Received 23 December 2023, accepted 3 February 2024, date of publication 8 February 2024, date of current version 29 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3364362

SURVEY

A Survey on Cyber-Physical Security of Active Distribution Networks in Smart Grids

MOHSEN KHALAF[1,2], (Senior Member, IEEE),
ABDELRAHMAN AYAD[3], (Graduate Student Member, IEEE),
MOSADDEK HOSSAIN KAMAL TUSHAR[4], (Member, IEEE),
MARTHE KASSOUF[5], AND DEEPA KUNDUR[1], (Fellow, IEEE)

[1]Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 1A1, Canada
[2]Electrical Engineering Department, Assiut University, Assiut 71515, Egypt
[3]Department of Electrical and Computer Engineering, McGill University, Montreal, QC H3A 0G4, Canada
[4]Department of Computer Science and Engineering, University of Dhaka, Dhaka 1000, Bangladesh
[5]Hydro Quebec Research Institute (IREQ), Montreal, QC J3X 1S1, Canada

Corresponding author: Mohsen Khalaf (m.khalaf@utoronto.ca)

This work was supported in part by a Collaborative Project between the University of Toronto, Hydro-Québec Research Institute, and the Communications Security Establishment Canada titled "Cybersecurity Enhancement for Smart Grids Using an Information Technology (IT)/Operational Technology (OT) Convergence Approach" funded by the Canadian Safety and Security Program (2017–2020) and by NSERC through the Discovery Grant program.

ABSTRACT Distribution systems are evolving from traditional passive networks into, what is known as, Active Distribution Networks (ADNs). Unlike traditional distribution networks, ADNs are characterized by bi-directional power flow, the high penetration of DERs, storage capabilities and sophisticated control strategies. Multiple layers of communications, sensing and computation are being integrated into ADNs for monitoring, control and protection of a variety of components and critical operations. This enhanced dependency on information and communication technologies, however, increases the exposure of ADNs to cyber-attacks. Several papers have been published in recent years with a focus on cyber-physical security (CPS) of smart grids. However, the published survey papers primarily emphasize the transmission level of smart grid threats and challenges, with little focus on the ADNs. Given the rapid deployment of ADNs and the increasing cyber threats against power grids and critical infrastructures, we are motivated, in this article, to present a review and survey focused, instead, on the latest research advancements in the area of CPS for ADNs. This paper represents the first survey of timely research in the area of CPS of ADNs with a focus on ADN critical operations and components. The cyber-physical aspects of each critical operation/component are analyzed. In addition, the challenges and requirements of associated communication protocols and standards are presented. Cybersecurity of ADN devices and sensors including Phasor Measurement Units (PMUs), smart meters, advanced metering infrastructure and protection relays are discussed in detail. Moreover, a thorough study of ADNs application drivers and enablers including microgrids, Electric Vehicles (EVs), Internet-of-Things (IoT) and smart homes is conducted. Potential and existing solutions by industry are highlighted. Finally, survey outcomes and directions for future work are presented to highlight emerging avenues of research.

INDEX TERMS Cyber-physical security, cybersecurity, active distribution networks, smart grids, volt/var control, false data injection, microgrids.

I. INTRODUCTION

Conventional distribution systems are passive networks, with unidirectional power flow and a minimal level of centralized control and monitoring. In contrast, active distribution networks (ADNs) are characterized by large shares of Distributed Energy Resource (DER) penetration, bidirectional power flow, storage capabilities, sophisticated control strategies, and multiple communication layers [1], [2]. These recent advancements are radically changing energy systems

The associate editor coordinating the review of this manuscript and approving it for publication was Ha Nguyen.

infrastructure in addition to the increasingly interactive role of consumers in accelerating the deployment of distribution resources [3]. For instance, the rise in Electric Vehicle (EV) penetration rates and the growing use of consumer mobile applications to control residential appliances would certainly contribute to the distribution grid becoming more "active" [4]. As a result, traditional distribution networks have been rendered into ADNs offering many technological advantages and economic benefits, as well as numerous challenges.

Cyber-physical security (CPS) is currently regarded as one of these major challenges. CPS enables the creation of technologies that promote climate change and energy security in a growingly complex geopolitical landscape. CPS facilitates the adoption of trusted sustainable energy systems while enhancing a nation's sovereign critical infrastructure capabilities. The cyberattack on the Ukrainian power grid in December 2015 [5] started at the distribution level and propagated to the whole grid causing catastrophic consequences. The attackers were able to launch a software-based cyberattack by installing BlackEnergy (BE) malware in the computers of 3 distribution companies in Ukraine. This attack disconnected substations and caused a blackout that affected more than 200,000 people. However, and despite the increasing attention regarding CPS of power systems in general [6], [7], [8], [9], [10], [11], disproportionately few papers have solely focused on ADNs CPS. Indeed, several research works have discussed CPS vulnerabilities, attack formulations and even mitigation techniques on all levels of the electric power grid [9], [10], [12], [13], [14], [15], [16], [17]. Nevertheless, it is important to mention that most of these investigations have been focused on the transmission level, for simplification in some cases and for presenting a general framework in others. Musleh et al. found that only 3.5% of published works focused on the distribution level [8]. Previous literature has primarily focused on transmission system cybersecurity for several reasons. First, attacks on transmission grids might have fatal consequences leading to significant impacts on service continuity and restoration costs [14], [18]. Second, transmission grid components such as substations and Wide-Area Monitoring, Protection and Control (WAMPAC) systems can often be described by environments that have a relatively small number of system components, equipment, and communication networks in comparison to distribution grids [13]. However, the proliferation of DERs has introduced new opportunities at the distribution level, and consequently, introduced new threats to the operation of ADNs. In addition, ADNs are typically spread over broad geographic areas that include a large number of heterogeneous devices and systems [19]. Moreover, the inherent fundamental differences between ADNs and transmission grids in terms of system topologies and feeder unbalance, control objectives hierarchy and large share integration of DERs [20] oblige a more detailed analysis of CPS to extend attack formulations, detection and mitigation to ADNs [9].

Due to the more general approach adopted by the above-mentioned works, detailed characteristics and operations of ADNs were not sufficiently discussed and reviewed with enough depth within any single work. Motivated by these research gaps, this survey work focuses -for the first time- on the ADN CPS requirements, challenges, strategies, and applications. The contributions of this paper can be summarized as follows:

- The modern distribution network components, devices and services are reviewed with a focus on the critical operations of ADNs such as Volt/Var Control (VVC), Distribution Systems State Estimation (DSSE) and Optimal Power Flow (OPF), and ADNs devices and sensors including PMUs, Advanced Metering Infrastructure (AMI) and protective devices are reviewed.
- The challenges and requirements of CPS in ADNs as well as the associated communication network and protocol characteristics are presented.
- The recent advancements in the CPS of ADNs application enablers and drivers including Microgrids (MGs), EVs and Internet-of-Things (IoT)-based smart homes are reviewed.
- Practical solutions that have been implemented recently by industry stakeholders are surveyed.

To do so, we adopt the following methodology to comprehensively discuss research in the interdisciplinary field of ADN CPS. First, a background of ADN operation and CPS is provided to establish the necessary foundation for the topics discussed in this survey. The structure and flow of the paper are depicted in Fig. 1. Section II of the paper presents an overview of ADN development including the major transformational changes from the conventional distribution network operational paradigm. We have categorized these changes into four main categories including i) the new critical operations in distribution systems such as VVC, DSSE and OPF, ii) the developments in the communication systems, iii) the advancements in metering technologies and introducing new metering devices and sensors, and iv) applications drivers and enablers such as MGs, EVs and IoT-based smart homes that are promoted by the first three categories and became main components in ADNs. Following this overview, and to pave the road for the discussion about the cybersecurity of ADNs, it is crucial to explain the CPS requirements and challenges in ADNs as well as timely communication standards, protocols and requirements in ADNs. This discussion, in addition to the threats targeting the current ADNs infrastructure, is reviewed in Section III.

Using advanced devices and sensors for monitoring, protection and control purposes in ADNs also resulted in compromising the cybersecurity of ADNs. This is because these devices are dependent on the vulnerable communication system. In addition, the attackers can implement device-level attacks by compromising the device itself. On the topic of

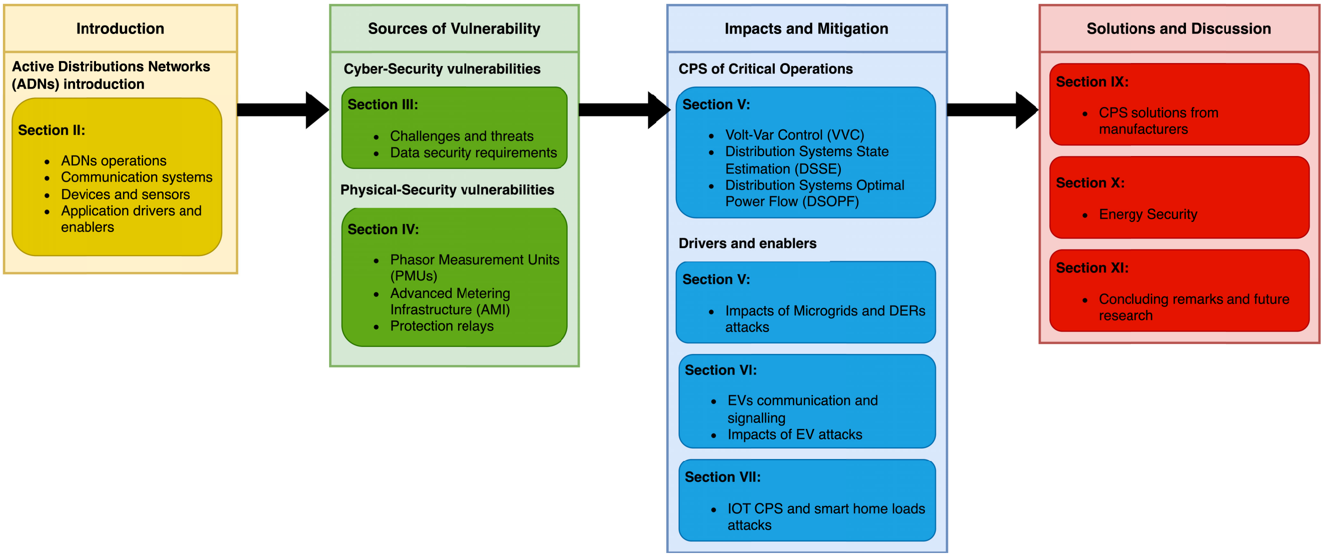
Introduction
Active Distributions Networks (ADNs) introduction
Section II:
ADNs operations
Communication systems
Devices and sensors
Application drivers and enablers
Sources of Vulnerability
Cyber-Security vulnerabilities
Section III:
Challenges and threats
Data security requirements
Physical-Security vulnerabilities
Section IV:
Phasor Measurement Units (PMUs)
Advanced Metering Infrastructure (AMI)
Protection relays
Impacts and Mitigation
CPS of Critical Operations
Section V:
Volt-Var Control (VVC)
Distribution Systems State Estimation (DSSE)
Distribution Systems Optimal Power Flow (DSOPF)
Drivers and enablers
Section V:
Impacts of Microgrids and DERs attacks
Section VI:
EVs communication and signalling
Impacts of EV attacks
Section VII:
IOT CPS and smart home loads attacks
Solutions and Discussion
Section IX:
CPS solutions from manufacturers
Section X:
Energy Security
Section XI:
Concluding remarks and future research

FIGURE 1. Paper structure and flow.

sensors and devices, Section IV considers the CPS of AMI, Phasor Measurement Units (PMUs), as well as advanced digital field devices. We consider different energy theft threats in ADNs and review countermeasures proposed in the literature.

After reviewing the sources of cyber vulnerabilities in the ADNs, we focus on the cybersecurity of critical operations as well as application drivers and enablers in ADNs. Each of the subsequent sections in this survey discusses a major aspect of ADN CPS. Cybersecurity aspects of critical operations in ADNs are defined in Section V. Next, the integration of Microgrids (MGs), DERs, EVs and IoT-based smart homes as well as the associated CPS aspects are reviewed. Section VI reviews approaches to enhance ADN CPS including impact assessment, attack detection, mitigation and self-healing of MGs and DERs. Section VII presents recent advances in CPS of EVs and charging stations. Section VIII analyzes the critical role that IoT currently plays in ADNs and its impact motivating the need to address CPS challenges including demand side management security and smart home controllable load attacks. The role of industry is also discussed in this survey in Section IX, which focuses on practical aspects of CPS of ADNs. In Section IX, commercially available solutions and devices from manufacturers are reviewed and assessed based on the associated requirements. Section X discusses the importance of energy security and sovereign capability on ADNs. Finally, the concluding remarks and the future research outlook in light of the findings are presented in Section XI.

