Pacific Northwest
NATIONAL LABORATORY

PNNL- 38478

ResDesign: Resilient by Design Platform for CPS Assessment and Validation

Final Project Report

September 2025

Sumit Purohit
Thiagarajan Ramachandran
Oceane M Bel
Armando Mendoza Sanchez
Garret E Seppala
Aowabin Rahman
Rounak Meyur
Sam Donald
Joshua H Bigler
Thomas W Edgar
Veronica A Adetola

U.S. DEPARTMENT of ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL- 38478

ResDesign: Resilient by Design Platform for CPS Assessment and Validation

Final Project Report

September 2025

Sumit Purohit
Thiagarajan Ramachandran
Oceane M Bel
Armando Mendoza Sanchez
Garret E Seppala
Aowabin Rahman
Rounak Meyur
Sam Donald
Joshua H Bigler
Thomas W Edgar
Veronica A Adetola

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

ResDesign project has developed integrated capabilities to help cyber physical system modelers and analysts to evaluate vulnerabilities and resilience of such systems using co-simulation-based attack testbed, graph-based visualization and monitoring tool, and Bayesian optimization-based co-design capability. The project demonstrates a collection of attack scenarios and use cases in an integrated software environment.

Summary

ResDesign project provides insight into worst-case impact assessment of cyber-physical attacks on distribution microgrids and optimal mitigation planning use cases by combining design parameters from 1) cyber physical model, 2) threat model, and 3) measurement and metrics requirements.

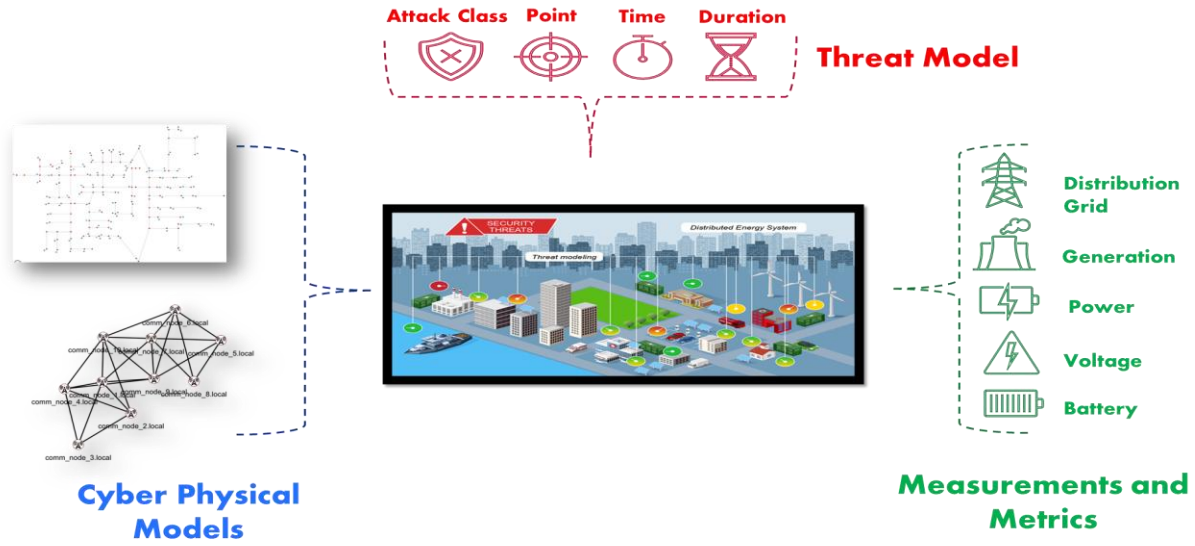

Figure 1 ResDesign Methodology

The project integrates existing PNNL capabilities and develops sector and sponsor-specific demonstrations of an end-to-end capability to perform cyber physical system (CPS) vulnerability assessment, optimal design selection, and adversarial impact assessment. The project deliverable can assist CPS designers, operators, and policy makers to model their custom CPS models and evaluate their risks to design a more resilient and secure system.

Acknowledgments

This research was supported by the Resilience through Data-Driven Intelligently Designed Control (RD2C), under the Laboratory Directed Research and Development (LDRD) Program at Pacific Northwest National Laboratory (PNNL). PNNL is a multiprogram national laboratory operated for the U.S. Department of Energy (DOE) by Battelle Memorial Institute under Contract No. DE-AC05-76RL01830.

Acronyms and Abbreviations

CPS: Cyber Physical System
DER: Distributed Energy Resources
CVE: Common Vulnerabilities and Exposures
CWE: Common Weakness Enumeration
CAPEC: Common Attack Pattern Enumeration and Classification
TTP: Tactics, Techniques, and Procedures
ICS: Industrial Control System
NATIG: Network Attack Testbed in Power Grid
GLIMPSE: Grid Layout Interface for Model Preview and System Exploration

Contents

Figures

Tables

1.0 Background

Cyber Physical Systems (CPSs) are increasingly getting more complex, heterogeneous, and interdependent to different vendor solutions, ownership profiles, and technology stack. Additionally, communication infrastructure penetration has increased because of smart devices integration and control strategies. This expands the possible cyber-attack surface and exasperates risk of possible adversarial scenarios. When combined with extreme weather events, resilience assessment of CPSs become a key requirement for reliable operations.

Resilient By Design (ResDesign) project builds upon existing PNNL capabilities to demonstrate multiple use cases relevant to sectors and sponsors. It integrates HAGEN (Purohit 2024), SCOREDEC [Ramachandran et al. 2024], and Communication Modeling projects that have been doing research and development in the fields of cyber threat modeling, cyber physical attack scenario generations, mitigation planning, CPS attack simulation, CPS co-design, and graph-based model visualization and monitoring.

Figure 2 Example of advance Cyber Physical System

HAGEN (Efficient Hybrid Attack Graph Generation for Cyber-Physical System Resilience Experimentation) project has developed threat modeling capability that leverages AI/ML methods to identify credible attack scenarios for specific CPS design. The scenarios are represented as a Hybrid Attack Graph (HAG), a collection of sequence of adversarial techniques, moving from cyber to physical domain. The project has developed a data-driven Graph Convolutional Deep-Q Network (GCDQ) to address the challenge of sparsity of ground-truth data. By leveraging limited real-world observations from the MITRE ATT&CK knowledge base, our GCDQ model synthesizes realistic graphs with some targeted attribute of minimum detectability via reinforcement learning. HAGEN has also developed knowledge-graph based cyber knowledge completion capabilities to connect device level vulnerabilities with system-level risks and possible adversaries across silos of cyber information. HAGEN has also developed dynamic visualization capability GLIMPSE [Sanchez et al., 2024], to provide insight into microgrid topology, measurement, and temporal changes in the CPS state.

