Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review

MUHAMMAD NOUMAN NAFEES, Cardiff University, UK
NEETESH SAXENA, Cardiff University, UK
ALVARO CARDENAS, University of California, Santa Cruz, USA
SANTIAGO GRIJALVA, Georgia Institute of Technology, USA
PETE BURNAP, Cardiff University, UK

The smart grid, regarded as the complex cyber-physical ecosystem of infrastructures, orchestrates advanced communication, computation, and control technologies to interact with the physical environment. Due to the high rewards that threats to the grid can realize, adversaries can mount complex cyber-attacks such as advanced persistent threats-based and coordinated attacks to cause operational malfunctions and power outages in the worst scenarios: The latter of which was reflected in the Ukrainian power grid attack. Despite widespread research on smart grid security, the impact of targeted attacks on control and power systems is anecdotal. This paper reviews the smart grid security from collaborative factors, emphasizing the situational awareness. Specifically, we propose a threat modeling framework and review the nature of cyber-physical attacks to understand their characteristics and impacts on the smart grid's control and physical systems. We examine the existing threats detection and defense capabilities, such as intrusion detection systems, moving target defense, and co-simulation techniques, along with discussing the impact of attacks through situational awareness and power system metrics. We discuss the human factor aspects for power system operators in analyzing the impacts of cyber-attacks. Finally, we investigate the research challenges with key research gaps to shed light on future research directions.

CCS Concepts: • **Security and privacy → Distributed systems security**; *Intrusion detection systems.*

Additional Key Words and Phrases: Smart Grid, Threat Modeling, Complex Cyber-Physical Attacks, Operational Technology Attacks, Intrusion Detection System, Deep Learning, Federated Learning, Moving Target Defense, Co-simulation, Situational Awareness, Metrics

ACM Reference Format:
Muhammad Nouman Nafees, Neetesh Saxena, Alvaro Cardenas, Santiago Grijalva, and Pete Burnap. xxxxx. Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review. 1, 1 (April xxxxx), 35 pages. https://doi.org/xxxxx

1 INTRODUCTION

Smart Grid (SG) networks, as a part of Critical National Infrastructure (CNI), are deemed to be the next evolutionary step of reliable and efficient power delivery networks [96]. Moreover, SG networks have become an epitome of Industrial Revolution 4.0 (a.k.a. Industry 4.0), which has launched the world into physical/virtual reality by introducing cyber-Physical Systems (CPSs), physical networks, and cyber network architecture to control various processes efficiently [27]. Industry 4.0 is known to optimize the computerization of Industry 3.0, and it is formed by combing Information and

Authors' addresses: Muhammad Nouman Nafees, nafeesm@cardiff.ac.uk, Cardiff University, UK; Neetesh Saxena, Cardiff University, UK, saxenan4@cardiff.ac.uk; Alvaro Cardenas, University of California, Santa Cruz, USA, alacarde@ucsc.edu; Santiago Grijalva, Georgia Institute of Technology, USA, sgrijalva@ece.gatech.edu; Pete Burnap, Cardiff University, UK, burnapp@cardiff.ac.uk.

XXXX-XXXX/xxxxx/4-ART $15.00
https://doi.org/xxxxx

Communication Technology (ICT) and Operational Technology (OT) for monitoring and control processes, maintenance and predicting failures, and many other functions [115]. Compared to other industry 4.0 environments such as the oil and gas industry, where implementing and leveraging the real-time IT-OT paradigm is falling behind since operations of most oil and gas companies are cross borders, and it is challenging to implement the industry 4.0 initiatives. However, SG networks effectively employ advanced ICTs, Industrial Internet of Things (IIoT), big data analytics, and Intelligent information processing along with OT to allow utilities to monitor and control power generation, transmission, and distribution processes more efficiently, reliably, and securely.

IT systems in SG networks include data servers, communication technologies, and cloud infrastructure. OT systems are defined as computing systems to monitor, control, and manage physical equipment and industrial operations. Such systems in SG infrastructure include Supervisory Control and Data Acquisition (SCADA): computing system used for monitoring and controlling assets over large geographical areas, Programmable Logic Controllers (PLCs)/Remote Terminal Units (RTUs): industrial computers to execute simple logic processes, Phasor Measurement Units (PMUs): devices used to estimate phase angle and magnitude of the voltage or current in the SG, and Actuators: components that are responsible for driving the actual physical mechanism based on commands from controllers such as PLCs.

Despite the significance of the SG's cybersecurity, much of what is known about the complex cyber-attacks against the SG is anecdotal. The attacks such as Advanced Persistent Threat (APT) attacks and coordinated attacks, the brand of attacks used in Stuxnet and Ukrainian power grid, challenge the SG's security despite the presence of Intrusion Detection Systems (IDSs). Stuxnet, which used zero-day exploits, covertly installed the malicious program onto the system to sabotage the nuclear development program of Iran [107]. On the other hand, attackers performed a coordinated cyber-attack on the Ukrainian power grid, which resulted in a massive power outage for several hours affecting approximately 225,000 customers in 2015 [41]. Power was lost for six hours, and the SG suffered a 130 MW load loss.

Cyber-attacks targeted at the SG's control operations are commonly referred to as cyber-physical attacks or OT attacks; the former is the major subset of the latter, and, as such, the terms can be used interchangeably. SG cyber-attacks may also disrupt the Confendetialty, Integrity, and Availability (CIA) triad of control systems: The CIA triad is an essential security goal of the SG in a communication network, protection, management, and operation of the energy system [25]. In this context, confidentiality attacks do not aim to modify the transmitted information; however, these attacks aim to obtain the desired information. For instance, an attacker can mount an eavesdropping attack to sniff wireless transmission between nodes on a communication network in the SG. To this end, data integrity attacks aim to modify the legitimate processes and content of original data in the SG. Some possible examples of such attacks are FDI, replay, message delay, and Man-in-the-Middle (MITM) attacks, where an attacker may alter voltage and power flow sensors measurements, billing data, and control commands to disable the operating states of the SG. Similarly, an availability attack may not only modify the information; however, such attacks aim to destabilize authorized access in the SG. Denial of Service (DoS), time-delay, and jamming attacks are the few common examples of such attacks in the SG [35].

The above threats and cyber-attacks emphasize and stipulate the importance of effective detection and monitoring system for the SG. Moroever, understanding the impact of such attacks and threats is critical. Creating a high-fidelity model of the SG entails significant resources, which can be beyond the reach of most, if not all, cyber-security researchers and experts. Therefore, co-simulation tools can provide the experimental platform to analyze the impact and implications of complex multistage attacks on the cyber and operational domain of the SG. Moreover, such co-simulation tools can effectively provide essential training to power system operators to enhance Situational Awareness

(SA) by demonstrating the impact of cyber-attacks. In this direction, SA includes being cognizant of the current state and identifying any potential changes to that state [5]. In this context, the power system operators should be able to discriminate disturbances between normal power operations and cyber-attack-led changes. Cyber-physical situational awareness metrics need to be systematically explored in conjunction with power system metrics to enhance SA. Metrics are critical in measuring the overall security of the SGs' SA, as also shown in [85].

1.1 Existing Surveys

As a popular area due to its critical significance, several studies (see, e.g., [57, 61, 67, 70, 124, 130]) have been dedicated to reviewing SG security from different perspectives. Surveys that focus on SG cyber-attacks and detection have been presented in [22, 35, 57, 124]. To this end, Liang et al. reviewed FDI attacks against modern power systems in which the authors discussed the physical and economic impacts of successful attacks on the SG [57]. As an early effort to review FDI attacks, they did not consider a broad range of cyber-physical attacks and did not cover other aspects of SG security. Similarly, in [22], the authors specifically considered coordinated data injection attacks and discussed defense in terms of secure PMU placement and distributed attack detection. In 2021, the authors provided a good summary of cyber-physical attacks in terms of their target components in the SG and provided several defenses, including watermarking and data-driven approaches [124]. In 2022, the authors analyzed the methods, tactics, and tools that attackers employ to perform reconnaissance activities in the APT-like attacks [92]. The work provided a brief overview of the coordinated power grid attack and linked the adversarial reconnaissance as part of complex attacks; however, the SG security was not the scope of the paper.

Various surveys have specifically focused on the detection of cyber-attacks in the SG [32, 61, 63, 73, 87]. In 2021, Liu et al. Provided a deep analysis of rule learning techniques concerning cyber-attack detection and their applications in IDS, emphasizing the potential of artificial neural networks for rule induction in the SG [61]. In [63], the authors particularly focused on anomaly detection using deep learning-based techniques for cyber-physical systems, including the SG. The work provided a detailed taxonomy in terms of anomaly types, implementation strategies concerning the deep learning model, and evaluation metrics. In [87], Radoglou-Grammatikis et el. provided a comprehensive analysis of 36 Intrusion Detection and Prevention Systems (IDPs). A survey on the detection algorithm, particularly for FDI attacks, is presented in [73]. The authors provided a summary of model-based and data-driven algorithms to detect FDI attacks in the SG, emphasizing the pros and cons of these algorithms. However, the work specifically considered the detection of FDI attacks only.

In 2022, the authors discussed new findings and development regarding SG security issues and privacy breaches [70]. In [130], a comprehensive overview of the cyber-physical energy system is provided, in which the authors demonstrated and leveraged threat modeling methodology to evaluate system performance under adverse scenarios while evaluating the system performance using specific metrics. In [25], potential vulnerabilities in SG are investigated along with classifying cyber-attacks based on confidentiality, integrity, availability, and accountability. The impact of FDI and jamming attacks are surveyed by conducting experiments using co-simulation tools in [53]. In this context, the authors reviewed various co-simulation tool and their characteristics applicable to SG research. However, SG security was not the scope of the work.

In 2022, the authors in [5] provided a comprehensive review of cyber SA systems, emphasizing key design principles, framework, classifications, data collection, analysis of the techniques, and evaluation methods. Nevertheless, the review of the SA framework did not specifically cover SG security. Moreover, the works [23] and [85] reviewed the application of SA technologies for SG and system security metrics, respectively. Resilience metrics for power systems are reviewed in

Table 1. Comparison with Existing Review Works

Ref.	Complex attack characteristics (e.g., APT)	SG cyber-physical attacks	IDS	Co-simulation	CPSA and metrics	PS metrics	Year
[70]	ND	✓	✓	ND	LD	ND	2022
[61]	ND	LD	✓	ND	LD	ND	2021
[5]	LD	ND	✓	ND	✓	ND	2022
[67]	ND	ND	✓	ND	ND	ND	2021
[130]	ND	✓	LD	LD	LD	✓	2021
[25]	ND	✓	✓	ND	ND	ND	2018
[92]	✓	ND	LD	ND	ND	ND	2022
[32]	ND	✓	✓	ND	✓	ND	2018
[124]	LD	✓	✓	ND	LD	ND	2021
[63]	ND	✓	✓	ND	LD	ND	2021
[13]	ND	LD	ND	ND	ND	✓	2020
[53]	ND	LD	ND	✓	ND	ND	2019
[73]	LD	✓	✓	ND	LD	ND	2019
[85]	ND	ND	LD	ND	✓	ND	2016
[22]	✓	✓	✓	ND	ND	ND	2012
[78]	ND	✓	✓	ND	ND	ND	2020
[87]	LD	✓	✓	ND	LD	ND	2019
[57]	ND	✓	✓	ND	ND	ND	2016
[88]	ND	ND	ND	ND	ND	✓	2020
[35]	✓	✓	LD	ND	LD	ND	2020
Ours	✓	✓	✓	✓	✓	✓	2022

IDS: Intrusion detection system; CPSA: Cyber-physical situational awareness; PS: Power system; ✓ - Detailed discussion; LD – Limited discussion; ND – No discussion

[78] and [13]. Bhusal et el. [13] provided a critical review of power system resilience metrics and evaluation methods. The survey also includes discussions on the universally accepted and standardized definitions of metrics. However, the cyber-security of the SG was not the focus of the survey paper.

1.2 Comparison with Our Survey

Despite the fact that SG security has become a central research topic for some time and previous reviews have their own advantages, there are many scattered security aspects tailored for the particular application domain, and a systematic organization of these individual aspects from an SA perspective is missing. For example, some of the works presented in [57] and [22] focused on reviewing the FDI and coordinated attacks, respectively. In contrast, our survey provides an in-depth analysis of complex attack characteristics and all major attack types that fit with the nature of SGs. In [124], cyber-physical attacks against the SG are discussed in terms of their target components, but cyber-physical SA and power system metrics were not discussed from the attack detection perspective. Other works [61, 63, 73] focused on reviewing the cyber-attack detection techniques, while the other aspects of the SG security were not the scope of these papers. In [130], threat modeling was used to evaluate system performance using metrics; however, complex attack characteristics and SA were not the scopes of the work. In [5] and [85], the authors discussed the cyber SA framework and system metrics, respectively. However, SG security was not the scope of these works. To the best of our knowledge, our work is the first contribution that studies the aspects of SG security from an SA perspective involving power system and security metrics, which differs from the aforementioned surveys. Table 1 provides a comparison between the existing survey papers and our paper in terms of the main covered areas and publication year.

1.3 Our Contributions

We believe that SG security entails recognizing the breadth of collaborative factors, including SA-based dimensions that contribute to the overall cyber-physical security of the SG. Specifically,

we need to answer the following research questions: (1) how can existing SG security be viewed in terms of the threat models from the attackers' perspective? (2) What are the complex cyber-attack characteristics and types of existing cyber-physical attacks, along with the impacts of such attacks? (3) What are the existing types of detection approaches, co-simulation, and visualization tools? How can existing detection methods be categorized in terms of the performance evaluation from the existing literature? (4) What key cyber-physical SA and power system metrics can be utilized to measure the SG security state (e.g., SA for security decision-making)? (5) What are the challenges, key research gaps, and future research directions for the SA-based cyber security of the SG?

Consequently, after recognizing a set of ways to motivate the understanding of the research questions, we have chosen to review the SG security by simultaneously considering multiple aspects. Therefore, this paper contributes to the literature by providing a detailed review of the SG security landscape from multiple factors and dimensions, highlighting overall SA. The main contributions are centered on answering the aforementioned research questions. This new security perspective that combines power system metrics with other security aspects provides the Security Operation Center (SOC) and power system operators with intuitive SA to respond to SG security threats. In this sense, our work makes the following contributions:

- **A comprehensive review of the nature of complex cyber-attacks:** We have provided an overview of the existing threat models and proposed a threat modeling framework, specifically tailored for the SG, which is comprised of three parts, the adversary model, the asset/vulnerability model, and the attack model. We then provided an in-depth analysis of complex attack characteristics such as APT attacks, coordinated attacks, and cascading attacks against the SG. More specifically, we discussed potential tactics and techniques in the APT attacks, specifically tailored for the SG. By doing this, we discussed different attack types that fit with the nature of the SG networks. We also revisited techniques and tactics commonly used by the attackers to identify current trends and evaluate the impacts of these attacks on critical operations.
- **Analyzing Detection and Monitoring Capabilities:** We have reviewed and detailed the taxonomy of IDS and threat detection techniques against advanced cyber-attacks with recent literature. To this end, we have reviewed the existing Machine Learning (ML), Deep Learning (DL), and Federated Learning (FL) based techniques for cyber-attack detection in the SG. Moreover, we have also discussed other detection and defensive techniques such as Moving Target Defense (MTD). We revisited the simulation and visualization tools and techniques employed in the SG, identified their limitations, and supported applicability (e.g., real-time) to reflect on their effectiveness in real-world settings. In addition, we also discussed the role and significance of the Security Operation Center (SOC) in the SG.
- **Cyber-Physical Situational Awareness:** We have provided an overview of the significance of Situational Awareness (SA) and provided insights into the phases of SA such as situation perception, comprehension, and projection. We have identified cyber-physical SA metrics for the system operators to improve their decision-making capabilities. We then analyzed cyber and power system metrics separately and discussed the importance of human factor and awareness training in noticing the footprint of attacks in the SG.
- **Challenges, key gaps, and future research directions:** Finally, we have reflected on identifying current research challenges and key gaps in line with our work's scope. We then highlighted the key areas of research where more work is needed as future research directions to address the cyber-security issues of the SG.

