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

Manisha Maharjan, Shiva Poudel, Scott R. Mix, and Thomas E. McDermott
Pacific Northwest National Laboratory (PNNL)
Richland, WA, USA
email: manisha.maharjan@pnnl.gov

***Abstract*—The integration of distributed energy resources (DERs) in distribution networks has become a pivotal strategy for achieving decarbonization, enhancing grid resilience, and optimizing grid efficiency. Remote monitoring and control operations of such resources rely on a network of sensors and communication infrastructure, exposing the system to potential cyber threats. Therefore, as the deployment of DERs increases, ensuring secure monitoring and control becomes an imperative challenge. In this paper, a cybersecurity assessment framework is introduced, alongside several pertinent operational scenarios that researchers can leverage for DER-rich distribution grids. The feeder model is accurately represented within ePHASORSIM, a real-time simulation tool, allowing users to conduct simulations of cyber-attacks within a real-world environment and to analyze power distribution operations under vulnerable conditions. Furthermore, we discuss several practical sets of grid parameters to identify critical levels of DERs and evaluate various scenarios that simulate cyber threats on sensitive DERs. The modified IEEE 123-bus model is used as the test case for demonstrating the proposed scenarios. The findings from this study provide valuable insights into the vulnerabilities and potential consequences of cyber attacks on DERs, allowing for better mitigation strategies and improved cyber resilience in future distribution networks.**

***Index Terms*—Distributed energy resources, cyber attack, resource criticality, power system simulation**

## I. Introduction

The modern power grid is integrated with a substantial number of distributed energy resources (DERs), which increases its complexity and vulnerability with advanced equipment, intelligent sensors, and intertwined communication channels among various entities [1]. High penetration of DERs, increasingly to be in remote locations, can be one of the vulnerable areas where the safety and security of the electric grid might be compromised. This could provide the attackers with both physical and cyber access to these locations to potentially disrupt the system operations. The security for next generation DERs connected to the distribution interconnection is crucial for safety and reliability of the greater electric grid [2].

One of the important areas to tackle such threats in the grid would be the assessment of possible cybersecurity risks with high penetration of DERs and identifying all the vulnerabilities associated with the addition of technologies in different locations of the grid [3]. The evaluation of the potential risks of attacks can provide a good understanding of the magnitude of impacts on the grid [4]. To identity risks and threats, National Electric Sector Cybersecurity Organization Resource (NESCOR) have presented a threat model framework with cyber-attack scenarios with several functional domains like DERs [5]. Similar work has been presented as MITRE ATT&CK framework which is an attack identification framework for understanding cyber attacker behavior in the industrial control system domain [6]. All of these learnings on assessing risks and measuring impacts can be valuable for creating regulatory standards and guidelines regarding cybersecurity practices, especially for integrating DERs in the distribution interconnection. The current standard IEEE Std. 1547-2018 [7] lacks detailed recommendations for cybersecurity related standards and practices for DER-rich grids. Thus, new and informed standards developed can be utilized by the utilities and grid operators to ensure the base-level security of the grid with integrated DERs.

We need more cyber-security-based model frameworks and scenarios for studies related to risk and impact assessment to provide information to researchers and policy-makers [8]. With similar motivation, the work under Pacific Northwest National Laboratory (PNNL) Cyber-PhYsical Detection And Range (CPYDAR) provides standard and publicly available cyber-physical test systems with different sizes and configurations to benchmark for cyber-security-related research [9]. These models are all available in Common Information Model (CIM), OpenDSS and GridLAB-D formats. The main goal of this work is to provide these models in form of cybersecurity testbeds suited for hardware-in-loop (HIL) simulation and preliminary testing for their use in cyber-security studies. These testbeds and outlined scenarios will be used to design cyber-physical framework to emulate the attack scenarios and analyze the detailed impacts in the distribution interconnection with multiple DERs.

This paper presents one of the converted models, IEEE 123 bus system [10] with integrated DERs to create scenarios for cybersecurity testing. R1 Resource criticality level from the EPRI Security Architecture for DER [11] is determined for the test model to assign risk-levels based on which the management and security of the assets can be planned. The potential damage of cyber-attacks is studied through different case studies, in which the attacker modifies the information released from the control center to the DERs. Section II describes the framework built to create the test scenarios. Section III discusses the evaluation of resource criticality

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

levels for DERs for cyber-security scenarios. The scenarios and findings are demonstrated in Section IV and the conclusion is presented in Section V.