HAGEN and Communication Modeling projects have also developed a co-simulation environment (NATIG) [Oceane et al., 2023] to orchestrate attack scenarios and measure their impact using multiple resilience metrics such as voltage/frequency violations, loss of access, and other topological metrics. It is a standalone, containerized, and reusable environment to enable cyber analysts and researchers to run different cyber security and performance scenarios on power grid and generate benchmark datasets. It supports IEEE123 and IEEE9500 as the reference power grid models with communication model using mesh/ring/star topologies. The communication model supports CSMA, WiFi, 4G, and 5G (optional) protocols. The co-simulation environment expedites CPS design phase by providing multiple physical and communications models and parameters to compute resilience metrics.

Scalable Control Co-Design for Resilient-by-Design Cyber-Physical Systems (SCOREDEC) project has developed a scalable and modular co-design framework to enable large-scale sensing and control co-design for assured resilience. SCROEDEC formulates the co-design as an optimization framework and since the CPS design is a challenging optimization problem to solve because of a lack of closed form expression for the microgrid performance objectives and system dynamics, SCOREDEC uses simulation-based approach to evaluate a system design and control.

2.0 Introduction

ResDesign project identified gaps and challenges to the existing PNNL capabilities to develop a more robust and usable prototype for CPS resilience assessment. The project uses a 3000 bus - based physical model and corresponding hybrid communication model with 11 microgrids to demonstrate a realistic use case. The project also develops "*Blended*" system-level attack with multiple entry points on multiple timestamps as observed in real-world cypher attack. The project leverage High Performance Computing (HPC) capabilities to optimize co-simulation and provide real-time updates to end user. The project also addresses usability challenges by using a dynamic event-driven user interface for CPS visualization and monitoring. For end users, ResDesign is an integrated tool to setup distribution microgrid, orchestrate attack scenarios, and monitor their impact in a low-fidelity simulation environment.

Figure 3 ResDesign Methodology

The project has developed a 3-layer approach to develop different resilience experimentation scenarios using CPS model, threat model, and a collection of metrics and measurements, as shown below. The CPS model defines instances of cyber and physical models. The threat model represents overall attack surface that can be computed for a given CPS. The metrics and measurements provide indicators of exploit movement across physical and cyber layer.

3.0 Use Cases Design

The ResDesign project has developed and demonstrated the integrated capability to enable users and stakeholders to better understand vulnerabilities, risks, and robust mitigation strategies for a collection of threats.

The project addresses following research questions for users and stakeholders:

1. Given an existing system, what are the most severe potential attacks that could compromise its resiliency and operational functionality?
2. Given a specific set of cyber-attacks or failures, what is the most effective mitigation strategy to ensure an optimally resilient response?
3. How can we improve existing methodologies for assessing security and resiliency preparedness at DoD installations, given that current approaches are manual, ad hoc, and incomplete?
4. What cost-effective investment decisions are needed to improve resilience?

3.1 Worst Case Impact Assessment

The project selected worst case impact assessment as a use case to demonstrate integrated capabilities to set up a CPS, orchestrate an attack scenario, and monitor its impact. The project used a 3000-bus grid model to design a utility scale physical system and orchestrated cyberattacks such as man-in-the-middle (MIM) and Distributed Denial of Service (DDoS) on the power grid. The project also developed real-time monitoring and visualization capabilities to better identify most critical and vulnerable parts of the CPS, how quickly problems could move from cyber to physical domain, and what protective measures would be most effective. This visual simulation helps bridge the gap between an abstract cybersecurity concept and real-world infrastructure protection, making it easier to develop targeted security strategies before an actual attack occurs.

We demonstrated a potentially dangerous attack involves strategically flipping switches to break up the grid. An attacker could open breakers at critical points that connect power plants to consumers, isolate important substations that link different regions, or disconnect lines that allow areas to share power during emergencies. They might also separate major power plants from the communities they serve or create bottlenecks that overload remaining lines. These actions could trigger a domino effect of failures across the system. Being able to visualize these attacks in real time is crucial because it's otherwise difficult to predict how one switch manipulation might cascade into widespread outages.

The project leverage GLIMPSE [Sanchez and Purohit 2024] and NATIG [Bel et al, 2024] to set up a MIM attack through the Scenario Setup. In this setup, we run the attack for 2 seconds, starting at 20 seconds in an 80-second run. At the beginning of the run before the attack starts, the switch is shown as closed with a blue color indicating that the switch is in its expected status. When the switch is attacked, it turns red and the icons open, indicating that the switch has been opened, as shown in figure 4. A user can attack multiple switches to isolate some of the grid's nodes from the main grid. The attacker might do that to increase the reliance of some nodes on the lesser power generation potential, causing harm or blackouts in specific areas of the grid.

Figure 5 shows the visualization of the attack using the GLIMPSE tool in real time. After some stress testing we found that the deltamode_timestep parameter in both the power flow and the generator can cause the simulation to crash if they are not parameterized well. For the 3000 model we found that setting both values to 10ms allowed the system to function correctly. Future work will involve working with GridLab-D development team to investigate this issue.