1.4 Paper Organization

Section 2 provides an in-depth discussion on the nature of cyber-attack. We discuss the recent threat models, explain the attack characterization, review various cyber-physical attack types along with their impacts, and provide specific attack classifications relevant to the nature of SG. Section 3 provides a survey of IDS, discusses the signification of Security Operation Center (SOC) monitoring and visualization tools, and reviews co-simulation tools and techniques in SG. Section 4 discusses cyber-physical situational awareness, power system metrics, human factors, and SA training needs. Section 5 highlights the research challenges, key gaps, and future directions. Finally, we provide the conclusion in section 6.

2 NATURE OF CYBER-ATTACKS

This section first explores the recent threat models to understand the possible combination of threat stages. We then propose a threat model specifically tailored for the SG. We discuss the in-depth analysis of complex attack characteristics such as APT, coordinated, and cascading attacks against the SG. Finally, we discuss different attack types that fit with the nature of the SG networks.

2.1 Threat Models

Threat modeling is vital in discovering potential vulnerabilities in SG infrastructure. The primary aim of threat modeling is to identify, classify and describe threats to highlight a campaign of attacks or attackers. However, SG comprises multiple layers and assets; therefore, modeling all possible scenarios can be challenging as it entails exhaustive resources and human effort.

STRIDE. Various threat modeling approaches have been proposed and adopted to understand the nature of cyber-attack scenarios. For example, STRIDE (Spoofing, Tampering, Repudiation, Denial of Service, and Elevation of Privilege) is a well-established threat modeling framework for the security assessment of the infrastructure [45]. STRIDE mainly uses data flow diagrams to map system threats to the corresponding vulnerable system asset to address security threats to integrity, confidentiality, availability, authentication, authorization, and nonrepudiation. In [38], the authors use the STRIDE model to create a threat model of a digital secondary substation and its communication with the control center. However, it primarily addresses general types of threats; therefore, to understand threat severity from the perspective of different components' vulnerabilities and additional attack vectors, threat modeling needs to be addressed from multiple perspectives.

MITRE ATT&CK. In 2020, MITRE corporation [6] launched the ATT&CK framework for ICS to describe tactics, techniques, and procedures an attacker could use to compromise an infrastructure stealthily. ATT&CK for ICS gathers threat intelligence from various sources such as enterprise networks to ICS networks, leveraging threat intelligence to incorporate into the ICS system and field devices such as PLCs, IEDs, and RTUs.Specifically, ATT&CK for ICS covers four primary categories: (1) assets, (2) functional level, (3) tactics, and (4) techniques. To this end, assets include systems such as engineering workstations, control servers, and HMI. Whereas functional level corresponds to the Purdue architecture; for example, level 0 includes physical devices (e.g., sensors and actuators), and level 2 includes SCADA, engineering workstations, and Human-Machine Interface (HMI). The last two categories of the framework, tactics and techniques, refer to an attacker's objective and the activities an attacker employs to achieve his goal. In [128], MITRE ATT&CK is extended to develop threat modeling against social-collective attacks. In this context, adversary behavior is reflected to represent social, cyber, and physical domains of the SG, while the motivation of the work is to demonstrate the propagation of the attack from the social-cyber interfaces to physical system malfunctions.

Table 2. SG Threat Model

Adversary Model	
Component/Detail	**Description**
Threat actors	State-sponsored actors, terrorists, cybercriminals, hacktivists, cyber fighters, disgruntled employees
Attacker motivation	Ransomware, competitor discrediting, cyberwarfare, economic gain, terrorism/political
Knowledge	Strong knowledge (operational information of cyber system and Jacobian measurement matrix of power system), limited knowledge (partial knowledge of network and system), zero-knowledge (Blackbox attack)
Access	Physical access, remote access, close proximity access
Resources	Substantial privileges, limited privileges
Asset/Vulnerability Model	
Component/Detail	**Asset/vulnerability**
Electrical assets	Sensors: insecure input validation [71]; Relays: buffer overflow [103]; Circuit Breakers: false authorization and tripping [39]; ADC: malicious sampling frequency and range [14]; transmission lines: physical attacks
Control system and wide-area monitoring control assets	PLCs: malicious firmware update and unauthorized command line access [30]; IEDs: time synchronization spoofing [104]; RTUs: weak protection mechanism [102]; HMI: vulnerable input/output values manipulation [25]; Gateway: vulerable to protocol translation attack [10]; PMUs: vulnerable to GPS spoofing [126]
ICT assets	Routers: vulnerable to various communication attacks, such as remote access and configuration settings; Switches: insecure authentication; Historian servers: buffer overflow vulnerability [14]
SG communication protocols	Modbus: vulnerable to integrity attacks [25]; DNP3: vulnerable scanning and packet modification attacks [25] ; ICCP: vulnerable to integrity violation, interception and alteration [89]; GOOSE: vulnerable to integrity attacks [80, 122]; MMS: vulnerable to DoS attack, SMV: non-routable and non-blocking; Profibus: lacks authentication and authorization controls; HART: vulnerable to integrity attack
Processes and applications	State estimation: injection/integrity attacks; AGC: malicious command injection and integrity attacks; LFC: injection and scale attacks; UFLS: injection/integrity attacks; wide-area frequency control: integrity attacks
Status	Circuit breaker status, power factor, MW, current, voltage, geolocation status
Persons	Power system operators, network engineers, administrators, developers, SCOs – vulnerable to social engineering attacks
Attack Model	
Component/Detail	**Description**
Initial access	Watering-hole, exploit internet-facing and remote access software, removable media, social engineering, supply chain, wireless compromise
Attack premise	Attacks on cyber domain, invasive attacks, non-invasive attacks
Exploit vulnerability	Exploitation of vulnerabilities in any critical assets, processes, and communication protocols to mounts malicious threats. For example, if an adversary modifies PLC's ladder logic, it can mount direct threats to control process security
Attack type	Cyber-attacks (Sinkhole, sybil, wireless compromise, MITM), physical attack (line cuts, damage equipment), cyber-physical attack (DoS, control logic modification, modify module firmware)
Attack propagation	Probability of attack propagation in any of the given domains - Electrical assets, control system assets, ICT assets, SG communication protocols
Lateral movement	Techniques/tools for lateral movement; for example, default credentials, socket duplication and lateral tool transfer
Attack frequency	Iterative attacks, non-iterative attacks
Attack impact	Outages, DoS, cascading effect of failures, control process loops malfunctions, irreparable damage to the expensive equipment and generators, falsify operator interface and monitoring, disrupt real-time data, historical data, and alarming

HMI: Human–Machine Interface, MUs: Merging Units, DNP3: Distributed Network Protocol 3, ICCP: Inter-Control Center Communications Protocol, GOOSE: Generic Substation Events, MMS: Manufacturing Message Specification, SMV: Sampled Measured Value, LFC: Load Frequency Control, AGC: Automatic Generation Control, UFLS: Under Frequency Load Shedding

Cyber Kill Chain. Another popular threat model framework is the "kill chain," which was initially used as a military concept to understand the structure of the attack in the various phases of the attack lifecycle. In this direction, the kill chain is defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. The kill chain can provide a holistic view of the attack patterns and phases, and it also includes mapping the tactics, techniques, and tools used to mount attacks [5]. Lockheed Martin constructed the evolution version of the kill chain known as the Lockheed Martin Intelligence-Driven Defense model (LMIDDM). The Cyber Kill Chain framework is a component of LMIDDM that aims to increase the threat modeling framework's situational awareness and methodology maturity.

Proposed Threat Model for SG. There is no perfect method that can fulfill all the essential criteria for infrastructure security; some threat models are focused on assets, others on adversaries, some methods prioritize risk, and many others are tailored for IT systems. Therefore, we recommend developing a holistic threat modeling that integrates both the IT and OT perspectives of the SG and

considers the business impact of the failure of physical components. The proposed threat modeling framework in this manuscript incorporates the elements of various threat models in which the MITRE ATT&CK knowledge base [9], NIST electric utility guidelines [68], and European Union Agency for Cybersecurity (ENISA) threat landscape [105] are used as foundations specifically tailored for the SG. The threat model is designed from an attacker's point of view; understanding the adversary model and types of attacks, processes, and the stages involved, greatly benefits the defenders to better defend against complex cyber-physical attacks. Towards this end, the model incorporates an adversary, an asset/vulnerability, and an attack model. We discuss the mitigation in terms of detecting cyber-physical attacks, incorporating useful ICT and power system metrics, and raising situational awareness in other Sections of this manuscript. Table 2 presents the proposed threat modeling framework for the SG.

2.2 Characteristics of Attacks

In this subsection, we explore the characteristics of cyber-attacks to enhance the understanding of challenges to SG security. Towards this end, we utilize the MITRE ATT&CK and the cyber kill chain threat modeling approach to explain the stages of cyber-attacks.

2.2.1 Advanced Persistent Threat (APT) Attack. Advanced Persistent Threat (APT) is a dangerous category of complex cyber-attacks against the SG infrastructure, and it is characterized by the combination of multiple attack components [69]. APTs are often achieved by state-sponsored threat actors that are well-funded, and they usually have significant resources to plan and execute the attack on the SG's infrastructure with an agenda of disrupting power operations at a large scale. The initial infiltration techniques used by the attackers focus on specific targets, and the attack is carried out surreptitiously. While some techniques used to establish a foothold are common, diverse types of new stealthy penetration tools and malware are mainly utilized for the aforementioned purpose. In this paper, we characterize stages of the APT attack based on Lockheed Martin's cyber kill chain [7] and MITRE ATT&CK framework [6] as these models are more relevant to the SG infrastructure. We divide the attack into six stages, and we explain the goal of each stage.

Stage 1: Reconnaissance – The first stage in APT against the SG entails understanding and learning about the target design and entry points. The threat actors employ various tactics to collect enough information before moving to initial access to the system [92]. Adversaries aim to obtain technical information such as SG topology and control system capabilities as well as information about operator personnel during the reconnaissance phase. In [44], Keliris et al. demonstrate the feasibility of collecting vital information of the power system, including its critical locations, by using the publicly available Open-Source Intelligence (OSINT) datasets. In addition, the web-based search engine "Shodan" can also provide essential information about the SG's discoverable components connected to the internet.

Stage 2: Weaponization – Adversaries create a malicious "remote" access malware tailored to a specific vulnerability to infiltrate the system [98]. In some instances, adversaries may inject malicious codes into the firmware of critical devices by performing supply chain attacks. For instance, attackers may gain access to devices such as PLCs, smart meters, and sensors during the supply chain process, thereafter, a malicious section of code can be inserted into the firmware of these devices in a reliable manner. Other potential methods of implanting malware include emails with infected attachments, the use of watering-hole domains, and injecting malware in removable media such as USB.

Stage 3: Delivery – During this phase of APT, attackers aim to deliver their created malware to the process control systems of the SG. Methods such as spear-phishing emails, spear-phishing via service, watering-hole attacks, social media interactions, supply chain, and removable media

Table 3. APT Tactics and Techniques for the SG

Reconnaissance		
Tactic	Technique/Tools	Description
Technical intelligence gathering	Obtain OSINT datasets for SG	Attackers can obtain essential information from publicly available resources such as Open Source Intelligence (OSINT) datasets
	Utilize web-based search engine "Shodan"	Adversaries may use "Shodan" search engine to identify SG's discoverable components connected to the internet to probe the SCADA system for weaknesses
	Search vulnerabilities from ICS-CERT	Attackers may use ICS-CERT advisories to search for vulnerabilities in SG components
	Identify supply chains	Understanding supply chains of SG's field devices and other components may provide adversaries with higher chances to exploit technology
	Determine firmware versions of the devices such as IEDs and PLCs	Acquiring firmware versions of PLCs can help adversaries to test and validate their malicious codes on similar firmware versions before launching an actual attack
	Social engineering for technical information	The attackers may masquerade as an internal employee to attempt to trick an actual employee to divulge technical information about SG's architecture
	Identify targeted SG's job postings	Job postings may give out information about the gaps or weaknesses in the skillset of any particular site
Employees information gathering	Social media exploration	Open-source information of SG's employees can be obtained by adversaries via Facebook, Twitter, Instagram, etc. This can make them potential target to social engineering attacks.
	Identify virtual groups	Adversaries may attempt to identify virtual groups of SG's employees and may attempt to join it using social engineering techniques
Weaponization		
Tactic	Technique/Tools	Description
Malware Implant	Supply chain compromise	An adversary may maliciously program the SG components during the manufacturing process
	Email attachment	Malware can be embedded as an attachment to emails e.g., MS word doc with macros
	Use of watering-hole domains	Attackers may plan to implant a malware in the websites expected to be visited by utility employees
	Injecting malware in removable media	USB can be used to transfer malware
Delivery		
Tactic	Technique/Tools	Description
Social engineering	Spear-phishing	Adversaries may send spear-phishing emails with a malicious attachment
	Spear-phishing via service	Attackers may masquerade as third-party vendors and send emails with a malicious attachment
	Social media interaction	Malicious attachments can be sent using social media platforms
Supply chain and removable media	Planned delivery manipulation or trusted relationship	Insider employee can be used by an adversary to install field devices with malicious firmware
Exploitation and Installation		
Tactic	Technique/Tools	Description
Exploitation for credential access	Internal spear-phishing	Attackers may use internal spear-phishing technique to gain access to other user accounts
Remote services	SMB/Windows admin shares	Valid accounts can be used by threat actors to gain access to remote connections
Zero-day exploits	Malware implant	Stealthy malware can be installed to use a zero-day exploit in the system for further exploitation
Password cracking	Hydra, SecretsDump, etc.	Open-source free tools can be used to crack passwords to gain high-level privilege access
Establishing local accounts	Use of script to create local accounts	Threat actors can create legitimate local accounts to prevent from being locked outside the system
Command and Control (C2)		
Tactic	Technique/Tools	Description
Remotely control of OT processes	Malicious commands to relays, opening of breakers	Having infiltrated from IT to OT, attackers can attempt to disrupt power operations by opening breakers
Post-Attack		
Tactic	Technique/Tools	Description
Remove traces	KillDisk	Use of various tools such as "KillDisk" to remove traces of intrusion

are often successful. In some cases, the threat actors may involve operator personnel to upload damaging malware to control system processes via USB [98]. Besides, backup paths are also created to ensure persistent access to the system.

Stage 4: Exploitation and Installation – In this stage of the attack, malicious malware code is executed to harvest user credentials in conjunction with the exploitation of vulnerabilities in the system. An adversary may steal user credentials with high-level privileges to access a high level of

power topology and sensitive information. Attackers may also try to access files pertaining to the SCADA systems, such as the SCADA wiring diagram, and transfer the critical files using remote file transfer software. Threat actors create local administrative accounts in the target system to maintain their persistence in the environment. Also, several tools and software are installed from a remote server to further exploit the communication between different devices.

Stage 5: Command and Control (C2) – The attackers move on to infiltrate from IT to OT in order to disrupt OT operations and processes. Threat actors may gain access to SCADA interfaces, and different critical power operations can be disrupted, such as power transmission to customers. For example, attackers can open the breakers to cause a blackout.

Stage 6: Post-Attack – Following the accomplishment of the mission, attackers remove all the traces of their operations for a clean exit. All the backdoors, log files, local user accounts, and any other critical files are deleted by the attackers. For example, the attackers can use "KillDisk" software to remove their traces of the intrusion.

