

CALL FOR PAPERS

SPECIAL SESSION ON

Trustworthy and Resilient AI for Cyber-Physical Systems: Security, Anomaly Detection, and Intelligent Diagnosis

for ICCAD 2027

July 6-8, 2027, Paris, France

Session Co-Chairs:

Dr. Loubna Ali, Faculty of Computer Science and informatics, BSBI, Berlin Germany.

Loubna.ali@berlinsbi.com

Session description:

Modern cyber-physical systems (CPS) integrate intelligent algorithms, industrial networks, sensors, and control processes. While AI enhances monitoring and automation, CPS remain exposed to cyberattacks, sensor manipulation, unexpected operating conditions, and equipment faults. These challenges raise critical questions about the security, robustness, and interpretability of AI-assisted control and diagnosis.

This special session addresses trustworthy and resilient AI for CPS, emphasizing reliable detection, discrimination, and diagnosis of cyberattacks and physical faults, as well as the operational consequences of incorrect or compromised AI decisions.

Contributions are encouraged from AI, cybersecurity, industrial IoT, control engineering, and intelligent fault diagnosis, including theoretical advances, reproducible benchmarks, simulations, and industrial case studies.

The goal is to foster interdisciplinary research on AI techniques that are accurate, explainable, robust to disturbances and adversarial manipulation, and practical for industrial monitoring and control.

The session aims to advance anomaly and fault diagnosis, attack-aware decision-making, uncertainty estimation, and resilient operation in interconnected industrial systems.

We particularly welcome rigorous experimental evaluations using public CPS benchmarks and realistic testbeds, including SWaT, HAI, WADI, Tennessee Eastman, and other relevant datasets.

The topics of interest include, but are not limited to:

- Trustworthy, explainable, and uncertainty-aware AI for CPS
- Machine/deep learning for anomaly detection and intelligent fault diagnosis
- Industrial intrusion detection and cyberattack–fault discrimination

• Adversarial robustness, secure learning, and attack-aware diagnosis

•Federated and privacy-preserving learning for industrial IoT
•Digital twins and physics-informed AI for monitoring and diagnosis
•Graph neural networks and causal models for fault/attack localization
• Resilient control, recovery, and safe decision-making under disturbances

•Edge AI and real-time detection in resource-constrained industrial systems
•Domain adaptation, generalization, and concept drift in CPS
• Benchmarking, reproducibility, datasets, and industrial case studies

---

SUBMISSION

Papers must be submitted electronically for peer review by: **January 31, 2027**
https://www.iccad-conf.com/submission/

All papers must be written in English and should describe original work. The length of the paper is limited to a maximum of 6 pages (in the standard IEEE conference double column format).