*energies*

MDPI

*Article*

# A Hybrid Physical Co-Simulation Smart Grid Testbed for Testing and Impact Analysis of Cyber-Attacks on Power Systems: Framework and Attack Scenarios

**Mahmoud S. Abdelrahman, Ibtissam Kharchouf, Tung Lam Nguyen and Osama A. Mohammed ***

Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174, USA; mabde046@fiu.edu (M.S.A.); ikhar002@fiu.edu (I.K.); tunguyen@fiu.edu (T.L.N.)
* Correspondence: mohammed@fiu.edu; Tel.: +1-305-348-3040

**Abstract:** With the deployment of numerous innovative smart grid technologies in modern power systems, more real-time communication and control are required due to the complexity and proliferation of grid-connected systems, making a power system a typical cyber-physical system (CPS). However, these systems are also exposed to new cyber vulnerabilities. Therefore, understanding the intricate interplay between the cyber and physical domains and the potential effects on the power system of successful attacks is essential. For cybersecurity experimentation and impact analysis, developing a comprehensive testbed is needed. This paper presents a state-of-the-art Hybrid Physical Co-simulation SG testbed at FIU developed for in-depth studies on the impact of communication system latency and failures, physical events, and cyber-attacks on the grid. The Hybrid SGTB is designed to take full advantage of the benefits of both co-simulation-based and physical-based testbeds. Based on this testbed, various attack strategies are tested, including man-in-the-middle (MitM), denial-of-service (DoS), data manipulation (DM), and setting tampering (change) on various power system topologies to analyze their impacts on grid stability, power flow, and protection reliability. Our research, which is based on extensive testing on several testbeds, shows that using hybrid testbeds is justified as both practical and effective.

**Keywords:** smart grid; cyber-physical power system; hybrid testbed; cyber-attacks; ns-3; OPAL-RT



**Citation:** Abdelrahman, M.S.; Kharchouf, I.; Nguyen, T.L.; Mohammed, O.A. A Hybrid Physical Co-Simulation Smart Grid Testbed for Testing and Impact Analysis of Cyber-Attacks on Power Systems: Framework and Attack Scenarios. *Energies* **2023**, *16*, 7771. https://doi.org/10.3390/en16237771

Academic Editor: José Matas

Received: 25 October 2023
Revised: 17 November 2023
Accepted: 19 November 2023
Published: 25 November 2023



## 1. Introduction

The smart grid is one of the fundamental technologies supporting sustainable economic and societal growth. Today's energy infrastructure is shifting significantly across all generation, transmission, and distribution systems to provide dependability and sustainability to the power system network. Therefore, electric power systems have evolved into densely interconnected cyber-physical systems that rely heavily on advanced communications due to the networked physical and electronic sensing, monitoring, and control devices connected to a control center in the energy control and protection system [1]. As a result, this expansion has increased the vulnerability of power systems to various cyber-attacks, which might have various negative consequences and cascading failures, from the destruction of interconnected critical infrastructure to the loss of life [2]. The power grid's primary goal is to deliver electricity to load centers with reliability. The physical layer of large electric power networks is coupled with a cyber system of information and communication technologies, including complex devices and systems like supervisory control and data acquisition (SCADA) systems and intelligent electronic devices (IEDs), to operate effectively and dependably. By using these devices and systems to control circuit breakers, transformers, capacitor banks, and other equipment, power systems are particularly vulnerable to cyber-attacks. The protection and control systems, which are known as the backbones of power networks because the former detects abnormal conditions and quickly corrects them, and the latter maintains the integrity of the system and stabilizes it in

the wake of physical disturbances, are the main beneficiaries of these communication-based schemes and components. Power system controllers in the SCADA hub process the data gathered and communicate the necessary commands to the appropriate actuators.

Cybercriminals recently launched a wave of expertly coordinated and sophisticated attacks. Utility grid operators deal with cyber incursions daily, including denial of service, physical systems, malicious intent, and authentication threats. The risk is substantially higher when it comes to SCADA systems, security, control, and protection equipment recognized vulnerabilities. Multiple cyber-attacks against smart grid systems have occurred in recent years. During the 2015 cyber-attack on the Ukrainian electricity grid, circuit breakers were opened and closed without the control centers' knowledge [3]. By simulating cyber-attacks in an Aurora generator test, researchers have examined the severity of malicious switching and DoS attacks on protective digital relays for the Ukrainian power grid [4]. A new discussion about limiting remote access to circuit breakers and managing them locally was triggered by this cyber-attack. However, restricting breakers' direct remote access does not guarantee that an online attack will not send them dangerous commands. Protective relays can control breakers locally, frequently relying on communication networks susceptible to cyber-attacks [5]. As a result, the corresponding breaker has been indirectly targeted if an attack can change the data sent to a relay so that the relay issues a false trip instruction. The automatic generation controller (AGC) controls the power exchange between adjacent areas at predetermined levels and maintains the system frequency within acceptable ranges by altering the load reference set-point. Through a communication system, all inputs and outputs are sent and received. AGC systems are, however, susceptible to cyber-attacks because they rely on the communication infrastructure. The grid's frequency, stability, and profitable functioning can all be directly impacted by cyber-attacks introducing false control or measurements into the AGC data stream [6]. A successful attack on a protection system may involve interfering with the measurements taken and judgments made by a remote relay in communication with a local relay [7]. According to [8], there are three main categories of research on the cybersecurity of protection systems in AC and DC systems. The first group concentrates on attack modeling and risk assessment in protection systems, a description of the framework for modeling coordinated switching attacks over circuit breakers and relays, and an assessment of the effect of bus and transmission line protection techniques on the cybersecurity of the power system [9–11]. The cybersecurity of substations has received a lot of attention in the second group of studies. In [12], the authors introduced a technique for detecting and thwarting cyber-attacks on substation automation systems. The third group of studies has created a mechanism that uses power networks' physical and digital characteristics to identify attacks and distinguish them from faults [9]. Therefore, a power network's cybersecurity of its protection and control mechanisms should be upgraded in addition to its physical security. This upgrade must be previously tested and validated before implementation.

The ability of energy assets to identify and comprehend such innovative and intelligent threats and system vulnerabilities to build smart, effective countermeasures while maintaining the real-time functioning of the energy system in a secure and reliable condition is a critical challenge. This requires efforts and endeavors from grid operators and researchers to study the system operation under these abnormal conditions with extensive testing and impact analysis without harming the system's security and reliability. However, the high cost of implementing and utilizing actual system hardware and software for testing purposes and the possible harm caused by simulating cyber-attacks on live power systems are major obstacles [13]. In addition, real measurements (such as voltages, currents, and frequency) and information and communications technology (ICT) data (such as communication protocols and security logs) are unavailable due to power companies' security concerns. Therefore, for research and demonstration purposes, one of the most important tools for investigating the cyber-physical security of power systems is a cyber-physical testbed, which is a useful choice for gathering accurate data from physical and cyber systems [14]. Research initiatives targeted at enhancing the resilience of the electrical

system can be conducted and evaluated in testbeds that can successfully incorporate both the cyber and physical components of the smart grid [15]. It is seen as a viable approach to investigating and addressing cybersecurity challenges. From the architecture viewpoint, the development of a cyber-physical smart grid and the accompanying testbeds, which include a variety of testing paradigms with related challenges and their solutions, were thoroughly reviewed by Smadi et al. [16]. According to this study, the authors classified and explained three categories of testbeds: hardware-based, software-based, and hybrid-based.

The cyber-physical testbed offers a realistic setting for studying how a sophisticated power and ICT systems interact through simulation and modeling. It is crucial to research the cause-and-effect correlations of cyber intrusions, the susceptibility and resilience of power systems, and the performance and dependability of applications in a testbed's realistic environment. Power, communication, and control/protection systems are the fundamental elements of the SG testbeds in the electric power sector. In the power system model, the measurements and status information needed for substation situational awareness are obtained. The communication system uses a variety of industry-standard protocols and communication media to communicate data between the substation and the control center, including measurements and commands necessary for the efficient operation of the power system. The control and protection systems encompass all the apparatus used and deployed in the control center. To the best of our knowledge, research in this area has been sparse, and the field has not been fully investigated despite the growing concern regarding the benefits and technical challenges of smart grid vulnerability analyses. Investigations into attack simulations and assessments of their effects on the infrastructure have not received much attention. Therefore, creating a new framework to facilitate smart grid attack simulation, emulation, and even real attacks is crucial.

Several smart grid testbeds have been created. Each testbed has particular characteristics and purposes of its own from the viewpoints of both architecture and functions. In [16], the authors provided a comprehensive list of existing cyber-physical smart grid testbeds from various research institutes. The majority of these testbeds are either simulation-based or use a co-simulation platform. Accordingly, the cyber-attack model may be simulated in the power system layer by some assumptions or emulated through the communication layer if the communication network is modeled. There are not many testbeds that are entirely hardware-based. Even though fully hardware-based testbeds are hard to implement, they can guarantee fidelity. Some of these testbeds [17–24] are listed and compared with the developed Hybrid SGTB in Table 1 of this paper. This study describes the cutting-edge Hybrid Physical Co-simulation SG Testbed at Florida International University, which was created for in-depth research on the effects of communication system latency and failures, physical events, and cyber-attacks on the grid. In the physical testbed part, the physical and network layers are deployed using real hardware and industrial-grade software, providing a high-fidelity model that closely mimics the real CPS. Since it is pretty challenging to reconfigure such testbeds for different research endeavors, the co-simulation testbed, which is mainly constructed from OPAL-RT as a modern real-time simulator that can accurately mimic the response of an actual physical system in real time and ns-3 for communication network emulation, is developed to overcome this challenge. This testbed can provide a more flexible configuration, easier expansion to large-scale CPSs, easier testing of evolving cyber-attacks, and full instrumentation through software probes to determine exactly what happened at every component of the CPS. It is designed to take full advantage of the benefits of co-simulation- and physical-based testbeds. Hence, the power system can either be an actual power system component of the physical testbed or simulated in real time, as in the OPAL-RT using the co-simulated testbed. Also, the measurements and actuation commands are either sensed directly from a physical device in the physical testbed or simulated and transmitted over the network emulation in the co-simulated testbed. To assess the effects of these cyber-attacks on grid stability, power flow, and protection dependability, a variety of attack tactics, including data manipulation (DM), setting change, man-in-the-middle (MitM), and denial-of-service (DoS), are tested on

the basis of this testbed on various power system topologies by real attackers and virtual attackers. Our study demonstrates that the usage of hybrid testbeds is justified as both feasible and efficient.

**Table 1.** Taxonomy of cyber-physical smart grid testbeds.

| Testbed | Power System | | Communication Network Model | Commercial Devices | Attack Model | |
|---|---|---|---|---|---|---|
| | Practical | Simulation | | | Real Agent | Emulation |
| [17] | N/A | RTDS | ns-3 | SEL IEDs | N/A | DaterLab |
| [18] | N/A | RTDS | ISEAGE | IEDs/PLC | N/A | ISEAGE |
| [19] | N/A | OPAL-RT | OMNeT++ | SEL IEDs | N/A | N/A |
| [20] | N/A | RTDS | WANE | N/A | N/A | WANE |
| [21] | N/A | PSCAD | OMNeT++ | N/A | N/A | OMNeT++ |
| [22] | N/A | GridLAB-D | ns-3 | N/A | N/A | ns-3 |
| [23] | N/A | OPAL-RT | Ethernet-based | SEL IEDs | N/A | Simulated |
| [24] | N/A | OPAL-RT | Exata CPS | SEL IEDs | N/A | Exata CPS |
| Hybrid SG-TB | Reduced scale power system | OPAL-RT | Ethernet-based and ns-3 | ABB/SEL IEDs | Real PCs | ns-3/ Docker container |

To summarize, the key contributions of the authors are as follows:

- We developed a hybrid smart grid testbed (SGTB) as a comprehensive environment for testing and impact analysis studies of cyber-attacks on the power grid, comprising a fully physical testbed and co-simulation testbed.
- In the physical testbed, we built a reduced-scale power system including generation, transmission, and loads with the full connection of instrument transformers and commercial devices to provide protection and control applications through a real Ethernet network.
- We developed a real-time cyber-physical co-simulation testbed on three different machines to fully represent the different layers in the CPS using OPAL-RT and ns-3 integrated with docker containers.
- We demonstrated the impact of different attacks on the tested grid using real agents (PCs) connected through the communication network in the physical testbed.
- We developed virtual attack models using the docker containers with the ns-3 model to emulate or closely imitate the attacker behavior in the co-simulation testbed.

The rest of this paper is organized as follows. In Section 2, we describe the architecture of the hybrid SGTB. Section 3 explains cyber-attacks in cyber-physical energy power systems and different techniques for testing these attacks. Cyber threats in digital substation protection are introduced with a brief description of relay configuration and its data model in Section 4. Implementations of two attack scenarios in the physical testbed are described in detail in Section 5. Section 6 discusses our proposed co-simulation testbed set-up in detail, including OPAL-RT, ns-3, and docker container. We discuss the attack model of DoS and MitM in the co-simulation platform in Section 7. In Section 8, we conclude this work and propose future evolution and enhancement of the platform.

