Workshop Proposal - ICFT 2026

Trustworthy and Secure AI for Critical Infrastructure:

From Vulnerability Detection to Resilient Deployment

Proposed Workshop at the International Conference on Future Technologies (ICFT 2026)
German Jordanian University (GJU), Amman, Jordan | 18-22 October 2026

Workshop Chairs
1) Dr.-Ing. Loui Al Sardy - Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany
2) Prof. Andrea Ceccarelli - University of Florence, Italy
3) Dr.-Ing. Uwe Koser - AUDI AG Ingolstadt, Germany (Lecturer at FAU Erlangen-Nürnberg)

---

1. Motivation

Artificial Intelligence (AI) is increasingly embedded in critical infrastructure systems, including smart grids, industrial automation, assisted and autonomous driving, healthcare platforms, transportation networks, and intelligent energy systems. While AI enhances efficiency, predictive capability, and automation, its integration into safety- and mission-critical environments introduces new cybersecurity risks and expands the system attack surface.

Recent studies reveal that AI frameworks and open-source model ecosystems may contain exploitable software vulnerabilities, including memory corruption flaws, unsafe deserialisation, concurrency defects, model manipulation, model poisoning, and supply-chain weaknesses. In particular, large-scale analyses of AI repositories demonstrate a significant presence of high-severity vulnerabilities in foundational AI libraries and dependencies. Such weaknesses can propagate across forked repositories and deployed systems, thereby amplifying systemic risk.

Given ICFT 2026's focus on advancing future technologies and real-world applications, this workshop addresses the urgent need for systematic approaches to secure, verify, and govern AI systems in critical infrastructure and data base contexts.

2. Objectives

The workshop aims to:

- Investigate software-level vulnerabilities in AI-enabled systems.
- Analyse AI supply-chain risks in open-source ecosystems.
- Explore formal, static, dynamic, and heuristic techniques for vulnerability detection.
- Adresses the trustworthiness of AI generated terms
- Discuss regulatory alignment (e.g., EU AI Act, NIS2, IEC 62443) for AI deployment.
- Promote secure-by-design and trustworthy AI lifecycle engineering.
- Foster collaboration between AI researchers, cybersecurity experts, and infrastructure engineers and application practioners.

3. Topics of Interest

The workshop welcomes original research papers, industrial case studies, and position contributions related to:

- Vulnerability detection in AI frameworks (buffer overflows, race conditions, unsafe memory usage)
- Static and dynamic security analysis of AI codebases
- Fuzzing and constraint-guided testing approaches for AI systems
- Security assessment of AI model hubs and repository ecosystems
- Vulnerability propagation across forked repositories
- AI security in smart grids and intelligent energy systems
- Resilient AI in embedded and cyber-physical systems
- Secure AI lifecycle management and certification
- Governance and regulatory frameworks for trustworthy AI

4. Format

Duration: Half-day (or less if required by ICFT scheduling)
Structure (The workshop could include**):**

- 1 invited keynote
- 6-8 peer-reviewed paper presentations
- Panel discussion: *"Can AI in Critical Infrastructure Ever Be Considered Secure?"*
- Open technical discussion session

The workshop will be organised in hybrid format (physical + virtual participation).

5. Relevance to ICFT 2026

This workshop directly aligns with ICFT Tracks:

- Track 1: Artificial Intelligence, Machine Learning & Big Data
- Track 2: IoT, Embedded Systems & Cybersecurity
- Track 6: Smart Grids, Electrification & Intelligent Energy Systems

By bridging AI innovation with cybersecurity engineering and infrastructure resilience, the workshop supports ICFT's mission to connect breakthrough technologies with real-world impact.

6. Target Audience

- AI and machine learning researchers
- Cybersecurity and software engineering experts
- Smart grid and energy system engineers
- Embedded systems developers
- Industry practitioners and regulatory stakeholders

Expected Outcome:

The workshop will establish a focused research dialogue on secure AI deployment in critical infrastructure, stimulate interdisciplinary collaboration, and lay foundations for future international research initiatives.

Al Sardy Bio:

Loui Al Sardy is an Assistant Professor and Head of Network Security Group at the Lab of Computer Networks and Communication Systems. He holds a master's degree in Software Engineering for Industrial Applications from Hof University of Applied Sciences and a bachelor's degree in Electrical Engineering from the University of Jordan. Before his current position, he worked as a Research Associate at the Chair of Software Engineering, where he contributed to advancing IT security and software testing between 2016 and 2023. His research has been part of major projects such as SMARTEST and SMARTEST2, focusing on enhancing the security of software-based control systems for nuclear power plants. Since June 2021, Loui has also been the Co-Founder and COO of Sakundi, a blockchain cybersecurity startup dedicated to securing blockchain solutions through AI and automation. Beyond academia and entrepreneurship, Loui actively contributes to professional and community development. He serves as the Committee Leader of the Jordanian Engineers Liaison Committee in Germany, is a member of (ISC)², a certified trainer with Human REstart, and participates in various international professional organizations, reflecting his ongoing commitment to innovation, education, and leadership in the field of cybersecurity.

Ceccarelli Bio:

Andrea Ceccarelli is an Associate Professor of computer science with the University of Florence. His research interests include the design, monitoring, and evaluation of dependable and secure systems, with a preference for experimental approaches, and his scientific activities originated more than 140 papers. He is regularly involved in the TPC of International Conferences in the domain of dependability and reliability engineering, and he has been the TPC CoChair of SafeComp, SRDS and LADC. He has been involved in multiple research projects and he led his unit in the MUR projects BREADCRUMBS, FLEGREA and the Regional Progject POR CREO WAU and SPACE. From 2009 until 2025, he has been a member of Resiltech, an ex-academic Spinoff of the University of Florence. He is a member of the IFIP WG 10.4 on "Dependable Computing and Fault-Tolerance. He has regular interactions with companies especially in the domain of safety critical systems, for research collaborations and to provide training courses on dependability, safety, quality and safety standards for electrotechnical systems. He has been a visiting researcher at the University of Coimbra (Portugal), Critical Software SA (Portugal), Universitade Estadual de Campinas (Brasil), Universitade Federal de Alagoas (Brasil).

Koser Bio:

Dr.-Ing. Uwe Koser is a manager and senior product analyst at AUDI AG Ingolstadt. He holds a PhD in air and space engineering from the Technical University Stuttgart, Germany. Before his current position, he worked as a research associate at the German Air and Space Research Institute, DLR, Stuttgart. He joined Audi as a testing engineer, changing to concept development, innovation management and the management of research cooperations between Audi and outstanding technical Universities in Germany, Hungary and the US. He was the founder of the Audi chair for automobile production technology at the Széchenyi University in Györ, Hungary, before returning to Germany again as the leader of the Audi Accident Research Unit within the department of Product Analysis. He is a longtime lecturer on the future of automobile technology at the Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany.