Cyber-physical power system security: Modeling, attack detection, assessment and testing platforms, and digital twins' solutions.

Undoubtedly, the operation of power systems has been improved through proper integration and management of renewables, advanced control/protection schemes, and reliable communication systems. However, due to their heavy reliance on digital communication and control, the power system became a Cyber-Physical Power System (CPPS), and consequently more vulnerable to cyberattacks. Therefore, understanding the intricate interplay between the cyber and physical domains and the potential effects on the power system control and protection of successful attacks is essential and will be presented in this tutorial. The power system protection and automation principles will be covered in this tutorial, with more focus on the communication-based protection schemes.

In addition, for cybersecurity experimentation and impact analysis, developing a comprehensive testbed is needed. Therefore, a state-of-the-art Hybrid Physical Co-simulation smart grid testbed at FIU developed for in-depth studies on the impact of communication issues and cyber-attacks on the grid was implemented. The infrastructure and implementation of this testbed will be covered in this tutorial including device configuration, functions programming, and testing scenarios. In this tutorial, two types of testbeds will be provided: (1) Hardware Physical testbed with cyber-physical different layers and hardware/software set-up and configuration, and (2) Co-simulation testbed using real-time power system simulator and communication network emulator. Different types of attacks will be presented including Denial-of-service attack (DoS), Data Manipulation attack (DM), Setting Change attack, and Man-in-the-Middle attack (MitM).

Furthermore, the need for enhanced security in power systems becomes evident when considering real-world incidents that have disrupted these systems and exposed their vulnerabilities. A real-time specification-based NIDS is introduced to tackle the security challenges. Compared to existing solutions, the designed NIDS is highly specialized, focusing on ensuring the correct operation and security of GOOSE/SV messages. It can detect any deviations from the expected semantics, helping identify anomalies or potential security threats. Therefore, we will show the impact of modeled cyber threats on power grid substations and the performance of a developed real-time NIDS. To this aim, different modeled cyber-attacks will be discussed. In addition, the proposed real-time network intrusion detection system for the detection of attacks targeting industrial standards, particularly GOOSE/SV messages will be discussed. Various test cases will be examined to validate the proposed NIDS.

Nowadays, the Digital Twin (DT) technology as an integrated solution for different applications is becoming more widespread. In the context of power system applications, this will give the ability to enhance the power system operation by implementing advanced and innovative techniques to detect and mitigate physical events and cyber events that target communication-based control and protection schemes. Therefore, the basic principles of the design and implementation of Digital Twin will be presented, along with a case study of the recently patented cloud DT for networked microgrids' resiliency against cyber-attacks. Also, proposing DT solutions to deal with the cyber-attack targeting the protection schemes will be covered in this tutorial, and special emphasis will be given to the communication-based protection schemes.