II. ACTIVE DISTRIBUTION NETWORKS

Distribution systems are witnessing radical transformations in their infrastructure [22], [23]. This shift from passive to ADNs is driven by the increasing penetration of DERs, sophisticated control techniques, and the integration of communication technologies resulting from consumer-directed energy management. CPS of ADNs is a vital area of research due to the severe consequences that may result from cyber-attacks on these critical infrastructures [24], [25], [26].

Modern ADNs are characterized by i) integration of large shares of DERs [21]; ii) reliance on interconnected communication infrastructures [12]; iii) distributed voltage and power-sharing control structures [27]; iv) utilization of AMI, PMUs and smart field devices [28], and v) consumer participation in energy management [29]. The "active" nature of these systems can largely be attributed to enhancements in functionality that make power distribution more adaptable and responsive to the changing energy landscape. Although currently, no official reference architecture for ADNs exists, we provide a brief overview of the different components such systems entail in Fig. 2. As shown in the figure, ADNs involve a range of components that enable advanced control, monitoring, and management of electricity distribution. Some of these components include Distributed Energy Resources (DERs), energy storage system, advanced monitoring and control center, grid automation and smart switchgear, load management facilities and advanced microprocessor-based protection devices. These components work together to create a more flexible, resilient, and efficient distribution network capable of accommodating a high penetration of renewable energy sources and meeting the evolving demands of the modern power system.

The sheer diversity of ADNs compared to transmission-level systems makes it challenging to develop a single framework to describe their operation. The reader is referred to the aforementioned references in this section for more information on each aspect. As evident, ADNs represent a more participatory network with greater engagement from consumers and increased coordination on the part of utilities.

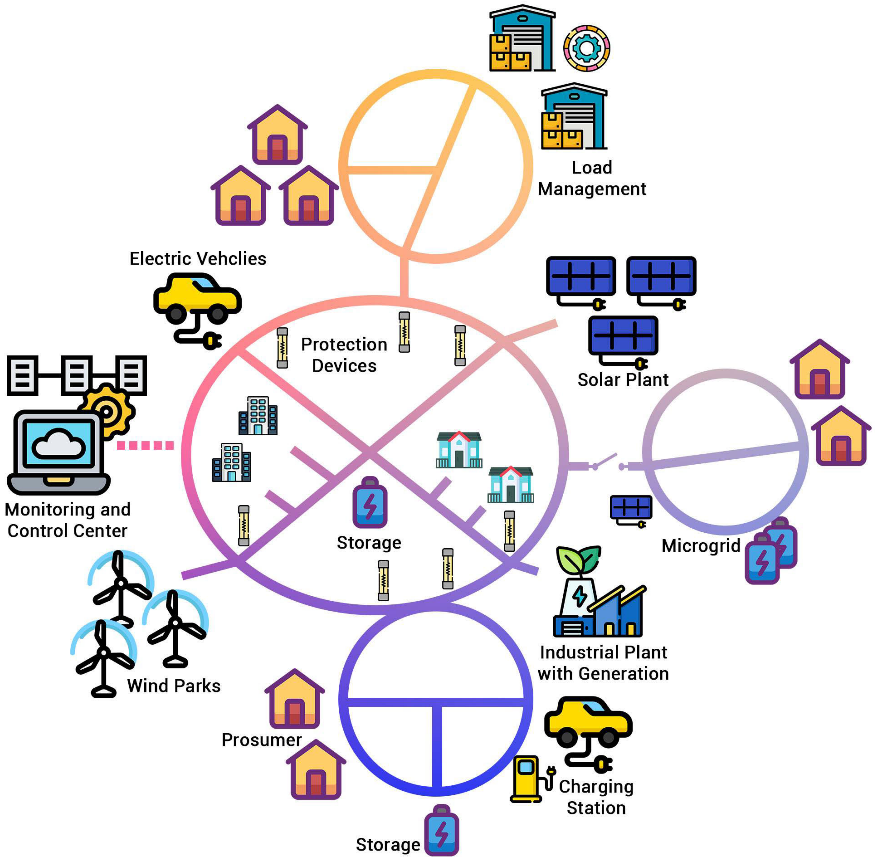

FIGURE 2. Main features of active distribution network [21].

ADN transformations can be categorized into four main areas: critical operations, ADN applications drivers and enablers, devices and sensors, and communication systems as explained below.

A. CRITICAL ADNs OPERATIONS

1) VOLT/VAR CONTROL

VVC is a critical function in ADNs that determines the best set of control actions for voltage regulating devices and Var control devices to manage system-wide voltage levels and reactive power flow for efficient operation [30], [31]. Here, the system operator aims to maintain the voltage level along the feeders within the specified limits at all times. This task is complicated by the increased number of DERs, which significantly alter the voltage profile [30], [31], [32]. The applied VVC strategies can be divided into two main categories: local (autonomous) control, and, communication-based control. The communication-based schemes can be further classified based on the communication architecture employed for control: i) No communication, ii) Centralized, iii) Distributed, or iv) Decentralized. The classification of different control schemes based on communication is depicted in Fig. 3 [33]. First, local control strategies, shown in Fig 3a, solely utilize measurements at the point of common coupling (PCC) without incorporating any other remote measurements on the grid. Local controllers, also referred to as intelligent electronic devices (IEDs), can quickly respond to power generation variability and remain unaffected by communication failures. However, due to the lack of coordination, they may not fully exploit the potential of distributed controllable components, leading to sub-optimal control solutions. In centralized control schemes, illustrated in Fig 3b, the central coordinator is the only network component capable of initiating a control action. The control controller receives the required grid measurements from smart meters and/or remote terminal units, calculates the VVC optimal operation point, and communicates the control command to all IEDs. In distributed control, shown in Fig 3c, all IEDs collaborate to reach a collective decision based on predefined VVC objectives. Communication is limited to neighbouring nodes, eliminating the need for global information about the grid (i.e., the state of all nodes) to determine the control decision. The goal is to establish a self-organized distribution grid that effectively addresses issues through local interactions, offering advantages such as ‘‘plug and play’’ capability. Decentralized control, as seen in

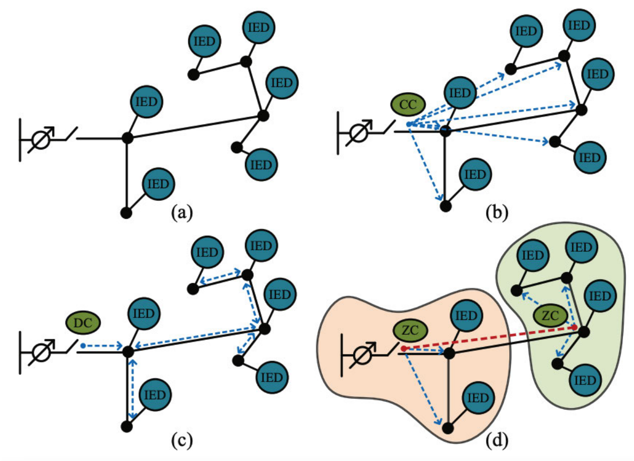

FIGURE 3. Classification of control schemes based on their communication network: (a) no communication, (b) centralized control, (c) distributed control, and (d) decentralized control. Note: CC = central coordinator, DC: distributed coordinator (grid operator interface), and ZC: zone coordinator [33].

