

DepDevOps Workshop

Call for Papers

3rd International workshop on Dependable Development-Operation Continuum Methods for Dependable Cyber-Physical Systems

In recent years it has become evident that the use of software to perform critical functions is on the rise. As a result, dependable embedded systems are getting more intelligent and automated. For instance, the automotive industry is a clear witness of this trend, where more and more Advanced Driver-Assistance Services (ADAS) are already embedded in cars. This results in a dramatic increase of software complexity, which also requires hardware platforms with higher computing power. All these trends hinder the safety certification, as it is increasingly difficult to guarantee at design time that system errors are prevented or controlled in such a way that there will be no unreasonable risk associated to the electrical/electronic system component at operation time. These challenges are leading to the need for new development practices that reduce the overall system development time and costs without compromising safety and certification.

The rise of new connection technologies (e.g., 5G) bring new opportunities in terms of the download of frequent software updates of new (improved) releases and sending back operation-time information for fixing bugs and enhance the design. Advances done in new development practices like DevOps have shown effectiveness in software development while reducing overall development costs. The DevOps paradigm aims at having seamless methods for the Design-Operation Continuum of software systems. This paradigm has shown promising results in different domains, including web and mobile engineering. Its practices can bring several advantages to dependable CPSs, including bug fixing based on operational data, the inclusion of new functionalities, etc.

However, in the context of dependable CPSs, several challenges arise, requiring DevOps paradigms to have adaptations from several perspectives: the environment in which the CPS operates needs to be considered when updating the software, dependability of software needs to be ensured to a certain level, software fault might lead to severe damages, etc. Furthermore, the safety-critical industry has well established safety-lifecycles dictated by safety standards and adopting the DevOps paradigm has several open research challenges.

The Dep-DevOps workshop explores innovative solutions towards the adoption of DevOps in the safety-critical domain, considering all software and hardware aspects from system specification and design up to its verification and validation considering continuous software deployment and monitoring features as well as the certification.

Topics of Interest

Contributions are sought in (but not limited to) the following topics:

- Safe and secure continuous deployment of software updates for CPSs
- Over the air software updates of CPSs
- Runtime verification methods of CPSs
- Assurance and certification of DevOps methodologies for CPSs
- Runtime monitoring on complex high-performance/heterogeneous platforms
- Secure data transmission
- Traceability between operational data with development data
- Automated methodologies for testing, verification and validation of CPSs

Important dates

Full paper submission: **9 May 2022**

Notification of acceptance: **31 May 2022**

Camera-ready submission: **18 June 2022**

Workshop: **6 September 2022**

Submission Guidelines

All papers will be reviewed by at least three members of the Program Committee. Papers must not have been previously published or concurrently submitted elsewhere. Accepted articles will be published by Springer in the LNCS Series. All paper submissions must be formatted according to the [LNCS templates provided by Springer](#).

Papers (6 - 12 pages) will be reviewed by at least three reviewers.

Manuscripts must be submitted as PDF files via EasyChair online submission system:

<https://easychair.org/my/conference?conf=safecom22>

ORGANIZING COMMITTEE

- Miren Illarramendi (Mondragon University)
- Aitor Arrieta (Mondragon University)
- Irune Agirre (IKERLAN)

CONTACT

- Miren Illarramendi (millarramendi@mondragon.edu)
- Irune Agirre (iagirre@ikerlan.es)

The organization of this workshop is supported by EU funded H2020 [ADEPNESS](#) and [UP2DATE](#) projects under grant agreement no. 871319 and no. 871465 respectively.

