Cybersecurity Assessment in DER-rich Distribution Operations: Criticality Levels and Impact Analysis

Manisha Maharjan, Shiva Poudel, Scott R. Mix, and Thomas E. McDermott

Introduction

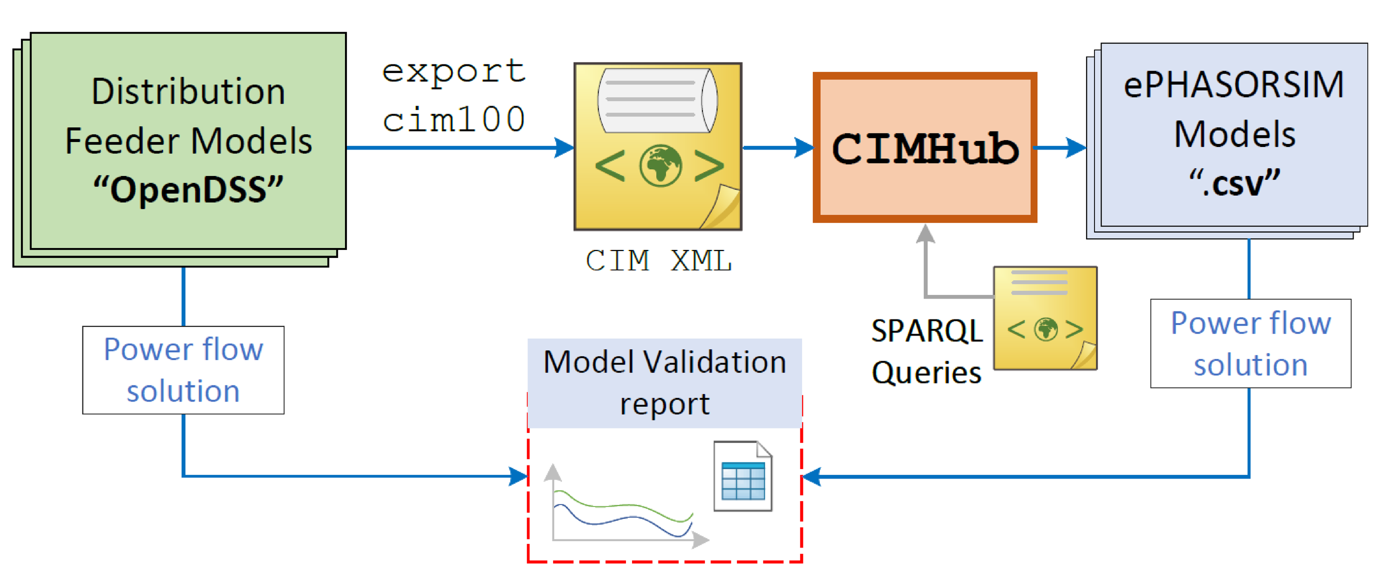
- Background
  - High penetration of distributed energy resources (DERs), increasingly to be in remote locations
    - ✓ Concerns safety and security of the electric grid
    - ✓ Security for next generation DERs connected to the distribution interconnection is crucial
  - Identification of vulnerabilities and evaluation of potential risks and impacts of cyber-attacks guide regulatory standards and guidelines for cybersecurity practices
  - Cyber-security-based model frameworks and scenarios necessary for risk and impact assessment [1]
  - **Standard, publicly available cyber-physical test systems (CPYDAR) in variety of sizes and configurations help researchers develop new algorithms or test procedures to benchmark their results**
- Objective
  - Translate publicly available distribution system models, covering a range of sizes from 13 to 9500 nodes, to enable the development, replication and benchmarking of cybersecurity test procedures and results
  - Construct DER attack scenarios to test one of the converted models, IEEE 123 bus feeder with integrated DERs
- Resource Criticality Levels for DERs
  - Determined R1 Resource Criticality Level for DER, from EPRI Security Architecture [2]
  - **Higher criticality DER units may require more robust cybersecurity measures and closer monitoring to mitigate potential risks effectively**

1. N. Duan, N. Yee, B. Salazar, J.-Y. Joo, E. Stewart, and E. Cortez, "Cybersecurity analysis of distribution grid operation with distributed energy resources via co-simulation," in 2020 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2020, pp. 1–5.
2. EPRI Security Architecture for the Distributed Energy Resources Integration Network: Risk-Based Approach for Network Design, [Online]. Available: https://www.epri.com/research/products/000000003002016781

