energies

MDPI

Article

Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid †

Matthew Boeding [1], Kelly Boswell [1], Michael Hempel [1], Hamid Sharif [1,*], Juan Lopez, Jr. [2] and Kalyan Perumalla [2]

[1] Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Lincoln, NE 68588, USA
[2] Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA
* Correspondence: hsharif@unl.edu
† This manuscript has been authored by UT-Battelle, LLC, under contract DE-AC05-00OR22725 with the US Department of Energy (DOE). The publisher acknowledges the US government license to provide public access under the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan).

Abstract: The convergence of Information Technologies and Operational Technology systems in industrial networks presents many challenges related to availability, integrity, and confidentiality. In this paper, we evaluate the various cybersecurity risks in industrial control systems and how they may affect these areas of concern, with a particular focus on energy-sector Operational Technology systems. There are multiple threats and countermeasures that Operational Technology and Information Technology systems share. Since Information Technology cybersecurity is a relatively mature field, this paper emphasizes on threats with particular applicability to Operational Technology and their respective countermeasures. We identify regulations, standards, frameworks and typical system architectures associated with this domain. We review relevant challenges, threats, and countermeasures, as well as critical differences in priorities between Information and Operational Technology cybersecurity efforts and implications. These results are then examined against the recommended National Institute of Standards and Technology framework for gap analysis to provide a complete approach to energy sector cybersecurity. We provide analysis of countermeasure implementation to align with the continuous functions recommended for a sound cybersecurity framework.

Keywords: smart grid; industrial control systems; industrial internet of things; cybersecurity; security; supervisory control and data acquisition; distributed control systems

Citation: Boeding, M.; Boswell, K.; Hempel, M.; Sharif, H; Lopez, J., Jr.; Perumalla, K Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid. *Energies* **2022**, *15*, 8692. https://doi.org/10.3390/en15228692

Academic Editor: Adel Merabet

Received: 20 October 2022
Accepted: 15 November 2022
Published: 19 November 2022

1. Introduction

Industrial Control Systems (ICS) entities are increasingly facing greater business demands to operate more efficiently, and in the United States,they are also under greater regulatory pressures as well. The Energy Independence and Security Act of 2007 [1] gave the Federal Energy Regulatory Commission (FERC) and the National Institute of Standards and Technology (NIST) responsibilities to develop smart grid guidelines and standards. Furthermore, FERC has certified that North American Electric Reliability Corporation (NERC) is responsible for developing Critical Infrastructure Protection (CIP) cybersecurity standards [2]. At the time of this writing, NERC has developed 12 CIP standards that are subject to enforcement. Furthermore, nuclear power generation facilities are governed by more laws, regulations, and standards as well. As a result, ICS operators have increasingly integrated Information Technology (IT) solutions with Operations Technology (OT), in order to meet demand. However, this so-called IT/OT convergence has exposed these once air-gapped OT networks to the Internet, where they are vulnerable to cyber attacks. The differences between IT and OT and their convergence are examined in depth by Kayan et al. in [3].

Since most OT assets were not designed with security in mind [4], ICS networks will benefit most by following a Defense-in-Depth (DiD) strategy with a De-Militarized Zone (DMZ) between the Enterprise Zone and the Manufacturing Zone, as shown in Figure 1. This provides some isolation of the OT network while specifically only allowing the network traffic that is needed to enable authorized parties to remotely monitor and control OT assets into the OT network. However, for proper defense-in-depth the OT section of the network architecture likely requires new or improved security controls for the devices, software, and communication protocols that are commonly utilized in these networks [5]. However, this is particularly challenging for OT networks, because new security measures will likely introduce more latency, while this additional latency in IT networks is normally acceptable, in OT networks it can easily become a productivity concern, as well as a safety concern in terms of human lives and/or the environment [6]. Ideally there would be a one-size-fits-all approach for ICS entities to establish a cybersecurity governance and management program. However, each organization must approach a cybersecurity program incrementally and strategically to account for various factors, including its work force, culture, finances, risk tolerance, as well as its current cybersecurity posture and the assets it manages.

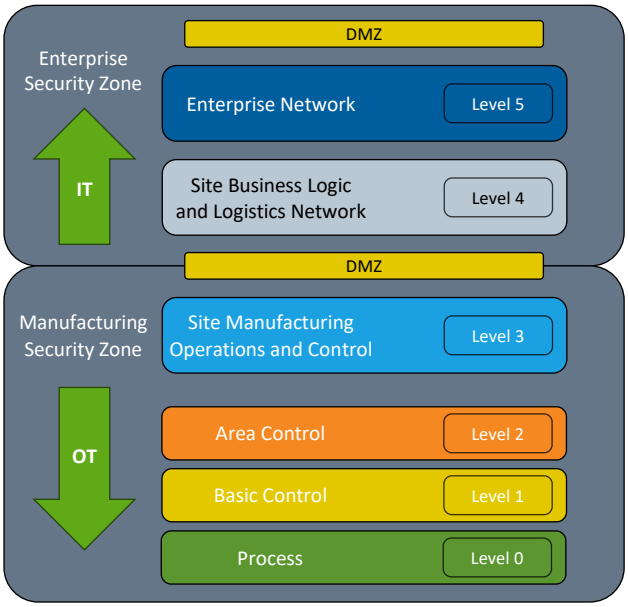

Figure 1. Common Architectural Zones.

With regards to managed assets, organizations must approach IT and OT cybersecurity differently as well. In IT-only networks, data is the primary commodity, and hence confidentiality is the highest priority, followed by integrity and availability. In OT networks, however, the primary objective is to maintain physical operations at optimal conditions, and to prevent physical harm to devices, but more importantly people and property. OT solutions are the path to achieving those objectives, and hence availability is typically of the highest priority [5], followed by integrity and confidentiality [7]. This prioritization is driven by the need to protect equipment and people. In order to quickly respond to abnormal behavior within the OT-monitored system, highly reliable low-latency communication are needed. Therefore, even a short degradation of availability can have disastrous consequences.

It sometimes, however, may be necessary for some organizations to adopt slightly different priorities, based on their architecture, assets, and configurations. In order to assist ICS entities to flexibly approach the establishment of a cybersecurity governance and management program, and to strategically manage risks, NIST has developed the Cybersecurity Framework (CSF). More specifically applicable to the energy sector, the US Dept of Energy has released the Cybersecurity Capability Maturity Model (C2M2) [8],

which aims to guide organizations through the process of assessing and furthering their cybersecurity posture.

A survey of primary cybersecurity concepts and principal threat taxonomy in Industrial Cyber-Physical Systems (ICPS) is provided in [3]. The paper broadly focuses on an introduction to cybersecurity concepts as they relate to ICPS, highlights prominent protocols, and presents categories of countermeasures as they relate broadly to ICPS. This focus on ICPS, however, results in a broad, high-level analysis of mostly IT-driven cybersecurity aspects within the ICPS domain. This includes an outline of the convergence of IT and OT systems and the effects on cybersecurity posture explored in academic research. They also identified available research into general testbeds and datasets for evaluation of cybersecurity proposals. However, the work presented in [3] is a broad high-level review without a focus on application domains. Therefore, our focus is specifically on the energy sector—a critical infrastructure sector and a cornerstone of our modern society. In this paper, we identify potential threats, industry guidelines and cybersecurity frameworks that are driven by the unique challenges and opportunities found in this key application domain. These frameworks are not only applicable to the energy sector, but can equally be of benefit in other ICS sectors.

In related works, some broad cybersecurity threads and solutions are given in [9–12]. In [13], several denial-of-service (DoS) attack taxonomies for the Smart Grid (SG) are defined and some potential solutions are explored. In [14], applications of blockchain for cybersecurity solutions in the smart grid are explored. The various communications architectures, technologies, protocols, cyber threats, and countermeasures are explored in [15–20]. In [21], a taxonomy of false data injection attack (FDIA) detection algorithms is presented and evaluated. In [22,23], some cyber threats and countermeasures related to time synchronization of measurement devices are presented.

In this paper, we focus on OT security issues, as the IT security issues are already well-covered by the IT industry. In particular, we focus on OT security issues in the energy sector, primarily in power generation and distribution systems, while significant research exists on OT cybersecurity, this survey is the first to review existing OT cybersecurity threats, countermeasures, and industry sector guidance to strengthen cybersecurity posture with primary applicability to the North American energy sector. This paper illustrates differences in priority assignment for confidentiality, integrity and availability between IT and OT networks, as a motivator for different cybersecurity approaches between the two domains. We provide an evaluation of known cybersecurity threats and their countermeasures, with a focus on OT specific threats and examine the recommended gap analysis provided by NIST.

The remainder of this paper is organized as follows. In Section 2, a survey of energy sector ICS security governance is provided. In Section 3 we provide some reference network architectures for OT networks. Section 4 presents a survey of security threats for OT networks. In Section 5, we provide a survey of countermeasures proposed in the literature. In Section 6, we analyze the current state of OT network security mitigation strategies (i.e., by assuming the countermeasures in the current literature may be applied), by analyzing how well they will assist entities to further manage cybersecurity risk. Finally, some concluding remarks are provided in Section 7.

2. Power Grid Cybersecurity Governance

Organizations responsible for the generation, transmission, and distribution of electrical energy are subject to a variety of laws, regulations, policies, standards, and guidelines. Ideally, there can be one universal governance framework for the Energy ICS sector. However, the reality is that each organization must determine its own governance structure based on its culture and existing organizational model. Furthermore, there is no single authority within an organization to determine the correct governance framework. However, the NIST Cybersecurity Framework [24] and the DoE C2M2 [8] are both valuable tools for each organization to strategically develop an appropriate cybersecurity governance and management framework. A list of available governance is outlined in Table 1.

Table 1. Summary of Regulations, Standards, and Guidance for the U.S. Energy Grid.

