25TH INTERNATIONAL CONFERENCE
ON EMERGING TECHNOLOGIES
AND FACTORY AUTOMATION
ETFA 2020 VIENNA, AUSTRIA
SEPTEMBER 08TH-11TH 2020

Call for Papers
SS11 – AI, Machine Learning and Formal Methods for Safe and Secure Real-time Cyber-Physical Systems

Organized and Co-Chaired by (sorted by last name)
Muhammad Taimoor Khan[1], Dimitrios Serpanos[2], Howard Shrobe[3]

[1] University of Greenwich, UK
[2] ISI Athena, ECE, University of Patras, Greece
[3] MIT CSAIL, USA

- **FOCUS**. Modern industrial control systems has evolved into industrial cyber-physical systems (ICPS) and Industrial Internet-of-Things (IIOTs), which combines cyber and physical industrial processes together using control and monitoring techniques. Typically, these systems have applications in all critical infrastructure domains with strict real-time requirements, e.g., healthcare, electric grid, transportation, to name a few. Any intentional or accidental error/threat to such systems have very severe consequences. Therefore, novel design methodologies are required to ensure that design of real-time cyber physical system applications (RT-CPS) is free of certain vulnerabilities and attacks. Since, physical process of CPS involves many such systems, thus, it is very challenging to ensure that the design is free from all known vulnerabilities or attacks. Therefore, it is required to develop run-time monitoring and analysis techniques that can help to detect run-time threats 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 has demonstrated their success in many application areas including cyber security, this special session is focused on investigating AI, machine learning and formal methods based techniques to develop safe and secure real-time cyber physical systems.

- **TOPICS.** Topics of interest include, but are not limited to:
  - AI, machine learning and formal verification based
    - Modelling of cyber and physical threats
    - Prevention techniques for real-time CPS (RT-CPS) applications against cyber and physical threats
    - Detection techniques for RT-CPS applications against cyber and physical threats
    - Mitigation techniques for RT-CPS applications against cyber and physical threats
    - Vulnerability analysis of RT-CPS applications
    - False data injection attacks in RT-CPS applications
  - Performance analysis of RT-CPS security
  - RT-ICS network and communication security
  - Benchmarks for security and safety of RT-CPS
  - Challenges in modelling, analysis and security of RT-CPS

- **AIM.** The aim of this special session is to investigate security solutions for RT-CPS by focusing on the challenges in modelling of cyber and physical with unique and variant functional characteristics and real-time performance requirements. Furthermore, the goal of the session is to promote AI, machine learning and formal methods based techniques that assure security of real-time CPS applications.

- **CONFERENCE FORMAT**. The conference will comprise multitrack 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 (2020)**

❖ 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