Fig 3d, represents an intermediary state between centralized and distributed control. It implies that control is both partly centralized and partly distributed concerning decisions, command/information signals, or computation. These controllers may be loosely coupled for coordination purposes, resembling distributed control, to achieve specific VVC goals. While centralized control can make decision-making more computationally and optimal than local control requiring smaller safety margins for remote measurements, it is dependent on the availability of expansive communication links and does not adapt to changing operation needs [34]. Moreover, the associated central controller (CC), represents a single point of failure if targeted for attack. Multiple authors have addressed the problem of centralized control for DG integration in distribution networks [35], [36], [37]. Mubbashir et al. [35] investigated the potential benefits of demand response under scenarios of large shares of wind penetration. The proposed framework optimized the revenue of the distribution system operator while minimizing energy curtailment and network reinforcements. In [36], coordinated voltage control algorithms are proposed to mitigate voltage rise problems and optimize the usage of DERs. An efficient dispatch of DG output voltages in cooperation with the control of load tap changers and shunt capacitors is proposed in [37].

Distributed control schemes establish communication between each Intelligent Electronic Device (IED) and neighbouring nodes. Distributed control, along with the decentralized counterpart, are largely viewed as superior approaches for modern ADNs due to their distributed intelligence, which enables greater overall response-time, robustness and resilience [38], [39]. While distributed control allows for more efficient DER integration, the benefits of multiple control nodes must be weighed against the increase in system vulnerability stemming from multiple points of decision-making. Further, local voltage control schemes do not require remote measurements as they depend only on measurements at points of common coupling (PCC). Due to their autonomous control structure, these methods require limited coordination and are generally more robust to communication-related challenges [40], [41]. However, they do not achieve optimal performance due to the limited situational awareness at each node compared to centralized approaches [33].

Decentralized control schemes aim to partition the power network into multiple sub-networks (zones), which communicate with each other [42], [43] to achieve VVC in the power networks. This allows for solving the voltage regulation problem in each sub-network area, rendering the overall optimization task easier to tackle. Yu et al. [44] achieved voltage regulation through a distributed algorithm based on the ϵ decomposition of the sensitivity matrix. The control process relies on the communication networks interconnecting the different zones to achieve the optimal DER generation.

2) DISTRIBUTION SYSTEMS STATE ESTIMATION

State Estimation (SE) aims to ensure reliable power system operation by providing an accurate representation of the system states from measurement field devices that inherently exhibit uncertainty and error [45]. Distribution networks are distinct from transmission networks [46] in the following ways. They have: i) system topologies with radial configurations, ii) higher degrees of phase unbalance, iii) high R/X ratio, iv) a larger number of nodes, and v) a lower number of measurement devices.

Consequently, many dedicated research works have developed specific techniques of DSSE tailored to fit the specific needs of ADNs. Figure 4 summarizes the classification of different DSSE algorithms. The first class of DSSE algorithms are based on the Weighted Least Squares (WLS). System states can be voltage nodes [47], [48], or branch currents [49], [50]. Another approach is based on load adjustments, where the modelling of the loads is dependent on the customers' profile curves [51]. Authors in [52] and [53] adopted the iterative Gauss-Seidel load flow algorithm to adjust bus loads. Another category of DSSE focuses on the robustness of the process against any bad data or corrupted measurements. Machine Learning (ML) techniques have been employed in [54] to adjust weights based on confidence in their validity. Authors in [55] utilized the concept of leverage measurements to reduce measurements with high residuals. The modern power distribution systems (PDS) can be divided into zones and sub-networks, and distributed monitoring and control techniques are applied to all the sub-networks. The distributive process reduces the stress on a centralized control center to handle huge amounts of data with accuracy and speed. To that end, algorithms of distributed DSSE have been proposed for multi-area State Estimation [56], [57]. These processes can be done in parallel or in sequence [57]. Another well-known class of DSSE is Dynamic based

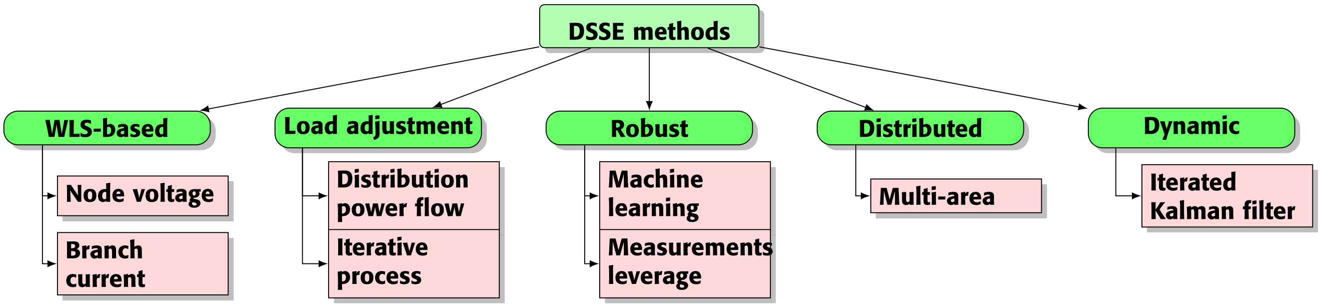

FIGURE 4. A classification of DSSE methods [46].

State Estimation. In this type of DSSE, recursive estimations are based on consecutive snapshot measurements. The most common technique utilized for this approach is the iterated Kalman Filter method [58], [59].

3) DISTRIBUTION SYSTEMS OPTIMAL POWER FLOW

OPF was first introduced by Carpentier in 1962 as an extension to economic load dispatch to minimize the total cost of electricity generation while maintaining the electrical system within the prescribed operation limits [60]. The Distribution Systems Optimal Power Flow (DSOPF) variant is considered to be critical for ADNs as it ensures optimal network operation in terms of power losses, voltage deviations or system costs based on the operators' decisions. Research works typically assume a single-phase model based on the assumption that multi-phase networks can be rendered into an equivalent single-phase network [61].