Regulation, Standard, or Guideline	Summary	Category
U.S. Regulation	Energy Policy Act of 2005	Statutory
U.S. Regulation	Energy Independence and Security Act of 2007	Statutory
NERC CIP Standards	Enforceable set of standards for the Bulk Energy System	Standard
DHS Nuclear Reactor Cybersecurity	Cybersecurity Framework Implementation Guidance for U.S. Nuclear Power Reactors	Guidance
ES-C2M2	Electricity Subsector Capability Maturity Model	Guidance
DoE	Energy Sector Cybersecurity Framework Implementation Guidance	Guidance
NIST CSWP 04162018	Framework for Improving Critical Infrastructure Cybersecurity	Guidance
NIST TN 2051	Smart Grid Profile of the NIST Framework	Guidance
NIST SP 1800-23	Energy Sector Asset Management	Guidance
NIST IR 7628	Guidelines for Smart Grid Cybersecurity	Guidance
NIST SP 1108r3	NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0	Standard
IEEE C37.1	Standards for SCADA and Automation Systems	Standard
IEEE 1379	Recommended Practice for Data Communications between RTUs and IEDs	Guidance
IEEE 1646	Standard Communication Delivery Time Performance Requirements or Electric Power Substation Automation	Standard
IEEE 1686	Standard for Intelligent Electronic Devices Cyber Security Capabilities	Standard
IEEE 692	Standard for Criteria for Security Systems for Nuclear Power Generating Stations	Standard
IEEE 1547.3	Guide for Monitoring, Information Exchange, and Control of Distributed Resources	Guidance
IEEE P1711	Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links	Standard
IEEE P2030	IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads	Guidance
IEEE P1901	High Speed Power Line Communications	Standard
IEC 61850	IED Communications (e.g., GOOSE)	Standard
IEC 62351	Security of Communication Protocols	Standard
IEC 62541	OPC Unified Architecture Security Model	Standard
ANSI C12	Metering Protocol	Standard
IEEE C37.118	Synchrophasor Measurements	Standard
IEC 60870	Family of Protocols for SCADA Communications	Standard
IEEE 1815	DNP3 Protocol	Standard
Modbus	Modbus Protocol	Standard
NRC Regulatory Guide 5.83	Cybersecurity Event Notifications	Guidance
NRC Regulatory Guide 5.71	Cybersecurity Programs for Nuclear Facilities	Guidance

The NIST Cybersecurity Framework Core is comprised of four areas: Functions, Categories, Subcategories, and References. The Functions represent a typical cybersecurity lifecycle with the following stages: Identify, Protect, Detect, Respond, and Recover. Each of

these Functions are divided into Categories that are the next layer of granularity of each lifecycle stage. Each of the Categories are further divided into another level of granularity called Subcategories. Subcategories provide context to each category with reference to other frameworks such as ISO, ISA, etc.

The NIST CSF also provides a scaled ranking system for organizations to evaluate the degree to which its cybersecurity risk management practices exhibit the characteristics defined in the framework in the following categories: Risk Management Process, Integrated Risk Management Program, and External Participation. The values in the scale are called Tiers and the values range from 1 to 4, 1 being the lowest level of implementation.

Lastly, the NIST CSF Profiles are a method by which organizations evaluate their current cybersecurity posture. These profiles furthermore allow organizations to determine recommended next steps for implementation that would help them to achieve their desired cybersecurity posture. It represents an alignment of the CSF Core with the organization's business requirements, capabilities, and risk appetite. For example, NIST provides a Profile for the Smart Grid in [25].

The C2M2 is a maturity model comprised of a set of common cybersecurity practices that may be used to evaluate, prioritize, and improve an organization's cybersecurity capabilities. It was derived from the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) [8], which was developed in response to the U.S. government's initiative to improve the cybersecurity posture of its critical infrastructure.

In 2005, the United States Energy Policy Act was signed by the Bush administration. It mandates the FERC to certify an Electricity Reliability Organization (ERO) to develop bulk power grid reliability standards to be enforced by FERC. Shortly after, FERC certified the NERC as the ERO. NERC's set of standards for the bulk power system are called the NERC Critical Infrastructure Protection (CIP) standards. At the time of this writing, there are 12 enforceable NERC CIP standards, 11 relating to cybersecurity and 1 relating to physical security [2]. Other than standards relating to nuclear facilities, these are the only set of enforceable standards for the power grid in the United States.

The NERC CIP standards define which entities will materially impact the reliability of the bulk power system if they are compromised. Any entities that meet the inclusion criteria and none of the exclusion criteria defined in CIP-002 are referred to as a Bulk Electric System (BES). The CIP standards require that BES entities identify their critical assets, and to regularly perform risk analysis on them. BES entities are required to establish an Electronic Security Perimeter (ESP) by creating appropriate firewall rules and policies, enforcing IT controls to protect critical assets, and implementing cyber attack monitoring tools. They are also required to regularly patch software and firmware vulnerabilities, use IDS/IPS tools, use antivirus and anti-malware tools, generate alarms on detected cyber events, and use secure account and password management. The standards also define requirements for establishing a cybersecurity policy and program, training personnel, establishing access controls for personnel, establishing an incident reporting and response planning program, and establishing recovery plans for critical assets and data.

The NERC CIP standards are the primary external influence of cybersecurity governance for Bulk Electric Systems. However, nuclear power generation systems are further governed by additional laws, regulations, and standards. These are primarily the Nuclear Regulatory Commission (NRC) regulation 10 CFR, Nuclear Energy Institute (NEI) standards 08-09, 10-04, 10-08, 10-09, and 13-10, and NRC Regulatory Guide 5.71. The US Department of Homeland Security (DHS) guideline titled "Nuclear Sector Cybersecurity Framework Implementation Guidance for U.S. Nuclear Power Reactors" is a useful tool to assist organizations with strategically implementing a cybersecurity program with respect to the applicable laws, regulations, standards and the NIST CSF.

Besides these, the following International Society of Automation (ISA) and International Electrotechnical Commission (IEC) standards are also important for cybersecurity management of the Smart Grid: ISA/IEC 62443, IEC 62351, IEC 62541, IEC 614500-25, IEC 62056-5-3 and ISO/IEC 14543. The IEC standards are available at a cost to organizations

and individuals but unlike the NERC CIP standards they are not enforceable. The ISA/IEC 62443 is a framework of standards whose goals are to improve the Confidentiality, Integrity, and Availability of general Industrial Automation and Control systems. The ISA/IEC 62351 are a framework of standards for improving the cybersecurity of communication system protocols used in power systems. IEC 62541, aka the OPC Unified Architecture, is a client-server based Machine-to-Machine (M2M) communication protocol for general Industrial Automation and Control systems.

Furthermore, the following Institute of Electrical and Electronics Engineers (IEEE) standards are also important for cybersecurity management of Smart Grid systems: IEEE 1646, IEEE 1686, IEEE 2030, and IEEE 1402.

3. Power Grid ICS Network Architectures

ICS Networks should be logically separated into the following zones [26]:

- Level 5 , Enterprise Network—Used for managing business-related activities.
- Level 4, Site Planning and Logistics Network—Used for managing production work flows.
- Level 3, Site Manufacturing Operations and Control—Used to manage control plant operations that produce the desired end product.
- Level 2, Area Control—Used for supervising, monitoring, and controlling the physical processes.
- Level 1, Basic Control—Sensing and manipulating the physical processes.
- Level 0, Physical Process—The physical process happens here.

As depicted in Figure 1, the OT network resides in Levels 0–2 while the IT network resides in Levels 3–5.

Since IT-OT convergence is a relatively new phenomenon, many Operational Technologies are still insecure by design [4]. IT technologies have evolved alongside the various threats to networking and computing technologies while OT networks were isolated until relatively recently. In [26], CISA recommends various traditional methods to implement a defense-in-depth strategy at the enterprise zone. This differs compared to traditional IT security services, shown in CISA's recommended firewall rule set layer, depicted in Figure 2. In particular, they recommend the use of a DMZ to provide logical separation of the enterprise zone from the Internet; virtual private networks to secure remote access connections; firewalls to restrict connections to trusted entities and content between zones; and various host security controls such as antivirus software, patch management, intrusion detection systems, etc.

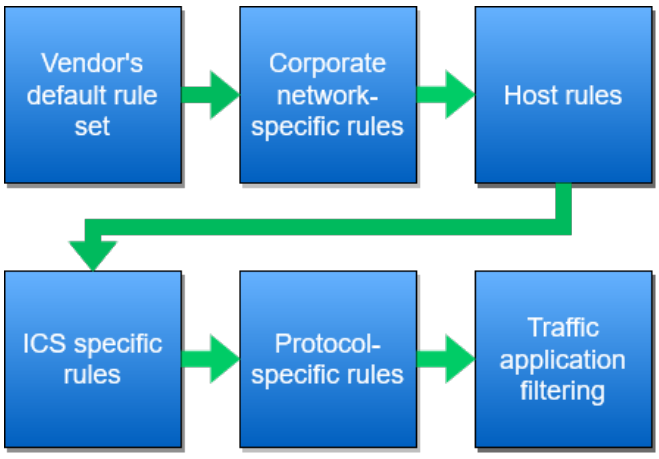

Figure 2. CISA Recommended Firewall Rule Set Layers.

While the above defense-in-depth strategy is a great start to securing ICS networks, the OT portion of the network may still require additional security controls to improve an organization's overall risk posture. Organizations responsible for power transmission and distribution are responsible for assets distributed over vast geographical areas. Therefore,

these systems typically use SCADA technologies to monitor and control these distributed systems. A typical SCADA system is shown in Figure 3.

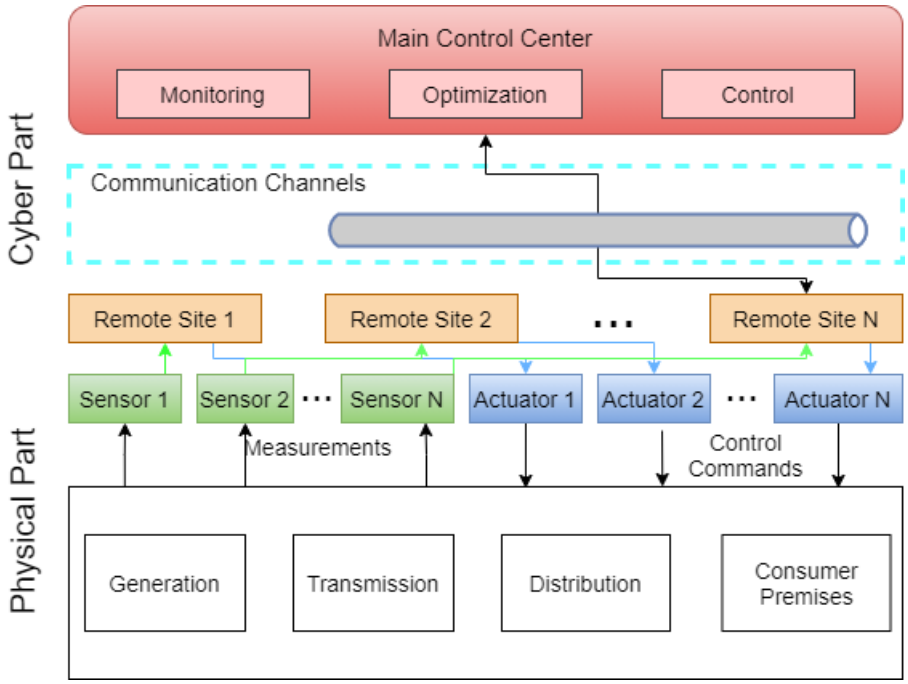

Figure 3. Typical Power SCADA Architecture.

