A Cyber-Physical Testbed Design for the Electric Power Grid

Zachary O'Toole, Christian Moya, Connor Rubin, Alec Schnabel, Jiankang Wang
Dept. of Electrical and Computer Engineering
The Ohio State University
Columbus, Ohio, USA
{otoole.53, moyacalderon.1, rubin.191, schnabel.24, wang.6536}@osu.edu

***Abstract*—A primary challenge to studying power system cybersecurity is understanding and validating attacks' cyber-physical causal chains. However, the electrical power grid is a critical infrastructure, and thus experimenting on the actual grid is rarely allowed. Aiming to address this challenge, this paper proposes a cyber-physical testbed design, consisting of three main components: energy management system, communications, and the physical power system simulator. The energy management system features real-time information processing. The communications are capable of emulating network delays and data transmission using industry standard protocols. Finally, the physical power grid is simulated in a cyber-physical synchronized environment. The performance of the testbed design's initial implementations is demonstrated with two attacks, False Data Injection and Denial-of-Service, on the IEEE-14 Bus system.**

***Index Terms*—Power grid cybersecurity.**

I. Introduction

The development of cyber-infrastructure has led to the advancement of many aspects of the electrical power grid, such as automatic control, real-time metering and end-user engagement. However, cyber-attacks are becoming a major threat to the grid's reliability and security [1]. Famous examples include the Denial-of-Service (DoS) call-center attack in conjunction with other attacks in Ukraine, December 2015. The attacks left 3 energy distribution companies paralyzed, 30 substations incapacitated, and about 230,000 people without power for a period of one to six hours [2].

To combat these potential attacks, it is crucial to develop new security measures to safeguard our energy economy as well as the infrastructure that it relies on. A primary challenge to the development of security is understanding attacks' cyber-physical causal chains. In addition, these security measures must be tested rigorously to ensure their reliability across all circumstances. However, experimenting on the public grid is not feasible for the following reasons. First, the power grid is one of the most complex networks, consisting of millions of nodes and lines, each of which may contain natural deviations. Hence it would be extremely difficult to isolate all contributing factors and identify the cyber-physical traces. Second, any power outage is always associated with a great amount of social and economic cost, making repetitive experiments unaffordable. Aiming to address this challenge, we present a design of a cyber-physical testbed that can be manipulated, measured, attacked, and defended for security testing purposes.

A. Related Works

Many testbeds have been built recently for the specific needs of smart grid research. Representative works include the testbeds constructed at Washington State University (WSU) and Iowa State University (ISU). WSU's testbed utilized a Real Time Digital Simulator (RTDS) to perform cyber-attacks and to measure the results. Phasor measurement units (PMUs), both simulated virtually within the RTDS and in physical form, are used to collect measurements via Giga-Transceiver Digital/Analog Input and Output cards meeting the IEEE C37.118-2011 protocol [3]. ISU's PowerCyber was built with a similar structure, and its network simulator is further customized to emulate the communication environment [5].

However, a weakness of their designs is the scalability. In particular, the testbeds do not support remote connection capabilities and wireless communication. This not only misses an important aspect of future smart grid communication, but also requires the test subjects to be physically connected to the testbeds, limiting the possibilities of interconnecting with other testbeds and experiments at a greater scale [4].

Improving on the scalability, University of South Florida (USF) [6] and Mississippi State University (MSU) [7] built testbeds consisting of a Plant Information (PI) system, which was developed by OSIsoft. In USF's design, the PI system replaces the energy management system (EMS) and serves as a central hub. On the contrary, MSU's design used an RTDS with a programmable logic controller (PLC) and NI-PXI system to emulate the EMS. Using LabVIEW as the main user portal, the NI-PXI system acts as the connection between human and the PLC.

In both designs, the PI system plays a critical role. On one hand, it can process many communication protocols, reading and sending back data. On the other hand, it can connect the real-time simulator with PMUs, the cloud, and other externals. These designs promise scalability as well as high-resolution data transmission. However, the designs omitted the network simulator and oversimplified the Supervisory Control And

This work is supported by American Electric Power and NSF under award number 1711048.

