An Integrated Testbed for Power System Cyber-Physical Operations Training

Manohar Chamana , Rabindra Bhatta * , Konrad Schmitt , Rajendra Shrestha , And Stephen Bayne

Posted Date: 18 July 2023

doi: 10.20944/preprints202307.1243.v1

Keywords: Cyber-Security; Cyber-Physical Systems; Education; Power Systems; Real-Time testbed Smart Grids

Article

An Integrated Testbed for Power System Cyber-Physical Operations Training

Manohar Chamana, Rabindra Bhatta *, Konrad Schmitt, Rajendra Shrestha and Stephen Bayne

[1] National Wind Institute, Texas Tech University, USA; m.chamana@ttu.edu
[2] Electrical and Computer Engineering Department, Texas Tech University, USA; rabindra.bhatta@ttu.edu, konradkorkschmitt@ieee.org, rajendra.shrestha@ttu.edu, stephen.bayne@ttu.edu.
* Correspondence: Rabindra Bhatta, rabindra.bhatta@ttu.edu

Abstract: The increased adoption of information and communication technology for smart grid applications will require innovative cyber-physical system (CPS) testbeds to support research and education in the field. The groundbreaking CPS testbeds with realistic and scalable platforms have progressively gained interest in recent years, with electric power flowing in the physical layer and information flowing in the network layer. However, CPSs are critical infrastructures and not designed for testing or direct training, as any misbehaving in an actual system operation could cause a catastrophic impact on its operation. Based on that, it is not easy to efficiently train professionals in CPSs. Aiming to support the advancement and encourage the training of industry professionals, this paper proposes and develops a complete testbed with commercial tools. The testbed can reliably replicate the performance of smart grid systems and the main potential cyber threats that electric grids may face. The complex interdependencies between the cyber and physical domains are discussed in detail, and different case scenarios are presented, providing insightful guidelines for key features and design decisions for future smart grid testbeds.

Keywords: cyber-security; cyber-physical systems; education; power systems; real-time testbed smart grids

1. Introduction

The smart grid is evolving to create a highly flexible and resilient cyber-physical system (CPS) based on the bidirectional flow of power and information. The smart grid concept is expected to embrace intelligent features such as distributed energy resources (DERs), adaptive protection and control, enhanced monitoring, and foundational support systems [1]. The smart grid consists of a group of intelligent loads, converters, and distributed energy resources with clearly defined boundaries that can operate synchronously with the grid [2]. With this advancement, the modern smart grid is expected to be coupled with better situational awareness, decision support, flexibility and highly scalable, and control of the physical system at different stages of the power grid. At the transmission level, the adoption of wide-area monitoring, control, and supervision improves the power systems' visibility and control for stable operation [3]. At the distribution level, optimization, automation, and power flow control are anticipated to be based on a smart grid integrated with advanced CPS sensors and devices [4]. Integrating information technology systems and networks has enabled all these promising prospects in power systems. However, the downward concern is that it will expose the grid to a wide range of security threats. Moreover, it introduces heterogeneity, diversity, complexity, and new vulnerabilities to the grid [5]. The increasing deployment of DERs, smart inverters, and advanced control in cyber-physical systems has driven power system operators to adopt novel technologies [6] and develop plans to mitigate the associated risks [7]. This calls for a strong need for a dynamic and flexible testbed to test the resilience of power systems to cyber-attacks and improve their cyber defenses, thereby ensuring the cybersecurity, reliability, and efficiency of such systems. Due to the interlaced characteristics of the physical and cyber components, the testing of emerging applications needs to be performed by aiming to characterize both the physical systems

 doi:10.20944/preprints202307.1243.v1

and the cyber networks [8]. Thus, testbeds are critical for understanding cyber-physical interactions and provide the environments for prototyping novel applications.

Previously published literature in this area has investigated the development of testbeds with physical systems built on a real-time simulator or offline power systems software. In [9], the impact of cyber-attacks on power systems has been analyzed. By using a comprehensive and reconfigurable testbed that integrates a simulated power grid with an emulated communication network, real-world cyber events, such as communication line outage, denial-of-service (DoS), man-in-the-middle, and delay, were simulated for security and performance validation. In [10], a cyber-physical testbed, which integrates industrial-grade supervisory control and data acquisition (SCADA) software with a Real-Time Digital Simulator (RTDS), and a non-real-time analysis was performed using the DigSILENT PowerFactory software. Different scenarios of attacks were created involving malicious breaker trip attacks, SCADA observability DoS and remedial action scheme DOS attacks, and the impact of an attack on system voltages and generation and line flow was effectively evaluated. In [11], a CPS testbed is built on top of an earlier version of the large-scale testbed (LTB), where the physical layer simulates power system dynamics, the network's physical layer is equipped with measurement devices and actuators, the communication emulation layer creates the software-defined networks (SDN) for data transmission, and the application layer consists of both power system applications and cyber-network applications including traffic monitoring and cyber-attack defense. The wide-area sophisticated replay attack using PMUs is simulated to provide a comprehensive demonstration of the cyber-physical simulation capability of the testbed for wide-area monitoring and control verification. In [12], a multi-objective comprehensive testbed is presented. This system uses real-time power system simulators with fiber and ethernet networks to test smart and distributed management control. The various challenges and future research for CPS testing have been analyzed, including big data analysis methods for in-depth testing, a combined schema for non-functional testing, a new test execution mechanism for hybrid CPS, and so on. A flexible hardware-in-the-loop (HIL) testbed was presented in [13]. This study aimed to demonstrate the performance of stability control equipment to analyze cyber events' effect on the power system by considering the impact of communication bit errors on the stability control system. A false data injection attack (FDIA) on voltage control and a man-in-the-middle (MITM) attack on the data link were simulated to demonstrate the impact of a cyber-attack on the stability control system. In [14], a comprehensive survey on cyber-physical smart grid testbeds is presented to provide a taxonomy and insightful guidelines for the development and identify the key features and design decisions while developing future smart grid testbeds. The MITM attack aimed to intercept messages between the control center and field devices to accomplish falsified messages over the network, while the DoS attack intended to overload and flood the network. The replay attack, which intends to modify the captured data to replicate activity, was also studied in the paper. The paper presented the research issues for the vision of actual smart grid realization, mainly focusing on communication infrastructure, the accurate selection of test platforms, distributed and decentralized control, and the interoperability of the testbeds. The cybersecurity landscape in the industrial control system (ICS) and the concepts and principles for deploying cybersecurity methods have been studied using different attack scenarios to emphasize the optimal distribution of security protection in large legacy ICSs [15]. In [16], a cyber-power system testbed to develop new educational modules on distribution systems was presented to analyze the impact of cyber events on the power grid dynamics and performances. In a smart grid environment, compromising a cyber-asset such as a control, protection, and monitoring device by an attacker can cause damage to the physical power system components such as loads, breakers, generators, and transformers. The severity of the attack determines the time required to take back the system into control [17]. In general, cyber-physical security requirement for a critical infrastructure includes three distinct properties, namely confidentiality, integrity, and availability [18]. For example, the confidentiality of the meter data is vital as power demand data provides important information about the usage pattern. The price of energy is also critical information, as an attacker may cause random electricity utilization spikes. The integrity of data, commands, and software is critical since the system can be compromised by any of its devices and

 doi:10.20944/preprints202307.1243.v1

components. The availability of the system against DoS attacks and distributed DoS attacks is a key aspect of the cyber-physical system, as those attacks are resource consumption attacks with fake requests to compromise smart meters and appliances. The rise from the fixed balance power grid to a dynamic balanced smart grid involves extending the control functionalities for targeting new balancing scenarios [19].

This study develops a complete cyber-physical testbed for training industry professionals on different CPS scenarios and cases. The main novelty presented in this paper is the design and implementation of a CPS testbed focused on training industry professionals about the interaction between physical and cyber layers and their performance under cyber-attacks. With the intention to develop a reliable and realistic test environment, the testbed topology is based on Hardware-In-the-Loop (HIL) concept, where IEDs from the Schweitzer Engineering Laboratories (SEL) and the Survalent SCADA software are integrated into OPAL-RT simulator. Besides that, the cutting-edge EXata CPS software is used for communication network modeling and cyber-attack simulation. Different scenarios are developed and tested under different types of cyber-attacks to analyze the response and performance of the system under critical periods. The rest of this paper is divided into Chapter 2 presents and discusses the concept of CPS in depth. Chapter 3 describes the proposed testbed setup and architecture, while Chapter 4 presents the different attack scenarios and the system response to each of them. Chapter 5 provides a discussion on CPSs and their future perspectives, and Chapter 6 concludes the present study.

2. Cyber-Physical Systems

The power system is a complex CPS consisting of power plants, substations, and transmission and distribution systems. The physical parcel of the power grid relies on the cyber system for monitoring, control, and operation. The cyber system comprises smart information and communication technology at the substations and the SCADA system at the control center [20]. Several power systems applications are supported by the SCADA system, and the measurements at the substations are delivered to the control center through the ICT network. The control commands, such as the opening and closing of a switch, can be sent from the control system to the remote terminal units or gateways in the power stations. The high penetration of the ICT system on the modern SCADA system makes it more vulnerable than before to cyber intrusions. Substations are also critical as they have power system components such as intelligent electronic devices, transformers, breakers, and switches. Usually, the information from the substation is analyzed for energy management systems in the smart power grid. Thus, it is crucial to enhance the cyber security of substations and analyze security as an integrated model to enhance the cyber-physical aspects of smart grids. Table 1. Summarizes the most recent research on cyber-physical aspects of power systems based on the simulation environment. These simulation environments provide an ideal platform to perform system evaluation, considering the cyber layer and physical layer together, under abnormal operational scenarios without disrupting the operation of the actual system. The study incorporating cyber and physical layers helps to investigate cyber threat models [21] and power grid dynamics by integrating real-world physical components commonly found in practical settings. They enable decision-making based not only on theoretical analyses but also on practical studies. Also, the use of these CPS testbeds can be expanded to facilitate the proactive assessment of cyber-attack or fault mitigation and control strategies before deploying the corresponding hardware in the field, thus reducing the risks associated with the costly and unpredictable deployment process. Thus, rather than focusing on the technical aspects, our research must be more inclined towards practical implementation within the real-time environment using real-time co-simulation testbeds.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

Table 1. Most recent studies on CPS testbeds for power systems applications.

