"Cybersecurity Trends and Challenges in Electrical Power and Energy Systems (EPES)"

Prof. Grigore Stamatescu
University Politehnica of Bucharest and TÜV Austria Romania

Accelerated adoption of modern automation technology in Electrical Power and Energy Systems (EPES) represents a key factor supporting the energy transition and ensuring a safe, reliable and clean energy supply. This allows for timely data collection, online monitoring and low-latency and robust control loops that enable flexible operation of the grid at the generation, transmission, distribution and consumer levels. Under the new Industrial Internet of Things and Cyber-Physical (Energy) Systems paradigms, new edge devices, such as smart meters, PLCs and RTUs, are entrusted with complex computing, communication and control tasks, in heterogeneous environments. Against a long list of benefits, this type of networked interoperability of previous isolated subsystems has however opened them up to multiple threats and vulnerabilities in a dynamic cybersecurity landscape.

The talk focuses on key technical challenges which are identified with regard to safeguarding EPES automation from a cybersecurity perspective. These relate to confidentiality, integrity and authenticity attacks, availability of the EPES entities and subsystems, up to coordinated cyber attacks, denoted as Advanced Persistent Threats (APTs). Privacy concerns are also of interest when handling large scale consumer data whereas new privacy-preserving algorithms can contribute to their protection while allowing efficient information extraction as is the case with state-of-the-art federated learning frameworks.

Further examples are provided with regard to the following topics:

- Upgrading legacy industrial communication protocols e.g. ModBus, for increased robustness to cyber attacks;
- Designing reliable anomaly detection and intrusion detection schemes, implemented at the ICS/SCADA layers;
- Mitigating false data injection targeting advanced algorithms and DS/ML/DL pipelines.

In complementary fashion, an overview of the applicable certification, standardization and regulatory frameworks will also be carried out. This includes by is not limited to the Network and Information (NIS) directive and the EU Cybersecurity act, relevant recommendations from the European Union Agency for Cybersecurity (ENISA) and national regulations, covering hardware, software and human factors alike. In particular, personnel (re-)training is seen as a stepping stone in assuring the effectiveness of enterprise cybersecurity policies and measures in EPES.

Early results in this area from the „rEsilient and seLf-healed EleCTRical pOwer Nanogrid" (ELECTRON) Horizon 2020 joint research and innovation project will also be discussed.