Data Acquisition (SCADA) system. This will likely lead to inaccurate results due to the lack of a detailed network model, such as network traffic and transmission delays.

Despite many variations in testbed components, other designs possess similar strengths and weakness of the previously discussed testbeds. For example, the design in [8] strengthened the communication network analysis by using OPNET, but does not support SCADA communication protocols. Another example includes the testbed at Texas A&M University, which allows real-time analysis by integrating OPNET, RTDS, and LabVIEW PXI [9], but lacks of scalability. The deficiencies of the existing works motivate a new design.

B. Our Work

To understand and validate attacks' cyber-physical causal chains in a more realistic and scalable environment, this paper proposes a cyber-physical testbed design, consisting of three main components: energy management system (EMS), communications network using different industry SCADA protocols (*i.e.,* DNP3 or IEC-61850), and a physical power system simulator. To address the shortcomings discussed in the previous section, the proposed testbed design has the following characteristics:

1) *Scalability.* Remote connection support provides a large-scale environment for testing, and wireless communication support provides an alternate communication infrastructure.
2) *Detailed cyber-systems.* A network simulator is incorporated to model realistic limitations (*e.g.,* transmission delays) from large-scale communication networks.
3) *Network Security Testing.* An Intrusion Detection System (IDS) is incorporated to monitor network traffic and attack's cyber-traces.

The rest of the paper is organized as follows. Section II analyzes the proposed system architecture. Section III describes the architecture of the testbed design's first prototype. The performance of the first prototype is tested in Section IV. Finally, Section V concludes the paper.

II. Proposed System Architecture

In this section, we describe the proposed design of a cyber-physical testbed. The infrastructure consists of three components (see Fig. 1): EMS, communications, and physical power grid.

A. Energy Management System (EMS)

The EMS is responsible for monitoring and controlling the power grid. As shown on the left block of Fig. 1, the communication protocol used on the EMS bus is Distributed Network Protocol (DNP3). This protocol is commonly used in SCADA systems to interface the control center and substations. Furthermore, everything contained in the EMS is under a local area network (LAN). This includes components such as Human-Machine Interface (HMI), a database of system logs, control functions, and the server. Finally, the server is used to send and receive data with the physical grid.

The EMS incorporates remote access, which enables the testbed to be used and integrated with other testbeds, providing a large-scale environment for testing. [14]. The remote access is implemented using secure shell (SSH) for direct operator control. An operator can initiate a connection request with the EMS server, on a designated port by sending credentials. The server accepts the connection if the credentials are valid, and the client and server communicate via encrypted messages. Additionally, a client system is placed on the EMS bus to connect with other control centers. This provides the desired scalability of large-scale SCADA system testing.

B. Physical Power Grid

The physical power grid response is simulated on a real-time simulator (OPAL-RT). The real-time simulator allows synchronized simulation with Hardware-In-the-Loop (HIL), permitting non-invasive tests. The real-time simulator is interfaced with Simulink, to which different power system configurations can be developed for testing.

Furthermore, a remote terminal unit (RTU) and IEDs are connected model a substation under EMS control, as shown in the right block of Fig. 1. The substation operates over its own LAN. Its setup is designed to be compliant with the IEC 61850 standard protocols and implemented on three levels: process, bay, and station. The process level is responsible for receiving time-critical messages from the bay level for the control of circuit breakers and transformers. Next, the bay level is composed of IEDs that control the components of the process level. Additionally, the bay level sends measurement data to the station level as well as controls to the process level. Finally, the station level provides an overview of the entire substation and connects to the EMS through the communication system [12].

Under the three-level structure, Manufacturing Messaging Specification (MMS) is commonly used at the station level, while Generic Object Oriented Substation Event (GOOSE) and Sampled Value (SV) are used at the process level. In particular, GOOSE messages are used by circuit breakers to communicate their status to the RTU in addition to subscribing to control commands from the EMS. SV is used by IEDs to send measurements values (current, power, voltage) to the RTU for transmission to the EMS [12].

