



**15<sup>th</sup> Advanced Doctoral Conference on Computing, Electrical and Industrial Systems**  
Caparica, Portugal – 3-5 July 2024  
**Technological Innovation for Human-Centric Systems**

## **Special Session on Security Issues in Cyber-Physical Systems**

### **Scope**

Cyber-Physical Systems (CPSs) effectively interconnect cyber and physical (sub)systems that exchange data and other sensitive information in a real-time by using modern sensor, computing, and network technologies. By sensing the surrounding environment, these systems are able to adapt and control the physical world around us. Their application potential is endless, being already embedded in systems such as power transmission, communication, agricultural/ecological, military, and autonomous systems (drones, robotics, autonomous cars, etc.), medical care domains (to enhance the medical services), supply chain management (to enable eco-friendly, transient, cost efficient, and safe manufacturing process), and many others, nowadays.

Regardless of the abundant benefits they offer, CPSs are susceptible to various cyber and/or physical security threats, attacks, and challenges. This is mostly owed to their heterogeneous nature, reliance on private and sensitive data, and their large-scale deployment. As such, accidental or intentional attacks (like economical, criminal, military, espionage, political, and terrorism, to name a few) can result into disastrous consequences with possible casualties. This poses many new challenges for digital forensics analysts, academics, law enforcement agencies (LEAs), and security professionals. Therefore, this special session aims to identify the main CPS security threats, vulnerabilities, and attacks, to discuss the advantages and limitations of the existing security solutions and to address these concerns and explore cutting-edge security methods through strategic and technical perspectives, without leading to unacceptable network overhead, especially in terms of latency.

### **Session organizers**

- Marko Beko (IST + COPELABS)
- Slavisa Tomic (UL-CUL + COPELABS)
- Nuno Mateus Coelho (UL-CUP + COPELABS)

### **Topics / Keywords**

- Anonymization in CPS
- Applications of AI and ML in CPSs security
- Age of information (Aol) to enhance security in CPSs
- Attack detection for CPS
- Autonomous vehicle security
- Big data and cybersecurity
- Cloud Security
- Cyber forensics
- Cybersecurity and cyber resilience
- Data security and privacy for CPS
- Digital Privacy
- Ethical and legal considerations
- Network security
- Secure Positioning
- Threat models for CPS
- Trustworthiness evaluation in CPSs and IoT networks

### **Submission procedure**

Special sessions are included in the main Conference and follow the same reviewing process.

- Short abstracts submission (100-150 words): 2 Feb 2024
- Full papers submission: 1 Mar 2024
- Acceptance Notice: 15 Apr 2024
- Final version Submission: 26 Apr 2024

Acceptance of papers is based on the full paper (up to 12 pages). Each paper will be evaluated by three members of the International Program Committee. Being DoCEIS a doctoral conference, the first author of each paper must be a PhD student.

When submitting on the web site, you should indicate the name of the special session. Submission procedure via EasyChair available on: <https://doceis.dee.fct.unl.pt/>, with copy by email to the chairs of the special session.