## II. Methodology

This section describes some key aspects that grid operators should consider when studying cybersecurity concerns related to DER integration. Additionally, we detail the features of the selected software tool for conducting the cybersecurity scenarios.

- Network modeling: Distribution system modeling is critical for studying cyber-security concerns related to DER integration. It involves creating a representation of an electrical power system, which includes network topology, buses, lines, transformers, and DER units.
- DER integration: The DER models should capture the characteristics and capabilities of different DER technologies, such as solar photovoltaic (PV), battery energy storage, and others. This includes specifying the DER unit's locations, power ratings, voltage regulation settings, and communication interfaces for control and monitoring.
- Communication and cyber-security scenarios: This process involves defining communication protocols and configurations. Additionally, it includes developing cyber-security attack scenarios specific to DER integration. By simulating these scenarios, operators can evaluate how the grid and DER units respond under different cyber threats.
- Impact analysis: By subjecting the system to simulated cyber threats, researchers can assess how these attacks influence grid parameters such as power flow, voltage profiles, and overall system stability.

We use ePHASORSIM [12] as the simulation tool because it offers HIL simulation options with large meshed networks. This feature allows us to incorporate physical devices, such as DERs, into the simulation, making it a valuable asset for testing and validating simple DER models and evaluating their performance under attack scenarios. Our primary focus in this study is on simple DER models and their responses to basic attack scenarios, which allowed us to establish a solid foundation for future investigations. However, it's worth noting that the testbed we developed has the potential to be further expanded and integrated with physical DERs with standard communication protocols, enhancing its applicability and usefulness for more comprehensive research in the future.

## III. Criticality Levels for DER

To comprehend the cybersecurity risk posed to the distribution grid due to the integration of various DERs, it is imperative to assess the criticality level of these resources [11]. By examining the criticality level of DER resources, stakeholders can prioritize cybersecurity efforts and allocate resources accordingly. Higher criticality DER units may require more robust cybersecurity measures and closer monitoring to mitigate potential risks effectively. Additionally, understanding the criticality of DER resources aids in formulating contingency plans and response strategies in case of cybersecurity incidents

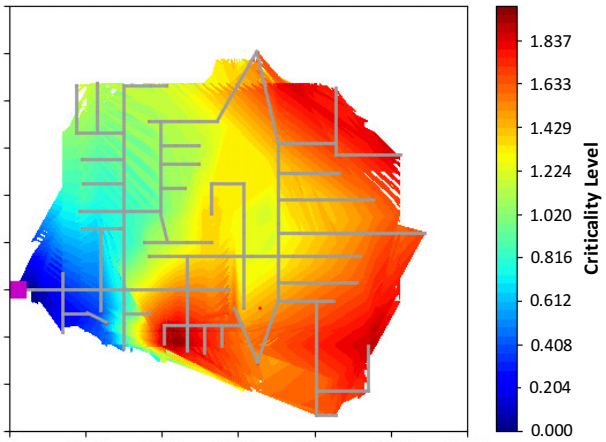


Fig. 1. Heat map showing criticality level of various nodes based on location (distance from substation) and DER injections.

to safeguard the distribution grid and ensure uninterrupted power supply to consumers.

### A. Resource Criticality in Distribution Operations

In this work, we discuss how the resource criticality level is important in evaluating voltage violation issues. To address overvoltage problems associated with the operation of DERs, it is important to consider the sensitivity of these resources based on their location, capacity, and operating profiles. Here are some factors to consider:

- **Grid topology**: The layout and structure of the distribution grid play a significant role in determining the impact of DERs on overvoltage. For instance, due to the radial nature of typical distribution networks, DERs farther away from substations will see higher voltages during periods of high reverse power flows. Conversely, DERs closer to the substation may experience low voltage rise during peak PV generation. Identifying DERs connected at critical points in the grid can help pinpoint sensitive locations.
- **Penetration level**: The total capacity of DERs connected to the grid, known as the penetration level, can affect voltage levels. High penetration levels of DERs can lead to increased voltage fluctuations and potential overvoltage conditions. Identifying areas with high DER penetration can help identify sensitive locations where overvoltage problems may arise.
- **Network impedance**: The distribution network impedance determines the voltage drop or rise between different points. DERs located in areas with high network impedance may be more susceptible to overvoltage issues. Identifying areas with high network impedance and significant DER integration can help identify sensitive locations.
- **Local load profile**: The local load profile in a particular area can influence the impact of DERs on voltage levels. DERs connected to areas with low load demand may experience voltage rise, potentially leading to overvoltage

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

problems. Identifying areas with significant load profiles and DER integration can help identify sensitive locations.

