Integrated Project
Cyber security of energy systems for the digital-energy transition

9 february 2026 h14:30

Faculty of Engineering and Architecture, Piazza d'Armi, Cagliari

Digitalization is a key element of the energy transition: it enables electricity, gas, hydrogen, water, and heat networks to communicate with each other and with producers, energy communities, charging infrastructure, and aggregators, improving efficiency, flexibility, and the integration of renewables. This growing interconnection, however, also increases exposure to cyber risks: cyber attacks, IoT device vulnerabilities, and data privacy issues. Digitalization enables the transition but makes the energy system a critical infrastructure that requires robust defenses across all its components. Energy system security must protect cyber-physical infrastructures by adopting advanced prevention, detection, and response measures. The *Integrated Project Cyber security of energy systems for the digital-energy transition* involves the three Italian research entities, RSE, ENEA, and CNR (and the universities co-beneficiaries of ENEA and CNR), in achieving the priority objective "Digitalization and evolution of networks" of the 2025-2027 Three-year Research Plan (dm_388_06-11-2024). The project aims to ensure the protection of digital data and processes in line with the Italian **Energy National Plan 2030**, the **European NIS2 Directive**, its implementation in **Legislative Decree 2024/138**, and the guidelines for the implementation of security measures issued by the **National Cybersecurity Agency**. The project's main actions are:

- **Protection of information exchanges** for the monitoring and control of energy networks and plants.
- **Adoption of international standards** based on cryptography and public key and digital certificate management infrastructures.
- **Preparation to quantum computing**, with algorithms resistant to quantum attacks and the use of quantum keys.
- **Development of innovative anomaly detection platforms**, based on artificial intelligence and anonymization techniques to ensure privacy.
- **Testing for compliance** to cybersecurity standards in digital laboratories and experimental energy infrastructures, using physical and virtualized architectures.

- **Digital twins** to simulate attack scenarios and evaluate the effectiveness of defense measures in reducing their impact on energy processes.

The activities benefit from research collaborations with stakeholders to accelerate the technological transfer and time to market of digital identity and cybersecurity certification services, certified energy control devices and their deployment in energy infrastructures. Thanks to numerous academic contacts, the project pays specific attention to cybersecurity **training** through internships, theses, doctoral scholarships, seminars, and lectures within the framework of bachelor's and master's degree programs.

Program

Agenda	Entity	Speaker
Integrated Project Cyber security of energy systems for the digital-energy	RSE	G. Dondossola
Securing the Power Grid: Strategic Methodologies and Technical Solutions	ENEA	M. Valenti
An integrated framework for evaluating standard-based and quantum-safe cybersecurity solutions for electrical energy applications	RSE	M.G. Todeschini
Power Consumption Anomaly Detection Using Threat-Driven Data Injection	UniFI	T. Zoppi
Design of cybersecurity twins based on ICT-power co-simulation	RSE	R. Terruggia
Damn Vulnerable Infrastructure: are you ready for the next StuxNet	IMT-Lucca	G. Costa
AI-based techniques and tools for cybersecurity energy ranges	RSE	R. Terruggia
Attack scenarios to charging infrastructure communications	UniCA	L. Pisu
A method for smart grid intrusion detection through explainable deep learning	CNR	G. Ciaramella

The registration information can be found at Registration - ITASEC.