## 2. Hybrid SGTB Architecture

A testbed is an experimental environment outfitted with state-of-the-art equipment and technology assembled to produce a test system or equipment. Through testbeds, it is possible to validate cutting-edge concepts for digital transformation and digitalization as well as products, systems, and technology. They are frequently used for instructive and demonstrative applications and in research, development, and invention projects. Most testbeds are created primarily for the assessment and validation of certain tasks. Few testbeds offer complete hardware and software assessment policies for research purposes; however, certain testbeds offer insights for particular study disciplines. This section examines the design and execution of a complete cyber-power testbed, including simulation, emulation, and real devices in a modular approach. Commercial hardware, software, and

simulated devices make up the data measuring and collection system. This testbed also has hardware-in-the-loop (HIL) and controller-in-the-loop (CIL) features enabling one to connect to and communicate with real hardware controllers and relays. However, with no power amplifier in the laboratory, it does not provide power hardware-in-the-loop (PHIL). Protection relays and every other control component in a microgrid may be evaluated early since they are real. Most current cyber-physical power system testbeds utilize this paradigm since commercial products provide both efficient ICT network integration and a broad degree of system-in-the-loop tests. The Hybrid SGTB at FIU is a composite of a physical testbed with everything real as a reduced-scale power system, and the co-simulation testbed is built using a combination of real-time simulators. The general architecture of the testbed is shown in Figure 1.

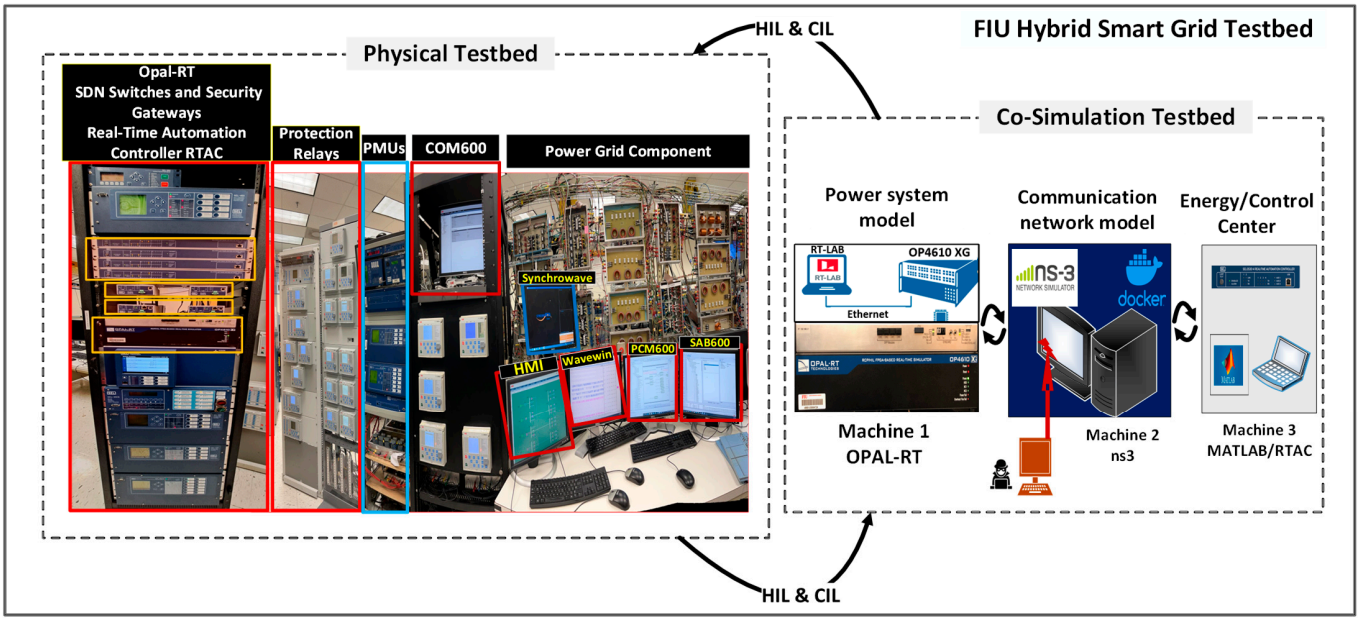


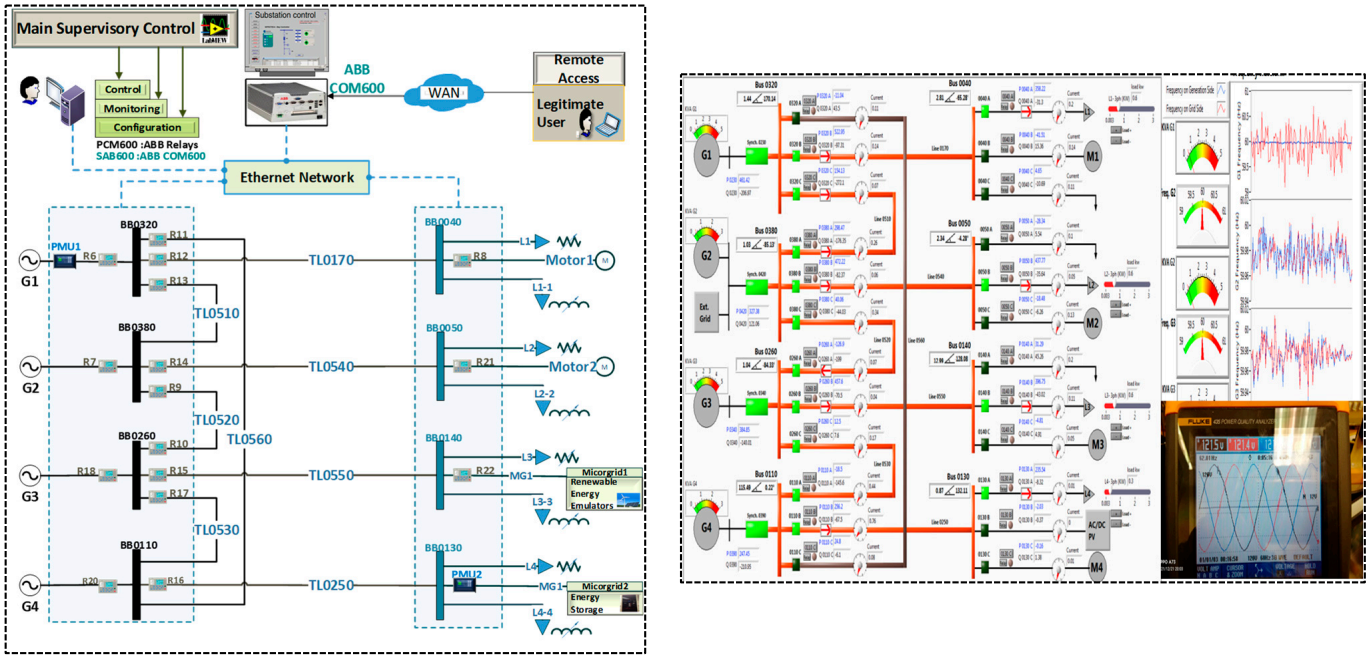

**Figure 1.** Hybrid SGTB architecture at FIU.

### *2.1. Physical Testbed*

Considering the smart grid broadly, it is defined by its capabilities and operational traits rather than by the use of any specific technology. The smart grid testbed at FIU is a cutting-edge research facility that was created as an integrated hardware-based AC/DC system. This state-of-the-art system's hardware, software, and communication components can all conceptualize a comprehensive cyber-physical smart grid framework. The physical testbed is a unique, reduced-scale low-voltage testbed that provides researchers with a way to evaluate the operation and cybersecurity of power systems. While all system components run at voltages below 230 volts, they imitate functions at higher voltages and larger sizes. As shown in Figure 2a, the components of the physical testbed system are interconnected. It features four AC generators set up in a ring configuration, and supply loads are linked to the load buses via line models.

Additionally, this system has connections to the available DAQs monitoring system's communication infrastructure and the wide-area communications network to implement the equipment for power system control and the SCADA system. Figure 2b depicts the control virtual instrument (VI) used in the LabVIEW environment to manage and display input/output data as data, curves, or indicators. The detailed parameters of power system components (generators, transmission lines, and loads) were discussed and illustrated in [25]. The platform is being used to create microgrid technologies, such as converters based on power electronics, energy storage, communications protocols, and integration of DERs and vehicles [26]. To simulate various power grid schemes, the configuration of the testbed may also be dynamically changed. This physical part of the testbed has been

modified several times with a new infrastructure to mimic the requirements and challenges of a smart grid regarding integrating renewables and energy storage devices and connecting various commercial IED types. Various protection relays and phasor measurement units (PMUs) from different vendors, including Schweitzer and ABB have been installed at different points through voltage and current sensors based on their functions, such as generator protection, line protection, and motor protection.




(**a**) (**b**)

**Figure 2.** Physical testbed infrastructure: (**a**) SLD and protection relays deployment; (**b**) main supervisory control panel using LabVIEW.

### *2.2. Co-Simulation Testbed*

The desire for co-simulation environments that embody several domains' characteristics is growing. Therefore, studies of the effects of data transfers on control systems can be carried out with better precision with network emulation capabilities. Regarding facilitating data connectivity on the testbed, Ethernet is a popular and easily accessible data communications technology that supports a wide range of protocols, including TCP/IP and UDP. As shown in Figure 3, the FIU testbed implements and builds a comprehensive cyber-physical power system of three-domain modeling and simulation of three different machines: (1) Machine 1 is OPAL-RT for power system domain modeling and simulation in real time, (2) Machine 2 is a Linux computer for communication network domain modeling and emulation using ns-3 and docker containers, and (3) Machine 3 is for power system application domain implementation which can be industrial-grade devices such as protection relays, real-time automation controllers, or simulation tools such as MATLAB/Simulink.

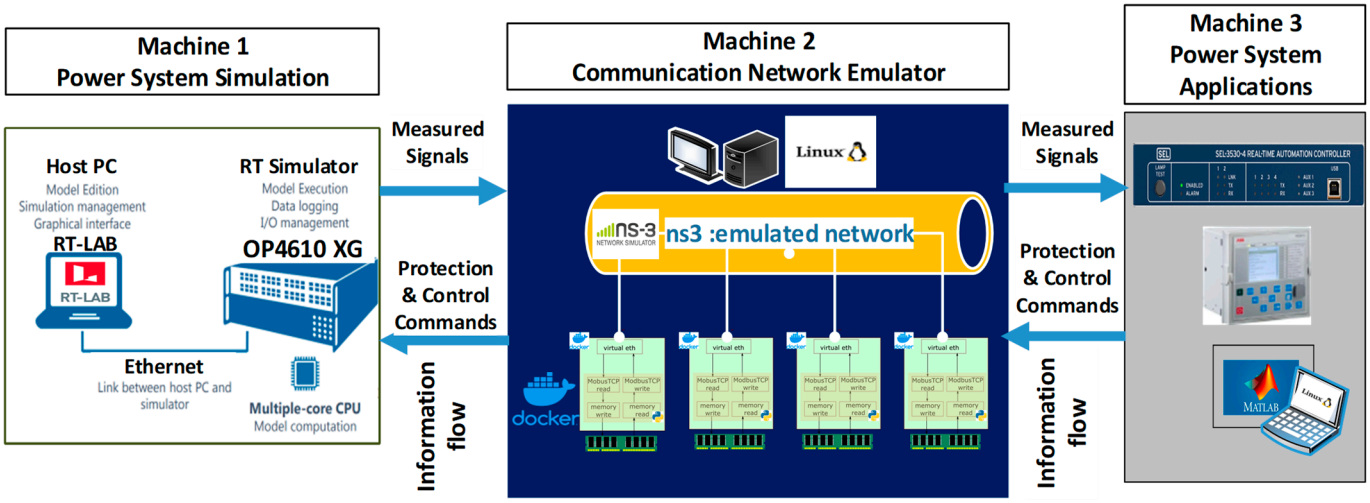



**Figure 3.** Co-simulation testbed architecture and main components.

## 3. Modeling and Testing of Cyber-Attacks in Energy Power Systems

### *3.1. CPS Layers and Attack Modeling*

Typical cyber-physical systems (CPSs) combine computational and communication components to control, protect, and manage physical objects. Understanding how cyber and physical components interact is necessary to research cyber-physical challenges. The three components of a power system are generation, transmission, and distribution, which are sensed and actuated through IoT devices. Sensors communicating with field devices (generators, transmission lines, etc.) send measurements to control centers using dedicated communication protocols. In the physical layer, the measurements $y(t)$ may refer to quantities such as voltage, current, and frequency. These measurements are processed by computational protection and control algorithms running in the control center to make operational decisions. Actuators are then given the decision $u(t)$ to alter the field devices. Figure 4 fully represents the interaction between physical and cyber layers. To better study the impacts of cyber-physical events such as cyber-attacks and/or communication failure, the communication layer in the middle must be modeled and appropriately simulated with a high level of flexibility.