The complexity of DSOPF arises from the presence of 3-phases and unbalanced radial configuration of the networks and several approaches have aimed to reduce complexity without sacrificing accuracy. Methods typically linearize the constraints, find local optima, or relax generalized constraints into convex versions [62]. The convex relaxation approach guarantees to find only one global optimum. One approach transforms the DSOPF into a convex Semi Definite Programming (SDP) problem. Authors in [63] implemented the SDP approach with a linear approximation of power flow to prove that the former is exact *iff* and the latter is exact as well. This work has been applied to multi-phase radial networks and is applicable to VVC and demand response. The three main concerns in regards to DSOPF convex relaxation are [63]: i) feasibility of global optimal solution through convex relaxation, ii) efficiency of convex relaxation computations, and iii) numerical stability.

B. ADN COMMUNICATION SYSTEMS

The infrastructure necessary to transmit data from one network entity to another has been described through layered models, where each layer groups similar networking functions together independently of the other layers. A layer is characterized by proper control data that is appended to the payload (in the form of a packet header and sometimes a packet tail) to ensure successful and reliable data transmission between the sender and the receiver. The Open Systems Interconnection (OSI) reference model was developed by the International Standards Organization (ISO) and represents an overall communication networking framework used as a basis to define protocols within a layered architecture. The OSI reference model facilitates the design of networked systems enabling communication between a variety of computer systems [64]. A simplified layered model is the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite, which has been widely used since the deployment of the Internet in the 1990s. The roles of each layer and a list of the most commonly used protocols for each layer are summarized in [64].

Operational data in ADNs are communicated from field-level devices to controllers (that are possibly grouped in several hierarchical loops) and eventually to the management and enterprise levels, and vice versa through different communication networks using various protocols. I/O networks link different field devices to controllers. Fieldbus networks are industrial automation Local Area Networks (LANs) used for distributed control over digital two-way multidrop communication links between intelligent field devices such as smart sensors, actuators, transducers and controllers. Fieldbus networks linking field devices to the higher-level control systems have different topologies such as point-to-point, multidrop, tree and daisy chain. Some Fieldbus networks and protocols include HART, Foundation Fieldbus, PROFIBUS, MODBUS, and Distributed Network Protocol (DNP3) [64].

There are several communication options for connectivity between ADNs and smart homes including wireless technologies and home broadband solutions. To manage the connection of a large number of homes, data concentrators are deployed around residential areas to gather all required data at periodic intervals and send them to utilities through line communications [65], as depicted in Fig. 5.

In a smart home setup, various smart meters, including those for electricity, gas, water, and potentially heat, are installed based on the available facilities in each home. These smart meters are interconnected and linked to a metering gateway within the home, which may be integrated into an existing home gateway device. The communication between

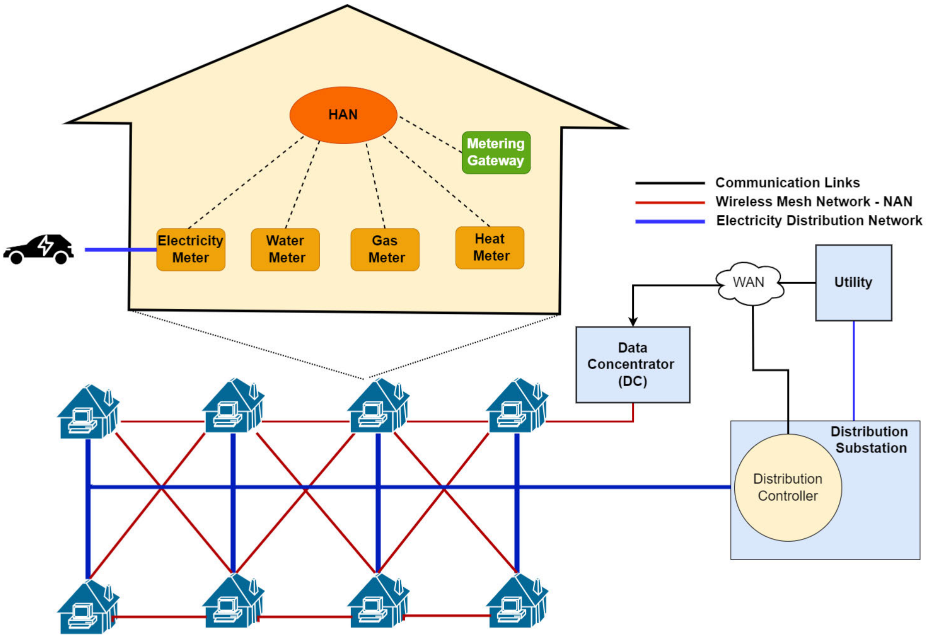

FIGURE 5. Representative ADN communication networks [65].

these meters and the metering gateway occurs through a Home Area Network (HAN), which may adopt multiple standards. This variability is necessary due to diverse meter locations and power availability constraints. For instance, gas and water meters might rely solely on battery power. These multiple HANs are then interconnected to form a Neighborhood Area Network (NAN) through a wireless mesh network. Figure 5 illustrates the connection of the smart metering gateway to both the utility, via a Wide Area Network (WAN), and the distribution control system (DCS). This design accommodates situations where the utility company may not own the DCS, especially in regions with high competition and fragmentation. The utility primarily handles services like billing, service management, and tariffs, while the distribution control system is responsible for tasks such as demand response, issuing commands to disable specific devices or appliances, and integrating renewable energy sources. This separation of responsibilities ensures efficient and specialized management of services in a dynamic and competitive utility landscape.

C. ADN DEVICES AND SENSORS

A smart meter is an advanced measurement device that identifies power consumption in much greater granularity than conventional meters. Smart meters typically communicate collected information back to the utility for load monitoring and billing purposes. Advanced Metering Infrastructure (AMI) represents a backbone designed to measure, collect and analyze energy usage data, including from in-home devices as well as EV charging systems, through automated, two-way communications between smart meters and the power utility via various communication media. This enables consumers, utilities and service providers to participate in scheduled energy management or provide demand/request response solutions, and consequently, control environmental impacts and increase reliability [12], [13], [66], [67], [68].

Smart meters can be collocated and interact with a gateway of a Home-Area Network (HAN) or a business-area network (BAN) [69]. Networking technologies within AMI infrastructure include RF, mesh, WiMax, WiFi, and power line carrier [13]. Meshed or point-to-point architectures with short local coverage or long-range communications are typical [70], [71]. Examples of practical deployments of the AMIs include the Smart Metering and Infrastructure (SMI) program launched by BC Hydro whereby they proposed multi-level common and integrated communication infrastructure to enable grid modernization [12]. In 2007, the ZigBee Alliance (specification for a communication protocol using small low-power digital radios based on the IEEE 802.15.4 standard), was assembled to tackle AMI challenges and develop the ZigBee Smart Energy protocol [67].