Table 3 shows the corresponding APT stages of tactics and techniques employed by adversaries along with their impacts as mapped in cyber kill chain stages.

2.2.2 Coordinated Attack. While a traditional cyber-attack aims to target the infrastructure opportunistically in one attempt, a coordinated attack follows the multi-stage attack pattern where adversaries carefully mount a series of cyber-attacks in a coordinated manner to cause maximum damage to the infrastructure [36]. The state-sponsored cyber terrorism has become more visible, and thus the integrated, coordinated attack has become an imminent threat to Critical National Infrastructure. The simultaneity of Distributed Denial of Service (DDoS) attacks coupled with other integrity attacks is employed in launching a synchronized coordinated attack by the adversaries [121].

The cyber-attack on the Ukrainian power grid is regarded as the epitome of a successfully synchronized and coordinated cyber-attack on the SG. On December 23, 2015, a power blackout occurred in Ukraine. Three power companies were mainly targeted and disturbed by this remote coordinated attack. This attack had affected up to 225,000 customers across three different distribution-level territories, including almost thirty substations and two power distribution centers. The finding reports [16] suggest that the attack lasted for several hours. We map cyber kill chain stages to reflect different phases of this attack.

Phishing Attack - The social engineering technique "Spear Phishing Email" was executed to gain initial access to the network by delivering a malware "BlackEnergy-3" embedded in a Microsoft Word document.

Malware Delivery - The destructive variant of malware "BlackEnergy-3" targeted Windows operating systems of the network by exploiting the backward compatibility of Windows 7. The malware successfully bypasses the watermark created by Windows upon switching on the boot configuration option.

Credential Theft - Once the adversaries compromised the Windows domain controllers where user networks are managed; user credentials were stolen to access the administrative level services.

Pivot to SG OT - The specific plugins in BlackEnergy were utilized to steal the users' credentials of the employees to get access to the SCADA control system. Upon getting access to Virtual Private Networks (VPNs), Uninterruptible Power Supplies (UPS) were reconfigured. This phase was also regarded as the reconnaissance phase in which attackers closely monitored the distribution management system.

Craft Payload - The adversaries modified the firmware of Serial-to-Ethernet converters at multiple substations. Such malicious firmware on the converters prevented the operators from

sending control commands to re-close circuit breakers in the event of a blackout from the SCADA network to substation control systems.

Execute Pre- Attack - The attackers managed to enter the SCADA system using the hijacked VPNs and disabled the backup UPS that they had already reconfigured.

Pivot to OT Attack - The attackers employed multistage attacks, which involved remote exploitation and lateral movements across multiple systems. More specifically, HMI was used to open the power breakers remotely, which caused the power outage. Simultaneously, the Telephone-Denial-of-Service (TDoS) attack was launched to prevent customers from reporting the outages by calling call centers. Thousands of illegitimate and bogus calls flooded the call center's system and provided extra time to the adversaries to complete their mission.

Post-Exploit Attack - At the end of the attack, a variant of KillDisk Malware was used to erase master boot records and log files on workstations to delay the restoration actions [56]. More specifically, KillDisk removed a Windows system process linked to serial-to-ethernet communications. According to the attack analysis report [16], the outages were caused by manipulation of the control systems, and BlackEnergy 3 and KillDisk were primarily used to enable the attack or delay restoration efforts.

2.2.3 Cascading Attacks. The SG is a complex system where hundreds of thousands of nodes are interconnected. The inter-dependencies of the components and functions in the SG make it susceptible to one of the most critical concerns known as cascading failures [77]. A Single Point of Failure (SPF) can propagate to other functions of the system, which can eventually trigger a power outage [119]. In other words, fault in one power transmission line triggers the power system's physics law, which can reroute the power to other power transmission lines. Such a scenario can potentially overload the power transmission line to the extent that it exceeds the threshold capacity of transmitting power, eventually triggering cascading failures. Cascading failures can be caused due to many factors such as human mistakes (e.g., inadvertently opening of breakers by any operator), system malfunctions (e.g., power transmission line failures), severe weather conditions (e.g., lighting strikes), and cyber-physical attacks (e.g., coordinated DDoS attacks launched by state-sponsored actors). Many past incidents of cascading failures were caused by inadvertent factors that triggered a power outage. For instance, the 2003 blackout in Italy was caused by an interdependent cascading failure; the failure of a few power nodes malfunctioned several communication nodes and triggered the failure of more power nodes [8]. Just because such failures occurred due to other factors does not preclude them from occurring due to cyber-attacks in the future.

A combination of cyber-physical attacks in conjunction with the exploitation of power function's time criticality can be employed to cause larger blackouts [119]. Attackers can cause cascading failures by launching a physical attack on sensitive branches or high voltage power transmission line causing the power flow redistribution across other power transmission lines. In turn, the other power transmission lines can get overloaded to the extent that they can exceed their threshold capacity to transmit power which can cause failures in those lines as well. This fault propagation can extend to other lines until most power transmission lines have failed, and it can eventually trigger cascading failures. Once cascading failures happen, the fast sequential outages along cascading paths can prevent corrective measures from controlling cascading propagation in time, leading to further cascading failures and sequential outages [86].

2.3 Types and Impacts of Cyber-Physical Attacks

One possible way to understand the nature of attacks is to classify SG attacks as cyber, physical, and cyber-physical attacks. In cyberattacks, adversaries manipulate the system without ever gaining physical access to the device. In a physical attack, an adversary may gain physical access to a critical

device or component in SG networks to physically damage it, disable it, or utilize the device in an undesirable way [109]. One possible example is physically damaging the power transmission lines. In cyber-physical attacks, the ultimate goal of the adversary is to manipulate or damage a particular device or component in the SG by using cyber-attacks to disable the physical operations of the SG [124]. For example, an adversary may mount False Data Injection (FDI) attacks on compromised sensors or controllers to modify the input of a power plant so that false feedback on load frequency control can be created: The attack can force the power system to oscillate at its resonant frequency. In this subsection, we mainly focus on the cyber-physical attacks in the SG.

2.3.1 Physics Aware Control Command Attacks. The models of the underlying physical dynamics that follow the laws of physics, such as Kirchhoff laws in power systems, are considered the driving factor behind the control of the physical plant. Control commands are often used to stabilize the physical plant based on the physical dynamics [34]. For example, control commands are used to update the generation set-points by the PLCs to ensure the equilibrium between power generation and consumption. Control signals and sensor readings are sent over a wireless communication network. High-capability attackers with knowledge of the deployed detection system can access the network, intercept the signals being sent, and manipulate the control commands by spoofing the packets corresponding to the actual device model and configuration.

Timing-based Optimum Power Flow (OPF) Attack. Optimum Power Flow (OPF) determines the generator set-points required for Automatic Generation Control (AGC) to minimize specific objectives such as generation cost or power loss while satisfying operating constraints and meeting demand [17]. A set of lower and upper bound thresholds are configured to define the system's safety. For example, 59.5-61 Hz is defined as the power grid's upper and lower bound frequency threshold. A controller such as PLC is used to send the control commands to the actuators to configure the generation set-points to the generators to ensure power generation and consumption stability. An advanced adversary who performs reconnaissance when attacking a targeted system can make malicious modifications to the OPF algorithm via a control command; the adversary can manipulate the safety-margin conditions of the system in conjunction with replacing the cost minimization function with maximization to cause a more severe impact.

Aurora Attack. The aurora attack is designed to manipulate the breakers when the system and generator slip out of synchronism before the protection system responds to the attack. Since factors contributing to generator protections are intentionally delayed preventing unnecessary tripping, attackers typically get a 15-cycle window to reclose the breaker before any protection device kicks in [124]. The damage to the generator is caused by the electrical power output variation from the generator and the rotating speed of the incremental generator during the aurora attack. Each time the breakers are reclosed, the difference of frequency and phase angle between the main grid and the generator may result in high torque and currents, leading to physical damage to the generators.

2.3.2 Measurement Integrity Attacks. The basic idea of a measurement integrity attack is to maliciously modify the critical measurement values received from the sensors in the SG. These actions can disrupt SG applications by modifying their control values, and certain attack types can benefit bad actors to gain illegitimate financial gains.

Price Modification Attack. A price modification attack is realized when the attackers manipulate the electricity prices in small but predictable ways, giving them a competitive advantage in the market. According to the US Energy Information Administration, the average price of electricity in the US was 75 USD/MWh, with approximately 220 billion USD transactions, accounting for all the energy consumption [106]. Therefore, price modification can also be utilized to manipulate the energy market. Attackers can start with identifying the actual price in the network, inject false pricing information over a more extended period to cause generation, economic, and financial losses

to the utility. An attacker can carefully choose specific time slots in such attacks, e.g., when the electricity is very expensive or cheap In [106], the authors used simulations to mount Manipulation of Demand via IoT (MaDIoT) attacks by utilizing real-world data obtained from two major energy markets to increase the profit of particular market players significantly.

AGC Attack. The Automatic Generation Control (AGC) is a wide-area frequency control application that ensures frequency stability and keeps the power interchange between Balancing Authority (BA) areas at the scheduled values. The tie-line power flow between BA areas and frequency measurements from these sensing devices are sent to supervisory control and data acquisition (SCADA) systems and control centers. AGC relies on remote sensors' power flow and frequency measurements to calculate the area control error (ACE). Automated control commands on AGC generators are computed once every few seconds based on the ACE values [114]. SE can reduce measurement noise and detect faulty sensor data. However, existing measurement validation techniques such as the state estimation and Bad Data Detection (BDD) typically run once every a few minutes, which cannot accommodate the second-level frequency of AGC. Therefore, attackers can access remote sensors to mount false data injection attacks on power flow measurements. The attacker may provide a wrong perception of the system load. For example, the attacker can trick any area of AGC into believing that the power flow has increased/decreased; the action can cause the incorrect computation of an ACE value sent to the generators [74]. Consequently, the wrong ACE value sent to the generator will falsely ramp up/down the generator, which can cause generation imbalance and destabilize systems' frequency.

2.3.3 False Data Injection Attacks (FDIA). False data injection attacks aim to target data integrity: An attacker forges sensor readings to introduce error into state variables and values calculations. In the SG's context, meters and sensors lacking tamper-resistance hardware increase the possibility of being falsely injected with malicious readings. The attacker can mount such attacks to disrupt the SG operations.

State Estimation Attack. State Estimation (SE) is one of the critical components in SG system operation; it is used by Energy Management System (EMS) at the control center to ensure the desired operation states of the SG. SE can be formalized by $Z = h(x) + e$, where Z is a measurement vector, x is a state vector, h(x) is a nonlinear vector function, and e is the error vector. Towards this end, the states estimator estimates voltages at all system buses in real-time by using SCADA data and the system model. For the false data injection attack vector a in DC model, $a = Hx'$, where H is the measurement matrix; x' is the estimated state deviation due to the attack. To this end, $x_{attack} = x'' + x'$ gets the same BDD residual r as the malicious measurements $Z_a = Z + a$. SE attack can significantly disrupt the auto control mechanism of the EMS, which could potentially lead to system voltage collapse and economic loss.

Load Redistribution Attack. An adversary injects malicious measurements to power flow and load buses measurements in a load redistribution attack. Such attacks are projected as a more realistic attack where the attacker is not required to have all the power system topology information; an attacker keeps the same phase angle variations at all targeted buses [124]. To increase the attack's impact, attackers can target initial contingency as a power system weak point. Towards this end, attackers can utilize the weak point to redistribute power to cause severe physical damage to the system. Moreover, coordinated load redistribution attacks with physical attacks can also cause a cascading effect of failures in the power system.

2.3.4 Control Logic Modification Attacks. Control logic modification attacks aim to maliciously manipulate the system's control devices such as PLCs, RTUS, protective relays, and IEDs. An attacker may also try to destabilize the control process loop functions of the SG. Attackers may

inject malicious control commands into the actuator and compromise the sensor readings to keep the attack stealthy [33].

Protection Relay Attack. An attacker can modify the control logic of protection relays. A protective relay is a device designed to function as a safety mechanism to guard against faulty and dangerous physical conditions in the SG. In the event of overheating power transmission lines or if a generator goes out of synchronization, protective relays detect the anomaly and open a circuit breaker, disconnecting the power transmission lines and saving critical hardware components [46]. An adversary can attempt to maliciously flip the control mechanism logic of protective relay zones to open or close circuit breakers. The attack can have drastic consequences and could damage generators beyond repair.

Generators' Synchronization Attack. In this attack scenario, an attacker aims to cause a severe impact on generators' synchronization by modifying the PLC's control logic, which is not protected by any measure in most cases. The attacker modifies the control logic of the PLC to destabilize the synchronization process by manipulating the speed of the generators. The effect of the disrupted synchronization disables the power-sharing process of the generators. When one generator supplies more power, the other generator cannot take over even after synchronization. The attack can cause frequency incursions equipment damage.

2.3.5 Denial of Services (DoS) Attacks. DoS attacks aim to maliciously disrupt and sabotage the availability of SG's critical functions by inhibiting its nominal functionality. Such attacks can be accomplished by blocking inbound or outbound communication or even time-critical functions of the SG. The catastrophic impact of DoS attacks in the SG is a cascading failure or a blackout that may leave thousands, if not millions, of customers without electricity.

Time-Delay Attack. A time-delay attack is a type of DoS attack where an attacker aims to delay communication packets or measurements of sensors and actuators. For example, an adversary can inject time delay in the AGC signal, the only automatic closed loop between the IT and the control area of the power system. In this direction, the adversary can inject delays in data coming from power flow and frequency measurement sensors. Attacks can be mounted by jamming the communication channels, and such attacks can mislead AGC secondary control mechanisms, leading to the wrong decisions at the wrong time and making the power system unstable [74].

Jamming Attack. Another type of DoS attack is a jamming attack, which aims to disrupt the physical layer of the SG's communication networks. In this attack scenario, an attacker can place a jammer in close proximity to the communication channel to disrupt the data transmission [28]. Moreover, a jamming attack can compromise a subset of meter measurements by emitting additive white Gaussian noise to the communication channels [49]. To this end, the financial loss to the utility can be catastrophic if the attacker targets many smart meters: The financial loss can be more significant if the attack is performed over a more extended period.

In Table 4, we summarize the objectives, means, and impacts of SG cyber-physical attacks.