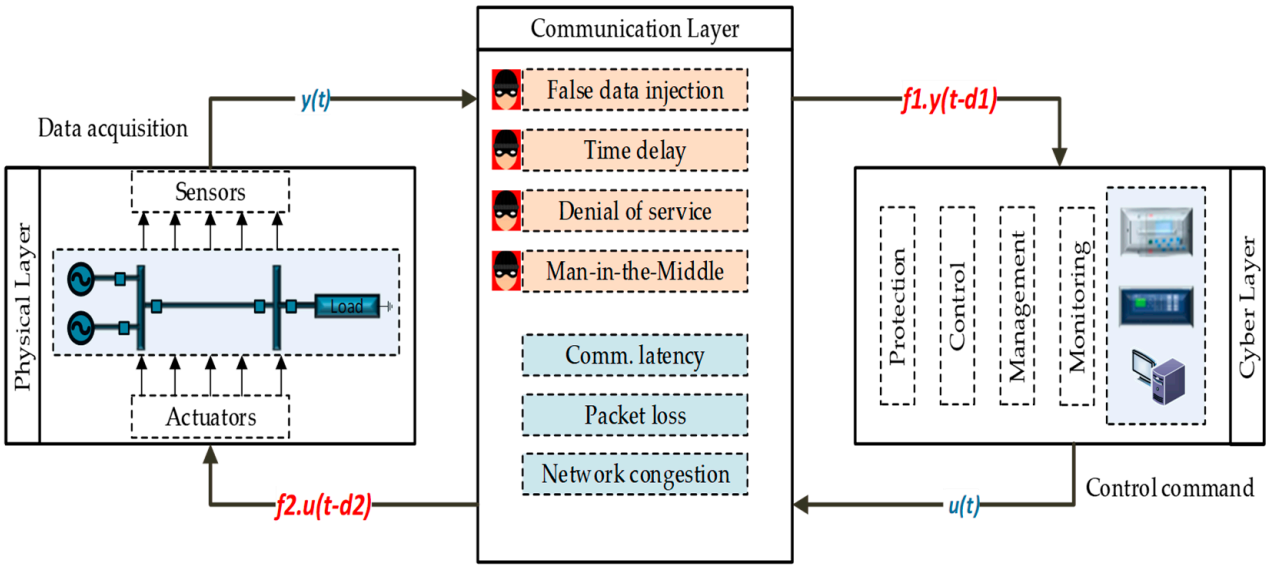


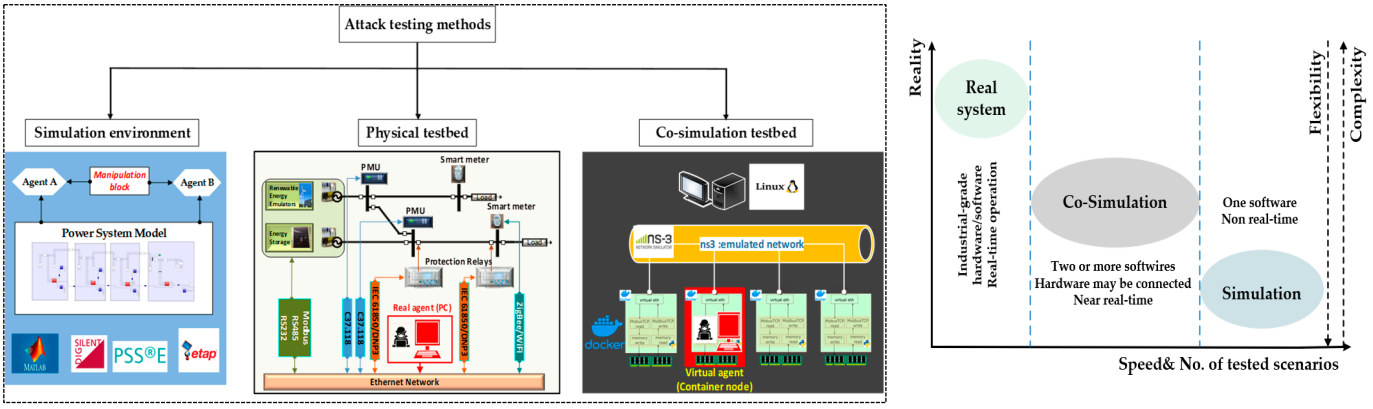

**Figure 4.** Cyber-physical system layer data and interaction.

An adversary could build attack templates intended to alter the content of or impose a time delay or denial in the communication of these control/measurement signals by exploiting weaknesses along the communication channels [27]. In this case, the sensor measurements utilized as an input to the control or protection algorithm will differ from the actual condition by $f1.y(t - d1)$. Similarly, the control or protection decision output from the control or protection system will be deviated from the correct one by $f2.u(t - d2)$. As these attacks can potentially seriously compromise the security and dependability of the power system, it is crucial to research and understand their effects. These effects can be quantified in terms of load loss, frequency and voltage violations, and their subsequent effects. Attack studies will also aid the development of defenses against attacks or ways to lessen their effects. Algorithms for attack-resistant control and bad data detection are examples of countermeasures [28].

### *3.2. Testing Methods of Cyber-Attacks*

The smart grid needs to be cyber-physically analyzed; hence, it is important to establish adequate modeling and simulation approaches for the different domains in the smart grid. These domains, which have traditionally been the focus of power system modeling, can be modeled and simulated using various techniques. Three basic types of experimental settings exist simulations, data from real-world systems (such as data obtained from a power company), and real-world testbeds, which are real-world systems used just for testing and not for actual use. Each of them has benefits as well as disadvantages. For instance, using simulations makes it feasible to examine the effects of attacks without posing any safety risks, but doing so ignores many of the issues that real-world practitioners face. Deploying attacks in a testbed, however, offers a more realistic investigation of the system's weaknesses but also carries the danger of causing costly equipment damage or even personal injury. However, deploying attacks in a testbed allows for a more realistic investigation of the system's vulnerabilities, but it also entails the risk of expensive equipment damage or even personal injury.

Based on the modeling technique used, the attack can be simulated, emulated, or even a real agent as shown in Figure 5a. Simulation is a powerful means of studying networking problems because it gives the flexibility to model a wide range of scenarios, has a low usage and deployment cost, and provides reproducible experimentation. A single simulator can be used to represent and simulate the power networks in these scenarios such as Matlab, DIgSILENT, PSSE, etc., representing the communication infrastructure as directly connected links. In this scenario, the attacker will be modeled and simulated as a manipulation block with a generalized function to modify the targeted signal for the attack as shown in the left block in Figure 5a. This type of simulation has been improved recently by using the same software to simulate both the power and communication networks. Power System Computer Aided Design (PSCAD), for instance, is a tool for power system simulation that can be utilized for cyber-physical simulation with the introduction of communication network components, as detailed in [29]. Applications might be testable but not actual devices because they are often built utilizing software packages. In addition, these models must undergo extensive testing and validation. It is a more practical and feasible solution to maintain the simulation of power and communication systems in separate simulators and integrate them through a common framework to function together as a co-simulation system [30]. The necessary data flow interface and time synchronization of the two simulators are realized using the shared framework. The key benefit is that a cyber-physical simulation environment may be created using industrial-grade commercial devices and tools. By emulating the attacker model through the communication network, this attack emulation may be made to look realistic as shown in the right block in Figure 5a. On the other hand, as shown in the middle of Figure 5a, real attackers can be settled at the testbed to launch attacks targeting the protection or control agents in the physical testbed through a PC connected to the Ethernet network, which means testing with a high-fidelity model and demonstration with accurate results.




(**a**) (**b**)

**Figure 5.** Testing of cyber-attacks on power systems: (**a**) methods of testing; (**b**) degrees of testing methods in terms of reality, flexibility, and complexity.

Figure 5b depicts the key differences in testing methods in terms of the number of scenarios that can be conducted, considering flexibility, complexity, and how close they are to reality. In this work, we focus on the cyber-attacks targeting the protection and automation system of the power grid, especially cyber-attacks at digital substations using the physical testbed. In addition, the co-simulation testbed will be used to virtualize the cyber-attacks associated with the distributed control scheme. Therefore, real attackers/agents will be used with the physical testbed with detailed descriptions and studies in Sections 4 and 5, while Sections 6 and 7 include the implementations of attack emulators in the co-simulation testbed with different scenarios.

## 4. Cyber-Physical Substation

The substation is a crucial part of the power grid, which plays a critical role in connecting power generation sources into the grid and transmitting energy to the end-user. Substation measurements are utilized as input to various physical and cyber devices that can be physically or electrically coupled for monitoring, protection, and control applications. The transformation of the power system to a smart grid is being driven by automation of the power system and communication standards. One such standard that is an extensively used standard for substation automation and protection is IEC 61850. It permits crucial substation automation and protection components in digital substations to communicate and exchange data in real time. However, the Sampled Values (SV) and Generic Object-Oriented Substation Event (GOOSE) protocols of IEC 61850 may be vulnerable to cyber-attacks. The standard does not implement any encryption due to complex real-time requirements of trip signals for protection systems, typically in the range of 3–4 ms. The exploit of GOOSE protocol vulnerabilities within IEC 61850 is demonstrated in [31,32].

Figure 6 depicts the testbed's fundamental four-tier architecture. Four levels make up this system [1]: the process layer, the bay layer, the substation layer, and the network layer. The process layer comprises components such as circuit breakers, circuit transformers, voltage transformers, current transformers, actuators, sensors, and main and secondary switchgear. The use of input/output terminal equipment decreases the amount of hard-wiring in the process. Station-level Ethernet switches connect IEDs in the bay layer for control and protection. The IEDs carry out operations such as bay control, protection, monitoring, and fault recording upon receiving communication commands from the station level. The station layer contains modems, Ethernet switches, HMI computers, and global positioning system (GPS) receivers. It is used for data storage, automation, archiving, and bay-level management. The network layer mainly allows remote access exchange of information and control. The substation and network layers are the main sources of cyber-attacks through the substation's insider or remote access. Blackouts may result from

several cascading events by simultaneous cyber-attacks on crucial substations. Therefore, to increase the resilience of power grids, it is essential to improve the cybersecurity of substations and assess both physical and cybersecurity as one integrated structure.

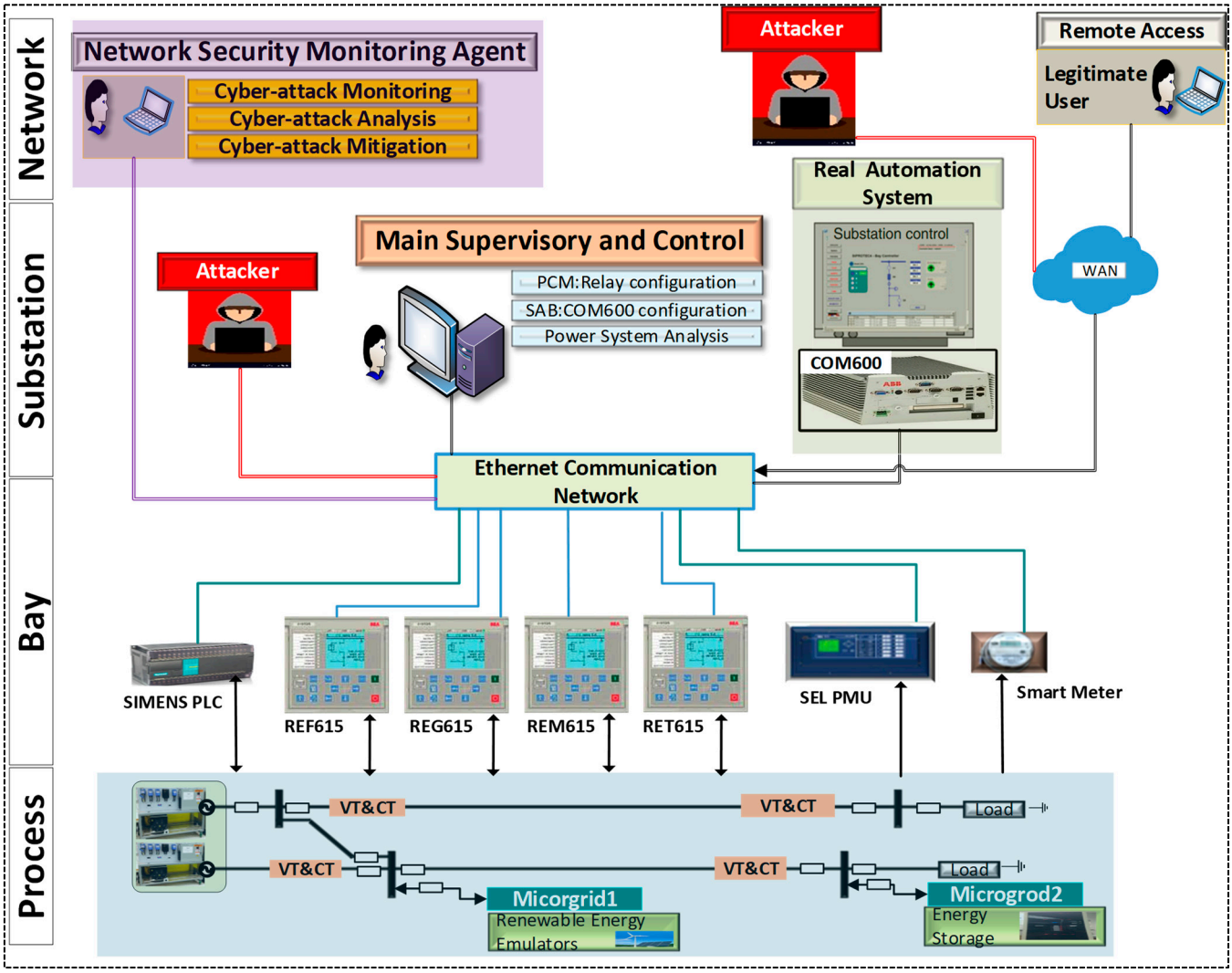



**Figure 6.** Cyber-physical substation layers.

### *4.1. Cyber Intrusions in Protective Relays*

Digital substation protection systems are vulnerable to cyber-attacks that could disconnect lines and generation, leading to cascading failures in the power grid. Protective relays were initially electro-mechanical switches, but as they developed into sophisticated networked digital devices with enormous processing power, they became intelligent electronic devices (IEDs). As a result, both IT network and control system vulnerabilities are making IEDs cyber-vulnerable. Not every IED is critical, but some must be protected.