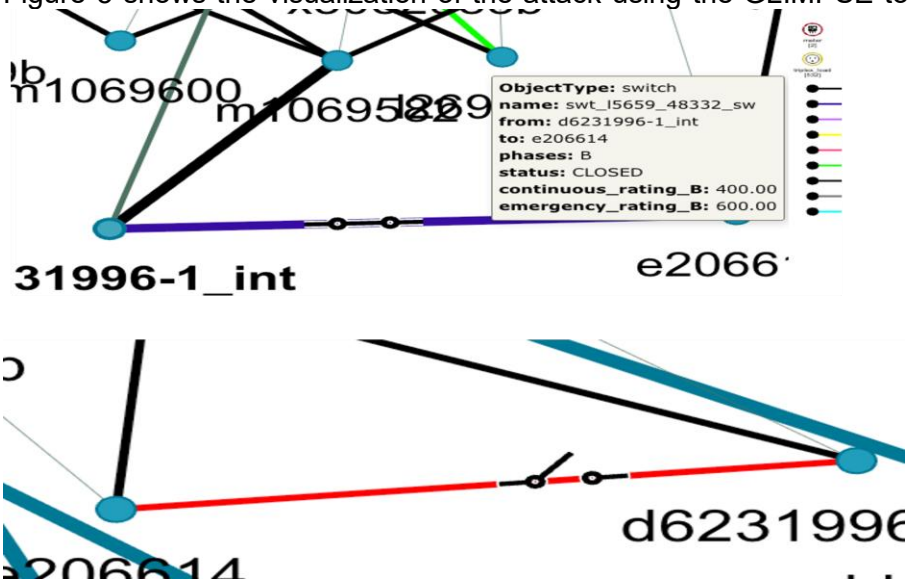

Figure 4 MIM attack on a switch

To communicate between NATIG and GLIMPSE, we used socket programming. In the ipv4 l3 layer module inside ns3 [Henderson et al., 2008], we added a listener that subscribe to packets

Figure 5 Visualization of MIM attack impact

arriving and being sent out by the nodes in the network. The packet size alongside the location of the network is sent back to GLIMPSE to show the corresponding animation of the traffic. The animation shows how fast or slow the traffic is running on an edge, which can be used by a user to understand if a potential DDoS attack might be occurring on the network. To understand the direction of the traffic, NATIG sends back GLIMPSE the ID of the nodes that the packet is coming from and is going to. Additionally, NATIG also sends back the size of the packet that is being transferred, which means that the faster the traffic is running on GLIMPSE, the larger the packet is being sent. GLIMPSE can be configured to visualize different cyber metrics such as bandwidth or latency.

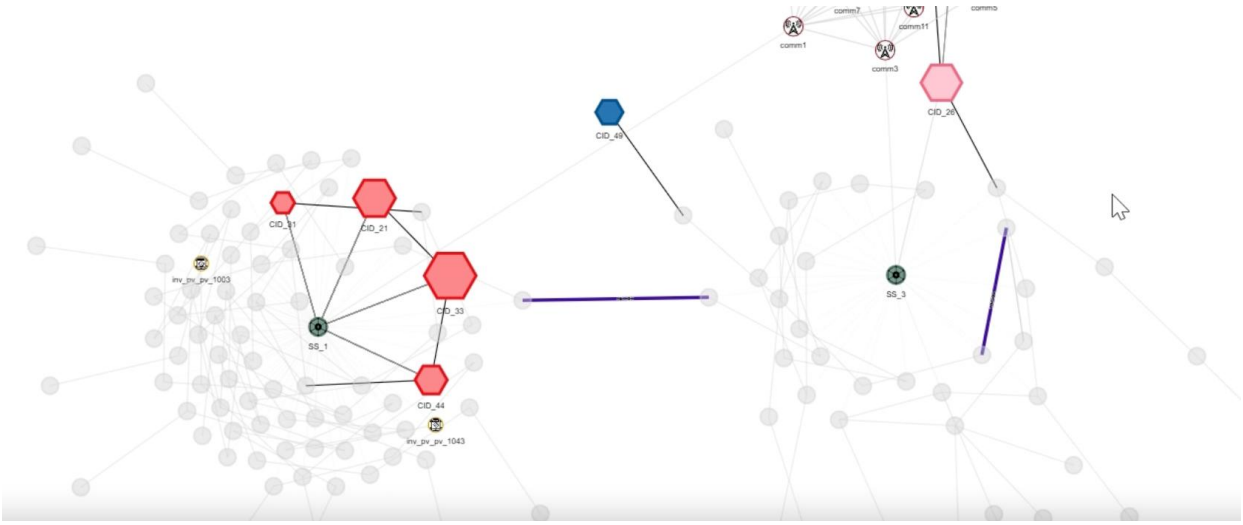

Figure 6 two switches visualization GLIMPSE

This figure 6 shows a case where, using GLIMPSE, we isolated two switches that are relatively close to one another. By attacking both switches, we can further stress the grid by gaining access to the power generated by the rest of the grid. Using this setup, we were able to demonstrate the impact of opening both switches on inverters that use these switches to communicate with the rest of the grid.

When attackers disable two nearby network switches at the same time, they can cut off power inverters from the main electrical grid. This creates several problems. The cut-off inverters can't receive instructions from the main grid control system, potentially causing them to operate incorrectly. The isolated area can't send excess power to other areas or receive more power when needed, which can cause unbalanced power levels that might damage equipment or cause blackouts. Grid operators lose visibility into the isolated area, preventing them from spotting or fixing problems. Important facilities like hospitals in the affected area might not have enough local power to function properly. Our simulation shows that attackers with the knowledge of physical topology could target just a few key communication nodes to cause widespread disruption as shown in figure 7.