2.4 Lessons Learned: Summary and Insights

Advancements in control systems and communication networks have automated the operation of the SG; however, this growing reliance on the computing systems also opens the door to complex cyber-physical attacks against the grid. In this context, a threat modeling can accurately represent the SG elements, their inter-dependencies, as well as the possible attack types and system vulnerabilities. Despite the available threat modeling frameworks, SG requires a framework that is specifically tailored for it, considering the dynamics of the underlying power and communication systems (see, e.g., [130]). To put into perspective, high-capability adversaries can use various tactics and techniques to impact the physical operations of the SG. The nature of these tactics and

Table 4. Objectives, Means, and Impacts of Smart Grid Cyber-Physical Attacks

Physics aware control command attacks				
Attack Type	Target	Objective	Means	Impact
Timing-based Optimum Power Flow (OPF) attack	OPF, AGC mechanism, generator	Cause damage to generators and power system failures	Compromises PLC, obtain device model and configuration of the PLC, modify OPF algorithm via control command	Incorrect observability, voltage instability, power outage
Aurora attacks	Generators in power plants	Cause damage to generators	Open and close circuit breakers	Electrical power output fluctuation, loss of stability
Measurement integrity attacks				
Attack Type	Target	Objective	Means	Impact
Price modification attack	IoT devices, smart meters, the price signal	Increase generation cost, undermine the economic operation	Inject false pricing information, manipulate IoT devices and smart meters	Economic losses, wrong control actions, loss of stability, power transmission line overload
AGC attack	AGC, Generator	falsely ramp up/down the generator to generation imbalance	Provide a wrong perception of the system load by ACE manipulation	Voltage instability, load imbalance, under-frequency load-shedding
False Data Injection (FDI) attacks				
Attack Type	Target	Objective	Means	Impact
State estimation attack	State estimation, BDD	Disrupt the auto control mechanism of the EMS	Measurement manipulation	Wrong control actions, loss of observability, and voltage stability
Load redistribution attack	State estimation, BDD	False perception of estimated states	Measurement manipulation	Tripping of power transmission lines, system instability, power outage
Control logic modification attacks				
Attack Type	Target	Objective	Means	Impact
Protection relay attack	Protection relay settings	power transmission lines disconnection	Relay zone settings manipulation	Wrong control actions, false power transmission line overload, damage to generators, load imbalance
Generators' synchronization attack	PLC, generator	Power generation/demand imbalance, generator's damage, blackout	PLC control logic modification	Rotor angle instability between power generators, damage to generators
Denial of Services (DoS) attacks				
Attack Type	Target	Objective	Means	Impact
Time-delay attack	Communication channel, AGC, smart meters	Mislead AGC secondary control mechanisms, cause financial losses to the utility	Inject delays in data, jamming the communication channel	Loss of control, incorrect observability, economic and financial losses
Jamming attack	Communication channel, smart meters	Disrupt the data transmission, cause financial losses to the utility	Placing a jammer, emit additive white Gaussian noise to the communication channels	Delay in control actions, incorrect observability, economic and financial losses

techniques may change as technology changes; new types of information are becoming relevant in conjunction with new techniques to extract useful information for reconnaissance and exploit vulnerabilities (see, e.g., [92]). To this end, adversaries can potentially launch a Ukrainian power grid like coordinated attacks, destroy several pieces of equipment in the SG that can trigger cascading effects of failures, and create blackouts lasting several orders of magnitude longer than the attacks in Ukraine.

Another challenge is to defend against the APT-based threats that is usually performed over a longer period; a collection of indicators of compromise and real-time monitoring can be an effective way to counter such threats (see, e.g., [69]). Therefore, to motivate the understanding, researchers need to generate novel attacks in their papers, analyze the impact of such attacks on the control and physical systems, and identify the indicators of compromise (see, e.g., [18, 75, 91, 113]).

3 CYBER-ATTACK DETECTION AND MONITORING IN SG

This section presents the existing detection and monitoring techniques and tools in the SG paradigm. In this direction, the significance of Security Operation Center (SOC) and existing co-simulation tools are also discussed.

3.1 IDS in SG

Fundamentally, IDS are characterized in two ways: IDS deployment and IDS technique. The deployment refers to how the data is collected before the intrusion detection analysis. Whereas the detection technique defines "how" the data is analyzed to detect the intrusions in the system.

3.1.1 Categorization based on IDS Deployments. According to IDS deployments, IDS can be categorized via many criteria such as Host-based IDS (HIDS), Network-based IDS (NIDS), cloud-based IDS, IoT-based IDS, edge-based IDS, and distributed IDS. This subsection discusses the popular but non-exhaustive categorization of IDS employed in the SG.

Host-based IDS (HIDS). HIDS is incorporated in independent devices on the network, and it inspects the data maintained by the audit source, such as the logs data and processes stored by an operating system. HIDS can be quite effective for the high-volume configurations as it provides distributed control. Additional computing resources are required in HIDS, which can be quite critical for the resource-constrained field devices in the SG as these devices are not designed to have the full capability of a computing system.

Network-based IDS (NIDS). NIDS can inspect passing traffic on the connected network by analyzing the patterns and attributes of communication protocols. Monitoring of external threats and malicious intrusions are mainly monitored and detected by NIDS. NIDS have comparatively limited visibility to monitor and inspect high bandwidth networks due to the high volume of data passing through the communication network of SGs.

Cloud-based IDS. Cloud-based IDS is deployed to protect SG in a distributed environment as a scalable and virtualized solution to protect against cyber-attacks in cloud computing. Such IDSs are deployed to monitor cloud networks for detecting malicious activity in the SG [15]. A typical cloud-based IDS framework consists of three principal components: data collector, cloud service component, and cloud intrusion detection component.

IoT-based IDS. Integrating IoT-based devices facilitates the SG architecture to enable universal monitoring for distributed energy generation and other applications. These IoT-based devices gather, send, and act on operational data from their surroundings using sensors, embedded systems, and communication hardware [112]. Adversaries may maliciously compromise these devices to enter an IoT botnet and perform massive attacks on the SG applications. Therefore, IoT-based are deployed to address stealthy and complex security threats against the SG. IoT-based IDS usually employ big data analytics to detect anomalies and intrusions in the exposed data. However, such IDS deployments must consider stringent conditions of low processing capability and high-volume data processing.

Distributed IDS. Fully distributed IDS are deployed to address some limitations in centralized-based IDS. In these types of IDSs, primarily two types of functions are incorporated: a detection unit to collect data and a correlation unit responsible for the distributed correlation to find an anomaly in the system. Distributed IDSs do not have a single point of failure as opposed to centralized IDS, where one primary node failure potentially impacts the whole IDS system. Moreover, distributed IDS can detect intrusion passing through the node itself, and these architectures are considered to have better scalability in the context of the SG [72]. However, it is challenging to balance intrusion detection accuracy and node resources such as processing power and memory in distributed IDS; it is challenging, particularly in the settings of the SG where many resource constrained-based edge devices are deployed.

3.1.2 Categorization based on Detection Technique. Intrusion detection techniques can be categorized into Signature-based detection, anomaly-based detection, hybrid IDS, specification-based detection, and Moving Target Defense (MTD) based IDS. Table 4 presents a survey of these types of IDSs in the SG, highlighting performance and features.

Signature-based IDS. The function of signature-based IDS is based on pattern matching techniques to detect known attacks or previous malicious intrusions into the system. In other words, if the characteristics of an attack are matched with the configured signatures, a corresponding alarm is generated. The false-positive rate is low for signature-based IDS; however, the flip side of

Table 5. Revisiting IDS in the Smart Grid

Signature-based IDS							
Ref.	Year	Target	Attack	Method/Algorithm	Dataset	Performance	Highlighting Feature
[43]	2016	Substation, Photovoltaic inverter	Data integrity attack	Stateful analysis	Not required	Not given	Stateful analysis plugin is developed for Suricata IDPS
[54]	2015	SCADA	DoS attack	A rule template-based detection	Not required	Not given	Utilizes an intrusion detection template to generate the signature rules for the DNP3 protocol
Machine Learning-based IDS (Centralized, Distributed, and Federated-based Algorithms)							
[108]	2021	SCADA, control center	Data integrity attack, control signal attack	Variational Mode Decomposition (VMD) and Decision Tree (DT)	Synthetic dataset	Accuracy = 99.85%, recall = 99.0%, precision = 99.0%, f-measure =99.0%	Cyber-Physical Anomaly Detection System (CPADS) is developed that utilizes synchrophasor measurements and properties of network packets to detect attacks
[20]	2020	Distribution systems	Scaling, ramping, random, and smooth curve attacks	Bayes Classifier (BC)	Pecan Street Dataport	TPR = 98.75%	Spatiotemporal patterns of system measurements are integrated into a flexible BC for cyberattack detection
[21]	2019	Load forecasting	Pulse, scaling, ramping, random, and smooth curve attacks	Naïve Bayes classification	Synthetic dataset	For scaling attack - Mean absolute percentage error = 10.22%, root mean square error = 8.54%	Machine learning-based anomaly detection is proposed to detect load forecasting attacks, and the aggregation approximation method is compared with the developed method
[74]	2021	AGC	FDI attack, time-delay attack	Gaussian process regression	New England ISO load data, synthetic dataset	100 % detection probability in a shorter time	Prior information based on the Gaussian process is utilized to detect cyber-attacks on AGC
[4]	2019	State estimation	Covert data integrity attack	Isolation forest	State-estimation measure feature dataset	For IEEE 118-Bus – Accuracy = 94.518%	An isolation forest algorithm is used to detect an attack on unlabeled data using unsupervised learning
[127]	2021	Solar PV dc/dc and dc/ac converters	FDI attack	Federated learning	Synthetic dataset	Accuracy = 0.9750, precision = 0.9690, recall = 0.9613	Federated learning is used to train data across devices in a decentralized manner to detect FDI attacks on solar PV converters
[120]	2021	Energy consumption data	Forgery attack, replay attack	Federated learning	State Grid Corporation of China (SGCC) dataset	Accuracy = 0.913 - 0.919	A decentralized, federated learning-based detection system is proposed to detect energy thefts
Deep Learning-based IDS							
[46]	2020	Substation automation, transmission protective relays	MITM attack, FDI attack	Unsupervised deep learning autoencoder-Based detection	Synthetic dataset	Precision = 100%, recall = 100%	A deep learning-based cyber attack detection system for power transmission line protective relays is proposed for various attack scenarios
[125]	2020	Distribution system state estimation	FDI attack	Semi-supervised deep learning autoencoder-based detection	Synthetic dataset	For 1250 labeled data – Accuracy = 96.70%, precision = 95.47%	Autoencoder is integration into d Generative Adversarial Network (GAN) framework for the cyber-attack detection in a semi-supervised deep learning setting
[29]	2021	AGC	Time-delay attack	A deep learning-based approach using hierarchical long short-term memory model	Synthetic dataset	For AGC – Accuracy = 98%	A deep learning-based system is proposed to detect and characterize time-delay attacks against the AGC
[110]	2021	SCADA, Modbus protocol (TCP), DNP3 protocol	Communication protocol attacks	Autoencoder-Generative Adversarial Network (GAN)	Datasets acquired from SG lab, substation, hydropower plant, and power plant	For Modbus/TCP power plant – Accuracy = 0.964, FPR = 0.018	A deep learning-based IDS is proposed is proposed to detect attacks in Modbus/TCP and DNP3 protocols

Hybrid-based IDS							
Ref.	Year	Target	Attack	Method/Algorithm	Dataset	Performance	Highlighting Feature
[81]	2015	Wide area monitoring system	Disable relay attack, command injection attack, replay attack	Common path mining	Synthetic dataset	Accuracy = 90.4%	Hybrid IDS technique based on common-path mining approach is proposed that learns temporal state-based specifications for power system scenarios, including disturbances, normal control operations, and cyber-attacks
[108]	2021	SCADA	Data integrity attack, DoS attack	Integration of network-based, model-based, and machine learning-based IDS	Synthetic dataset	For OT attacks – Accuracy = 98.71%	The proposed IDS utilizes attack signatures, network packets, and secure phasor measurements to detect different stages of cyber-attacks while following the cyber-kill chain
Specification-based IDS							
[82]	2015	Substation, protection relay	Malicious command attack, control logic modification attack	Bayesian network is used to create patterns with temporal state transitions	Not required	Correct classification of attacks for most of the given attack scenarios	A specification-based IDS is proposed, which reads PMU current measurements, relay trip status, the snort log, and the control panel log and uses this information to track system states
[51]	2015	Substation	DoS attack, GOOSE attack	Behavior and specification-based method is used	Real data was used from a substation in South Korea	FPR = 0, TPR = 1, precision = 1	A behavior-based IDS is proposed for the IEC 61850 protocol using both statistical analysis of network features and specification-based metrics
Moving Target Defense (MTD) based IDS							
[59]	2021	Transmission system, state estimation	FDI attack	Graph-theory-based topology analysis for D-FACTS placement	Not required	Detection probability = 0.9	D-FACTS placement algorithm is proposed to enhance the detection of cyber-attacks
[116]	2019	Secondary voltage control	Stuxnet like attacks, stealthy FDI attack	MTD based approach to change system configuration	Not required	100 % detection probability in a shorter time	MTD based approach is applied to detect stealthily and Stuxnet ike attacks in the control loops of the SG
[52]	2019	State estimation	Coordinated cyber-physical attack, FDI attack	MTD based approach by actively perturbing the grid's power transmission line reactance using D-FACTS devices	Not required	Highest detection probability for MTD based approach	MTD based approach is proposed to detect coordinated cyber-physical attacks by perturbing the power transmission line reactance

this technique lies in the inability to detect zero-day or unknown attacks. To detect active power limitation attacks in substations, [43] uses Signature-based IDS by developing a stateful analysis plugin consisting of three main functions: 1) the application layer protocol decoder, 2) the rule match engine, and 3) the state manager.

Anomaly-based IDS. In the anomaly-based IDS, a normal model of the behavior of a system is defined using various techniques, including machine learning, deep learning, artificial intelligence, and statistical methods. The deviation from the normal defined behavior is regarded as an anomaly, which indicates a malicious activity or intrusion into the system [50]. Unlike most of the IDS in IT infrastructure, where signature-based IDS are more commonly deployed due to the availability of an abundance of signatures, anomaly-based IDS are more popular in ICS such as SGs due to the diverse nature of protocols and networks. Even though anomaly-based IDS have a more false-positive rate as compared to signature-based IDS, the ability to detect unknown attacks in anomaly-based IDS is favored in SGs.

Machine Learning and Deep Learning-based IDS. Machine Learning (ML) and Deep Learning (DL) techniques are applied in various fields of SG applications for anomaly-based methods. Feature engineering is commonly employed in ML to extract leading attributes and features for classifying attacks in the SG networks [63]. On the other hand, linear and non-linear processing layers are used in DL techniques to extract discriminative or generative features for pattern analysis [37]. The standard ML algorithms that are used to detect intrusions in the SG are Support Vector Machines (SVM), Bayesian algorithms, k-nearest neighbor (KNN), random forest (RF), association rule (AR)

algorithms, ensemble learning, k-means clustering, decision trees (DT), and Principal Component Analysis (PCA). In contrast, DL techniques can be classified into discriminative and generative techniques [60]. In this direction, Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs) are known as discriminative techniques. To this end, restricted Boltzmann Machine (RBM), Deep Belief Network (DBN), Generative Adversarial Network (GAN), and Deep Autoencoder (AE) are known as generative techniques.

In [108], the authors proposed architecture and methodology for a cyber-physical anomaly detection system (CPADS). The proposed ML-based methodology utilizes synchrophasor measurements and network packet inspection to detect integrity attacks on measurement and control signals. The relevant input features are derived using a rule-based approach, and variational mode decomposition (VMD) and decision tree (DT) algorithms are used for cyber-attack event classification and decision logic. The proposed system exhibits promising results with 99.85% accuracy. In [46], a DL-based cyber-attack system is proposed for power transmission line protective relays, including distance protective relays, overcurrent protective relays, differential protective relays, and multiple fault scenarios. The authors employed unsupervised learning by utilizing a convolutional-based autoencoder for previously unseen cyber-attack detection. The proposed system is trained with current and voltage datasets which are then utilized to detect malicious measurements. To detect time-delay attacks in cyber-physical systems, a DL-based method leveraging a short-term memory model to process raw data streams from sensors is proposed in [29]. The authors evaluated the proposed model on the power plant control system and AGC, obtaining promising results with a detection accuracy of 92% and 98%, respectively.

Federated Learning (FL) based IDS. Although ML and DL techniques are widely efficient in detecting cyber-attacks in the SG, the prediction and true-positive accuracy decrease when network scale increases; these techniques use a central entity to process all the data in the network. To overcome such issues, Google proposed the concept of Federated Learning (FL) in 2016 [123]. Compared to distributed ML, a multi-nodal system known to build a training model by utilizing different nodes for independent training, FL algorithms are fundamentally different and are particularly effective for addressing data privacy. FL algorithm enables the nodes to learn collaboratively without data sharing with a centralized server; it uses a centralized model using decentralized model training. The models are trained on the local nodes independently, and once the training phase is completed, the models are sent back to the central server to be combined to create an efficient model. In [120], the authors proposed a privacy-preserving FL framework to detect energy theft. The FL framework consisted of a data center, a control center, and multiple detection stations. The results showed high detection accuracy with low computation costs for energy theft detection.

