IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

Cyber-Physical Security in Industrial Environments

"Smart" is slowly becoming a concept that infiltrates all branches of everyday life and environments in which we are living. The "Smart Industrial Environments" term can be coined to describe everything every aspect of future-focused industrial environments, being it smart transportation systems, smart vehicles, smart factories, smart grids, smart devices (smartphones, wearables), smart services (e.g. individual just-in-time production piplines adjusted to the needs of the supply-chain) to smart management of plants using information technology. In addition of being a term that contains all these aspects, it also includes the inter-connection of all these smart technologies, crossing any kind of technological and political borders.

The Smart Industrial Environments, developed under the support of a new generation of cyber-physical systems, can realize information resource in a highly concentrated manner. With the increase of information sharing, this underpins the increasing importance of information and network security.

Securing a Smart Industrial Environment is a great challenge as there are many actors, complex systems, and interplays between them. One of the key issues in a Smart Industrial Environments is to ensure users' information security and privacy as well as security of systems that it consists of. Therefore effective technical and policy measures shall be derived to deal with the potential threats. The Smart Industrial Environments shall establish and perfect various cyber-physical system security technology mechanisms, such as the establishment of remote disaster recovery and backup, physical access control, cyber-physical system emergency response in distributed heterogeneous environments, cyber-physical system security monitoring and situational awareness as well as other mechanisms. The Smart Industrial Environments shall particularly strengthen security awareness, promote the security strategy and network legislation, strengthen security management and adopt self-control based hardware and software among other methods and measures. This will allow to build a Smart Industrial Environments on the basis of security and reliability to support the stable operation and the healthy development of cyber-physically supported societies.

This special section will focus on (but not limited to) the following topics:

- Secure, dependable and trustable cyber-physical systems for the Smart Industrial Environments
- Electronic authentication and certification for the Smart Industrial Environments
- System design methodologies for Cyber-Physical system security
- Security frameworks and solutions for Cyber-Physical systems
- Cyber-Physical system emergency response for the Smart Industrial Environments
- Cyber-Physical system security capability evaluation for the Smart Industrial Environments
- Methodologies for modeling and assessment of cyber-physical security and privacy
- Privacy protection and trust management
- Sensing and control for attack detection and mitigation
- Secure and trustworthy demand-response management
- Sensor security supervision
- Cyber-physical security of energy storage and management systems
- Cyber-physical security of renewable energy systems (e.g., large-scale PV and wind farms)
- SCADA and industrial control system (ICS) system security
- Access control systems and policies for the Smart Industrial Environments
- Privacy and data protection for the Smart Industrial Environments
- Intrusion detection/prevention solutions for cyber-physical systems for the Smart Industrial Environments
- Internet of Things Network Protocol Security
- Protection of legacy sub-systems in the Smart Industrial Environments
- Situational awareness and monitoring
- Security of smart system-interconnection
- Discussion of novel threat scenarios
- Forensics in the Smart Industrial Environments
- Teaching and education for the Smart Industrial Environments securityManuscript 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 **Cyber-Physical Security in Industrial Environments**

Editor-in-Chief: Prof. Dr.-Ing; Ren C. Luo tii@ira.ee.ntu.edu.tw

IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

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 1, 2019**
	Expected publication date (tentative)	**October 2019**

Guest Editors:

- Dr. Zhihan Lv, University of Barcelona, Spain lvzhihan@gmail.com
- Dr. Wojciech Mazurczyk, Warsaw University of Technology, Poland wmazurczyk@tele.pw.edu.pl
- Prof. Steffen Wendzel, Worms University of Applied Sciences, Germany wendzel@hs-worms.de
- Dr. Houbing Song, Embry-Riddle Aeronautical University, USA h.song@ieee.org