IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

Resilience, Reliability, and Security in Cyber-Physical Systems

Theme: The research and development of Cyber-Physical Systems (CPSs) have been greatly charging forward in recent years with advanced sensing, communication, control, and actuation. Commercial and industrial CPSs, such as aircrafts, automobiles, power transmission and distribution networks, microgrids, smart factories, robotics, and smart phones, process significant amount of important and sensitive data. With the increase of devices, software, and intelligent sensors in CPSs, resilience, reliability, and security of CPSs become more and more important. Resilience requires the system being able to adapt and survive in the presence of faults and failures, resulted from natural faulty conditions or malicious attacks, by efficiently mitigating or isolating the affected subsystems or devices. Reliability is to reduce the probability of failure of the CPSs by proper design technologies. Security, on the other hand, aims to prevent, detect, and mitigate the activities of malicious attacks such as stealing of important information from target computers or networks. There are urgent needs of research and development in CPSs to enhance their resilience, reliability, and security to ensure the safety, availability, and survivability of CPSs under various conditions and scenarios. This Special Session aims to promote new research concepts and achievements in resilience, reliability, and security in CPSs.

We solicit papers covering the following topics of interest in CPSs, but not limited to:

- Resilience, reliability, and security of industrial control systems
- Machine learning for resilience and security
- Resilient system design and development
- Fault diagnosis and fault tolerant control
- Security in networked systems
- Industrial systems design for resilience, reliability, and security
- Extreme phenomena modeling and analysis for renewable energy systems
- Modeling, analysis and detection of cyber physical attacks
- Advanced data analytics for improving cybersecurity resilience
- Formal methods for microgrids resilience
- Programmable networked microgrids
- Security in software-defined-networking-enabled microgrids
- Reliable control for distributed energy resources
- Storm preparedness and emergency response

Manuscript Preparation and Submission

Follow the guidelines in "Information for Authors" in the IEEE Transaction on Industrial Informatics http://www.ieee-ies.org/pubs/transactions-on-industrial-informatics . Please submit your manuscript in electronic form through Manuscript Central web site: https://mc.manuscriptcentral.com/tii . On the submitting page #1 in popup menu of manuscript type, select: SS on **Resilience, Reliability, and Security in Cyber-Physical Systems**

Submissions to this Special Section must represent original material that has been neither submitted to, nor published in, any other journal. Regular manuscript length is 8 pages.

Note: The recommended papers for the section are subject to final approval by the Editor-in-Chief. Some papers may be published outside the special section, at the EIC discretion.

Timetable:	**Deadline for manuscript submissions**	May 31, 2019
	Expected publication date (tentative)	**October 2019**

Guest Editors:

Dr. Bin Zhang, Dept of Electrical Engineering, University of South Carolina, Columbia, zhangbin@cec.sc.edu
Dr. Peng Zhang, Dept of Electrical and Computer Engineering, University of Connecticut, Storrs, peng.zhang@uconn.edu
Dr. Tuyen Vu, Dept of Electrical Engineering, Clarkson University, Potsdam, tvu@clarkson.edu
Dr. Mo-Yuen Chow, Dept of Electrical and Computer Engineering, North Carolina State University, Raleigh, chow@ncsu.edu