C. Communications

The design of communications linking EMS and the physical power grid is illustrated in the middle block of Fig. 1. The communication are realized through a system of clients, servers, and the network simulator. First, the clients subscribe or connect to servers to send/receive data. Next, the servers are open to client connections for data transmission. Finally, the network simulator emulates of network traffic for the transmission of data between the LANs, over which EMS and substations are operated.

Data transmission in emulated network (*i.e.,* WAN) can be modeled with graph theories, in which each node represents a LAN corresponding to EMS or substations. For every data

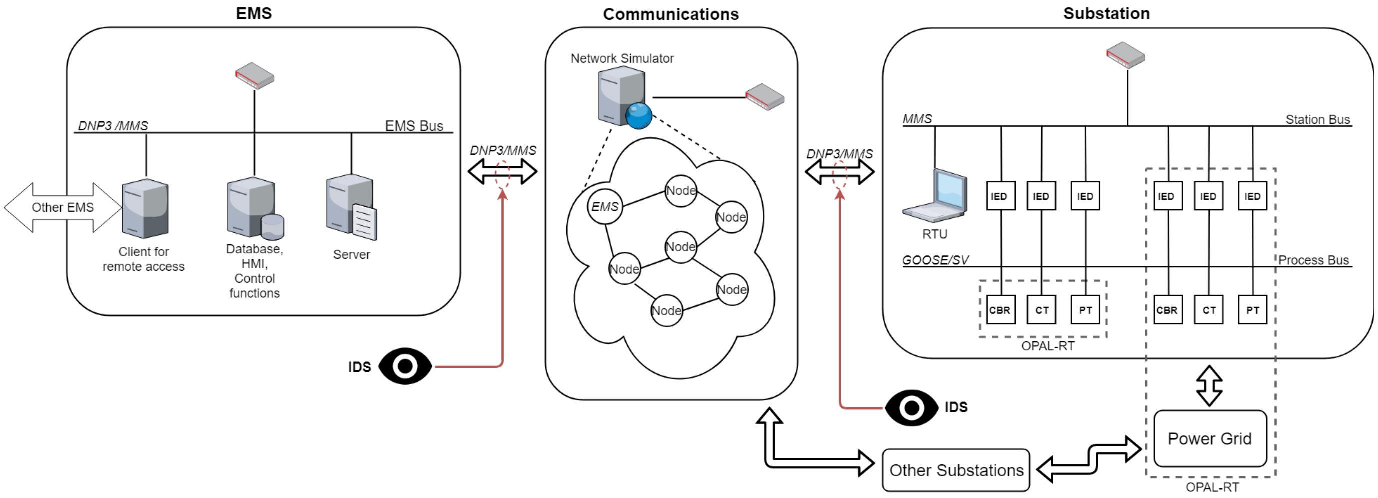

Fig. 1. Overall System Design.Each node in the network represents a LAN corresponding to where EMS and substations are operated.

transmission, the simulator routes the data packets according to predetermined algorithms, such as shortest path, to comply with different communication protocols. For example, a client-server communication system can transmit data over TCP/IP using IEC 61850 standard protocols or DNP3. To develop the IEC 61850 standard protocols, the libiec61850 API can be used [10]. Furthermore, DNP3 can be deployed using OpenDNP3 [11]. Each provides a programming toolkit for encoding the different protocols. In addition, each edge in the graph can be weighed differently, allowing for the manipulation of delays based on the desired design.

To allow development and test defense against cyber-attacks in an integrated manner, the design incorporates a network IDS. The prototype of the design places an open-source IDS, Bro, on the substation network and EMS network to monitor each system. It captures all of the traffic on the network and generates alerts based on rules created by the administrator.

Finally, this design supports wireless communication as well. By using high-speed Wi-Fi cards, strong and stable connections are made with the contemporary networking infrastructure. This alternative medium allows for two advantages: (1) the study and validation of implementing a new medium for the cyber-infrastructure, and (2) thorough testing of security before any sort of deployment.

III. Currently Implemented Systems

Based on the design, two prototype systems are realized to gather preliminary results.