Beyond the transmission and distribution domains in the smart grid, there are also the generation, customer, markets, operations, and service provider domains as defined in the NIST Smart Grid Framework 3.0 [27]. The domains that are of primary concern in this paper are the transmission, distribution, operations and customer domains of the smart grid. The next two sections of this paper will focus on the potential cyber threats to the Smart Grid and potential countermeasures.

4. Cybersecurity Threats in Energy System OT Networks

Cybersecurity threats in Energy System OT Networks may be categorized by the security services targeted by the attack. From a risk perspective, it is also particularly useful to order these services by priority. In OT networks, systems not only govern critical operational processes, such as manufacturing machinery, power generators and distributions systems, but may also be responsible for the safety of workers or, in the case of smart grids, perform time critical tasks to prevent cascading failures and facilitate a key service on which national security is built. A failure in the power grid not only puts people's lives at risk, but can have disastrous impact on everything from transportation to financial services, defense, and more. Such critical OT operations require quick system responses to perform as intended. The low latency requirements of these systems would therefore rely on constant availability. Even a momentary outage could cause a safety critical system to fail to respond within a defined time - with potentially fatal consequences. For this reason, OT Networks rank availability typically as their highest priority, followed by integrity and confidentiality. Therefore, we categorize attack impacts in terms of security services in the following order of priority: Availability, Integrity, and Confidentiality.

This is in contrast to IT networks, where confidentiality and data integrity would be of higher priority than a momentary lapse of availability. In IT networks, data is the important commodity. Hence, protecting that data is more important than a temporary lapse in availability. The focus of IT networks are aimed at an organization's day to day operation, such as the the storage of information or completion of automated processes. Provided that the integrity and confidentiality of the systems are maintained, short outages

will have little impact on an organization. Most tasks that would fail due to outages can be completed once systems become available again.

In some cases, an attack may impact more than one security service. In such cases, the attack will only be described in the higher priority service category but the other services that are potentially impacted will be mentioned as well. For instance, although a FDIA is primarily an attack against data integrity, it may potentially impact availability [13]. Since availability is the higher priority category, it will be described in the Availability Threats subsection and not in the Integrity Threats subsection.

4.1. Availability Threats

In DoS attacks, the perpetrator seeks to make information or operational technology systems unavailable, either temporarily or indefinitely, to authorized users or other systems in the network. For instance, this may be accomplished in traditional IT by overloading a web service with superfluous requests. In OT systems, there may be unique attack vectors for carrying out DoS attacks compared to IT systems. For instance, perpetrators of DoS attacks may target systems or data that are critical for correct operation of automated control systems. DoS attacks represent significant threats to power systems because the control systems in such systems are sensitive to timing and any disruption to critical information can compromise the entire system's availability.

As explained in [13], there are several different taxonomies of DoS attacks in the Smart Grid. They can be classified by vulnerabilities in common SG communications protocols, by major SG applications, or by attacker exploitation techniques. With regards to exploitation techniques, the major categories are jamming [18,28–31], resource exhaustion [32–38], cryptography algorithm exploits [39], data attacks, de-synchronization attacks [40,41], routing-based attacks, and reflector attack.

Jamming attacks are a form of DoS attack, and present a significant threat to the availability of smart grid systems. In jamming attacks, the shared nature of wireless channels is exploited by sending a continuous flow of data to prevent legitimate users from utilizing the channel. The authors in [42] propose a jamming channel attack called Maximum Attacking Strategy using Spoofing and Jamming (MAS-SJ). This attack targets PMUs of the cognitive radio network (CRN) used for providing time-synchronized data of power operating states in a wireless smart grid network (WSGN).

In [32,37], the authors introduce the puppet attack, where a vulnerability in the Advanced Metering Infrastructure (AMI) dynamic source routing protocol is exploited, causing the network bandwidth to become exhausted. In [43], the Time-Delay-Switch (TDS) attack is proposed, where attackers introduce time delays into control loops to cause general instability of the smart grid system. The Time Synchronization Attack (TSA) [40] targets the integrity of the GPS information of Phasor Measurement Units (PMUs) of various smart grid applications, including transmission line fault detection, voltage stability monitoring, and event locationing. In [44], the effects of flooding attacks on time-critical communications of the Smart Grid are explored. Another potential threat against availability and integrity are wormhole attacks, as shown in [45].

Attacks that primarily target data integrity may impact their availability as well. In power grid applications, the false data injection attack [40] is a well-known example of this. In FDIA, the power grid state-estimation systems are targeted in order to distort real energy supply and demand figures, which may cause blackouts, physical damage, or even the loss of human lives [18]. FDIA attacks may also effectively become a denial-of-service attack as they may cause critical services to become unavailable. The research of detection strategies for FDIA is a highly active area, because it carries the potential for large impact and benefits to a very challenging problem. Due to the time-sensitive nature of the communications involved in these state-estimation systems, detection schemes must be very efficient. Some additional attacks that target data integrity that may lead to DoS are presented in [46–48].

Some basic attacks may have a large impact on availability as well. Viruses, worms, and trojan horses pose a significant threat to IT and OT systems, not only in terms of

availability, but in terms integrity and confidentiality as well. The Stuxnet worm and Duqu malware [37] are two examples of such attacks. These attacks may be able to bypass any existing defense-in-depth strategies, which makes them particularly dangerous. Furthermore, masquerade attacks may be carried out [35] to penetrate a system and/or elevate permissions in order to carry out a larger attack that may compromise the availability of the system.

4.2. Integrity Threats

Cyber attacks that affect the integrity of systems within energy OT networks are primarily focused on the transmission and distribution domains of the conceptual model. As mentioned in the previous section, the primary focus of research in this area is on FDIA in state-estimation systems, as these types of attacks not only impact availability and integrity of energy systems, but can cause blackouts, damage to systems, harm and even the loss of lives. However, other types of data tampering attacks may also have serious consequences for the smart grid. In this section, we present a survey of threats to data integrity in energy OT networks.

Since most attacks that impact data integrity in smart grids may also impact availability, most of the survey in this section has already been compiled in the previous section. However, many of those same attacks may have less severe consequences. For instance, a malicious attacker may target the smart metering infrastructure to create financial losses for the utility company. Or, an opportunistic attacker may alter the measurement data to get free power [49]. Attackers may also initiate man-in-the middle or spoofing attacks against AMI via unauthorized data manipulation. These are just a few examples of data integrity threats that may not necessarily impact availability.

4.3. Confidentiality Threats

Cyber attacks that affect the confidentiality of users in the power grid are mainly focused on the customer, distribution, and service provider domains of the NIST Smart Grid Conceptual Model [27]. AMIs enable more precise, real-time monitoring of customer energy consumption for more precise billing and to provide feedback to customers about their energy consumption habits. This level of customer feedback necessitates communications of potentially sensitive customer information in the AMI communication networks, presenting a potential threat to customer confidentiality. In addition to customers, intrusions within almost all domains in the conceptual model may reveal sensitive user information (e.g., employees). In this section, we present a survey of threats to confidentiality in energy grid OT networks.

As explained in [49], the primary challenges concerning confidentiality in AMI are customer privacy and operations integrity and availability. Since the latter concerns have been discussed in previous sections, the primary focus in this section concerning confidentiality in AMI is regarding customer privacy. As shown in [50], smart devices may be identified by an attacker by analyzing their energy consumption, and sensitive customer information may be revealed by analyzing meter readings. The main attacks targeting confidentiality are packet capturing for traffic scanning, port scanning directed at specific protocols such as DNP3, and social engineering or password phishing attacks.

5. Potential Countermeasures to Cybersecurity Threats

Countermeasures to cybersecurity threats in OT networks are also categorized by the security model category, as shown in Section 4. However, the category of attack may affect multiple security model categories. In particular, attacks that affect integrity and confidentiality require network access to be deployed. For this reason, countermeasures for integrity and confidentiality threats have been combined in this section, while countermeasures to availability threats are individually addressed. A summary of the countermeasures outlined in this section can be found in Table 2.

Table 2. Cyber Attacks in the Smart Grid and Their Countermeasures.

Impacted Security Model Category	Attack Category	Possible Countermeasures	Compromised Application, Protocol, or Device	Attack Example
Availability	Denial of Service	SIEM, IDS, flow entropy, signal strength, sensing time measurement, transmission failure count, pushback, reconfiguration methods	AMI	puppet attack [32]
			smart grid	TDS [43]
			PMU, GPS	TSA [40]
	False Data Injection Attack	FDIA Detection [51–125] applied in DLP, IDS, SIEM, etc.; Secure DNP3; TLS; SSL; encryption, authentication; PKI	AMI, RTU, EMS, SCADA	[21]
	Jamming	JADE, anti-jamming, (FHSS, DSSS)	PMU	[126]
			CRN in WSGN	MAS-SJ [42]
	Malware Injection	DLP, IDS, SIEM, Anti-virus, Diversity technique	SCADA, PMU, Control device	Stuxnet [37]
			SCADA	Duqu [37]
	Masquerade attack	DLP, IDS, Secure DNP3, SIEM, TLS, SSL, encryption, authentication, PKI	PLC	[35]
Integrity	Man-in-the-middle	Secure DNP3, PKI, TLS, SSL, encryption, authentication	HMI, PLC	eavesdropping
			SCADA	
			DNP3, SCADA	
			AMI	intercept/alter
	Replay attack	Secure DNP3, TLS, SSL, encryption, authentication, PKI	IED, SCADA, PLC	
			AMI authentication	
Confidentiality	Privacy violation	Secure DNP3, PKI, TLS, SSL, encryption, authentication	Demand response program, smart meters	
	Scanning (IP, Port, Service, Vulnerabilities)	IDS, SIEM, automated security compliance checks	Modbus protocol	Modbus network scanning
			DNP3 protocol	DNP3 network scanning
	Social engineering	Secure DNP3, PKI, SSL, encryption, authentication	Modbus protocol, DNP3 protocol	phishing
			Modbus protocol, DNP3 protocol	password pilfering
	Traffic analysis	Secure DNP3, PKI, SSL, encryption, authentication	Modbus protocol, DNP3 protocol	

5.1. Potential Countermeasures for Availability Threats

Cybersecurity threats that impact availability in the smart grid present major challenges to researchers. As demonstrated in previous sections, many of these threats are related to threats that impact data integrity, including some DoS and FDIA attack vectors. In general, there is no single solution to prevent DoS and DDoS attacks. Consequently, a multitude of different solutions may have to be implemented to successfully limit the effectiveness of such attacks [13]. Furthermore, state-estimation systems in the SG are highly sensitive to time synchronization and latency degradation. Due to the real-time nature of state-estimation systems, research in this area is heavily focused on efficient and effective detection algorithms. As explained in [13], DoS countermeasure strategies may be categorized by non-technical security controls, filtering, Intrusion Detection/Prevention Systems (IDS/IPS), rate limiting, cryptographic authentication, protocol solutions, architectural solutions, honeypots, device solutions, wireless communications-specific solutions, and system-theoretic solutions. Some examples of non-technical security controls are to limit access to critical assets to authorized personnel and implementing an effective and strategic cybersecurity governance and management framework. A brief survey of technical solutions for DoS attacks, organized by category, follows below.