Literature	Year	Research Topic	Novelty	Co-simulation	Real-time	IDS
[38]	2015	The impact of cyber-attacks on power grids was studied in a simulated power network and emulated communication network.	Reconfigurable testbed	No	No	No
[39]	2015	Development and application of real-time testbed for CPS	Real-time simulation	No	Yes	No
[40]	2016	ICS for the deployment of cybersecurity methods has been studied using different attack scenarios	Emphasize the optimal distribution of security protection in large legacy ICSs	No	No	No
[41]	2018	Detection of stealthy cyber-attacks in smart grid	Study of hybrid and stealthy attacks in power system	No	Yes	Yes
[42]	2020	CPS testbed for wind energy systems	HIL simulation	Yes	Yes	No
[43]	2021	CPS testbed studying MITM attacks detection and defense	FDIA and MITM attacks simulated in the data link layer	No	No	Yes
[44]	2021	Real-time co-simulation testbed for inverter-based microgrids	Use of SEL-3530 with OPAL-RT	Yes	Yes	No
[45]	2021	A real-time CPS testbed to study cyber threats and risk assessments	Use of EXata CPS for attack simulation in real-time	Yes	Yes	No

3. CPS Testbed Architecture

The proposed CPS testbed is designed to be flexible enough to provide interactive training to industry professionals and be as reliable as possible when compared to real-world applications. Figure 1 presents the testbed structure, which is divided into four different layers: The power layer, the Hardware layer, the Communication layer, and the Application layer.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

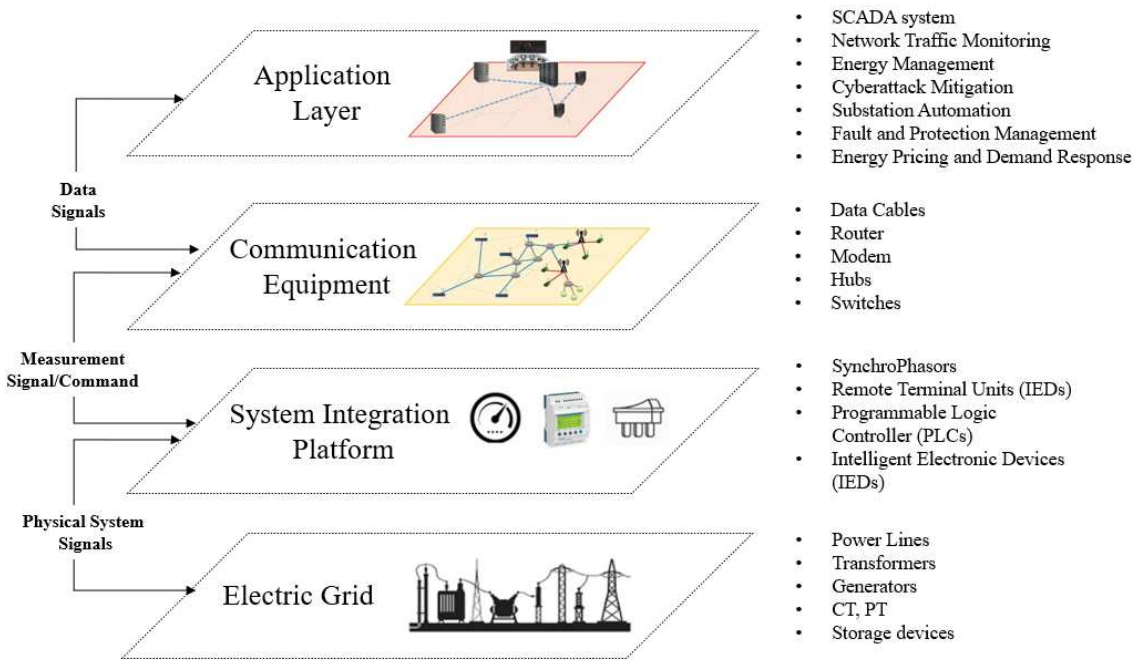


Figure 1. Cyber-physical testbed topology.

Within the OPAL-RT Real-Time Digital Simulator, both the network and physical layers are modeled. At the bottom level, the power network is modeled through lines, loads, generators, switches, and transformers. Above it, there are virtual IED models responsible for measuring the point of connection. In equipment such as switches, the IED is also responsible for controlling the opening and closing of that device according to its internal logic or external commands. On a third level, the communication for each of these IEDs is defined by MODBUS and DNP3 protocols. Even though still inside the OPAL-RT, the simulator has the capabilities to model IP addresses and communication protocols and use simulated values as data points. Besides virtual modeling, the OPAL-RT is also integrated into real IEDs. The hardware layer is based on the connection between the simulator and IEDs, which is achieved by analog and digital wires, which provide voltage and current measurements to the IED inputs. From a real IED point of view, its measurements are coming from an actual real system, as they would be installed in the field. It is worth highlighting that the IEDs are protective relays and automation controllers from the Schweitzer Engineering Laboratories (SEL) manufacturer, which are widely used worldwide for power systems monitoring, protection, and control. The application layer is primarily compounded by the SCADA software, along with physical and cyber models of the system. USA power utilities commonly use the Survalent system to provide visibility and control power systems networks and substations. The platform works as a server, obtaining information from the system, displaying it through a graphical user interface (GUI), and dispatching back commands from the operators to the IEDs. The communication layer is compounded by all communication links between the OPAL-RT and SEL and SCADA. The connections are also mapped into EXata CPS software, which runs within OPAL-RT and is able to model the network points to create cyber-attacks between them.

3.1. Power System Layer

The power system models, monitoring, and control devices are modeled on the power system analysis platform HYPERSIM from OPAL-RT Technologies. It offers a cost-efficient, scalable, and flexible real-time platform with a highly incorporated Linux-based real-time operating system for extreme performance [22]. The advantage of using the real-time simulator is that it guarantees hard real-time constraints, synchronization accuracy, minimal overhead, and maximal data throughout [23]. It can run test scenarios that are simply impossible to perform with physical test benches. With

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

this tool, the modeled system can interact with external devices through the simulator's I/O and communication protocols. Different electrical system topologies were developed based on different use cases. The tested networks are modeled with passive and active power systems elements, and different points are mounted with current transformers (CTs) and potential transformers (PTs) to measure electrical quantities that are sent to external hardware through DNP3 and MODBUS communication protocols as well as hardwire connections.

3.2. Hardware Layer

The HIL concept uses the real-time capability of the OPAL-RT simulator to both send the model's measurements and receive signals from external monitoring, control, and protection devices [24]. In an electrical power systems environment, this information exchange can emulate the performance of a power substation, where RTUs are responsible for aggregating analog signals measured by CTs and PTs, sending them to the SCADA system through a communication protocol. In parallel, protective relays also receive analog signals from CT and PT measurements to identify fault situations and control the simulated switch models. The simulator can create virtual IP addresses for each RTUs, using the information from the simulation model. These virtual IEDs can exchange data through the most common communication protocols, such as DNP3, Modbus, C37.118, IEC 61850, etc. At the hardware layer, the present testbed has two protection relays (SEL-351S) and one Real-Time Automation Controller (RTAC/SEL-3530) as controller and data concentrator. The two SEL-351S are connected to OPAL-RT through analog (voltage and current measurements) and digital (breaker status and open/close commands) wires. The relays are configured based on a protection study for the power network under test and may act under fault conditions. Besides, the relays are configured to send measurements to RTAC and receive open/close commands from RTAC through DNP3.

3.3. Communication Layer

The EXata CPS software from Scalable Technology provides a communication network emulation platform to simulate and predict the behavior of networked environments based on various operational scenarios, including different cyber-attacks. The emulation runs in real-time and models connections, computers, protocols, firewalls, and other network nodes [25]. The software runs within OPAL-RT and is integrated with HYPERSIM software to offer a complete real-time cyber-physical situation for developing, testing, and assessing electrical grids with communication networks [26]. This solution offers low-latency communications to analyze cyber threats that can be injected into the network layer. Besides that, as soon as all communication nodes and connections are mapped, it allows users to create controlled cyber-attacks on the network.

3.4. Application Layer

Several power engineering applications have been integrated with the developed cyber-physical testbed. One of these applications includes real-time-voltage stability monitoring and control using an industry-standard Survalent SCADA system. Survalent is a Windows-based platform that allows systems monitoring, awareness, control, and alarm processing through its GUI [27]. The database stores system status and measurements using industry-standard communication protocols besides enabling pre-defined computations [28]. The main visualization of the data and system is through the Survalent SMART VU, which allows one-line diagrams modeling and data displaying [29]. SMART VU also provides integrated features and functionality to interface industry-standard modules, components, and devices and supports different communication protocols [30] to easily integrate different modules, components, and devices for better visualization.

4. CPS Testbed Applications

Testbed development requires the integration of different types of system components, which is a key challenge for many CPS projects. The TTU CPS testbed has been designed and periodically

 doi:10.20944/preprints202307.1243.v1

upgraded to perform co-simulation and reconfiguration studies. Figure 2 shows the CPS testbed at TTU with hardware components (right) and the corresponding network architecture (left). The testbed has hybrid architecture and can include physical hardware components and emulated power systems following the Power Hardware-in-loop approach. In addition, it utilizes industry-standard equipment and communication protocols. The laboratory setup is completely reconfigurable and primarily employs hardware components from the leading industry supplier power systems. However, its interoperability is second to none as it supports multiple other vendor components. It can perform real-time and end-to-end system simulations with the HIL capability to evaluate the existing prospects of the cyber-physical system alongside advanced management systems and SCADA applications via OPAL-RT. OPAL-RT real-time simulator (OP5700) is a potent target computer with a high-end reconfigurable FPGA, signal conditioning for up to 256 I/O lines, and 16 high-speed fiber-optic SFP ports.

The SEL-351S, SEL-421, SEL-751, and SEL-651R are advanced protection, automation, and control system devices. The protective relays utilize analog I/O and digital I/O cards to reflect the values of the physical modeling. They communicate with Survalent SCADA or RTAC to receive any control command and execute it. All of these devices are equipped with synchro phasor applications, allowing them to capture precise phasor measurements from different nodes in the power system. The synchrophasor measurements can be transmitted using protocols such as DNP3, IEEE-C37.118, and SEL fast message protocols. This enables the exchange of data with other devices and systems in a standardized and interoperable manner. Additionally, they can receive commands using the IEC-61850 protocol, which facilitates seamless integration with other intelligent electronic devices in the power grid.