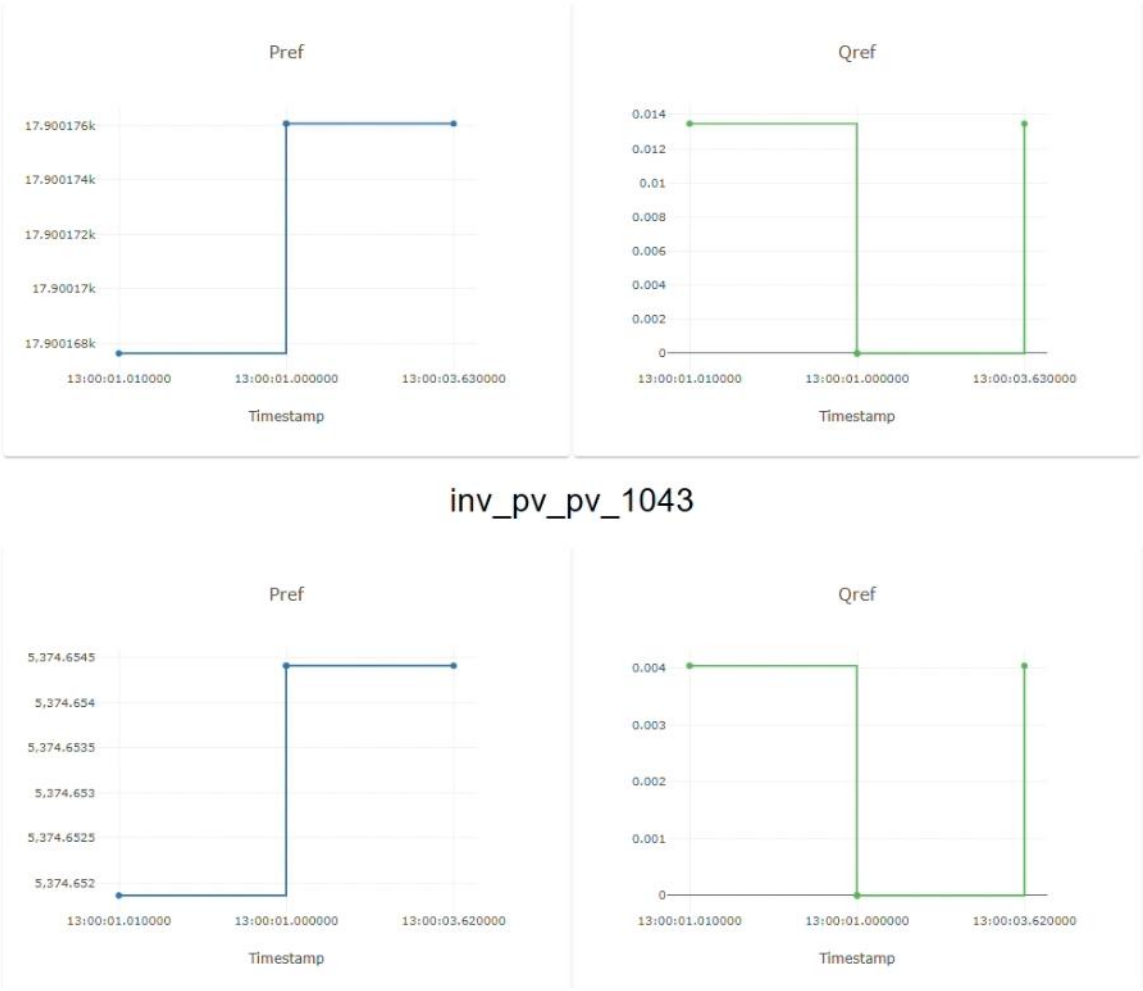

Figure 7 Impact of the attack on inverters

3.1.1 Future updates

When compiling NATIG in a container, there is a spike in CPU usage. It might be prudent to expand the size of the Docker container or create a cleanup script that removes unnecessary data before attempting the compilation process. If that is not possible, then for the first compilation phase, the user will have to keep compiling the code until it is done.

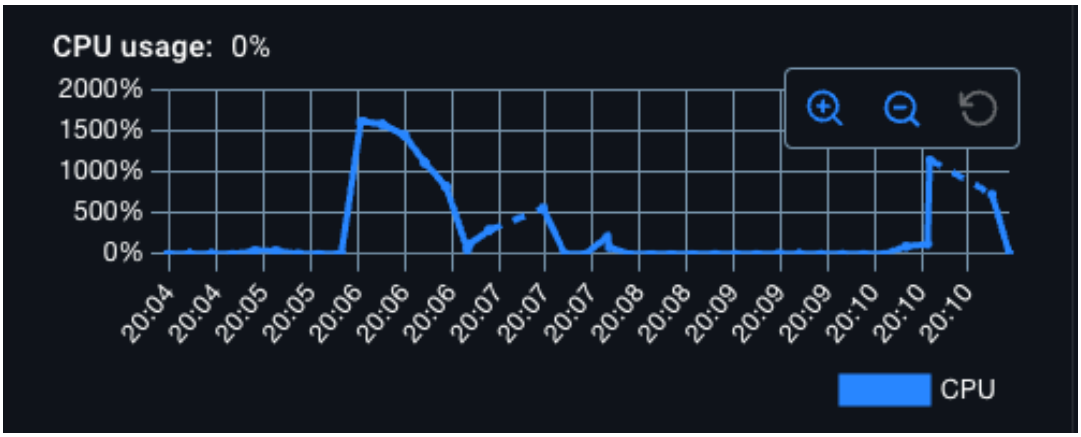

Figure 8 CPU usage while compiling the container

We've also identified several areas of improvement. When users start a simulation and then go back to the home screen, the previous simulation keeps running in the background, which wastes resources. We'll fix this by making sure simulations properly shut down when no longer needed. We also noticed that our ring-shaped network displays don't show the moving data traffic they're supposed to, so we'll update the visualization to make it work correctly. Our development environment sometimes crashes during system building, requiring multiple attempts to complete the process - we'll solve this stability issue in our next update. Finally, we found a problem where our Miramar model sometimes sends the same information twice, causing confusion in the system. We plan to improve our software to recognize when this happens and handle it properly. All these improvements will be addressed in our upcoming work.

3.2 Risk Assessment of Existing Installations

In the second use-case, we evaluated the risk posed to a cyber-physical system by an adversary and utilized optimal design methodologies to mitigate the risk by designing mitigation strategies. Military microgrids serve as an example of a cyber-physical system that have mission-critical loads that need to be served consistently. As such, there is need to minimize the impact of adversarial attacks on the ability of the system to perform those mission critical tasks. In this use-case, we developed an approach to identifying least cost cyber-physical mitigation approach that will minimize the attacker's access to the system. The approach was demonstrated on a simplified Gridlab-D version of the Miramar defense installation located in Miramar, California.

3.2.1 Mitigation models:

MITRE Mitigation strategies (see Figure 6) for securing cyber-physical systems can be broadly classified into two kinds of measures:

Preventive measures decrease the likelihood of an attacker gaining access to the system by either implementing stricter access policies to various physical assets or by segmenting the

network architecture so that the attacker is unable to gain access to the entire system via a single access point.