Filtering is the implementation of effective firewall rules to limit incoming traffic to expected network addresses, ports, etc. In [127], the authors present a firewall called smart tracking firewall that is specialized for a wireless mesh network (WMN)-based smart distribution grid (SDG). In their scheme, any nodes that detect a potential intruder are able

to notify their neighbors who may then be able to filter the source's traffic from advancing any further in the multihop network. The authors in [128] propose an openflow SDN-based firewall for preventing DDoS attacks in AMI. By connecting the firewall to the SDN controller and the cloud firewall agent, the firewall policies are able to ensure that incoming data is safe and filtering of the traffic occurs at the cloud edge.

Intrusion detection systems (IDS) are devices or software applications that typically exhibit more sophisticated capabilities compared to firewalls, which are primarily configuration-driven to filter harmful traffic. IDS may be developed with specific use cases in mind, such as detection for a specific ICS protocol. They are usually designed to detect more sophisticated intrusion scenarios than firewalls. Intrusion prevention systems add some automated prevention capabilities to an IDS, e.g., automatically block a source address when a certain attack scenario is detected. One key difference between firewalls and IDS is that an IDS can likely decrypt incoming traffic while firewalls likely cannot. Therefore, they may be more useful for detecting sophisticated attack scenarios, while still allowing for the data to be encrypted. IDS systems may be classified as signature-based, anomaly-based, or specification-based.

Signature-based IDSs rely on a rules-based engine of known attack signatures. In [129], a set of signature rules for detecting intrusions in Modbus communications for SCADA applications are presented. The authors in [130] present a set of signature rules for the DNP3 protocol for SCADA. Each of the signature-based IDSs provide rules for preventing DoS attacks.

Anomaly-based IDSs typically rely on machine learning algorithms or other statistical methods. In [131], the authors use a time-series model of process measurements to detect anomalies related to DoS attacks. The authors in [132] develop a deep learning model to detect anomalies in PMU data. In [133], a machine-learning based anomaly detector to detect attacks on load forecasting data. Each of these anomaly-based IDS algorithms are useful for preventing DoS attacks.

Specification-based IDSs rely on manually developed specifications of legitimate behavior. In [134], a specification-based IDS algorithm to monitor AMI C12.22 transmissions for anomalies using device-based, network-based, and application-based constraints. In [135], the authors propose a specification-based network-based cyber intrusion detection system (NIDS) for detection of anomalies in GOOSE and SV multicast messages in substation automation systems. Each of the presented specification-based anomaly detectors are useful for preventing DoS attacks.

Cryptographic authentication refers to the use of cryptographic solutions to prevent the types of data integrity attacks that may lead to a DoS. Some key challenges for the smart grid, however, are the combined use of resource-constrained computing devices and long-lived devices that are typical of power systems. Due to the use of low-power devices, the cryptographic algorithms must be lightweight and due to the use of the long-lived devices, they must also be stable over long periods of time. Furthermore, the scalability of key management approaches is a major concern [136]. In short, the use of cryptography in the SG carries the potential for itself to become a target of DoS attacks [39]. In [137], the authors propose a hybrid solution of combined public and symmetric key techniques.

Protocol-based solutions refer to research related to improving communication protocols used in the SG. The protocols used in the SG carry some unique challenges compared to those used in the Internet. For instance, since many of the devices have a long lifetime, the protocols need to be able to evolve over time. In addition to current standardization efforts to deal with various security requirements, including DoS attacks [138], there is active research to improve SG protocols further. For instance, in [139], a lightweight and efficient authentication scheme using one-time signatures for multicast data is presented.

Architectural solutions refer to the design of network topology to mitigate the effectiveness of certain DoS scenarios. Since the SG is relatively new, there is opportunity to design the architecture from the ground up to address such needs [140]. For instance, a subnetwork may be able to isolate itself in the event of a DoS attack to continue operations until the

parent network recovers. This type of architectural design is known as islanding [141]. Islanding can be an effective architectural solution in smart grids [141–143].

Honeypots are devices and systems that mimic legitimate network components that are likely targets of attack in a network. They are typically monitored and isolated from the production network so that security operations may detect potential attacks early and potentially block malicious sources before they have a chance to attack the production systems. A recent survey paper explores the use of honeypots and honeynet [144] in the smart grid. They find that Conpot [145,146] is a promising open-source project able to support many smart grid use cases out of the box and may be extensible to support other use cases as well. There is large potential for future research work in this area, particularly with a focus on expanding support for more protocols and devices.

The SG presents many challenges for device-level cybersecurity, including (1) physical security concerns, (2) patching may be difficult or impossible, (3) limited computation abilities, and (4) cost efficiency of solutions. Plus, many of the legacy devices in the power grid were designed without security in mind. Some promising solutions for the smart grid include, (1) trusted computing [147], (2) attestation [148], (3) diversity, (4) secure bootstrapping [141], and (5) secure patching [141].

Since Smart Grid applications can have strict delay requirements (on the order of a few milliseconds), DoS attacks against their wireless channels are particularly effective. Countermeasures in this category are primarily concerned with anti-jamming solutions and they may be categorized by (1) efficient and robust detection and (2) DoS-resilience schemes. [36]. In [126], the authors propose a method to detect the jamming channel attacks. In [30], the authors introduce a new metric called message invalidation ratio to analyze the effectiveness of a designed jamming detection system in different attack scenarios.

System-theoretic solutions relate to solutions for False Data Injection Attacks. As described in [21], FDIA detection algorithms may be categorized as follows: model-based and data-driven detection algorithms. Model-based attacks are further categorized by static state-estimation techniques, dynamic state-estimation techniques, and other model-based techniques. In [149], the authors model the False Data Injection Attack, enabling the design of model-based detection schemes. The authors in [51–61] present static state-estimation techniques. In [62–77], some dynamic state-estimation techniques are presented. Some other model-based detection schemes are presented in [78,80–91,150]. Similarly, data-driven detection algorithms may be further subdivided into machine-learning based algorithms, data-mining based algorithms, and other data-driven algorithms. Some supervised machine-learning based algorithms are presented in [92–108,151,152]; some unsupervised machine-learning based algorithms are presented in [106,109–117,153]; and reinforcement-learning based algorithms are presented in [116]. Data-mining based detection algorithms are presented in [117–120], and other data-driven detection algorithms are described in [121–124].

Perhaps one of the more challenging aspects of securing ICS networks in general is to implement effective countermeasures against malware threats. Some recent high-profile attacks, including Stuxnet and Havex, utilized zero-day exploits and concealment [154]. In [154], the authors propose the use of multi-layered strategies (i.e., defense-in-depth) to mitigate some of these threats, among others. An effective defense perimeter for the OT and IT portions of the network, as shown in Figure 4 may prevent some of these attacks from starting. However, due to misconfigurations, backdoors, etc. this is not a guarantee. The IT side of the network should also use endpoint protection, a SIEM, etc., in order to detect known threats. However, there are also zero-day threats, supply-chain threats, social engineering threats, USB devices with malware, etc. The NERC CIP standards [2] include standards for supply chain management and device patching. All of these are a good place to start to defend against malware threats. However, development of more effective countermeasures for these threats offers a good opportunity for future research into SG and ICS networks in general.

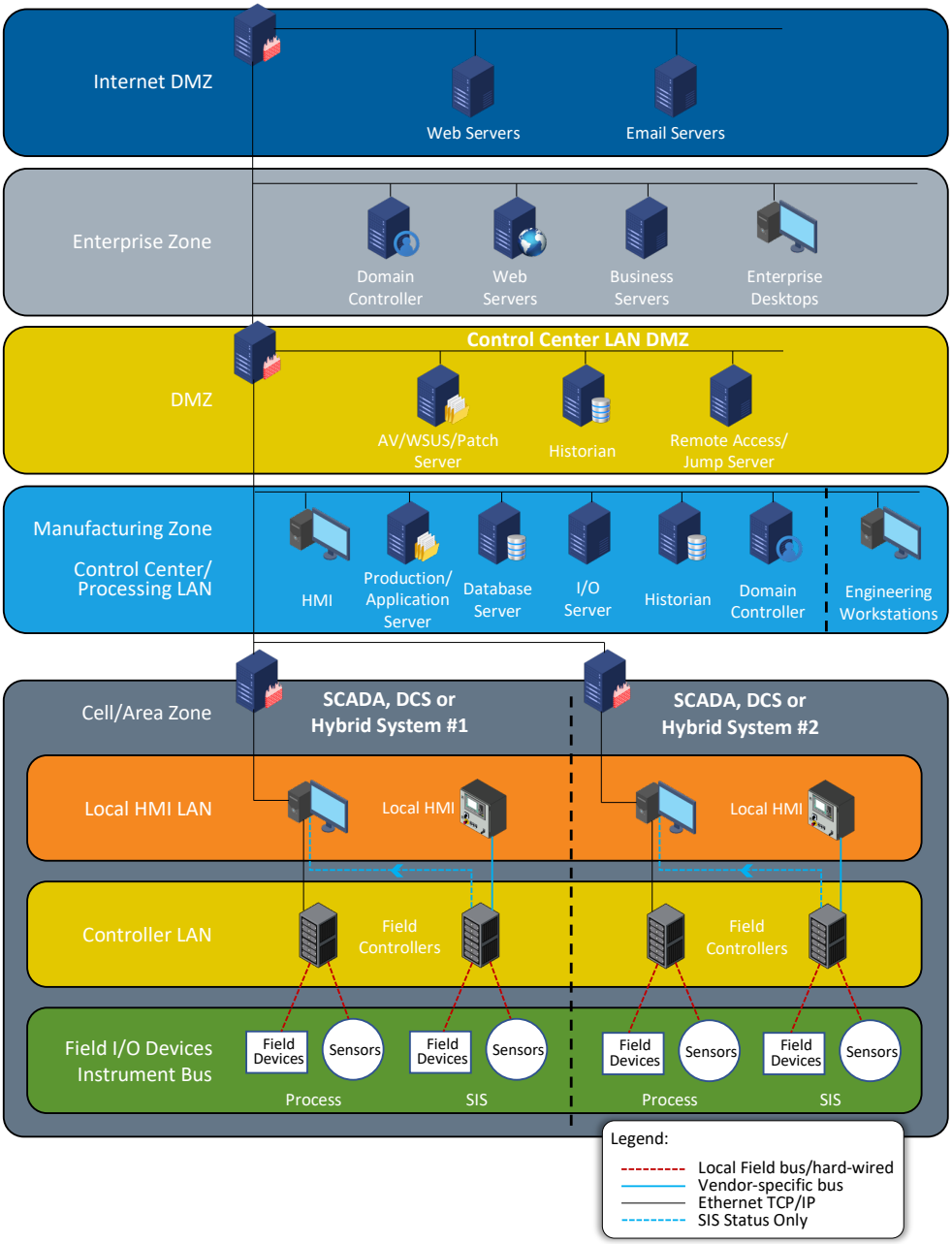

Figure 4. CISA Recommended Secure Architecture.