Hybrid-based IDS. To overcome the high false-positive rate in anomaly-based detection, many researchers have proposed hybrid IDS, which combines the aspects of signature-based IDS and anomaly-based IDS to enhance the detection accuracy of all the attacks. In [81], authors have proposed a hybrid IDS technique based on the common-path mining approach and Snort [90] to detect anomalies in PMU's data. Aspects of normal behavior and known cyber-attack signatures are characterized in the common path. The proposed IDS can detect and differentiate between normal operations, system disturbance, and cyber-attacks with an accuracy of 90.4%.

Specification-based IDS. Another IDS technique in the SG is specification-based detection. This detection technique is similar to anomaly-based detection; however, it relies on manually developed specifications instead of ML techniques. Therefore, predetermined rules for normal behavior are defined for the specification-based technique, and any sequence of operations executed outside of these rules is regarded as a security threat. To achieve high detection accuracy, the specification-based technique is combined with anomaly-based detection. The cost of defining the rules for specification-based detection in large CPS systems such as SG is a key disadvantage of

this technique. In [51], the authors propose an IDS for IEC 61850 protocols using specification-based metrics and statistical analysis of network features. The IDS was evaluated on the real data from a substation in South Korea, and the results demonstrated optimum accuracy with the least false-positive ratio.

Moving Target Defense (MTD) based IDS. Moving Target Defense (MTD) has emerged as a solution to address security concerns against an adaptive attacker who aims to mount stealthy attacks against the SG. The primary concept of the MTD includes constantly moving between multiple surfaces such as network configurations and changing the open ports in order to add uncertainty for the attacker. In the context of the SG, the MTD approach is mainly used to alter the power system configurations by varying setpoints of Distributed Flexible AC Transmission System (D-FACTS) devices in flexible AC transmission [58]. In [52], the authors proposed an MTD design to detect coordinated cyber-physical attacks against the SG. The work incorporated the MTD-based detection mechanism to invalidate the adversary's knowledge by varying the SG's power transmission lines reactance's via D-FACT devices. To minimize the defense cost, the authors used a game-theoretic approach to identify the adequate subset link of the D-FACT deployment set. The experimental results showed that the MTD-based approach could efficiently detect coordinated cyber-physical attacks against the SG with low defense cost. To detect stealthy attacks, the authors in [31] proposed an MTD-based approach that randomly changes the availability of the sensor data; thus, making it harder for the adversary to mount stealthy attacks against the SG. To this end,the authors formulated an optimization problem to find the parameters such as switching signal probability that increases the detection of stealthy attacks.

3.2 SOC Monitoring and Visualization Tools

SG security requires a high alert-based monitoring system that allows the operators to query, monitor, and visualize alerts. This subsection highlights the significant role of SOC in SG security, and then we review current monitoring and visualization-based tools suitable for the SG infrastructure.

3.2.1 Security Operation Centre (SOC). A security operation Centre (SOC) is defined as a centralized infrastructure made up of a team or a facility dedicated to detecting, preventing, evaluating, and responding to security breaches in the infrastructure [2]. Moreover, a SOC is also referred to by other names, such as Information Security Operations Centre (ISOC), Security Intelligence Centre (SIC), and Cyber Security Operations Centre (CSOC). SOC plays a crucial role in implementing and assessing regulatory compliance in the SG networks; tracking abnormal and security events, vulnerability management, network flow monitoring, intrusion detection, and response planning are integral roles of SOC.

The architecture of SOC in the context of SG can be divided into three parts: People, processes, and technology. People are the most crucial part of SOC operations, where they ensure incident monitoring management, alerting, event analysis, coordination and reporting, and investigations and post-incident reports. Processes help SOC achieve its objectives, such as the incident response process, SOC access control policy, and security operating procedures [24]. Technology in SOC includes devices that can generate a log and feed the Security Information and Event Management (SIEM) with the required data and events to be monitored.

In [3], the authors constructed semi-structured interviews with ten analysts to examine the thought process in SOC analysts facing security threat events. The work results suggested that simulation environments and physical proximity with analysts and vendors effectively transfer the tacit knowledge in SOCs.

3.2.2 Visualization Tools. The real-time intelligent visualization system for the critical operations of SG holds significant importance. Real-time monitoring and visualization tools can significantly

Table 6. Smart Grid Co-Simulators and their Applications

Reference	Name	Power Simulator	Network Simulator	Real-time	Targeted Application
[53]	EPOCHS	PSLF	NS-2	No	WAMS
[55]	VPNET	Virtual Test Bed (VTB)	OPNET	No	Network Control
[53]	GECO	PSLF	NS-2	No	WAMS
[66]	TASSCS	PowerWorld	OPNET	Yes	SCADA security
[97]	CPSA	MATLAB, PowerWorld	GridSim	Yes	Power system monitoring
[19]	FNCS	PowerFlow, GridLAB-D	NS-3	Yes	Real-time pricing
[53]	GridSim	TSTAT	GridStat	Yes	WAMS
[94]	Simulink, OPNET	Simulink	OPNET/OMNeT ++	No	SCADA security

improve SG's operational security capabilities and monitoring processes. These tools can provide operators in the control center with a much more dynamic view of the security posture of the SG's operations and services. Appropriate visualization tools can enable operators to respond to dynamic threats and vulnerabilities in the infrastructure efficiently. The main components required for monitoring and visualization tools in the SG infrastructure are detailed as follows [68].

Security Information and Event Management (SIEM) system – Aggregate and correlate all the collected data from multiple sensors and generate alerts.

Physical Access Control System (PACS) – Contains sensors to monitor physical access in the control center and sends information to Security Information and Event Management (SIEM) system.

Log Aggregator - Collects log data from the operations facilities and sends it to the SIEM system.

Historian – Receives SG's operational data and stores in a server.

Application Monitor – Monitors IT applications for any anomalous behavior and sends it to the SIEM system.

Analysis Workflow Engine – Automates executions of actions of events received in SIEM system.

Analysis Tools – Examines data collected from the SIEM for any intrusions and report any incident to security operators via visualization tool.

Visualization Tool – Generate alerts and provide visualization dashboard to correlate security events.

3.3 Existing Co-Simulation Tools

Simulation tools are generally based on mathematical models depicting a real-world phenomenon utilizing mathematical rules and language. There are many functions and security concepts in the SG that cannot be directly applied to such infrastructure. Therefore, simulation tools are required to test the functions and security-related concepts. In this direction, co-simulation is a special kind of simulation in which communication and power system simulations are coupled together. Co-simulation tools can provide insights into the relationship between power and communication systems, and these tools are also actively used to analyze the impacts of different advanced cyber-attacks on the different domains of SG infrastructure. For instance, the integrated simulation tool for power and communication network can evaluate the impact of a malicious command attack on RTUs concerning both power and communication systems [100].

Various communication networks and power system simulation tools already exist. For instance, the most common power grid simulation tools are PowerWorld, OpenDSS, MATLAB/Simulink, Modelica, and GridLAB-D. Similarly, NS-2, NS-3, OPNET, OMNeT ++, GridSim, and NeSSi are popular network communication simulation tools.

Table 6 provides an overview of some existing SG co-simulators. Each co-simulation tool is based on targeted applications of the SG to understand the reciprocal effect under any event. For instance, the co-simulator "Electric Power and Communication Synchronizing Simulator" (EPOCHS) presented by [40] targets the application of wide-area monitoring and security. The EPOCHS is an integration framework of PSLF, a power simulator, with NS-2, an open-source communication network simulator. The co-simulator CPSA [97] evaluates the impact of malicious commands on CPS. The tool can also detect bad measurement data in real-time and provide visualization dashboards to guide the operators to take actions to mitigate the impacts of cyber-attack.

3.4 Lessons Learned: Summary and Insights

Few existing works proposed signature and specification-based techniques to detect attacks (see, e.g., [43, 82]); the central issue can be associated with the requirements of power system and expert knowledge and a substantial amount of human efforts in crafting rules. In the context of ML and DL-based techniques, IDSs must incorporate temporal, spatial, and logical features to enhance contextual based-detection (see, e.g., [47]). Generally, RNN models are used to capture temporal relations, and CNN models are utilized to learn the context of the power flow and voltage time-series sensor data (see, e.g., [50, 65]). However, the influence of the network traffic is not captured in the detection approaches: The communication data can be quite valuable in providing context to the attack detection, an essential factor for the SA of the SG [79]. For example, the same anomaly can be classified as malicious or benign, depending on the correlation of communication and power system metrics.

There are still many challenges to put into actual operation, such as integrating the additional capabilities within the existing IDSs. More specifically, there are no publicly available datasets for complex cyber-physical attacks such as APT attacks, coordinated attacks, and cascading attacks; therefore, it is difficult to study the performance of detection systems against such attacks using ML and DL techniques. Therefore, one of lesson is to develop an environment to generate artificial attack sequences, based on frameworks like MITRE ATT&CK, to perform integrated monitoring, detection, and analysis study, as well as generate datasets based on different scenarios (see, e.g., [18, 75, 91, 113]).

Some related works [59, 116] used MTD to detect stealthy attacks in the SG. However, more research is required to efficiently place a reduced number of D-FACT devices to minimize the cost of MTD deployment. Some work on federated learning, including intrusion detection in the SG, is explored in [120, 127], showing prominent potential in the detection of coordinated-based attacks. Finally, more detailed discussions need to be included in the papers regarding the pros and cons of using real data from the SG, datasets from testbeds, and co-simulations. Without providing a detailed analysis of the efficacy of the utilized datasets, it is elusive to determine the performance of the IDS. Lastly, more work is needed to tackle the limitations of visualization tools that offer human analysts and SOCs efficient perception, comprehension, and decision making in an automated and real-time manner. For example, graph-based tools can be revisited to analyze the scalability issues, and the tools can be hybridized by incorporating artificial intelligence-based contextual awareness of the cyber-physical events in the SG.

4 CYBER-PHYSICAL SITUATIONAL AWARENESS (CPSA)

Understanding the environment at a macroscopic and microscopic level is essential for a system operator to identify anomalies in the system and surroundings efficiently. This understanding is referred to as Situational Awareness (SA) [129]. SA has been defined by various perspectives, but the most widely accepted definition of SA is defined as "perception of the elements in the

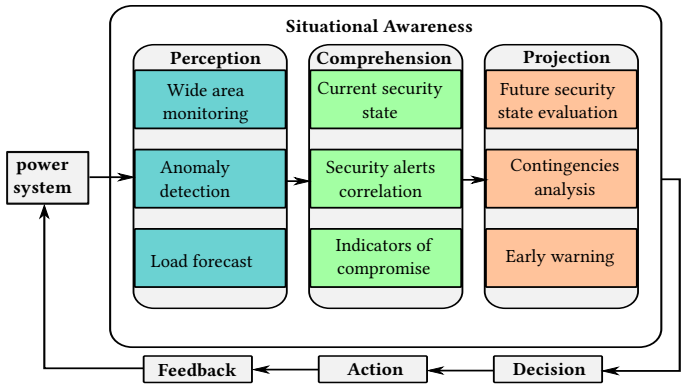

Fig. 1. Situational awareness framework for smart grid.

environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future" [26]. SA framework for SG is shown in Fig. 1

4.1 Cyber-Physical Situational Awareness Metrics

According to the NIST, "metrics are tools that are designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data" [42]. In line with the NIST guidance on security metrics, we construct a CPSA group of metrics for SG that can assist SOCs and security analysts to make incisive and informed decisions to alleviate the potential threats in the system. For example, network security metrics can be used to examine the performance of deployed IDS and the efficacy of the reported incidents. The use of these metrics also includes awareness around the protocol vulnerabilities in the network and any failed logging attempt, which can assist SOCs in keeping track of any initial intrusion attempt.

Similarly, system security, process security, and asset security metrics help SOCs to be familiar with the vulnerabilities in the system, processes, and critical assets. These metrics also provide guidance on the available operational and security capability the SOCs must deal with any security threat. However, these metrics are not static, and the SOCs must ensure these metrics are updated regularly. User vulnerability metrics relate to the user capabilities and security training of the SOCs in dealing with the security threats to the SG. These metrics are useful in reflecting and realizing an organization's vulnerability and preparedness in a security threat-related event. In addition, adversary model metrics provide the understanding of the threat capability of an adversary based on other given metrics such as publicly available information or the probability of an insider threat. However, such metrics have challenges when mapping the possible attacks, associated events, and activities with the organization's environment due to the decentralized nature of the SG. Table 7 lists cyber-physical situational awareness metrics and presents each given metric's numerical score/value.

4.2 Power System Metrics

Maintaining power system security is paramount in the operation of a SG. Power system metrics provide quantifiable measures to assess the overall power system health. Good quality of power

Table 7. Cyber Situational Awareness Metrics

Network/Communication Security Metrics		
Metric Title	**Description**	**Score/Value**
IDS detection rates	Determines the reliability of installed IDS systems in the network and can be estimated in the ratio scale.	n: total number of detected threats.
Loggings	Keeps a track of all logging attempts including abnormal VPN sessions into the SCADA system.	n: number of failed login attempts and abnormal VPN sessions.
Protocol vulnerabilities	Categorization of communication protocols based on security vulnerabilities.	n: number of communication protocols with no encryption mechanism.
Access points	The number of all possible I/O of a system and determines the vulnerable access paths.	n: total number of potential entry points in the system.
Reported incidents	A number of previously reported incidents for all the network components and paths.	n: total number of previously reported incidents for intrusions.
Asset Security Metrics		
Metric Title	**Description**	**Score/Value**
Critical components	Identifies the significance of the components with respect to critical operations and functions.	[0,1]: 0 means not critical; 1 means critical component.
Physical accessibility	The number of critical field devices that can be physically accessed by an adversary	[0,1]: 0 means not easily accessible; 1 means not easily accessible.
System susceptibility	Probability of an attack based on vulnerabilities in the system.	[0,1]: 0 means susceptible; 1 means not susceptible.
Attack paths	The number of attack paths that a system can be compromised can be calculated using attack graphs.	n: total number of paths available for an intruder to breach the system.
Supply chains	Categorization of 3rd party devices for the contingency analysis following a security breach event.	n: number of 3rd party software and devices with known vulnerability or previously reported for bugs.
Process Security Metrics		
Metric Title	**Description**	**Score/Value**
Operational capacity	The operational capacity of critical power devices following a cyber-attack.	[0,1]: 0 means not operational; 1 means operational.
Reaction time analysis	Evaluation of the delay between the identification of a malware and mitigation response.	[t' – t]: total delay between identification and response.
Initial disruption and restoration	Length of time between initial disruption of operational process and restoration of essential functions.	[t' – t]: total delay between disruption and availability.
Permanently lost data	Percentage of irrecoverable data lost relevant to operational processes.	[%]: higher percentage means more susceptible.
Confidence level in the control loop processes	This metric defines the overall confidence in the components of control loop processes such as trust level in sensor values and control commands in controller.	[0,1,2,3,4…]: higher values means more reliable.
System Vulnerability Metrics		
Metric Title	**Description**	**Score/Value**
Severe vulnerabilities	Percentage of system with severe vulnerabilities based on Common Vulnerability Scoring System (CVSS) scoring.	[%]: higher percentage means more susceptible.
Vulnerability analysis	Percentage of systems for which vulnerability has not been done.	[%]: higher percentage means more susceptible.
Time criticality	Percentage of communication protocol paths and processes in a system for which time criticality is high.	[%]: higher percentage means more time critical.
User Vulnerability Metrics		
Metric Title	**Description**	**Score/Value**
Malware susceptibility	Evaluates the malware possibility that relates to the operator's online behavior with respect to installing the application. It can be estimated in the ratio scale.	[0,1]: 0 means more susceptible; 1 means less susceptible.
Phishing susceptibility	Relates to human cognitive bias and awareness to flag a suspicious email as a phishing email and can be measured on a ratio scale.	[0,1]: 0 means more susceptible; 1 means less susceptible.
SA training	The number of staff in the control center with adequate knowledge and training of SA.	n: total number of well-trained staff vs total number of staff with insufficient SA training.
Adversary Model Metric		
Metric Title	**Description**	**Score/Value**
Threat capability	Mapping the assets and operations with the required level of technical skills to compromise the system.	[0,1]: 0 means less technical skills needed to compromise the operational process; 1 means more sophisticated skills are needed to breach the operational process.
Insider attack	Percentage of insider attack possibility based on confidential reports.	[%]: higher percentage means more probability of an insider attack.
Supply chain	This metric determines the susceptibility level of supply chain risks for different components in the SG.	[0,1,2,3,4…]: higher values means more vulnerable to supply chain attacks.
Publicly available information	Percentage of publicly available information of different assets in the SG from different sources such as Open-Source Intelligence (OSINT) datasets and Shodan.	[%]: higher percentage means more susceptible.