M1043 - Code Signing
M1044 - Data Loss Prevention
M1046 - MITM Attack Prevention
M1048 - Privileged Process Integrity
M1036 - Password Policies
M1013 - Application Developer Guidance
M1033 - Limit Software Installation
M1042 - Isolation and Segmentation
M1045 - Update Software
M1052 - Safe Browsing Practices
M1015 - Active Directory Configuration
M1034 - Network Intrusion Prevention
M1024 - Disable Inactive Accounts
M1018 - User Account Management
M1022 - Restrict File and Directory Permissions
M1026 - Multi-factor Authentication
M1027 - Audit
M1028 - Execution Prevention
M1030 - Network Segmentation
M1032 - Software Restriction Policy
M1035 - Limit Login Attempts
M1037 - Filter Network Traffic
M1038 - Credential Guard
M1040 - Behavior Monitoring
M1054 - Software Update
M1056 - Network Boundaries
M1057 - Parameter Elevation Prevention

Detection measures increase the likelihood of detecting an adversarial presence within the system via methods like behavior monitoring and audit.

For the purpose of demonstration, we simplify these measures and represent preventive measures via an attack success probability that determines the likelihood with which an attacker can gain access to the system and b) attack detection probability that determines the likelihood with which an attacker can be detected.

Furthermore, as an example, we model an abstract linear cost model associated with deployment of these mitigation strategies based on their complexity. The proposed optimization approach is general enough to accommodate more sophisticated cost models for other real-word applications if they are available and is not a limitation of the approach.

Figure 9 MITRE Mitigation strategies

3.2.2 System model:

For the purpose of demonstration, we utilize the Miramar microgrid model presented in [Sarker et al, 2020]. The Miramar microgrid is a defense installation consisting of 6.4 MW power plant with a 1.5 MW battery. It also consists of several buildings with critical loads grouped into 8 loads. Each of these loads also have access to backup generation and is connected to the main grid via switches.

As part of the project, we developed a simplified model of the Miramar microgrid using GridlabD and integrated it with the NATIG testbed (see Figure 8).

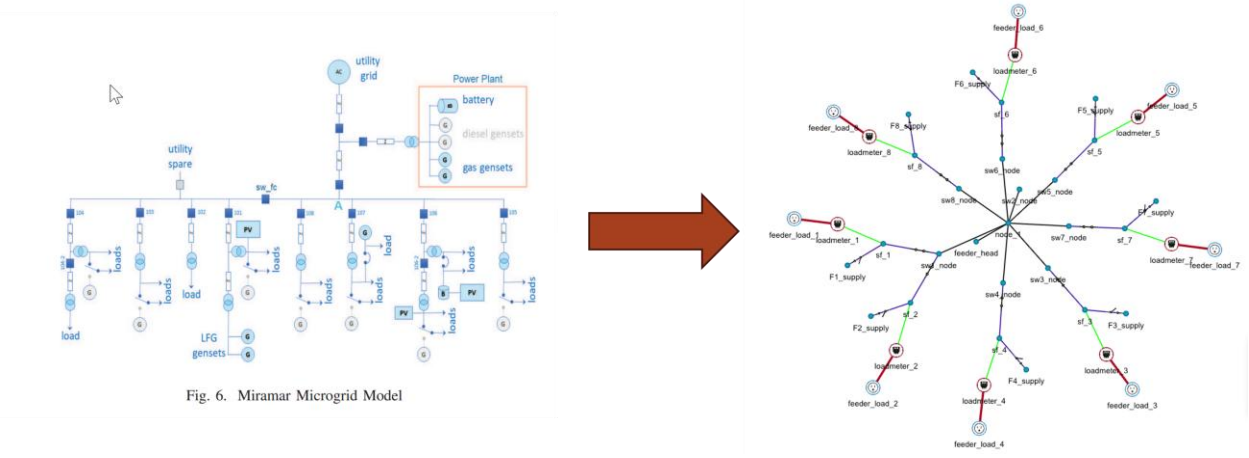

Fig. 6. Miramar Microgrid Model

Figure 10 Miramar microgrid model

We also developed a simple attacker model where the attacker can generate attack sequences which will maximize the dependency on the backup generation over a course of an hour by disconnecting the loads from the main grid. This is achieved by conducting a man-in-the-middle attack on the switches forcing them to open at intervals determined by the attacker. The attacker's objective is to drain the fuel reserves and energy stored in the backup generation making the system more vulnerable to future attacks. The generated attacks are then simulated in the integrated Gridlab-D/NS3 testbed to evaluate the impact on the system.

3.2.3 Optimal Mitigation Design

As part of the RD2C SCOREDEC project, we had developed a simulation-based co-design framework (See Figure 9) that can interface with a parameterized simulator and identify optimal parameters that will maximize a pre-specified resiliency criteria. In this use-case, the criteria is a linear combination of the cost associated with the mitigation and the total amount of energy drawn from the back-up generation.