The testbed as shown in Figure 2, consists of a regular switch, managed switch (SEL-2730M), and Software Defined Networking (SDN) switch (SEL-2742S) for communications. SEL-2730M offers advanced features and configuration options for networking applications in industrial environments. The managed switch (SEL 2730M) connects and provides the physical link to all the devices via ethernet cables. In contrast to the regular switch, the managed switch provides an additional security layer against cyberattacks with its functionality, such as Port Management, MAC address filtering, and VLAN creation. The RTAC (SEL-3530) is integrated into the testbed as the data concentrator. It can also perform any necessary control function depending upon the user's requirement. It combines the functionality of a protective relay with the capabilities of a programmable logic controller (PLC) and RTUs.

The controllers receive the control command from the Survalent SCADA, or RTAC, or a Python-based algorithm can be run on it to implement the advanced management function and generate its control command. The host computer is responsible for both performing the physical and communication layers modeling, as well as running Survalent SCADA.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

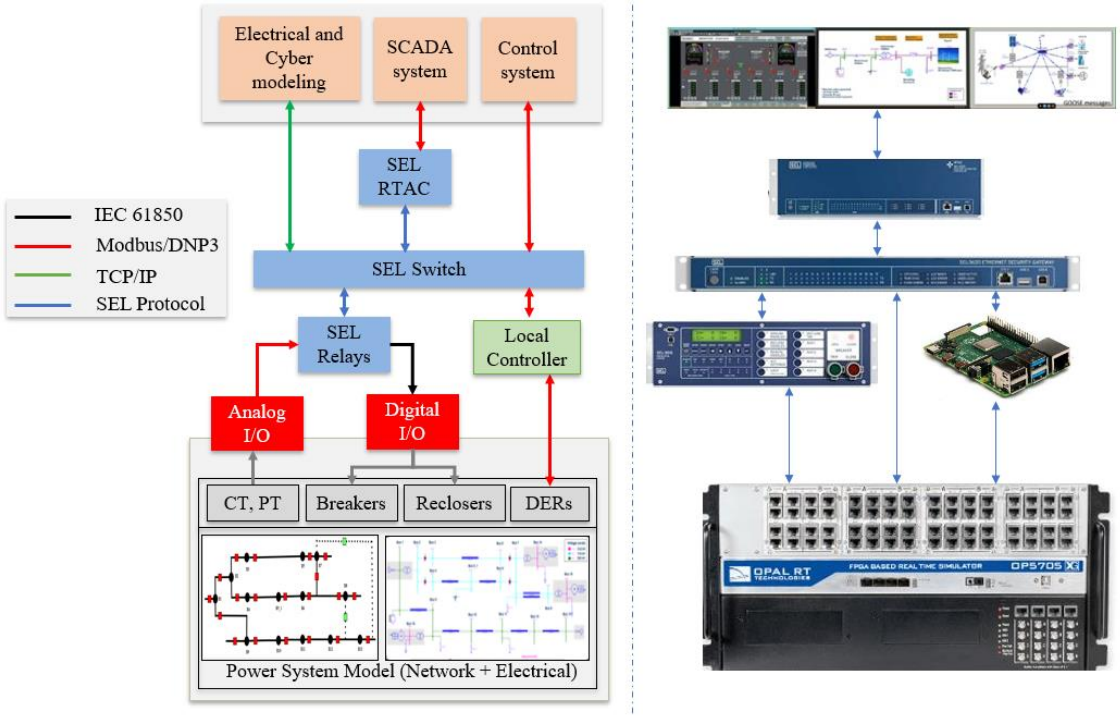


Figure 2. CPS testbed at TTU facility a) Communication Architecture b) Hardware Components.

The first module is based on an integrated sub-transmission and distribution systems model that is simulated along with SEL devices and Survalent SCADA to analyze protection performance. The second module develops a standalone cyber-attack analysis to clarify the impact of these actions on the data exchange. The third module is compounded by a wind turbine system connected to a distribution network. This simulation model is integrated with Survalent SCADA and EXata CPS to analyze the network performance under cyber-attacks in the wind turbine operation. The final module models a wide-area wind power plant with the underlying communication architecture to observe the influence and impact of cyber-attacks in these systems.

4.1. Module 1: Power Distribution Systems SCADA Operator Training

Power distribution systems are responsible for delivering power from transmission systems to end customers through high, medium, and low-voltage lines. A co-simulation between the Survalent SCADA and the power distribution system is performed in this module to primarily study the protection performance in HIL testbeds. The power network simulated in OPAL-RT is based on an integrated sub-transmission and distribution network from Lubbock, Texas, USA. It consists of 3 voltage levels, 345kV, 69kV, and 12.47kV, and has 24 substations and 41 lines. Figure 3 shows the CPS testbed and system models.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

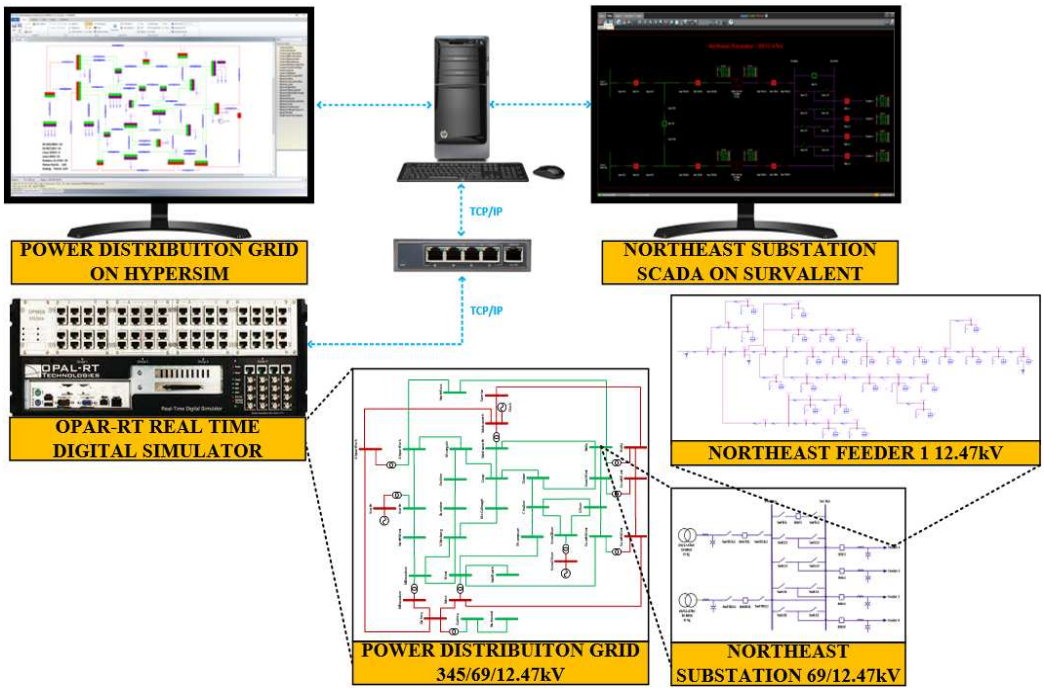
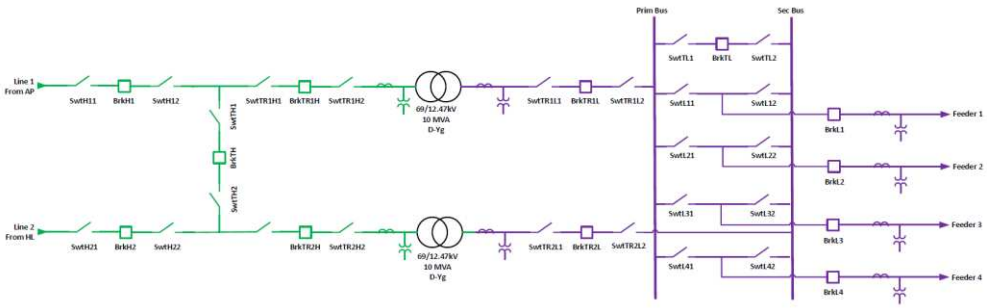


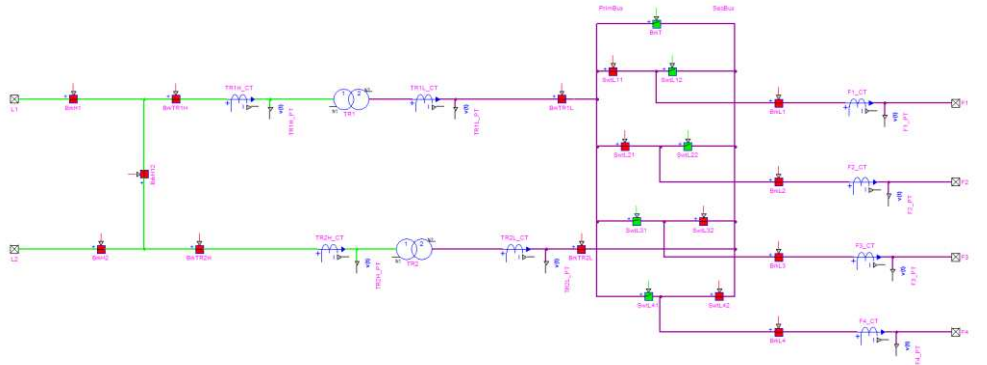
Figure 3. Distribution systems testbed topology.

For simulation efficiency, only four of the 24 substations were modeled in detail: Hurld Wood (HW), Wolfforth (WF), Vicksburg (VB), and Northeast (NE). These substations have a proper bus arrangement configuration, measurements, and controllable breakers and switches, while others only have bus connections. Figure 4 shows the NE substation modeling; similar modeling was made for HW, WF, and VB, but with different bus configurations. NE has a sectionalized bus on its HV side (69kV) and a double bus single breaker configuration on its MV side (12.47kV). This substation is responsible for 4 MVA feeders. There are measurements on both high and low-voltage sides of the transformers and each feeder output.

(a)



(b)



Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

(c)

Figure 4. Northeast Substation: (**a**) One-line Diagram; (**b**) Hypersim Modeling; (**c**) Survalent GUI.

For each of the detailed substations, virtual IEDs were created as DNP3 slaves. These IDEs are responsible for collecting and organizing all the analog and status points from the substation, such as breaker status, three-phase voltage, and current magnitude and angle. All the available points from the substations' IED are mapped and organized in Survalent SCADA. The SCADA GUI is responsible for providing an operator's interface with the electrical system. When the simulation and the SCADA are initialized and the communication is established, it is possible to visualize the real-time information for each bus, breaker, and switch on the four detailed substations. The green color indicates that the switch/breaker is open, and red indicates that it is closed. Also, red lines represent 345kV, green 69kV, and purple 12.47kV, while de-energized lines are shown in white. With this system setup, the module's test case is based on a short-circuit and protection analysis. A protection study was developed for the first feeder of the NE substation, where instantaneous (ANSI 50) and temporized (ANSI 51) overcurrent settings were computed along with reclosing (ANSI 79) shots and temporizations for two real SEL relays.