5.2. Potential Countermeasures for Integrity and Confidentiality Threats

Cybersecurity threats affecting integrity of ICS communication are often targeted at specific protocols. The Modbus and DNP3 protocols that are compatible with legacy serial devices are especially vulnerable to eavesdropping and alteration. The major cybersecurity threats that impact confidentiality in the smart grid are primarily focused on the Advanced Metering Infrastructure (AMI). The AMI is a system of smart meters, communication networks, and data management systems that enables two-way communication between customers and utilities. This two-way communication enables better monitoring and more accurate billing for utilities and more accurate consumption behavior for customers. However, since more customers use this model, there are increased access points for security attacks.

In both of these cases, encryption is an effective countermeasure for data integrity and confidentiality. The IEEE Secure SCADA Communications Protocol (SSCP) [155] is

targeted at employing encryption on serial implementation of protocols. In [156], Ferst et al. employed TLS to the Modbus protocol to produce a significant improvement in secrecy of data. The combination of these countermeasures removes the gap between security of legacy devices to their modern IED counterparts.

6. Recommended Gap Analysis Strategies for Cybersecurity Assurance in the Energy Sector

While previous sections have identified individual cybersecurity threats and countermeasures for them, a combination of these security services will be required to prevent gaps in protection. NIST recommends that gap analysis be performed on individual company networks and provides a Cybersecurity framework specific for smart grids with five continuous functions [25].

- Identify—Determine assets within the organization and their risk factors for potential Cybersecurity risks.
- Protect—Create safeguards to ensure delivery of infrastructure services through access control, awareness and training, data security, and information protection procedures.
- Detect—Identify any Cybersecurity events with continuous monitoring.
- Respond—Implement predefined procedures for response planning and communications.
- Recover—Develop plans to maintain resilience and restore capabilities of services.

The framework provides an in-depth procedure, recommended considerations, and information references to successfully implement each of these five functions to align with DoE's C2M2. All five functions are reliant on each other for proper implementation. For example, a failure in identification can lead to shortcomings in the implementation of protection services. For "identification", categories that are defined include asset management, business environment, governance, risk assessment, risk management strategy, and supply chain risk management. This set of categories is where most variability will appear within different organizations, as assets and protocols used by different devices will have different associated risks. The organization will need to identify critical functions and assets to tailor their profile for effective risk management.

The goal of the "protect" function is to ensure security and resilience of systems, while ensuring all personnel are aware of their roles of cybersecurity within an organization. The protection service is where most of the countermeasures mentioned in the previous sections are implemented, with categories for access control, training, data security, information protection processes and procedures, maintenance, and protective technologies. These categories map directly to the countermeasures for integrity and confidentiality attacks shown in Table 2. Access control can effectively counter man-in-the-middle, replay, and privacy violation attacks. FDIA detection is also the primary detection countermeasure focused on in this paper, with the NIST "detect" function comprised of categories for anomalies and events, continuous monitoring, and detection processes. Implementation of these services should also identify the scope and impact of any events that take place.

The final two categories in the NIST profile are aimed at the occurrence of a cybersecurity event, with "respond" and "recover". Respond is divided into categories of response planning, communications, analysis, mitigation, and improvements, whereas Recovery is divided into planning, improvements and communication. The procedures for these categories should be in place before an attack occurs, as proper response planning and communications will allow for improved response and recovery timelines. With every event, analysis and mitigation is expected to be performed, with any lessons incorporated into future improvements of response planning. After a successful response, recovery procedures will be enacted with future improvements added to procedures for future events.

The goal of the framework is to aid stakeholders of any organization to identify, assess, and manage any risks that may be in their organizational network. Compliance with this framework can look vastly different between different organizations, so NIST also provides steps to implement or improve a Cybersecurity program.

1. Prioritize and Scope

2. Orient
3. Create a Current Profile
4. Conduct a Risk Assessment
5. Create a Target Profile
6. Determine, Analyze, and Prioritize Gaps
7. Implement Action Plan

To aid in determination of a target profile, NIST also provides a set of four tiers that an organization can reference for their management goals. There are 4 tiers referenced: partial, risk informed, repeatable, and adaptive. The higher the tier, the more rigorous the protections that are in place within an organization. For example, at tier 1 (partial) there are no formalized policies in place, with the organization addressing each risk individually without an evolving procedure. These tiers expand cybersecurity awareness and risk mitigation up to adaptive, where advanced technologies are implemented and risk management practices evolve to combat current and past cybersecurity threats.

7. Conclusions

In this paper, we have identified the challenges facing the cybersecurity of ICSs with the convergence of OT and IT systems. By examining the current standards and organizations for power grid cybersecurity governance, we showed recommended architectures and security services specific to the energy sector. We also examined the areas of ICS cybersecurity model of availability, integrity, and confidentiality.

We specifically illustrated the differences in priority assignment for confidentiality, integrity and availability between IT and OT networks, as this difference is a key motivator for different approaches to cybersecurity between these two domains. An evaluation of known cybersecurity threats and their countermeasures was provided in each of these three areas, with a focus on OT specific threats. We provided an examination of NIST's recommended gap analysis strategy for smart grid profiles with recommended continuous functions of identify, protect, detect, respond, and recover. Each of these functions was examined and examples of applicable implementations of presented countermeasures were provided.

From this survey it is apparent that great strides have been made in the OT realm's cybersecurity approaches, while significant work remains, the growing number of tools, specifications, and capabilities show the amount of effort being vested in securing OT operations, many of which are at the core of critical infrastructure sectors, such as the energy grid.

Author Contributions: Investigation, M.B., K.B., M.H. and H.S.; writing—original draft preparation, M.B., K.B. and M.H.; writing—review and editing, M.B., M.H., H.S., K.P. and J.L.J.; supervision, H.S., M.H., K.P. and J.L.J.; project administration, K.P. and J.L.J.; funding acquisition, H.S., M.H., K.P. and J.L.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially funded by the Department of Energy Cybersecurity for Energy Delivery Systems program, and the Oak Ridge National Laboratory project No. 4000175929. It has also been supported in part by the University of Nebraska-Lincoln's Nebraska Center for Energy Sciences Research (NCESR) under Cycle 16 Grant# 20-706.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: This study did not report any data.

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

Abbreviations

The following abbreviations are used in this manuscript:

ICS	Industrial Control System
FERC	Federal Energy Regulatory Commission
NIST	National Institute of Standards and Technology
NERC	North American Electric Reliability Corporation
CIP	Critical Infrastructure Protection
IT	Information Technology
OT	Operations Technology
DiD	Defense-in-Depth
DMZ	Demilitarized Zone
CSF	Cybersecurity Framework
C2M2	Cybersecurity Capability Maturity Model
ICPS	Industrial Cyber-Physical Systems
DoS	Denial of Service
SG	Smart Grid
FDIA	False Data Injection Attack
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
CIP	Critical Infrastructure Protection
ERO	Electricity Reliability Organization
BES	Bulk Electric System
ESP	Electronic Security Perimeter
NRC	Nuclear Regulatory Commission
NEI	Nuclear Energy Institute
DHS	US Department of Homeland Security
ISA	International Society of Automation
IEC	International Electrotechnical Commission
M2M	Machine-to-Machine
MAS-SJ	Maximum Attacking Strategy using Spoofing and Jamming
PMU	Phasor Measurement Unit
AMI	Advanced Metering Infrastructure
TDS	Time-Delay-Switch
PMU	Phasor Measurement Units
TSA	Time Synchronization Attack
IDS/IPS	Intrusion Detection/Prevention Systems
CRN	Cognitive Radio Network
WSGN	Wireless Smart Grid Network

References

1. Skodvin, T. "Pivotal politics" in US energy and climate legislation. *Energy Policy* **2010**, *38*, 4214–4223. [CrossRef]
2. CIP Standards. NERC 2022. Available online: https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx (accessed on 28 April 2022)
3. Kayan, H.; Nunes, M.; Rana, O.; Burnap, P.; Perera, C. Cybersecurity of Industrial Cyber-Physical Systems: A Review. *ACM Comput. Surv.* **2022**, *54*, 229.. [CrossRef]
4. Hassanzadeh, A.; Rasekh, A.; Galelli, S.; Aghashahi, M.; Taormina, R.; Ostfeld, A.; Banks, M.K. A review of cybersecurity incidents in the water sector. *J. Environ. Eng.* **2020**, *146*, 03120003. [CrossRef]
5. Krause, T.; Ernst, R.; Klaer, B.; Hacker, I.; Henze, M. Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors* **2021**, *21*. [CrossRef] [PubMed]
6. Jacobs, N.; Hossain-McKenzie, S.; Jose, D.; Saleem, D.; Lai, C.; Cordeiro, P.; Hasandka, A.; Martin, M.; Howerter, C. Analysis of System and Interoperability Impact from Securing Communications for Distributed Energy Resources. In Proceedings of the 2019 IEEE Power and Energy Conference at Illinois (PECI), Champaign, IL, USA, 28 February–1 March 2019; pp. 1–8. [CrossRef]
7. Shapsough, S.; Qatan, F.; Aburukba, R.; Aloul, F.; Al Ali, A.R. Smart grid cyber security: Challenges and solutions. In Proceedings of the 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), Offenburg, Germany, 20–23 October 2015; pp. 170–175. [CrossRef]
8. Christopher, J.D.; Gonzalez, D.; White, D.W.; Stevens, J.; Grundman, J.; Mehravari, N.; Dolan, T. *Cybersecurity Capability Maturity Model (C2M2)*; Department of Homeland Security: Washington, DC, USA, 2014; pp. 1–76.