A. Real-time Communication Network Analysis

In this system, data transmission is simulated between an EMS and a substation. The EMS acts as the client to the substation server. Measurements, such as load consumption of the buses, are sent from the server to the client. Then, the client sends the generation controls to the server. The implementation is illustrated in Fig. 2.

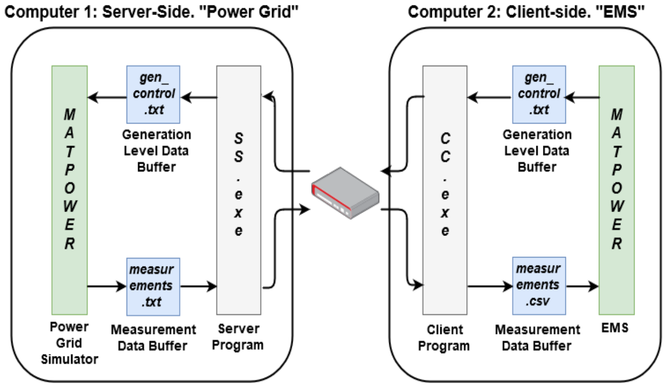

Fig. 2. Block diagram of the implemented system.

The server is composed of the server program, named *SS.exe*, and two data buffers. *SS.exe* is a custom program using libiec61850. The two data buffers hold the data used in the power grid simulation. In particular, one buffer holds the measurement values, *measurements.txt*, while the other holds the generation controls, *gen_control.txt*. Mirrored to the server, the client has a client program, *CC.exe*, and two data buffers.

The programs were built to fit into a SCADA system containing an EMS and power grid. They transmit data via the IEC 61850 standard protocol MMS which operates over TCP/IP. The purpose of this system was to create a communication network that can be built upon in the future. The programs provide real-time data transmission for the testbed design.

B. Steady State Analysis

Fig. 2 shows the architecture of the system, where the power grid simulator and the EMS are implemented by MATPOWER. On one hand, the EMS outputs the data for steady-state power system analysis. The tester, playing the role of system operator, can manipulate the generation levels. On the other hand, the power grid generates the load consumption

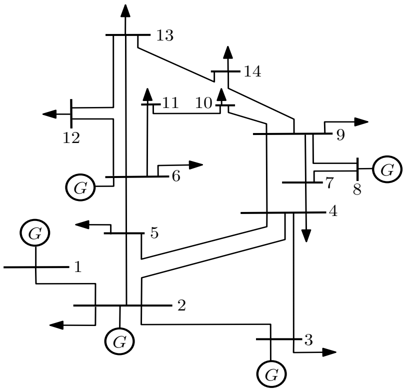

Fig. 3. Single-line diagram of the IEEE-14 Bus system. Five generators are connected.

data. In a normal system, the grid response converges with static demand and supply. In contrast, if the power grid parameters are manipulated through an attack, the grid response will change or fail to converge, indicating instability. Thus, the purpose of this system is to understand the effects of data manipulation.

IV. Testing

In this section we demonstrate the performance of two prototype systems on the IEEE-14 Bus system, as shown in Fig. 3.

A. Denial-of-Service Attack

The Denial-of-service (DoS) attack is an attack in which the attacker attempts to starve or deplete vital resources of a victim. This can be achieved in a multitude of ways. The attack mechanism used in the following experiment involves flooding the victim with SYN packets. This is performed on the client-server network from Section III.A. The goal is to understand the effect the DoS has on the throughput of MMS packets in the communication system.

To execute the attack, the attacker targets the server, *i.e.,* substation RTU. Then, the attacker sends SYN (synchronize) packets to the RTU, where every SYN packet opens a connection request. The victim responds to each SYN packet with an SYN-ACK (Synchronize-Acknowledge) packet, creating a half-open connection to which the attacker never responds to establish a full connection. The accumulation of these half-open connections depletes the victim of its resources and decreases the throughput of MMS packets.

In the test, a 60-second interval was used. Packet I/O was captured for the server under normal operation and under DoS attack. Fig. 4 shows the packet I/O for each operation.