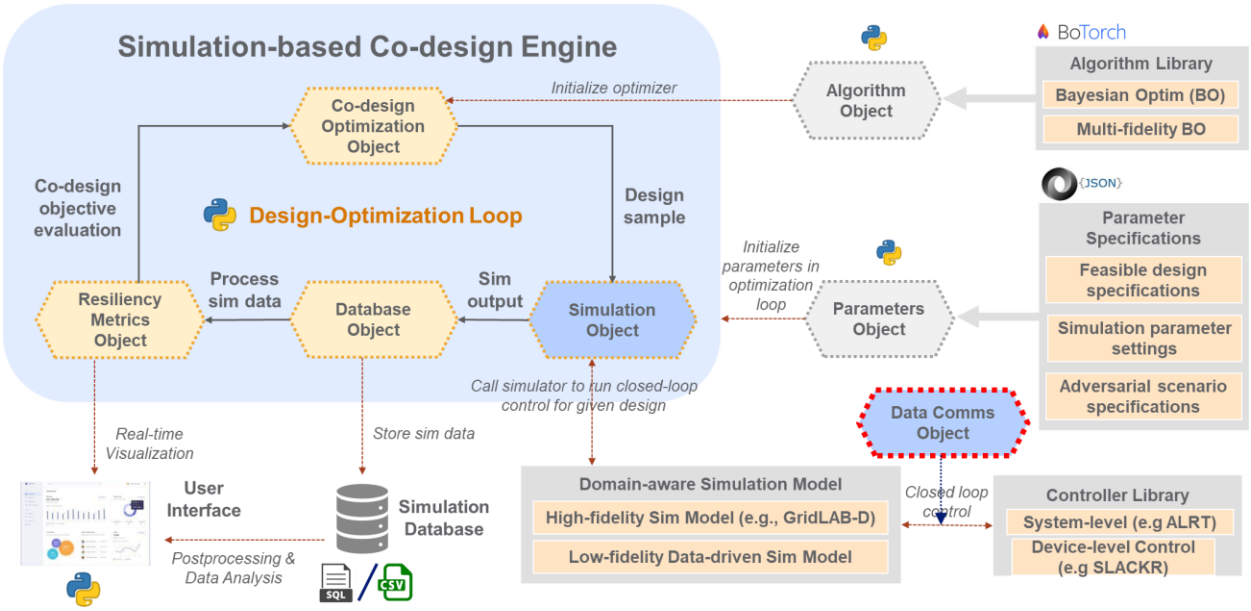

Figure 11 SCOREDEC Architecture

We leverage the SCOREDEC tool to identify the optimal mitigation parameters (specified by the optimal attack probability and the optimal detection probability) that will result in the least amount of dependency on the backup generation. The optimization approach utilizes an ask-tell Bayesian Optimization (BO) loop. The model is queried (or "asked") for the next set of mitigation parameters to be tested given the past record of simulations. Then, the mitigation parameters are passed on to the co-simulation environment. The results are then passed on (or "told") to the BO model which then utilizes an adaptive sampling approach to generate the next set of parameters. This process continues until a pre-specified number of iterations are complete and the result is the set of parameters with lowest value for the resiliency criteria.

3.2.4 Results

Backup generation reliability (Input weight between 0 and 1)	Optimal Attack Success Probability	Optimal Detection Probability	Fraction of power served by backup generation	Mitigation Measure deployment cost (Normalized)
1	0.7	0	1	0.0
0.8	0.3	0.2	0.7341	0.66
0.5	0.3	0.34	0.693	0.822
0.2	0.3	0.5	0.6043	1.0

Table 1: Optimal Mitigation Strategies for varying levels of backup generation reliability

Using the framework described in the previous sections, we run multiple experiments to understand how the mitigation strategy changes as we vary the reliability of the available backup generation. The reliability of the backup generation can change depending on several factors. For e.g, if the backup generation is an energy storage that is fully charged and can consistently meet load in the short-term horizon, we can assign a higher value of reliability to it. It can be seen (from the Table [1]) that when the reliability of the backup generation is set to 1, the optimal approach to minimize investment in mitigation as there are sufficient backup generation to serve the critical load and ride through the attack successfully. As we start to decrease reliability, there is a need to increase the investment in mitigation. This is reflected in the attack success probability and the detection probability parameters. As the reliability of the generation goes down, the attack success probability starts to decrease, and the detection probability starts to increase to reflect increased investment in the mitigation measures.

4.0 Capability Integration and Demonstration

The final integrated capability provides a simple user interface to perform model setup, attack orchestration, and monitoring functions. It removes the need to build and deploy individual tools, develop various configuration files and scripts to monitor the progress of the simulation. This section provides a working tutorial of the tool describing different user inputs and selections.

4.1 Model Setup

Using the integrated GLIMPSE tool, a custom, simple, and descriptive form is created to allow users to configure an attack scenario in NATIG and visualize the scenario on a power grid model with GLIMPSE. At the top of the form users can select the model and the communication topology they wish to use. By loading a model and applying a topology the rest of the form will be enabled for further configuration, and the model will be visualized in the background.

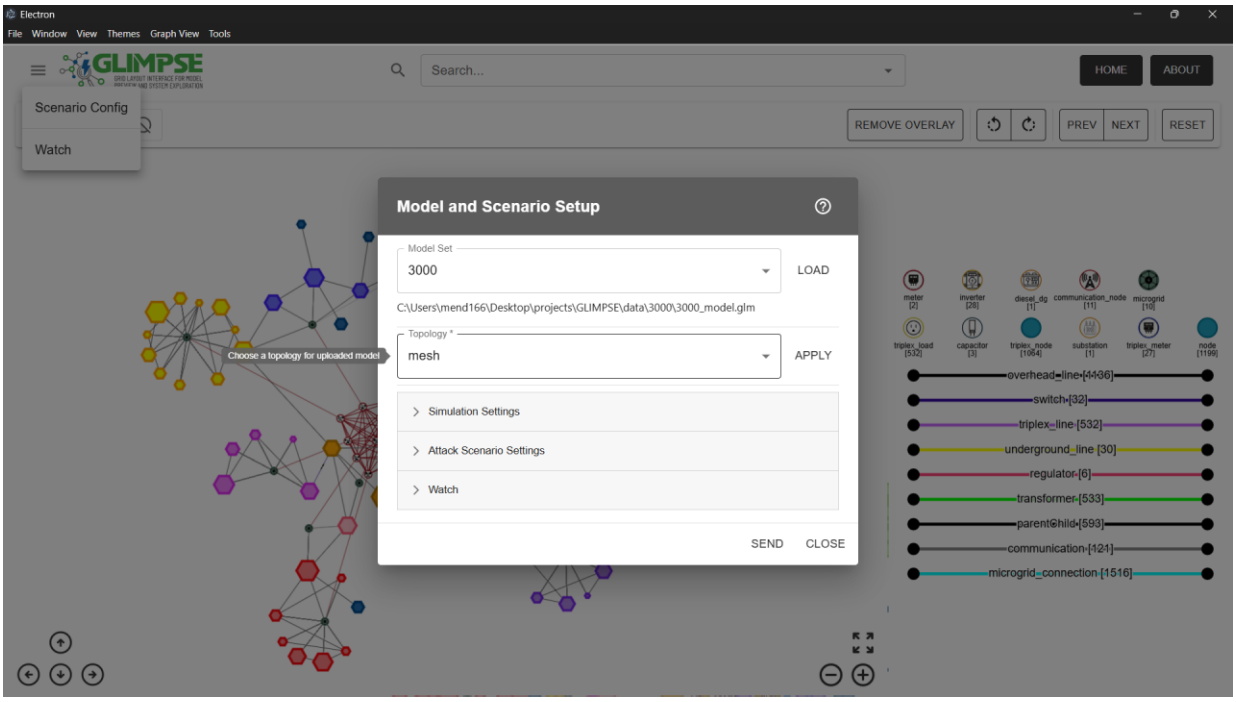

Figure 12 GLIMPSE Model and Scenario Setup form with 3000 model and mesh topology selected

4.2 Simulation Setup

In the simulation settings section, the user can configure duration of the simulation in number of seconds. Along with the simulated duration, users must input a frequency for pull requests in milliseconds. The rest of the simulation setup includes 3 switches for custom topology (switched on by default), generating PCAP for traffic information, and a seed input when the seed switch is selected.