Out of these factors, the penetration level, grid topology, and network impedance can be combined to determine the resource criticality level based on location (i.e., electrical distance), whereas the local load profile provides insights into the time of the attack.

### B. Resource Criticality Level in IEEE 123 bus feeder

The case study is carried out using the modified IEEE 123 bus feeder—the ePHASORSIM model is exported following the process outlined in the Appendix. The resource criticality level according to the electrical distance of the DERs has been evaluated on the test feeder. Fig. 1 shows the heat map showing the electrical distance of different buses from the substation of the IEEE 123 bus feeder. According to the heat map, the resource criticality level for all the PVs connected to the feeder is determined. For IEEE 123-bus feeder, the most sensitive PVs, which are located the farthest from the feeder source, are at buses 104, 113, 75, 96, and 87, and are highlighted in Fig. 2. These critical PVs may be identified by the attackers for higher attack impact on the feeders and are chosen for various types of attacks as detailed in the scenarios below. In summary the above-mentioned PV buses have HIGH resource criticality level, and are subjected to risks with possibilities of higher disruptions.

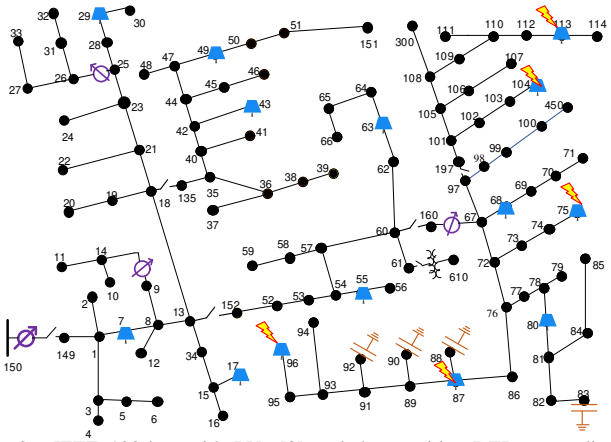

Fig. 2. IEEE 123-bus with PVs [9] and the sensitive DERs according to resource criticality levels.

## IV. Case Studies

In this section, we discuss the three different case studies to demonstrate the usability of the models created in ePHASORSIM. We assume in these cases that the attacker interrupts the communication signals from the control center to the controllers at the local DERs and modifies the information being exchanged between the two parties. Mostly the attacker disrupts the settings or setpoints of DERs to communicate false information from the control center to the PV controllers. This hinders the normal operation of DERs causing disruption from remote DER locations into the normal operation of the feeder.

### A. Scenario 1: Change in PV curtailment signals

Here, we simulate the case of high PV generation and low demand, which can cause over-voltage in the system. In such cases, curtailment signals are sent to PVs by DSO to avoid voltage violation in the system [13]. The scenario is generated with 25% reduced load in the IEEE 123 bus system and 50% curtailment signals sent by operator to all the PVs connected to the feeder. Fig.3 shows the voltage at different buses at this condition, which has the maximum voltage of 1.055 p.u. and a total of 1660 kW PV power injected into the feeder after the curtailment signals.

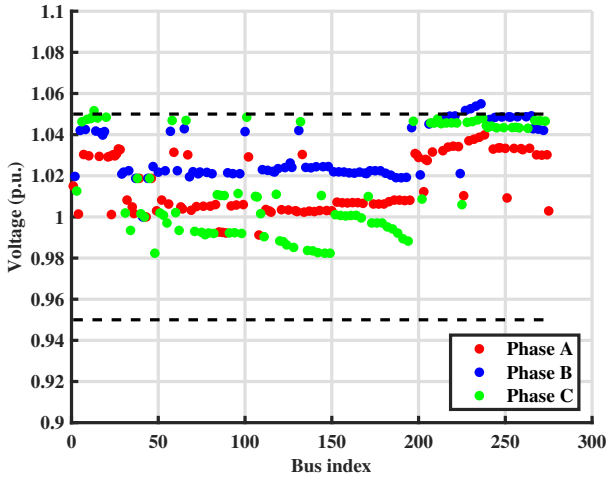


Fig. 3. Scenario 1: Voltage at different buses in IEEE 123-bus feeder with 25% load reduced and 50% PV curtailment signal, normal conditions.

