IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

Trustworthiness in Industrial IoT Systems and Applications

Theme: According to the World Economic Forum, “The Industrial Internet of Things (IIoT) will transform many industries, including manufacturing, oil and gas, agriculture, mining, transportation and healthcare. Collectively, these account for nearly two-thirds of the world economy.” Recently, innovations in IIoT computing and communication devices and hardware, connectivity, big data analytics, and machine-learning have converged to generate huge opportunities for industries. The IIoT broadly deals with the two areas: increasing efficiency and improving health/safety. To achieve these, the biggest hurdle part, looking into the future, is the “trustworthiness” in terms ultra-high data trust, cross-border data flow, data retention, QoS, service trust, availability, fault-tolerance, data quality, data security, and data privacy risks, and reliable industrial monitoring, as many of these are still the early stage of research in IIoT. The IIoT integrates numerous "smart things" with “smart computations” and “smart communications” that can be endowed with different levels/forms of intelligence and even capable of thinking. As the number of IIoT devices increases in industrial environments, data communication increases, and the data scale, veracity, and complexity increase, the “dependability” concerns increases drastically.

More specifically, dependability of industrial sensor services, data collection, processing, and decision-making in the IIoT can be the top-notch concerns for IIoT-enabled monitoring systems and applications. (1) What would be the quality of industrial monitoring or decision-making if low-quality, meaningless, or untrustworthy data are collected and this undependable data is processed and transmitted over the network for decision-making? (2) What would be the situations once the untrustworthy data are already encrypted, stored, or processed in cloud servers? (3) What would be the trustworthiness of the IIoT-enabled predictive maintenance, whereas a faulty or security compromised industrial machines/devices in a manufacturing process can mean millions of dollars in lost productivity, while production halts to fix the issue? These can lead to massive decreases in productivity. (4) There is a lack of design tools/models for assessing the dependability of IIoT applications at the early planning and design phases that prevents system designers from optimizing their decisions so as to minimize the effects of security attacks or IIoT device faculty. Regarding numerous concerns similar to these, we immensely need to build IIoT systems and applications with the dependability to provide steady operations and high-quality results in order to support the increasing efficiency and improving health/safety in the IIoT.

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

- Trustworthiness in architectures, platforms, and system designs of IIoT
- Trustworthiness in industrial sensor designs for IIoT
- Trustworthiness in terms of security, privacy, trust, and risk in IIoT
- Trustworthiness in networking big data in IIoT
- Trustworthiness through fault prevention, fault tolerance, and fault removal in IIoT
- Trustworthiness in sensing, detection, and decision-making in IIoT
- Trustworthiness in data collection (acquisition, transmission, aggregation) in IIoT
- Trustworthiness in industrial equipment and process monitoring in IIoT
- Trustworthiness in industrial event detection and monitoring in IIoT
- Trustworthiness in cloud computing, storage, and cloud servers for IIoT
- Trustworthiness in machines, tools, mobile apps and techniques for IIoT
- Trustworthiness in terms of reliability, availability, plant safety, quality control in IIoT
- Trustworthiness in holistic co-design of wireless and control in IIoT
- Trustworthiness in industrial applications (e.g., SHM, robotics, predictive maintenance) of IIoT
- Trustworthiness in leveraging supply chain and blockchain for IIoT
- Trustworthiness in demand-response management and situational-awareness in IIoT
- Trustworthiness assessment, metrics, and evaluation for IIoT

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 **Trustworthiness in Industrial IoT Systems and Applications**

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**	**August 30, 2019**
	Expected publication date (tentative)	**January 2020**

Guest Editors:

Prof. Zakirul Alam Bhuiyan, Fordham University, USA zakirulalam@gmail.com; mbhuiyan3@fordham.edu
Prof, Sy-Yen Kuo, National Taiwan University, Taiwan sykuo@ntu.edu.tw
Prof. Jiannong Cao, Hong Kong Polytechnic University, China csjcao@comp.polyu.edu.hk
Prof. Guojun Wang, Guangzhou University, China csgjwang@gmail.com ; csgjwang@gzhu.edu.cn

Editor-in-Chief: Prof. Dr.-Ing; Ren C. Luo tii@ira.ee.ntu.edu.tw
http://www.ieee-ies.org/pubs/transactions-on-industrial-informatics