# IEEE Internet of Things Journal Special Issue on "RRCPS: Reliable and Resilient Cyber-Physical Systems"

Cyber-physical systems (CPSs) can provide both improved and new functionality with efficiency and convenience; but the increasing use of CPSs and their application to key infrastructure components means that failures can result in disruption, damage and even loss of life. Avoiding these consequences is not a trivial problem, because a CPS which can readily communicate with users, remote computers, as well as other CPSs, is naturally vulnerable to network failures and malicious interference. Reports of such attacks, and public concern about them, have increased in recent years.

It is essential to develop CPSs which are reliable (or trustworthy), because their functionality and timing are provably correct; and which are resilient, because they are designed to cope with both internal errors and external attacks. A resilient CPS will continue to operate normally as long as possible, and then provide functionality that reduces gracefully and safely if problems increase and cannot be overcome. The design of reliable and resilient CPSs (RRCPS) directly involves topics such as real-time control, sensor design, and security; and the use of machine learning and data mining to provide more sophisticated and versatile behavior. In particular, special attention needs to be paid to the application of Internet of Things (IoT) in building RRCPS, because the IoT is essential to realize a vision of the future CPSs where numerous devices are tightly connected over the Internet, allowing them to collect information about the real world in real time, and share it with other systems and physical devices. In fact, CPS can be considered as real-time IoT, which requires end-to-end real-time performance on top of conventional characteristics of IoT.

This special issue will cover both theory and practice, with a focus that ranges from the platforms on which RRCPS can be built to applications of RRCPS. Topics of interest include, but are not limited to, the following:

Theoretical foundations for RRCPS
- Design theories for RRCPS and the IoT • Modeling and verification of RRCPS and the IoT

Platform support for RRCPS
- Fault-tolerant design of RRCPS platforms and IoT infrastructure
- Software platforms with monitoring and recovery capabilities
- Failure detection and autonomous recovery with graceful performance degradation
- Real-time scheduling, resource allocation, and middleware support for RRCPS
- Virtualization to increase reliability of CPSs and the IoT

Networked control for RRCPS
- Reliable networks and robust end-to-end communications • Protocol design for real-time communications
- Cyber-physical security and resilience in networked control system
- Design, modeling, and implementation of resilient control • Detection and analysis of attacks on control systems

Security and safety of CPS and the IoT
- Evaluation of risks, threats, and attacks • Analysis of vulnerabilities • Attack resistance
- Intrusion detection • Software reliability and audit

Novel RRCPS and IoT applications
- Architectures • Applications of artificial intelligence • Testbed implementations and case studies
- Co-design of communication, computing and control for security and privacy

## Schedule

Submission Deadline: **August 1, 2018**
First Reviews Due: October 15, 2018
Revision Due: November 15, 2018
Second Reviews Due/Notification: December 15, 2018
Final Manuscript Due: January 15, 2019
Publication Date: 2019

## Submission

All original manuscripts or revisions to the IEEE IoT Journal must be submitted electronically through IEEE Manuscript Central, http://mc.manuscriptcentral.com/iot. Author guidelines and submission information can be found at http://ieee-iotj.org/. The IEEE IoT Journal encourages authors to suggest potential reviewers as part of the submission process, which might help to expedite the review of the manuscript. Please suggest only those without conflict of interest. Each submission must be classified by appropriate keywords.

## Gest Editors

Prof. Kyungtae Kang (ktkang@hanyang.ac.kr), Hanyang University, Republic of Korea
Prof. Insup Lee (lee@cis.upenn.edu), University of Pennsylvania, PA, USA
Prof. Kai Liu (liukai0807@cqu.edu.cn), Chongqing University, China
Dr. Man-Ki Yoon (man-ki.yoon@yale.edu), Yale University, CT, USA
Prof. Kyung-Joon Park (kjp@dgist.ac.kr), DGIST, Republic of Korea