The introduction of PMUs in ADNs has enhanced system measurement accuracy through the introduction of high temporal resolution and synchronized measurements. Due to their demonstrated effectiveness and speed in acquiring phasor measurement values (30 to 120 measurements per second), PMUs render conventional measurement devices obsolete and are predicted to eventually replace legacy devices [72].

D. ADN APPLICATION DRIVERS AND ENABLERS

1) MICROGRIDS AND DISTRIBUTED ENERGY RESOURCES

As the number of deployed MGs continues to increase worldwide, their growing diversity in terms of scale, functionality and application is evident. Researchers and industry leaders firmly believe that MGs represent an important pillar for future smart grids and modern distribution networks because they enhance grid resiliency against bulk power disruption and serve as fast recovery resources if a disturbance takes place in the main grid [73]. However, their continuous operation and reliability must be ensured [1], [74].

The high integration of MGs and DERs in power systems has led to a unique set of opportunities, including limiting greenhouse gas (GHG) emissions and improving power quality and reliability. In addition, the diversification of MGs and DERs enhances energy security and supports market competition. However, MG and DER integration has technical, commercial and regulatory challenges [75] discussed in detail in [76]. In addition to these challenges, with the increase in communication-dependent control and protection, CPS of MGs and DERs has arisen to be a primary dilemma in recent years [77], [78]. While a modern MG is typically configured to be resilient to faults and natural disasters, there is always a compelling necessity to secure MGs against adversaries and CPS attacks.

2) ELECTRIC VEHICLES

The two-way flow of information and energy between MGs and electric vehicle supply equipment (EVSE) installed in distribution systems is a key enabler for EV smart charging. Numerous stakeholders are developing charging infrastructures (public charging stations, roadside charging points, battery swapping stations, and on-road induction chargers) to provide smart charging known as Grid-to-Vehicle (G2V) and discharging recognized as Vehicle-to-Grid (V2G) services [79], [80], [81], [82], [83], [84], [85], [86], [87], [88], [89], [90], [91]. ISO, IEC, AUTOSAR have defined standard protocols for EV charging, associated payment systems, and communications to the ADN charging station using the Open Charge Point Protocol (OCPP) protocol for authorization, billing, grid management, and intelligent charging. The standard EV charging protocols and ADN communication are discussed in Section VII-A. These charging infrastructures can significantly impact a distribution system's stability and reliability due to future growth of EVs and the resulting high energy capacity [92], [93], [94], [95], [96]. A Level-1 charging station operates at 120 V, whereas Level-2 operates at 208 V or 240 V, and DC chargers, similar to Level-3 and supercharging, operate at 440 V taking a shorter charge duration [97], [98].

3) IoT AND SMART HOMES

Interconnected ADNs have connected power providers and customers through various communication layers. Consequently, smart homes are rapidly increasing as an important part of ADNs. A key player in this evolution is IoT technology, as it brings significant advantages over traditional telecommunications for ADNs and smart home applications including real-time monitoring, situational awareness and intelligence, control and CPS [99]. However, IoT is extremely vulnerable to cyber-attacks because of the way in which data is transmitted [100], [101].

III. CYBERSECURITY CHALLENGES, THREATS AND REQUIREMENTS IN ADNs

The evolution of ADNs and, consequently, its cyber-attack surface, necessitate a comprehensive analysis of its CPS requirements. Two main CPS aspects drive this urgent need to better understand the resulting challenges and threats. First, typical ADN applications rely on the use of heterogeneous wired and/or wireless communication networks that are possibly managed and controlled by different entities (e.g. electric power utilities, public telecommunications service providers, and consumers) and that employ distinct protocols each of which has its own security challenges. Second, ADN infrastructures are often spread over large geographical areas, thus, yielding complex communication network interconnectedness for which comprehensive situationally aware cybersecurity controls are still lacking. Third, the proliferation of consumer-related applications that require interactions with utility-owned systems, such as those used for EV charging and demand-side management programs, provides growing opportunities for intruders to leverage vulnerabilities in consumer-based tools to perpetrate attacks with direct impact on the power distribution and transmission infrastructures.

The first part of this section presents the main CPS threats and challenges and categorizes the different types of CPS attacks and their impacts in the ADNs operation context. Subsequently, the second part of the section presents the main CPS data security requirements in ADNs required to overcome the above-mentioned challenges and challenges.

A. CYBER-PHYSICAL THREATS AND CHALLENGES

We briefly review how distribution network modernization creates new CPS risks. In the general context of power grids, Operational Technologies (OT) consists of the components and mechanisms used to monitor and control electricity generation, transmission and distribution. These systems belong to a more general category of Industrial Control Systems (ICS) which are used in a variety of industries and have been evolving through the integration of Information and Communication Technologies (IT). The greater dependence of ADNs on IT makes them vulnerable to a myriad of attacks at both the physical and cyber levels [67], [68], [102]. Examples of vulnerabilities stemming from ADN modernization are provided in Table 1.

In 2013, The MITRE Corporation initiated a program entitled ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) [103]. ATT&CK® aimed to document common Tactics, Techniques, and Procedures (TTPs) that advanced persistent threats used against ICSs including those used in power systems. A vulnerability or weakness in a system, device, hardware or software component can be

TABLE 1. ADNs CPS risks stemming from grid modernization.