Test Feeders

- **Three publicly available cyber-physical test systems[3]**
  - IEEE 13 node, IEEE 123 node, EPRI DPV J1
  - Model files available for hardware-in-loop (HIL) simulation

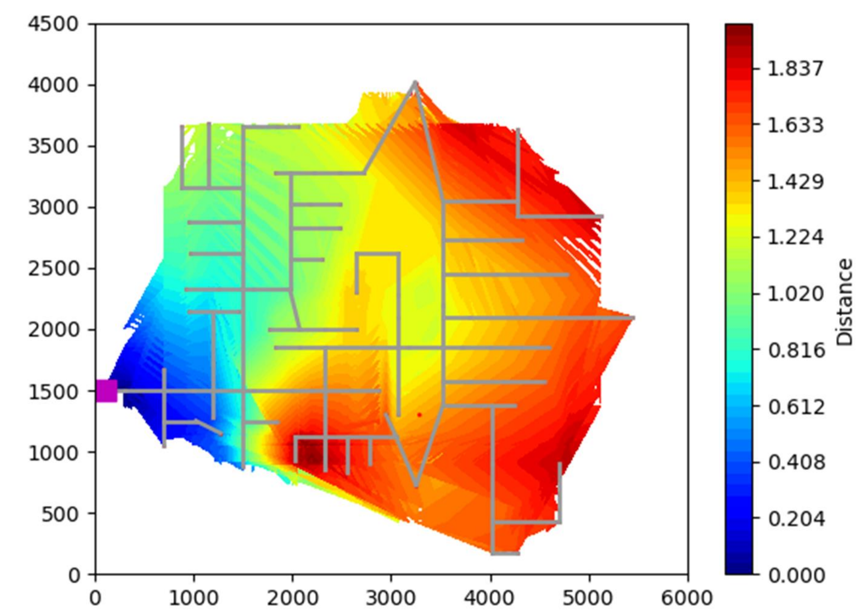
Model translation and validation[4]: OpenDSS models are converted to CIM XML, then CIMHub generates ePHASORSIM spreadsheets



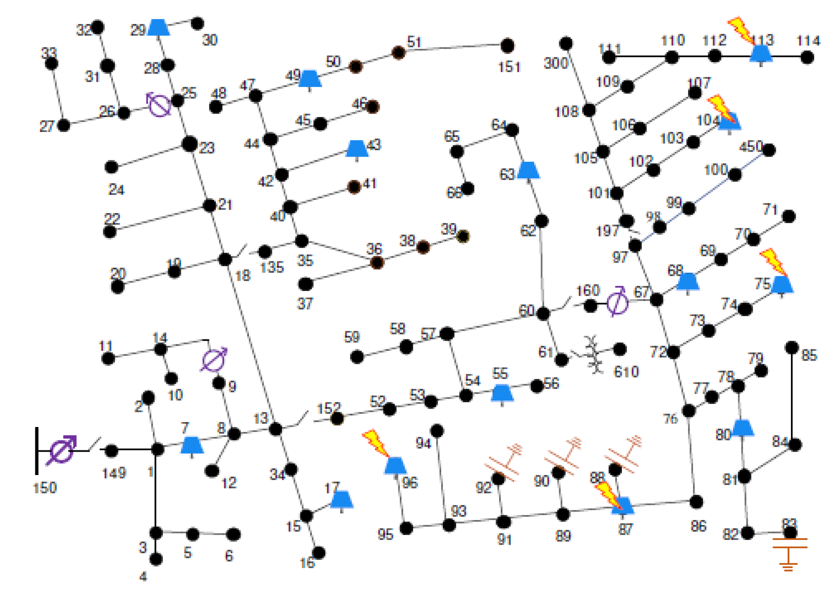
3. CIMHub Test Cases for S2G CPYDAR, Online: https://github.com/GRIDAPPSD/CIMHub/tree/feature/SETO/CPYDAR
4. CIMHub, "Tool set for translating electric power distribution system models between various formats, using the IEC Standard 61970/61968 Common Information Model (CIM) as the Hub", Online: https://cimhub.readthedocs.io/en/latest/

Resource Criticality Levels in IEEE 123-bus

Criticality level of various nodes based on location (distance from substation) and DER injections