The protection study starts with the feeder's current levels, presented in Table 2. Where $I_{maxload}^{bus}$ is the maximum load current, $I_{3\phi SC}^{bus}$ is the three-phase short-circuit current, and $I_{1\phi SC}^{bus}$ is the single-phase short-circuit current for each relay's bus.

Table 2. Relays' Buses Current Levels.

Bus	$I_{maxload}^{bus}$ [A]	$I_{3\phi SC}^{bus}$ [kA]	$I_{1\phi SC}^{bus}$ [kA]
A	115	17.5	2.7
B	90	10.5	2.5
C	43	2.7	1.6

The CTs are dimensioned based on Eq. (1), considering a secondary level of 5A. The obtained value is rounded up to the closest commercial value.

$$CTR^{bus} = \frac{I_{3\phi SC}^{bus}}{20} \quad (1)$$

Equations (2) and (3) show the element 50 pickup, I_{pickup}^{50-bus}, calculation based on the bus current levels for buses A and B, respectively.

$$I_{pickup}^{50-A} > 1.25 \cdot \frac{I_{3\phi SC}^{B}}{CTR^{A}} \quad (2)$$

$$I_{pickup}^{50-B} > 1.25 \cdot \frac{I_{3\phi SC}^{C}}{CTR^{B}} \quad (3)$$

Equations (4) and (5) show the pickup current for element 51 of buses A and B, respectively.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

$$1.5 \cdot \frac{I^{A}_{maxload}}{CTR^{A}} < I^{51-A}_{pickup} < \frac{I^{B}_{1\phi SC}}{2 \cdot CTR^{A}} \quad (4)$$

$$1.5 \cdot \frac{I^{B}_{maxload}}{CTR^{B}} < I^{51-B}_{pickup} < \frac{I^{C}_{1\phi SC}}{2 \cdot CTR^{B}} \quad (5)$$

The coordination study is then developed based on the IEC 60255 standard. Equation (6) shows the temporized overcurrent formulation.

$$t(I) = TD \cdot \left[\frac{k}{\left(\frac{I}{I^{51-bus}_{pickup}} \right)^{\alpha} - 1} \right] \quad (6)$$

A Very Inverse curve is considered for this module, where k is 13.5 and α is 1. TD is the time-dial which is defined as 0.05 for relay on bus B and computed for relay on bus A by considering a 0.5-second delay between the curves on 80% of the line. Element 79 is responsible for automatically reclosing the recloser switch based on the number of shots and temporizations after a trip. Figure 5 presents the operational diagram of the 50, 51, and 79 operations.

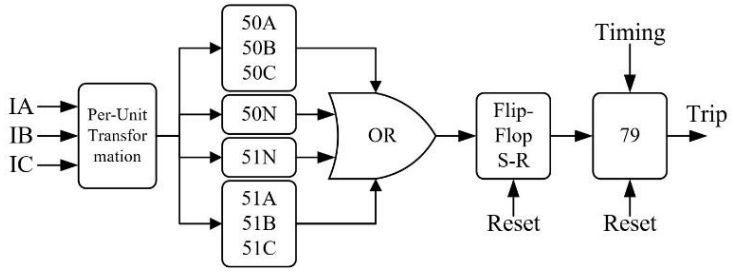


Figure 5. AC-Recloser generic operation.

Figure 6 shows the protection scheme for two reclosers (R) in a cascade over the feeder backbone, where bus A at the substation and B downstream A.

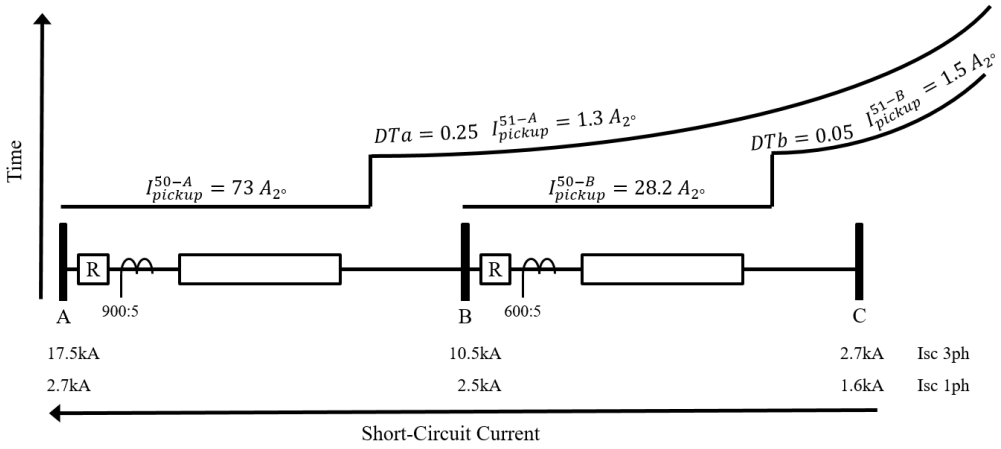


Figure 6. NE feeder's 50 and 51 protection coordination.

The reclosers are set with two reclosing attempts. For simulation proposes, recloser at bus A, R_A, has a dead time interval of 0.1 and 0.2 seconds, and recloser at bus B, R_B, has 0.3 and 0.5 seconds of dead time. Under a permanent fault, the recloser detects the short-circuit levels and cycles its reclosing attempts until lockout. On the other hand, for a temporary fault, the recloser should be able to cycle and successfully reclose when the fault is gone. Figure 7 shows the R_A operation under a permanent and temporary fault.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

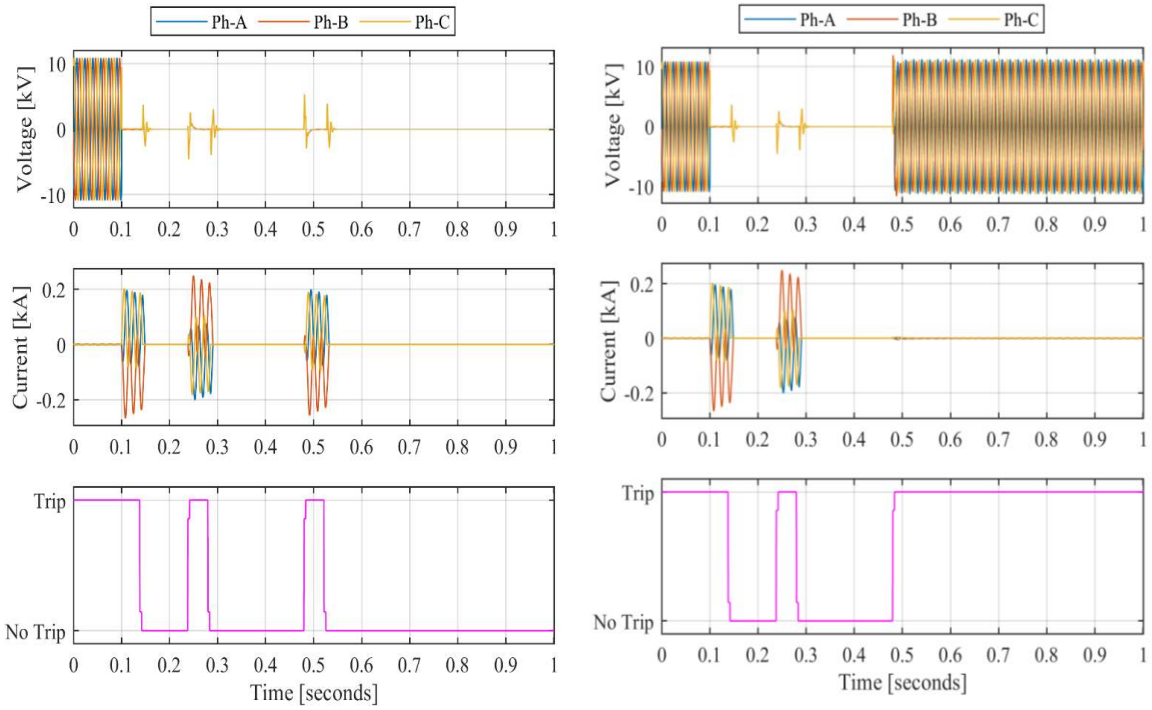


Figure 7. R_A operations under: (**a**) permanent fault; (**b**) temporary fault.

The SCADA systems are not designed to observe high-speed status, such as protection operations. However, every event on the power systems creates an alarm for the operator. If the recloser operates on a permanent fault, the operator receives an alarm informing which breaker is opened, as well as graphical visualization. Figure 8 shows the Survalent SCADA GUI before and after a fault event.

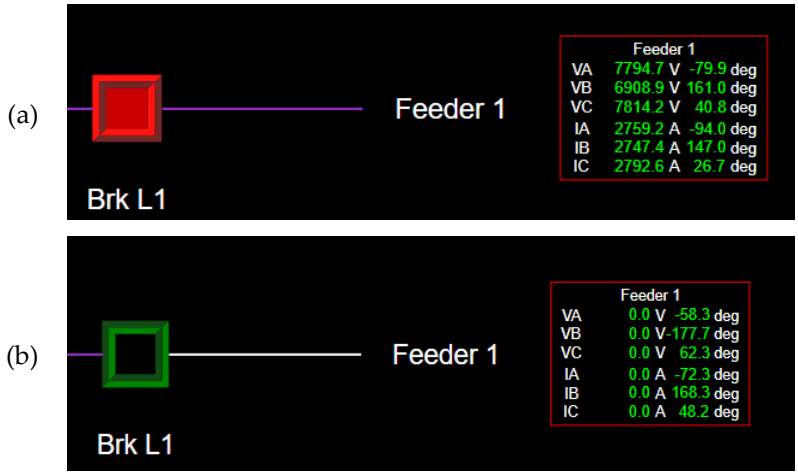


Figure 8. R_A status: (**a**) before fault; (**b**) after the lockout.

Nevertheless, under a temporary fault, the recloser may be able to successfully reclose, without the operator even observing it. For these events, there are alarms to notify and ensure that the operator knows everything that happened on the grid.