Conventional distribution networks	ADNs	Potential vulnerabilities
Unidirectional flow	Bidirectional power flow	Data integrity attacks on VVC [105], [106]
Centralized control	Sophisticated and distributed control	Intrusion attacks on ADNs with DERs [107], [108]
Non-existing distributed generation	Large share of DERs and microgrids	Attacks on microgrid control systems [19], [109]
Minimum level of communication	Multiple communication layers	Failure of physical and network layers [12], [110]
Local measurements units	Smart sensors	Attacks on PMUs [111], [112]

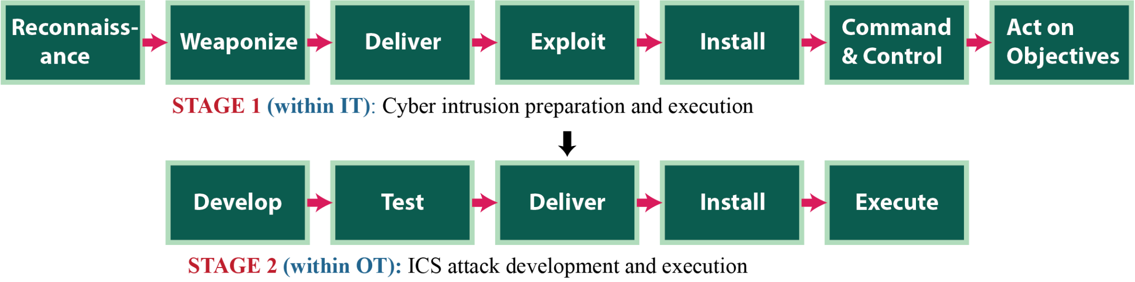
Reconnaiss-ance
Weaponize
Deliver
Exploit
Install
Command & Control
Act on Objectives
STAGE 1 (within IT): Cyber intrusion preparation and execution
Develop
Test
Deliver
Install
Execute
STAGE 2 (within OT): ICS attack development and execution

FIGURE 6. Exaggerated kill chain model for industrial control systems [113].

intentionally (through malicious intrusions) or unintentionally (through human error) exploited to negatively impact its own operations or the operations of the environment in which it is deployed. Typically, such unwanted effects translate to compromised security objectives. Using several sources, the NISTIR 7628 report [104] presents a list of vulnerabilities that can be incorporated for detailed risk analysis of actual or proposed power grid systems. Such vulnerabilities include weaknesses in software/firmware, software and hardware platforms, communication networks, policies, procedures and people.

To represent the different stages that attackers follow to perpetrate a cyber-attack, researchers from Lockheed Martin Corporation have introduced in [114] a model for the systematic process to target and engage an adversary to create the desired effect. Known as the kill chain, this process consists of seven phases and it is appropriate to depict the attacker progression in targeted IT environments. These phases can be defined as 1) Reconnaissance: involves research, identification, and the selection of the target for the attack, 2) Weaponization: the process of coupling a remote access Trojan with an exploit to create a deliverable payload, typically facilitated by an automated tool known as a weaponizer, 3) Delivery: encompasses the transmission of the weapon to the designated environment targeted by the attack, 4) Exploitation: involves triggering the intruder's code to exploit vulnerabilities in an application or operating system. This stage may also exploit users directly or leverage features of the operating system, 5) Installation: focuses on maintaining persistence within the targeted environment through the installation of a remote access Trojan or backdoor on the victim system, 6) Command and Control: this entails establishing an outbound connection to the intruders' server, providing them with "hands on the keyboard" access inside the targeted environment, and 7) Actions on Objectives: involves executing the attack by violating data integrity or availability, moving from the targeted system to potential targets within the network, or conducting data exfiltration. Data exfiltration includes the processes of collecting, encrypting, and extracting information from the targeted system. Authors in [113] built upon the kill chain model of [114] and present an "exaggerated kill chain" model, shown in Fig. 6, that is more appropriate for the characterization of ICS cyber-attacks and attacks that target OT environments. In contrast to attacks stemming from conventional IT network breaches, cyberattacks on ICS demand intruders to possess in-depth knowledge of the specific processes being automated, as well as a comprehensive understanding of the engineering decisions and design principles governing the targeted ICS systems. This heightened level of knowledge empowers intruders to impose substantial impacts on processes or equipment, enabling the execution of a genuine cyber-physical attack. This stands in contrast to attacks that may be categorized as espionage, ICS disruption, or intellectual property theft. A cyber-attack is averted or stopped by breaking the kill chain at any phase preceding the last execution phase. If the attacker's actions remain undetected and successfully reach the attack execution phase, the system defender's actions would be limited to restricting the attack damages and initiating an efficient incident response.

Different threats and cyber-attacks can be launched against ADNs according to the access and knowledge levels of the attacker. The most common types of attacks are man-in-the-middle, Denial-of-Service (DoS), FDI, and rogue device attacks. These attacks can be summarized as follows:

- *MitM attacks:* By getting access to a communication channel between two communicating entities, an adversary infiltrates the communication flow and impersonates the two communicating nodes, thus, compromising the availability and integrity of power system data. The conditions and impacts of such attacks are presented in [115]. Another example of Man-in-the-Middle (MitM) attack, labelled data framing attack, is proposed in [116].

- *The replay attack:* This attack does not require the attacker to have detailed knowledge about the targeted system since it consists of recording and replaying the communications between the network entities. The replayed packets can be possibly altered by the attacker before being replayed, and they might lead the receiving entity into an erroneous behaviour [117], [118].
- *Denial of Service (DoS):* DoS attacks target the availability security objective, by exhausting device resources or attempting to corrupt, delay or block critical communication links by flooding the communication with a bogus traffic [119], [120]. Different communication layers in the power systems can be targeted by DoS attacks [68]: (i) Channel Jamming can occur on the Physical layer, with effects ranging from delayed delivery of messages to complete denial of service [121], (ii) Media Access Control (MAC) layer attacks, as attackers can modify MAC parameters, and result in a spoofing attack and (iii) targeted DoS attacks on the network and transport layers which can severely affect the performance of end-to-end communication. Furthermore, real hardware and software vulnerabilities that can be exploited to launch DoS attacks have been investigated in [122]. More detailed classifications of DoS attacks against CPS are presented in [123] and [124].

