electronics

MDPI

Review

A Comprehensive Survey on Cyber-Physical Smart Grid Testbed Architectures: Requirements and Challenges

Abdallah A. Smadi [1], Babatunde Tobi Ajao [1], Brian K. Johnson [1], Hangtian Lei [1,*], Yacine Chakhchoukh [1] and Qasem Abu Al-Haija [2]

[1] Department of Electrical and Computer Engineering, University of Idaho, Moscow, ID 83844, USA; smad4875@vandals.uidaho.edu (A.A.S.); ajao0553@vandals.uidaho.edu (B.T.A.); bjohnson@uidaho.edu (B.K.J.); yacinec@uidaho.edu (Y.C.)

[2] Department of Data Science and Artificial Intelligence, University of Petra, Amman 961343, Jordan; Qasem.abualhaija@uop.edu.jo

* Correspondence: hlei7@uidaho.edu

Abstract: The integration of improved control techniques with advanced information technologies enables the rapid development of smart grids. The necessity of having an efficient, reliable, and flexible communication infrastructure is achieved by enabling real-time data exchange between numerous intelligent and traditional electrical grid elements. The performance and efficiency of the power grid are enhanced with the incorporation of communication networks, intelligent automation, advanced sensors, and information technologies. Although smart grid technologies bring about valuable economic, social, and environmental benefits, testing the combination of heterogeneous and co-existing Cyber-Physical-Smart Grids (CP-SGs) with conventional technologies presents many challenges. The examination for both hardware and software components of the Smart Grid (SG) system is essential prior to the deployment in real-time systems. This can take place by developing a prototype to mimic the real operational circumstances with adequate configurations and precision. Therefore, it is essential to summarize state-of-the-art technologies of industrial control system testbeds and evaluate new technologies and vulnerabilities with the motivation of stimulating discoveries and designs. In this paper, a comprehensive review of the advancement of CP-SGs with their corresponding testbeds including diverse testing paradigms has been performed. In particular, we broadly discuss CP-SG testbed architectures along with the associated functions and main vulnerabilities. The testbed requirements, constraints, and applications are also discussed. Finally, the trends and future research directions are highlighted and specified.

Keywords: Advanced Metering Infrastructure (AMI); Cyber-Physical-Smart Grids (CP-SGs); Critical Infrastructure (CI); Smart Grid Communications (SGC); Supervisory Control and Data Acquisition (SCADA)

Citation: 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. https://doi.org/10.3390/electronics10091043

Academic Editors: Francesco Liberati and Alessandro Di Giorgio

Received: 27 March 2021
Accepted: 23 April 2021
Published: 28 April 2021

1. Introduction

In previous decades, the global consumption of electricity has jumped approximately three times from 7.323 TWh in 1980 to 22.3 TWh in 2017 [1]. Consequently, to adapt to the considerable consumption increase, the National Institute of Standards and Technology (NIST) rolled out nationwide endeavors to develop the next-generation electric power system, commonly referred to as the SG [2]. Comparing the conventional power grid with SG, the investments and improvements have improved the efficiency, reliability, and sustainability [3,4] . The critical infrastructure (CI) of SG has been considered to be at high risk for cyber-attacks [5–7]. Because of the SG idiosyncrasies, the disruptions of the SG due to cyber-attacks transcend the cyber-realm to affect the physical realm as well. Hence, the combination of both cyber-security and physical security leads to the term CP-SG security [3].

Essentially, cyber-physical systems are the leading influence of the upcoming smart grids as an integrated groundwork system comprising of computing techniques, communication network, and exogenous structures [8].

A typical end-to-end CP-SG architecture consists of three main layers: the SG application layer, the power or physical layer, and the communication layer [9–11]. The physical layer can be divided into two sub-layers including the physical structure that hosts the external system being controlled and the smart connection of sensors-actuators. The application layer provides all CP-SG applications and services that interface between the CP-SG and human operators. The network layer provides a communication environment for transmitting the data collected from the surrounding environment and thus actuates on a prescribed physical system, while the cyber-layer is responsible for producing the decisions and providing the communication structure for the CP-SG [11].

In large Industrial Control Systems (ICS), the cyber-layer is typically composed of a Supervisory Control and Data Acquisition (SCADA) system [10,12]. The integration of SCADA by CP-SG poses numerous challenges to the stability, reliability, and resilience of the power grid. Hence, the cyber, cognitive and human composite inter-dependencies, which may lead to system failures, malfunctions, and faulty events, and tend to aggravate security vulnerabilities, need a robust framework that can handle them [13].

The integration of Industrial Process Automation (IPA), which resulted in SCADA system implementation, has reduced the Operation Cost (OC) and is expected to double the investments in the market. As mentioned in [14] "the electrical SCADA market was USD 1.42 Billion in 2016 and is expected to grow at a Compound Annual Growth Rate (CAGR) of 7.48 percent from 2017 to 2022 to reach a market size of USD 3.29 Billion by 2022". As such, designing a robust supervision system and providing it with effective data/information processing and appropriate evaluation of the system performance is done by identifying the critical vulnerabilities first.

ICS system operators are looking for appropriate, reliable, and secure techniques to implement different layers, for next-generation SG, such as monitoring, metering, operation, automation, protection, and markets [15–18]. However, because of the complication and diversity of CP-SGs, a high fault/fail ratio and security risks are presented and lead to major privacy, reliability, safety, and economic issues [19], which are essential matters in CP-SGs. Consequently, CP-SG examination is essential prior to the deployment in real-time systems [20–22] . Such examination should be performed for both hardware and software components of the SG system prior to the actual system construction. This can take place by developing a prototype to mimic the real operational circumstances with adequate configurations and precision.

The majority of testbeds are primarily developed for specific task assessment and validation. Some testbeds provide insights for specific research fields, but few give a full hardware and software assessment policies for research purposes. The closely connected network infrastructure of the SG necessitates a comprehensive testbed concept to have the ability to enable a variety of research needs. All SG fields need to be assessed independently and should be connected to attain a comprehensive consciousness of the continuing research. SG testbeds involve two parts including the physical/hardware elements and cyber/software packages. The physical part contains three main elements including the generator bases, transmission lines, and load models, while the cyber part comprises communication and information infrastructure. Implementing the testbed systems requires a high-cost and experienced workforce. Also, SG investigations necessitate electrical research and practical tests such as protection and energy management as well as rigorous safety conditions for testbeds. Furthermore, owing to the excessive financial and safety requirements of hardwired power systems, the majority of testbeds embrace simulation/emulation models. Quite a few of them are qualified for conducting experiments using real physical components such as the actual generators or distribution connections. While the current testbed models are limited, modern research is investing in the area of SG.

Indeed, it is predictable that testbeds with a variety of functionalities will be developed in the foreseeable future [23]. The main objectives of this work can be summarized as follows:

- Provide a thorough investigation of CP-SG along with the vital role of testbeds in actual implementation.
- Explore the latest developments of testing techniques for CP-SG architecture including dedicated functionality paradigms and objectives.
- Summarize the techniques for evaluating CP-SG regarding the modelling techniques, tools involved, simulation methods employed, as well as vulnerabilities and threats.
- Evaluate the features and functionalities of the existing testbeds.
- Discuss the current and future trends that are needed to be considered while building new CP-SG testbeds or rehabilitating the existing ones.

The research questions and subsequent methodology adopted in this paper include:

- What is the current status of the CP-SG and CP-SG testbeds? This has been addressed by conducting a thorough investigation on CP-SG along with the vital role of testbeds in actual smart grid implementation.
- What are the latest testing techniques employed in CP-SG architecture including the functionality paradigms and objectives? This has been addressed by summarizing the essential components of the CP-SG testbeds and by categorizing them based on their respective layers.
- What are the gaps that need to be addressed to improve the quality of CP-SG testbeds? This has been discussed by summarizing the techniques used to evaluate CP-SG vulnerabilities and threats. We have also assessed the features and functionalities of the existing testbeds.
- What is the cutting-edge research in this field and future trend that are needed to be considered while building new CP-SG testbeds or rehabilitating the existing ones? This has been addressed by highlighting the important current and future trends implemented in CP-SG testbed deployment to provide valuable insights for CP-SG researchers to create their own CP-SG testing environments.

The remainder of this paper is organized as follows: Section 2 presents the CP-SG with emphasis on the incorporation of Information-Communication Technology (ICT) into the power system then the challenges of CP-SG followed by the vulnerabilities of CP-SG and ended with the needs of the testbed. Section 3 describes the CP-SG Testbed, which highlights the essential components of the CP-SG testbed, requirements, Classification, overview of the existing testbeds, challenges and limitations of testbeds, and recent advancements made in testbeds. The conclusion of this paper is provided in Section 4.

2. CP-SG Perspective

Conventional power grids have drawbacks including varied generator types, high cost and expensive assets, time-consuming demand response (the time to reduce the stress on the power grid and high electricity prices), and relatively high carbon emissions. On the other hand, the SG power network relies on communication and information technology in all its domains of generation, transmission, and consumption of energy, which provide real-time effective control, operational efficiency, grid resilience, and decreased carbon footprint [24]. SG structure, as illustrated in Figure 1, provides the vital infrastructure and communication channels allowing real-time bidirectional interaction between utility companies and consumers. The dissemination of the information via digital mediums such as Fiber Optics (FO), Power Line Communications (PLC), Digital Subscriber Line (DSL), etc. to provide transport of high bit-rate digital information. The advantages of this communication are observed in processes that allow auto metering and maintenance, efficient energy management, self-healing, reliability, and security [25–27].

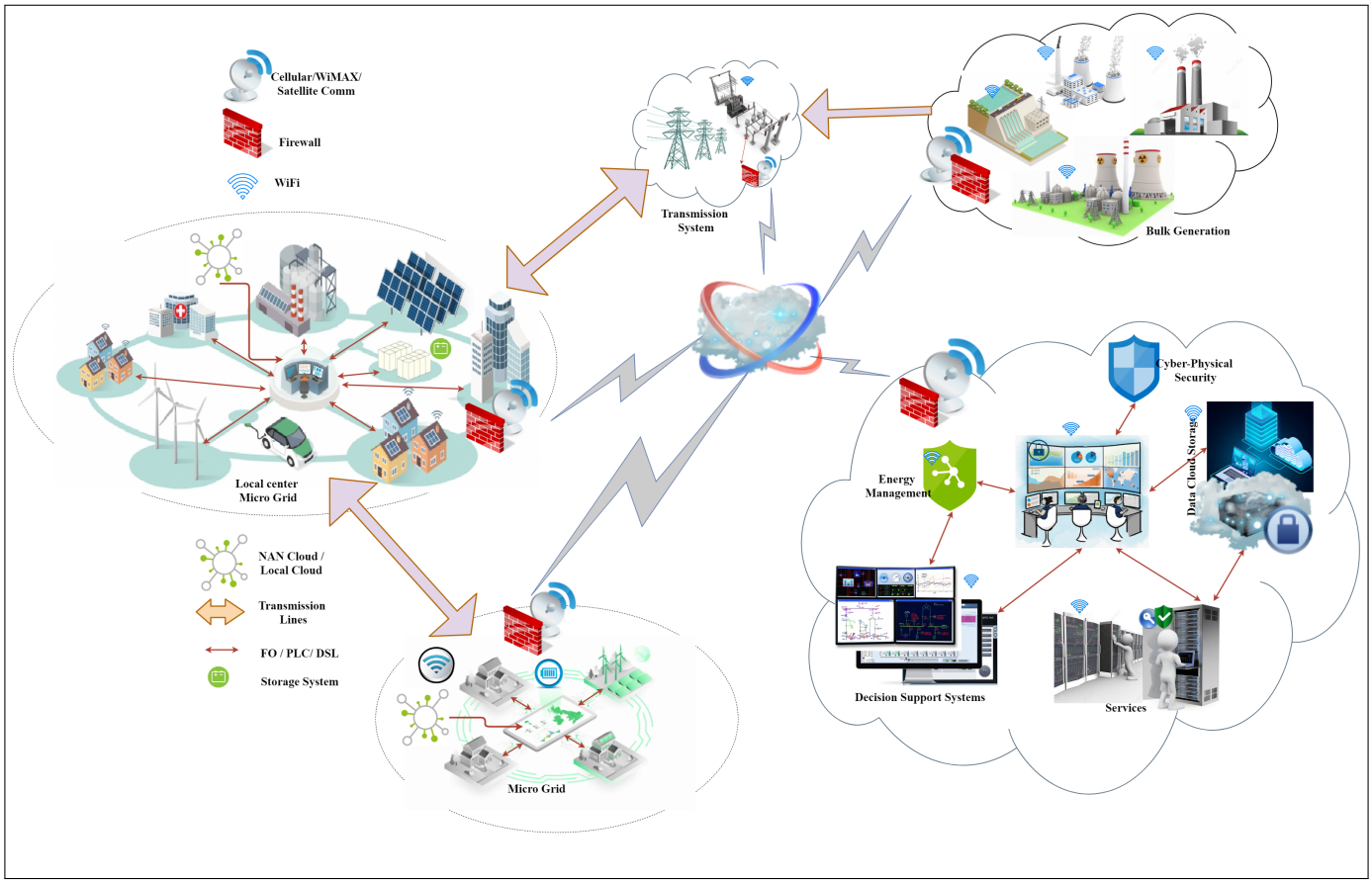

Figure 1. Typical Architecture of CP-SG Conceptual Model.