According to the attack tree in [12], opening CB as the attacker's primary goal may be achieved due to four malicious actions that can originate from different points, either by the station's insiders or remote access. However, some attackers may want to leave the CB closed to activate other relays to trip their associated CBs, negatively impacting the protection system operation and consequently resulting in service disruptions. Suppose the attackers have gained access to the station communication bus through the internal communication network or remote access from an external network. In that case, they might jeopardize the communication protocols and the station's hardware (protective relays or user interfaces). For instance, they might open circuit breakers using malicious commands or control. Another possible attack scenario is to modify the protective relay's settings

so that the relay trips during normal operation or mal-operates due to miss-coordination, which could lead to a cascading issue. As shown in Figure 7, according to the attacker's goals, the protective relay under attack may send an unnecessary trip signal or not a necessary trip signal to the associated CB, causing inappropriate operation of the protection system. During normal operation (no-fault), the unnecessary trip signal from the primary protection, which may result from direct malicious command or changing the relay setting, will impact the system operation by service interruption and may lead to cascading failures. During the abnormal operation (fault condition), the prevented necessary trip signal from the primary protection, which may result from a DoS attack or relay setting altering, will impact the system operation by expanding the service interruption area, consequently leading to cascading failures. These severe consequences are mainly due to several trips through activating the backup protection system or the miss-coordination resulting from the attack.

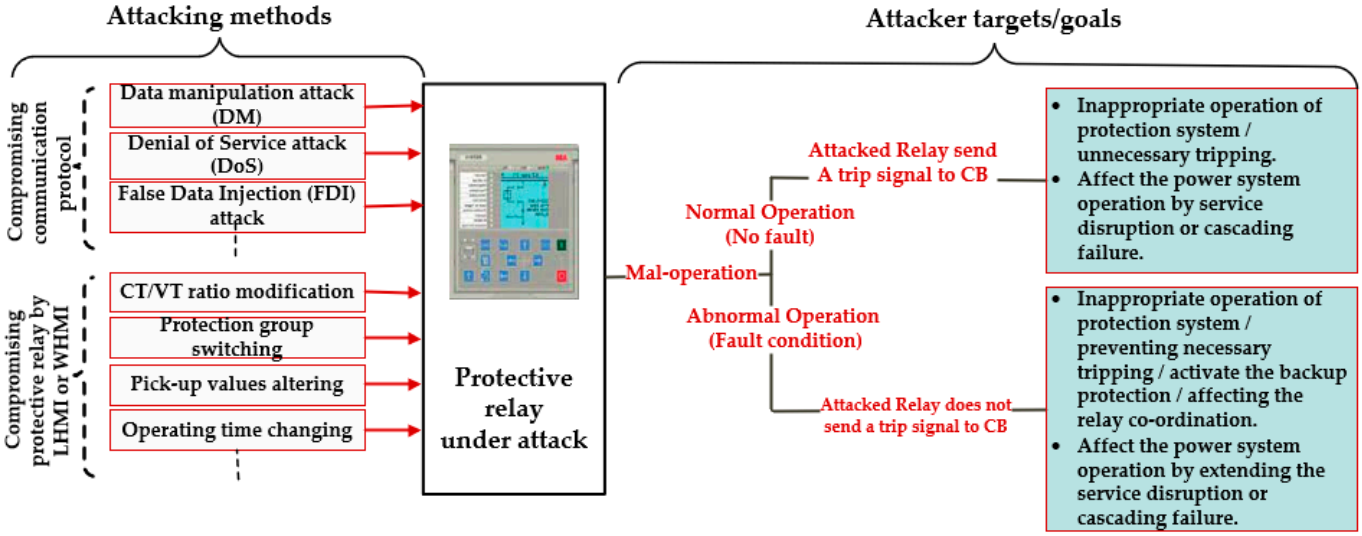



**Figure 7.** Attacker targets and attacking methods in protective relays.

### *4.2. Digital Relay Configuration and Data Model*

The digital overcurrent relay, which is the major target of cyber-attacks in this work, is explained in this section along with a set of protective configurations. It is a potential target for several types of cyber-attacks, such as DoS, message suppression (MS), replay, man-in-the-middle, false data injection (FDI), data manipulation (DM), etc. Figure 8a depicts a simplified schematic diagram according to the IEC61850 definition of the digital overcurrent relay. A source of continuous measurement of current is each set of current signals at each node, which are derived from the current transformer (CT), which can be acquired as follows:

$$I^{meas} = [I_{R1}, I_{R2}, I_{R3}, I_{R4}, \ldots I_{Rn}] \quad (1)$$

where $I^{meas}$ is the measured three-phase analog current signals from CTs, and $I_{R1} : I_{Rn}$ are the currents for Relay-1 through Relay-n. The relay protection block compares the measured values with the threshold or pickup values after receiving the values of the processed current signals from the CT measurements. Carefully choosing the pickup value requires considering the protection relay's operation's minimum fault current and maximum allowable load current. The typical relay pickup current ($I^{pu}$) can be represented as [33] and typically falls between the system's maximum load currents and minimum fault currents. The Protection and Control IED Manager PCM600 makes it easy to configure these relays, and the application configuration tool allows one to design, choose, and configure the necessary functionalities. Device configuration data are contained in the XML-based Substation Configuration Language (SCL) as a common language to achieve device interoperability. The configured SCL file is imported by IEC 61850-based devices

over the ICT network, negating the requirement for human configuration. Multi-vendor interoperability is improved through standardized communication protocols and logical nodes. According to the standard, as shown in Figure 8a, the hierarchical model of the physical devices is composed of five layers, starting from the physical device (PD) layer to the data attribute (DA) layer [34]. According to IEC 61850-7-4, each PD in this data model has a group of logical devices (LDs), and each LD has several logical nodes (LNs) that define specific power system functions. All LNs have a class name consisting of four letters, the first of which denotes a group of LNs. Additionally, groups of data objects (DOs) are assembled into the LNs to gather data values, control outputs, and parameters. Figure 8b shows that the relays were configured and programmed using PCM600 2.10 32bit, with different IP addresses and technical keys.

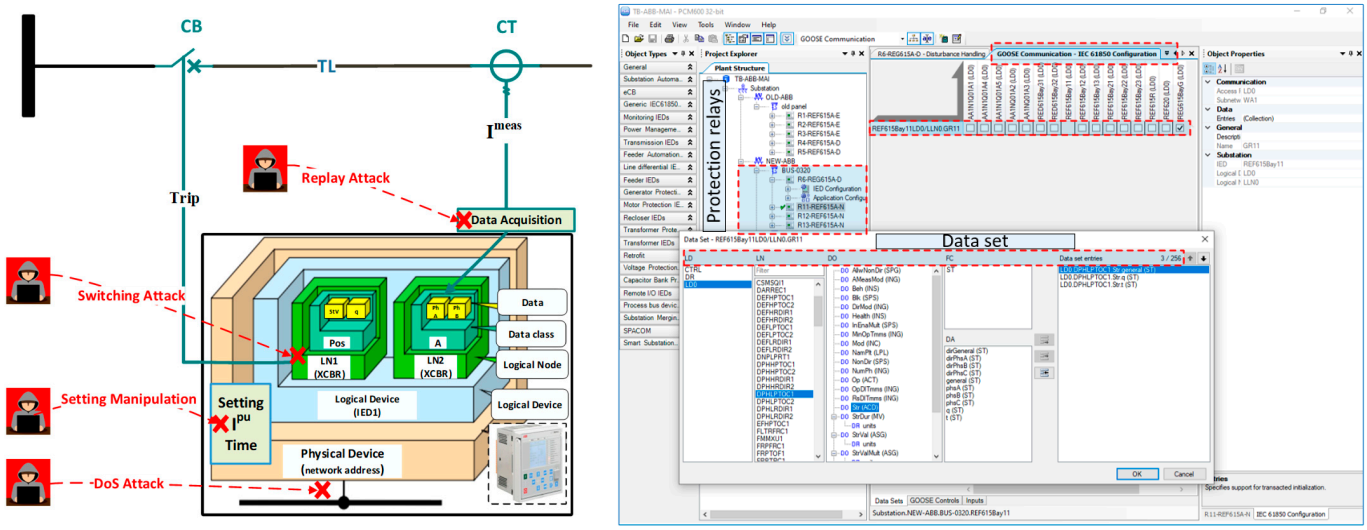



**Figure 8.** Protection relay data model and configuration: (**a**) digital relay schematic diagram with the data model; (**b**) relay configuration using PCM.

### *4.3. IEC 61850 Cybersecurity Threats*

Cybersecurity is a major concern with the growing integration of communication technologies aimed at enhancing the performance of protection systems. Within this framework, three fundamental security objectives focus on confidentiality, integrity, and availability. Communication systems must fulfill these three security objectives. Despite the protective measures introduced by IEC 62351 [35] to secure IEC 61850 against certain types of attacks, the IEC 61850 communication standard remains susceptible to a range of potential threats. Consequently, it is essential to identify potential attacks that may target protection systems and assess their potential impact. The origin of attacks on protection systems can vary from low- to high-skilled attackers. Skilled intruders may cause big damage to the utility because they may have good knowledge of the standard and the message content. Therefore, they may cause undesirable tripping even before the intrusion is detected. In this paper, we will test and assess the impact of a DM attack (switching attack) on the relay, causing the targeted relay to subscribe to the malicious GOOSE message and opening its associated circuit breaker.

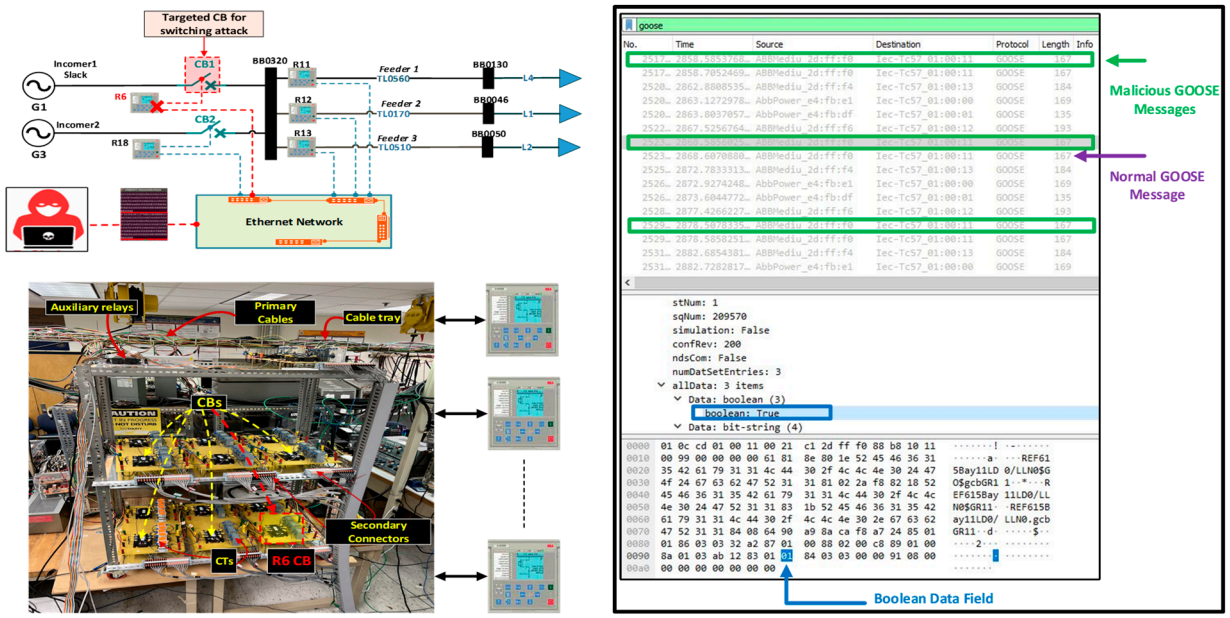
## 5. Physical Testbed Attack Scenarios

Users can research plausible scenarios of cyber-attacks and defense techniques using a real-time cyber-physical testbed. This section will address situations that could occur, such as potential entry points to the substation systems and substation-compromising cyber-attacks by analyzing two different attacks. It is assumed that the attacker has gained

access to the network data and IEDs by breaching the private network to emulate the attack in the testbed.

### *5.1. Switching Attack Scenario*

The set-up consists of five IEDs as shown in Figure 9a: two for incomers (generators G1 and G3) and three for outgoing feeders. Communication between these IEDs and the substation control system is through the IEC 61850 GOOSE protocol. In this scenario, the attacker is represented by an agent (PC) connected to the local network, as shown in the figure. Suppose this intruder can successfully spoof a GOOSE message frame. In that case, it can increment the stNum, reset the sqNum, alter the Boolean data field, and then multicast the malicious message to subscribing IEDs. If the receiving IED accepts the manipulated GOOSE message, they will initiate the opening of the circuit breaker. The circuit breaker emulation was implemented with the help of the I/Os on the IEDs and enables a realistic emulation of the switching process.




