Guest Editorial
Security, Reliability, Privacy, and Quality in Industrial Automation and Control

INDUSTRIAL Internet of Things (IoT) has enabled many new applications such as remote asset monitoring, predictive maintenance in factory, wearable and implanted biomedical sensors-based health and well-being monitoring, smart agriculture and viticulture monitoring, infrastructure monitoring, power system monitoring, energy system security, power grid quality, machine control, and many others. The IoT devices may be embedded, implanted, submerged, or monitor the activity remotely, and feed data to a control system using wired or a variety of wireless networks. A comprehensive infrastructure consisting of densely deployed sensors, actuators, data aggregators, and sophisticated decision and control systems can truly realize the concept of a *smart world*.

The industrial automation systems may operate by making the use of feedback control loop, cascade, feed-forward, and advanced process control. These systems operate in an open environment. Thus, exhibit a large surface area for cyber-attacks. The cyber infrastructure, in these industrial environments, is a network of IoT and information and communication technology devices, and attacks could be in the form of configuration changes, data corruption, manipulating state estimation matrices, SCADA system malfunctioning, and others. The attacks could be launched by organised criminals, hacktivists, or state nations. During the course of attack research, criminals compromise the privacy and steal information. Stolen information about the architecture of the industrial critical industrial automation and control systems plays important role in designing the attack strategy. Extensive investigation can result in identifying the vulnerabilities in the systems, then malware can be written to exploit these vulnerabilities to cause harm to physical systems.

This Special Issue (SI) was organized to provide a multi-aspect up-to-date reference for solutions that leverage techniques and insights from the domains of artificial intelligence, Internet of Things, edge computing, and big data, to address security, reliability, privacy, and quality challenges in industrial applications. We received a total of sixty-five original submissions from various institutions all over the world. After a rigorous review process, nineteen papers were accepted and are presented for inclusion in this SI of the IEEE Transactions on Industry Applications. Each paper is multidisciplinary and addresses differing challenges in industrial automation and control systems. The papers have been organized in the following categories to facilitate their reading.

- Security, privacy, and trust aspects of industrial automation and control systems including threat intelligence, collaborative trust, authentication, key agreement protocols, state estimation, and false data injection attacks (9 papers);
- Reliability issues in power control and management in cyber-physical systems and their communication networks (6 papers); and
- Power quality in power systems and electrical machines (4 papers).

ACKNOWLEDGMENT

As guest editors, we would like to convey our heartiest gratitude to all the authors who have submitted their knowledgeable contributions and to the highly qualified anonymous reviewers. We would also like to thank Dr. Thomas A. Nondahl, the Editor-in-Chief (EiC) of the IEEE Transactions on Industry Applications and Professor Massimo Mitolo, the Deputy EiC of the IEEE Transactions on Industry Applications, for giving us the opportunity to organize this SI and for all the encouragement, help, and support given throughout the process. Finally, a special thank you goes to the IEEE Industry Applications Society Publications Editorial Office, particularly, Dr. Peter Wung for sharing their experience and knowledge of the review process and for continuous suggestions and technical support. We also sincerely appreciate the effective and dedicated work of the associate editors, who made the management of the reviews possible: (i) Prof. Akshay Kumar Rathore, Concordia University, Canada; (ii) Prof. Sukumar Kamalasadan, University of North Carolina at Charlotte, USA; (iii) Prof. Kashem Muttaqi, University of Wollongong, Australia; and (iv) Prof. Anurag Srivastava, Washington State University, USA.

MUHAMMAD USMAN, *Guest Editor*
Faculty of Computing, Engineering and Science
University of South Wales
Cardiff, Newport CF37 1DL, UK

ALIREZA JOLFAEI, *Guest Editor*
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia

IQBAL GONDAL, *Guest Editor*
School of Science, Engineering and Information Technology
Federation University Australia
Mt. Helen, 3355 VIC, Australia

KRISHNA KANT, *Guest Editor*
Department of Computer and Information Sciences
Temple University
Philadelphia, PA 19122, USA