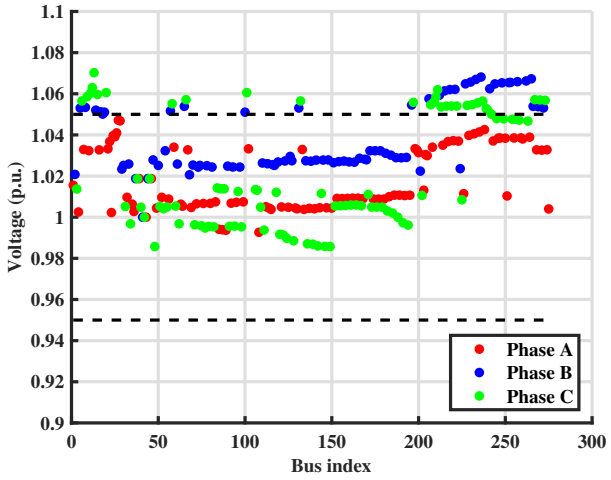


Fig. 4. Scenario 1: Voltage at different buses in IEEE 123-bus feeder with 25% load reduced and 50% PV curtailment signal, and attack signal on high criticality level PV units.

The attacker disrupts the curtailment signal of 5 PV units which have high resource criticality levels and thus, the compromised PVs inject 1340 kW, rather than curtailing by 50% to 670 kW. Thus the total power injected by PVs into the feeder increased to 2330 kW. Fig. 4 shows the voltage at different buses with reduced load and curtailed PV power but with

modified curtailment signals at 5 PV units by the attackers. The magnitude of maximum over-voltage is 1.0702 p.u. and there are around 61 buses with voltage over 1.05 p.u. in the feeder. The results show that the insufficient curtailment in PV power due to the attack on DERs that have sensitive resource criticality, causes increased reverse power flow from DERs towards the source and over-voltage in several locations of the feeder.

### *B. Scenario 2: Change in PV Inverter active power setpoints*

Here, we assume the distribution feeder utilizes the maximum capacity of all the PV generation. In this scenario, the attacker toggles the active power setpoints of PV inverters with high criticality levels to cause voltage disruptions. As seen in Fig. 5, the power generated for PVs located at buses 104 and 113 (PV units with high resource criticality level) toggles from its actual value to zero multiple times with different attack frequency for these two PV units.

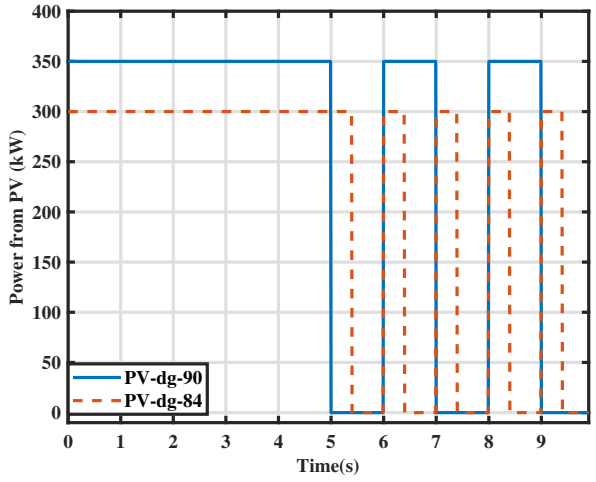


Fig. 5. Scenario 2: Toggling of active power for PVs at buses 104 and 113.

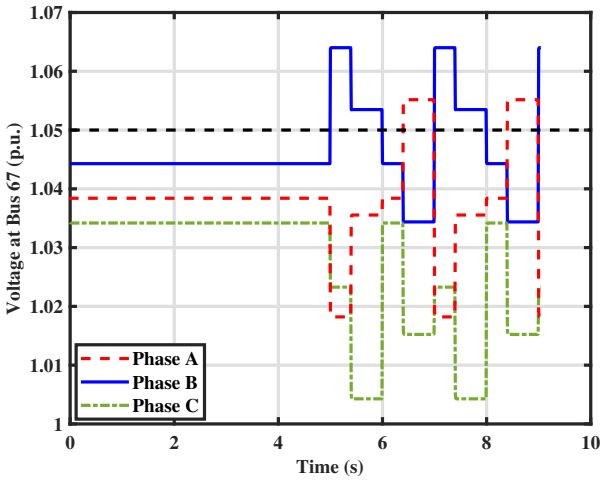


Fig. 6. Scenario 2: Voltage at bus near regulator (bus 67) in IEEE 123-bus feeder with toggling of power at PVs located at 104 and 113.

