Security and Communication Networks

Special Issue on
Safety and Security Coengineering in Embedded Systems

WILEY | Hindawi

CALL FOR PAPERS

Driven by large-scale scientific, technologic, and socioeconomic developments, virtually any domain of embedded (cyber-physical) systems (ES, CPS) is presently subject to the same megatrends of increasing levels of interconnection and cooperation.

In the automotive domain, future cars will be highly automated and they will cooperate to optimize the overall performance (traffic flow; platooning scenarios, etc.) and to prevent accidents (e.g., warning because of obstacle on the road and general awareness with respect to the driving behavior and plans of the other cars). This opens up diverse security attack vectors and attacks might well be affecting system safety. In the railway domain, there is, for instance, the ETCS system as part of the ERTMS (European Rail Transport Management System) providing high interoperability and standardized communication and control replacing the large number of national train protection systems; vulnerability to attacks would be extremely safety critical. In the manufacturing and process industry domain, highly automated and partially autonomous systems of all kinds are interconnected and controlled, respectively, exchange critical data, where cyberattacks may lead to safety-critical incidents of high impact on people and environment. Our dependency on particularly electric energy leads to the same critical implications in our power grids and other critical infrastructures.

Consequently, in context of such domains of safety-critical embedded systems of systems, we presently see a very high potential in new cooperation-based applications and services, but we also see significant engineering challenges regarding the indispensable assurance of the trustworthiness of the systems. In particular, from a safety perspective, basic assumptions like predictability of system behavior and environment, which are foundational for the state of the practice approaches and established standards, are not sufficient anymore. One reason for that is that the significant increase in communication links (connectivity) and the potential dynamic integration of unsecure systems as well as the reconfiguration in adaptive open systems provide plenty of attack surface from a cybersecurity point of view. However, a safety-critical system that is not secure may also be not sufficiently safe what in turn could have an impact on the question of placing the product in the market. Consequently, safety can no longer be engineered isolated from security and we require new integrated approaches with respect to analysis, engineering, and validation of these important properties over the whole system lifetime.

This special issue aims to address a corresponding range of topics related to the coengineering of cybersecurity and safety in embedded systems (of systems).

Potential topics include but are not limited to the following:

- Safety and security coanalysis (e.g., extended hazard analyses, vulnerability and threat analysis) in embedded systems (of systems)
- Coengineering of safety and security for embedded systems (of systems)
- Safety and security patterns for embedded systems (of systems)
- System architectures for safe and secure embedded systems (of systems)
- Safety and security in open systems of systems (e.g., trustworthiness of third-party systems)
- Integrated risk assessment (i.e., what does the interplay imply with respect to the notion of risk, which is different for functional safety and security)
- Integrated cause-effect analyses
- Software and hardware design aspects for safety and security
- Methods, tools, and techniques for engineering safe and secure embedded systems
- Safety and security measures for embedded systems, conflicts, and synergies
- Verification and validation with respect to safety and security in the context of embedded systems
- Integrated safety and security argumentation and cases for typical domains of embedded systems
- Domain-specific problems and solutions
- Concrete case studies and experience reports
- Standardization, qualification, and certification issues
- Current related developments in standardization

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/secoen/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Daniel Schneider, Fraunhofer IESE, Kaiserslautern, Germany
daniel.schneider@iese.fraunhofer.de

Guest Editors
Jens Braband, Siemens AG, Braunschweig, Germany
jens.braband@siemens.com

Erwin Schoitsch, AIT Austrian Institute of Technologie, Seibersdorf, Austria
erwin.schoitsch@ait.ac.at

Sascha Uhrig, Airbus, Munich, Germany
sascha.uhrig@airbus.com

Stefan Katzenbeisser, TU Darmstadt, Darmstadt, Germany
skatzenbeisser@acm.org

Submission Deadline
Friday, 30 November 2018

Publication Date
April 2019