Call for Papers

Important dates

Paper submission deadline:
April 13, 2026
Authors' notification:
May 4, 2026
Camera-ready submission:
May 25, 2026
Registration deadline (authors):
May 25, 2026
Workshop dates:
August 3–5, 2026

Workshop chairs

Panagiotis Radoglou-Grammatikis (GR)
Panagiotis Sarigiannidis (GR)

Organizing committee

Panagiotis Radoglou-Grammatikis (GR)
Panagiotis Sarigiannidis (GR)
Thomas Lagkas (GR)
Vasilios Argyriou (UK)
Dimitrios Pliatsios (GR)
Anna Triantafyllou (GR)

Technical program committee

Wissam Mallouli (FR)
Erkuden Rios (ES)
Eider Iturbe (ES)
Phu Nguyen (NO)
Evangelos Markakis (GR)
George Amponis (BG)
Aristeidis Farao (GR)
Igor Kotsiuba (UK)

Publicity chairs

Panagiotis Radoglou-Grammatikis (GR)

Contact us

psarigiannidis@uowm.gr
pradoglou@uowm.gr

The smart technologies digitise the conventional model of the Electrical Power and Energy Systems (EPES) into a new architectural paradigm, known as the Smart Grid (SG), thus introducing multiple services, such as two-way communication, pervasive control and self-healing. However, despite the benefits, this progression leads to challenging cybersecurity issues due to the vulnerabilities of the new technologies and the necessary presence of legacy and insecure systems, such as Supervisory Control and Data Acquisition (SCADA) / Industrial Control Systems (ICS). On the other side, anticipating the critical issues of EPES/SG, both academia and industry have developed appropriate countermeasures, considering the advances in the Artificial Intelligence (AI) and the networking domains. AI and especially Machine Learning (ML) and Deep Learning (DL) allow the implementation of detection mechanisms capable of discriminating malicious behaviours as well as zero-day vulnerabilities. Emerging solutions in this sector include Security Information and Event Management (SIEM) systems and Intrusion Detection and Prevention Systems (IDPS). Other emblematic technologies that can mitigate or even prevent cyberattacks are honeypots, Software-Defined Networking (SDN), Network Function Virtualisation (NFV) and intentional islanding. The workshop focuses on high-quality applied research and innovation results that are obtained from projects (project workshops). The workshop will be held in conjunction with the IEEE CSR 2026 conference as a **physical event**, during August 3–5, 2026. Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- Agentic AI for cybersecurity in EPES/SG
- AI-powered cybersecurity in EPES/SG
- Quantum-resilient security mechanisms in EPES/SG
- Sophisticated security orchestration in EPES/SG
- SDN/NFV-based architectures for resilient EPES/SG
- Threat intelligence mechanisms in EPES/SG
- Threat correlation, prioritization and mitigation mechanisms in EPES/SG
- Federated intrusion/anomaly detection and mitigation in EPES/SG
- Business continuity in EPES/SG
- EPES/SG honeypots, honeynets and digital twins
- Self-healing mechanisms in EPES/SG
- Risk assessment, threat modelling and vulnerability analysis in EPES/SG
- AR/VR cybersecurity training, evaluation and certification in EPES/SG

The CSR 2026 workshop will accept high-quality research papers presenting strong theoretical contributions, applied research and innovation results obtained from funded cyber-security and resilience projects, and industrial papers that promote contributions on technology development and contemporary implementations.

Submitted manuscripts should not exceed 6 pages (plus 2 extra pages, being subject to overlength page charges) and should be of sufficient detail to be evaluated by expert reviewers in the field. Accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore's scope and quality requirements. Detailed information about paper submission and guidelines for authors can be found at the workshop's website `https://www.ieee-csr.org/acronym`.

Supported by

The EPES SPR workshop is supported by the following EU-funded projects: XTRUST-6G, SECASSURED, CIRCAT