AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

SECURING THE ENERGY SECTOR: STRATEGIES FOR BUILDING RESILIENCE AGAINST CYBER ATTACKS

International Digital Security Forum; Vienna, 21st September 2023

Francesca Soro
francesca.soro@ait.ac.at

RESILIENCE FOR FUTURE ENERGY SYSTEMS

- What is resilience?

  Resilience is the ability of a system to detect and predict disruptive events, respond by securely transitioning to a stable (sub-optimal) operation point, and take appropriate measures for fast recovery to a desired normal operation mode”

- Resilience of future digitalized energy systems can only be promised if a cyber-physical view is taken

MAIN GOALS

- Resilience engineering support
  - Support system operators to optimally design, plan, and evaluate cyber-physical system architectures
  - Contributions: **optimal scheduling tool** for planning of resilient architectures and an **AI-based analysis tool** for evaluation of attacker/defender strategies
- Implementing resilient applications
  - Rapid implementation and validation solution, which can significantly reduce the time-to-market of new strategies
  - Contributions: toolkit for **resilient integration of applications** and a **rapid validation framework** based on digital twins
- Resilience runtime support
  - Proposal of a runtime support system, which will be able to suggest, and execute, actions (physical and cyber actions) that will recover a system back to a normal state
  - Contributions: **incident and anomaly detection system** with root cause analysis, new methods for **consolidation of sensor data**, and **resilient operation strategies** based on AI-analysis

CHALLENGES AND OPEN QUESTIONS

- What system architectures can promise resilience for future scenarios?
- How to design and implement resilient applications?
- How to integrate resilient operation in the existing energy systems?
- **How to take into account the human factor and unpredictable events?**