4.2. Module 2: General Power Systems CPS Operator Training

The second module is based on studying common cyber-attack scenarios and observing the impact of cyber intrusion on data flow and control aspects. Different use cases are developed to

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

perform standalone simulations on EXata CPS. The mathematical representation of the physical layer and cyber layer for each of these use cases follows the relation presented by Eqs. (7)-(9).

$$x(t+1) = G * x(t) + B * u(t) \quad (7)$$

$$y(t) = C * x(t+1) + e \quad (8)$$

$$u(t+1) = H * y(t) \quad (9)$$

Where $x(t)$ represents the state variables, $u(t)$ represents the control variables, $y(t)$ represents the system measurements at time t and e is the measurement error. G, B, C, and H are namely system matrix, input matrix, output matrix, and control matrix, respectively. Figure 9 shows the diagrammatic representation of the above-stated variables of the system. The presence of the cyber intruder will modify the control variables and system measurements. Besides modifications, the control signals can also be delayed or fabricated with dummy variables.

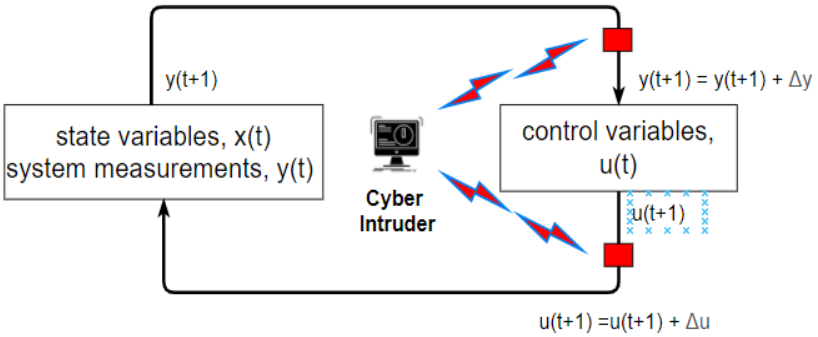


Figure 9. Diagrammatic representation system variables under attack.

4.2.1. Denial-of-Service Attack

The first use case was to observe the DoS attack on the SCADA server, which is communicating with several wind farm substations. The attack attempts to minimize the service offered by the node by reducing the access or completely failing the resource of the node [31]. The attack is implemented by dividing the network nodes into two sections: attack nodes and target nodes. The attack nodes are further categorized into susceptible, N_s, and infectious nodes, N_I, and the changing rate of attacks is denoted by the Eqs. (10) and (11).

$$\frac{\partial N_s}{\partial t} = \alpha - \beta N_s N_I - \alpha N_s + \gamma N_I \quad (10)$$

$$\frac{\partial N_I}{\partial t} = \beta N_s N_I - (\alpha + \gamma) N_I \quad (11)$$

Where α is the device failure rate, β is the packet ramp-up rate, and γ is the rate of the target node being susceptible to failure. The rate of failure of the susceptible nodes ϑ, with modification parameter δ, is defined by Eq. (12).

$$\vartheta = \beta(N_I + \delta * N_I) \quad (12)$$

A cyber-attack scenario is created according to the parameters presented in Table 3. The server node is the victim of a denial of service, and the attacker node is the wind farm substation.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

Table 3. General configuration for Standalone attacks.

Property	Value	Property	Value
Attack Type	DOS	Attack Type	Jammer
Victim Node	Node 2	Jammer Node	Node 15
Victim IP	10.10.1.33	Start Time	1
DOS Attack Type	Basic Attack	End Time	25
Victim Port	7200	Scanner Index	0
Configure	Interval	Jamming Power	Power (dBm)
Interval, β	0.1 sec	Power	100 dBm
Duration	30 sec	Silent Jammer	Yes
Ramp-Up Time	0 sec	Ramp Up Time	0 sec
		Data Rate	1 Mbps

The DoS works in conjunction with the OS resource model. Thus, the OS resource for each node must be enabled before starting the cyber-attack. The nodes are flooded by the excess data packets every 0.1 seconds, eventually forcing the node with a greater number of packets than it can handle. The node will fail and will ignore all other incoming packets. The results can be seen in Figure 10, where the packets received by the server are less than the ones sent by wind farm IEDs.

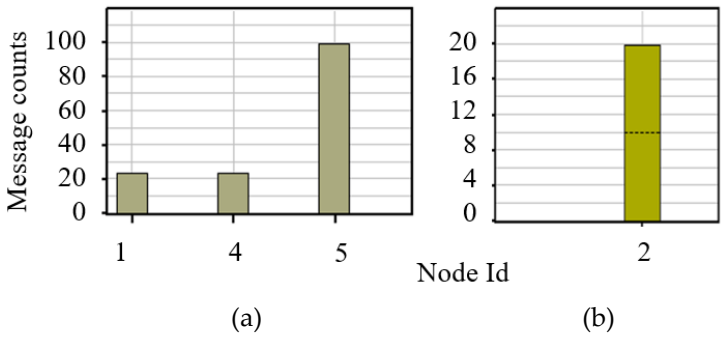


Figure 10. Quantity of messages: (a) sent; (b) received with DoS attack.

4.2.2. Jammer Attack

For the distribution system using wireless sensor networks, protection schemes must be employed against the aggressive nature of the jamming of the transmitted signal [32]. The jammer acts as high-power random Gaussian noise [33]. For a given n channel with energy $H_N(t)$ and N number of samples, the average jamming pulse observed is given by Eq. (13).

$$J(t) = \frac{\sum_{j=t-N+1}^{t} H_N(j)^2}{N} \quad (13)$$

The jamming pulse is compared with the threshold value, φ, to detect the presence of the jammer. The effect of the jammer also depends on the jamming rate r, which is given by Eq. (14).

$$r = \frac{(\Delta H = H_{observed} - H_{network}) > 0}{Total\ sampling\ window\ time} \quad (14)$$

If $\Delta H > \varphi$, the presence of a jammer in the channel is detected. The use case in this section simulates the scenario where the network is under a jammer attack and reveals its impact on data transmission. It involves wireless and wired communication of wind farms to demonstrate the effect of the jammer attack. The individual subnet in the wind farm distribution network was connected to the remote server via a controlled wide area network (WAN). The jamming device is placed within the wireless network. Data from Table 3 is used to configure the jammer behavior, such as the physical characteristics of the jammer devices, such as antenna gain, antenna height, jammer power,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

and data extraction rate. Figure 11 shows the result of the attack, where the total messages received at the SCADA server are observed to be less than the messages sent from the wind farm.

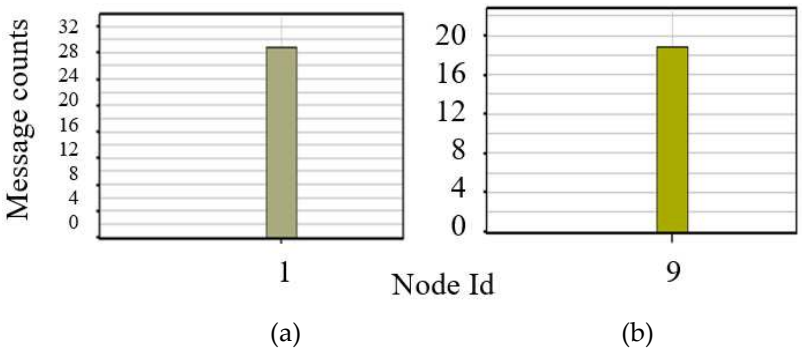


Figure 11. Quantity of messages: (**a**) sent; (**b**) received with the Jamming attack.

4.3. Module 3: Wide-Area Monitoring System (WAMS) CPS Training

For the third module, a Software-In-the-Loop (SIL) testbed is developed to perform the co-simulation of the electrical layer and network layer in the real-time simulator. The general architecture of the testbed using EXata CPS as the network emulation software and HYPERSIM for the electric power network simulation is shown in Figure 12.

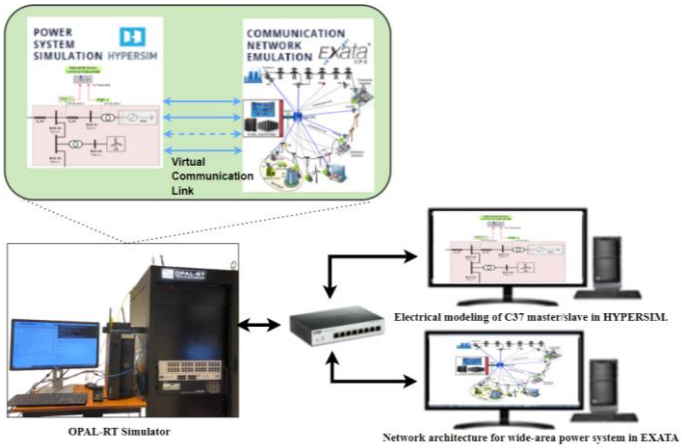


Figure 12. The co-simulation testbed architecture of the cyber-physical system.

In this module, the control architecture for the WAN in a power system network is simulated. The consists of generation units, distribution & transmission sub-stations, transmission transformers, and Phasor Measurement Units (PMUs) located at multiple locations within the power grid. PMUs are responsible for measuring the phasor signals like the voltage, current, frequency, and Frequency Rate of Change (ROC) and sending them to the Phasor Data Concentrator (PDC) located at the control center [34]. The PDC receives time-synchronized phasor data (voltage, current, frequency) from multiple PMUs to produce a real-time data stream using IEEE C37.118 master/slave protocol. C37.118 is a standard communication protocol in a power system that defines synchro phasors, frequency, and frequency ROC under all operating conditions [35]. The super PDC at the control center is configured to be C37 master and the PMUs at the microgrid are configured to be C37.118 slaves. The phasor information at multiple buses is transmitted to the control center using slave nodes. These PDC and PMU blocks in the electrical model are emulated with unique device nodes and are mapped to the virtual ethernet ports within the simulator. These ports will be assigned IP addresses and the port number configured for each master and slave. The analog points are mapped between master and slave, and the co-simulation between the electrical and network model was done in the OPAL-

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

RT simulator, and the real-time results were observed. The parameters for network delay attacks are shown in Table 4.

Table 4. General configuration for packet multiplication and delay attacks.

Property	Attack 1	Attack 2
Attack Type	Packet Multiply Attack	Delay Attack
Attacker Node	Node 2 (PDC Node)	Node 2 (PDC Node)
Layer Type	Network	Network
Destination Port	7200	7200
MODP Attack Type	Multiply	Delay
Value	2	100 ms
Number of Bytes	2	-
Start Byte	112	-

The impact of the delayed attack is shown in Figure 13, where the PMU and PDC phase angles are compared with and without the attack. The red waveform is the actual signal sent by the PMU, while the blue waveform is the signal received by the PDC. As the power system parameters are critically dependent on the synchronization of the transmitted signal, even the milli-second delay of the phasor signal will hugely impact the stability and operation of the system.

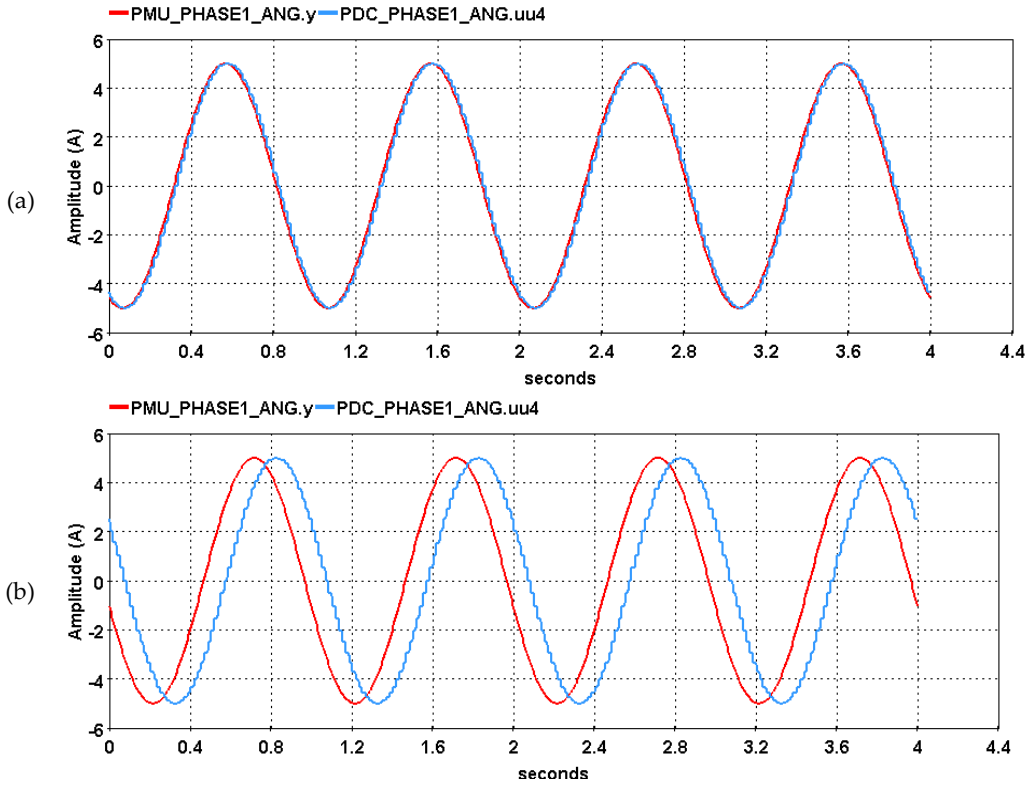


Figure 13. Comparison of the phase angle between PDC and PMU: (**a**) without delay attack; (**b**) with delay attack.

Another scenario is created to modify the packets by multiplying the signals transmitted between these two nodes. The setup follows the data presented in Table 3. This attack scenario intends to feed the PDC node with a random manipulated value. The results are presented in Figure 14, where it is possible to observe that the phasor signal received by the PDC node is considerably distorted with random values, which can critically affect the power systems' operation.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

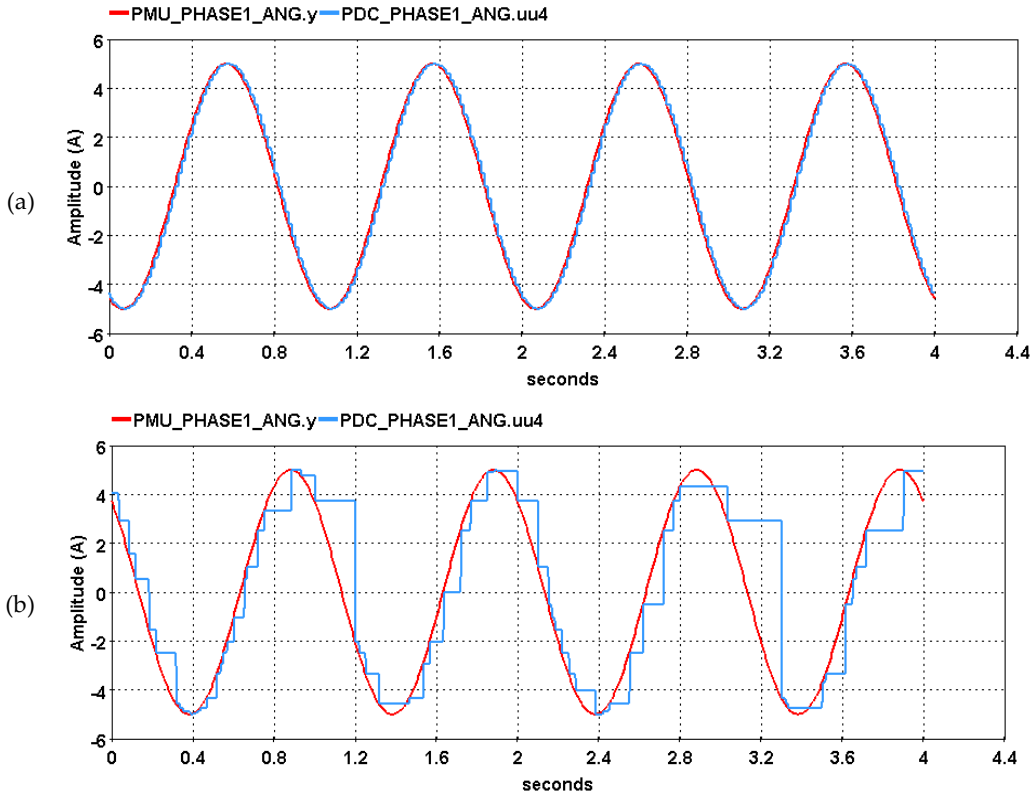


Figure 14. Comparison of the phase angle between PDC and PMU: (**a**) without multiplication attack; (**b**) with multiplication attack.

4.4. Module 4: Wind Turbine CPS Operator Training

The last module is developed to present the cyber vulnerabilities associated with the integration of renewable energy resources into power systems networks. The testbed demonstrates the simulation of a cyber-physical Wind Power Plant (WPP) connected to a transmission system subjected to cyber-attacks. The WPP is developed with 50 equivalent wind turbines, each producing 2 MW of power. The wind turbine is modeled through an equivalent mechanical formulation considering direct-drive-based type-IV, with 425V. The turbines are connected to the 34kV collector system via a double-winding saturation transformer 34.5kV/425V. The wind farm is connected to the 230kV transmission system through a 230kV/34.5kV, 125 MVA sub-station transformer. Figure 15 shows the system modeling in HYPERSIM.

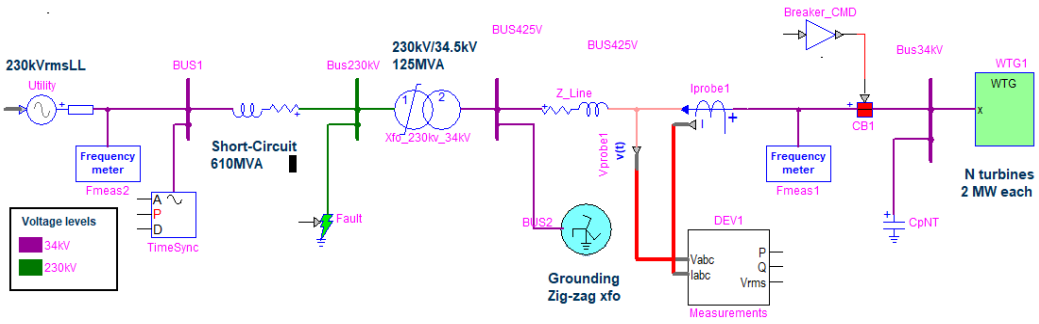


Figure 15. Wind farm and power systems physical model in HYPERSIM.

The network layer is modeled with multiple wind turbine nodes connected to the SCADA system node, as shown in Figure 16.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

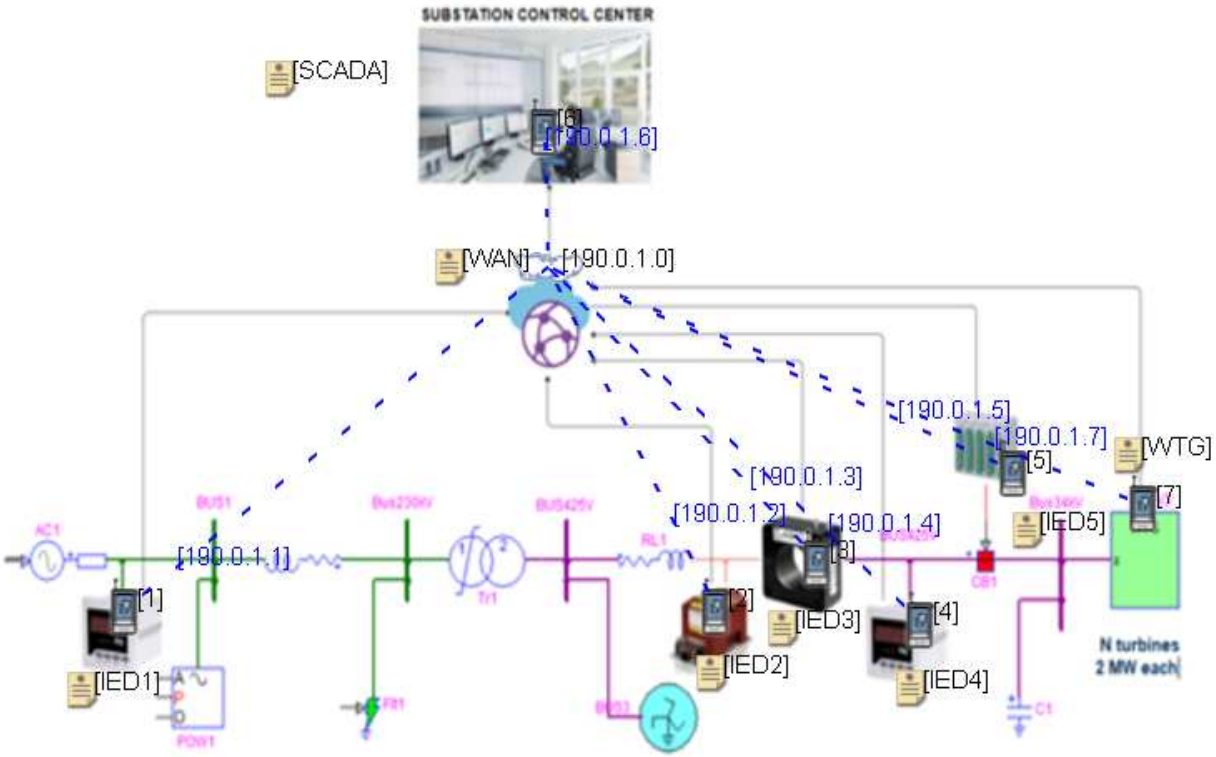


Figure 16. Schematic of the wind farm and power system communication model in EXata CPS.

A network switch is used to facilitate communication between these nodes. It is assumed that the SCADA system is connected to the controller of each wind turbine without any modification needed to the control. IEC 61850 GOOSE protocol is used to communicate between multiple IEDs and SCADA [36]. IEC 61850 is the standard communication protocol for IEDs within electrical substations. The subscriber and publisher nodes are assigned unique IP addresses, MAC addresses, and virtual ethernet ports. These virtual ethernet ports represent the common node for each device in the network and electrical layer. The SCADA is responsible for polling the nodes and communicating over the site nodes. The polling consists of monitoring the wind speed measurements, voltage, current, and power measurements. The turbine starts generating when the wind speed is above the cut-in speed and will follow the power curve [37] as the wind speed changes. When the wind speed measurements received by the control center exceed the cut-off value, a triggered alarm is sent to trigger the breaker to prevent defects and damage. To study and analyze the effect of cyber-attacks, a malicious packet manipulation attack is used to modify the packets between the wind farm and the SCADA control room. The test scenario demonstrates the multiplication of wind speed measurements by a factor that changes the actual power generated by the wind turbines. The attack scenario is represented in state equation form, defined by Eqs. (15) and (16).

$$x(t+1) = G * x(t) + B * [u(t) + \Delta u(t)] \quad (15)$$

$$y(t) = C * [x(t+1) + B * \Delta u(t)] + e \quad (16)$$

Figures 17 and 18 present the study of packet manipulation in wind speed measurement signals received at the SCADA control center with and without attack.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1243.v1

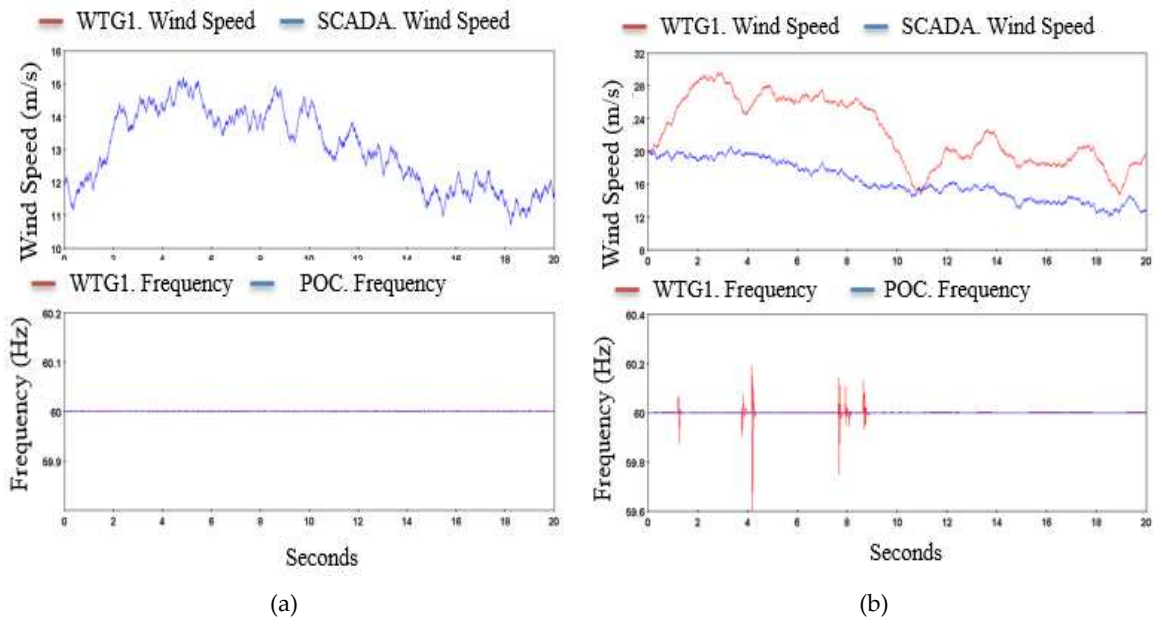


Figure 17. Comparison of wind speed and frequency: (**a**) without attack; (**b**) with attack.

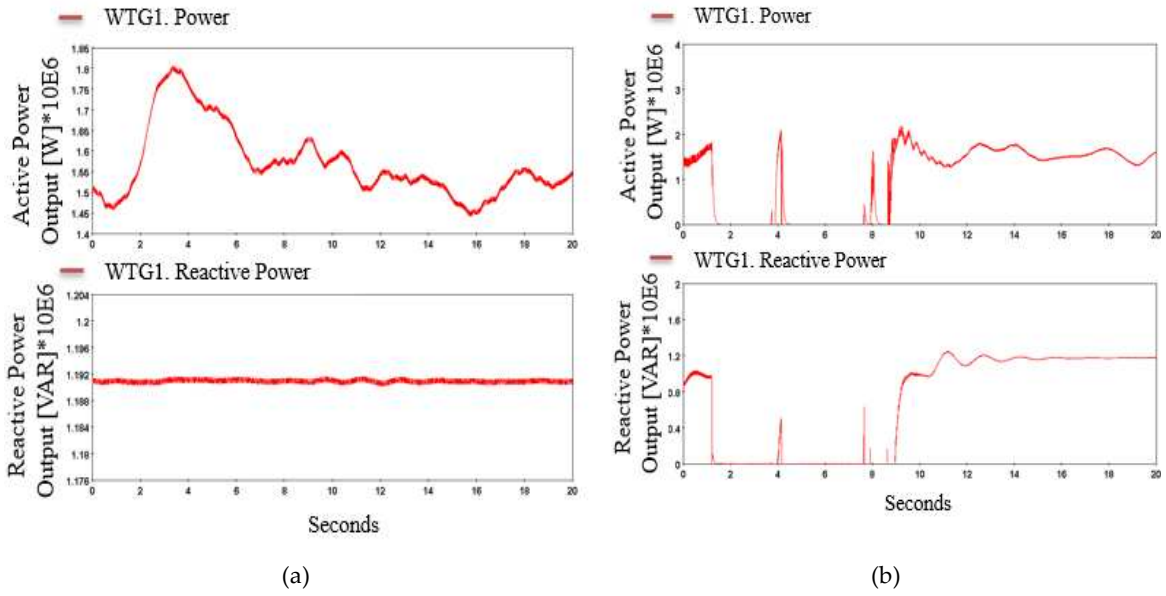


Figure 18. Comparison of the active and reactive power: (**a**) without attack; (**b**) with attack.

The normal operation shows that the actual wind speed matches the value received at the control center. Thus, the output power measured is the actual output power of the wind turbine. Under the operation of a packet manipulation attack, the actual wind speed measurement and the data received at the SCADA control differ by a scale of the random multiplier. By manipulating the wind speed, the SCADA control becomes based on a fictitious value, which decides to turn on and off of the turbine, creating frequency oscillation at the point of common coupling. It is worth highlighting that the frequency reaches approximately 60.2 and 59.6 Hz, values that are beyond the acceptable operational limits [46]. This will also affect the actual power measured from the turbine. The false information to the controller forces it to make false decisions like curtailing the output power, increasing the load demand, shutting down the turbine, or even shutting down the entire wind farm.

5. Discussion and Future Perspectives

In this paper, we performed a detailed analysis of CPS using a real-time simulator, with a focus on power system applications. To showcase the efficacy of the methodology and description of the CPS security landscape, we examine four different modules- one distribution system operation and a SCADA system, and three cyber-attack scenarios. Each scenario is accompanied by pertinent background details, a mathematical formulation, and a discussion of the threat model and attack configurations involved. These case studies undergo simulation in both typical and atypical operating conditions to reveal their comprehensive effects on the entire system. The paper provides a comprehensive approach and valuable studies that provide guidelines for modeling threats in Cyber-Physical Systems (CPS). It also offers insights into designing, simulating, and evaluating detailed CPS models. The framework introduced in the paper is a valuable tool for conducting rigorous security analyses of CPS, ultimately contributing to a deeper and more thorough understanding of CPS security.

By building upon the existing foundation, our objective is to push the boundaries and unlock new possibilities for the framework, enabling more comprehensive and sophisticated assessments of CPS security.

- Module 4.1 can be expanded to include dynamic reconfiguration and self-healing capabilities during faults and/or power blackout events.
- Module 4.2 can incorporate multiple cyber-attack scenarios such as Man-in-the-middle (MitM) attacks, False data injection attacks, Vulnerability attacks, Software-based attacks, Passive attacks such as Eavesdropping, Port Scanning, Network scanning, and Signal intelligence attacks.
- Module 4.3 can add wide-area synchro phasor monitoring, protection, and control to simulate loss of generation or load due to cyber-attacks on power system frequency and/or voltages.
- Module 4.4 can be further studied to develop simulation-aided risk assessments, real-time intrusion detection systems, and cyber defense mechanisms on DERs integrated smart grids.

6. Conclusion

The paper presents insight into the intrinsic correlation between the physical and cyber elements of the electric power system. With the current wide use of IEDs to support power systems operation and the advancement of fast communication protocols and control actions, cyber security is critical to ensure reliability. However, to ensure security, it is first necessary to understand the malicious behaviors and their impact on the system's performance. This study proposed and developed a complete cyber-physical testbed, with a focus on teaching and training industry professionals on different CPS aspects. The testbed was designed to demonstrate cyber vulnerabilities by simulating different cyber-attacks in real-time power systems models and actual IEDs. The testbed design prioritized the creation of a reliable and realistic environment by using HIL and SIL concepts. IEDs from the Schweitzer Engineering Laboratories (SEL) and the Survalent SCADA software are integrated into OPAL-RT real-time digital simulator to create a complete system from the electrical model to the operator's GUI. Besides that, the cutting-edge EXata CPS software was used for communication network modeling and cyber-attack simulation.

Different operational scenarios were developed and tested under different types of cyber-attacks to analyze the response and performance of the system under intrusions. The proposed modules provide vital insights into information security management, secured communication architecture, system and device security, and software-based attestation. Using secured broadcasting capable of detecting DoS and jamming mechanisms will aid the design of highly resilient SCADA systems for the emerging smart grids that can mitigate the cyber-attack while achieving high-level availability. This testbed has already been used to train more than 100 students and industry professionals through a Texas Work Force Grant, and it is expected that the development of this testbed will

support and encourage advancements in training, teaching, and developing CPS solutions in other institutions.

Author Contributions: Conceptualization, MC and RB; methodology, RB and KS; software, RB; validation, RB, KS and MC; formal analysis, RB and KS; investigation, KS; resources, RS; data curation, RS; writing—original draft preparation, RB; writing—review and editing, MC and KS; visualization, KS; supervision, MC; project administration, MC; funding acquisition, MC. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Texas Workforce under the Wagner Peyser Program, Award Number W912HQ20C0022.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki, "Networked Microgrids for Enhancing the Power System Resilience," Proceedings of the IEEE, vol. 105, no. 7. Institute of Electrical and Electronics Engineers Inc., pp. 1289–1310, Jul. 01, 2017. doi: 10.1109/JPROC.2017.2685558.
2. D. T. Ton and M. A. Smith, "The U.S. Department of Energy's Microgrid Initiative," Electricity Journal, vol. 25, no. 8, pp. 84–94, Oct. 2012, doi: 10.1016/j.tej.2012.09.013.
3. "Reliability Considerations from the Integration of Smart Grid," 2010. [Online]. Available: www.nerc.com
4. "Design of the HELICS High performance transmission distribution communication market".
5. J. Bryson and P. D. Gallagher, "NIST Special Publication 1108R2 NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0," 2012.
6. J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for Distributed Energy Resources and Smart Inverters."
7. Electric Power System Resiliency CHALLENGES AND OPPORTUNITIES POWER SYSTEM TRANSFORMATION."
8. K. Marashi, S. Sedigh Sarvestani, and A. R. Hurson, "Consideration of Cyber-Physical Interdependencies in Reliability Modeling of Smart Grids."
9. R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," IEEE Trans Smart Grid, vol. 6, no. 5, pp. 2444–2453, Sep. 2015, doi: 10.1109/TSG.2015.2432013.
10. 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. 847–855, 2013, doi: 10.1109/TSG.2012.2226919.
11. H. Cui, F. Li, and K. Tomsovic, "Cyber-physical system testbed for power system monitoring and wide-area control verification," IET Energy Systems Integration, vol. 2, no. 1, pp. 32–39, Mar. 2020, doi: 10.1049/iet-esi.2019.0084.
12. X. Zhou, X. Gou, T. Huang, and S. Yang, "Review on Testing of Cyber Physical Systems: Methods and Testbeds," IEEE Access, vol. 6. Institute of Electrical and Electronics Engineers Inc., pp. 52179–52194, Sep. 12, 2018. doi: 10.1109/ACCESS.2018.2869834.
13. H. Tong, M. Ni, L. Zhao, and M. Li, "Flexible hardware-in-the-loop testbed for cyber physical power system simulation," IET Cyber-Physical Systems: Theory and Applications, vol. 4, no. 4, pp. 374–381, Dec. 2019, doi: 10.1049/iet-cps.2019.0001.
14. M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A Survey on Smart Grid Cyber-Physical System Testbeds," IEEE Communications Surveys and Tutorials, vol. 19, no. 1. Institute of Electrical and Electronics Engineers Inc., pp. 446–464, Jan. 01, 2017. doi: 10.1109/COMST.2016.2627399.
15. S. McLaughlin et al., "The Cybersecurity Landscape in Industrial Control Systems," Proceedings of the IEEE, vol. 104, no. 5, pp. 1039–1057, May 2016, doi: 10.1109/JPROC.2015.2512235.
16. J. Xie, J. C. Bedoya, C. C. Liu, A. Hahn, K. J. Kaur, and R. Singh, "New educational modules using a Cyber-Distribution system testbed," IEEE Transactions on Power Systems, vol. 33, no. 5, pp. 5759–5769, Sep. 2018, doi: 10.1109/TPWRS.2018.2821178.
17. C. B. Vellaithurai, S. S. Biswas, R. Liu, and A. Srivastava, "Real time modeling and simulation of cyber-power system," Power Systems, vol. 79, pp. 43–74, 2015, doi: 10.1007/978-3-662-45928-7_3.
18. Y. Mo et al., "Cyber-physical security of a smart grid infrastructure," Proceedings of the IEEE, vol. 100, no. 1, pp. 195–209, 2012, doi: 10.1109/JPROC.2011.2161428.
19. G. Dondossola and R. Terruggia, "Cyber security of smart grid communications: Risk analysis and experimental testing," Power Systems, vol. 79, pp. 169–193, 2015, doi: 10.1007/978-3-662-45928-7_7.
20. J. Hong, Y. Chen, C. C. Liu, and M. Govindarasu, "Cyber-physical security testbed for substations in a power grid," Power Systems, vol. 79, pp. 261–301, 2015, doi: 10.1007/978-3-662-45928-7_10.

21. MITRE Enterprise Engineering. Crown Jewels Analysis. Accessed: Oct. 10, 2020. [Online]. Available: https://www.mitre.org/publications/ systems-engineering-guide/enterprise-engineering/systems-engineering- for-mission-assurance/crown-jewels-analysis
22. "MICROGRID REAL-TIME SIMULATION." Accessed: Mar. 10, 2022. [Online]. Available: https://www.opal-rt.com/microgrid-overview/
23. YOTTAVOLT, "https://www.yottavolt.com/shop/rt-lab/."
24. H. Tong, M. Ni, L. Zhao, and M. Li, "A Flexible Hardware-in-the-loop Testbed for Cyber Physical Power System Simulation."
25. "SCALABLE Network Technologies Cyber Security Solutions for Critical Infrastructure."
26. L. Zhang et al., "Cybersecurity Study of Power System Utilizing Advanced CPS Simulation Tools." [Online]. Available: http://conference-americas.pacw.org/
27. "SCADA SurvalentONE." Accessed: Mar. 10, 2022. [Online]. Available: https://www.survalent.com/adms-platform-overview/
28. H. Padullaparti et al., "Peak Load Management in Distribution Systems Using Legacy Utility Equipment and Distributed Energy Resources Preprint," 2021. [Online]. Available: www.nrel.gov/publications.
29. "SCADA SurvalentONE." Accessed: Mar. 11, 2022. [Online]. Available: https://www.survalent.com/adms-platform-overview/.
30. University of Nebraska--Lincoln, IEEE Region 4, IEEE Computer Society, IEEE Communications Society, IEEE Power & Energy Society, and Institute of Electrical and Electronics Engineers, 2017 IEEE International Conference on Electro Information Technology (EIT) : 14-17 May 2017.
31. A. Ahmad, Y. Abuhour, and F. Alghanim, "A novel model for distributed denial of service attack analysis and interactivity," Symmetry (Basel), vol. 13, no. 12, Dec. 2021, doi: 10.3390/sym13122443.
32. A. Cortés-Leal, C. Del-Valle-soto, C. Cardenas, L. J. Valdivia, and J. A. del Puerto-Flores, "Performance metric analysis for a jamming detection mechanism under collaborative and cooperative schemes in industrial wireless sensor networks," Sensors, vol. 22, no. 1, Jan. 2022, doi: 10.3390/s22010178.
33. J. Zhao, M. Netto, and L. Mili, "A Robust Iterated Extended Kalman Filter for Power System Dynamic State Estimation," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3205–3216, Jul. 2017, doi: 10.1109/TPWRS.2016.2628344.
34. M. Hojabri, U. Dersch, A. Papaemmanouil, and P. Bosshart, "A comprehensive survey on phasor measurement unit applications in distribution systems," Energies, vol. 12, no. 23. MDPI AG, Nov. 29, 2019. doi: 10.3390/en12234552.
35. J. Ritchie and C. F. R. Robertson, "A Comparison of Phasor Communication Protocols and the Streaming Telemetry Transport Protocol (STTP) for the Transfer of Synchrophasor and Other Streaming Data," 2019. [Online]. Available: https://gridprotectionalliance.org
36. Y. Bhamare, "Utilization of IEC 61850 GOOSE messaging in protection applications in distribution network."
37. Y. A. Katsigiannis and G. S. Stavrakakis, "Estimation of wind energy production in various sites in Australia for different wind turbine classes: A comparative technical and economic assessment," Renew energy, vol. 67, pp. 230–236, 2014, doi: 10.1016/j.renene.2013.11.051.
38. R. Liu, C. Vellaithurai, T. Gamage, and A. Srivastava, "IEEE TRANSACTIONS ON SMART GRID Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid."
39. C. B. Vellaithurai, S. S. Biswas, and A. K. Srivastava, "Development and Application of a Real-Time Test Bed for Cyber–Physical System," IEEE Syst J, pp. 1–12, 2015, doi: 10.1109/JSYST.2015.2476367.
40. S. McLaughlin et al., "The Cybersecurity Landscape in Industrial Control Systems," Proceedings of the IEEE, vol. 104, no. 5, pp. 1039–1057, May 2016, doi: 10.1109/JPROC.2015.2512235.
41. M. N. Kurt, Y. Yilmaz, and X. Wang, "Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid," IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 498–513, 2018, doi: 10.1109/TIFS.2018.2854745.
42. A. Gambier, "Real-time control and hardware-in-the-loop simulation for educational purposes of wind energy systems," IFAC-PapersOnLine, vol. 53, no. 2, pp. 17344–17349, 2020, doi: 10.1016/j.ifacol.2020.12.2084.
43. P. Wlazlo et al., "Man-in-The-Middle Attacks and Defense in a Power System Cyber-Physical Testbed," Feb. 2021, doi: 10.1049/cps2.12014.
44. K. Gupta, S. Sahoo, B. K. Panigrahi, F. Blaabjerg, and P. Popovski, "On the assessment of cyber risks and attack surfaces in a real-time co-simulation cybersecurity testbed for inverter-based microgrids," Energies (Basel), vol. 14, no. 16, Aug. 2021, doi: 10.3390/en14164941.
45. R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," IEEE Trans Smart Grid, vol. 6, no. 5, pp. 2444–2453, 2015, doi: 10.1109/TSG.2015.2432013.
46. M. Jayachandran, C. R. Reddy, S. Padmanaban, and A. H. Milyani, "Operational planning steps in smart electric power delivery system," *Sci. Rep.*, vol. 11, no. 1, Dec. 2021, doi: 10.1038/s41598-021-96769-8.