9. Scali, D. Developing a Security Strategy to Cover ICS Assets. 17 August 2016. Available online: https://www.fireeye.com/blog/executive-perspective/2016/08/developing_a_securit.html. (accessed on 28 April 2022)
10. Komninos, N.; Philippou, E.; Pitsillides, A. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1933–1954. [CrossRef]
11. Line, M.B.; Tøndel, I.A.; Jaatun, M.G. Cyber security challenges in Smart Grids. In Proceedings of the 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, Manchester, UK, 5–7 December 2011; pp. 1–8.
12. Tan, S.; De, D.; Song, W.Z.; Yang, J.; Das, S.K. Survey of security advances in smart grid: A data driven approach. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 397–422. [CrossRef]
13. Huseinović, A.; Mrdović, S.; Bicakci, K.; Uludag, S. A survey of denial-of-service attacks and solutions in the smart grid. *IEEE Access* **2020**, *8*, 177447–177470. [CrossRef]
14. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.Y.; Zhang, X.; Ghias, A.M.; Koh, L.H.; Yang, L. Blockchain for future smart grid: A comprehensive survey. *IEEE Internet Things J.* **2020**, *8*, 18–43. [CrossRef]
15. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambotharan, S.; Chin, W.H. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 21–38. [CrossRef]
16. Le, T.N.; Chin, W.L.; Chen, H.H. Standardization and security for smart grid communications based on cognitive radio technologies—A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 423–445.
17. Peng, C.; Sun, H.; Yang, M.; Wang, Y.L. A survey on security communication and control for smart grids under malicious cyber attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1554–1569. [CrossRef]
18. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 5–20. [CrossRef]
19. Rehmani, M.H.; Davy, A.; Jennings, B.; Assi, C. Software defined networks-based smart grid communication: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2637–2670. [CrossRef]
20. Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies* **2021**, *14*, 5894. [CrossRef]
21. Musleh, A.S.; Chen, G.; Dong, Z.Y. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Trans. Smart Grid* **2019**, *11*, 2218–2234. [CrossRef]
22. Beasley, C.; Zhong, X.; Deng, J.; Brooks, R.; Venayagamoorthy, G.K. A survey of electric power synchrophasor network cyber security. In Proceedings of the IEEE PES Innovative Smart Grid Technologies, Europe, Istanbul, Turkey, 12–15 October 2014; pp. 1–5.
23. Moussa, B.; Debbabi, M.; Assi, C. Security assessment of time synchronization mechanisms for the smart grid. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1952–1973. [CrossRef]
24. Barrett, M.P. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]
25. Allnutt, J.; Anand, D.; Arnold, D.; Goldstein, A.; Li-Baboud, Y.; Martin, A.; Nguyen, C.; Noseworthy, R.; Subramaniam, R.; Weiss, M. Timing challenges in the smart grid. *NIST Spec. Publ.* **2017**, *1500*, 08.
26. Department of Homeland Security, U.D. Industrial Control Systems Cyber Emergency Response Team. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-In-Depth Strategies. 2016. Available online: https://www.cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems (accessed on: 28 April 2022)
27. Greer, C.; Wollman, D.A.; Prochaska, D.; Boynton, P.A.; Mazer, J.A.; Nguyen, C.; FitzPatrick, G.; Nelson, T.L.; Koepke, G.H.; Hefner, A.R., Jr.; et al. *Nist Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014.
28. Temple, W.G.; Chen, B.; Tippenhauer, N.O. Delay makes a difference: Smart grid resilience under remote meter disconnect attack. In Proceedings of the 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), Vancouver, BC, Canada, 21–24 October 2013; pp. 462–467.
29. Ma, J.; Liu, Y.; Song, L.; Han, Z. Multiact dynamic game strategy for jamming attack in electricity market. *IEEE Trans. Smart Grid* **2015**, *6*, 2273–2282. [CrossRef]
30. Lu, Z.; Wang, W.; Wang, C. Modeling, evaluation and detection of jamming attacks in time-critical wireless applications. *IEEE Trans. Mob. Comput.* **2013**, *13*, 1746–1759. [CrossRef]
31. Li, H.; Lai, L.; Qiu, R.C. A denial-of-service jamming game for remote state monitoring in smart grid. In Proceedings of the 2011 45th Annual Conference on Information Sciences and Systems, Baltimore, MD, USA, 23–25 March 2011; pp. 1–6. [CrossRef]
32. Yi, P.; Zhu, T.; Zhang, Q.; Wu, Y.; Li, J. A denial of service attack in advanced metering infrastructure network. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 1029–1034.
33. Choi, K.; Chen, X.; Li, S.; Kim, M.; Chae, K.; Na, J. Intrusion detection of NSM based DoS attacks using data mining in smart grid. *Energies* **2012**, *5*, 4091–4109. [CrossRef]
34. Jin, D.; Nicol, D.M.; Yan, G. An event buffer flooding attack in DNP3 controlled SCADA systems. In Proceedings of the 2011 Winter Simulation Conference (WSC), Phoenix, AZ, USA, 11–14 December 2011; pp. 2614–2626.

35. Cleveland, F.M. Cyber security issues for advanced metering infrasttructure (AMI). In Proceedings of the 2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008; pp. 1–5.
36. Wang, W.; Lu, Z. Cyber security in the smart grid: Survey and challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
37. Yi, P.; Zhu, T.; Zhang, Q.; Wu, Y.; Pan, L. Puppet attack: A denial of service attack in advanced metering infrastructure network. *J. Netw. Comput. Appl.* **2016**, *59*, 325–332. [CrossRef]
38. Asri, S.; Pranggono, B. Impact of distributed denial-of-service attack on advanced metering infrastructure. *Wirel. Pers. Commun.* **2015**, *83*, 2211–2223. [CrossRef]
39. Kolesnikov, V.; Lee, W. MAC aggregation protocols resilient to DoS attacks. *Int. J. Secur. Netw.* **2012**, *7*, 122–132. [CrossRef]
40. Zhang, Z.; Gong, S.; Dimitrovski, A.D.; Li, H. Time synchronization attack in smart grid: Impact and analysis. *IEEE Trans. Smart Grid* **2013**, *4*, 87–98. [CrossRef]
41. Risbud, P.; Gatsis, N.; Taha, A. Vulnerability analysis of smart grids to GPS spoofing. *IEEE Trans. Smart Grid* **2018**, *10*, 3535–3548. [CrossRef]
42. Gai, K.; Qiu, M.; Ming, Z.; Zhao, H.; Qiu, L. Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. *IEEE Trans. Smart Grid* **2017**, *8*, 2431–2439. [CrossRef]
43. Sargolzaei, A.; Yen, K.; Abdelghani, M.N. Delayed inputs attack on load frequency control in smart grid. In Proceedings of the ISGT 2014, Washington, DC, USA, 19–22 February 2014; pp. 1–5.
44. Li, Q.; Ross, C.; Yang, J.; Di, J.; Balda, J.C.; Mantooth, H.A. The effects of flooding attacks on time-critical communications in the smart grid. 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.
45. Beigi-Mohammadi, N.; Mišić, J.; Khazaei, H.; Mišić, V.B. An intrusion detection system for smart grid neighborhood area network. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 4125–4130.
46. Goel, S.; Hong, Y.; Papakonstantinou, V.; Kloza, D. *Smart Grid Security*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 1–39. [CrossRef]
47. Mohsenian-Rad, A.H.; Leon-Garcia, A. Distributed internet-based load altering attacks against smart power grids. *IEEE Trans. Smart Grid* **2011**, *2*, 667–674. [CrossRef]
48. Li, Y.; Wang, R.; Wang, P.; Niyato, D.; Saad, W.; Han, Z. Resilient PHEV charging policies under price information attacks. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 389–394.
49. Anzalchi, A.; Sarwat, A. A survey on security assessment of metering infrastructure in smart grid systems. In Proceedings of the SoutheastCon 2015, Fort Lauderdale, FL, USA, 9–12 April 2015; pp. 1–4.
50. Asghar, M.R.; Dán, G.; Miorandi, D.; Chlamtac, I. Smart meter data privacy: A survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2820–2835. [CrossRef]
51. Chung, H.M.; Li, W.T.; Yuen, C.; Chung, W.H.; Wen, C.K. Local cyber-physical attack with leveraging detection in smart grid. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 461–466.
52. Jiang, Q.; Chen, H.; Xie, L.; Wang, K. Real-time detection of false data injection attack using residual prewhitening in smart grid network. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 83–88.
53. Sreenath, J.; Meghwani, A.; Chakrabarti, S.; Rajawat, K.; Srivastava, S. A recursive state estimation approach to mitigate false data injection attacks in power systems. In Proceedings of the 2017 IEEE Power & Energy Society General Meeting, Chicago, IL, USA, 16–20 July 2017; pp. 1–5.
54. Xu, R.; Wang, R.; Guan, Z.; Wu, L.; Wu, J.; Du, X. Achieving efficient detection against false data injection attacks in smart grid. *IEEE Access* **2017**, *5*, 13787–13798. [CrossRef]
55. Liu, T.; Sun, Y.; Liu, Y.; Gui, Y.; Zhao, Y.; Wang, D.; Shen, C. Abnormal traffic-indexed state estimation: A cyber–physical fusion approach for smart grid attack detection. *Future Gener. Comput. Syst.* **2015**, *49*, 94–103. [CrossRef]
56. Lukicheva, I.; Pozo, D.; Kulikov, A. Cyberattack detection in intelligent grids using non-linear filtering. In Proceedings of the 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Sarajevo, Bosnia and Herzegovina, 21–25 October 2018; pp. 1–6.
57. Kallitsis, M.G.; Bhattacharya, S.; Stoev, S.; Michailidis, G. Adaptive statistical detection of false data injection attacks in smart grids. In Proceedings of the 2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Washington, DC, USA, 7–9 December 2016; pp. 826–830.
58. Moslemi, R.; Mesbahi, A.; Velni, J.M. A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids. *IEEE Trans. Smart Grid* **2017**, *9*, 4930–4941. [CrossRef]
59. Chen, Y.; Huang, S.; Liu, F.; Wang, Z.; Sun, X. Evaluation of reinforcement learning-based false data injection attack to automatic voltage control. *IEEE Trans. Smart Grid* **2018**, *10*, 2158–2169. [CrossRef]