[t' - t]: Total delay between the events

Table 8. Power System Metrics

Power/Voltage Metrics		
Metric Title	**Description**	**Score/Value**
Rapid Voltage Changes (RVC) [12]	Parameter to quantify voltage disturbances and quality.	[0,1]: 0 means no contingency; 1 means contingency
Production and load mismatch [88]	Relates to mismatch between demand and supply mismatch due to cyber-attack manipulation or misconfigurations.	[0,1]: 0 means no contingency; 1 means contingency
Survivability [13]	Relates to the ability of the power system to match generation and demand in case of cyber-attacks or power system failures.	[0,1]: 0 means non-survivable; 1 means survivable
Transmission related events resulting in loss of load [84]	Relates to transmission related events resulting in loss of load, excluding weather related power outages.	[0,1]: 0 means survivable; 1 means non-survivable
Voltage dips [13]	Temporary drop of voltage in electrical system.	[0,1]: 0 means no contingency; 1 means contingency
Frequency Metrics		
Metric Title	Description	Score/Value
Customer average disconnection frequency index [13]	Relates to customer average disconnection or interruption frequency.	n: total number of customers disconnected vs time
Number of offline power transmission lines [84]	Total number of power transmission lines that go offline frequently.	n: total number of offline power transmission lines vs time
Industrial Customer Average Interruption Frequency Index (ICAIFI) [101]	Relates to average frequency of all sustained interruptions to industrial and commercial customers.	n: total number of industrial and commercial customers disconnected vs time
Multiple interruptions frequency [13]	Relates the percentage of customers with multiple disconnections or interruptions.	%: percentage of customers with power disconnection vs time
Duration Metrics		
Metric Title	**Description**	**Score/Value**
System Average Interruption Duration Index (SAIDI) [101]	Relates to average duration of power disconnections or interruptions.	t: average duration of power disconnection
Recovery duration [83]	Relates to time required to full infrastructure recovery.	t: duration of full recovery
Customer Average Interruption Duration Index (CAIDI) [48]	Relates to customer average duration of power disconnections or interruptions.	t: average duration of customer power disconnection
Interruption duration [101]	Relates to sustained outages lasting more than X hours.	t: duration of sustained power outage

system metrics can assess and quantify the initial power system events to prevent large system blackouts [118].

4.2.1 Aggregate Megawatt Contingency Overload (AMWCO). The AMWCO metrics provide the sum of all the megawatts of overload in a given set of contingencies and are considered as the security criteria for power systems [97]. The AMWCO for the whole system is calculated using the aggregate percentage contingency overload (APCO) for each line. To this end, APCO for single line j - k on Branch JK can be computed as:

$$APCO_{BRANCH_{JK}}\% = \sum_{Oveloaded_{jk}} (\%Overload - 100)$$

Next, the product of APCO and line ratings gives us the AMWCO for the whole system in MW that is calculated as [110]:

$$AMWCO_{BRANCH_{JK}} = \sum_{jk} APCO_{JK}(MVArating_{jk})$$

The sum of AMWCOs for all power transmission lines can be calculated as: [99]

$$AMWCO_{System} = \sum_{Sum-of-all-lines} AMWCO_{line}$$

The higher value of the metric AMWCO points to the overloaded elements, whereas lower values correspond to a more secure system [95]. To this end, AMWCO equals zero shows no overloaded elements under any contingency. The co-simulation result using the 42-bus system presented in [100] shows that AMWCO (system) is an efficient and reliable metric that can indicate malicious events in the power system. For instance, results in [100] show that AMWCO (System) value significantly deviated from the forecast value under the malicious command attack.

4.2.2 Other Power System Metrics. In [12], Rapid Voltage Change (RVC) has been defined as the power quality metric to quantify voltage disturbance in the power grid. In [117], authors used data obtained from PMU to identify RVC event that points to voltage disturbances in the power grid. A global metric 'Survivability' has been introduced in [13]. This metric evaluates the power system's ability to match the generation and demand of electricity in case of failures and malicious cyber-attacks. 'Survivability' metric is measured on a scale from "0-1", where "0" refers to the lowest survivability/resilient level, and "1" represents the highest level. The authors applied this metric to a real-transmission system in order to illustrate its effectiveness. An approach to link Faulted Circuit Indicators (FCIs) to power outage using the Average Interruption Duration Index (SAIDI) and Customer Average Interruption Duration Index (CAIDI), to track reduction in outage duration has been proposed in [48]. These metrics indicate the total duration of power interruptions for the average customer and the time required for restoration. Table 8 presents the power system metrics along with description and score/value.

4.3 Human Factor and Situational Awareness Training

Human mistakes are considered as one of the major issues in security-related incidents in the SG [11]. Weak security implementation and human/system operator mistakes can lead to the propagation of faults, cascading effects, and even blackouts. Sophisticated adversaries can surreptitiously isolate the power components from the rest of the system by performing false command injection attacks, and power operators must be able to identify these malicious commands, which could be legitimate but false commands in the power system [100]. For example, the Ukrainian power grid attack, which caused a blackout, targeted IT staff and system administrators of utility companies responsible for electricity distribution [99]. According to the North American Electric Reliability Corporation (NERC), sophisticated malware was inserted into the software supply chain, which exposed many energy utilities to vulnerabilities [76]. Power operators need to be equipped and trained on the cyber domain of the SG to understand the impact of cyber-attacks on power systems control processes such as voltage control algorithms, topology re-configurations, and energy management systems so they should be able to quickly identify the disturbances in the power and communication system.

4.4 Lessons Learned: Summary and Insights

As defined by Endsley, SA comprises three main levels: perception, comprehension, and projection. To achieve situation perception, understanding the attack types and threats is vital to help the data gathering. Incorporation of suitable CPSA and power system metrics in the detection and threat evaluation system can provide a higher perspective of the events with respect to their current perspective and their future impact; an increased comprehension and projection of the evolving cyber-physical events in the SG. To this end, the ultimate level of SA can be accomplished by threat evaluation, decision making, and planning [5]. One lesson is that the overall SA of the SG is mainly tied to the integration of CPSA metrics with the power system metrics. In turn, it will allow the detection system to detect and predict contingencies in the overall system of the SG. Furthermore, the ability to assess security posture, effectiveness, and impact for predictive analysis is mainly dependent on the assumption that system operators have a comprehensive understanding of the impacts caused by cyber-attacks on the communication and power systems. Therefore, it poses severe challenges to maintaining SA as it involves the human factor and cyber and physical interactions. Therefore, co-simulation tools need to be revisited from the perspective of operators' training and analysis (see, e.g., [62, 97, 100]).

5 RESEARCH CHALLENGES, KEY GAPS, AND FUTURE DIRECTIONS

In this section, we endeavor to summarize open research challenges along with discussing key gaps, and the future directions.

5.1 Understanding the impact of complex cyber-attacks

Challenges: The vision of an optimum defense and detection mechanism against complex cyber-attacks is elusive without the deep analysis and understanding of the nature and impact of these attacks. With such a small history of known coordinated and other complex attacks against the SG, an experimental method to generate and execute attack sequences needs investigation [113]. Many researchers use assumptions such as probability and periodic distributions to model the attack experiments. However, the attacks may not follow such distributions in realistic settings. For example, Bernoulli distribution may not reflect the pattern for the drop of packets in all the DoS attacks in the SG. Therefore, another challenge is to perform experiments with realistic assumptions and manners.

It is not viable to perform experiments on the real SG system due to its critical nature. Moreover, it is usually beyond the resources of researchers and cyber security experts to emulate the cyber-physical system of the SG in order to perform analytical impact-based experiments. Therefore, there is less confidence in assessing and understanding the nature and consequences of such advanced attacks.

Key Gaps: Many researchers have performed experiments using co-simulation tools consisting of communication and power system modules. A few researchers have also employed Hardware-in-the-loop (HIL) simulation environment to simulate the complex cyber-attacks to comprehend the effect of such attacks on the communication and power system. Other works include the construction of a cyber-physical testbed [1], which is considered an instrumental technique for evaluating cyber-attack. However, all these techniques and tools have some trade-offs; for instance, the co-simulation tool may not offer accurate impact assessment. Similarly, cyber-physical testbed does not offer a cost-effective solution.

Future Directions: Recently, an initiative "MITRE'S ATT&CK framework," has dedicated its work towards collecting and categorizing techniques that are employed by the adversaries against the ICS. Therefore, one of future work is to generate sequences of complex cyber-attacks based on

the data provided by this framework and as well as data from other threat intelligence systems such as Malware Information Sharing Platform (MISP) using a simulation tool in order to understand the nature and impact of such attacks on the cyber and physical operations of the SG (see, e.g., [18, 75, 113]). The experiments should also include identifying the Indicators of Compromise (IoC) in communication and power systems for all types of attacks.

Relevant mathematical equations of the power system need to be utilized to realistically simulate the power system dynamics. Similarly, communication network simulation should consider the packet loss, delay, and cyber security-related events to emulate the behavior of the system realistically. We also suggest that more work is required to practically use the co-simulators for real-time impact monitoring of various cyber-attacks.

5.2 Detection, Visualization and, Monitoring of Attacks

Challenges: For cyber-physical attacks on the control process and communication system of the SG, detection solutions are proposed based on state estimation (e.g., Kalman filter), specification, rule, and statistical models (e.g., Gaussian model) [63]. The aforesaid methods learn the normal operations and processes of the SG, including the communication traffic; however, these methods entail power system and expert knowledge to classify the distribution of normal data. On the other hand, ML and DL methods require realistic labeled datasets for better classification and regression-based detection techniques: There are no publicly available datasets to study the patterns of attacks such as APT and cascading attacks in the SG [111].

MTD has been proposed to detect stealthy attacks on cyber-physical systems such as SG. The main advantage of MTD is that it makes it difficult for an adversary to mount a stealthy attack due to the uncertainty added by the MTD mechanism. However, it is quite a challenging task to decide precisely about the movement of the prevention surface. In addition, the precise timing of the movement is also crucial [116]. In addition, employing a larger number of D-FACT devices can increase the cost of the MTD application.

Key Gaps: The majority of existing work focuses on the detection of FDI attacks [73]. In this direction, the existing works incorporate sensor values (e.g., power flow, frequency, voltage magnitude) to detect attacks, ignoring communication and control system logs, which are quite essential in Spatio-temporal correlation-based detection since FDI attacks are mainly mounted through network packet injection. In this context, other works utilize PMU data for wide-area monitoring and cyber-attack detection [64]. However, the sampling rate of PMU is quite high: Vast computing resources are needed to process the multitude of generated data to detect cyber-attacks.

The existing detection and monitoring solutions are usually based on a SIEM system, which can aggregate different events from different resources, such as intrusion events from SCADA systems and control centers. However, the SIEM system is usually not entirely effective in correlating events generated from industrial communication protocols. In light of the aforementioned problems and gaps, we believe that more research and analysis are still required for SG intrusion detection and monitoring.

Future Directions: Creating an optimal IDS and monitoring system for sophisticated attacks would entail combining and correlating various anomaly detection events in communication and the power system (see, e.g., [79]). For instance, many cyber-attacks on the communication layer can induce an impact on the power system layer and vice versa. Detection tools in SG need to have technological intelligence with a view to discriminate between cyber-attacks, natural events, and normal load disturbances in power systems for optimum SA.

Many potential applications of federated learning, including intrusion detection in the SG, are under-explored. To pick areas that are close to the authors' interests, coordinated and cascading attack detection in the wind turbines and other SG applications can be studied to benefit significantly

from the use of privacy-preserving federated deep learning solutions (see, e.g., [120, 127]). In this direction, federated learning can be further explored to utilize the correlation of temporal, spatial, and logical features of actuators and sensors in the inter-process control loops of the SG to detect stealthy FDI attacks.

More research work is required to formulate an automated way for the timing and movement of MTD parameters. In addition, implementing MTD with the minimum number of D-FACT devices can reduce the overall cost of the MTD-based detection solutions. Therefore, more work is required to efficiently utilize the minimum D-FACT devices to enhance the detection system.

5.3 Cyber-Physical Situational Awareness (CPSA) and Power system Metrics

Challenges: While there are enough SA tools and products for enterprise networks for various security events, these tools are ineffective in controlling system networks such as SGs. In addition, human operators in the control centers of the SG are overwhelmed with a large amount of complex data received from various field devices on different display screens. The abundance of data generated from various devices can also prevent SA among human operators.

The significance of CPSA and power system metrics for SA has been emphasized in NIST guidelines for "Situational Awareness for Electric Utilities" [68]. The metrics should incorporate the Spatio-temporal variations in the SG and should be goal-oriented. Creating efficient CPSA security metrics for power and communication systems entails real data for verification and validation purposes. However, the lack of sharing such datasets among academic researchers and industrialists for legitimate concerns is also a hindrance. Furthermore, all proposed metrics should be tested and validated on reliable data obtained from the SG or testbed environments.

Key Gaps: Information sharing about threat intelligence and new malware is an important step towards better SA within CNI. Some organizations contribute towards this by providing SA information about malicious activity that they observe on their own sensor networks [93]. For instance, the Brazilian National Computer Security Incident Response Team (CSIRT) uses its own deployed honeypot project to collect information about attacks against the honeypots and provide information to the requesting CSIRTs in other countries [93]. However, information about cyber-attacks against real systems is not shared due to legitimate privacy and confidentiality concerns. The contemporary SA tools collect data by PMU sensors to integrate the information for anomalous data. However, the work mostly focuses on PMU-based SA, which does not offer overall SA in SG for different applications. SA framework for SG requires the detection and monitoring across the OT, IT, and physical Access of Control Systems (PACS) in a timely manner. The gap between theoretical guidelines and practical tool development for the SG has not been fulfilled yet.

Future Directions: The integration of complex data from different system displays into a single presentation screen would allow system operators to quickly visualize ongoing malicious activity. The impacts of visualizing correlated information can minimize the analysis and response time. This can be aided by automated cyber situational awareness software tools for optimum alert correlation, damage assessment, and vulnerability analysis. Threat intelligence consisting of technical data should be shared among academic researchers and industrialists. Organization may have non-disclosure agreements and policies in place to ensure that confidential information shared between academic researchers and industrialists is handled appropriately and remain secured.

5.4 Human Factor and Situational Awareness Training

Challenges: Human factors play a crucial role in maintaining overall security in the SG system. Many complex attacks involve adversaries gaining initial access to the system due to human mistakes. Most of the existing work lacks the stress on the human factor and the consequences aroused from their mistakes.

Key Gaps: There is clearly a gap between policy recommendation and policy implementation practices in the SG. The OT security in the SG is yet to formulate more concise norms and standards, which adds yet another obstacle in avoiding human mistakes.