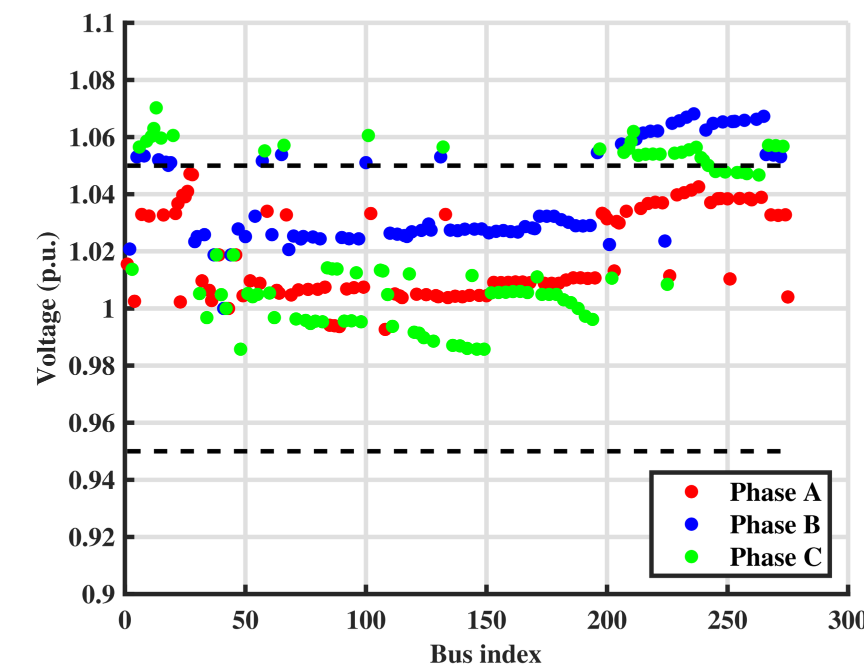
Most sensitive PVs are located farthest from the substation; i.e., buses 104, 113, 75, 96, and 87



Demonstration

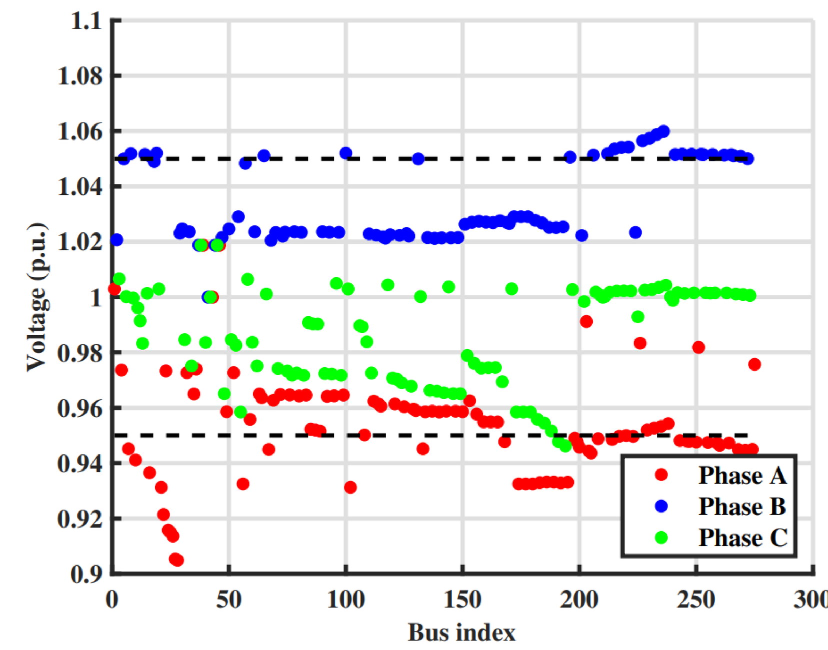
Scenario 1: Change in PV curtailment signals

- Attack on 5 PVs during low load period
  - ✓ Blocked curtailment signals
- Increase in voltage violations and reverse flow



