293

Regulation Compliant Co-Simulation Platform for German Smart Grids

Julian Behrensen[1,2], Sascha Kaven[3], Julian Britz[3], Felix Scholl[3]
[1]TH-Lübeck, Lübeck, Germany. [2]University of Lübeck, Lübeck, Germany. [3]HAW Hamburg, Hamburg, Germany

Extended Abstract

Download file

Abstract Summary

In this extended abstract we present a regulation compliant co simulation platform for German smart grids focused on the low voltage level. The motivation is that increasing renewable generation, decentralised prosumers and flexible loads (EVs, heat pumps) strain traditional grids and require digitally monitored, controllable distribution networks. The German rollout relies on intelligent metering systems with Smart Meter Gateways (SMGWs) governed by the Messstellenbetriebsgesetz and the BSI TR 03109 guideline family. The platform is explicitly designed to reflect this architecture. It couples three simulators via the mosaik framework. Pandapower is used for power flow and grid analysis using SimBench LV benchmark networks, rettij as a Kubernetes based ICT network simulator using the Linux network stack, and custom Python/socket based communication components that implement SMGW centric data flows. This enables joint study of power system dynamics, communication behaviour and higher level control or attack scenarios, including blackout situations and known cyberattacks. The planned evaluation builds on our prior STRIDE style threat modelling for TR 03109 and §14a EnWG control chains, using the co simulation to test which theoretically identified attack vectors are practically exploitable and to quantify their impact on both information and communication technology and power domains. The platform is intended to be released as open source, providing utilities, vendors and regulators with a reusable, realistic testbed for benchmarking control strategies and security mechanisms.

Presenting Author Biography

Sascha Kaven ist Doktorand und wissenschaftlicher Mitarbeiter an der HAW Hamburg. Seine Forschung konzentriert sich auf Cybersicherheit in intelligenten Energiesystemen, insbesondere auf die Erkennung und Abwehr von Angriffen in Smart Grids sowie auf simulationsbasierte Ansätze zur Bewertung der Systemsicherheit.