In addition, physical testbeds and HIL simulations are effective ways of providing education and training about the system. However, it may entail significant resources for constructing such a setup. In comparison, co-simulation tools can be quite useful, particularly for power system operators. However, co-simulation tools may not reflect the accurate behavior of communication and power systems. In addition, existing co-simulation tools lack the 3D representation of the system, which may be quite useful for the early career system operators to understand the impact dynamics of cyber-attacks on critical operations of the SG.

Future Directions: Further research should be done to make the policy implementation practices more viable in the SG, ensuring to minimize human mistakes and errors. System operators must be given appropriate SA training to understand the notion of "risk" and "proportionate measures" in tackling security issues in the SG. In addition, the social engineering attack detection framework needs to be revisited to tackle initial infiltration attacks in the SG. Based on the regular training session results, an internal vulnerability scoring system for the employees can construct metrics for the social engineering attack detection framework.

6 CONCLUSION

In this review paper, we focused on the studies that provide detailed analysis about the nature of complex cyber-attacks and their impacts on critical operations of the smart grid. We discussed the recent threat models while proposing the threat modeling framework specifically tailored for the smart grid. We then reviewed various complex attack characteristics and types from the attackers' techniques and tactics perspective. Afterward, we reviewed the detailed taxonomy of existing cyber-attack detection techniques in the smart grid and discussed their performances and capabilities. Additionally, we provided an overview of security operation centers and existing visualization and co-simulation tools and provided their limitations and supported applicability (e.g., real-time) to reflect on their effectiveness in real-world settings. Moreover, we identified cyber-physical situational awareness and power system metrics for the system operators to improve their decision-making capabilities. Furthermore, we discussed the human factor and the significance of awareness training for the system operators to improve their capabilities in noticing the footprints of attacks in the operational smart grid. We finalize this paper by reflecting current challenges and key gaps in line with the scope of our work along with future directions to address them. To conclude, we hope this review paper positively impacts the research community, and guides and motivates researchers and operational technology engineers to build onto the existing promising work that incorporates the trends of hybridizing existing techniques to improve cyber-attack detection, impact monitoring, and visualization by leveraging security and power system metrics.

ACKNOWLEDGEMENT

Authors would like to thank Thales, UK and a team of OT security engineers at the National Digital Exploitation Center (NDEC), Wales for their valuable discussions and constructive feedback for improving this work.

REFERENCES

[1] Sridhar Adepu, Nandha Kumar Kandasamy, and Aditya Mathur. 2018. Epic: An electric power testbed for research and training in cyber physical systems security. In *Computer Security*. Springer, 37–52.

[2] Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke, and Pete Burnap. 2020. Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology* 4, 3 (2020), 125–152.

[3] Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke, and Pete Burnap. 2020. Towards a framework for measuring the performance of a security operations center analyst. In *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE, 1–8.

[4] Saeed Ahmed, YoungDoo Lee, Seung-Ho Hyun, and Insoo Koo. 2019. Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. *IEEE Transactions on Information Forensics and Security* 14, 10 (2019), 2765–2777.

[5] Hooman Alavizadeh, Julian Jang-Jaccard, Simon Yusuf Enoch, Harith Al-Sahaf, Ian Welch, Seyit A Camtepe, and Dan Dongseong Kim. 2022. A Survey on Cyber Situation Awareness Systems: Framework, Techniques, and Insights. *ACM Computing Surveys (CSUR)* (2022).

[6] Otis Alexander, Misha Belisle, and Jacob Steele. 2020. MITRE ATT&CK® for industrial control systems: Design and philosophy. *The MITRE Corporation: Bedford, MA, USA* (2020).

[7] Michael J Assante and Robert M Lee. 2015. The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room* 1 (2015).

[8] Rachad Atat, Muhammad Ismail, Shady S Refaat, Erchin Serpedin, and Thomas Overbye. 2021. Cascading Failure Vulnerability Analysis in Interdependent Power Communication Networks. *IEEE Systems Journal* (2021).

[9] MITRE ATT&CK. 2022. *ICS Techniques.* Retrieved June 8, 2022 from https://attack.mitre.org/techniques/ics/.

[10] Marco Balduzzi, Luca Bongiorni, Ryan Flores, P Lin, Charles Perine, and Rainer Vosseler. 2020. Lost in Translation: When Industrial Protocol Translation Goes Wrong. *Trend Micro* (2020).

[11] Yingkai Bao, Chuangxin Guo, Jinjiang Zhang, Jiaxin Wu, Suhong Pang, and Zhiping Zhang. 2018. Impact analysis of human factors on power system operation reliability. *Journal of Modern Power Systems and Clean Energy* (2018).

[12] Julio Barros, Jose Julio Gutiérrez, Matilde De Apraiz, Saiz, Ramón I Diego, and Andoni Lazkano. 2015. Rapid voltage changes in power system networks and their effect on flicker. *IEEE Transactions on Power Delivery* (2015).

[13] Narayan Bhusal, Michael Abdelmalak, Md Kamruzzaman, and Mohammed Benidris. 2020. Power system resilience: Current practices, challenges, and future directions. *IEEE Access* 8 (2020), 18064–18086.

[14] Alexander Bolshev, Jason Larsen, Marina Krotofil, and Reid Wightman. 2016. A rising tide: Design exploits in industrial control systems. In *10th USENIX Workshop on Offensive Technologies (WOOT 16)*.

[15] Jonathon Brugman, Mohammed Khan, Sneha Kasera, and Masood Parvania. 2019. Cloud based intrusion detection and prevention system for industrial control systems using software defined networking. In *2019 Resilience Week (RWS)*, Vol. 1. IEEE, 98–104.

[16] Defense Use Case. 2016. Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)* 388 (2016).

[17] Zheyuan Cheng and Mo-Yuen Chow. 2021. Resilient Collaborative Distributed AC Optimal Power Flow against False Data Injection Attacks: A Theoretical Framework. *IEEE Transactions on Smart Grid* (2021).

[18] Seungoh Choi, Jongwon Choi, Jeong-Han Yun, Byung-Gil Min, and HyoungChun Kim. 2020. Expansion of {ICS} Testbed for Security Validation based on {MITRE}{ATT&CK} Techniques. In *13th USENIX Workshop on Cyber Security Experimentation and Test (CSET 20)*.

[19] Selim Ciraci, Jeff Daily, Jason Fuller, Andrew Fisher, Laurentiu Marinovici, and Khushbu Agarwal. 2014. FNCS: A framework for power system and communication networks co-simulation. In *Proceedings of the symposium on theory of modeling & simulation-DEVS integrative*. 1–8.

[20] Mingjian Cui, Jianhui Wang, and Bo Chen. 2020. Flexible machine learning-based cyberattack detection using spatiotemporal patterns for distribution systems. *IEEE Transactions on Smart Grid* 11, 2 (2020), 1805–1808.

[21] Mingjian Cui, Jianhui Wang, and Meng Yue. 2019. Machine learning-based anomaly detection for load forecasting under cyberattacks. *IEEE Transactions on Smart Grid* 10, 5 (2019), 5724–5734.

[22] Shuguang Cui, Zhu Han, Soummya Kar, Tung T Kim, H Vincent Poor, and Ali Tajer. 2012. Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions. *IEEE Signal Processing Magazine* 29, 5 (2012), 106–115.

[23] Zhiquan Dong, Tianqi Xu, Yan Li, Peilei Feng, Xin Gao, and Xueying Zhang. 2017. Review and application of situation awareness key technologies for smart grid. In *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*. IEEE, 1–6.

[24] Junhong Duan, Bo Zhao, and Sensen Guo. 2020. The Design and Implementation of Smart Grid SOC Platform. In *2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA)*, Vol. 1.

[25] Zakaria El Mrabet, Naima Kaabouch, Hassan El Ghazi, and Hamid El Ghazi. 2018. Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering* 67 (2018), 469–482.

[26] Mica R Endsley. 1995. Toward a theory of situation awareness in dynamic systems. *Human factors* 37, 1 (1995), 32–64.

[27] Muhammad Faheem, Syed Bilal Hussain Shah, Rizwan Aslam Butt, Basit Raza, Muhammad Anwar, Muhammad Waqar Ashraf, Md A Ngadi, and Vehbi C Gungor. 2018. Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. *Computer Science Review* 30 (2018), 1–30.

[28] Keke Gai, Meikang Qiu, Zhong Ming, Hui Zhao, and Longfei Qiu. 2017. Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. *IEEE Transactions on Smart Grid* 8, 5 (2017), 2431–2439.
[29] Prakhar Ganesh, Xin Lou, Yao Chen, Rui Tan, David KY Yau, Deming Chen, and Marianne Winslett. 2021. Learning-based Simultaneous Detection and Characterization of Time Delay Attack in Cyber-Physical Systems. *IEEE Transactions on Smart Grid* (2021).
[30] Luis Garcia, Ferdinand Brasser, Mehmet Hazar Cintuglu, Ahmad-Reza Sadeghi, Osama A Mohammed, and Saman A Zonouz. 2017. Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit.. In *NDSS*.
[31] Jairo Giraldo, Alvaro Cardenas, and Ricardo G Sanfelice. 2019. A moving target defense to detect stealthy attacks in cyber-physical systems. In *2019 American Control Conference (ACC)*. IEEE, 391–396.
[32] Jairo Giraldo, David Urbina, Alvaro Cardenas, Junia Valente, Mustafa Faisal, Justin Ruths, Nils Ole Tippenhauer, Henrik Sandberg, and Richard Candell. 2018. A survey of physics-based attack detection in cyber-physical systems. *ACM Computing Surveys (CSUR)* 51, 4 (2018), 1–36.
[33] Jairo Giraldo, David Urbina, Alvaro A Cardenas, and Nils Ole Tippenhauer. 2019. Hide and seek: An architecture for improving attack-visibility in industrial control systems. In *International Conference on Applied Cryptography and Network Security*. Springer, 175–195.
[34] Qinchen Gu, David Formby, Shouling Ji, Brendan Saltaformaggio, Anu Bourgeois, and Raheem A Beyah. 2021. This Hacker Knows Physics: Device Physics Aware Mimicry Attacks in Cyber-Physical Systems. *IEEE Transactions on Dependable and Secure Computing* (2021).
[35] Muhammed Zekeriya Gunduz and Resul Das. 2020. Cyber-security on smart grid: Threats and potential solutions. *Computer networks* 169 (2020), 107094.
[36] Xi He, Xuan Liu, and Peng Li. 2020. Coordinated false data injection attacks in AGC system and its countermeasure. *IEEE Access* 8 (2020), 194640–194651.
[37] Youbiao He, Gihan J Mendis, and Jin Wei. 2017. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Transactions on Smart Grid* 8, 5 (2017), 2505–2516.
[38] Filip Holik, Lars Halvdan Flå, Martin Gilje Jaatun, Sule Yildirim Yayilgan, and Jørn Foros. 2022. Threat modeling of a smart grid secondary substation. *Electronics* 11, 6 (2022), 850.
[39] Junho Hong, Reynaldo F Nuqui, Anil Kondabathini, Dmitry Ishchenko, and Aaron Martin. 2018. Cyber attack resilient distance protection and circuit breaker control for digital substations. *IEEE Transactions on Industrial Informatics* 15, 7 (2018), 4332–4341.
[40] Kenneth Hopkinson, Xiaoru Wang, Renan Giovanini, James Thorp, Kenneth Birman, and Denis Coury. 2006. EPOCHS: A platform for agent-based electric power and communication simulation built from commercial off-the-shelf components. *IEEE Transactions on Power Systems* 21, 2 (2006), 548–558.
[41] ICS-CERT. 2016. Cyber-attack against ukrainian critical infrastructure. *Cybersecurity Infrastruct. Secur. Agency, Washington, DC, USA, Tech. Rep. ICS Alert (IR-ALERT-H-16-056-01)* (2016).
[42] Wayne A Jansen. 2009. *Directions in security metrics research.* Diane Publishing.
[43] BooJoong Kang, Kieran McLaughlin, and Sakir Sezer. 2016. Towards a stateful analysis framework for smart grid network intrusion detection. In *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4*. 124–131.
[44] Anastasis Keliris, Charalambos Konstantinou, Marios Sazos, and Michail Maniatakos. 2019. Open source intelligence for energy sector cyberattacks. In *Critical infrastructure security and resilience*. Springer, 261–281.
[45] Rafiullah Khan, Kieran McLaughlin, David Laverty, and Sakir Sezer. 2017. STRIDE-based threat modeling for cyber-physical systems. In *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*.
[46] Yew Meng Khaw, Amir Abiri Jahromi, Mohammadreza FM Arani, Scott Sanner, Deepa Kundur, and Marthe Kassouf. 2020. A deep learning-based cyberattack detection system for transmission protective relays. *IEEE Transactions on Smart Grid* 12, 3 (2020), 2554–2565.
[47] Anna Magdalena Kosek. 2016. Contextual anomaly detection for cyber-physical security in smart grids based on an artificial neural network model. In *2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*. IEEE, 1–6.
[48] David J Krajnak. 2000. Faulted circuit indicators and system reliability. In *2000 Rural Electric Power Conference. Papers Presented at the 44th Annual Conference (Cat. No. 00CH37071)*. IEEE, A4–1.
[49] Mehmet Necip Kurt, Yasin Yılmaz, and Xiaodong Wang. 2018. Real-time detection of hybrid and stealthy cyber-attacks in smart grid. *IEEE Transactions on Information Forensics and Security* 14, 2 (2018), 498–513.
[50] Sungmoon Kwon, Hyunguk Yoo, and Taeshik Shon. 2020. IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system. *IEEE Access* 8 (2020), 77572–77586.
[51] YooJin Kwon, Huy Kang Kim, Yong Hun Lim, and Jong In Lim. 2015. A behavior-based intrusion detection technique for smart grid infrastructure. In *2015 IEEE Eindhoven PowerTech*. IEEE, 1–6.
[52] Subhash Lakshminarayana, E Veronica Belmega, and H Vincent Poor. 2019. Moving-target defense for detecting coordinated cyber-physical attacks in power grids. In *2019 IEEE International Conference on Communications, Control,*