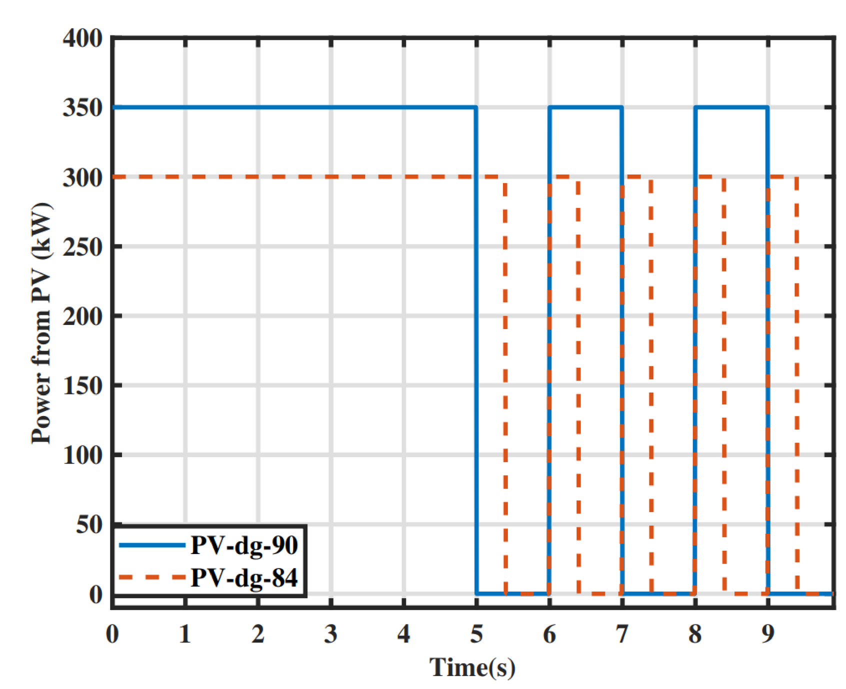
Scenario 3 : Change in Q setpoints

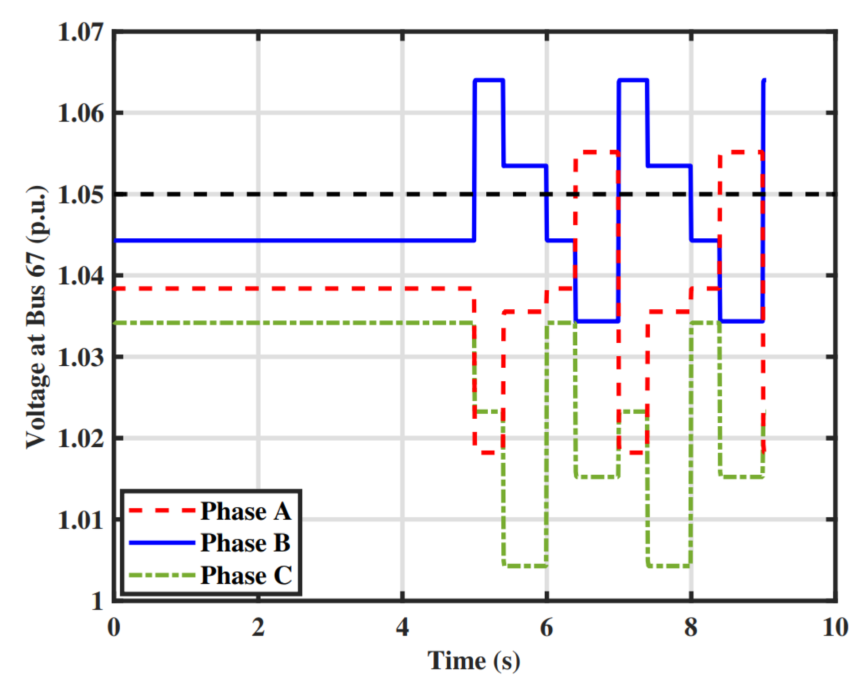
- Attack on 2 PVs with highest criticality levels
  - ✓ Q increased during low irradiance time
- Increase in voltage violations



Scenario 2 : Attacker toggles P setpoints of PVs with high criticality levels

- Voltage variations at bus 6, near the regulators, resulting frequency tap-changing actions; additional wear and thermal overloads





Summary

- Presented a framework for modeling different cyber-security scenarios in a real-time simulation platform, ePHASORSIM
- Demonstrated impacts of emulated cyber scenarios on the feeder through voltage violations in different locations of the feeder.

IEEE PES ISGT INNOVATIVE SMART GRID TECHNOLOGIES NORTH AMERICA

U.S. DEPARTMENT OF ENERGY BATTELLE

PNNL is operated by Battelle for the U.S. Department of Energy

For additional information, contact:

Manisha Maharjan| manisha.maharjan@pnnl.gov

02/20/2024 | PNNL-SA-194784

Pacific Northwest NATIONAL LABORATORY

www.pnnl.gov

This work is supported by the U.S. Department of Energy's Office of Renewable Energy and Energy Efficiency (EERE) under the Solar Energy Technologies Office Award Number 38451.