(**a**) (**b**)

**Figure 9.** Switching attack scenario: (**a**) power system and relay connections; (**b**) switching attack technique.

#### 5.1.1. Attack Model

Goose messages are designed for fast communication, adhering to a 4 ms transmission time specified by the IEC 61850 standard, where it does not employ encryption algorithms. Consequently, an eavesdropper with access to the network can intercept these unsecured GOOSE packets and efficiently collect the plaintext information. A familiar intruder with the message's content can manipulate the data field effectively. The attacker is implemented on a desktop computer that hosts Ubuntu 16.04.7 LTS on it and has 8 GB of RAM and 4 CPU cores. Based on the relay data model described in Section 5.2, each data name is specified by the standard and functionally correlates to a particular power system component. The LN with the name XCBR is used to mimic a circuit breaker with various data elements including, for example, *Pos*, which contains two attributes: *ctlVal*, which represents the opening and closing command, and *stVal*, which identifies the position. In the scenario we assessed, the intruder changed the Boolean data field of *ctlVal* from false to true, resulting in the tripping of the circuit breaker. In our adversarial model, we assume the attacker can intercept network traffic, extract essential fields from GOOSE messages, and execute a multicast attack by setting the Boolean data field to true, initiating the corresponding IED circuit breaker opening, as shown in Figure 9b.

5.1.2. Testing Scenario

During normal operation, the two generators supply the three loads, as shown in the first portion of Figure 10. The first incomer is slack, while the second generator is controlled with a specific input torque, which means G3 can supply a limited power at a certain frequency. Accordingly, if the load demand increases or the power output from G3 decreases, G1 will provide the increased power. When R6 attacked and opened the associated CB1, the system lost power coming from the main source; this led to an increase in the requested power from G3 and islanded G1 with zero load. In this case, the scenario was performed with no additional protection functions such as frequency protection to effectively demonstrate the impact of such attacks on power system operation. A significant overload may result from generators exceeding the allowed power limit due to a general rise in power. As shown in the figure, the power generated from G3 is increasing divergently with a severe drop in the frequency, which may result in catastrophic damage to the generator. In this scenario, G3 will provide the power demand with a very low frequency, as shown in the figure, which may also affect the connected loads. The frequency protection function must be activated with proper under-frequency settings to trip the CB if the frequency is below the threshold ($\cong$ 59.7 Hz). When the attacker opens R6 CB, the relay R18 connected to G2 will pick up as under frequency and, accordingly, send a trip signal to CB2. No power source will feed the three loads connected to the load buses. As a result of these attacks, a severe impact can be observed either through the operation under low frequency or with the blackout when the whole loads served by this substation lose supply. By increasing the grid connection, cascaded outages are expected.

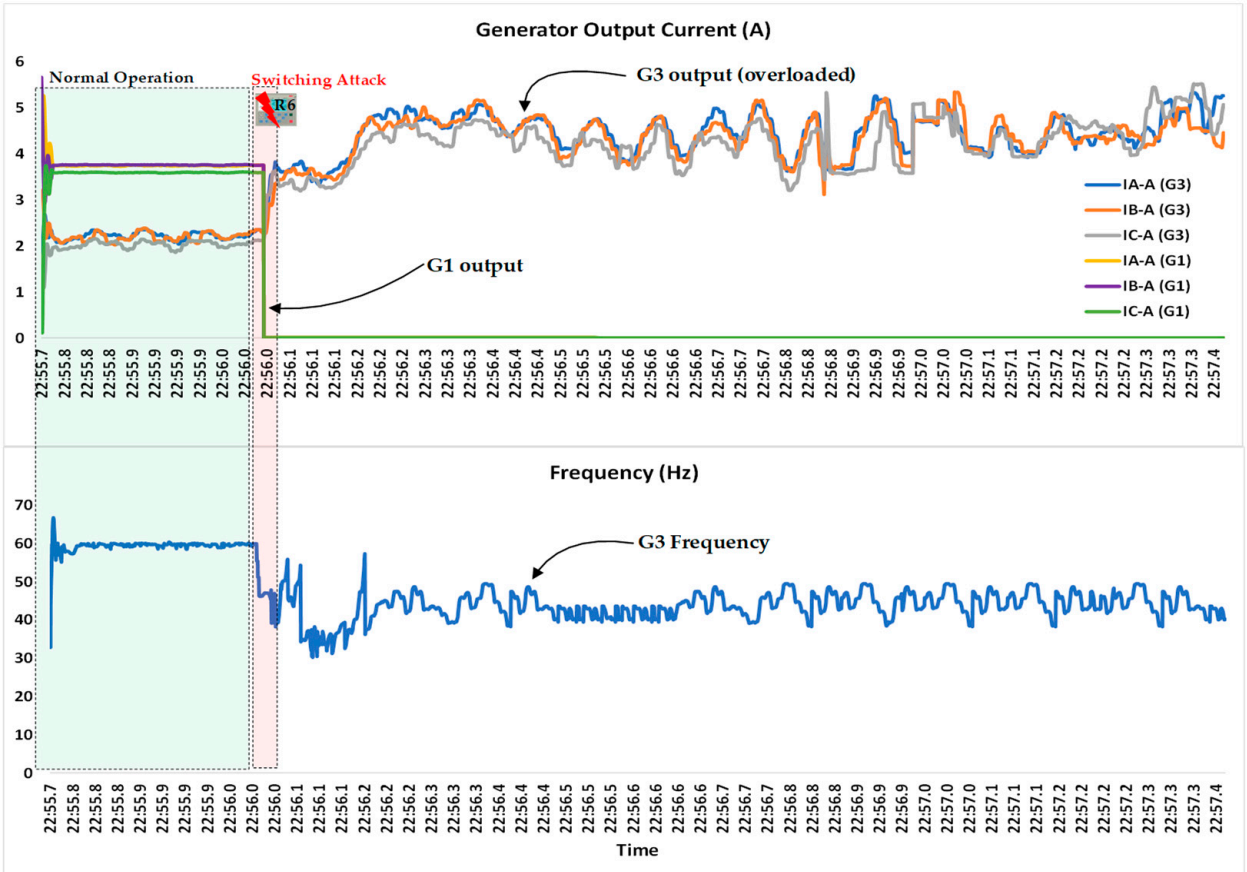



**Figure 10.** Switching attack results.

### *5.2. Relay Setting Tampering (Change) Attack Scenario*

The protection system aims to compute the system state, measure signals such as voltages, currents, and frequencies using sensors, and take corrective action if any deviation from normal operation is identified based on appropriate configurations and settings. The faulted area can be isolated by switching actions when a fault occurs at any component inside the substation after picking up a certain time. The relay can be accessed and configured using PCM600, LHMI, or WHMI. The substation's communication protocol does not affect communication between the IED and PCM600 or WHMI. It might be seen as an additional communication channel using Ethernet and TCP/IP protocol. The attack on the protection scheme prevents us from achieving this goal. One of the most frequent attacks in protection relays is the setting tampering (setting change) attack; the attacker may maliciously change the relay configurations or setting functions, preventing the relay operation during a fault or forcing the relay to operate normally. In this scenario, these attackers could severely impact the security and stability of the power system and the communication between protective equipment. Therefore, studying the impacts of such types of attacks on the protection system is crucial.

#### 5.2.1. Relay Configuration and Attack Model

This section focuses mostly on cyber-attacks against digital overcurrent relays. In overcurrent protection, the protection relays first receive the current measured by the current transformers, subsequently comparing it with the preset threshold values. Relays trip under fault current, changing their output from an open contact to a closed state to clear the fault after a certain time based on the selected overcurrent characteristics. Time overcurrent (TOC) or inverse time over current denotes that the relay's trip time is inversely proportional to the applied fault current. Modern digital relays are programmable; thus, curve shapes can easily be changed without needing replacement. Nearly any mix of definite-time, inverse-time, and instantaneous elements can be applied. In general, the trip time for each standardized relay protection curve will be determined using the IEC 60255 or IEEE C37.112 [36] formulas as in (2),

$$t(I^{meas}) = TD * (\frac{K}{P^x - 1} + C) \tag{2}$$

where $t$ is the relay trip time, $TD$ is the time dial setting, $P$ is the ratio of measuring current or fault current to pick up current ($I^{meas}/I^{pu}$), and $K$, $C$, and $x$ are constants depending on the curve types. In this work, IEC standard inverse curves were selected such that $C = 0$, $k = 0.14$, and $x = 0.02$. Typically, a certain principle guides the selection of decision thresholds or pickup values, which are represented by (3) between the maximum load current of that feeder and the system's minimum short-circuit fault current.

$$I_{\max-load} \leq I_{pu} \leq I_{min-fault} \tag{3}$$

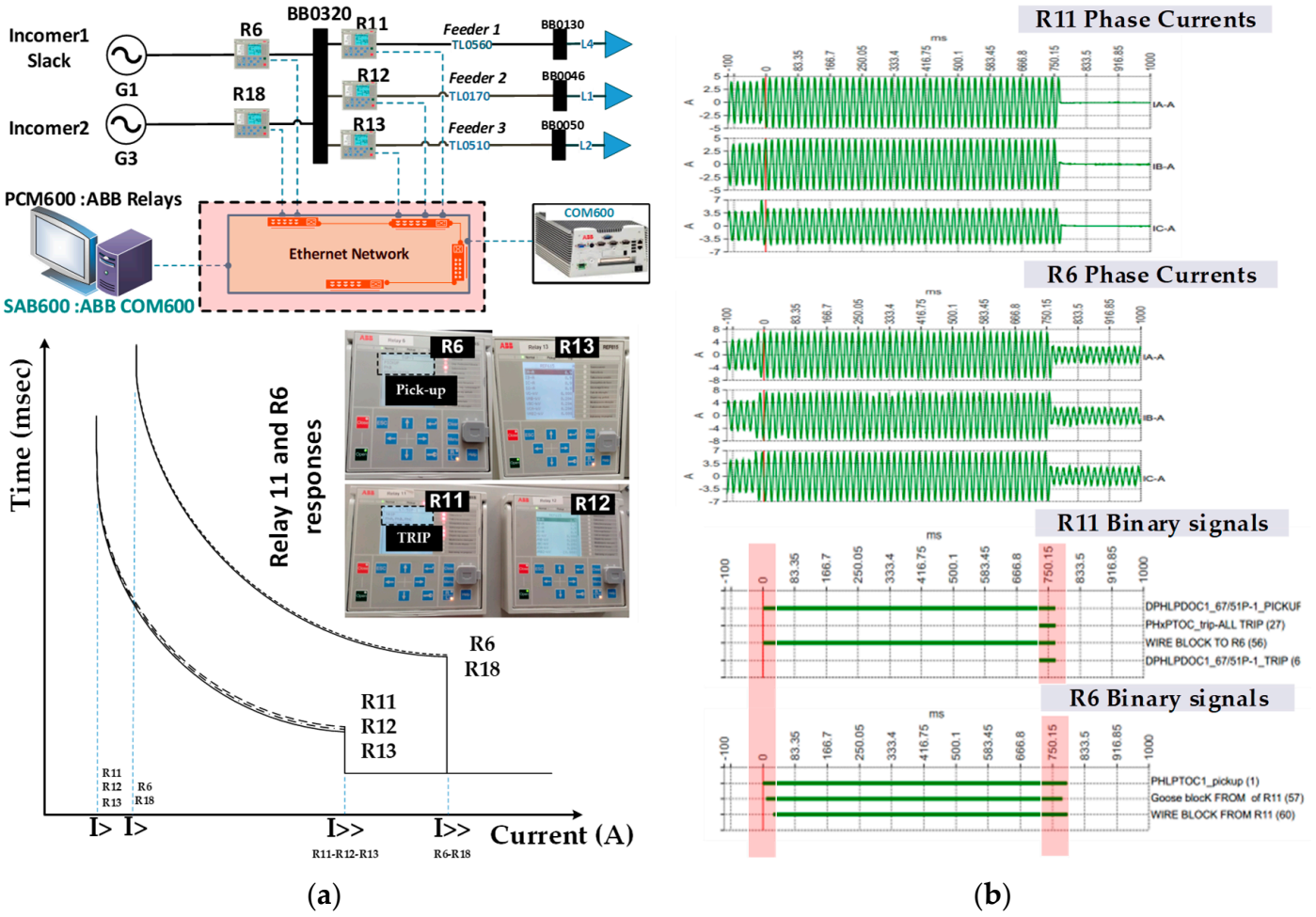
However, in this work, some assumptions were considered due to the practical component limitations and avoiding harmful actions in testing fault scenarios. Therefore, the $I_{pu}$ was selected only depending on the maximum loading conditions. Hence, pick up current settings for R11, R12, and R13 should be above their associated feeder load currents. The standards state that the threshold value set should be twice (or equal to 200%) the nominal current flowing through lines TL0560, TL0170, and TL0510 for proper detection. IED settings are calculated for various operation conditions in advance and assigned to various configuration groups. The IED application or a manual menu selection can be used to alter the active configuration group. In addition to giving read/write access to executable files that perform monitoring, configuration, and essential operating tasks, reading configuration files reveals which services are currently active. The researchers claim that an attacker can take advantage of the flaw to access private data, including usernames and passwords, which they can then use to take complete control of the intended device.

To establish a WHMI connection to the protection relay, after opening the explorer, the protection relay's IP address must be typed in the address bar, and then the username and password must be typed. The IED settings can now be changed maliciously because the attacker has access to them. The attacker reconfigured the IED to operate under high-load conditions or fail to sense the fault currents, especially low fault currents. Therefore, under normal circumstances, feeder relays are anticipated to trip the respective breakers when a fault occurs in their lines. But if even one of these breakers or relays malfunctions due to a physical or digital abnormality, this leads to incorrect operation of the protection system.

#### 5.2.2. Testing Scenario

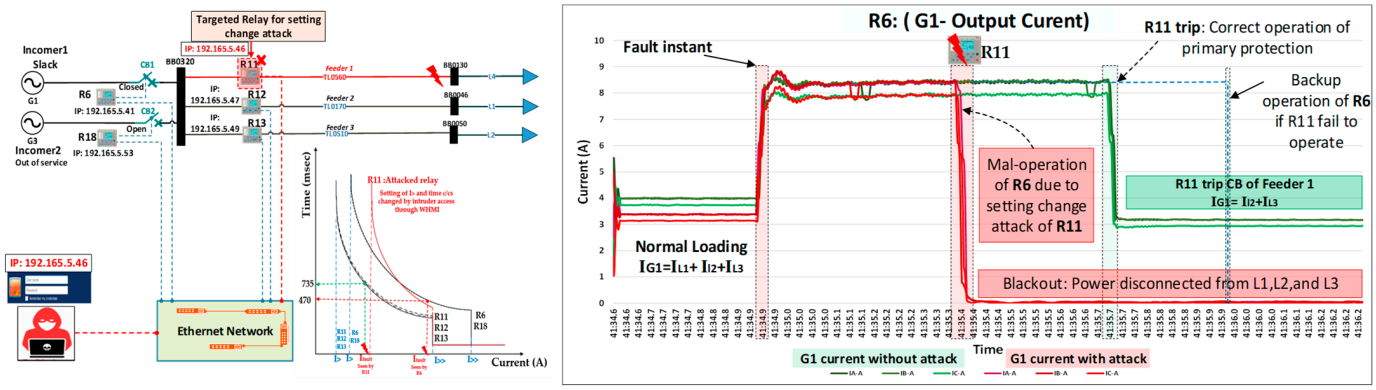
The cyber-physical system comprises a reduced-scale power system, a communication network, and IEDs. The physical ABB relays were connected through an Ethernet communication network. The relays used in this section are the REF615 for feeder protection and REG615 for generator protection. In this work, both relays (IEDs) offer a protection unit PTOC with "time over-current" as its primary protection feature. Each relay is configured with two OC stages: stage I> is a standard inverse, and stage I >> is definite time as shown in Figure 11a. In normal operation, with the proper setting configuration of the five relays in either low- or high-loading conditions, physical faults will lead to normal protection system operation. When a fault occurs on a transmission line, the feeder relays R11, R12, and R13 trip, open the breakers, and send a GOOSE block to the generators' relays R6 and R18 to prevent a false operation in the unlikely event that one of them is detected as a second stage I >> [37]. However, we assumed low loading conditions such that G3 is out of service and only G1 supplies the total power to the loads L1, L2, and L3. By abruptly raising the load L1, an imitation of the three-phase fault on feeder TL0560 is applied. The stage PTOC.str picked up right away according to the setting of R11 $I \geq 3.8$ A with an approximate time delay of 735 msec, according to the selected inverse characteristic. In addition, R6 was picked up as a first stage $I \geq 7.5$ A; however, it was not trip due to the relay coordination scheme. In the case of high-fault conditions, R6 may have been picked up as a second stage I >> and trip before R11, and therefore, a GOOSE message was transmitted instructing the incomer relay R6 to stop stage I >> operation. R11 issued a trip order to the circuit breaker at a time delay of 735 msec, and the breaker was opened at 750 msec. As a result, the current through R11 decreased to zero, while the incoming current from G1 decreased to about 3.5 A to feed the other loads L2 and L3 through the healthy feeders. Individual disturbance recordings must be uploaded from the IED using PCM600 to monitor the recorded data as shown in Figure 11b. All disturbance recordings can be found in the C:\COMTRADE directory.

On the other hand, the protective mechanism was not functioning correctly due to the setting tampering (change) attack R11. A setting change attack was carried out on the suggested protective method using almost identical loading conditions and fault scenarios. Relay R11 was maliciously altered, as shown in Figure 12a, putting the protective relay's coordination and the protection system's dependability at risk. With the manipulation in the threshold values of the relays by the attacker through moving the threshold values upward, the relay will probably not detect the short-circuit fault, and the circuit breaker will not work under this abnormal condition or isolate the faulted line. Under the same fault conditions, the overcurrent relay R11 cannot detect the fault current caused by the fault, while stage I> of R6 was picked up almost simultaneously. In this case, the I> stage of R6 as a backup protection for R11 was activated, and the relay issued a trip signal to the linked CB after the calculated time on the relay characteristic, which is indicated by the red lines as shown in Figure 12b. Consequently, all the generator's power was lost on busbar BB0320, which rendered the remaining loads connected to the functional feeders unusable.




(**a**) (**b**)

**Figure 11.** Normal protection system operation: (**a**) power system and relay setting configuration; (**b**) disturbance recorders of relays' analog and binary signals.




(**a**) (**b**)

**Figure 12.** Protection system response under setting change attack: (**a**) relay coordination is altered by attacker; (**b**) generator current without/with attack.

A power protection system's reliability is a measure of the extent of certitude that it will work as intended and is made up of two components: dependability and security. Dependability is a measure of the degree of certainty that a protective system will function successfully when required and at the intended speed when the fault is in the protected zone. Security is a measure of the degree of assurance that the protection system will

not act erroneously or quicker than intended when the fault is outside the protective zone. The correction operation of the protection system is operated correctly since R6 acted as a backup protection for R11. However, from the perspective of power system protection dependability, the system is unreliable because the primary protection (R11) did not operate correctly, which means the system is undependable, and R6 issued a trip signal to the associated CB, which means the system is insecure. From the reliability of the power system point of view, the loads connected to the healthy feeders lost power, and consequently, this was a complete blackout. Figure 12b shows the G6 current output in both cases, with green lines without attack and red lines if R11 is under attack. Conversely, if the threshold values are lowered because of the attack, any rise in the system load could potentially be regarded as a fault, and the relay will transmit the trip command under normal operation.

## 6. Cyber-Physical Co-Simulation Testbed Implementation and Set-up

### *6.1. System Overview*

Despite the higher degree of reality introduced by the physical testbed in terms of testing and analysis of cyber-attack impacts on power system controls and protection, there is a lack of flexibility in conducting different attack scenarios and power system topologies. Therefore, building a real-time cyber-physical co-simulation testbed is crucial. The cyber-physical co-simulation system simulates the three domains of real-time power system operation, with information flowing continuously across a simulated communication network utilizing the ns3 tool between the power system domain and the control and energy management domain. The experimental platform was created to more broadly assess how the communications network and controls perform when used for grid control and protection applications. Any additional controllable device—a "smart grid device"—can be integrated into this platform in the future with only modest set-up adjustments. Figure 13 illustrates the implementation and construction of a comprehensive three-domain modeling and simulation cyber-physical power system on various machines. Machine 1 is the real-time power system simulator (OPAL-RT: OP4610XG), a compact mid-range simulator, while the third machine is used for implementing the power system control or protection scheme. Both machines are connected to machine 2 through the Ethernet network as shown on the right and left of the figure.

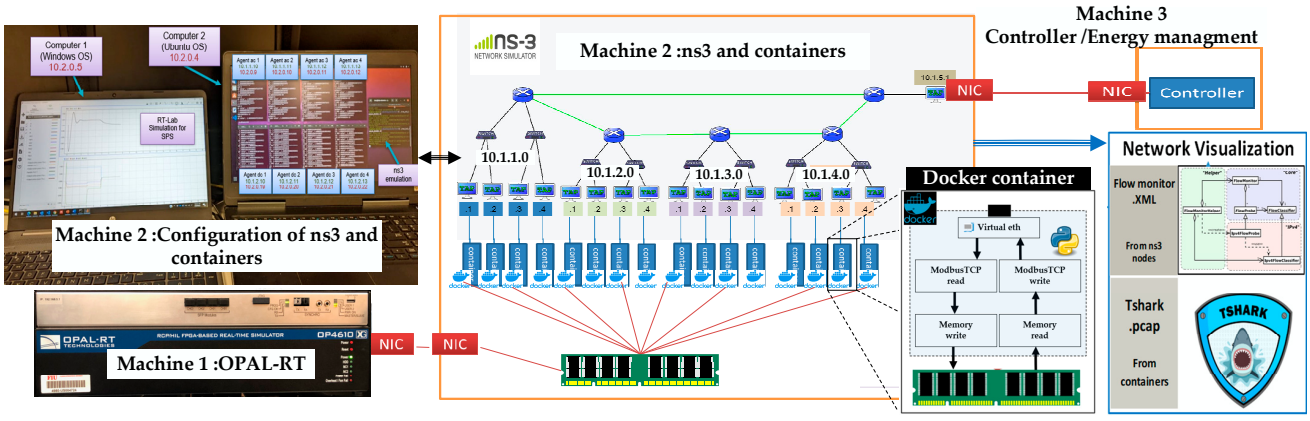



**Figure 13.** Cyber-physical co-simulation testbed.

### *6.2. Communication Network Emulation and Docker Containers*

Regarding the set-up of machine 2, which is the core element of this research work as an excellent environment for testing and emulating not only cyber-attacks but also different communication issues such as latency, packet loss, and losing network links, it is running with Linux OS to host two major parts of the communication network infrastructure as shown in the middle of the figure. The first part is ns-3 for communication network emulation. ns-3 is a free, extendable, advanced network simulation framework [38]. An

extensive library of network model protocols, including those for multicasting, IP-based applications (TCP, UDP), routing, and wireless and wired networks, is accessible on top of the ns-3 architecture. The ns-3 core, a time sync module, a simulated communication network, and a network application module are the four primary ns-3 components available in an ns-3 process to support all additional simulator aspects. The second part is docker containers that serve as intermediaries to convey data between the network nodes in ns-3 and the OPAL-RT simulation. These containers can be considered as local/primary controllers or agents that receive commands from a secondary/tertiary controller or as local sensors that transmit measurements. A docker is a software development tool and virtualization technology that makes it easier to develop, deploy, and manage programs utilizing containers [39]. A container is a small, independent executable software package that includes all the libraries, dependencies, configuration files, and other components required to run a program. Multiple containers can run concurrently on a single host since containers are secure due to their isolation. In this work, the docker containers are designed for interfacing between the ns-3 nodes and their corresponding device in the power system model, which runs in the OPAL-RT. Based on the structure of a container, as illustrated in Figure 14, agents within containers can connect with the power system modeled on OPAL-RT, and they can communicate with other containers using ns-3 by two virtual network interfaces: veth1 and veth2. veht1 is used to exchange data with other containers via ns-3 through Linux bridge and tapping device connection by the host operating system, while veth2 is used to send/receive measurements or control signals from/to OPAL-RT. In this work, the application inside the container is configured to act as an agent representing the sensor or controller. However, one of these containers or additional containers can be inserted into the network to behave like an attacker receiving information and sending it after some modifications.

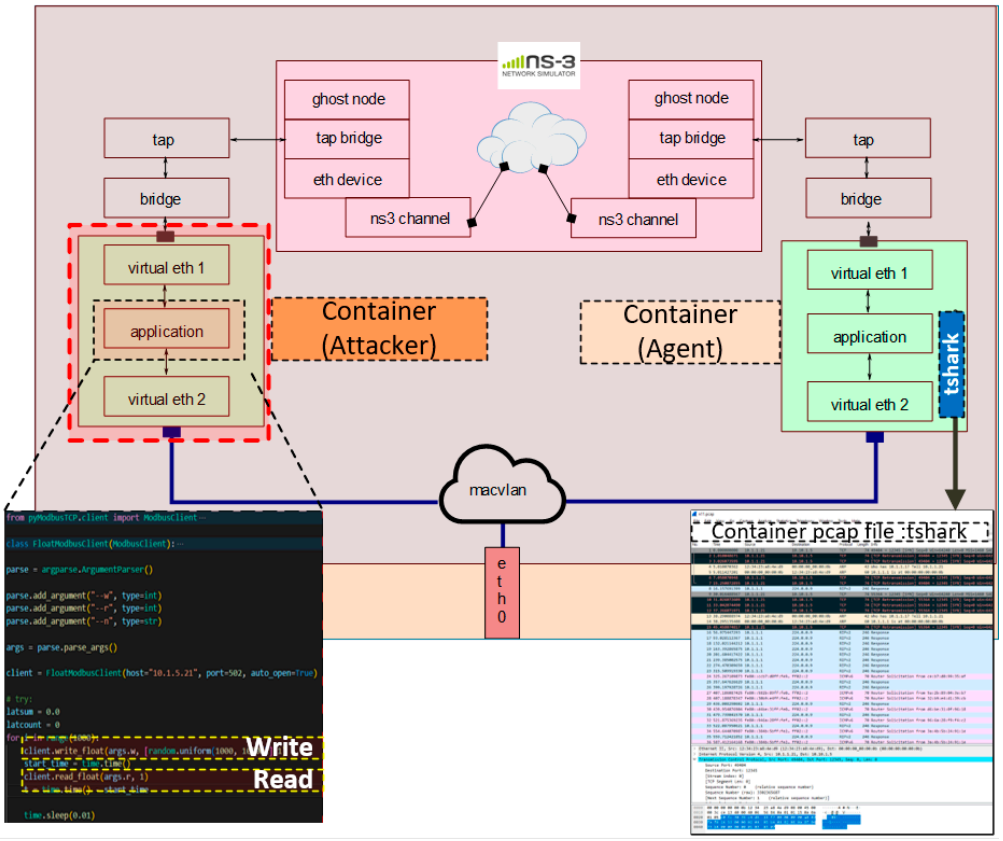
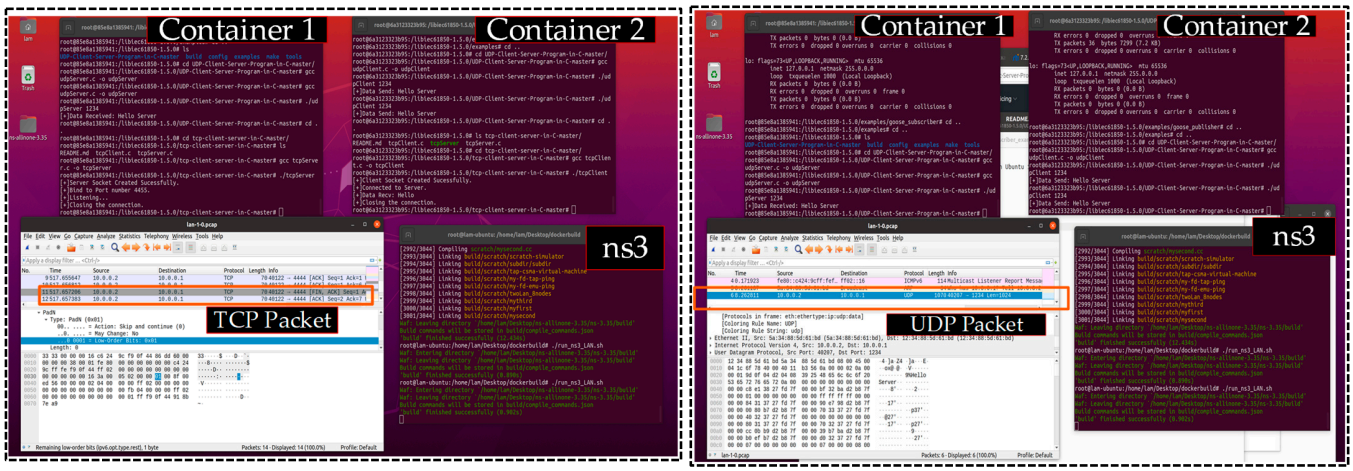



**Figure 14.** Container/ns-3 connectivity.

### *6.3. Network Performance Tests and Visualization*

The communication network is a crucial system for ensuring the dependability of control and protection applications, and its condition depends on where the application is applied. The network's behavior and performance can considerably impact the system's availability, stability, and performance as a whole. Communication network tests are necessary to reproduce and evaluate these impacts before implementation, including network performance and communication protocols. In [40], the network latencies are stochastically characterized by natural probabilistics to evaluate the network performance for the shipboard power system application. Different communication protocols may be utilized in power systems since the controllers/agents may be supplied by multiple vendors and employed for a variety of control/protection functions. With the proposed platform, the communication between agents in docker containers through ns-3 using different protocols such as UDP/IP, TCP/IP, DDS RTPS, and IEC61850 GOOSE was conducted by running applications in two different containers to send and receive messages. Testing of the communication using TCP/IP and UDP/IP by assigning one container as a server and the other as a client, with checking the results using the Wireshark is shown in Figure 15. In addition, to visualize, monitor, and analyze the communication network model, some additional tools have been installed recently in the second machine such as FlowMonitor and tshark. The FlowMonitor module is a core feature of ns-3 that facilitates the collection of a common set of network performance measurements of packet-related data, such as throughput, loss ratio, packet delay, bit rate, and round-trip time. It saves them to permanent storage in XML files describing the flow of information between all the system's nodes in ns-3. Moreover, to evaluate the communication system's performance in real time, a network packet analyzer tool (tshark) was installed in all the containers (nodes) in the system to capture and analyze network packets through the generated PCAP files as shown in Figure 14.




(**a**) (**b**)

**Figure 15.** Container-based testing protocols: (**a**) TCP protocol testing; (**b**) UDP protocol testing.

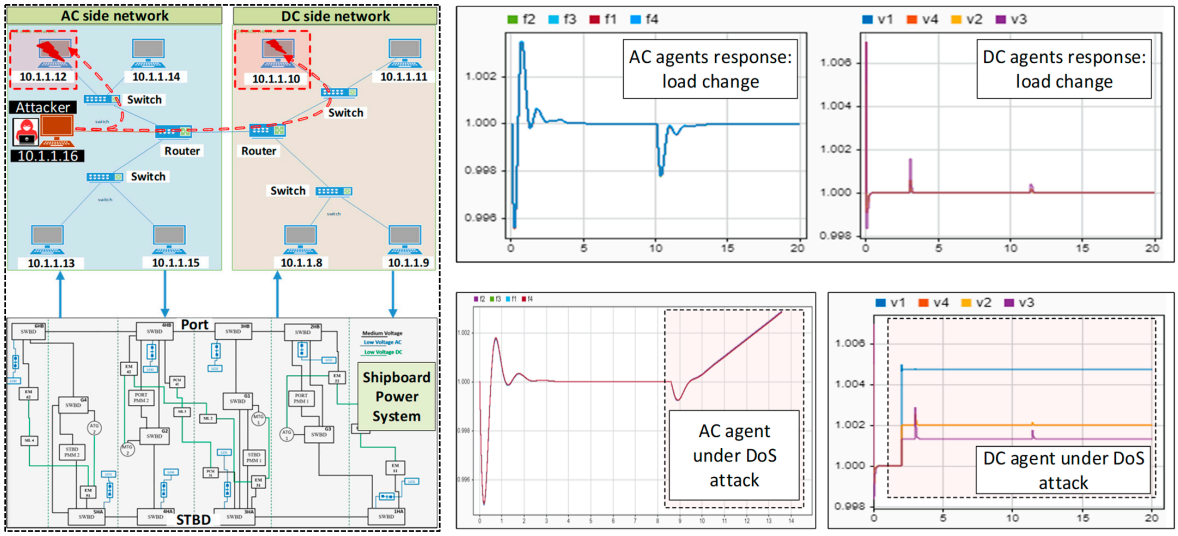
## 7. Co-Simulation Testbed Attack Scenarios

The objective of the test case in this section is to assess the control system's performance under cyber-attacks. Using the well-developed co-simulation testbed, potential cyber risks with proper attack models through emulation of their behaviors will be studied. This section will develop and discuss two types of attacks: DoS attack and MitM attack. By carrying out actions specifically designed to target the system under investigation and to power system protocols, the adversary can carry out DoS and MiTM attacks that have tangible consequences. The threat model we present and implement in this work is based on emulating the attacker behavior through ns-3 and docker containers; however, the

adversary is restricted by the available resources in the Linux containers in ns-3 and docker containers.

### *7.1. DoS Attack Scenario through ns-3*

This section evaluates the resilience of the MVAC/DC ship power system under DoS attack. To conduct the evaluation, the network emulator ns-3 is used to simulate the ship communication network in real time, as illustrated in Figure 16a. The considered network consists of two local networks corresponding to the system's AC and DC sides. Docker containers coexist with the ns-3 network emulation system on a Linux host computer and serve as interfaces between the power system simulation in Opal-RT and ns3. Specifically, each container links a device in Opal-RT to a network node in ns-3. The goal of the control system is to maintain stability in the ship power system under uncertainties in the overall system. It ensures that the voltage and frequency remain at their designated reference values. A distributed control strategy [41] is employed, where individual local controllers or agents are implemented within containers. These agents communicate with each other through the provided communication network. The proper functioning of the communication network is crucial for the system to operate effectively.




(**a**) (**b**)

**Figure 16.** System study under DoS attack: (**a**) SPS under study and agent's implementation in ns-3; (**b**) agent's response under normal operation, DoS attack of an AC agent, and DoS attack of a DC agent.

The investigation assumes that an attacker can gain access to communication. There are numerous techniques for launching denial of service (DoS) attacks, such as ping of death (PoD), Internet control message protocol (ICMP) flood, and user datagram protocol (UDP) flood. All DoS attack techniques aim to interfere with the targeted node's communication channels, even though they employ various Open Systems Interconnection (OSI) layers, including application, presentation, session, transport, network, data link, and even physical layer protocols [42]. In our threat model, an additional container is used to act as the attacker and is connected to the ns-3 network using open-source tools. In the test case, the attacker employs the hping3 tool to launch a DoS attack by flooding the target with traffic. This command-line tool generates DoS attacks that overload the network or the application layer, causing delayed message delivery. The flooding attack can take various forms depending on the network protocol used. While simple to perform, this type of attack can cause significant disturbances. The test results depicted in Figure 16b show that the cyber-attack affects the AC system when the attacker is attached to the AC local network. As a result, the target agent or controller becomes unavailable, rendering the

control system non-functional. The frequency of the AC system is no longer maintained at the reference value, and in the worst case, the system becomes unstable, resulting in a blackout event for the entire ship power system. Similarly, if the attacker is targeting a DC agent in the DC side network, this will impact the DC voltage, as shown in the figure, when compared to the normal operation without attack.

### *7.2. MitM Attack Scenario through ns-3*

In a similar approach, a MiTM attack is carried out using the co-simulation part of the platform, and Wireshark is used to observe the network flow to discover the attack behavior and impacts. A MiTM attack is a type of attack in which an intruder positions themselves between two communicating agents to intercept and/or alter data traveling between them. By embedding themselves within a conversation, the intruder can eavesdrop or impersonate one of the devices, allowing them to perform false data injection (FDI) and false command injection (FCI) attacks that can compromise power system operations. As shown in Figure 17, the additional container is used to simulate the intruder in the network. This container uses the Address Resolution Protocol (ARP) spoofing technique to link its MAC address with the IP address of the victim container. When a packet is sent from the source agent in the AC side network, it is routed through the MitM attacker before reaching the destination agent. The evidence of the MiTM attack is determined by analyzing the average round trip time (RTT), retransmission rate, and average processing time of packets. When a packet is sent, the sender starts a variable-length retransmission timer and waits for the acknowledgment. If no acknowledgment is received before the timer expires, the sender assumes the packet is lost and retransmits it. To detect if there is a MitM attack, the ping command can calculate round-trip times and packet loss statistics and display a summary on completion. As depicted in the upper right figure, the test results indicate that when the packet is sent through ns-3 via appropriate nodes, the recorded time is t = 1.28 ms, marked by the yellow dotted lines. However, when the MitM attacker captures the message to modify it, the recorded time increases to t = 2.29 ms (almost doubled). This significant discrepancy in the recorded time strongly suggests the presence of a MiTM attack, which can be used as an indicator to detect the presence of attackers in the system.

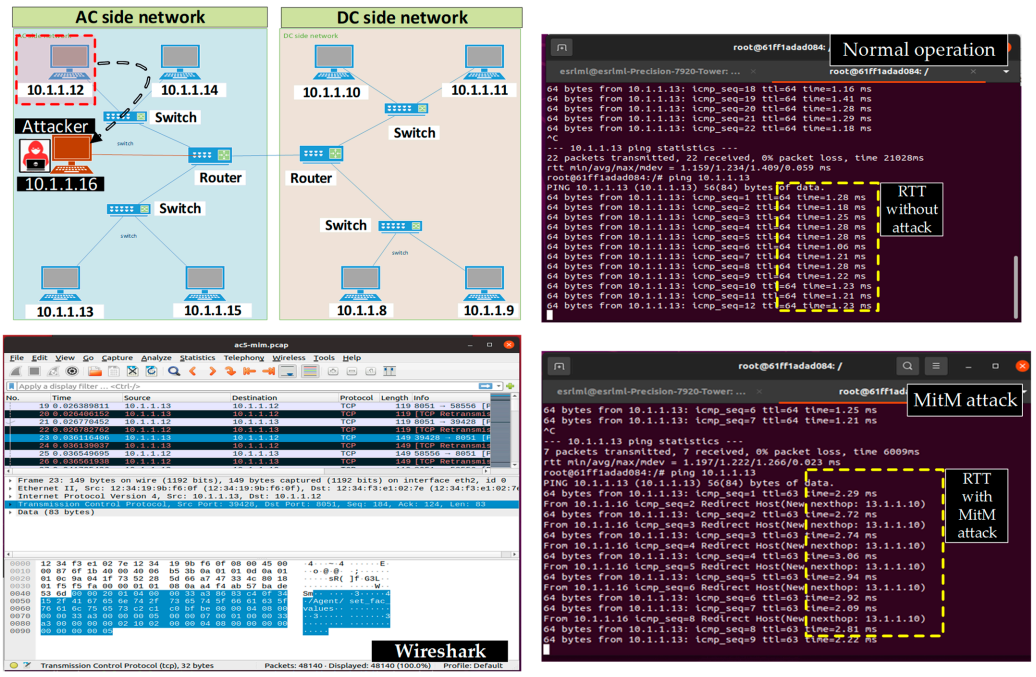



**Figure 17.** The effect of MitM attack on an AC agent in the ship power system.

## 8. Conclusions

The effective way to comprehend security threat events and their effects on the power grid is through cyber-physical testbeds, which can help facilitate grid resiliency to cyber threats. The FIU Hybrid SGTB offers a realistic testing environment with real power system components, controls, and protective software. While this offers the best testing conditions, many research projects find it impractical to test modern communication systems or large-scale power systems due to their complexity and flexibility. Integrating a co-simulation-based testbed to the physical testbed can make testing and validation more convenient and flexible, enabling the incorporation of both real and virtual components.

In this study, the Hybrid SGTB introduced a comprehensive framework for running and simulating various power system topologies' physical and cyber components by using components like industrial-grade devices, real-time simulators, and various automation tools for experiment orchestration, data collection, and visualization. The attack model, impact on system dynamics, and cascading failures are experimentally proven through a suggested cyber-physical experimental framework that closely replicates real-world conditions within a digital substation, including IEDs and protection measures. Various experimental scenarios were used to implement cases of data manipulation and setting change attacks by real agents (attackers) using the physical testbed. In addition, two emulated attacks on the shipboard power system model using the co-simulation testbed, MitM and DoS, were performed through virtual agents using the integration of ns-3 and docker containers. In the future, a network security monitoring agent as a vulnerability scanner component will be implemented in the physical testbed for monitoring, analysis, and intrusion detection. In addition, a real-time automation controller will be integrated into the co-simulation testbed for different control applications. Moreover, the communication network will be fully modeled using Exata CPS running on OPAL-RT to evolve testing attack scenarios and help implement intrusion detection techniques.

**Author Contributions:** Conceptualization, M.S.A., and O.A.M.; Methodology, M.S.A., and T.L.N.; Software, I.K., and T.L.N.; Validation, M.S.A., and T.L.N.; Formal analysis, M.S.A., and I.K.; Investigation, O.A.M.; Resources, O.A.M.; Writing—original draft, M.S.A., and I.K.; Writing—review & editing, T.L.N., and O.A.M.; Visualization, M.S.A., and I.K.; Supervision, O.A.M. All authors have read and agreed to the published version of the manuscript.

**Funding:** The work in this article was partially supported by grants from the Office of Naval Research, ESRDC, and the National Science Foundation.

**Data Availability Statement:** Data are contained within the article.

**Acknowledgments:** We acknowledge the collaborative discussions, equipment support, and software provided by ABB and Schweitzer Engineering Laboratories.

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

## References

1. Buchholz, B.M.; Styczynski, Z. *Smart Grids-Fundamentals and Technologies in Electricity Networks*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 225–275.
2. Krause, T.; Ernst, R.; Klaer, B.; Hacker, I.; Henze, M. Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors* **2021**, *21*, 6225. [CrossRef] [PubMed]
3. Whitehead, D.E.; Owens, K.; Gammel, D.; Smith, J. Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies. In Proceedings of the 2017 70th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA, 3–6 April 2017; pp. 1–8.
4. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Trans. Power Syst.* **2017**, *32*, 3317–3318. [CrossRef]
5. Ward, S.; O'Brien, J.; Beresh, B.; Benmouyal, G.; Holstein, D.; Tengdin, J.T.; Fodero, K.; Simon, M.; Carden, M.; Yalla, M.V.V.S.; et al. Cyber Security Issues for Protective Relays; C1 Working Group Members of Power System Relaying Committee. In Proceedings of the 2007 IEEE Power Engineering Society General Meeting, Tampa, FL, USA, 24–28 June 2007; pp. 1–8.
6. Tan, R.; Nguyen, H.H.; Foo, E.Y.; Yau, D.K.; Kalbarczyk, Z.; Iyer, R.K.; Gooi, H.B. Modeling and mitigating impact of false data injection attacks on automatic generation control. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1609–1624. [CrossRef]

7. Rahman, M.S.; Mahmud, M.A.; Oo, A.M.T.; Pota, H.R. Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems. *IEEE Trans. Ind. Inform.* **2017**, *13*, 436–447. [CrossRef]
8. Ameli, A. Application-Based Measures for Developing Cyber-Resilient Control and Protection Schemes in Power Networks. Ph.D. Thesis, UWSpace, Waterloo, ON, Canada, 2019.
9. Liu, S.; Mashayekh, S.; Kundur, D.; Zourntos, T.; Butler-Purry, K. A framework for modeling cyber-physical switching attacks in smart grid. *IEEE Trans. Emerg. Top. Comput.* **2013**, *1*, 273–285. [CrossRef]
10. Liu, X.; Shahidehpour, M.; Li, Z.; Liu, X.; Cao, Y.; Li, Z. Power system risk assessment in cyber-attacks considering the role of protection systems. *IEEE Trans. Smart Grid* **2017**, *8*, 572–580. [CrossRef]
11. Touhiduzzaman, M.; Hahn, A.; Srivastava, A. A diversity-based substation cyber defense strategy utilizing coloring games. *IEEE Trans. Smart Grid* **2018**, *10*, 5405–5415. [CrossRef]
12. Hong, J.; Nuqui, R.F.; Kondabathini, A.; Ishchenko, D.; Martin, A. Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations. *IEEE Trans. Ind. Inform.* **2018**, *15*, 4332–4341. [CrossRef]
13. Ani, U.D.; Watson, J.M.; Green, B.; Craggs, B.; Nurse, J. Design Considerations for Building Credible Security Testbeds; A Systematic Study of Industrial Control System Use Cases. *J. Cyber Secur. Technol.* **2021**, *5*, 71–119. [CrossRef]
14. Yang, Y.; Mclaughlin, K.; Littler, T.; Sezer, S.; Im, G.; Yao, Z.Q.; Pranggono, B.; Wang, H.F. Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in Smart Grid SCADA systems. In Proceedings of the International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012), Hangzhou, China, 8–9 September 2012; pp. 1–8.
15. Siaterlis, C.; Garcia, A.P.; Genge, B. On the use of Emulab testbeds for scientifically rigorous experiments. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 929–942. [CrossRef]
16. Smadi, A.A.; Ajao, B.T.; Johnson, B.K.; Lei, H.; Chakhchoukh, Y.; Abu Al-Haija, Q. A Comprehensive Survey on Cyber-Physical Smart Grid Testbed Architectures: Requirements and Challenges. *Electronics* **2021**, *10*, 1043. [CrossRef]
17. Liu, R.; Vellaithurai, C.; Biswas, S.S.; Gamage, T.T.; Srivastava, A.K. Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid. *IEEE Trans. Smart Grid* **2015**, *6*, 2444–2453. [CrossRef]
18. Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M. Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid. *IEEE Trans. Smart Grid* **2013**, *4*, 847–855. [CrossRef]
19. Nelson, A.; Chakraborty, S.; Wang, D.; Singh, P.; Cui, Q.; Yang, L.; Suryanarayanan, S. Cyber-physical test platform for microgrids: Combining hardware, hardware-in-the-loop, and network-simulator-in-the-loop. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; pp. 1–5.
20. Zhang, H.; Ge, D.; Liu, J.; Zhang, Y. Multifunctional cyber-physical system testbed based on a source-grid combined scheduling control simulation system. *IET Gener. Transm. Distrib.* **2017**, *11*, 3144–3151. [CrossRef]
21. Wei, M.; Wang, W. Greenbench: A benchmark for observing power grid vulnerability under data-centric threats. In Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 2625–2633.
22. Duan, N.; Yee, N.; Salazar, B.; Joo, J.Y.; Stewart, E.; Cortez, E. Cybersecurity Analysis of Distribution Grid Operation with Distributed Energy Resources via Co-Simulation. In Proceedings of the 2020 IEEE Power & Energy Society General Meeting (PESGM), Montreal, QC, Canada, 2–6 August 2020.
23. Gupta, K.; Sahoo, S.; Panigrahi, B.K.; Blaabjerg, F.; Popovski, P. On the Assessment of Cyber Risks and Attack Surfaces in a Real-Time Co-Simulation Cybersecurity Testbed for Inverter-Based Microgrids. *Energies* **2021**, *14*, 4941. [CrossRef]
24. Chamana, M.; Bhatta, R.; Schmitt, K.; Shrestha, R.; Bayne, S. An Integrated Testbed for Power System Cyber-Physical Operations Training. *Appl. Sci.* **2023**, *13*, 9451. [CrossRef]
25. Salehi, V.; Mohamed, A.; Mazloomzadeh, A.; Mohammed, O.A. Laboratory-Based Smart Power System, Part I: Design and System Development. *IEEE Trans. Smart Grid* **2012**, *3*, 1394–1404. [CrossRef]
26. Hussein, H.; Aghmadi, A.; Nguyen, T.L.; Mohammed, O. Hardware-in-the-loop implementation of a Battery System Charging/Discharging in Islanded DC Micro-grid. In Proceedings of the SoutheastCon 2022, Mobile, AL, USA, 26 March–3 April 2022; pp. 496–500.
27. Huang, Y.L.; Cárdenas, A.A.; Amin, S.; Lin, Z.S.; Tsai, H.Y.; Sastry, S. Understanding the physical and economic consequences of attacks on control systems. *Int. J. Crit. Infrastruct. Prot.* **2019**, *2*, 73–83. [CrossRef]
28. Deng, W.; Yang, Z.; Xun, P.; Zhu, P.; Wang, B. Advanced Bad Data Injection Attack and Its Migration in Cyber-Physical Systems. *Electronics* **2019**, *8*, 941. [CrossRef]
29. Menike, S.; Yahampath, P.; Rajapakse, A. Implementation of Communication Network Components for Transient Simulations in PSCAD/EMTDC. In Proceedings of the International Conference on Power Systems Transients (IPST2013), Vancouver, BC, Canada, 18–20 July 2013.
30. Le, T.D.; Anwar, A.; Loke, S.W.; Beuran, R.; Tan, Y. GridAttackSim: A Cyber Attack Simulation Framework for Smart Grids. *Electronics* **2020**, *9*, 1218. [CrossRef]
31. Hoyos, J.; Dehus, M.; Brown, T.X. Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure. In Proceedings of the 2012 IEEE Globecom Workshops, Anaheim, CA, USA, 3–7 December 2012; pp. 1508–1513.
32. Youssef, T.A.; El Hariri, M.; Bugay, N.; Mohammed, O.A. IEC 61850: Technology standards and cyber-threats. In Proceedings of the 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), Florence, Italy, 7–10 June 2016; pp. 1–6.

33. Amin, B.; Taghizadeh, S.; Rahman, M.S.; Hossain, M.J.; Varadharajan, V.; Chen, Z. Cyber-attacks in smart grid–dynamic impacts, analyses and recommendations. *IET Cyber-Phys. Syst. Theory Appl.* **2020**, *5*, 321–329. [CrossRef]
34. Azeem, A.; Jamil, M.; Qamar, S.; Malik, H.; Thokar, R.A. Design of Hardware Setup Based on IEC 61850 Communication Protocol for Detection & Blocking of Harmonics in Power Transformer. *Energies* **2021**, *14*, 8284.
35. Hussain, S.S.; Ustun, T.S.; Kalam, A. A review of IEC 62351 security mechanisms for IEC 61850 message exchanges. *IEEE Trans. Ind. Inform.* **2019**, *16*, 5643–5654. [CrossRef]
36. Benmouyal, G.; Meisinger, M.; Burnworth, J.; Elmore, W.A.; Freirich, K.; Kotos, P.A.; Leblanc, P.R.; Lerley, P.J.; McConnell, J.E.; Mizener, J.; et al. IEEE standard inverse-time characteristic equations for overcurrent relays. *IEEE Trans. Power Deliv.* **1999**, *14*, 868–872. [CrossRef]
37. Abdelrahman, M.S.; Kharchouf, I.; Alrashide, A.; Mohammed, O.A. A Cyber-Physical Smart Grid Testbed for Validation of GOOSE-Based Protection Strategies. In Proceedings of the 2022 IEEE Industry Applications Society Annual Meeting (IAS), Detroit, MI, USA, 9–14 October 2022; pp. 1–12.
38. NS3, NS3 Homepage. Available online: https://www.nsnam.org/ (accessed on 25 August 2023).
39. Wang, W. Research on Using Docker Container Technology to Realize Rapid Deployment Environment on Virtual Machine. In Proceedings of the 2022 8th Annual International Conference on Network and Information Systems for Computers (ICNISC), Hangzhou, China, 16–19 September 2022; pp. 541–544.
40. Abdelrahman, M.S.; Nguyen, T.L.; Mohammed, O.A. Stochastic Characterization-Based Performance Analysis of an Emulated Communication Network for Cyber- Physical Shipboard Power Systems. In Proceedings of the 2023 IEEE Electric Ship Technologies Symposium (ESTS), Alexandria, VA, USA, 1–4 August 2023; pp. 528–533.
41. Yoo, H.J.; Nguyen, T.T.; Kim, H.M. Consensus-based distributed coordination control of hybrid AC/DC microgrids. *IEEE Trans. Sustain. Energy* **2019**, *11*, 629–639. [CrossRef]
42. Kalluri, R.; Mahendra, L.; Kumar, R.S.; Prasad, G.G. Simulation and Impact Analysis of Denial-of-Service Attacks on Power SCADA. In Proceedings of the 2016 National Power Systems Conference (NPSC), Bhubaneswar, India, 19–21 December 2016; pp. 1–5.