The operation of power systems is undergoing a rise in complex cyber-infrastructures which is a crucial component of the future SG. As the spread of SG deployments in power systems continues, threats to its critical infrastructures have increased substantially [28]. CP-SG consists of a collection of interconnected physical and computing resources employed in order to achieve a specific mission [29]. In the critical infrastructure networks, CP-SG plays a significant role from power distribution to utility networks. The evolving concept of SG is a significant critical CP-SG infrastructure that depends on two-way communications between SG devices to enhance efficiency, reliability and reduce costs. However, compromised devices in the SG lead to numerous security challenges which can be costly to manage. As a result, new security concerns arise from the use of CP-SG [30,31]. Therefore, vulnerabilities of the widely automated distributed power system security have become a significant target for attackers which is getting the attention of government, energy industries and consumers [24].

A typical CP-SG incorporates cyber system, as represented in the control center, containing computation and communication operations and physical system managing the utility networks as a whole. According to the CP-SG model of Figure 1, sensors are used to measure physical quantities, after which they are converted into electrical signals. These electrical signals are sent to the control center to be sampled for computing. The CP-SG uses various algorithms including state estimation to analyse the sampled values and sends control commands to the physical system, as represented in the substations, through the actuators which convert the electrical signals into physical actions [32,33]. Power system engineers can control tasks based on data acquired from remote facilities thanks to the integrated ICT in SG. In CP-SG, communication between remote sites and control centers can be performed using public or private networks as a result of the wide geographical area. Therefore, the ICT systems support the on-line data acquisition to monitor and control the power system [34].

2.1. Incorporating ICT into Power Systems

ICT schemes have turned into a substantial portion of each facet of our everyday life and its assimilation into the power networks has been increased to suit the growing need in the electric power system [35]. As shown in Figure 2, the implementation of ICT consists of four essential categories for the operations of power system including acquisition, implementation, processing and communication of subsystems [35–39].

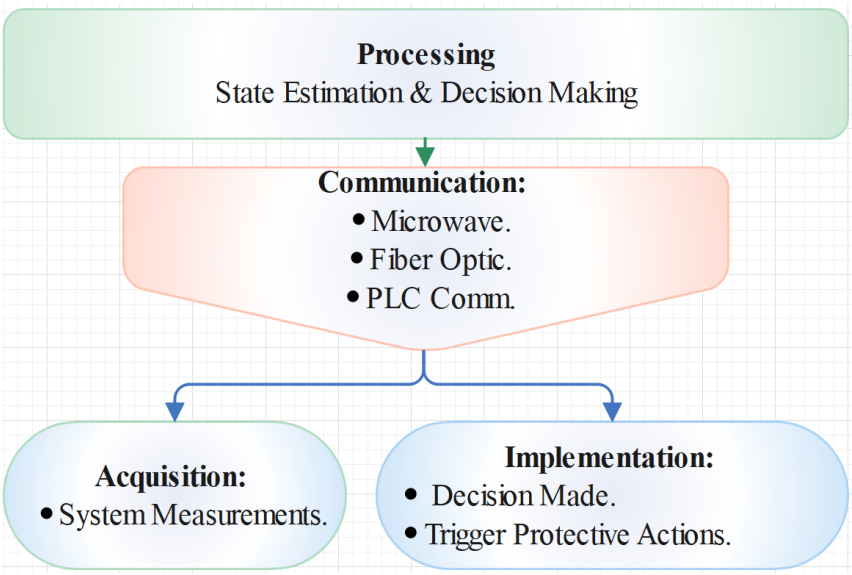

Figure 2. ICT Categories in Power System.

- **Acquisition:** Collects system data such as instantaneous power flow measurements, bus voltages and frequency calculations, the state of circuit breaker, the status of switching tools and then conveys all the data via the communication medium to the processing stage.
- **Processing:** Based on data collected from the acquisition stage, regulates the state of power system and notifies the system operator about the status of the real-time system. At this stage, the existence of state estimator tool is crucial in order to obtain reliable power network based on suitable decisions for implementation.
- **Implementation:** Carries out the required actions based on the system processing results. Some of the actions include activating the protecting relays and circuit breakers next to any failure detected on the power system.
- **Communication:** Coordinates all subsystems with the power network using wired or wireless communication channels. ICTs deployment in power system assists operators to be efficient and improve the power system reliability. Intelligent applications such as intelligent monitoring, protection and control, two-way real-time communication enhances the situational awareness of the network. Consequently, this helps in making correct decisions to operate the power system efficiently. Adequate awareness ultimately improves the reliability of the power system to its highest levels [40].

The frequency and duration of power supply interruptions have decreased drastically with the integration of ICT. In addition, ICT infrastructure implemented in power network provides efficient Energy Management System (EMS) as the increase of its size and complexity has contributed to a reduction of total operation costs [36]. The overall power system reliability and efficiency are enhanced as the increase of the tight coupling of the ICT and power system in the cyber power network. Therefore, these ICT factors should be considered adequately in the planning stage of the power network [35].

2.2. Challenges in CP-SGs

The development and use of CP-SG is confronted with several challenges related to its design, operation, scalability and cybersecurity.

1. ***Design and Operation Challenges:*** The CP-SG consists of many applications that are designed for achieving various purposes such as improving small-signal stability and transient stability, enhance voltage profiles, reduce power losses, and minimizing the probability of cascading failures [41]. Such applications require fast data sampling, otherwise the expected performance might not be attained. Therefore, latency challenges in the communication networks prompted by time delay might result in link failure and packet loss. Hence, this factor has to be effectively considered in designing CP-SGs. On the other hand, some applications does not require such fast data sampling resulting in minor impacts on CP-SG performance [41,42].
2. ***Cybersecurity Challenges:*** The SG network comprises several legacy systems combined with modern technologies and architectural methods within a common interaction communication system to confront the challenges of the forthcoming electric power network systems. To achieve this goal, cybersecurity architecture for future power grid communications is based on cybersecurity requirements, legacy installation dependency, and regulations and industry standards. However, major challenges [43] are facing the desired objective to obtain a secure power grid communication system which includes the following:
    - *Security Policy and Operation:* Adequate operations of many components of the power grid and the connection between them determines the reliability of the power grid. Federated identity management is essential to consider which authenticating entities involved in power production from a remote organization [43]. Technical solutions are possible to such issues based on different security policies such as Security Assertion Markup (SAML) [44], Web Services Trust (WS-Trust) [45], and PKI [46].
    - *Security Services:* Network operators are capable of identifying, controlling, and managing the security risks of the power grid with the assistance of security services. The typical security services in the future power grid are described by the operationalization of cybersecurity across people, process, policy, and technology foundation for each organization.
    - *Internetworking:* Due to the lack of built-in security of power grid communication networks applications and devices, vulnerabilities are introduced across the various internet-connected networks. Commercial networks connected to the Internet might trigger the grid to threats in a form of multiple types of attacks which cause interruption of power [43].
    - *Efficiency and Scalability:* To ensure efficiency and scalability, system availability should be seriously considered in cyber-physical networks such as SG. Key issues have to be considered to fulfill the availability objective of a system including the efficiency of the computation and communication resources, adequate error management functions for handling failures, proper redundancy built-in to avoid system collapses, and auxiliary security support functions to detect cyber-attacks [47].
    - *Differences between Enterprise Network and SG Network Security objectives:* For SG, the most significant objective is ensuring the reliability of the system and protecting the equipment and power lines. On the other hand, enterprise networks are mainly concerned with data protection including data integrity, confidentiality, and availability. The differences in objectives between the two networks are challenging the cybersecurity as the enterprise networks are short in providing cybersecurity solutions at the control and automation levels [43,48].

2.3. Vulnerabilities of CP-SG

The heterogeneity and complexity of the CP-SG introduce significant difficulties to the privacy and security of the CP-SGs. The composite cyber-physical interaction poses vulnerabilities to both cyber and physical systems of SG [49].

1. ***Cyber Vulnerabilities:*** a Cyber-vulnerability is identified as the weakness that can be used by an attacker to execute harmful activities on the CP-SG parties using a networked system. Cyber-vulnerabilities of the CP-SG can be usually targeted through CP-SG communication, CP-SG software, or CP-SG privacy.
    - *Communication Vulnerabilities:* Local area networks in substations are Ethernet-based networks that are vulnerable to interception and Man-in-the-Middle (MitM) attacks. Such attacks enable attackers to impersonate components and injects false data as well as releasing confidential information [50–52]. The information infrastructure of the power network depends on limited internet protocol standards involving known vulnerabilities that might be used to launch attacks on the network. The connectivity of some communication protocols such as the Internet-connected general-purpose TCP/IP is supposed to connect to control centers. Though, due to network misconfiguration, the Internet-based networks are connected directly or indirectly to control centers which cause vulnerabilities to the network [49,53].
    - *Software vulnerabilities:* Servers in control centers that are internet-connected to the local network can be vulnerable to malicious attacks impacting the desired operations. Historical and customer information could be exposed through web-related vulnerability using SQL injection that enables attackers to unauthorized access to database records [51,54,55]. Some devices such as the Expanded Smart Meters (SMs), which can be upgraded remotely, bring about critical vulnerability. Such features open doors to attackers to control switches causing blackouts [49]. In addition, software bugs can take advantage of such vulnerability by malicious attackers as the network components are accessible in every household [56,57].
    - *Privacy vulnerabilities:* The two-way communications connecting the customer's meter to the utility are providing a new type of vulnerabilities regarding customer's privacy. Private information of customers such as daily habits and the presence or absence can be exposed by attackers seizing traffic from smart meters [49,58].
2. ***Cyber-Physical Vulnerabilities:*** Cyber-physical vulnerabilities are identified as the weakness resulting from the integration of the Cyber part with the physical part of the CP-SGs. Cyber-Physical vulnerabilities of the CP-SG commonly exist through the network communication vulnerabilities or smart meters vulnerabilities.
    - *Network Communication vulnerabilities:* Power system infrastructure depends on protocols such as Modbus and DNP3 in which each protocol is vulnerable. Modbus protocol, which is the standard communication in many ICS, is limited to basic security measures which make it vulnerable to a variety of attacks [49]. Attacks such as eavesdropping attacks resulting from lack of encryption make data integrity disputed [49,59–61]. Unlike the Modbus protocol, DNP3 has a simple integrity measure using a Cyclic Redundancy Check (CRC). Similar to Modbus, DNP3 protocol has no encryption or authentication mechanisms [62,63].
    - *Smart meter vulnerabilities:* Interactions between the two-end communication of smart meters pose serious security concerns. Smart meters might have back-doors that could be taken advantage of the factory login account which gives full control to the user over the SG as Santamarta analyzed in [64]. Another major security weakness is that the communication is transmitted through telnet which sends unencrypted data in "cleartext". As attackers take over the control of smart meters, power disruption occurs by malicious interactions with other devices or inject wrong data to make wrong decisions. Also, attackers could use the meter

as "bot" to launch attacks against other systems within the network. In addition, the power bill can be changed to false data in order to reduce the power cost [64].

2.4. CP-SG and the Need for Testbeds

The two-way power and information flow enhanced the conventional power grid forming a smart grid that is equipped with intelligent features of self-healing, customer involvement, and adaptive protection and control [23,65]. The major driving force of the smart grid is the implementation of CP-SG as a foundational support system despite its deployment challenges. Adequate ways to implement future smart grid concepts are the focus of power systems operators to obtain security for different application layers such as operation, monitoring, metering, protection, automation, and markets [15,16,23].

The complex nature of smart grid structure requires the implementation of testbeds including different capabilities for extensive experimental verifications. Prototype implementations are required to achieve real-world application results on actual testbeds. Such testbed implementations and their fast verification will stimulate research results for the power systems industry. In addition, testbed provide educational platforms for researchers with multi-user experimental facilities and proof of concept of verifications for numerous smart grid domains [23,66]. Cybersecurity vulnerabilities and interpretability are major concerns to be tested using properly developed smart grid testbeds with extensive capabilities. However, most testbeds do not provide complete hardware and software platforms to test for all research applications simultaneously. As a result, the tightly coupled structure of the smart grid necessitates a comprehensive testbed structure in order to facilitate experiments at the same time [67,68].

