

Preliminary Modeling of Cyber Attackers in Microgrids: An Agent-Based and System Dynamics Approach Enhanced with Statecharts

Jose Gonzalez-de-Durana

University of the Basque Country
Basque Country, Spain

Luis Rabelo and Juan Pablo Zamora-Aguas

University of Central Florida
Orlando FL, USA

Cristian Rincon-Guio

Corporación Universitaria Minuto de Dios – UNIMINUTO
Bogotá, Colombia
luis.rabelo@ucf.edu

Abstract

Microgrids significantly enhance the resilience and sustainability of modern energy infrastructures; however, they are increasingly vulnerable to cyber threats due to their dependence on interconnected digital systems. This preliminary work proposes a hybrid simulation framework that combines System Dynamics (SD) and Agent-Based Simulation (ABS), with a particular focus on incorporating statechart models to effectively represent cyber attackers. The SD component captures macro-level interactions and strategic responses to long-term cybersecurity risks, while the ABS component utilizes statecharts to encapsulate detailed attacker behaviors within agents, allowing for granular modeling of cyberattacks, such as ARP spoofing and smart meter data manipulation. By explicitly modeling the progression of cyber threats through distinct attack phases, the statechart-driven ABS approach provides clarity in understanding threat dynamics, improving the capability to simulate realistic scenarios. A preliminary case study demonstrates the framework's potential for analyzing cybersecurity vulnerabilities, optimizing mitigation strategies, and evaluating defensive tactics within Internet of Things (IoT)- enabled microgrids. The results indicate promising directions for future refinement and full-scale implementation of the framework to enhance cybersecurity management and operational resilience of microgrid systems.

Keywords

System Dynamics, Agent-Based Simulation, Microgrids, Cybersecurity, Statecharts, Cyber Kill Chain, SysML