Call for Papers: IEEE Embedded Systems Letters

Special Issue on Emerging Topics in Secure and Trustworthy Cyber-Physical Systems

Cyber-Physical Systems (CPS) tightly couple cyber components (used for computation and communication) with sensing and actuation components to control multi-physics systems. These systems are extremely heterogeneous and require novel and holistic design methods to completely capture the requirements and the constraints, such as low power and energy consumption and real-time capabilities to reliably interact with the physical world, imposed by their dual nature. Nevertheless, the sensitivity of sensed data and the presence of actuators impose also high security requirements in CPS. Standard design techniques used for securing embedded systems are not suitable for CPS, due to the often restrict computation and communication budget available in the latter. Furthermore, current research efforts mainly focus on securing only the cyber-part of CPS, ignoring security threats caused by physical component and thereby cross-domain and cross-layer security issues. To address these issues, it is required to have a novel design approach in which security is considered from the beginning of the whole design flow and addressed in a holistic way, tackling both cyber and physical components of the whole system. Additionally, novel modeling strategies and methods to measure and evaluate the security of CPSs needs to be devised, developed, and formalized.

Topics of Interest

The special issue will cover all aspects of security and trustworthiness in cyber-physical systems. **All the papers in this special issue must focus on cyber-physical security. Each of the submitted manuscript should clearly explain and demonstrate the implications in the cyber-physical domain. Papers addressing the problem of security purely at software or hardware level which do not have implication with the cyber-physical domain will not be considered for publication.** Papers highlighting challenges and solutions for connected CPSs used in harsh environment and to monitor critical infrastructures, as well as papers proposing novel methodologies to evaluate, measure and assert the security of CPSs are encouraged. In addition to research articles, we invite papers describing early stage research and state of industrial practice in this area. Wild and crazy ideas, interesting demonstrations in various CPS domains (e.g., manufacturing, transportations, smartgrid, bio-medical/engineering systems, etc.) are particularly encouraged. Perspective authors should submit a 4 pages manuscript describing their contributions. Topics of interest include, but are not limited to, the following:

- Modeling cross-domain CPSs security
- Measuring CPSs security
- Attacking and defending the cyber part of CPSs
- Attacking and defending the physical part of CPSs
- Architectures for secure CPSs
- CPSs security evaluation and validation techniques
- Formal methods for secure CPSs design
- CPSs security and reliability
- CPSs security in harsh environments and in critical applications
- Security performance trade-offs for CPSs
- Lightweight and low energy security for CPSs
- Supply-chain security for cyber-physical systems
- Application-specific CPS security (e.g., bio-logical systems, electro-chemical systems, etc.)

Paper Submission Guidelines

Submitted manuscripts must be four pages or fewer, including all figures, tables, and references. Submissions exceeding this length will be returned without review. Papers should use 7.875 in x 10.75 in (20 cm x 27.30 cm) trim size and the IEEE transactions two-column format in 10-pt. font. In word counts, this corresponds to roughly 2200 words. Further details are available at:
http://ieee-ceda.org/publication/esl-publication/author-guidelines
Submissions to IEEE ESL must consist of original work that has not been previously published and is not currently under review elsewhere. Please upload manuscripts using ScholarOne Manuscript Central at: https://mc.manuscriptcentral.com/les-ieee Authors should select the "Special Issue on Emerging Topics in Secure and Trustworthy Cyber-Physical Systems" when submitting the paper at manuscript central.

Guest Editors

Francesco Regazzoni, ALaRI – USI, Lugano, Switzerland
Arquimedes Canedo, Siemens Corporation, Princeton, NJ, USA
Mohammad Abdullah Al Faruque, University of California Irvine, Irvine, CA, USA

Important Dates

Manuscript submission	February 28, 2018
First round of reviews	April 30, 2018
Second round of reviews	August 30, 2018
Final Manuscript	October 1, 2018