3. CP-SG Testbed

Following the widely publicized cyber-attack events in the smart grid in recent decades, the security and resilience of the ICS have become a major concern to power operators and various governments alike. These attacks are a result of the enhanced integration of information and communication technologies into the control and operations of the power grid. As discussed in the previous section, to overcome these challenges without impacting the real-time environment negatively, testbeds are required for the exploration, development, evaluation, and validation of security controls and algorithms in the power system. The cyber-physical testbed must be able to faithfully model and simulate the power grid for the test and validation of various control, operation, and security algorithms. The testbeds are also important for vulnerability and impact analysis of cyber-attacks on smart power systems.

Testbed design and development have grown in the past few years to the point where replicating ICS networks through simulation and modeling is considered a viable option to explore and address cybersecurity challenges [69]. This is partly due to the potential negative impact of testing cyber-attacks on the live power systems and also the high cost of deploying and using real system hardware and software for testing purposes [70]. Hence, testbeds make it possible to use a model of an actual power grid rather than directly working on the real physical system.

Testbeds that are able to successfully integrate both cyber and physical components of the smart grid provide ideal environments to perform and evaluate research efforts geared towards making the power system more resilient. Unfortunately, the development process of the testbed is not well established because of the complexity involved in integrating the required cyber and physical resources while also incorporating simulation mechanisms needed to model power systems, cyber network dynamics, and security events [71]. Several design strategies will normally lend themselves to different research endeavors. Therefore, a full understanding of the testbed architecture and its development constraints are important to enhance future efforts in ICS research.

A generic physical architecture of a typical CP-SG testbed is illustrated in Figure 3. The testbed is essentially sectioned into three layers; the physical layer, the cyber layer, and the

control layer. The physical layer consists of the physical components in the substations such as Remote Terminal Units (RTUs) , Real-Time Digital Simulator (RTDS), and Intelligent electronic devices (IEDs). The cyber layer is what makes the power grid smart. It makes provision for real-time communication between components in the substation and the control center. It also enhances the automation of various processes in the smart grid. As shown in Figure 3, the control layer is essentially the control center where all measurements are analyzed and control actions are communicated to the substation for the actuators to carry out.

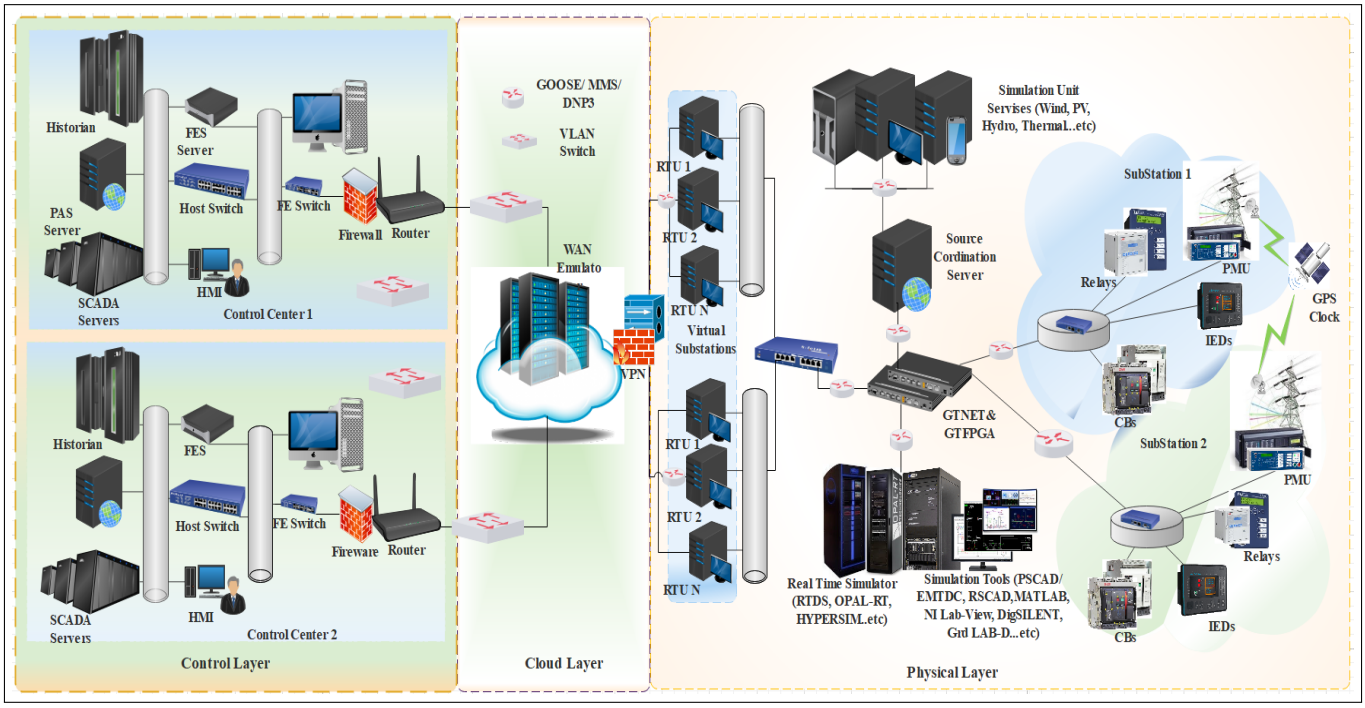

Figure 3. Generic Physical Architecture of CP-SG Testbed.

3.1. Essential Components of CP-SG Testbeds

The essential components of the CP-SG testbeds in the electric power domain can be categorized into communication, control, and power systems. The measurements and status data required for situational awareness of the substations are obtained in the power system model. Both the measurement and the commands required for the smooth running of the power system are transmitted between the substation and the control center via the communication system using various standard protocols and communication media. Various equipment used and deployed in the control center are all categorized under the control system.

The logical architecture of the testbed is illustrated in Figure 4. The power system component of the testbed can either be an actual power system or simulated as is the case in the RTDS [71]. As illustrated in Figure 4, the measurements and actuation commands are either sensed directly from a physical device (represented as *A*) or simulated and transmitted over the network (represented as *B*). The RTDS implementation is more widely used as it is more economical. Item *C* shows how information such as device status, measurements, and protection commands are transmitted through the substation. If regional control is simulated in the testbed, it is carried out as shown in item *D* where substations communicate with regional control and energy management functions via Wide Area Network (WAN). Finally, item *F* shows how inter-control center communication also via WAN is executed for system scheduling. A detailed description of these components is provided as follows:

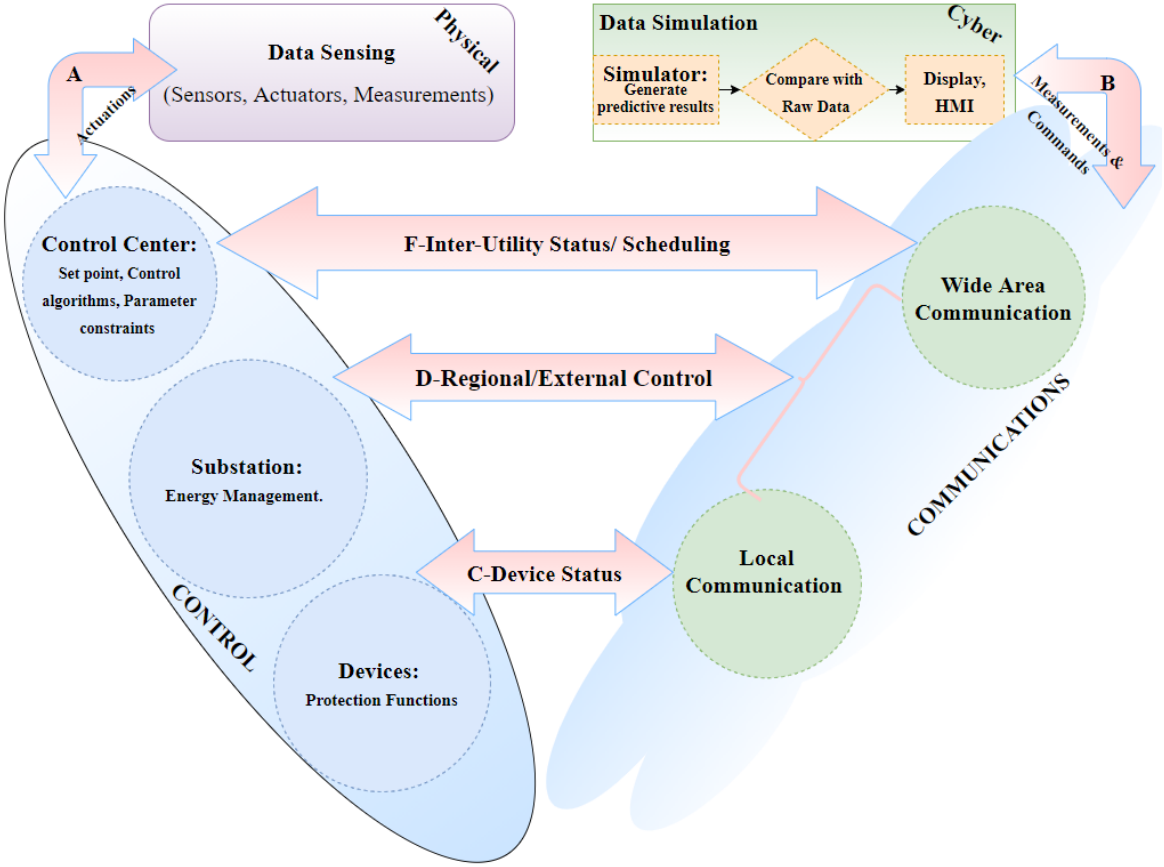

Figure 4. Logical Architecture of CP-SG Testbed.

- **Power System:** Owing to the fact that the control center software is time-dependent, power system simulation in the testbed must run in real time and operate for a long period of time with high precision. These are the factors that make RTDS [72] the most widely used application for power system simulation in real time [73–75]. The RTDS is not only capable of implementing a real-time electromagnetic transient simulation of the power system, but it also supports several data interfaces which makes it convenient for data exchange with other external devices in the testbed setup. PowerWorld simulation tool [76] is another commercially available application used for simulating the operation of large power systems [77–79]. It is a flexible and useful tool to simulate system states and perform contingency analysis. This tool is also very efficient for cost analysis, power flow analysis, and voltage control. The DIgSILENT "PowerFactory" software is another popular application used for power system simulations [80–82]. It is often used to perform non-real-time power system simulations. Although it does not have the inter-connectivity capability that the RTDS has, it provides means for more advanced system analysis and includes algorithms for state estimation and contingency analysis [71].
- **Control System:** The CP-SG testbeds typically use industry-standard software and protocols for all control functions to achieve more realistic cyber vulnerability research. The control system part of the testbed is usually made up of a multifunctional control center and substations [71,74]. EMS from different vendors are adopted in the testbeds to act as the master station at the control center. Either hardware-based or software-based RTUs are implemented to provide consistency with real events in the power system. The RTUs are responsible for aggregating data from the power system (e.g., RTDS model) and transmitting them to the control center. It also serves as the channel for the remote control and remote regulation signals produced by the control center.

- **Communication System:** The essential communication components of the testbed includes physical network architecture and substation network protocols. It is very important to create a WAN network within the testbed which mimics the interconnectivity of the control center to the RTUs in the substations. The IEC 61850 protocol is typically deployed to communicate status and commands between the IEDs and RTUs within a substation. On the other hand, the communication between the control center and the RTU is usually performed with the DNP3 similar to real world SCADA systems. Modbus is another substation protocol that can be implemented in the testbed. It is the actual standard that is openly published, and is approximately used for 40% of the communication within industrial appliances [83]. In the CP-SG testbed, it can be used for communication between master stations and RTUs [77,78,84].

