OPAL-RT TECHNOLOGIES

Technical Papers

Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies

Authors: IOANNIS ZOGRAFOPOULOS , (Graduate Student Member, IEEE),
JUAN OSPINA , (Member, IEEE), XIAORUI LIU , (Student Member, IEEE),
AND CHARALAMBOS KONSTANTINOU , (Senior Member, IEEE)

Abstract:

Cyber-physical systems (CPS) are interconnected architectures that employ analog and digital components as well as communication and computational resources for their operation and interaction with the physical environment. CPS constitute the backbone of enterprise (e.g., smart cities), industrial (e.g., smart manufacturing), and critical infrastructure (e.g., energy systems). Thus, their vital importance, interoperability, and plurality of computing devices make them prominent targets for malicious attacks aiming to disrupt their operations. Attacks targeting cyber-physical energy systems (CPES), given their mission-critical nature within the power grid infrastructure, can lead to disastrous consequences. The security of CPES can be enhanced by leveraging testbed capabilities in order to replicate and understand power systems operating conditions, discover vulnerabilities, develop security countermeasures, and evaluate grid operation under fault-induced or maliciously constructed scenarios. Adequately modeling and reproducing the behavior of CPS could be a challenging task. In this paper, we provide a comprehensive overview of the CPS security landscape with an emphasis on CPES. Specifically, we demonstrate a threat modeling methodology to accurately represent the CPS elements, their interdependencies, as well as the possible attack entry points and system vulnerabilities. Leveraging the threat model formulation, we present a CPS framework designed to delineate the hardware, software, and modeling resources required to simulate the CPS and construct high-fidelity models that can be used to evaluate the system's performance under adverse scenarios. The system performance is assessed using scenario-specific metrics, while risk assessment enables the system vulnerability prioritization factoring the impact on the system operation. The overarching framework for modeling, simulating, assessing, and mitigating attacks in a CPS is illustrated using four representative attack scenarios targeting CPES. The key objective of this paper is to demonstrate a step-by-step process that can be used to enact in-depth cybersecurity analyses, thus leading to more resilient and secure CPS