Fig. 6 shows the steady-state voltage variations at bus 67 (located near one of the regulators) after toggling of active power injection from critical PV units. Such steady-state voltage changes during the attack period show the voltages exceeding the voltage limits in many locations. To mitigate these steady-state voltage fluctuations, the regulator in the feeder needs to operate frequently for its tap-changing actions and might encounter difficulties in maintaining normal voltage profiles. Increasing the regulator actions frequently and switching tap changers with larger deviations also creates additional wear and thermal overloads on the regulators. Such attacks on critical-level DERs not only cause disturbances in the normal operation of the distribution feeder but reduce the lifespan of the important equipment in the feeder.

### *C. Scenario 3: Change in PV Inverter reactive power setpoints*

Usually, reactive power injection by DERs is used to regulate the voltage across the feeder, but it may provide possibility of adversarial attacks. In this scenario, while the PV units are operated in 30% irradiance level, the attackers target the most vulnerable DERs to change the reactive power setpoints of PV inverters with the intention to disrupt the voltage profile across the feeder. The reactive power setpoints for two PVs with sensitive criticality levels are modified to the maximum possible values within the inverter limit. Fig. 7 shows the voltage profile under the permissible limits for different buses during 30% irradiance level for all PVs connected to the feeder during normal operating conditions.

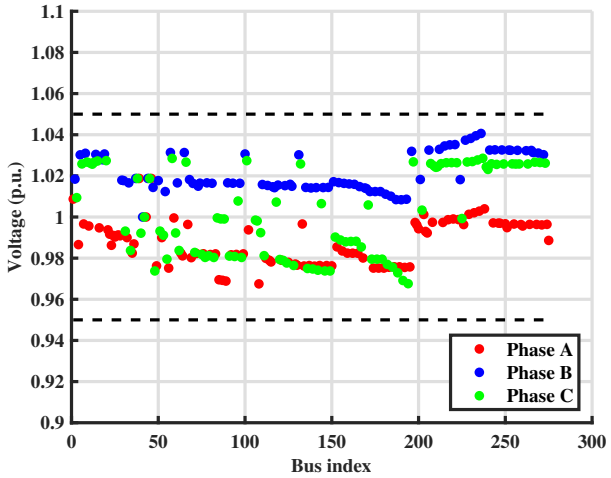


Fig. 7. Scenario 3: Voltage at different buses in IEEE 123-bus feeder with 30% irradiance level, normal conditions.

The reactive power values that can be absorbed or injected by the PV inverters are calculated as shown in Table. I, with respect to the nominal values of the inverters and the active power generated during 30% irradiance level by PV units. The PVs connected to buses 104 and 113 are considered for the attack as these buses locate vulnerable DERs according to calculated resource criticality. The voltage profile after the attack as shown in Fig. 8, depicts that violations of voltage limits occur in multiple locations throughout the feeder. This shows that attackers with knowledge of the criticality levels of DERs and network topology need not attack all the DERs.

TABLE I
REACTIVE POWER SETPOINTS FOR SCENARIO 3

| DER | Bus | P nominal (kW) | Q actual (kVA) | P 30% irradiance (kW) | Q setpoint (kVA) |
|---|---|---|---|---|---|
| PV_dg_84 | 104 | 300 | 0 | 90 | 286.18 |
| PV_dg_90 | 113 | 350 | 0 | 105 | 333.88 |

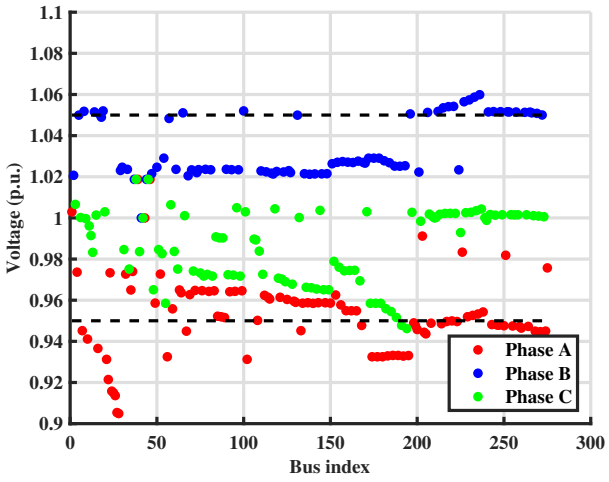


Fig. 8. Scenario 3: Voltage at different buses in IEEE 123-bus feeder with 30% irradiance level, and modified reactive power setpoints on 2 PV units.