3.2. Testbed Requirements

A CP-SG testbed should provide an avenue for researchers to deploy, test, and verify complex scientific methods and algorithms by ensuring the fidelity, repeatability, measurement accuracy, and safe execution of experiments [85]. Furthermore, the testbed should also be able to support the execution of complex, large-scale, and disruptive experiments seamlessly [86]. The most important features and requirements of CP-SG testbed in the power domain are listed as follows:

1. **Fidelity**: It is the degree of correlation between simulation results and real-world observation [87–89]. It simply connotes the ability of the testbed to accurately reproduce real power systems in terms of tools (hardware and software technologies), functionalities and operations [70]. Testbeds that involve physical simulation is usually considered to have the highest fidelity, while software-based testbeds have much lower fidelity [90].
2. **Repeatability:** The results from CP-SG testbed must be repeatable and capable of producing consistent results when performed independently [22]. It refers to the ability of the testbed to produce similar outcomes when an identical design or setup is replicated. However, the important point that has to be stressed is what are the differences in the results that could occur during actual testing. To achieve this feature, a researcher must be able to set up the experiment platform in the initial state and trigger the necessary events in the right order and at the appropriate time frame [86,87,91].
3. **Flexibility:** It is the ability of the CP-SG testbed to be easily redefined for alternative test cases or scenarios [92]. For instance, a testbed is said to be flexible if it was initially set up for vulnerability analysis, but can easily be restructured for security impact analysis [70].
4. **Safe Execution:** One of the major reasons for the deployment of a testbed is to be able to run different tests and scenarios in a safe manner. Hence, the testbed must be able to support disruptive experiments with physical processes safely [84].
5. **Scalability:** This refers to the ability of the testbed to increase the size of the setup [71,87]. This feature can be demonstrated by the ability to add components to the existing testbed setup without the need for extensive redesign or re-configuration [70]. This feature is especially important for testbeds used to validate new processes or algorithms.
6. **Cost-Effectiveness:** The cost implication required to achieve the goals and objectives of a testbed must be within the financial budget affordable for research purposes [89,93]. Since the initial aim of deploying testbed is to reduce cost (in comparison to the cost of using the actual system) and still achieve the same design objectives and scenario as the real one, it is important that the overall cost of putting the testbed together is reduced to the barest minimum. One way of achieving this aim is through the design of a portable testbed system that is able to simulate several services and scenarios [94].

7. **Diversity:** This is the ability of a testbed to incorporate a wide range of components and devices without affecting its scalability [70]. Such a testbed system is said to be effective since it can mirror a variety of CP-SG setups [87,95].

3.3. Classification of CP-SG Testbeds Based on Methodologies

While the legacy testbeds were predominantly software-based, most of the contemporary testbed deployment are integrating more real physical components to the implementation of testbed design. The main advantage of including industrial-grade physical devices in the design of testbed is high fidelity. The trade-off, however, is the cost of implementing a physical simulation testbed. To take full advantage of the benefit from both software-based and physical-based testbeds, most institutions and research organizations are now deploying hybrid testbeds that have improved fidelity and cost much less than physical-based testbeds. As shown in Table 1, hybrid testbeds save cost and have a higher fidelity compared to both software-based and Hardware-based testbeds. The remainder of this subsection will provide details regarding the advantages, disadvantages, and implementation methods of each testbed classification.

Table 1. Classification of Testbed Based on Methodologies.

Classifications	Cost	Fidelity	Flexibility	Time	Methodology
Software-Based	Low	Low	High	Low	Modeling
Hybrid-Based	Medium	Medium	Medium	Medium	Modeling and Replication
Hardware-Based	High	High	Low	High	Replication

1. **Software-based Testbeds:** This type of testbeds is considered to be economical because instead of using physical devices and information systems, modeling mechanisms are used for their deployment and implementations. Several software-based testbeds use modeling tools such as Matlab, Modelica, Ptolemy, and PowerWorld to model various ICS processes, while applications such as OPNET, OMNet++, and more recently NS3 are used to simulate wide area network models in the testbeds [96]. The major disadvantage of using virtual devices deployed in the tools mentioned above is low fidelity. Another disadvantage is their limitation in simulating certain cybersecurity scenarios due to the unavailability of software models of some devices.
2. **Physical-based Testbeds:** The physical and network layers of physical-based testbeds are deployed using real hardware and industrial-grade software. This type of testbeds typically has very high fidelity as they closely mimic the real smart power grid. An example of such a testbed is the National SCADA Testbed (NSTB) built by Idaho National Laboratory. This testbed is made up of 61-mile 138 kV transmission lines, seven substations, and more than 3000 monitoring sites. NSTB is the first actual grid testing environment in the world with full replication of real hardware and software [97]. The major disadvantage of this type of testbed is the cost, as it requires a very high cost of implementation. Another limitation introduced by the implementation of a physical-based testbed is lack of enough flexibility and reconfiguration capability.
3. **Hybrid Testbeds:** The idea behind the hybrid testbed is to take full advantage of the replication ability of physical-based testbeds and the flexibility and easy reconfiguration ability of software-based testbeds. In a nutshell, it integrates the methodology of model and replication. This is an effective method of deploying testbeds because it is cost-effective and provides improved replication of the real power grid components and processes. A typical example of hybrid-based testbed is the one deployed at the Washington State University [23]. Industrial grade physical components such as protective relays, RTUs, Phasor Measurement Units (PMUs), and several net-

work switches are integrated with simulators such as RTDS and Network Simulator (NS3) [98].

3.4. Overview of Existing CP-SG Testbed Applications

The review of previous developmental efforts conducted by researchers over the years has demonstrated several research applications supported by CP-SG testbeds. Table 2 provides a comprehensive list of existing CP-SG testbeds from various research institutes. Moreover, it highlights the applications, hardware and software components as well as the communication protocols adopted in these testbeds. The most essential applications of the existing testbeds include the following:

1. **Control Validation:** Testbeds are used to validate the correctness of the control logic in complex CP-SGs. Since one of the primary objectives of deployment of ICS in the power grid is the remote control of the grid processes and devices, it is important to have an environment that supports the testing and validation of the control logic implemented in such setup. For instance, the Florida International University (FIU) deployed a testbed mainly with the objective of conducting research studies that relate to various control logic implemented in the smart grid [99]. A Chinese-based company (NARI Technology) also developed a flexible hardware-in-the-loop CP-SG testbed which provides an environment for studies in the performance of the stability control system of the smart grid [82]. The testbed was designed to assess the impact of communication error on the stability control equipment of the power system.
2. **Vulnerability and Impact Analysis:** The cyber-physical system uses multiple hardware, software, communication protocols, and media to achieve its objectives. Many of these technologies are deployed in environments that are not readily available to the general public. Moreover, they are very expensive to set up, hence creating a bottleneck in conducting vulnerability and impact analysis on the system. The deployment of a testbed creates an avenue for researchers to evaluate the physical impact of different types of cyberattacks on the power systems [100]. Vulnerability analysis activities such as vulnerability scanning, cryptography analysis, and software testing are also conducted on the CP-SG testbeds [71]. For instance, the testbed deployed in the University of Arkansas was designed mainly for research tasks on the detection of false data injection attacks and vulnerability analysis of the Distributed Energy Resources (DER) cybersecurity schemes [101]. The Institute for the Protection and Security of the Citizen in Italy also designed a CP-SG testbed for cyber vulnerability studies of the SCADA system in the power system [102]. The National SCADA testbed at the Idaho National Laboratory (INL) is also being used extensively for several research studies on vulnerability and impact analysis [103]. The Electric Power and Intelligent Control (EPIC) testbed at Missouri University of Science and Technology has been developed to uncover potential integrity vulnerabilities in electrical synchronous generators [104]. Also, this testbed is used to assess the impact of cyber threats against physical infrastructures and provides a repeatable assessment of the effect of cyber attacks [18,86]. In the same vein, an CP-SG testbed that creates an environment for testing the impact of various time delays cyber-attacks on SCADA systems was developed at the University of Binghamton [105]. The testbed has been used for various research projects to study the physical impact of such attacks on the ICS system [106,107].
3. **Performance Studies:** Reliability is critical to the operations of any CP-SG due to its reliance on communication. Hence, there is a need for testbeds to have the capability of testing the performance of the CP-SG in the electric power domain under different operating conditions. CP-SG Health testbed [108] was designed to observe any maloperation in the cyber, physical, and overall health of the smart power grid. The health of CP-SG is tested and calculated during Denial-of-Service (DoS) attacks. Real-Time Automation Controller (RTAC) was deployed in the testbed for storage of the control decisions required if the health of the power system is depleting, and the power

system is simulated using RTDS. Ghada et al. [109,110] designed a cost-effective software-based testbed to assess the performance of IEC 61,650 under various cyber-attack scenarios on the sensors, communication network and embedded systems of the testbed. A Microgrid testbed platform that is made up of hardware-in-the-loop and network-simulator-in-the-loop was designed to study and test the effect of different communication channel delays in the performance of the smart power grid [111].

4. **Security Validation:** A lot of CP-SG testbeds focus on different aspects of power system security concerns such as cybersecurity, communication security, and physical security. Cybersecurity compliance requirements are becoming increasingly common as a way of ensuring the security and protection of critical infrastructures [71]. Due to the smart grid's high availability requirement and the heavy usage of proprietary systems, there is a constraint in the applicability of common vulnerability scanning methods [112]. Hence, there is a need for testbed environments that implement industrial software, communication protocols, and configurations which would help validate the effectiveness of traditional security assessment techniques while also providing a medium for testing new security algorithms. An example of such a testbed was developed at the University of Arizona [113]. The testbed is extensively used to validate the effectiveness and performance of various protection techniques used in the smart power grid [77]. The University of Illinois also developed an CP-SG testbed to support decision-making in the power grid cyber-infrastructure for cyber-security purposes [78]. Apart from this primary objective, the testbed was also intended to be integrated into other testbeds for the exploration of the performance and security of SCADA protocols and equipment in an inter-connected testbeds setup [84]. Some testbeds are also designed for protection device validation and tuning. An example of such a testbed is developed at the University of North Carolina, where it is used mainly for the validation of synchrophasor relays [114]. Some other testbeds are designed mainly for security research that involves intrusion detection in synchronous generators. One of such testbeds was developed at the Mississippi State University where it has been used for research studies that involve the deployment of Intrusion Detection System (IDS) for synchronous generator security monitoring [75]. Another testbed with similar functionality was developed at the Center for Development of Advanced Computing (C-DAC), where it is used to detect potential intrusions at the RTU of the synchronous generator [115]. The testbed developed at the University of Idaho (ISAAC) is another security-oriented testbed that emulates a realistic power utility and is used to test various integrated cybersecurity solutions [116–118]. This testbed was used for experimental evaluations, whereby the data of normal and attacked communications were collected for data-driven stochastic anomaly detection on smart grid communications [29].
5. **Multi-functional:** To make the most of the various research possibilities presented by the testbed environment, some existing testbeds are set up to be multi-functional in nature. This type of testbeds is usually very robust, flexible, and easily scalable. They provide a platform on which a variety of tests and validations can be conducted on the same testbed unit. An example of such a testbed is the one developed at Iowa State University. This testbed was designed for multipurpose use, although its primary objective is to create an environment for testing and validating smart grid algorithms in real time [71,119–121]. Some of the capabilities of this testbed include cyber-attack detection in the smart grid, measurement of the impact of the attacks, and intensive vulnerability analysis [119]. Other research studies conducted on this testbed concentrate on mitigation research, data and model development, security validation, interoperability, and cyber forensics [71]. Extensive studies on the impact of cyber-attack on the Automation Generation Control (AGC) have also been conducted on this testbed [121]. Washington State University has also designed and deployed a state-of-the-art testbed which is intended to be flexible enough to accommodate

diverse research studies [122–124]. The authors in [3,125] gave a detailed description of how this testbed was designed, assembled, and configured. They also validated the performance of the setup by conducting a cyber-attack impact assessment on the testbed to study the impact of cyber-attack on the smart power grid. The testbed has also been used to test the accuracy of synchrophasor devices such as PMUs and Phasor Data Concentrators (PDCs) [126]. In addition to the research efforts described above, the authors in [127,128] provided an in-depth description of various cybersecurity vulnerability and impact analysis conducted on the testbed. This robust testbed has also been used for the validation of distributed application as described in [129] where the authors validated a Distributed Remedial Action Schemes (DRAS) on the testbed. As it is very essential to deploy a standardized security assessment metric on the cyber-physical system, the authors in [130] were able to propose and validate Multi-Criteria Decision-Making (MCDM) technique on this testbed. The Sandia National Laboratories also developed a multi-functional testbed which has been used for vulnerability analysis [79], validation of new topologies, hardware, controls, communication, and security of microgrid [131,132]. In another research study, the testbed was used to compare the performance of a virtual testbed to an actual physical system [133]. The North China Electric Power University (NCEPU) designed a multi-functional CP-SG testbed for various research application that ranges from vulnerability analysis, cybersecurity, to integration of different renewable energy resources [74,134]. This testbed is very versatile because the physical layer of the testbed was realized with a source-grid co-simulation system (in which the energy sources and the power grid network were simulated separately). Various security-oriented research tasks have been carried out on this testbed with the main targets of the attack being the AGC modules and the measurement collected at the tie lines of the power system. Pacific Northwest National Laboratory (PNNL) designed and deployed a robust multi-functional CP-SG testbed called PRIME [135]. This realistic testbed environment is made up of industry-grade software coupled with hardware-in-the-loop to perform various verification and validation studies. It is also used for several Wide-Area Monitoring, Protection, and Control (WAMPAC) prototyping, impact analysis of diverse cyber-attack scenarios on the operation of the grid, and operator training.