and Computing Technologies for Smart Grids (SmartGridComm). IEEE, 1–7.
[53] Tan Duy Le, Adnan Anwar, Razvan Beuran, and Seng W Loke. 2019. Smart grid co-simulation tools: Review and cybersecurity case study. In *2019 7th International Conference on Smart Grid (icSmartGrid)*. IEEE, 39–45.
[54] Hao Li, Guangjie Liu, Weiwei Jiang, and Yuewei Dai. 2015. Designing snort rules to detect abnormal DNP3 network data. In *2015 International Conference on Control, Automation and Information Sciences (ICCAIS)*. IEEE, 343–348.
[55] W Li, A Monti, Mt Luo, and Roger A Dougal. 2011. VPNET: A co-simulation framework for analyzing communication channel effects on power systems. In *2011 IEEE Electric Ship Technologies Symposium*. IEEE, 143–149.
[56] Gaoqi Liang, Steven R Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong. 2016. The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems* 32, 4 (2016), 3317–3318.
[57] Gaoqi Liang, Junhua Zhao, Fengji Luo, Steven R Weller, and Zhao Yang Dong. 2016. A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid* 8, 4 (2016), 1630–1638.
[58] Bo Liu and Hongyu Wu. 2020. Optimal D-FACTS placement in moving target defense against false data injection attacks. *IEEE Transactions on Smart Grid* 11, 5 (2020), 4345–4357.
[59] Bo Liu and Hongyu Wu. 2021. Optimal Planning and Operation of Hidden Moving Target Defense for Maximal Detection Effectiveness. *IEEE Transactions on Smart Grid* (2021).
[60] Hongyu Liu and Bo Lang. 2019. Machine learning and deep learning methods for intrusion detection systems: A survey. *applied sciences* 9, 20 (2019), 4396.
[61] Qi Liu, Veit Hagenmeyer, and Hubert B Keller. 2021. A Review of Rule Learning-Based Intrusion Detection Systems and Their Prospects in Smart Grids. *IEEE Access* 9 (2021), 57542–57564.
[62] Zengji Liu, Qi Wang, and Yi Tang. 2020. Design of a cosimulation platform with hardware-in-the-loop for cyber-attacks on cyber-physical power systems. *IEEE Access* 8 (2020), 95997–96005.
[63] Yuan Luo, Ya Xiao, Long Cheng, Guojun Peng, and Danfeng Yao. 2021. Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. *ACM Computing Surveys (CSUR)* 54, 5 (2021), 1–36.
[64] Rui Ma, Sagnik Basumallik, and Sara Eftekharnejad. 2020. A PMU-based data-driven approach for classifying power system events considering cyberattacks. *IEEE Systems Journal* 14, 3 (2020), 3558–3569.
[65] Srinidhi Madabhushi and Rinku Dewri. 2021. Detection of Demand Manipulation Attacks on a Power Grid. In *2021 18th International Conference on Privacy, Security and Trust (PST)*. IEEE, 1–7.
[66] Malaz Mallouhi, Youssif Al-Nashif, Don Cox, Tejaswini Chadaga, and Salim Hariri. 2011. A testbed for analyzing security of SCADA control systems (TASSCS). In *ISGT 2011*. IEEE, 1–7.
[67] Mohamed Massaoudi, Haitham Abu-Rub, Shady S Refaat, Ines Chihi, and Fakhreddine S Oueslati. 2021. Deep learning in smart grid technology: A review of recent advancements and future prospects. *IEEE Access* 9 (2021), 54558–54578.
[68] James McCarthy, Otis Alexander, Sallie Edwards, Don Faatz, Chris Peloquin, Susan Symington, Andre Thibault, John Wiltberger, and Karen Viani. 2019. *Situational awareness for electric utilities*. Technical Report. National Institute of Standards and Technology.
[69] Sadegh M Milajerdi, Rigel Gjomemo, Birhanu Eshete, Ramachandran Sekar, and VN Venkatakrishnan. 2019. Holmes: real-time apt detection through correlation of suspicious information flows. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1137–1152.
[70] Parya Haji Mirzaee, Mohammad Shojafar, Haitham Cruickshank, and Rahim Tafazolli. 2022. Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures). *IEEE Access* (2022).
[71] Mitre. 2022. *Common Weakness Enumeration: CWE Most Important Hardware Weaknesses*. Retrieved June 1, 2022 from https://cwe.mitre.org/index.html
[72] Sathya Narayana Mohan. 2019. *Distributed intrusion detection/prevention system design and implementation for secure SCADA communication in smart grid*. Ph.D. Dissertation. Iowa State University.
[73] Ahmed S Musleh, Guo Chen, and Zhao Yang Dong. 2019. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Transactions on Smart Grid* 11, 3 (2019), 2218–2234.
[74] Muhammad Nouman Nafees, Neetesh Saxena, and Pete Burnap. 2021. Optimized Predictive Control for AGC Cyber Resiliency. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 2450–2452.
[75] Sai Pushpak Nandanoori. 2021. *Nominal and adversarial synthetic PMU data for standard IEEE test systems*. Technical Report. Pacific Northwest National Lab.(PNNL), Richland, WA (United States).
[76] Barry C Newburn. 2015. *Implementing national electrical reliability corporation/critical infrustructure protection standards (NERC/CIP) in the real world utility industry*. Ph.D. Dissertation. Utica College.
[77] Tu Nguyen, Bing-Hong Liu, Nam Nguyen, Braulio Dumba, and Jung-Te Chou. 2021. Smart Grid Vulnerability and Defense Analysis Under Cascading Failure Attacks. *IEEE Transactions on Power Delivery* (2021).
[78] Tien Nguyen, Shiyuan Wang, Mohannad Alhazmi, Mostafa Nazemi, Abouzar Estebsari, and Payman Dehghanian. 2020. Electric power grid resilience to cyber adversaries: State of the art. *IEEE Access* 8 (2020), 87592–87608.
[79] Xiangyu Niu, Jiangnan Li, Jinyuan Sun, and Kevin Tomsovic. 2019. Dynamic detection of false data injection attack in smart grid using deep learning. In *2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference*

(ISGT). IEEE, 1–6.
[80] Fraser Orr, Muhammad Nouman Nafees, Neetesh Saxena, and Bong Jun Choi. 2021. Securing Publisher–Subscriber Smart Grid Infrastructure. *Electronics* 10, 19 (2021), 2355.
[81] Shengyi Pan, Thomas Morris, and Uttam Adhikari. 2015. Developing a hybrid intrusion detection system using data mining for power systems. *IEEE Transactions on Smart Grid* 6, 6 (2015), 3104–3113.
[82] Shengyi Pan, Thomas H Morris, and Uttam Adhikari. 2015. A Specification-based Intrusion Detection Framework for Cyber-physical Environment in Electric Power System. *Int. J. Netw. Secur.* 17, 2 (2015), 174–188.
[83] Mathaios Panteli and Pierluigi Mancarella. 2015. The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience. *IEEE Power and Energy Magazine* 13, 3 (2015), 58–66.
[84] Mathaios Panteli, Pierluigi Mancarella, Dimitris N Trakas, Elias Kyriakides, and Nikos D Hatziargyriou. 2017. Metrics and quantification of operational and infrastructure resilience in power systems. *IEEE Transactions on Power Systems* 32, 6 (2017), 4732–4742.
[85] Marcus Pendleton, Richard Garcia-Lebron, Jin-Hee Cho, and Shouhuai Xu. 2016. A survey on systems security metrics. *ACM Computing Surveys (CSUR)* 49, 4 (2016), 1–35.
[86] Da-Tian Peng, Jianmin Dong, Jungang Yang, Zhongmin Cai, and Qinke Peng. 2022. Dynamical Failures Driven by False Load Injection Attacks Against Smart Grid. *IEEE Transactions on Information Forensics and Security* (2022).
[87] Panagiotis I Radoglou-Grammatikis and Panagiotis G Sarigiannidis. 2019. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access* 7 (2019), 46595–46620.
[88] Habibollah Raoufi, Vahid Vahidinasab, and Kamyar Mehran. 2020. Power systems resilience metrics: A comprehensive review of challenges and outlook. *Sustainability* 12, 22 (2020), 9698.
[89] Mark J Rice, Christopher A Bonebrake, Greg K Dayley, and Larry J Becker. 2017. *Secure ICCP final report.* Technical Report. Pacific Northwest National Lab.(PNNL), Richland, WA (United States).
[90] Martin Roesch et al. 2011. Snort, network intrusion detection/prevention system.
[91] Martin Rosso, Michele Campobasso, Ganduulga Gankhuyag, and Luca Allodi. 2020. Saibersoc: Synthetic attack injection to benchmark and evaluate the performance of security operation centers. In *Annual Computer Security Applications Conference*. 141–153.
[92] Shanto Roy, Nazia Sharmin, Jaime C Acosta, Christopher Kiekintveld, and Aron Laszka. 2022. Survey and Taxonomy of Adversarial Reconnaissance Techniques. *ACM Computing Surveys (CSUR)* (2022).
[93] Robin M. Ruefle and M. Murray. 2014. *CSIRT Requirements for Situational Awareness:*. Technical Report. Defense Technical Information Center, Fort Belvoir, VA. https://doi.org/10.21236/ADA596848
[94] Mohammad Ashraf Hossain Sadi, Mohd Hassan Ali, Dipankar Dasgupta, and Robert K Abercrombie. 2015. OPNET/simulink based testbed for disturbance detection in the smart grid. In *Proceedings of the 10th Annual Cyber and Information Security Research Conference*. 1–4.
[95] Mohammad Reza Salehizadeh, Ashkan Rahimi-Kian, and Majid Oloomi-Buygi. 2015. Security-based multi-objective congestion management for emission reduction in power system. *International Journal of Electrical Power & Energy Systems* 65 (2015), 124–135.
[96] Neetesh Saxena and Bong Jun Choi. 2015. State of the art authentication, access control, and secure integration in smart grid. *Energies* 8, 10 (2015), 11883–11915.
[97] Neetesh Saxena, Victor Chukwuka, Leilei Xiong, and Santiago Grijalva. 2017. CPSA: A cyber-physical security assessment tool for situational awareness in smart grid. In *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*. 69–79.
[98] Neetesh Saxena, Emma Hayes, Elisa Bertino, Patrick Ojo, Kim-Kwang Raymond Choo, and Pete Burnap. 2020. Impact and key challenges of insider threats on organizations and critical businesses. *Electronics* 9, 9 (2020), 1460.
[99] Neetesh Saxena, Vasilis Katos, and Neeraj Kumar. 2017. Cyber-Physical Smart Grid Security Tool for Education and Training Purposes. (2017).
[100] Neetesh Saxena, Leilei Xiong, Victor Chukwuka, and Santiago Grijalva. 2018. Impact evaluation of malicious control commands in cyber-physical smart grids. *IEEE Transactions on Sustainable Computing* 6, 2 (2018), 208–220.
[101] Robert Schuerger, Robert Arno, and Neal Dowling. 2016. Why existing utility metrics do not work for industrial reliability analysis. *IEEE Transactions on Industry Applications* 52, 4 (2016), 2801–2806.
[102] Cyber Security and Infrastructure Security Agency. 2020. *ICS Advisory.* Retrieved May 22, 2022 from https://www.cisa.gov/uscert/ics/advisories/icsa-20-343-07
[103] Cyber Security and Infrastructure Security Agency. 2022. *ICS Advisory: Schneider Electric Easergy P5 and P3.* Retrieved May 20, 2022 from https://www.cisa.gov/uscert/ics/advisories/icsa-22-055-03
[104] Neeraj Seth and Faruk S Kazi. 2018. Vulnerability of Intelligent Electronic Devices (IED) to Time Synchronization Spoofing in Power Grid and Jamming of GNSS Receiver. In *2018 IEEE 8th Power India International Conference (PIICON)*. IEEE, 1–6.

[105] Andreas Sfakianakis, Christos Douligeris, Louis Marinos, Marco Lourenço, and Omid Raghimi. 2019. Enisa threat landscape report 2018: 15 top cyberthreats and trends. *DOI* 10 (2019), 622757.

[106] Tohid Shekari, Celine Irvene, Alvaro A Cardenas, and Raheem Beyah. 2021. MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 1338–1356.

[107] PW Singer. 2015. Stuxnet and its hidden lessons on the ethics of cyberweapons. *Case W. Res. J. Int'l L.* 47 (2015), 79.

[108] Vivek Kumar Singh and Manimaran Govindarasu. 2021. A Cyber-Physical Anomaly Detection for Wide-Area Protection using Machine Learning. *IEEE Transactions on Smart Grid* (2021).

[109] Ayush Sinha, Manasi Mohandas, Pankaj Pandey, and OP Vyas. 2021. Cyber Physical Defense Framework for Distributed Smart Grid Applications. *Frontiers in Energy Research* (2021), 407.

[110] Ilias Siniosoglou, Panagiotis Radoglou-Grammatikis, Georgios Efstathopoulos, Panagiotis Fouliras, and Panagiotis Sarigiannidis. 2021. A unified deep learning anomaly detection and classification approach for smart grid environments. *IEEE Transactions on Network and Service Management* (2021).

[111] Branka Stojanović, Katharina Hofer-Schmitz, and Ulrike Kleb. 2020. APT datasets and attack modeling for automated detection methods: A review. *Computers & Security* 92 (2020), 101734.

[112] Seyedeh Mahsan Taghavinejad, Mehran Taghavinejad, Lida Shahmiri, Mohammad Zavvar, and Mohammad Hossein Zavvar. 2020. Intrusion detection in IoT-based smart grid using hybrid decision tree. In *2020 6th International Conference on Web Research (ICWR)*. IEEE, 152–156.

[113] Yusuke Takahashi, Shigeyoshi Shima, Rui Tanabe, and Katsunari Yoshioka. 2020. {APTGen}: An Approach towards Generating Practical Dataset Labelled with Targeted Attack Sequences. In *13th USENIX Workshop on Cyber Security Experimentation and Test (CSET 20)*.

[114] Rui Tan, Hoang Hai Nguyen, Eddy YS Foo, Xinshu Dong, David KY Yau, Zbigniew Kalbarczyk, Ravishankar K Iyer, and Hoay Beng Gooi. 2016. Optimal false data injection attack against automatic generation control in power grids. In *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 1–10.

[115] Khalid Hasan Tantawi, Alexandr Sokolov, and Omar Tantawi. 2019. Advances in industrial robotics: From industry 3.0 automation to industry 4.0 collaboration. In *2019 4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON)*. IEEE, 1–4.

[116] Jue Tian, Rui Tan, Xiaohong Guan, Zhanbo Xu, and Ting Liu. 2019. Moving target defense approach to detecting stuxnet-like attacks. *IEEE transactions on smart grid* 11, 1 (2019), 291–300.

[117] Ana Ruxandra Toma, Ana-Maria Dumitrescu, and Mihaela Albu. 2015. Assessment of rapid voltage changes using PMU data. In *2015 IEEE International Workshop on Applied Measurements for Power Systems (AMPS)*. IEEE, 126–131.

[118] Eric D Vugrin, Andrea R Castillo, and Cesar Augusto Silva-Monroy. 2017. *Resilience Metrics for the Electric Power System: A Performance-Based Approach.* Technical Report. Sandia National Lab, United States.

[119] Mingkui Wei, Zhuo Lu, and Wenye Wang. 2017. On characterizing information dissemination during city-wide cascading failures in smart grid. *IEEE Systems Journal* 12, 4 (2017), 3404–3413.

[120] Mi Wen, Rong Xie, Kejie Lu, Liangliang Wang, and Kai Zhang. 2021. FedDetect: A Novel Privacy-Preserving Federated Learning Framework for Energy Theft Detection in Smart Grid. *IEEE Internet of Things Journal* (2021).

[121] Yingmeng Xiang, Lingfeng Wang, and Nian Liu. 2017. Coordinated attacks on electric power systems in a cyber-physical environment. *Electric Power Systems Research* 149 (2017), 156–168.

[122] Jie Yang, Yihao Guo, Chuangxin Guo, Zhe Chen, and Shenghan Wang. 2021. Cross-Space Risk Assessment of Cyber-Physical Distribution System Under Integrated Attack. *IEEE Access* 9 (2021), 149859–149869.

[123] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. 2019. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)* 10, 2 (2019), 1–19.

[124] Hang Zhang, Bo Liu, and Hongyu Wu. 2021. Smart grid cyber-physical attack and defense: a review. *IEEE Access* 9 (2021), 29641–29659.

[125] Ying Zhang, Jianhui Wang, and Bo Chen. 2020. Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach. *IEEE Transactions on Smart Grid* 12, 1 (2020), 623–634.

[126] Ying Zhang, Jianhui Wang, and Jianzhe Liu. 2019. Attack identification and correction for PMU GPS spoofing in unbalanced distribution systems. *IEEE transactions on smart grid* 11, 1 (2019), 762–773.

[127] Liang Zhao, Jiaming Li, Qi Li, and Fangyu Li. 2021. A Federated Learning Framework for Detecting False Data Injection Attacks in Solar Farms. *IEEE Transactions on Power Electronics* 37, 3 (2021), 2496–2501.

[128] Peidong Zhu, Peng Xun, Yifan Hu, and Yinqiao Xiong. 2021. Social collective attack model and procedures for large-scale cyber-physical systems. *Sensors* 21, 3 (2021), 991.

[129] C Zimmerman. 2014. Ten Strategies of a World-Class Cybersecurity Operations Centre. The Mitre Corporation.

[130] Ioannis Zografopoulos, Juan Ospina, Xiaorui Liu, and Charalambos Konstantinou. 2021. Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access* 9 (2021), 29775–29818.