60. Tang, B.; Yan, J.; Kay, S.; He, H. Detection of false data injection attacks in smart grid under colored Gaussian noise. In Proceedings of the 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, 17–19 October 2016; pp. 172–179.
61. Akingeneye, I.; Wu, J. Low latency detection of sparse false data injections in smart grids. *IEEE Access* **2018**, *6*, 58564–58573. [CrossRef]
62. Kurt, M.N.; Yılmaz, Y.; Wang, X. Real-time detection of hybrid and stealthy cyber-attacks in smart grid. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 498–513. [CrossRef]
63. Manandhar, K.; Cao, X.; Hu, F.; Liu, Y. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Trans. Control. Netw. Syst.* **2014**, *1*, 370–379. [CrossRef]
64. Rawat, D.B.; Bajracharya, C. Detection of false data injection attacks in smart grid communication systems. *IEEE Signal Process. Lett.* **2015**, *22*, 1652–1656. [CrossRef]
65. Khalaf, M.; Youssef, A.; El-Saadany, E. Detection of false data injection in automatic generation control systems using Kalman filter. In Proceedings of the 2017 IEEE Electrical Power and Energy Conference (EPEC), Saskatoon, SK, Canada, 22–25 October 2017; pp. 1–6.
66. Khalaf, M.; Youssef, A.; El-Saadany, E. Joint detection and mitigation of false data injection attacks in AGC systems. *IEEE Trans. Smart Grid* **2018**, *10*, 4985–4995. [CrossRef]
67. Kurt, M.N.; Yılmaz, Y.; Wang, X. Distributed quickest detection of cyber-attacks in smart grid. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2015–2030. [CrossRef]
68. Jiang, Y.; Hui, Q. Kalman filter with diffusion strategies for detecting power grid false data injection attacks. In Proceedings of the 2017 IEEE International Conference on Electro Information Technology (EIT), Lincoln, NE, USA, 14–17 May 2017; pp. 254–259.
69. Khalid, H.M.; Peng, J.C.H. Immunity toward data-injection attacks using multisensor track fusion-based model prediction. *IEEE Trans. Smart Grid* **2015**, *8*, 697–707. [CrossRef]
70. Musleh, A.S.; Khalid, H.M.; Muyeen, S.; Al-Durra, A. A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications. *IEEE Syst. J.* **2017**, *13*, 710–719. [CrossRef]
71. Karimipour, H.; Dinavahi, V. Robust massively parallel dynamic state estimation of power systems against cyber-attack. *IEEE Access* **2017**, *6*, 2984–2995. [CrossRef]
72. Karimipour, H.; Dinavahi, V. On false data injection attack against dynamic state estimation on smart power grids. In Proceedings of the 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 14–17 August 2017; pp. 388–393.
73. Shi, W.; Wang, Y.; Jin, Q.; Ma, J. PDL: An efficient prediction-based false data injection attack detection and location in smart grid. In Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018; Volume 2, pp. 676–681.
74. Zhao, J.; Zhang, G.; La Scala, M.; Dong, Z.Y.; Chen, C.; Wang, J. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks. *IEEE Trans. Smart Grid* **2015**, *8*, 1580–1590. [CrossRef]
75. Anwar, A.; Mahmood, A.N.; Tari, Z. Ensuring data integrity of OPF module and energy database by detecting changes in power flow patterns in smart grids. *IEEE Trans. Ind. Inform.* **2017**, *13*, 3299–3311. [CrossRef]
76. Li, Y.; Li, J.; Luo, X.; Wang, X.; Guan, X. Cyber attack detection and isolation for smart grids via unknown input observer. In Proceedings of the 2018 37th Chinese Control Conference (CCC), Wuhan, China, 25–27 July 2018; pp. 6207–6212.
77. Wang, X.; Luo, X.; Zhang, M.; Guan, X. Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers. *Int. J. Electr. Power Energy Syst.* **2019**, *110*, 208–222. [CrossRef]
78. Sahoo, S.; Mishra, S.; Peng, J.C.H.; Dragičević, T. A stealth cyber-attack detection strategy for DC microgrids. *IEEE Trans. Power Electron.* **2018**, *34*, 8162–8174. [CrossRef]
79. Li, B.; Ding, T.; Huang, C.; Zhao, J.; Yang, Y.; Chen, Y. Detecting False Data Injection AttacNs Against Power System State Estimation with Fast Go-Decomposition (GoDec) Approach. *IEEE Trans. Ind. Inform.* **2014**, *15*, 2892–2904. [CrossRef]
80. Liu, L.; Esmalifalak, M.; Ding, Q.; Emesih, V.A.; Han, Z. Detecting false data injection attacks on power grid by sparse optimization. *IEEE Trans. Smart Grid* **2014**, *5*, 612–621. [CrossRef]
81. Kushal, T.R.B.; Lai, K.; Illindala, M.S. Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system. *IEEE Trans. Smart Grid* **2018**, *10*, 4741–4750. [CrossRef]
82. Singh, S.K.; Khanna, K.; Bose, R.; Panigrahi, B.K.; Joshi, A. Joint-transformation-based detection of false data injection attacks in smart grid. *IEEE Trans. Ind. Inform.* **2017**, *14*, 89–97. [CrossRef]
83. Ashok, A.; Govindarasu, M.; Ajjarapu, V. Online detection of stealthy false data injection attacks in power system state estimation. *IEEE Trans. Smart Grid* **2016**, *9*, 1636–1646. [CrossRef]
84. Kumar, R.J.R.; Sikdar, B. Efficient detection of false data injection attacks on AC state estimation in smart grids. In Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 9–11 October 2017; pp. 411–415.
85. Sridhar, S.; Govindarasu, M. Model-based attack detection and mitigation for automatic generation control. *IEEE Trans. Smart Grid* **2014**, *5*, 580–591. [CrossRef]
86. Hao, J.; Kang, E.; Sun, J.; Wang, Z.; Meng, Z.; Li, X.; Ming, Z. An adaptive Markov strategy for defending smart grid false data injection from malicious attackers. *IEEE Trans. Smart Grid* **2016**, *9*, 2398–2408. [CrossRef]

87. Ameli, A.; Hooshyar, A.; El-Saadany, E.F. Development of a cyber-resilient line current differential relay. *IEEE Trans. Ind. Inform.* **2018**, *15*, 305–318. [CrossRef]
88. Chaojun, G.; Jirutitijaroen, P.; Motani, M. Detecting false data injection attacks in AC state estimation. *IEEE Trans. Smart Grid* **2015**, *6*, 2476–2483. [CrossRef]
89. Khanna, K.; Singh, S.K.; Panigrahi, B.K.; Bose, R.; Joshi, A. On detecting false data injection with limited network information using transformation based statistical techniques. In Proceedings of the 2017 IEEE Power & Energy Society General Meeting, Chicago, IL, USA, 16–20 July 2017; pp. 1–5.
90. Li, S.; Yılmaz, Y.; Wang, X. Quickest detection of false data injection attack in wide-area smart grids. *IEEE Trans. Smart Grid* **2014**, *6*, 2725–2735. [CrossRef]
91. Huang, Y.; Tang, J.; Cheng, Y.; Li, H.; Campbell, K.A.; Han, Z. Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis. *IEEE Syst. J.* **2014**, *10*, 532–543. [CrossRef]
92. Yip, S.C.; Wong, K.; Hew, W.P.; Gan, M.T.; Phan, R.C.W.; Tan, S.W. Detection of energy theft and defective smart meters in smart grids using linear regression. *Int. J. Electr. Power Energy Syst.* **2017**, *91*, 230–240. [CrossRef]
93. Esmalifalak, M.; Liu, L.; Nguyen, N.; Zheng, R.; Han, Z. Detecting stealthy false data injection using machine learning in smart grid. *IEEE Syst. J.* **2014**, *11*, 1644–1652. [CrossRef]
94. Yan, J.; Tang, B.; He, H. Detection of false data attacks in smart grid with supervised learning. In Proceedings of the 2016 International Joint Conference on Neural Networks (IJCNN), Vancouver, BC, Canada, 24–29 July 2016; pp. 1395–1402.
95. Binna, S.; Kuppannagari, S.R.; Engel, D.; Prasanna, V.K. Subset level detection of false data injection attacks in smart grids. In Proceedings of the 2018 IEEE Conference on Technologies for Sustainability (SusTech), Long Beach, CA, USA, 11–13 November 2018; pp. 1–7.
96. Foroutan, S.A.; Salmasi, F.R. Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method. *IET Cyber-Phys. Syst. Theory Appl.* **2017**, *2*, 161–171. [CrossRef]
97. Vimalkumar, K.; Radhika, N. A big data framework for intrusion detection in smart grids using apache spark. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 13–16 September 2017; pp. 198–204.
98. Jindal, A.; Dua, A.; Kaur, K.; Singh, M.; Kumar, N.; Mishra, S. Decision tree and SVM-based data analytics for theft detection in smart grid. *IEEE Trans. Ind. Inform.* **2016**, *12*, 1005–1016. [CrossRef]
99. Wang, D.; Wang, X.; Zhang, Y.; Jin, L. Detection of power grid disturbances and cyber-attacks based on machine learning. *J. Inf. Secur. Appl.* **2019**, *46*, 42–52. [CrossRef]
100. Khanna, K.; Panigrahi, B.K.; Joshi, A. AI-based approach to identify compromised meters in data integrity attacks on smart grid. *IET Gener. Transm. Distrib.* **2018**, *12*, 1052–1066. [CrossRef]
101. Zhao, H.; Liu, H.; Hu, W.; Yan, X. Anomaly detection and fault analysis of wind turbine components based on deep learning network. *Renew. Energy* **2018**, *127*, 825–834. [CrossRef]
102. Xue, D.; Jing, X.; Liu, H. Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework. *IEEE Access* **2019**, *7*, 31762–31773. [CrossRef]
103. Yang, L.; Li, Y.; Li, Z. Improved-ELM method for detecting false data attack in smart grid. *Int. J. Electr. Power Energy Syst.* **2017**, *91*, 183–191. [CrossRef]
104. Punmiya, R.; Choe, S. Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing. *IEEE Trans. Smart Grid* **2019**, *10*, 2326–2329. [CrossRef]
105. Razavi, R.; Gharipour, A.; Fleury, M.; Akpan, I.J. A practical feature-engineering framework for electricity theft detection in smart grids. *Appl. Energy* **2019**, *238*, 481–494. [CrossRef]
106. McLaughlin, S.; Holbert, B.; Fawaz, A.; Berthier, R.; Zonouz, S. A multi-sensor energy theft detection framework for advanced metering infrastructures. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1319–1330. [CrossRef]
107. Sedghi, H.; Jonckheere, E. Statistical structure learning to ensure data integrity in smart grid. *IEEE Trans. Smart Grid* **2015**, *6*, 1924–1933. [CrossRef]
108. Sedghi, H.; Jonckheere, E. Statistical structure learning of smart grid for detection of false data injection. In Proceedings of the 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, Canada, 21–25 July 2013; pp. 1–5.
109. Zanetti, M.; Jamhour, E.; Pellenz, M.; Penna, M.; Zambenedetti, V.; Chueiri, I. A tunable fraud detection system for advanced metering infrastructure using short-lived patterns. *IEEE Trans. Smart Grid* **2017**, *10*, 830–840. [CrossRef]
110. Viegas, J.L.; Vieira, S.M. Clustering-based novelty detection to uncover electricity theft. In Proceedings of the 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Naples, Italy, 9–12 July 2017; pp. 1–6.
111. Ahmed, S.; Lee, Y.; Hyun, S.H.; Koo, I. Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2765–2777. [CrossRef]
112. Wei, L.; Gao, D.; Luo, C. False data injection attacks detection with deep belief networks in smart grid. In Proceedings of the 2018 Chinese Automation Congress (CAC), Xi'an, China, 30 November–2 December 2018; pp. 2621–2625.
113. He, Y.; Mendis, G.J.; Wei, J. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Trans. Smart Grid* **2017**, *8*, 2505–2516. [CrossRef]
114. Ghasemi, A.A.; Gitizadeh, M. Detection of illegal consumers using pattern classification approach combined with Levenberg–Marquardt method in smart grid. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 363–375. [CrossRef]