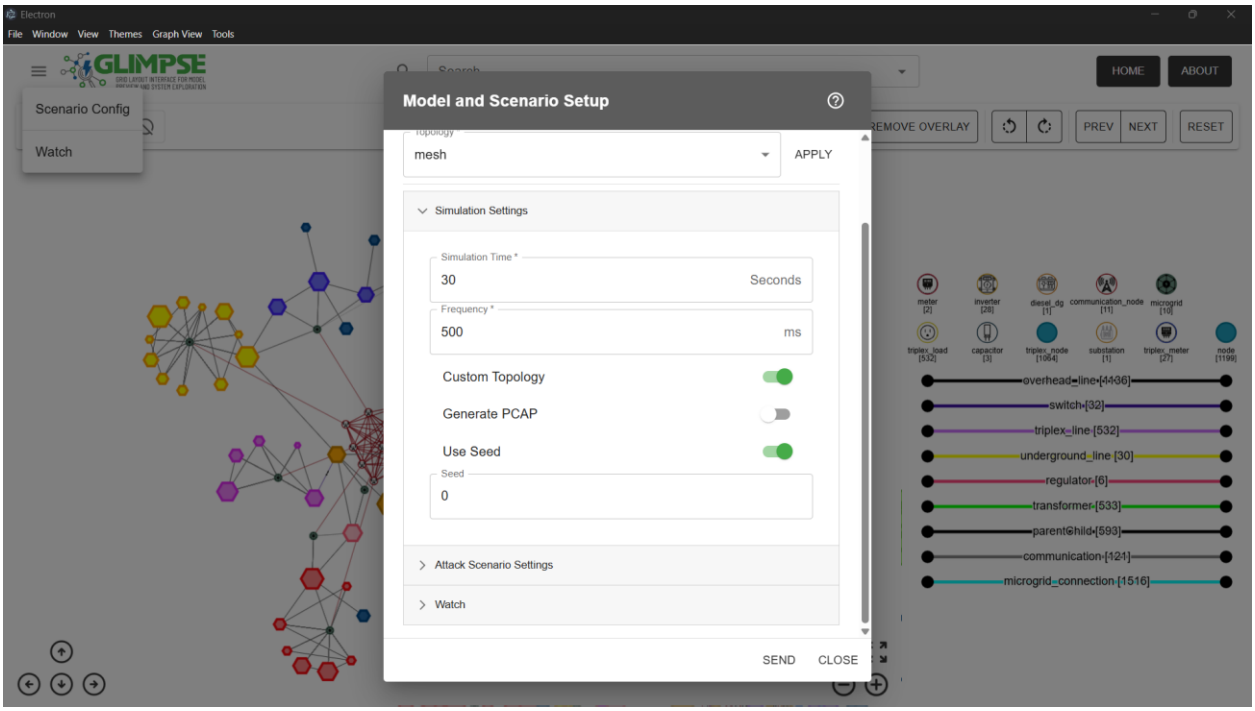

Figure 13 Figure Simulation Settings with filled in fields for simulation time and frequency

4.3 Attack Setup

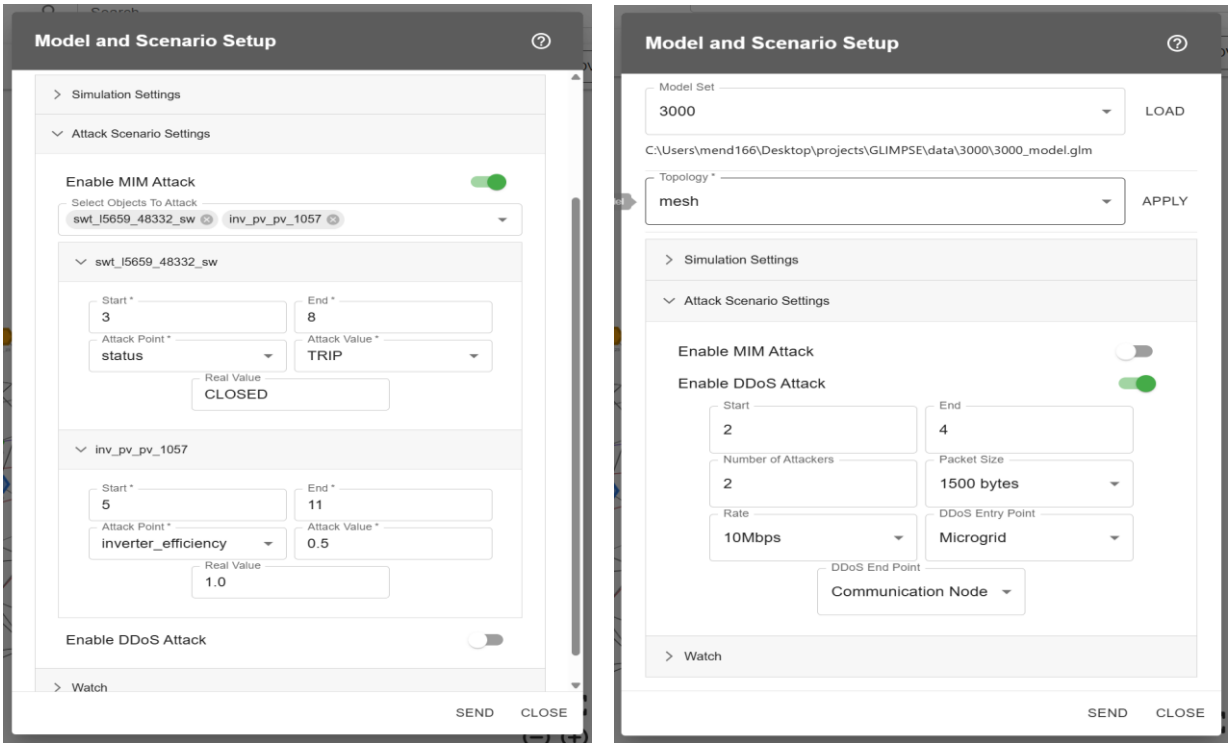

Figure 14MIM and DDoS configuration options

To setup an attack using the form, users can enable a MIM (Man in the Middle) attack or enable a DDoS (Distributed Denial of Service) attack each with its own set configuration fields. When enabling a MIM attack the user can attack one or multiple objects by selecting the object's ID in the search box. Each selected object has its own configuration allowing for further control of the attack. Currently only switch, generator, and valid inverter IDs show for the attack via MIM. By enabling the DDoS attack, users are presented with some fields to configure the attack. The user can enter the start and end time for the attack, the number of attackers, the packet size in bytes, the rate of bytes set from the attacker that ranges from 100Kbps to 10Gbps, the entry point and the end point. When filling out the form there is a tooltip that provides additional information for each input field.

