SysTol’21

Invited Session: “Formal methods for the safety and security of cyber physical systems”

Organizers: Isabel Demongodin, Aix Marseille Université (isabel.demongodin@lis-lab.fr)
Dimitri Lefebvre, Université Le Havre Normandie (dimitri.lefebvre@univ-lehavre.fr)

Cyber-physical systems are engineered systems with strong interactions between computational and physical components. In particular, the recent advancement of information and communication sciences and Internet-of-Things make Cyber-physical systems pervasive in today’s technological society.

The price paid for such unprecedented connectivity is an increase in cybercrime and violations, making cybersecurity a key research focus in many different research communities. Generally speaking, cybersecurity is the protection of computer systems and networks from the damages to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

The ever-increasing demand for safety and security of cyber-physical systems puts stringent constraints on their analysis and design, and necessitates the use of formal approaches. In recent years, we have witnessed a substantial increase in the use of formal techniques for the verification and design of privacy-sensitive, safety-critical cyber-physical systems.

The main objective of this invited session is to gather recently developed novel approaches devoted to analysis and enforcement of security, privacy and safety of cyber-physical systems using formal techniques. In particular, new contributions for the development of modeling and analysis methods, of verification algorithms and of specific controller design for such complex systems are encouraged including theoretical and application issues related to cybersecurity. A non-exhaustive list of some potential topics is provided below:

- Security and privacy analysis of cyber-physical systems,
- Fault diagnosis, intrusion detection, and attack mitigation of cyber-physical systems
- New modeling frameworks for cyber attacks
- Analysis of impacts of attacks on closed-loop system behaviors
- Formal synthesis of attack models
- New concepts and models of resilience of controllers and supervisors
- Fault diagnosis in the presence of cyber attacks
- New modeling frameworks and analysis methods for privacy and confidentiality of information
- New analysis methods to determine system ability of preserving privacy and and confidentiality
- Formal methods and reactive synthesis for safety of cyber-physical systems
- Algorithms and tools for verification and synthesis of safety-critical systems
- Applications in security and/or safety of manufacturing systems, transportation systems, energy systems, robotic networks, telecommunications, and computer networks.

Contributors are invited to send the title and abstract of their proposal to the session organizers.