## V. CONCLUSION

This paper presents the preliminary framework for modeling different cyber-security scenarios in a real-time simulation platform, ePHASORSIM. The scenarios are framed based on the resource criticality levels categorized using a heat map so that the possible risks and impacts of the DERs can be identified and managed in an appropriate way. The impacts of emulated cyber scenarios on the feeder were shown through voltage violations in different locations of the feeder. We demonstrate that intelligent attackers with information on the network and the criticality levels can misuse the responses from different buses to trigger significant impacts on the network and its components. In the future, this framework can be used to model such attack scenarios in HIL simulation setup for more realistic scenarios based on communication protocols and control functionalities of DERs. The proposed simulation framework can also host large distribution interconnections with high-performance processing units and can facilitate external hardware interfacing for closed-loop testing of controls and protection of DERs.

## APPENDIX

The test feeder model needed to be translated from other formats into ePHASORSIM. CIMHub provides network model translation, with OpenDSS playing a central role [14]. First, a CIM XML file is created from the OpenDSS model. The exported model is then uploaded into a triple-store database, and the conversion to ePHASORSIM is executed with a Python script, including a comparison of power flow solutions. The overall process is summarized in Fig 9. The translated ePHASORSIM models are publicly available from [9].

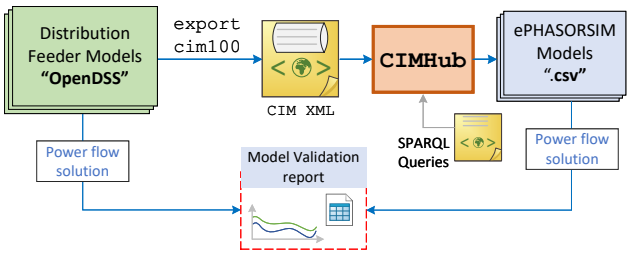


Fig. 9. Model translation and validation: OpenDSS models are converted to CIM XML, then CIMHub generates ePHASORSIM spreadsheets.

## ACKNOWLEDGEMENTS

This material is based upon work 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.

## REFERENCES

[1] R. S. de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," in *2019 Resilience Week (RWS)*, vol. 1, 2019, pp. 226–231.
[2] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 2018.
[3] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 28–39, 2016.
[4] 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.
[5] A. Lee *et al.*, "Electric sector failure scenarios and impact analyses," *National electric sector cybersecurity organization resource (NESCOR) technical working group*, vol. 1, 2013.
[6] O. Alexander, M. Belisle, and J. Steele, "Mitre att&ck for industrial control systems: Design and philosophy," *The MITRE Corporation: Bedford, MA, USA*, vol. 29, 2020.
[7] "Ieee standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)*, pp. 1–138, 2018.
[8] C. Powell, K. Hauck, A. D. Sanghvi, A. Hasandka, J. Van Natta, and T. L. Reynolds, "Guide to the distributed energy resources cybersecurity framework," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2019.
[9] CIMHub Test Cases for Securing Solar for the Grid (S2G) Cyber-PhYsical Detection And Range (CPYDAR) , [Online]. Available: https://github.com/GRIDAPPSD/CIMHub/tree/feature/SETO/CPYDAR.
[10] W. Kersting, "Radial distribution test feeders," in *2001 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No.01CH37194)*, vol. 2, 2001, pp. 908–912 vol.2.
[11] 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.
[12] V. Jalili-Marandi, F. J. Ayres, E. Ghahremani, J. Bélanger, and V. Lapointe, "A real-time dynamic simulation tool for transmission and distribution power systems," in *2013 IEEE Power & Energy Society General Meeting*, 2013, pp. 1–5.
[13] S. Poudel, M. Mukherjee, R. Sadnan, and A. P. Reiman, "Fairness-aware distributed energy coordination for voltage regulation in power distribution systems," *IEEE Transactions on Sustainable Energy*, vol. 14, no. 3, pp. 1866–1880, 2023.
[14] Common Information Model Conversion (CIMHub), [Online]. Available: https://cimhub.readthedocs.io/en/latest/Overview.html.