER 7TH-10TH 2021

Call for Papers

SS07 - AI and Machine Learning for Safety and Security in Society 5.0

Organized and Co-Chaired by (sorted by last name)

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

[1] University of Greenwich, UK
[2] ISI Athena, ECE, University of Patras, Greece
[3] MIT CSAIL, USA
[4] AI Chip Design Centre, Japan

- **FOCUS**. In this Special Session Computing constitutes a fundamental component of the emerging Society 5.0, which combines cyber and physical spaces (i.e., processes) and requires control and monitoring techniques for its operation and management. In Society 5.0, people, things, 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 and secure real-time cyber physical systems at all levels, from hardware components to applications.

- **TOPICS.** Topics of interest include, but are not limited to:
  - AI and Machine Learning based
    - Safety and security of cyber-physical systems (CPS), networks and communication
    - Prevention, detection and mitigation techniques for real-time CPS (RT-CPS) applications against cyber and physical threats
    - Hardware design for safe and secure 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 and security of citizens in Society 5.0 including pandemics and disasters
  - Impact of pandemic and natural disasters on safety and security of citizens
  - CAD tools for AI-based cyber-physical systems (CPS)
  - CAD tools for safe and secure RT-CPS
  - Case studies for AI and machine learning-based RT-CPS
  - Benchmarks for security and safety of RT-CPS
  - Challenges in modelling, analysis, safety and security of RT-CPS

- **AIM.** The aim of the Special Session is to bring together 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 safety and security employing AI, ML and FM based techniques.

- **CONFERENCE FORMAT**. The conference will comprise multi-track sessions for regular papers, to present significant and novel research results with a prospect for a tangible impact on the research area and potential implementations, as well as work-in-progress (WiP) and industry practice sessions.

- **AUTHOR'S SCHEDULE (2021)**

Regular and special sessions papers

Submission deadline	April 1
Acceptance notification	May 6
Deadline for final manuscripts	June 17

Work-in-progress/Industry practice papers

Submission deadline	May 13
Acceptance notification	June 10
Deadline for final manuscripts	June 17