Call for Contributions
Special Issue on Cyber Security for Embedded Controls in Cyber Physical Systems

Modern industrial control systems (ICS) and other complex cyber-physical systems (CPS) such as smart grid, unmanned vehicles, manufacturing plants, chemical plants, and nuclear reactors are complex interconnections of heterogeneous hardware and software components. With increasing complexity, connectivity, and programmability of embedded CPS devices, the potential cyberattack surface has also been increasing making the study of related cyber-security issues highly relevant and timely. Several attacks on CPS have been widely publicized over the past few years. Besides computing/communications/networking based cyber-attacks, CPS are vulnerable to process-aware attacks that aim to disrupt the proper functioning or hamper performance/efficiency/stability/safety of the physical systems/processes of the CPS. By modifying the information flow (e.g., sensor spoofing) or the computational behavior of the system, process-aware attacks can disrupt the functioning of the real-time control mechanisms in the CPS to thereby hamper the performance or stability of the overall system or its components.

In this context, the special issue on Cyber-Security for Embedded Controls in Cyber-Physical Systems will explore challenges and new directions in design, modeling, simulation, and practical applications of the next-generation cyber-security mechanisms for embedded controls in CPS (specific topics of interest are outlined below). The goal of this special issue is to provide a reader a broad perspective of the state-of-the-art in the field from both academic and industrial viewpoints. The special issue will span the wide gamut of crucial facets including theoretical foundations, experimental implementations, and practical deployments in the industry.

Topics of Interest include but are not limited to:

- Resilient control design, modeling, simulation, and implementation
- Side channel analysis for cyber security of CPS
- Process monitoring for cyber security of CPS
- Application domains: Cyber security for smart grid, transportation systems, healthcare/biochips/medical devices, industrial control systems andfor human-machine interfaces

Submission Guidelines:

Guidelines for IEEE D&T papers are given at: http://ieee-ceda.org/publication/ieee-design-test-dt/paper-submission-instructions. Please choose SI: Cyber Security for Embedded Controls in Cyber Physical Systems while submitting the manuscript to the ScholarOne Manuscripts website (https://mc.manuscriptcentral.com/dandt).

Paper Submission Deadline – Jan 15th 2018

Guest Editors Contacts:
Farshad Khorrami, NYU,
khorrami@nyu.edu
Sek Chai, SRI International,
Princeton, NJ, U.S.A.
Balaguruna Chidambaram, Boeing