The data was captured using Wireshark on the server. The graph shows the average number of packets sent or received over the 60 second time interval. The system under DoS attack experienced a substantial increase in packet transmission. This resulted in a significant increase of the response time of the server. This was measured by pinging the server with another computer. A ping is a small amount of arbitrary data sent from one system to another, through which the connection speed, i.e. response time of the system, can be measured. So, the response time was captured before and after the attack initiation. The response time of the server was measured with the attack initiation and is shown in Fig. 5.

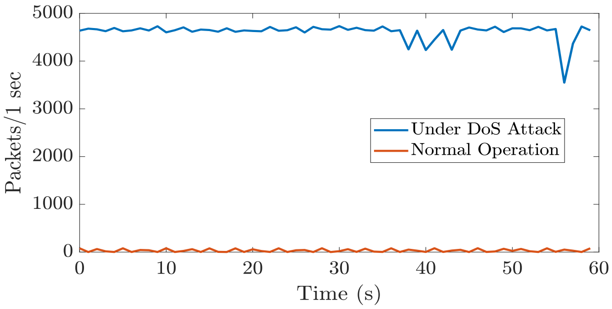

Fig. 4. Packet input and output for normal operation and under DoS attack.

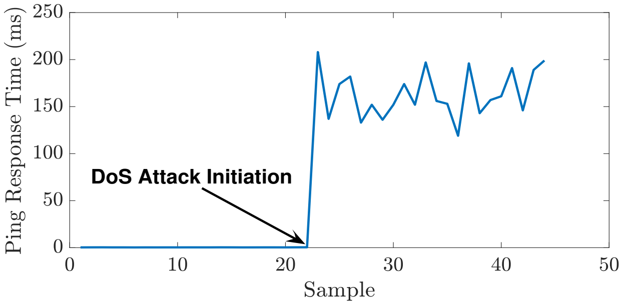

Fig. 5. Response time of the server.

Before the DoS attack, the system operated with an average response time of <1 ms. However, after the attack was initiated, the average response time increased to approximately 164 ms. Due to the delay, the RTU could no longer uphold the required performance specifications set by IEC 61850 [15]. In addition, the EMS no longer received the data in real-time, delaying control signals. For a real SCADA power system, this would result in the EMS losing observability and ultimately control. If the EMS does not have the correct real-time data from the power grid, then the automated controls are invalid.

B. False Data Injection Attack

The false data injection (FDI) attack is defined as adversarial attempts to modify data, such as measurements and control command. In particular, manipulation of measurements cannot be directly spotted at HMI. It could mislead EMS dispatch incorrect amount of generation, undermining the power grid reliability.

We simulate the case that an attack has successfully penetrated through the cyber-layer, meaning that s/he (1) obtains access to the station RTU, (2) manipulates out-going measurement values, and (3) bypasses the security system. Ultimately, this attack could represent an attacker gaining elevated privileges internally in the network or substation by obtaining a password or installing a beachhead on the system.

The FDI attack was implemented using MATPOWER in an offline scenario running optimal power flow (OPF). Both the attacked scenario and normal operation started with equal parameters for the generation levels, bus demand, generator cost, and branch data. To implement the FDI attack, the bus demands were increased by 27.6 percent relative to their initial levels. Table I shows the generators' real power generation response to the increased demands under the FDI attack.

TABLE I
GENERATOR DATA

Generator	**Real Power Generation (MW)**		
on Bus	***Initial***	***Normal Op.***	***FDI Attack***
1	232.4	194.3	199.4
2	40.0	36.7	37.8
3	0.0	28.7	55.4
6	0.0	0.0	13.3
8	0.0	8.5	34.7

The increase in generation levels is a result of the EMS recalculating the generation levels based on the injected data. From the table, the generators under the attack scenario produce higher real power levels, sometimes significantly. This increased generation produces a higher power flow on the system. Table II shows the real power flow of the system. Note, only lines close to the generators were included.

TABLE II
REAL POWER FLOW DATA

Bus	***Normal Op.***	***FDI Attack***
1→2	129.7	133.9
1→5	64.7	65.5
2→3	55.6	55.2
2→4	48.9	48.7
2→5	37.3	37.0
3→4	11.2	11.0
6→11	6.1	7.5
6→12	7.7	9.8
6→13	17.1	21.8
7→8	8.5	34.7

Overall, the power flow of the system increased. The average percent increase was approximately 25 percent, and the average power flow increase was about 2.3 MW. Notably, the power flow from bus 7 to 8 resulted in a large increase.