115. Ntalampiras, S. Fault diagnosis for smart grids in pragmatic conditions. *IEEE Trans. Smart Grid* **2016**, *9*, 1964–1971. [CrossRef]
116. Kurt, M.N.; Ogundijo, O.; Li, C.; Wang, X. Online cyber-attack detection in smart grid: A reinforcement learning approach. *IEEE Trans. Smart Grid* **2018**, *10*, 5174–5185. [CrossRef]
117. Adhikari, U.; Morris, T.H.; Pan, S. Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection. *IEEE Trans. Smart Grid* **2016**, *9*, 3928–3941. [CrossRef]
118. Adhikari, U.; Morris, T.H.; Pan, S. Applying hoeffding adaptive trees for real-time cyber-power event and intrusion classification. *IEEE Trans. Smart Grid* **2017**, *9*, 4049–4060. [CrossRef]
119. Pan, S.; Morris, T.; Adhikari, U. Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. *IEEE Trans. Ind. Inform.* **2015**, *11*, 650–662. [CrossRef]
120. Adhikari, U.; Morris, T.H.; Pan, S. A causal event graph for cyber-power system events using synchrophasor. In Proceedings of the 2014 IEEE PES General Meeting | Conference & Exposition, National Harbor, MD, USA, 27–31 July 2014; pp. 1–5.
121. Beg, O.A.; Nguyen, L.V.; Johnson, T.T.; Davoudi, A. Signal temporal logic-based attack detection in DC microgrids. *IEEE Trans. Smart Grid* **2018**, *10*, 3585–3595. [CrossRef]
122. Ding, Y.; Liu, J. Real-time false data injection attack detection in energy internet using online robust principal component analysis. In Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017; pp. 1–6.
123. Li, B.; Lu, R.; Wang, W.; Choo, K.K.R. Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. *J. Parallel Distrib. Comput.* **2017**, *103*, 32–41. [CrossRef]
124. Villar-Rodriguez, E.; Del Ser, J.; Oregi, I.; Bilbao, M.N.; Gil-Lopez, S. Detection of non-technical losses in smart meter data based on load curve profiling and time series analysis. *Energy* **2017**, *137*, 118–128. [CrossRef]
125. Saad, A.A.; Faddel, S.; Mohammed, O. A secured distributed control system for future interconnected smart grids. *Appl. Energy* **2019**, *243*, 57–70. [CrossRef]
126. Lu, Z.; Wang, W.; Wang, C. From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic. In Proceedings of the 2011 Proceedings IEEE INFOCOM, Shanghai, China, 10–15 April 2011; pp. 1871–1879.
127. Wang, X.; Yi, P. Security framework for wireless communications in smart distribution grid. *IEEE Trans. Smart Grid* **2011**, *2*, 809–818. [CrossRef]
128. Diovu, R.; Agee, J. A cloud-based openflow firewall for mitigation against DDoS attacks in smart grid AMI networks. In Proceedings of the 2017 IEEE PES PowerAfrica, Accra, Ghana, 27–30 June 2017; pp. 28–33.
129. Morris, T.H.; Jones, B.A.; Vaughn, R.B.; Dandass, Y.S. Deterministic intrusion detection rules for MODBUS protocols. In Proceedings of the 2013 46th Hawaii International Conference on System Sciences, Wailea, HI, USA, 7–10 January 2013; pp. 1773–1781.
130. Li, H.; Liu, G.; Jiang, W.; Dai, Y. Designing snort rules to detect abnormal DNP3 network data. In Proceedings of the 2015 International Conference on Control, Automation and Information Sciences (ICCAIS), Wailea, HI, USA, 7–10 January 2015; pp. 343–348.
131. Kemal, M.S.; Aoudi, W.; Olsen, R.L.; Almgren, M.; Schwefel, H.P. Model-free detection of cyberattacks on voltage control in distribution grids. In Proceedings of the 2019 15th European Dependable Computing Conference (EDCC), Naples, Italy, 17–20 September 2019; pp. 171–176.
132. Wang, J.; Shi, D.; Li, Y.; Chen, J.; Ding, H.; Duan, X. Distributed framework for detecting PMU data manipulation attacks with deep autoencoders. *IEEE Trans. Smart Grid* **2018**, *10*, 4401–4410. [CrossRef]
133. Cui, M.; Wang, J.; Yue, M. Machine learning-based anomaly detection for load forecasting under cyberattacks. *IEEE Trans. Smart Grid* **2019**, *10*, 5724–5734. [CrossRef]
134. Berthier, R.; Sanders, W.H. Specification-based intrusion detection for advanced metering infrastructures. In Proceedings of the 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing, Pasadena, CA, USA, 12–14 December 2011; pp. 184–193.
135. 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.
136. Smith, S.W. Cryptographic scalability challenges in the smart grid. In Proceedings of the 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–20 January 2012; pp. 1–3.
137. Wu, D.; Zhou, C. Fault-tolerant and scalable key management for smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 375–381. [CrossRef]
138. Rosinger, C.; Uslar, M. Smart grid security: Iec 62351 and other relevant standards. In *Standardization in Smart Grids*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 129–146.
139. Wang, Q.; Khurana, H.; Huang, Y.; Nahrstedt, K. Time valid one-time signature for time-critical multicast data authentication. In Proceedings of the IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 19–25 April 2009; pp. 1233–1241.
140. Pillitteri, V.Y.; Brewer, T.L. *Guidelines for Smart Grid Cybersecurity*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014. [CrossRef]
141. Tesfay, T.T.; Hubaux, J.P.; Le Boudec, J.Y.; Oechslin, P. Cyber-secure communication architecture for active power distribution networks. In Proceedings of the 29th Annual ACM Symposium On Applied Computing, Gyeongju, Republic of Korea, 24–28 March 2014; pp. 545–552.
142. Lasseter, R.H. Microgrids. In *Proceedings of the 2002 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No. 02CH37309), New York, NY, USA, 27–31 January 2002*; IEEE: New York, NY, USA, 2002; Volume 1, pp. 305–308.

143. Isikman, A.O.; Altun, C.; Uludag, S.; Tavli, B. Power scheduling in privacy enhanced microgrid networks with renewables and storage. In Proceedings of the 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2016; pp. 405–410.
144. Dalamagkas, C.; Sarigiannidis, P.; Ioannidis, D.; Iturbe, E.; Nikolis, O.; Ramos, F.; Rios, E.; Sarigiannidis, A.; Tzovaras, D. A survey on honeypots, honeynets and their applications on smart grid. In Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 24–28 June 2019; pp. 93–100.
145. Rist, L. Introducing conpot. *The Honeynet Project* Available online: https://www.honeynet.org/2013/05/11/introducing-conpot/ (accessed on: 14 November 2022).
146. Jicha, A.; Patton, M.; Chen, H. SCADA honeypots: An in-depth analysis of Conpot. In Proceedings of the 2016 IEEE conference on intelligence and security informatics (ISI), Tucson, AZ, USA, 28–30 September 2016; pp. 196–198.
147. Paverd, A.J.; Martin, A.P. Hardware security for device authentication in the smart grid. In *Proceedings of the International Workshop on Smart Grid Security, Berlin, Germany, 3 December 2012*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 72–84.
148. Castelluccia, C.; Francillon, A.; Perito, D.; Soriente, C. On the difficulty of software-based attestation of embedded devices. In Proceedings of the 16th ACM conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009; pp. 400–409.
149. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur. TISSEC* **2011**, *14*, 13. [CrossRef]
150. Pal, S.; Sikdar, B.; Chow, J.H. Classification and detection of PMU data manipulation attacks using transmission line parameters. *IEEE Trans. Smart Grid* **2017**, *9*, 5057–5066. [CrossRef]
151. Wang, Y.; Amin, M.M.; Fu, J.; Moussa, H.B. A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids. *IEEE Access* **2017**, *5*, 26022–26033. [CrossRef]
152. El Hariri, M.; Harmon, E.; Youssef, T.; Saleh, M.; Habib, H.; Mohammed, O. The iec 61850 sampled measured values protocol: Analysis, threat identification, and feasibility of using nn forecasters to detect spoofed packets. *Energies* **2019**, *12*, 3731. [CrossRef]
153. Li, B.; Lu, R.; Xiao, G. HMM-based fast detection of false data injections in advanced metering infrastructure. In Proceedings of the GLOBECOM 2017–2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6.
154. Marali, M.; Sudarsan, S.D.; Gogioneni, A. Cyber security threats in industrial control systems and protection. In Proceedings of the 2019 International Conference on Advances in Computing and Communication Engineering (ICACCE), Sathyamangalam, India, 4–6 April 2019; pp. 1–7.
155. Mix S.; Hadley M.; Becker F.; Cenzon E.; Corrigan R.; Dood M.; Edgar T.; Formea J.; Goransan C.; Huntley C.; et al. *IIEEE 1711.2-2019*; IEEE Standard for Secure SCADA Communications Protocol (SSCP). EEE Standards Association: Piscataway, NJ, USA, 2020; pp. 1–37. [CrossRef]
156. Ferst, M.K.; de Figueiredo, H.F.; Denardin, G.; Lopes, J. Implementation of secure communication with modbus and transport layer security protocols. In Proceedings of the 2018 13th IEEE International Conference on Industry Applications (INDUSCON), Sao Paulo, Brazil, 12–14 November 2018; pp. 155–162.