IEEE Transactions on Industrial Informatics

CALL FOR PAPERS

for Special Section on

Securing the Industrial Internet of Things: From Technical Innovations to Management Practices

Theme: With Modern industrial organizations harness digital technologies to drive agility, optimize decision-making, and improve operational efficiency in diverse sectors such as manufacturing, energy, transportation, mining, healthcare, and transportation and logistics. Known as Industry 4.0 or the Industrial Internet of Things (IIoT), these networks of industrial systems create unprecedented business opportunities for private enterprise on the one hand but also increases risk exposure of cyber attack on the other.

From the perspective of the organizational technology layer, attack surfaces have dramatically expanded (e.g., new entry points from endpoints and legacy devices, more vulnerable industrial control systems without suitable cybersecurity solutions, more proprietary software that is hard to update and patch, and poor security design), whereas security countermeasures have developed comparatively slowly. Whereas from the management perspective, security practices have not followed a unified security strategy that successfully integrates IT and OT (e.g., fragmentation in the security organizational structure and processes, reliance on manual practices, poor situation awareness of activity in the OT environment, shortage of appropriate cyber skills in the workforce).

At the same time, the proliferation of advanced cyber weaponry and the introduction of highly trained teams of cyber-soldiers backed by nation-states or organized crime syndicates has led to the rapid militarization of the global internetworking environment. This development has given rise to knowledgeable, well-trained, and organized human attackers using sophisticated tools and techniques to disrupt and destroy cyber-physical infrastructures and deny organizations access to their own technology infrastructures and services. Cyber attacks against IIoT have dramatically increased in both volume and sophistication. For example, the level of organization and meticulous attention to detail involved in the recent Triton attack on the safety instrumented systems indicates the intent and increasing capability of threat actors against IIoT.

The increased capability of threat actors and the increased risk exposure to organizations from their IIoT calls for urgent and holistic research into the cybersecurity of IIoT. This special section encompasses both management and technical cybersecurity research in IIoT. Of particular interest is research that integrates management and technical approaches to IIoT security; research that studies the real-world problem of IIoT security in organizations, and research that contributes sound practical advice to the industry.

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

— Innovative security solutions for IIoT infrastructures
— Security frameworks and network protocols for IIoT
— Machine Learning-based security solutions for IIoT
— Blockchain technologies for reliable and trustworthy computing in IIoT
— Biometric modalities for individuals' authentication in IIoT
— Security perimeters for resource-constrained IIoT devices
— Device authentication and device identity management in IIoT
— Attack prevention and response strategies for IIoT
— Situation Awareness of IIoT environment
— Risk identification, assessment, and mitigation in IIoT
— Policy and training approaches for securing IIoT
— Cybersecurity risks arising from IIoT deployments in 5G networks
— Dynamic threat and vulnerability analysis approaches

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 **Securing the Industrial Internet of Things: From Technical Innovations to Management Practices**

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 **October 30, 2021**
Expected publication date (tentative) May 2022

Guest Editors:

Dr. Ali Ismail Awad, Luleå University of Technology, Sweden ali.awad@ltu.se
Dr. Atif Ahmad, University of Melbourne, Australia atif@unimelb.edu.au
Dr. Ali Hassan Sodhro, Mid Sweden University, Östersund, Sweden alihassan.sodhro@miun.se