Journal of Software: Evolution and Process

Special Issue: Security and Safety in Cyber-Physical Systems

The design of modern Cyber-Physical Systems (CPSs) comprises systems of systems that, in turn, include heterogeneous components as subsystems. Manufacturers of such systems have to address several networking, dynamic and uncertain environmental constraints. CPSs are often safety-critical, i.e., any malfunctioning of the system may seriously harm its user. However, the involved communicating peripherals also necessitate the consideration of security issues, so that the proper functioning of a CPS is not affected by cybersecurity threats.

The engineering of a CPS requires high safety integrity levels and strong assurances for their fitness for public use against safety hazards and cybersecurity threats. Considering safety and security requirements in the design of CPSs increases their reliability, confidentiality, integrity and availability. This also ensures the continuous provision and protection of essential services and assets. However, contemporary systems and software engineering methods and approaches are often not adequate for the high-confidence design and manufacturing of CPSs.

The overall aim of this special issue is to address a broad range of issues related to cybersecurity, functional safety and their interplay within the context of CPSs – including but not limited to:

- Model-driven engineering
- Functional safety, cybersecurity and their interplay
- Privacy and confidentiality
- Specification, verification & validation
- System architecture designs, decisions and tradeoffs, e.g., correct-by-design and privacy-by-design
- Artificial intelligence and deep learning approaches
- Regulation, homologation, legalization and certification
- Case studies, experience reports, benchmarking and best practices
- Healthcare, transportation, aerospace, energy, robotics, finance, business, etc.

Guest editors:

- Miklos Biro, Software Competence Center Hagenberg GmbH
- Alexander Egyed, Johannes Kepler University Linz
- Atif Mashkoor, Software Competence Center Hagenberg GmbH
- Johannes Sametinger, Johannes Kepler University Linz

Requirements for submission:

Original, high quality contributions that are not yet published or that are not currently under review by other journals or peer-reviewed conferences are sought. In addition, high-quality papers from "IWCFS'18: 2nd International Workshop on Cybersecurity and Functional Safety in Cyber-Physical Systems" are invited to this special issue, which will need to be significantly updated and extended. Papers invited from IWCFS2018 must have at least 30% new content compared to the original workshop version.

All submissions must conform, at the time of submission, to Wiley formatting guidelines available at the following URL:
https://onlinelibrary.wiley.com/page/journal/20477481/homepage/forauthors.html.

The special issue "**Cybersecurity**" has to be selected in the drop down list on the bottom of the "Step 1: Type, Title, & Abstract" page of the submission process.

Reviewing details:
Both the papers from IWCFS2018 and the independent papers will be peer reviewed by reviewers and selected based on originality, scientific quality and relevance to this special issue. The special issue editors will make final decisions on the acceptance of the papers.

Paper submission deadline: January 15, 2019