5th Workshop on

# Security and Dependabilty of Critical Embedded Real-Time Systems

https://certs2022.di.fc.ul.pt

Co-located with 43rd IEEE Real-Time Systems Symposium

Houston, Texas, USA

## Workshop Organizers

**Antonio Casimiro**
Faculdade de Ciências
Universidade de Lisboa

**Marcus Völp**
Interdisciplinary Center for Security, Reliability and Trust
University of Luxembourg

## Important Dates

**Submission Deadline**
October 3, 2022 (AOE)

**Notification of acceptance**
October 10, 2022

**Camera ready deadline**
October 24, 2022

**Workshop**
December 5, 2022

## Submission site

https://easychair.org/conferences/?conf=certs2022

## Call for Papers

At their heart, many critical systems and system infrastructures are composed of real-time and embedded systems (RTES). For example, RTES control our power grids, maintain our smart homes, steer our vehicles or they host the software in road-side units that allow our vehicles to drive more safely and more efficiently. For sure, they will open the way to even more challenging applications, such as in autonomous and cooperating vehicles, terrestrial or aerial. However, most of these RTES are distributed and networked, which makes them vulnerable to accidental faults, targeted attacks, and advanced and persistent threats. Worse, compromise of a few nodes may bring down the entire system, in particular if attacks persist.

The grand challenges brought in by these scenarios include ensuring continuous unmaintained operation under faults and attacks. Systems may possibly utilize easier to upgrade computation resources in mobile phones or road side units whose trustworthiness needs to be established while the RTES approaches these units. And while attackers may try to compromise the RTES' functionality or timing, we seek to protect the integrity and timeliness of systems and the privacy of their users. Mastering these challenges requires the expertise of several research areas, and so, the goal of this workshop is to bring together researchers and engineers from the security and dependability, distributed systems and real-time communities, in order to discuss and promote new and exciting research ideas and initiatives, and to identify and discuss the challenges that lie ahead for such critical applications. Additionally, new artificial-intelligence-based sensing, control, and decisions introduces new challenges in real-time guarantees, dependability and security threats.

CERTS'22 aims to bring together researchers and practitioners from the security, dependability and real-time domain in a highly interactive workshop to discuss such challenges.

**Topics of interest** include, but are not limited to:

- Security and dependability of cyber-physical and other real-time and embedded systems,
- Vulnerabilities and protective measures of CPS infrastructure,
- Fault and intrusion tolerant distributed real-time systems,
- Confidentiality and privacy in real-time and embedded systems,
- System architectures encompassing combinations of distribution, security, dependability and timeliness, and
- Threats and vulnerabilities due to the use of artificial intelligence techniques
- AI and ML in and for security and dependability in real-time systems

**Submission format:** extended abstracts (~2 pages) plus a poster (1 page). More details on the webpage: https://certs2022.di.fc.ul.pt

## Program Committee

to be announced