If the bus demands are increased to a high enough level, MATPOWER fails to converge. This indicates that the system load has exceeded the maximum loading capacity for steady-state analysis, resulting in an unstable system. Therefore, FDI attacks that increase the generation levels can result in wasted resources, higher costs, or instability.

Furthermore, FDI attacks can occur in the reverse direction, *i.e.,* false data can be injected into the control signals from the EMS to the power grid. This can result in a variety of different adverse effects such as repeatedly tripping breakers to cause a blackout [3].

V. CONCLUSION

In this paper, a testbed design has been proposed for cyber-security testing. The three-level design utilized OPAL-RT for real-time power grid simulation, an energy management system, and a real-time communication network. Additionally, the design encompassed an IDS for security testing, remote connection for scalability, network simulator and wireless communication support. As evidenced by the testing, an attack can manipulate or gain control of a system. Using DoS, the attacker was able to deny the power grid of time-critical control commands. The EMS also lost observability of the power grid. Furthermore, the FDI attack resulted in an attacker gaining control over the system by changing measurement data. This type of attack can be devastating due to its invisibility and loss of control.

REFERENCES

[1] M. Aiello, G. A. Pagani, "The Smart Grids Data Generating Potentials", http://www.cs.rug.nl/∼aiellom/publications/fedcsisKeynote.pdf

[2] K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, Mar. 2016.

[3] C. Vellaithurai, S. Biswas, and A. Srivastava, "Development and application of a real-time test bed for cyber-physical system," IEEE Syst. J., vol. PP, no. 99, pp. 112.

[4] P.P. Parikh, M. G. Kanabar, T.S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in Proc. IEEE Power and Energy Society General Meeting, Minneapolis, MN, Jul. 25-29, 2010, pp.1-7.

[5] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," IEEE Trans. Smart Grid, vol. 4, no. 2, pp. 847855, Jun. 2013.

[6] H. G. Aghamolki, Z. Miao, and L. Fan, "A hardware-in-the-loop SCADA testbed," in Proc. North Amer. Power Symp. (NAPS), Charlotte, NC, USA, 2015, pp. 16.

[7] R. Reddi and A. Srivastava, "Real time test bed development for power system operation, control and cyber security," North American Power Symposium 2010, Arlington, TX, 2010, pp. 1-6.

[8] D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman and Y. Wu, "Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid performance," 2015 IEEE Power & Energy Society General Meeting, Denver, CO, 2015, pp. 1-5.

[9] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in RTDS and OPNET," in Proc. North Amer. Power Symp. (NAPS), Pullman, WA, USA, 2014, pp. 16

[10] Michael Zillgith. libIEC61850 — open source library for IEC 61850. [Online]. Available: http://www.libiec61850.com/libiec61850/ (2016)

[11] Automatak. Opendnp3 — de facto reference implementation of IEEE-1815 (DNP3). [Online]. Available: https://www.automatak.com/opendnp3/ (2013)

[12] Mark Adamiak, Drew Baigent, and Ralph Mackiewicz, '"IEC 61850 Communication Networks and Systems In Substations," pp. 61-68, 2010.

[13] C. -C. Sun, J. Hong, and C. -C. Liu, "A coordinated cyber attack detection system (CCADS) for multiple substations," 2016 Power Systems Computation Conference (PSCC), Genoa, Italy, 2016, pp. 1-5.

[14] M. Cintuglu, O. Mohammed, K. Akkaya, and A. Uluagac, "A survey on smart grid cyber-physical system testbeds," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 446464, 2017

[15] S. A. Obaidli, V. Subramaniam, H. Alhuseini, R, Gupta, IEC 61850 Beyond Compliance: A Case Study of Modernizing Automation Systems in Transmission Power Substations in Emirate of Dubai Towards Smart Grid in 2017 Saudi Arabia Smart Grid, Dec. 2017.