6. **Education:** The application of testbed in the education system plays a vital role. It allows students to work and gain experience with Industrial security systems. It is dangerous to direct research and training on valuable plants, as slight distraction can rapidly prompt harmful instances. Because of this justification, testbeds are very essential in education as well as research. Purchasing genuine industrial hardware for testbeds is very costly especially for the education field. Therefore, researchers have come across few testbeds with low cost for purpose of education. For instance, the LICSTER (A Low-Cost ICS Security Testbed for education and research) [136]. It is an open-source testbed that helps students and researchers to gain knowledge and experience related to industrial security. It costs 500 Euro to build the testbed. The educational testbed developed for a course on industrial communication networks at the Engineering Faculty, University of Catania [137]. A WoT Testbed for Research and Course Projects, building a WoT testbed is implemented in two main axes; the first axis is to configure and connect hardware components that simulate the set of environmental events (IoT layer), and the second axis is to build the application layer in terms of mini-projects on top of the IoT layer [138]. As illustrated in the paper [139] "Development of Smart Grid Testbed with Low-Cost Hardware and Software for Cybersecurity Research and Education", the testbed is a useful resource for cybersecurity research and education on different aspects of SCADA systems such as protocol implementation, and PLC programming [139].
7. **Forensic**: SCADA systems run 24/7 to control and monitor industrial and infrastructure processes. In case of potential security incidents, several challenges exist

for conducting an effective forensic investigation [140]. In the light of the significance of SCADA for the resilience of critical infrastructures and the related targeted incidents against them (e.g. the development of Stuxnet), cybersecurity and digital forensics emerge as priority areas [141]. The paper [142] describes an architecture that supports the forensic analysis of SCADA systems and networks. The design is actualized in a prototype networked condition using the Modbus TCP protocol. The study of forensic attacks plays an important role in the SCADA system to reach the accountability requirement of the data security objectives. Probable vulnerabilities are detected by forensic attacks before they get manipulated by malicious entities. As stated by Chris et al. in [143], the first step in preparing for any forensic attack is to identify and exploit weaknesses. In [144], a four-stage approach is made by the authors to perform forensic attacks on SCADA systems. The main technique for cyber defense when a security breach occurred is digital forensics. It is a method of acquisition, examination, study, and recording of the evidence. For instance, the authors in paper [145] have implemented and improvised a forensic testbed by implementing a sandboxing technique in the context of real time-hardware-in-the-loop setup. The paper [146] presents a SCADA testbed recently built at the University of New Orleans for purpose of cybersecurity and forensic research, and education on diverse aspects of SCADA systems such as PLC programming, protocol analysis, and demonstration of cyberattacks.

8. **Safety Standards Development:** Because of the susceptibility and security concerns of a conventional SCADA/DCS, the power system managers should consider building and implementing emergency plans to define the appropriate steps to be followed by their workers or suppliers in a situation where the facility is deliberated in a cyber-attack. The typical cyber-attack emergency plan ought to incorporate several elements including the logical network diagram, the network connection loss impact analysis, the zones of vulnerabilities identified on the logical network diagram, the access-control lists that identify which personnel should be allowed access to the industrial network, the step-by-step standard operating procedures of what activities to perform immediately following an incident, and finally, the access logs detailing time-stamped activities on the network IT. For instance, the paper [147] implemented "An integrated testbed for locally monitoring SCADA systems in smart grids". Using the developed testbed, a recently proposed local monitoring approach was investigated [147]. The paper [148] has developed a "Testbed for Secure and Robust SCADA Systems" for checking vulnerabilities and validating security solutions.

3.5. Challenges Facing the Existing Approaches of Testbeds

One of the major factors limiting the effectiveness of the existing testbeds is fidelity. As in-depth knowledge regarding a plethora of parameters is simulated for CP-SG testbeds, managing the fidelity of such setup becomes a major challenge [149]. High fidelity of the cyber layer of the testbed can be achieved by the deployment of real components, including real software, network devices, and standard protocols [86]. As discussed in Section 3.2, researchers must be able to set up the experiment platform in the initial state and trigger the necessary events in the right order and at the right time to obtain consistent results. For this reason, it is important that the experimentation workflow of different cases simulated on the testbed must be automated in order to achieve repeatability and measurement accuracy. On the other hand, testbed with a fully simulated cyber layer such as those described in [109,150], provide precise repeatability and measurement accuracy, although at the expense of decreasing the setup's fidelity [151]. The hybrid setup of real components with simulators in the cyber layer also poses its own limitation as the strong fidelity provided by the real components is weakened by the simulated cyber layer [86,152].

The major bottleneck of testbeds with full real component deployment both for the physical and cyber layer is its lack of flexibility and its very high-cost. Security experiments conducted on such setups can be highly disruptive and the use of advanced malware

tools can have an unpredictable impact on the physical setup [153,154]. Re-configuring these testbeds to explore diverse research studies is often complicated and could even be financially infeasible. Hence, the fidelity provided by this setup is offset by its poor flexibility, high-cost implication, and high safety risk [86].

Another factor limiting the functionalities of the existing testbeds is insufficient diversity and heterogeneity of equipment. Most of these testbeds are assembled with devices from a single vendor or supplier. This factor makes it difficult to meet the requirement of vulnerability assessment of certain protocols and equipment [97].

Table 2. Taxonomy of existing cyber-physical smart grid testbeds.

Testbed Name	Year	RC/ Institute	Application Domain	Attack Type	Detection Techniques	Communication Protocols	Architecture Type	Software Used	Hardware Used	Reference
PowerCyber	2010-2019	Iowa State University	SG ecosystem	DoS, Intrusion	Anomaly Detection	IEC 61850, DNP3, GOOSE	HWIL	ISEAGE, DIgSILENT Power Factory	Power TG EMS, SICAM RTU, RTDS, Siemens relays,	[71,120,119,118]
SGDRIL	2012-2019	WSU	Smart Grid	PMU Testing	Intrusion Detection	TCP/IP	HWIL	RSCAD,	RTS, Relay/PMU tester, SEL Relays, PDC, SVP and RTAC	[125,3,124,126,127,128,73,121, 122,123]
FREEDM	2013	FSU	Distributed energy management	Dynamic behavior of smart grid	SE	TCP/IP	HWIL	PSS	RTDS, Embedded Single Board Computers	[73]
VPST	2009	University of Illinois	Smart Grid	DOS, MiM	BiW Cryptography	Modbus, DNP3,	HWIL	PowerWorld	Relays, Data Aggregator	[78,84]
UCD	2011-2012	University College Dublin	Smart Grid	Intrusion	DIDS	DNP3, IEC 61850-7-2, IEC 61850-8-1, ICCP	HWIL	DigSilent, MATLAB	Relays, IEDs	[81]
VCSE	2010-2019F	Sandia National Laboratories	Smart Grid	Intrusion and network scanning	Deployment of firewalls	NA	HWIL	Umbra Framework, PowerWorld	Networking devices, RTUs, Firewall, OPNET	[79,130,131,132]
TASSCS	2011-2018	University of Arizona	Smart Grid	DoS, Spoofing, MiM	Intrusion Detection, ASPS	Modbus, DNP3	HWIL	PowerWorld, ASPS	OPNET	[77, 112]
DERT	2015-2019	University of Arkansas	DER	FDIA, Attack on PLL	State Estimation	DNP3, IEC61850, MODBUS	HWIL	OPAL-RT, LabVIEW	SEL IEDs, RTAC, routers and switches	[101]
ESRL-FIU testbed	2015	Florida international university	Efficiency of smart grid	FDI	API	DDS	HWIL	Matlab Simulink, NI LabView	DAQ- STM32F4, DAQ9206 inputs, -PDC PMUs	[99, 133]
Multifunctional testbed	2017-2018	North china electric power university	RTU for substation power output	Upstream attacks Downstream attacks	SE	DNP3 IEC60870-5-104 GTNET	HWIL	PSS, lab simulation source grid	RTDS, HIS, RTUs, GTNET, GTFPGA	[74]
MSU SCADA Security Laboratory	2011-2015	Mississippi State University	Power system attacks	Shunt fault, DoS, MITM	IDS Specification Signature, SE	PDC in C37.118, Modbus, DNP3	HWIL	Matlab	RTDS, OSISoft PI Historian, PDC, PLC, RTU, MTU	[75]
SCADA testbed	2015-2017	C-DAC	ICS attacks	RTU & MTU intrusions	RTU-malware, Anomaly Detection so	IEC-60870-5-101 DNP3	HWIL	MATLAB, PSAT	Traffic generator, RTU, MTU	[114]
EPIC	2013-2018	Missouri S&T	Smart grid	DDOS, MITM	MSDND	Proxy units, MPLS, Modbus, DNP3, IEC 61850	Emulation	MATLAB Emulab, SSim	AMI, PLC, IEDs, Historian	[86,104]
CPS health measurement framework	2018	Virginia Commonwealth University	Microgrid	DoS	Anomaly-based	DNP3, TCP	HWIL	RSCAD/RTDS	RTAC Grid Controller, Data historian Storage	[108]
ENSURE	2018-2019	Karlsruhe Institute of Technology, Germany	Communication Network,	Replay, Modification	Anomaly detection	GOOSE	Hybrid	libiec61850, Matlab/Simulink, GNS3,	RTDS, CTs, VTs, Relays, CBs	[109, 110]
ISAAC	2019	University of Idaho	Microgrid, ICS servers Network, EMS	DoS, Spear phishing, MITM	Anomaly detection, SE	DNP3, IEC 61850 GOOSE, TCP/IP, IEEE 802.3 based Ethernet	HWIL	RSCAD, PSCAD	RTDS, RTU SEL relays, SCADA Control, IEDs	[116,150] [117] [29,118]
PRIME	2020	PNNL	Power Transmission Systems	Fault detection, operator training	Anomaly-based	IEC 61850 GOOSE, DNP3, ISD, IEEE C37.118.2	Simulator/ HIL	e-terra platform EMS, LabVIEW, PWDS	SEL 421 relays, SEL 651R relays, and SEL 734B capacitor controllers, NI CRIO platform	[135]
HIL testbed	2019	NARI Co. China	AVC, Stability Control System,	FDIA, MITM	NA	Ethernet-based	HWIL	Real-time HIL co-simulator	DIgSILENT, QualNet, AVC, RTDS, SDH	[82]
ICS Security	2016-2017	Binghamton University	Power Grid, ICS	DoS, MITM, Modification	Anomaly-based	Virtual Network Platform	Hybrid	PLC-VM, GE-iFix HMI/SCADA, SoftLogix-VM,	MG (0.24, 0.5 KW) , TG(0.5KW), PLCs, VFDs, FlexIO 1794	[105, 106, 107]

3.6. Current Trends in CP-SG Testbed

In this section, we will highlight some of the important current trends implemented in CP-SG Testbed deployment.

- **Hybrid Testbeds:** As discussed in Section 3.5, fidelity is an essential factor that must be considered when designing and deploying a testbed. The result and dynamics of the components of a testbed are expected to be as close as possible to that of an actual power system. The fidelity of the legacy CP-SG testbeds was often compromised because the majority of them are predominantly software-based. While the physical-based testbeds have high fidelity, it is quite difficult to reconfigure such testbeds for different research endeavors and their deployment can be very expensive as well. Due to these factors, most of the contemporary testbeds are designed to incorporate both hardware and industry-grade software. This paradigm shift has tremendously improved the reliability and fidelity of the CP-SG testbeds in the power domain.

- **Inter-connectivity of Testbeds:** Another advancement in the implementation of CP-SG testbed is the inter-connectivity of testbeds from different universities and research institutes. This development affords researchers a medium and platform to perform intensive research tasks using robust infrastructure which gives room for an open and convenient collaboration across vast distances. A good example of such a setup is the Idaho Regional Optical Network (IRON) in Idaho state. IRON is a regional optical network used by researchers and educators to transfer big data between research universities, other educational entities, the national laboratory system, and the health sector. The connected institutions include Boise State University, Brigham Young University-Idaho, Idaho Hospital Association, Idaho National Laboratory, Center for Advanced Energy Studies (CAES), Idaho State University, State of Idaho – Department of Administration, University of Idaho, and Washington State University. The platform has allowed for productive collaborative research projects among the listed institutions.
- **Software Defined Networking (SDN):** Incorporation of SDN into the CP-SG testbed network is another paradigm being considered by several research institutions. SDN aids the creation of an open networking architecture which makes it possible to get a holistic perspective of the entire network and make global changes in the network without having to access individual device hardware [23]. The overall security and resilience of the CP-SG testbed network can be improved by the deployment of SDN technology. ISAAC testbed at the University of Idaho, for instance, has deployed several SDN switches in their testbed, with the aim of comparing the security and performance of a network with and without the presence of SDN technology. This would go a long way in helping to verify the feasibility of SDN technology in the existing smart grid infrastructure.
- **Distributed Control:** The vast inter-connectivity and complexity of the contemporary smart grid makes it almost impossible to have a single centralized control system for the whole grid. Due to this factor, distributed control is one of the current trends in smart grid technology [23]. The dynamic nature of the smart grid even makes it necessary to deploy distributed control in the grid. Since the CP-SG testbed is meant to represent a faithful replication of the actual smart grid, it is important for institutions and research organizations to start incorporating distributed control into their CP-SG testbeds so that diverse test scenarios can be conducted to evaluate the performance of distributed control on the smart grid.