4.4 Co-Simulation Monitoring

Before initiating a scenario, the user then can select some objects to watch in the watch drop down. By selecting objects to watch the user can check off any attributes they do not wish to monitor in the watch window. This watch window will contain a chart for each attribute of the selected object for monitoring. Once the user clicks the *SEND* button at the bottom of the form, they can open the watch window and wait for it to update as GLIMPSE receives simulation updates from NATIG.

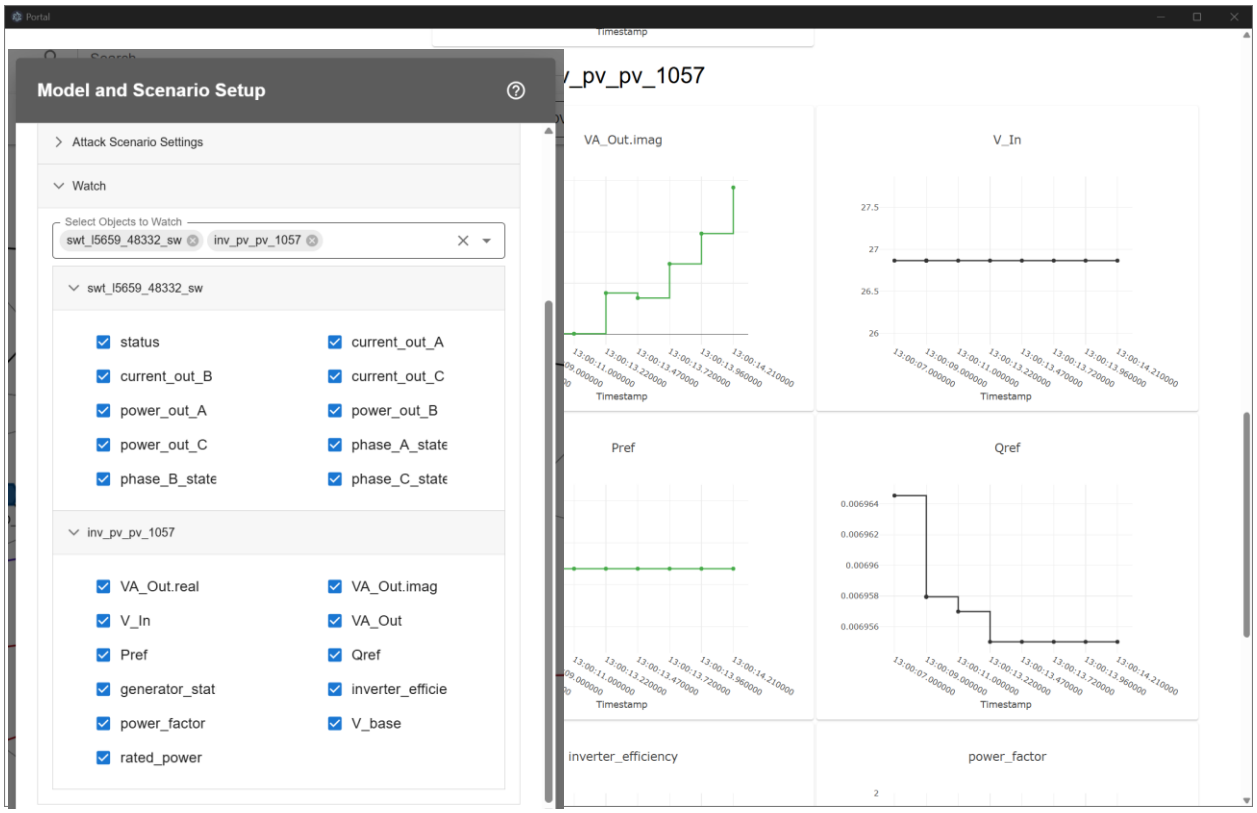

Figure 15 Watch section showing a switch and inverter selected to be watched showcasing the charts for each inverter attribute

5.0 References

Purohit, Sumit, Rounak Meyur, Oceane M. Bel, Armando Mendoza Sanchez, Braden K. Webb, and Sam A. Donald. *Efficient Hybrid Attack Graph Generation for Cyber-Physical System Resilience Experimentation: Final Project Report*. No. PNNL-36847. Pacific Northwest National Laboratory (PNNL), Richland, WA (United States), 2024.

Sanchez, Armando Mendoza, and Sumit Purohit. "GLIMPSE of Future Power Grid Models." In 2024 IEEE 18th International Conference on Semantic Computing (ICSC), pp. 224-225. IEEE, 2024.

Bel, Oceane, Joonseok Kim, William J. Hofer, Manisha Maharjan, Burhan Hyder, Sumit Purohit, and Shwetha Niddodi. "Co-simulation framework for network attack generation and monitoring." IEEE Access (2024).

Henderson, Thomas R., Mathieu Lacage, George F. Riley, Craig Dowell, and Joseph Kopena. "Network simulations with the ns-3 simulator." SIGCOMM demonstration 14, no. 14 (2008): 527.

Ramachandran, Thiagarajan, Aowabin Rahman, Soumya S. Vasisht, and Ramij Raja Hossain. Scalable Control Co-design for Resilient-by-Design Cyber Physical Systems. No. PNNL-37048. Pacific Northwest National Laboratory (PNNL), Richland, WA (United States), 2024.

Sarker, Partha S., et al. "Cyber-physical security and resiliency analysis testbed for critical microgrids with IEEE 2030.5." *2020 8th workshop on modeling and simulation of cyber-physical energy systems*. IEEE, 2020

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov