A Multi-level Fidelity Microgrid Testbed Model for Cybersecurity Experimentation

Aditya Ashok, Siddharth Sridhar, Tamara Becejac, Theora Rice,
Mathias Engels, Scott Harpool, Mark Rice, Thomas W. Edgar
Pacific Northwest National Laboratory

Abstract

When experimenting with cybersecurity technologies for industrial control systems, it is often difficult to develop a realistic, self-contained model that provides an ability to easily measure the effects of cyber behavior on the associated physical system. To address this challenge, we have created and instantiated a microgrid cyber-physical model, where both the power distribution and the individual loads are under the control and authority of one entity. This enables cybersecurity experimentation where attacks against the physical system (grid and buildings) can be measured and defended from a single entity's infrastructure. To achieve the appropriate levels of fidelity for cybersecurity effects, our microgrid model integrates multiple levels of simulation, hardware-in-the-loop, and virtualization. In this paper, we present how we designed and instantiated this test case model in a testbed infrastructure, our efforts to validate its operation, and an exemplary multistage attack scenario to showcase the model's utility.

1 Introduction

Cybersecurity for control systems is increasingly important, as it is strongly connected with the reliability of critical infrastructures that form the lifeline of modern society. The number and sophistication of attacks against these systems is increasing [1]. Recent attacks have been tailor-made to compromise and inflict damage on specific industrial control processes. It is understood that attackers, in addition to targeting control systems to impact their operation, may also seek to gain monetarily by holding the control system for ransom. There is a great need for field-tested cybersecurity solutions that help prevent and mitigate attacks against control systems while ensuring normal business function operation.

It is necessary to test cybersecurity solutions in realistic environments to truly evaluate their effectiveness. Real-world operational environments are generally unavailable for testing of new research, as any glitches could directly impact system availability. On the other hand, it is also extremely expensive to recreate dedicated real-world environments for testing. Testbeds offer an experimentation platform wherein the physical process and associated controls are represented using a combination of simulation, emulation, and industry-grade hardware and software.

There is a community stated need for cross-domain critical infrastructure testbed models [2]. The scale and scope of interconnected cross-domain systems quickly become unmanageable and unrealistic for a testbed. Self-contained or segment-able test cases that provide the desired interrelated systems while at a testbed implementable scale are highly valuable. A campus microgrid provides a special contained system that provides multiple cross-domain opportunities such as electrical, building, manufacturing, cyber, water, and physical security systems all within a self-contained model. A campus microgrid also provides a single authority of control where the various critical infrastructures are all driven by a single policy. This provides a great opportunity to test and experiment with various security technologies and processes and how they integrate. Essentially, a campus microgrid is an ideal test system that nicely balances the scale of system modeled on the testbed while still maintaining a high-level of fidelity to allow realistic cybersecurity experimentation.

A novel methodology and capability to instantiate a campus microgrid model within a cyber-physical testbed is presented in this paper. The overall model of the microgrid is provided, including three high-fidelity sub-models for direct integration to perform cybersecurity testing and experimentation. An architecture of simulation, emulation, and hardware-in-the-loop technologies is detailed that is capable of implementing the microgrid model in a cyber-physical testbed. Finally, an exemplar multistage cyber attack is demonstrated to showcase the value and capability of this approach.

2 Related Work

Real systems provide the perfect fidelity for an experiment. Campus microgrid testbeds like the one described in [3] provide all the features you would want to fully explore the effects of threat actions upon system operation. However, these

systems are operational and generally off limits to the cybersecurity research of interest or when they are available they are independent disconnected systems [4]. Using hobbyist systems, complex and large scale systems can be modeled [5], however, the generality of their behavior to industrial systems is tenuous at best. Replicas of realistic systems like [6] are generally too small-scale and lack the full features desired in critical infrastructure systems. This generally leads to utilizing simulation to achieve the scale of system models of interest. Simulation-based models of physical processes such as power grids and buildings have been well validated against real-world data and can achieve satisfactorily good results for quantifying physical impacts, but cyber targets need the highest levels of fidelity. These fidelity trade-offs of simulation and hardware-in-the-loop (HIL) are always an important concern when creating a hybrid testbed environment [7].

Simulators can be combined together to implement models of complex cyber-physical systems [8][9]. However, it is important to select high-fidelity sub-components of the model to study the attack injects and the interaction between cyber and physical domains. In [10] real controllers are connected to simulated processes, enabling the study of specific devices under various conditions, but not the whole system. Both [11] and [12] provide HIL power system equipment with emulated and simulated cyber components, which allows the study of cyber injects against the physical system, but neither provide inter-domain study. Finally, the authors of [13] and [14] have developed a testbed model that enables the study of cross-domain interaction between a train and electrical systems with simulated physical processes and integrated cyber components that only lacks the high-fidelity cyber network modeling that enables the demonstration, testing, and study of the common pivoting mechanisms utilized in recent public attacks [15][16] to gain access to and attack the Operational Technology (OT) components. The following sections describe a microgrid model and the integrated architecture of emulation, simulation, and HIL necessary to implement it in a cyber-physical testbed.

3 Campus Microgrid Model

As mentioned earlier, a microgrid that spans a single organization is an ideal test system that captures both the cyber and physical system aspects of a control system along with their interdependencies. Such an environment also presents a system of reasonable size to perform cybersecurity experimentation and to validate novel cybersecurity technologies.The following subsections briefly describe the components and their details.

3.1 Grid Model

The electrical distribution grid model serves as the centerpiece of the physical system model in the microgrid. This includes detailed modeling of the power distribution system including the feeders, transformers, voltage regulators, tap changers, and electrical loads on the microgrid. The use case scenario involves a microgrid that is representative of a large campus/organization. This microgrid has 37 nodes and is based on the standard IEEE 37 node distribution feeder model [17]. It consists of a single diesel generator to supply power when it is not in grid connected mode or islanded mode. There are two protection relays in this model. One controls the connection of the microgrid to the rest of the power grid and another controls the connection of the diesel generator to the microgrid. The buildings are connected as loads across the distribution system. The physical interaction between the building loads and the distribution system are the voltages of the grid to power the building systems and the power draw load amount used by the buildings. Figure 1 shows the grid model used.

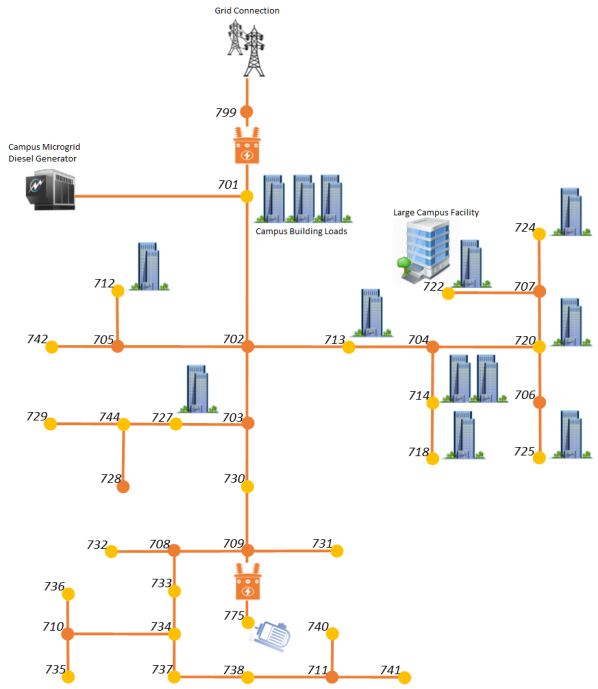

Figure 1: Microgrid model used for our experimentation

3.2 Building Model

The building models serve as the electrical loads on the grid model and are modeled at two different fidelities - (1) a low-fidelity building model that is able to accurately represent the buildings as an electrical load and (2) a high-fidelity building model that includes detailed modeling of the building's Heating and Ventilation Control (HVAC) System, in addition to representing its thermal and electrical characteristics. Specifically, this high-fidelity model was developed to represent the characteristics of a typical large office building in the United

States [18]. Ambient temperature and load conditions are provided from historical recordings.

3.3 Cyber Model

A microgrid system has computing and communication infrastructure at several levels. First, it includes a corporate network of the organization that connects to the external wide-area network. Second, it also has building and grid operations networks where physical controllers and sensors exist. Finally, control centers and their associated control network tie the other two layers together. In addition to the computing and communication infrastructures that are related to the control system, the cyber model also needs to include cybersecurity components. These include tools that are commonly found in real-world industrial control systems, such as tools for situation awareness, attack prevention, and incident response. To address these requirements, commonly found cybersecurity technologies in control systems, such as firewall hardware and intrusion detection systems have been integrated into the model. These technologies provide a baseline cybersecurity configuration that closely mimics real-world industrial control systems. The model is also designed to be flexible enough to host other novel technologies for verification and validation. Figure 2 depicts the cyber model of the microgrid.

4 Instantiating a Microgrid Model on a Testbed

Creating a high-fidelity microgrid model is beyond the resources of most, if not all, researchers. Implementing the complexity and interaction of the various models in a testbed requires a mix of simulation, emulation, and real hardware. In this section, we describe how we instantiated the various aspects of the microgrid model into a testbed (shown in Figure 3) for enabling realistic cybersecurity experimentation.

4.1 Physical System Simulation

As described earlier in Figure 1, the electrical model of the microgrid is one of the central pieces. We used the OPAL-RT eMEGASim real-time power system simulator [19] to implement our microgrid electrical model. The electrical model consists of various loads that are the buildings and facilities within the organization's campus. These electrical loads on the microgrid are modeled using two simulation tools namely GridLAB-D [20] and Dymola [21].

While the building load models in GridLAB-D include simplified thermal and electrical models of typical small office buildings within the campus, the corresponding model implemented in Dymola includes a detailed modeling of the building automation control systems within a critical facility on the campus. These include the Air Handling Units (AHU) and Variable Air Volume (VAV) boxes. The building thermal components that are modeled also have an electrical equivalent, providing power consumption information to the microgrid model. We utilized a Python-based application programming interface (API) provided by OPAL-RT to update load information coming from building models running in GridLAB-D and Dymola.

In order to orchestrate the co-simulation between the OPAL-RT grid model and the GridLAB-D and Dymola building models, we leveraged the Framework for Network Co-simulation (FNCS) [22] and the VOLTTRON platform [22, 23]. The OPAL-RT grid model provided the electrical voltages at periodic intervals and received load consumption information from GridLAB-D and Dymola. While GridLAB-D building models directly published and subscribed to messages on the FNCS, we developed a VOLTTRON agent that connected to Dymola over a socket connection to exchange co-simulation information, which was then published to FNCS.

While there are several equivalent tools for modeling a distribution level microgrid, we used the OPAL-RT eMEGASim model (MATLAB Simscape Electrical-based) due to its high-fidelity. We used a modified version of the IEEE 37 node test feeder model that has been well-studied and validated by IEEE Distribution Systems Analysis Subcommittee [17]. We also leveraged a vast library of realistic, widely-used distribution feeder models developed in GridLAB-D for the low-fidelity building models in the microgrid [24]. Similarly, Dymola was chosen to model the high-fidelity buildings as this also builds on top of an existing model that has been validated by a detailed prior work at PNNL in this area [18]. While the individual microgrid and building models have been validated by several researchers separately, we would like to acknowledge that there has not been any major effort to validate these models as an integrated co-simulation so far. This is also due to the sheer complexity of creating an integrated microgrid and buildings model in a single software tool such as the OPAL-RT eMEGASim simulator as a benchmark. We intend to validate our microgrid co-simulation more thoroughly as a part of our future work.

4.2 Control System

In the instantiated microgrid model there are two types of control system components, (1) grid control system and (2) building control system components. Grid control systems include the sensors and controllers interacting with the generator and switching infrastructure of the distribution system. The building control systems components include the sensors and controllers interacting with the HVAC systems. Both are integrated with a campus control center where operators can oversee the operation of the microgrid.

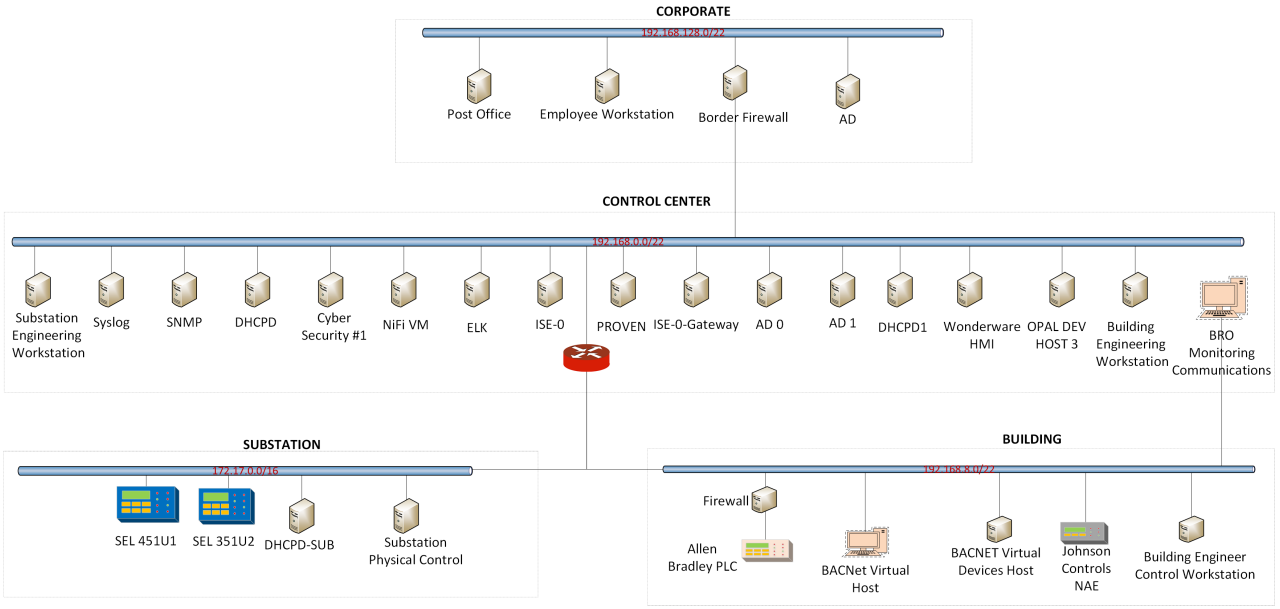

Figure 2: Multi-level fidelity microgrid testbed architecture - cyber system

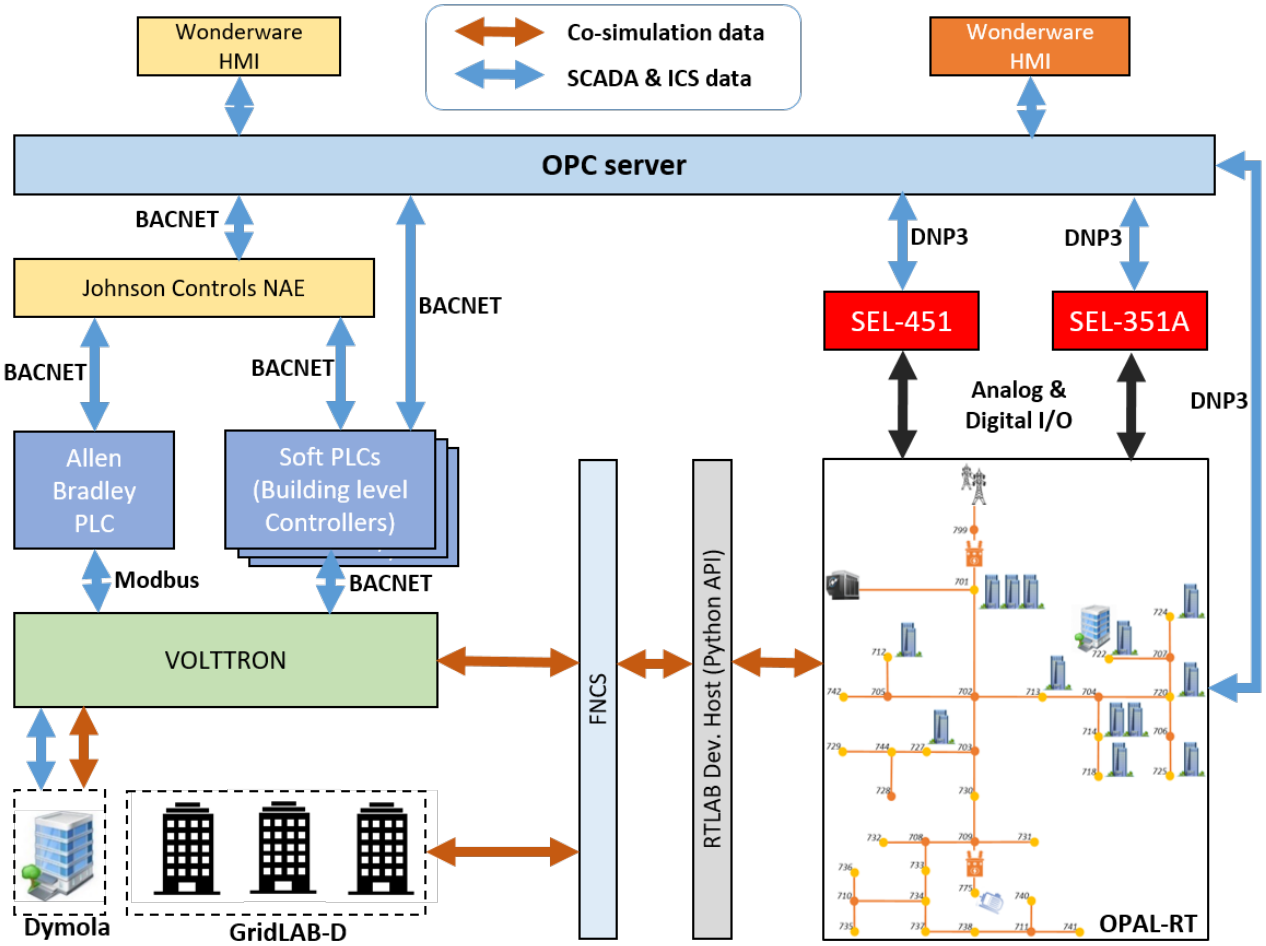

Figure 3: Architecture of integrated testbed technologies for implementing microgrid models

4.2.1 Grid Control System

Real power system distribution protection relays, SEL 351 and 451, were integrated to protect the microgrid electrical assets. These relays were interfaced directly to the analog output cards on our OPAL-RT simulator and received the electrical signals directly to sense the voltages and currents on the microgrid. Relay commands and breaker status information were exchanged with the grid model using the digital input and output cards on the OPAL-RT simulator. The protection relays send telemetry information to the grid operations control center in the campus over the DNP3 protocol where the data is collected in an Open Platform Communications (OPC) server. This data is then fed into Wonderware to visualize the information collected about the state of the microgrid.

4.2.2 Building Control System

We instantiated several virtual building controllers that received measurements from the building models running in GridLAB-D over the BACnet protocol via the VOLTTRON platform. This data would then be passed to the OPC server at the building operations control center. Similarly, the data coming from the detailed building model running in Dymola was passed on to both real programmable logic controllers (PLC) and virtual devices to implement controllers for AHUs in the building modeled. The data from Dymola was sent over Modbus to the real PLC and over BACnet to the virtual devices implementing the building automation controllers. This building control system data from both the real and virtual controllers is collected by a building supervisory controller, Johnson Controls Network Automation Engine, over BACnet and then passed on to the OPC server at the building operations control center. Building data in the OPC server was also visualized using Wonderware in a manner similar to the microgrid data.

4.3 Cyber Systems

As mentioned in Section 3, the cyber system is composed of the corporate infrastructure, the control system operation elements, the computing interfaces to the field devices, and implemented cybersecurity technologies. Within this model, we deployed software on both dedicated hardware and virtual machines (VMs), paired with virtual networking, to achieve the amount of flexibility and fidelity needed for our experimentation. The networking for the model was broken up into five subnets: corporate, control center, building, substation, and under network. The first four can be seen in Figure 2, but a fifth, out of experimental bounds, network was necessary to provide communication between the simulators and testbed orchestration tools.

The corporate network represents common corporate operational machines for the model. This includes employee workstations, email servers, active directory, and a basic software firewall. These different types of computers are instantiated as VMs within the testbed environment, so that they can be reconfigured, manipulated, and deployed in a flexible manner determined by the experiment.

The control center network contains a large number of VMs concerned with process operation. This includes substation and building control engineering workstations, the human machine interaction (HMI) computer, and other support type devices. However, it also includes some VMs dedicated to logging and security, such as a syslog server, an ELK instantiation, and a deployment of Radiflow iSID. Radiflow iSID was chosen because it is representative of security software that can be found deployed in these environments. This network also hosts the management interface for the Etherwatch Firewall we have deployed in the substation environment.

To maintain high fidelity in our experimentation, both the building and substation networks primarily contain the field control devices that are part of the represented physical process. Within the building network, we have also deployed an engineering access host as well as a virtual devices host that simulates multiple endpoint devices speaking to the control system via BACnet. An Ultra Electronics Etherwatch industrial firewall has been placed in line with the Allen Bradley PLC, to allow for security monitoring and access control. Floating outside of these networks there is a Raspberry Pi that is tapped into the port communications of all of the physical field control devices. This is utilized for both cybersecurity experiments in addition to experiment monitoring and troubleshooting purposes. In the substation network, there is also a physical device display connected that allows us to visually demonstrate substation activity.

The last subnet is the "under network", which is a physics instrumentation layer of our model. It contains the OPAL-RT, GridLAB-D, FNCS, Dymola, and VOLLTRON endpoints, as well as another physical device display that indicates building control system status. This modeling software is run on a combination of bare metal and VMs, depending on the resources required.

5 A Multistage Cyber Attack Case Study

The architecture and model that has been presented provides the ability to target and provide experimental injects within the enterprise network, control room, building control system, and electrical substation. The modeled system provides interaction and study of impacts of attacks across each of the three infrastructure domains; cyber, building, and power. A multistage cyber attack is necessary to showcase how the various models interact and can demonstrate the interrelated effects of one on the others.

The ICS kill chain is a model of cyber attacks that requires multiple stages [15]. Where the traditional cyber kill chain model ends at the exploitation of the enterprise cyber environment, the ICS kill chain has a second stage of pivoting

to and manipulating a physical process. To provide fidelity and realism to our case study, the two cyber attacks on the Ukraine power grid were modeled. Our multistage test case involves an initial infection and attack on a power substation device to island the campus microgrid which is modeled around the BlackEnergy malware and techniques used in the 2015 Ukraine power grid cyber attack [15]. A second phase of the cyber attack targets building controllers to cause a generator protection scheme to disrupt power in the microgrid, which is modeled after the CrashOverride malware [16].

In this use case scenario, the objective of the attacker is to disrupt the power supply to the entire microgrid, thereby causing an impact to a critical building on the campus and to cause fear, uncertainty, and doubt in the campus operators. In order to achieve this, the attacker performs the following actions:

1. Isolates the microgrid from the bulk power grid by opening the first protective relay. To achieve this, the attacker changes settings on the substation relay such that the breaker is always stuck at "open".

2. Sends commands to all large buildings on campus to turn off the AHU fans and thereby drop load instantly. This action results in a large frequency spike in the microgrid, eventually causing the distributed generator to trip due to over-frequency protection. This action would isolate the last remaining source of power in the microgrid, causing a blackout.

5.1 Attack Execution

In order to achieve the above actions, the attacker executes the following steps. Note, the detailed integration of cyber and physical models along with associated technologies enabled us to implement the following realistic attack execution. This attack was designed based on real-world industrial control system cybersecurity incidents [16, 15]. All of the steps of the example attack were implemented using open source capabilities like the Kali Linux distribution and free networking tools.

1. *Phishing Attack* - Execute a phishing attack on a user in the corporate network by sending an email with a malicious attachment using a Metasploit Microsoft Word Macro exploit. The user opening the attachment creates a reverse shell persistent connection to a remote command and control server into the corporate network of the organization.

2. *Credentials Theft* - Installs a keystroke logger on victim machine and successfully steals credentials.

3. *Pivot to Grid OT* - Uses stolen credentials to virtual private network (VPN) into an engineering workstation on the control network.

4. *Craft Payload* - Searches the workstation for protective device settings and is able to craft relay settings to a target relay to achieve the attack objective.

5. *Execute attack stage 1* - Executes a script to login to the relay using default credentials and performs a settings change (always open and disable update).

6. *Pivot to Building OT* - Leverages the email account of first corporate victim to target a building engineer to compromise a workstation that is used to program building automation controllers across campus by network pivoting.

7. *Perform reconnaissance* - Observes that improper network segmentation enables access to BACnet network cards on these building controllers.

8. *Prepare for attack* - Uses the BACnet protocol feature to perform tag discovery on the building controllers to determine the tags for controlling AHU fans.

9. *Execute attack stage 2* - Crafts and executes a script that will trip the AHU fans by turning them off using BACnet commands to multiple buildings.

5.2 Experimental results

In order to study the impact of the multistage cyber attack on the microgrid, we instrumented several recorders in our grid simulation to capture essential quantities such as voltages, currents, system loads, and microgrid frequency. Figure 4 presents a plot of voltages at node 701 in the microgrid, the power supplied by the grid, power supplied by the diesel generator (DG), and the frequency of the generator, respectively, for a run of the attack scenario where no defense mechanisms have been instantiated.

From Figure 4, we can see the impact of attacker actions on voltage, power, and frequency, respectively. As we observe in the bottom subplot, the voltages across the three phases on node 701 are impacted differently during the islanding of the microgrid. In the middle subplot, we observe that the total load initially is supplied by a combination of power from the grid and the DG. Whereas, after the first attack on the grid protection relay where the breaker opens, the total load is taken by the DG and then eventually, the load drops to zero when the various buildings on the microgrid drop out, causing the DG to trip based on over-frequency protection.

On the top subplot, we can see how the frequency of the microgrid DG varies through the scenario. Initially, the frequency is around the nominal frequency of 60 Hz. When the grid protection relay trips and islands the microgrid, we can see a frequency drop temporarily due to the sudden loss of generation (item 1 in Figure 4). Frequency recovers quickly as the DG picks up the total load quickly and stays around the nominal value until the dropout of building loads due

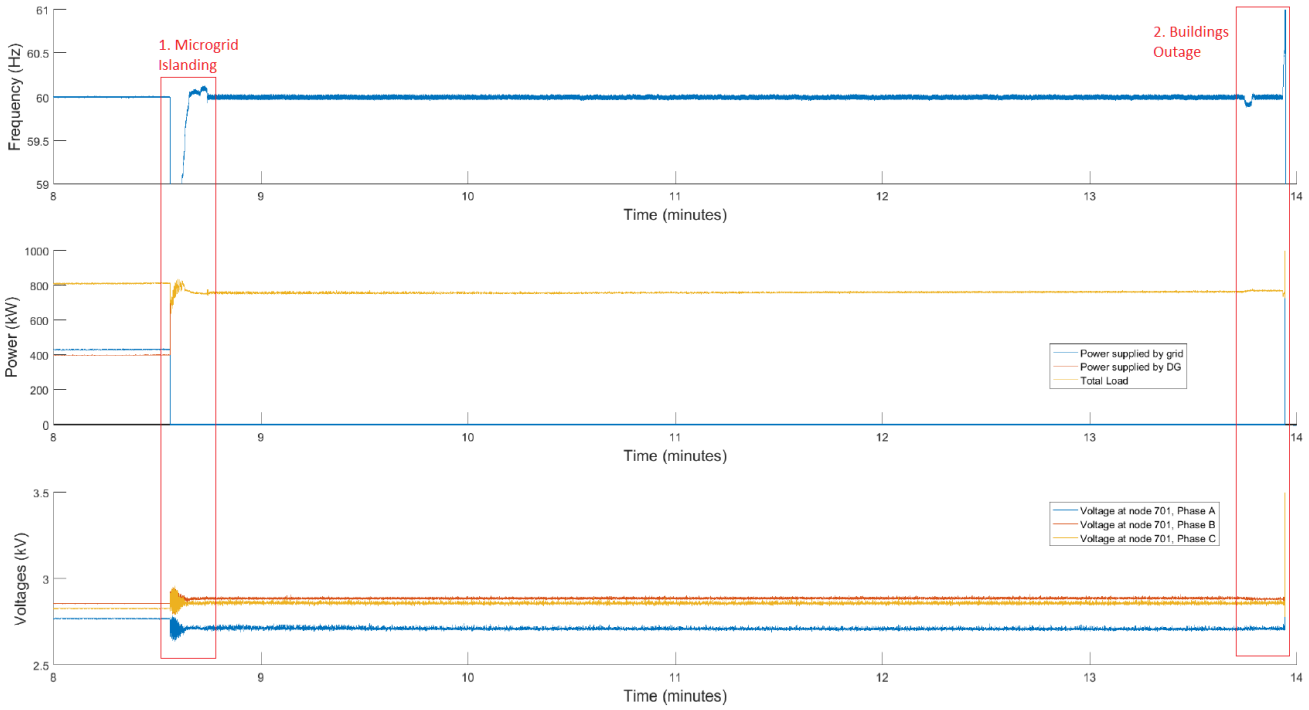

Figure 4: Experimental results for cyber attack scenario from the grid simulator

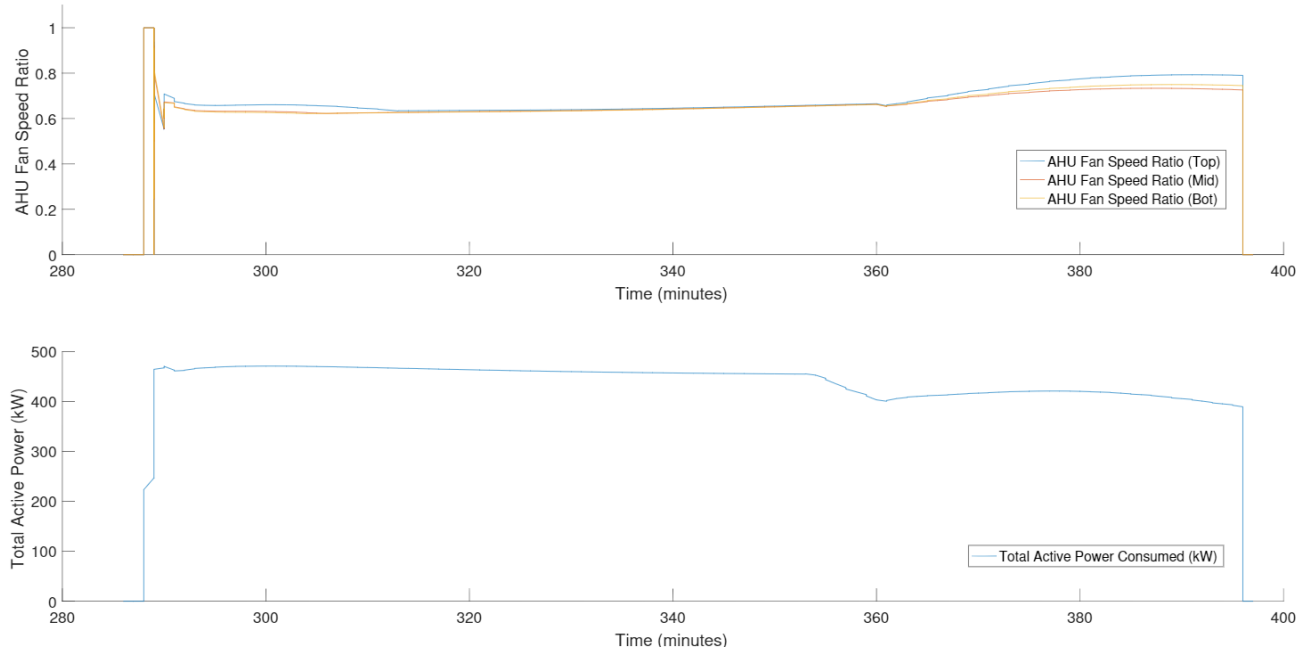

Figure 5: Experimental results for a generalized scenario from the high-fidelity building simulator

the second stage of the attack. The impact of the building loads dropping out can be seen as a sudden spike in frequency as there is an excess of power produced by the DG. This frequency spike crosses 60.5 Hz, which has been set up as an over-frequency threshold to protect the DG from damage. Consequently, the DG trips and this causes a disruption of power to the critical loads in the microgrid after a quick transient surge (item 2 in Figure 4).

The high-fidelity building model in our microgrid test system includes a detailed modeling of the various building automation components including the Air Handling Units (AHU) and their controllers, in addition to the electrical characteristics. In order to showcase how the attack scenario would impact the buildings on the microgrid, we have specifically plotted the AHU fan speed ratios and the total power consumed by the high-fidelity building for a generalized scenario where the fans are on and off over the period of a few hours in a day. Figure 5 shows results from the high-fidelity building model running in Dymola for the generalized scenario. Typically, an AHU's fan speed ratio varies based on the temperature settings, external weather, and occupants in the building. As we can see in Figure 5, AHUs are a major source of electrical demand on the microgrid when the fans are on varying their consumption according to the fan speeds. This is clearly seen by the variation in the total active power consumed by the building when the fans are on. When the attacker turns the AHU fans off, the building power consumption drops to almost zero. Similar to the impact shown in Figure 5, when the attacker executes the second attack to simultaneously turn off all the AHUs across the various buildings on campus, a large portion of the microgrid load demand is suddenly lost causing a surplus in generation. Consequently, this results in a frequency spike that isolates the DG causing a total blackout in the microgrid (item 2 in Figure 4).

6 Conclusion

There is a strong need to create scalable, high-fidelity, and realistic operational environments to test and evaluate cybersecurity research. At the same time, identifying, developing, and instantiating a self-contained, reasonably complex, interdependent, and non-trivial test system on a testbed is extremely valuable in verifying and validating novel security technologies and their interplay. We believe that a microgrid model as a test case provides multiple cross-domain opportunities such as electrical, building, manufacturing, cyber, water, and physical security systems, while being self-contained.

In this paper, we presented a novel methodology and described a capability to instantiate a campus microgrid model within a cyber-physical testbed. The overall model of the microgrid that we described includes three high-fidelity submodels for direct integration to perform cybersecurity testing and experimentation. We have described an architecture consisting of simulation, emulation, and HIL technologies that is capable of implementing the microgrid model in a cyber-physical testbed in detail. Finally, we presented an exemplar multistage cyber attack to demonstrate and showcase the value and capability of our approach.

Acknowledgments

PNNL is a multi-program national laboratory operated by Battelle for the U.S. Department of Energy under contract No. DE-AC05-76RL01830.

Availability

The model, tools, and data developed for the described capability will be hosted at: https://cyberphysical.pnnl.gov/data-sets.aspx

References

[1] R. Lemos. *Five Trends in Attacks on Industrial Control Systems*. Oct. 2018. URL: https://www.eweek.com/security/five-trends-in-attacks-on-industrial-control-systems.

[2] D Balenson, L Tinnel, and T Benzel. "Cybersecurity experimentation of the future (CEF): catalyzing a new generation of experimental cybersecurity research". In: *SRI International, Tech. Rep.* (2015).

[3] A. Bonfiglio et al. "The Smart Polygeneration Microgrid test-bed facility of Genoa University". In: *2012 47th International Universities Power Engineering Conference (UPEC)*. Sept. 2012, pp. 1–6. DOI: 10.1109/UPEC.2012.6398656.

[4] I. N. Fovino et al. "An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants". In: *3rd International Conference on Human System Interaction*. May 2010, pp. 679–686. DOI: 10.1109/HSI.2010.5514494.

[5] Jose Rubio-Hernan, Juan Rodolfo-Mejias, and Joaquın Garcıa-Alfaro. "Security of Cyber-Physical Systems. From Theory to Testbeds and Validation". In: *CoRR* abs/1711.11464 (2017). arXiv: 1711.11464. URL: http://arxiv.org/abs/1711.11464.

[6] E. E. Miciolino et al. "Communications network analysis in a SCADA system testbed under cyber-attacks". In: *2015 23rd Telecommunications Forum Telfor (TELFOR)*. Nov. 2015, pp. 341–344. DOI: 10.1109/TELFOR.2015.7377479.

[7] H. Gao et al. “The Design of ICS Testbed Based on Emulation, Physical, and Simulation (EPS-ICS Testbed)”. In: *2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. Oct. 2013, pp. 420–423. DOI: 10.1109/IIH-MSP.2013.111.

[8] M. Mallouhi et al. “A testbed for analyzing security of SCADA control systems (TASSCS)”. In: *ISGT 2011*. Jan. 2011, pp. 1–7. DOI: 10.1109/ISGT.2011.5759169.

[9] Daniele Antonioli et al. “Gamifying ICS Security Training and Research: Design, Implementation, and Results of S3”. In: *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*. CPS ’17. Dallas, Texas, USA: ACM, 2017, pp. 93–102. ISBN: 978-1-4503-5394-6. DOI: 10.1145/3140241.3140253. URL: http://doi.acm.org/10.1145/3140241.3140253.

[10] Kumaraguru Prabakar et al. “Hardware-in-the-Loop Test Bed and Test Methodology for Microgrid Controller Evaluation”. In: *2018 IEEE/PES Transmission and Distribution Conference and Exposition* (2018), pp. 1–9.

[11] Seokcheol Lee et al. “Design and implementation of cybersecurity testbed for industrial IoT systems”. In: *The Journal of Supercomputing* 74.9 (Sept. 2018), pp. 4506–4520. ISSN: 1573-0484. DOI: 10.1007/s11227-017-2219-z. URL: https://doi.org/10.1007/s11227-017-2219-z.

[12] A. Ashok, S. Krishnaswamy, and M. Govindarasu. “PowerCyber: A remotely accessible testbed for Cyber Physical security of the Smart Grid”. In: *2016 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. Sept. 2016, pp. 1–5. DOI: 10.1109/ISGT.2016.7781277.

[13] Béla Genge, Christos Siaterlis, and Marc Hohenadel. “AMICI: An Assessment Platform for Multi-domain Security Experimentation on Critical Infrastructures”. In: *Critical Information Infrastructures Security*. Ed. by Bernhard M. Hämmerli, Nils Kalstad Svendsen, and Javier Lopez. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 228–239. ISBN: 978-3-642-41485-5.

[14] Y. Soupionis and T. Benoist. “Cyber-physical testbed - The impact of cyber attacks and the human factor”. In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. Dec. 2015, pp. 326–331. DOI: 10.1109/ICITST.2015.7412114.

[15] Robert M Lee, Michael J Assante, and Tim Conway. “Analysis of the cyber attack on the Ukrainian power grid: Defense use case”. In: *SANS Institute & the Electricity Information Sharing and Analysis Center* (2016).

[16] Robert M Lee, MJ Assante, and T Conway. “CRASHOVERRIDE: Analysis of the threat to electric grid operations”. In: *Dragos Inc., March* (2017).

[17] IEEE Power and Energy Society - Distribution System Analysis Subcommittee Report. *Radial Distribution Test Feeders*. URL: http://sites.ieee.org/pes-testfeeders/files/2017/08/testfeeders.pdf.

[18] Sen Huang et al. “A Control-oriented Building Envelope and HVAC System Simulation Model for a Typical Large Office Building”. In: (Sept. 2018).

[19] OPAL-RT Technologies. *eMEGASim - Real-Time Digital Simulator for Power System Engineers*. URL: https://www.opal-rt.com/system-emegasim/.

[20] D. P. Chassin, K. Schneider, and C. Gerkensmeyer. “GridLAB-D: An open-source power systems modeling and simulation environment”. In: *2008 IEEE/PES Transmission and Distribution Conference and Exposition*. 2008, pp. 1–5. DOI: 10.1109/TDC.2008.4517260.

[21] The University of California through Lawrence Berkeley National Laboratory. URL: http://simulationresearch.lbl.gov/modelica/.

[22] R. Huang et al. “Open-source framework for power system transmission and distribution dynamics co-simulation”. In: *IET Generation, Transmission Distribution* 11.12 (2017), pp. 3152–3162. ISSN: 1751-8687. DOI: 10.1049/iet-gtd.2016.1556.

[23] Jereme Haack et al. “Volttron: An Agent Platform for the Smart Grid”. In: *Proceedings of the 2013 International Conference on Autonomous Agents and Multi-agent Systems*. AAMAS ’13. St. Paul, MN, USA: International Foundation for Autonomous Agents and Multiagent Systems, 2013, pp. 1367–1368. ISBN: 978-1-4503-1993-5. URL: http://dl.acm.org/citation.cfm?id=2484920.2485228.

[24] Schneider K.P., Y. Chen, D.P. Chassin, R.G. Pratt, D.W. Engel, and S.E. Thompson. *Modern Grid Initiative Distribution Taxonomy - Final Report, PNNL-18035, Richland, WA: Pacific Northwest National Laboratory.* Nov. 2008.