4. Conclusions

In this paper, we illustrated the challenges faced by the conventional power grid which necessitated the development of the smart grid. We elaborated on the factors that make smart grid testbeds essential in analyzing power systems. We provided three major components that make up the CP-SG testbed. Then we presented a comprehensive overview of the existing CP-SG testbeds. We thoroughly investigated the infrastructures of these CP-SG testbeds from the perspectives of their architecture and corresponding functional analyses, the main vulnerabilities and threats, testbed requirements, constraints, and their applications. We also discussed current trends and future research directions to provide valuable insights for CP-SG researchers to create their own CP-SG testing environments.

In conclusion, the main points that can be derived from this comprehensive survey of CP-SG testbeds are:

- The major drawbacks of actual testing on the conventional power grid include time-consuming demand response, high computational costs, and expensive assets. As a result, testbeds are required to simulate an actual CP-SG to verify various concepts and extensive research purposes.
- Communication infrastructure is an essential component of a smart grid. It is used in generation, transmission, and distribution domains of the power grid. This vastly improves the operational efficiency of the power system. However, the introduction

of communication into the power grid exposes the system to various types of cyber-attacks. CP-SG testbeds are used to perform vulnerability and impact analysis of cyber-attacks on the smart grid.

- Most of the existing testbeds are simulation-based due to the complexity involved in modeling the actual smart grid system. Simulation-based testbeds are known to be economical because software is deployed instead of using physical devices. However, the major disadvantage of this type of testbed is the limited capability to represent the real-time features of actual systems.
- Physical-based testbeds have a relatively high capability to represent the real-time features in actual systems, but the cost implication increases drastically as the scale of the system increases. Another disadvantage of this implementation is the lack of flexibility and reconfiguration capability.
- Control Validation, Security Validation, Performance Studies, Vulnerability, and Impact Analysis are some of the most common applications of existing CP-SG testbeds.
- Inter-connectivity of CP-SG testbeds from different research institutes provides researchers with a platform for extensive and expansive research tasks using robust infrastructure which promotes highly productive collaborations across vast distances.
- Some research institutions are already integrating SDN into their CP-SG testbed setup. This will aid and enhance the feasibility study of the deployment of SDN technology in existing smart grid infrastructure.
- Distributed control is an aspect of the contemporary smart grid that must be considered for integration into the existing CP-SG testbeds.

Funding: Work supported through the INL Laboratory Directed Research and Development (LDRD) Program under DOE Idaho Operations Office Contract DE-AC07-05ID14517.

Data Availability Statement: Not applicable.

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

References

1. Wang, T. *Net Consumption of Electricity Worldwide from 1980 to 2017*; Statista: Berlin, Germany, 2020; pp. 4514–4525.
2. Greer, C.; Wollman, D.A.; Prochaska, D.E.; Boynton, P.A.; Mazer, J.A.; Nguyen, C.T.; FitzPatrick, G.J.; Nelson, T.L.; Koepke, G.H.; Hefner, A.R., Jr.; et al. *Nist Framework and Roadmap for Smart Grid Interoperability Standards*, Release 3.0; Technical Report; NIST Pubs: Gaithersburg, MD, USA, 2014.
3. Vellaithurai, C.B.; Biswas, S.S.; Srivastava, A.K. Development and application of a real-time test bed for cyber–physical system. *IEEE Syst. J.* **2015**, *11*, 2192–2203. [CrossRef]
4. Cecati, C.; Citro, C.; Piccolo, A.; Siano, P. Smart operation of wind turbines and diesel generators according to economic criteria. *IEEE Trans. Ind. Electron.* **2011**, *58*, 4514–4525. [CrossRef]
5. Cardenas, A.; Amin, S.; Sinopoli, B.; Giani, A.; Perrig, A.; Sastry, S. Challenges for securing cyber physical systems. In *Workshop on Future Directions in Cyber-Physical Systems Security*; Homeland Security: Washington, DC, USA, 2009; Volume 5.
6. Alcaraz, C.; Zeadally, S. Critical infrastructure protection: Requirements and challenges for the 21st century. *Int. J. Crit. Infrastruct. Prot.* **2015**, *8*, 53–66. [CrossRef]
7. Kundur, D.; Feng, X.; Mashayekh, S.; Liu, S.; Zourntos, T.; Butler-Purry, K.L. Towards modelling the impact of cyber attacks on a smart grid. *Int. J. Secur. Netw.* **2011**, *6*, 2–13. [CrossRef]
8. Romanovsky, A.; Ishikawa, F. *Trustworthy Cyber-Physical Systems Engineering*; CRC Press: Boca Raton, FL, USA, 2016.
9. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. A survey on smart grid potential applications and communication requirements. *IEEE Trans. Ind. Inform.* **2012**, *9*, 28–42. [CrossRef]
10. Januário, F.; Cardoso, A.; Gil, P. A Distributed Multi-Agent Framework for Resilience Enhancement in Cyber-Physical Systems. *IEEE Access* **2019**, *7*, 31342–31357. [CrossRef]
11. Rajkumar, R.; Lee, I.; Sha, L.; Stankovic, J. Cyber-physical systems: The next computing revolution. In Proceedings of the Design Automation Conference, Anaheim, CA, USA, 13–18 June 2010; pp. 731–736.
12. Ali, S.; Qaisar, S.B.; Saeed, H.; Khan, M.F.; Naeem, M.; Anpalagan, A. Network challenges for cyber physical systems with tiny wireless devices: A case study on reliable pipeline condition monitoring. *Sensors* **2015**, *15*, 7172–7205. [CrossRef]
13. Jin, X.; Haddad, W.M.; Yucelen, T. An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems. *IEEE Trans. Autom. Control* **2017**, *62*, 6058–6064. [CrossRef]

14. SCADA. Electrical SCADA Market by Architecture (Hardware, Software, and Services), Component (Master Terminal unit, Remote Terminal unit, Human Machine Interface), Application (Generation, Transmission, and Distribution), and Region—Global Forecast to 2022. In *Markets and Markets*; SCAD: Abu Dhabi, United Arab Emirates, 2020.
15. Hernandez, L.; Baladron, C.; Aguiar, J.M.; Carro, B.; Sanchez-Esguevillas, A.J.; Lloret, J.; Massana, J. A survey on electric power demand forecasting: Future trends in smart grids, microgrids and smart buildings. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1460–1495. [CrossRef]
16. Colak, I.; Kabalci, E.; Fulli, G.; Lazarou, S. A survey on the contributions of power electronics to smart grid systems. *Renew. Sustain. Energy Rev.* **2015**, *47*, 562–579. [CrossRef]
17. Lei, H.; Singh, C. Power system reliability evaluation considering cyber-malfunctions in substations. *Electr. Power Syst. Res.* **2015**, *129*, 160–169. [CrossRef]
18. Siaterlis, C.; Genge, B. Cyber-Physical Testbeds. *Commun. ACM* **2014**, *57*, 64–73. [CrossRef]
19. Rajkumar, R. A cyber–physical future. *Proc. IEEE* **2012**, *100*, 1309–1312. [CrossRef]
20. Fink, G.A.; Edgar, T.W.; Rice, T.R.; MacDonald, D.G.; Crawford, C.E. Security and privacy in cyber-physical systems. In *Cyber-Physical Systems*; Elsevier: Amsterdam, The Netherlands, 2017; pp. 129–141.
21. Lei, H.; Singh, C. Developing a benchmark test system for electric power grid cyber-physical reliability studies. In Proceedings of the 2016 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Beijing, China, 16–20 October 2016; pp. 1–5.
22. Li, Z.; Kang, R. Strategy for reliability testing and evaluation of cyber physical systems. In Proceedings of the 2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Singapore, 6–9 December 2015; pp. 1001–1006.
23. Cintuglu, M.H.; Mohammed, O.A.; Akkaya, K.; Uluagac, A.S. A survey on smart grid cyber-physical system testbeds. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 446–464. [CrossRef]
24. El Mrabet, Z.; Kaabouch, N.; El Ghazi, H.; El Ghazi, H. Cyber-security in smart grid: Survey and challenges. *Comput. Electr. Eng.* **2018**, *67*, 469–482. [CrossRef]
25. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access* **2019**, *7*, 46595–46620. [CrossRef]
26. Tuballa, M.L.; Abundo, M.L. A review of the development of Smart Grid technologies. *Renew. Sustain. Energy Rev.* **2016**, *59*, 710–725. [CrossRef]
27. Bharothu, J.N.; Sridhar, M.; Rao, R.S. A literature survey report on Smart Grid technologies. In Proceedings of the 2014 International Conference on Smart Electric Grid (ISEG), Guntur, India, 19–20 September 2014; pp. 1–8.
28. Aravinthan, V.; Balachandran, T.; Ben-Idris, M.; Fei, W.; Heidari-Kapourchali, M.; Hettiarachchige-Don, A.; Jiang, J.N.; Lei, H.; Liu, C.C.; Mitra, J. Reliability modeling considerations for emerging cyber-physical power systems. In Proceedings of the 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Boise, ID, USA, 24–28 June 2018; pp. 1–7.
29. Marino, D.L.; Wickramasinghe, C.S.; Amarasinghe, K.; Challa, H.; Richardson, P.; Jillepalli, A.A.; Johnson, B.K.; Rieger, C.; Manic, M. Cyber and Physical Anomaly Detection in Smart-Grids. In Proceedings of the 2019 Resilience Week (RWS), San Antonio, TX, USA, 4–7 November 2019; Volume 1, pp. 187–193.
30. Babun, L.; Aksu, H.; Uluagac, A.S. A system-level behavioral detection framework for compromised cps devices: Smart-grid case. *ACM Trans. Cyber-Phys. Syst.* **2019**, *4*, 1–28. [CrossRef]
31. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on cyber security for smart grid communications. *IEEE Commun. Surv. Tutorials* **2012**, *14*, 998–1010. [CrossRef]
32. Madhan, E.; Ghosh, U.; Tosh, D.K.; Mandal, K.; Murali, E.; Ghosh, S. An Improved Communications in Cyber Physical System Architecture, Protocols and Applications. In Proceedings of the 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, 10–13 June 2019; pp. 1–6.
33. Ghosh, U.; Chatterjee, P.; Shetty, S.; Kamhoua, C.; Njilla, L. Towards secure software-defined networking integrated cyber-physical systems: Attacks and countermeasures. In *Cybersecurity and Privacy in Cyber-Physical Systems*; CRC Press: Boca Raton, FL, USA, 2019.
34. Sun, C.C.; Hahn, A.; Liu, C.C. Cyber security of a power grid: State-of-the-art. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 45–56. [CrossRef]
35. Jimada-Ojuolape, B.; Teh, J. Impact of the Integration of Information and Communication Technology on Power System Reliability: A Review. *IEEE Access* **2020**, *8*, 24600–24615. [CrossRef]
36. Panteli, M.; Kirschen, D.S. Assessing the effect of failures in the information and communication infrastructure on power system reliability. In Proceedings of the 2011 IEEE/PES Power Systems Conference and Exposition, Phoenix, AZ, USA, 20–23 March 2011; pp. 1–7.
37. Tornqvist, B.; Fontela, M.; Mellstrand, P.; Gustavsson, R.; Andrieu, C. Overview of ICT components and its application in electric power systems. In *Distributed Intelligence for Distributed Energy Resources: Selected Publications from the CRISP Project*; Vienna International Centre: Vienna, Austria, 2005.
38. Lei, H.; Chen, B.; Butler-Purry, K.L.; Singh, C. Security and reliability perspectives in cyber-physical smart grids. In Proceedings of the 2018 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia), Singapore, 22–25 May 2018; pp. 42–47.

