



Cyber-Physical Security for Critical Infrastructures

Guest Editors:

Prof. Dr. Isabel Praça

Prof. Dr. Silvio Ranise

Dr. Luca Verderame

Dr. Habtamu Abie

Deadline for manuscript
submissions:

closed (30 September 2022)

Message from the Guest Editors

Because of the increasing interconnection between the digital and physical worlds, these infrastructures and services are more critical, sophisticated, and interconnected than ever before. This makes them increasingly vulnerable to attacks, as confirmed by the steady rise of cyber-security incidents such as phishing or ransomware, but also cyber-physical incidents, such as the physical violation of devices or facilities in conjunction with malicious cyber activities. To address all these challenges, this Special Issue has the objective of bringing together security researchers and practitioners from the various verticals of critical infrastructures (e.g., the financial, energy, health, air transport, communication, gas and water domains) to rethink cyber-physical security in light of the latest technological developments (e.g., cloud computing, blockchain, big data, AI, internet-of-things (IoT)).

- critical infrastructures
- cyber-physical security
- collaborative risk assessment
- predictive security