39. Hsiao, Y.C.; López, J.; Hsiao, T.Y.; Lu, C.N. Considering ICT in reliability assessment of system protection scheme. In Proceedings of the 2015 18th International Conference on Intelligent System Application to Power Systems (ISAP), Porto, Portugal, 11–16 September 2015; pp. 1–6.
40. Sooriyabandara, M.; Ekanayake, J. Smart grid-technologies for its realisation. In Proceedings of the 2010 IEEE International Conference on Sustainable Energy Technologies (ICSET), Kandy, Sri Lanka, 6–9 December 2010; pp. 1–4.
41. Chen, B.; Wang, J.; Shahidehpour, M. Cyber—physical perspective on smart grid design and operation. *IET Cyber-Phys. Syst. Theory Appl.* **2018**, *3*, 129–141. [CrossRef]
42. Stahlhut, J.W.; Browne, T.J.; Heydt, G.T.; Vittal, V. Latency viewed as a stochastic process and its impact on wide area power system control signals. *IEEE Trans. Power Syst.* **2008**, *23*, 84–91. [CrossRef]
43. Rajhans, A.; Cheng, S.W.; Schmerl, B.; Garlan, D.; Krogh, B.H.; Agbi, C.; Bhave, A. An architectural approach to the design and analysis of cyber-physical systems. *Electron. Commun. EASST* **2009**, *21*.
44. Komura, T.; Nagai, Y.; Hashimoto, S.; Aoyagi, M.; Takahashi, K. Proposal of delegation using electronic certificates on single sign-on system with saml-protocol. In Proceedings of the 2009 Ninth Annual International Symposium on Applications and the Internet, Bellevue, WA, USA, 20–24 July 2009; pp. 235–238.
45. Cai, Y.; Tang, S. Security Scheme for Cross-Domain Grid: Integrating WS-Trust and Grid Security Mechanism. In Proceedings of the 2008 International Conference on Computational Intelligence and Security, Suzhou, China, 13–17 December 2008; Volume 1, pp. 453–457.
46. Perlman, R. An overview of PKI trust models. *IEEE Netw.* **1999**, *13*, 38–43. [CrossRef]
47. Jensen, M.; Sel, C.; Franke, U.; Holm, H.; Nordström, L. Availability of a SCADA/OMS/DMS system—A case study. In Proceedings of the 2010 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe), Gothenburg, Sweden, 11–13 October 2010; pp. 1–8.
48. Thomas, R.J. Putting an action plan in place. *IEEE Power Energy Mag.* **2009**, *7*, 26–31. [CrossRef]
49. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-physical systems security—A survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
50. Francia, G., III; Thornton, D.; Brookshire, T. *Cyberattacks on SCADA Systems*; Colloquium for Information Systems Security Education: Lutherville, MD, USA, 2012; pp. 9–14.
51. Paukatong, T. SCADA security: A new concerning issue of an in-house EGAT-SCADA. In Proceedings of the 2005 IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific, Dalian, China, 18 August 2005; pp. 1–5.
52. Wang, W.; Lu, Z. Cyber security in the smart grid: Survey and challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
53. Cleveland, F. Iec tc57 wg15: Iec 62351 security standards for the power system information infrastructure. In *White Paper*; IEEE: Dallas, TX, USA, 2012.
54. Cardenas, A.A.; Roosta, T.; Sastry, S. Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems. *Ad Hoc Netw.* **2009**, *7*, 1434–1447. [CrossRef]
55. Zhu, B.; Joseph, A.; Sastry, S. A taxonomy of cyber attacks on SCADA systems. In Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, 19–22 October 2011; pp. 380–388.
56. Anderson, R.; Fuloria, S. Who controls the off switch? In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 96–101.
57. Mo, Y.; Kim, T.H.J.; Brancik, K.; Dickinson, D.; Lee, H.; Perrig, A.; Sinopoli, B. Cyber—Physical security of a smart grid infrastructure. *Proc. IEEE* **2011**, *100*, 195–209.
58. Cho, S. Privacy and Authentication in Smart Grid Networks. Ph.D. Thesis, Department of Computer Science and Engineering, Stony Brook, NY, USA, 2014.
59. Alcaraz, C.; Zeadally, S. Critical control system protection in the 21st century. *Computer* **2013**, *46*, 74–83. [CrossRef]
60. Byres, E.J.; Franz, M.; Miller, D. The use of attack trees in assessing vulnerabilities in SCADA systems. In Proceedings of the International Infrastructure Survivability Workshop, Lisbon, Portugal, 5–8 December 2004; pp. 3–10.
61. Fovino, I.N.; Carcano, A.; Masera, M.; Trombetta, A. An experimental investigation of malware attacks on SCADA systems. *Int. J. Crit. Infrastruct. Prot.* **2009**, *2*, 139–145. [CrossRef]
62. East, S.; Butts, J.; Papa, M.; Shenoi, S. A Taxonomy of Attacks on the DNP3 Protocol. In Proceedings of the International Conference on Critical Infrastructure Protection, Arlington, VA, USA, 16–17 March 2009; Springer: Berlin, Germany, 2009; pp. 67–81.
63. Huitsing, P.; Chandia, R.; Papa, M.; Shenoi, S. Attack taxonomies for the Modbus protocols. *Int. J. Crit. Infrastruct. Prot.* **2008**, *1*, 37–44. [CrossRef]
64. Santamarta, R. Here be backdoors: A journey into the secrets of industrial firmware. In Proceedings of the Black Hat USA, Las Vegas, NV, USA, 6 August 2012.
65. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart grid—The new and improved power grid: A survey. *IEEE Commun. Surv. Tutor.* **2011**, *14*, 944–980. [CrossRef]
66. Yang, C.H.; Zhabelova, G.; Yang, C.W.; Vyatkin, V. Cosimulation environment for event-driven distributed controls of smart grid. *IEEE Trans. Ind. Inform.* **2013**, *9*, 1423–1435. [CrossRef]

67. Bera, S.; Misra, S.; Rodrigues, J.J. Cloud computing applications for smart grid: A survey. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *26*, 1477–1494. [CrossRef]
68. Genge, B.; Beres, A.; Haller, P. A survey on cloud-based software platforms to implement secure smart grids. In Proceedings of the 2014 49th International Universities Power Engineering Conference (UPEC), Cluj-Napoca, Romania, 2–5 September 2014; pp. 1–6.
69. Davis, J.; Magrath, S. *A Survey of Cyber Ranges and Testbeds*; Technical Report; Defence Science and Technology Organisation: Edinburgh, Australia, 2013.
70. 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. *arXiv* **2019**, arXiv:1911.01471.
71. 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]
72. Kuffel, R.; Giesbrecht, J.; Maguire, T.; Wierckx, R.; McLaren, P. RTDS-a fully digital power system simulator operating in real time. In Proceedings of the 1995 International Conference on Energy Management and Power Delivery EMPD'95, Singapore, 21–23 November 1995; Volume 2, pp. 498–503.
73. Stanovich, M.J.; Leonard, I.; Sanjeev, K.; Steurer, M.; Roth, T.P.; Jackson, S.; Bruce, M. Development of a smart-grid cyber-physical systems testbed. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6.
74. 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]
75. Adhikari, U.; Morris, T.H.; Pan, S. A cyber-physical power system test bed for intrusion detection systems. In Proceedings of the 2014 IEEE PES General Meeting | Conference & Exposition, National Harbor, MD, USA, 27–31 July 2014; pp. 1–5.
76. Version, P.S. *1.80: User's Guide*; West Virginia University: Morgantown, WV, USA, 1995.
77. Mallouhi, M.; Al-Nashif, Y.; Cox, D.; Chadaga, T.; Hariri, S. A testbed for analyzing security of SCADA control systems (TASSCS). In Proceedings of the ISGT 2011, Anaheim, CA, USA, 17–19 January 2011; pp. 1–7.
78. Nicol, D.; Davis, C.; Overbye, T. A virtual power system testbed for cyber-security decision support. In Proceedings of the 2009 INFORMS Simulation Society Workshop on Simulation: At the Interface of Modeling and Anaylsis, Coventry, UK, 25–27 June 2009; pp. 62–66.
79. Stamp, J.; Urias, V.; Richardson, B. Cyber security analysis for the power grid using the virtual control systems environment. In Proceedings of the 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24–28 July 2011; pp. 1–4.
80. *Anual and PowerFactory. Version 14.0*; DIgSILENT GmbH: Gomaringen, Germany, 2009.
81. Hong, J.; Wu, S.S.; Stefanov, A.; Fshosha, A.; Liu, C.C.; Gladyshev, P.; Govindarasu, M. An intrusion and defense testbed in a cyber-power system environment. In Proceedings of the 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24–28 July 2011; pp. 1–5.
82. Tong, H.; Ni, M.; Zhao, L.; Li, M. Flexible hardware-in-the-loop testbed for cyber physical power system simulation. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 374–381. [CrossRef]
83. Thomas, M.S.; McDonald, J.D. *Power System SCADA and Smart Grids*; CRC Press: Boca Raton, FL, USA, 2017.
84. Bergman, D.C.; Jin, D.K.; Nicol, D.M.; Yardley, T. The Virtual Power System Testbed and Inter-Testbed Integration. In Proceedings of the CSET'09: 2nd Conference on Cyber Security Experimentation and Test, Vancouver, BC, Canada, 10–14 August 2009.
85. 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]
86. Siaterlis, C.; Genge, B.; Hohenadel, M. EPIC: A testbed for scientifically rigorous cyber-physical security experimentation. *IEEE Trans. Emerg. Top. Comput.* **2013**, *1*, 319–330. [CrossRef]
87. Green, B.; Lee, A.; Antrobus, R.; Roedig, U.; Hutchison, D.; Rashid, A. Pains, gains and PLCs: Ten lessons from building an industrial control systems testbed for security research. In Proceedings of the 10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17), Vancouver, BC, Canada, 16–18 August 2017.
88. Gardiner, J.; Craggs, B.; Green, B.; Rashid, A. Oops I did it again: Further adventures in the land of ICS security testbeds. In Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy, London, UK, 11 November 2019; pp. 75–86.
89. Holm, H.; Karresand, M.; Vidström, A.; Westring, E. A survey of industrial control system testbeds. In Proceedings of the Nordic Conference on Secure IT Systems, Stockholm, Sweden, 19–21 October 2015; pp. 11–26.
90. Kavak, H.; Padilla, J.J.; Vernon-Bido, D. A characterization of cybersecurity simulation scenarios. In Proceedings of the CNS '16: 19th Communications & Networking Symposium, Pasadena, CA, USA, 3–6 April 2016; p. 3.
91. Koutsandria, G.; Gentz, R.; Jamei, M.; Scaglione, A.; Peisert, S.; McParland, C. A real-time testbed environment for cyber-physical security on the power grid. In Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, Denver, CO, USA, 12–16 October 2015; pp. 67–78.
92. Candell, R.; Zimmerman, T.; Stouffer, K. An industrial control system cybersecurity performance testbed. *Natl. Inst. Stand. Technol. NISTIR* **2015**, *8089*.
93. Gao, H.; Peng, Y.; Dai, Z.; Wang, T.; Han, X.; Li, H. An industrial control system testbed based on emulation, physical devices and simulation. In Proceedings of the International Conference on Critical Infrastructure Protection, Arlington, VA, USA, 17–19 March 2014; pp. 79–91.

94. Urias, V.; Van Leeuwen, B.; Richardson, B. Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed. In Proceedings of the MILCOM 2012—2012 IEEE Military Communications Conference, Orlando, FL, USA, 29 October–1 November 2012; pp. 1–8.
95. Hankin, C.; Chana, D.; Green, B.; Khan, R.; Popov, P.; Rashid, A.; Sezer, S. *Open Testbeds for CNI*; Lancaster University: Lancaster, UK, 2018.
96. Gao, H.; Peng, Y.; Jia, K.; Dai, Z.; Wang, T. The design of ics testbed based on emulation, physical, and simulation (eps-ics testbed). In Proceedings of the 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Beijing, China, 16–18 October 2013; pp. 420–423.
97. Geng, Y.; Wang, Y.; Liu, W.; Wei, Q.; Liu, K.; Wu, H. A survey of industrial control system testbeds. In *IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2019; Volume 569, p. 042030.
98. Vellaithurai, C.; Biswas, S.; L.R.; A, S. Real Time Modeling and Simulation of Cyber-Power System. In *Cyber Physical Systems Approach to Smart Electric Power Grid*; Power Systems; Springer: Berlin, Germany, 2015; Volume 1.
99. Youssef, T.A.; Elsayed, A.T.; Mohammed, O.A. DDS based interoperability framework for smart grid testbed infrastructure. In Proceedings of the 2015 IEEE 15th International Conference on Environment and Electrical Engineering (EEEIC), Rome, Italy, 10–13 June 2015; pp. 219–224.
100. Cebula, J.L.; Young, L.R. *A Taxonomy of Operational Cyber Security Risks*; Technical Report; Software Engineering Institute: Pittsburgh, PA, USA, 2010.
101. Albunashee, H.; Farnell, C.; Suchanek, A.; Haulmark, K.; McCann, R.; Di, J.; Mantooth, A. A Testbed for Detecting False Data Injection Attacks in Systems with Distributed Energy Resources. *IEEE J. Emerg. Sel. Top. Power Electron.* **2019**. [CrossRef]
102. Fovino, I.N.; Masera, M.; Guidi, L.; Carpi, G. An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants. In Proceedings of the 3rd International Conference on Human System Interaction, Rzeszow, Poland, 13–15 May 2010; pp. 679–686.
103. Barnes, K.; Johnson, B. *National SCADA Test Bed Substation Automation Evaluation Report*; Technical Report; Idaho National Laboratory (INL): Idaho Falls, ID, USA, 2009.
104. Palaniswamy, P.; McMillin, B. Cyber-physical security of an electric microgrid. In Proceedings of the 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Taipei, Taiwan, 4–7 December 2018; pp. 74–83.
105. Korkmaz, E.; Dolgikh, A.; Davis, M.; Skormin, V. ICS security testbed with delay attack case study. In Proceedings of the MILCOM 2016—2016 IEEE Military Communications Conference, Baltimore, MD, USA, 1–3 November 2016; pp. 283–288.
106. Korkmaz, E.; Dolgikh, A.; Davis, M.; Skormin, V. Industrial control systems security testbed. In Proceedings of the 11th Annual Symposium on Information Assurance, Albany, NY, USA, 8–9 June 2016.
107. Korkmaz, E.; Davis, M.; Dolgikh, A.; Skormin, V. Detection and mitigation of time delay injection attacks on industrial control systems with PLCs. In Proceedings of the International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, Warsaw, Poland, 28–30 August 2017; pp. 62–74.
108. Amarasinghe, K.; Wickramasinghe, C.; Marino, D.; Rieger, C.; Manicl, M. Framework for data driven health monitoring of cyber-physical systems. In Proceedings of the 2018 Resilience Week (RWS), Denver, CO, USA, 20–23 August 2018; pp. 25–30.
109. Elbez, G.; Keller, H.B.; Hagenmeyer, V. A Cost-efficient Software Testbed for Cyber-Physical Security in IEC 61850-based Substations. In Proceedings of the 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aalborg, Denmark, 29–31 October 2018; pp. 1–6.
110. Elbez, G.; Keller, H.B.; Hagenmeyer, V. Authentication of GOOSE Messages under Timing Constraints in IEC 61850 Substations. In Proceedings of the 6th International Symposium for ICS & SCADA Cyber Security Research, Athens, Greece, 10–12 September 2019; Volume 6, pp. 137–143.
111. 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.
112. Duggan, D.; Berg, M.; Dillinger, J.; Stamp, J. *Penetration Testing of Industrial Control Systems*; Sandia National Laboratories: Albuquerque, NM, USA, 2005.
113. McMahon, E.; Patton, M.; Samtani, S.; Chen, H. Benchmarking Vulnerability Assessment Tools for Enhanced Cyber-Physical System (CPS) Resiliency. In Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA, 9–11 November 2018; pp. 100–105.
114. Tran, V.P.; Kamalasadan, S.; Enslin, J. Real-time modeling and model validation of synchronous generator using synchrophasor measurements. In Proceedings of the 2013 North American Power Symposium (NAPS), Manhattan, KS, USA, 22–24 September 2013; pp. 1–5.
115. Singh, P.; Garg, S.; Kumar, V.; Saquib, Z. A testbed for SCADA cyber security and intrusion detection. In Proceedings of the 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 5–7 August 2015; pp. 1–6.
116. Oyewumi, I.A.; Challa, H.; Jillepalli, A.A.; Richardson, P.; Chakhchoukh, Y.; Johnson, B.K.; Conte de Leon, D.; Sheldon, F.T.; Haney, M.A. Attack Scenario-based Validation of the Idaho CPS Smart Grid Cybersecurity Testbed (ISAAC). In Proceedings of the 2019 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 7–8 February 2019; pp. 1–6. [CrossRef]

117. Oyewumi, I.A.; Jillepalli, A.A.; Richardson, P.; Ashrafuzzaman, M.; Johnson, B.K.; Chakhchoukh, Y.; Haney, M.A.; Sheldon, F.T.; de Leon, D.C. ISAAC: The idaho CPS smart grid cybersecurity testbed. In Proceedings of the 2019 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 7–8 February 2019; pp. 1–6.
118. Momen, A.; Chakhchoukh, Y.; Johnson, B.K. Series Compensated Line Parameters Estimation Using Synchrophasor Measurements. *IEEE Trans. Power Deliv.* **2019**, *34*, 2152–2162. [CrossRef]
119. Ashok, A.; Hahn, A.; Govindarasu, M. A cyber-physical security testbed for smart grid: System architecture and studies. In Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, TN, USA, 12–14 October 2011; p. 1.
120. Hahn, A.; Govindarasu, M. An evaluation of cybersecurity assessment tools on a SCADA environment. In Proceedings of the 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24–28 July 2011; pp. 1–6.
121. Ashok, A.; Sridhar, S.; McKinnon, A.D.; Wang, P.; Govindarasu, M. Testbed-based performance evaluation of attack resilient control for agc. In Proceedings of the 2016 Resilience Week (RWS), Chicago, IL, USA, 16–18 August 2016; pp. 125–129.
122. Hong, J.; Liu, C.C.; Govindarasu, M. Detection of cyber intrusions using network-based multicast messages for substation automation. In Proceedings of the ISGT 2014, Washington, DC, USA, 19–22 February 2014; pp. 1–5.
123. Hong, J.; Liu, C.C. Intelligent electronic devices with collaborative intrusion detection systems. *IEEE Trans. Smart Grid* **2017**, *10*, 271–281. [CrossRef]
124. Sun, C.C.; Hong, J.; Liu, C.C. A coordinated cyber attack detection system (CCADS) for multiple substations. In Proceedings of the 2016 Power Systems Computation Conference (PSCC), Genoa, Italy, 20–24 June 2016; pp. 1–7.
125. Sun, C.C.; Hong, J.; Liu, C.C. A co-simulation environment for integrated cyber and power systems. In Proceedings of the 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, USA, 2–5 November 2015; pp. 133–138.
126. Biswas, S.S.; Kim, J.H.; Srivastava, A.K. Development of a smart grid test bed and applications in PMU and PDC testing. In Proceedings of the 2012 North American Power Symposium (NAPS), Champaign, IL, USA, 9–11 September 2012; pp. 1–6.
127. 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]
128. Liu, R.; Srivastava, A. Integrated simulation to analyze the impact of cyber-attacks on the power grid. In Proceedings of the 2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Seattle, WA, USA, 13 April 2015; pp. 1–6.
129. Krishnan, V.; Gopal, S.; Nie, Z.; Srivastava, A. Cyber-power testbed for distributed monitoring and control. In Proceedings of the 2018 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Porto, Portugal, 10 April 2018; pp. 1–6.
130. Venkataramanan, V.; Hahn, A.; Srivastava, A. CP-SAM: Cyber-physical security assessment metric for monitoring microgrid resiliency. *IEEE Trans. Smart Grid* **2019**, *11*, 1055–1065. [CrossRef]
131. Glover, S.; Neely, J.; Lentine, A.; Finn, J.; White, F.; Foster, P.; Wasynczuk, O.; Pekarek, S.; Loop, B. Secure scalable microgrid test bed at sandia national laboratories. In Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), Bangkok, Thailand, 27–31 May 2012; pp. 23–27.
132. Van Leeuwen, B.; Urias, V.; Eldridge, J.; Villamarin, C.; Olsberg, R. Cyber security analysis testbed: Combining real, emulation, and simulation. In Proceedings of the 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, San Jose, CA, USA, 5–8 October 2010; pp. 121–126.
133. Crussell, J.; Kroeger, T.M.; Brown, A.; Phillips, C. Virtually the same: Comparing physical and virtual testbeds. In Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 18–21 February 2019; pp. 847–853.
134. Mazloomzadeh, A.; Cintuglu, M.H.; Mohammed, O.A. Development and evaluation of a laboratory based phasor measurement devices. In Proceedings of the 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–20 February 2015; pp. 1–5.
135. Becejac, T.; Eppinger, C.; Ashok, A.; Agrawal, U.; O'Brien, J. PRIME: A real-time cyber-physical systems testbed: from wide-area monitoring, protection, and control prototyping to operator training and beyond. *IET Cyber-Phys. Syst. Theory Appl.* **2020**, *5*. [CrossRef]
136. Sauer, F.; Niedermaier, M.; Kiessling, S.; Merli, D. LICSTER—A Low-cost ICS Security Testbed for Education and Research. *arXiv* **2019**, arXiv:abs/1910.00303.
137. Lo Bello, L.; Mirabella, O.; Raucea, A. Design and Implementation of an Educational Testbed for Experiencing With Industrial Communication Networks. *Ind. Electron. IEEE Trans.* **2008**, *54*, 3122–3133. [CrossRef]
138. Younan, M.; Khattab, S.; Bahgat, R. A wot testbed for research and course projects. In *Managing the Web of Things*; Elsevier: Amsterdam, The Netherlands, 2017; pp. 181–204.
139. Annor-Asante, M.P. Development of Smart Grid Testbed with Low-Cost Hardware and Software for Cybersecurity Research and Education. *Wirel. Pers Commun.* **2018**, *101*, 1357–1377. [CrossRef]
140. Ahmed, I.; Obermeier, S.; Naedele, M.; Richard III, G.G. SCADA Systems: Challenges for Forensic Investigators. *Computer* **2012**, *45*, 44–51. [CrossRef]

141. Spyridopoulos, T.; Tryfonas, T.; May, J. Incident analysis digital forensics in SCADA and industrial control systems. In Proceedings of the 8th IET International System Safety Conference incorporating the Cyber Security Conference 2013, Cardiff, UK, 16–17 October 2013; pp. 1–6.
142. Kilpatrick, T.; González, J.; Chandia, R.; Papa, M.; Shenoi, S. Forensic analysis of SCADA systems and networks. *IJSN* **2008**, *3*, 95–102. [CrossRef]
143. Evangelopoulou, M.; Johnson, C.; Harkness, R. Forensic Attacks Analysis and the Cyber Security of Safety-Critical Industrial Control Systems. In Proceedings of the 34th International System Safety Conference, Orlanda, FL, USA, 8–12 August 2016.
144. Karabiyik, U.; Celebi, N.; Yildiz, F.; Holekamp, J.; Rabieh, K. Forensic Analysis of SCADA/ICS System with Security and Vulnerability Assessment. In Proceedings of the 2018 ASEE Annual Conference & Exposition, Salt Lake City, UT, USA, 24–27 June 2018.
145. Iqbal, A.; Mahmood, F.; Ekstedt, M. Digital Forensic Analysis of Industrial Control Systems Using Sandboxing: A Case of WAMPAC Applications in the Power Systems. *Energies* **2019**, *12*, 2598. [CrossRef]
146. Ahmed, I.; Roussev, V.; Johnson, W.; Senthivel, S.; Sudhakaran, S. A SCADA System Testbed for Cybersecurity and Forensic Research and Pedagogy. In Proceedings of the Proceedings of the 2nd Annual Industrial Control System Security Workshop, Los Angeles, CA, USA, 6 December 2016; pp. 1–9.
147. Chromik, J.; Remke, A.; Haverkort, B. An integrated testbed for locally monitoring SCADA systems in smart grids. *Energy Inform.* **2018**, *1*. [CrossRef]
148. Giani, A.; Karsai, G.; Roosta, T.; Shah, A.; Sinopoli, B.; Wiley, J. A testbed for secure and robust SCADA systems. *ACM SIGBED Rev.* **2008**, *5*, 4. [CrossRef]
149. Pourbeik, P. Approaches to validation of power system models for system planning studies. In Proceedings of the IEEE PES General Meeting, Minneapolis, MN, USA, 25–29 July 2010; pp. 1–10.
150. Koganti, V.S.; Ashrafuzzaman, M.; Jillepalli, A.A.; Sheldon, F.T. A virtual testbed for security management of industrial control systems. In Proceedings of the 2017 12th International Conference on Malicious and Unwanted Software (MALWARE), Fajardo, PR, USA, 11–14 October 2017; pp. 85–90.
151. Chertov, R.; Fahmy, S.; Shroff, N.B. Fidelity of network simulation and emulation: A case study of tcp-targeted denial of service attacks. *ACM Trans. Model. Comput. Simul. (TOMACS)* **2009**, *19*, 1–29. [CrossRef]
152. Wang, C.; Fang, L.; Dai, Y. A simulation environment for SCADA security analysis and assessment. In Proceedings of the 2010 International Conference on Measuring Technology and Mechatronics Automation, Changsha, China, 13–14 March 2010; Volume 1, pp. 342–347.
153. Asadollah, S.A.; Inam, R.; Hansson, H. A survey on testing for cyber physical system. In Proceedings of the IFIP International Conference on Testing Software and Systems, Sharjah and Dubai, United Arab Emirates, 23–25 November 2015; pp. 194–207.
154. Liu, Y.; Peng, Y.; Wang, B.; Yao, S.; Liu, Z. Review on cyber-physical systems. *IEEE/CAA J. Autom. Sin.* **2017**, *4*, 27–40. [CrossRef]