  DoS attacks can be considered to compromise both the availability and integrity of of ADN services and the scale of such attacks can range from low to high. Spatially, DoS attacks can target different segments of ADNs including control centers, distribution substations, metering and protection devices and EVs charging/discharging infrastructure. Further, a DoS attack may target vulnerabilities in commonly used communications protocols in ADNs such as IEC 61850, ANSI C12.22/IEEE 1703, IEEE C37.118 and DNP3. DoS attacks in communication systems can originate anywhere between the physical and data link layers and also other communication layers such as the network, transport, and application layers [123]. Moreover, DoS can target major ADNs applications including AMIs, DSSE, OPF and demand side management. In the following sections, we visit in detail the effect of DoS and other attacks on these applications.
- *False Data Injection (FDI):* The FDI attacks result from injecting (corrupting) measurement data and/or control commands, with the goal of initiating incorrect control actions. A well-known FDI model, first introduced by Liu et al. [125], targets measurements used by the Power Systems State Estimation (PSSE) process and constructs attack vectors to bypass Bad Data Detection (BDD). Several assumptions, conditions and scenarios have been studied to launch successful attacks such as the usage of AC power flow model [126], [127], [128], attacks on PDS [24], attacks with incomplete information [129], and attacks targeting electricity markets [130]. Potential attack detection and mitigation techniques have been investigated in [131], [132], and [133].
- *Session hijacking*: This attack corresponds to the situation where an intruder takes over a valid communication session by taking control of the authorized node that has set up this session. The attacker would then use the hijacked session for unauthorized communications with the victim [117].
- *Address Resolution Protocol (ARP) spoofing:* The ARP is used to provide the mapping between the network layer (using Internet Protocol, IP, addresses) and the data link layer (using MAC addresses). Networked systems keep an ARP lookup table where they store the IP address - MAC address associations. When trying to send a packet with a destination IP address, the system first consults its ARP table to find the destination MAC address. If this address is found then ARP is not used, otherwise, a broadcast message is sent over the network using the ARP protocol and the machine with the requested IP address will respond with its MAC address (yielding an update of the sending host ARP table). An ARP spoofing attack corresponds to the situation where attackers send falsified ARP messages linking their MAC address with the IP address of a legitimate node on the network and causing an intentional alteration of the IP address - MAC addresses mappings. Once the attacker's MAC address is mapped to an authentic IP address, the attacker will begin receiving any data packets intended for this IP address. This attack can be used for eavesdropping, alteration of data packets or DoS attacks [117].
- *MAC flooding:* Communication network switches rely on a structure called Content Addressable Memory (CAM) to make message-forwarding decisions. Typically, for Layer 2 switching, the entries of this table are built by recording the source MAC address, the switch inbound port number, the virtual LAN (VLAN) and the frame arrival timestamp for all received frames. The CAM table entries are dynamically updated according to the most recent frame arrivals. For Layer 2 switching, when a frame arrives at the switch with a destination MAC address that is stored in the CAM, the frame is only forwarded through the port that is associated with the specific MAC address. If the switch does not find

an exact match to the destination MAC address, then the frame is flooded out on all VLAN ports. The aim of a MAC flooding attack is to take down the CAM table by flooding the switch with a large number of frames that have various source MAC addresses, thus, causing the CAM to run out of space and becoming unable to store new mappings. This leads the CAM entries associated with legitimate network nodes to be pushed out and all the frames received at the switch to be broadcast on all ports. Similar to ARP spoofing attacks, this attack can be used for the alteration of data packets, data gathering and launching more sophisticated attacks such as MitM, session hijacking or DoS attacks [117].

- *Supply Chain Attack:* The proliferation of cyber-attacks against critical infrastructures including power grids is expected over the next few years along with an increasing level of sophistication and impact. Driven by a quest for monetary gain or geopolitical objectives, attackers are leveraging new and complex attack vectors to perpetrate large-scale attacks that can inflict significant damage. Such a trend has been confirmed following the SolarWinds supply chain attack in 2020 [134], [135], [136] that led to the compromise of thousands of systems owned by industrial entities worldwide and several government agencies, and the Colonial Pipeline ransomware attack in 2021 that disrupted fuel supplies across the United States.

Within ADN environments, it is important to note that the exhaustion of IT or OT (such as Supervisory Control and Data Acquisition (SCADA)) resources can lead to DoS attacks. Further classes of cyber-attack can be cited. For example, a delay attack refers to a malicious situation where data communication between two entities is purposely delayed by an intruder in order to lead a receiving entity into erroneous behaviour. Attacks on time synchronization systems (such as Global Positioning System (GPS) spoofing or jamming) in critical infrastructures can inflict significant and large-scale damages resulting in, for instance, untimely decisions made by controllers based on false measurement timestamps. Note that the characteristics of data communication protocols (such as the lack of data encryption in operational environments) can be exploited by intruders to perpetrate and/or amplify their attacks. Finally, sophisticated intruders can resort to a combination of several types of cyber-attacks in order to inflict significant and simultaneous damages in different parts of the targeted systems. Examples of such sophisticated attacks include blended attacks [31] where elements of multiple types of malware are combined and multiple attack vectors are exploited to increase the severity of damage and the speed of contagion. Blended threats have recently increased in complexity using (as in the case of the Stuxnet attack) a single and mutating malware framework capable of behaving in multiple ways depending on the targeted environment.

B. DATA SECURITY REQUIREMENTS

Communication systems are critical components of ADNs, as such, it is important to include data security as part of a comprehensive strategy to protect modern distribution systems. There are different technical and regulatory challenges for the security in modern distribution systems [137], [138] including 1) the complexity and scale of future power distribution systems, 2) traditional communication vulnerabilities, 3) emerging communication requirements due to the deployment of new infrastructures such as EVs and DERs, 4) the need for trustworthy communications between all participants (user, protocol, devices, etc.), 5) the dependence on legacy devices, 6) the use of heterogeneous technologies and protocols, 7) the use of proprietary systems, and 8) user privacy.

To overcome these challenges, several security properties are required by the power distribution systems i.e., availability, confidentiality, integrity, authentication, authorization, freshness, efficiency, privacy, scalability, adaptability, and evolvability and authenticity [12], [68], [69], [70], [137], [139], [140], [141], [142], [143], [144], [145], [146]. Among these requirements, availability, confidentiality, and integrity are the most significant and are defined as follows:

- **Availability:** systems and data must be available to authorized parties when there is a need without security compromise [143], [144], [145], [146]. This ensures network resources (e.g., data, bandwidth, equipment, servers) are always available at all nodes for legitimate use [68], [139], [142]. The importance of data availability stems from the essential role information systems and communication networks (cyber) play in the management of the continuous power flow (physical) in power grids. Thus, data shortages/delays or communication link disruptions may drive power system operations to make incorrect or untimely decisions.
- **Confidentiality:** data is disclosed only to authorized individuals or systems [68], [142], [143], [144], [145], [146]. Critical power system distribution data (e.g., from (smart) meters) should be confidential. Meter data can be highly sensitive due to the ability to glean personal information and activities from energy usage information. For this purpose, the meter data should be protected such that only intended parties can access it. Pricing information and control commands are not critical if they are public knowledge [69].
- **Integrity:** provides assurance that the accuracy and consistency of data are maintained. No unauthorized modifications, destruction or losses of data go without being detected [68], [139], [142], [143], [144], [145], [146]. The integrity of pricing information, system measurements, meter data, control commands, and software used in power system substations is critical. For instance, negative prices injected by an attacker can cause an electricity utilization spike as numerous devices would simultaneously turn on to take advantage of the ‘‘low’’ price. The impact of attacking the integrity

TABLE 2. Classification of cyber-physical attacks types, targets, and defense strategies.

Attack	Cyber	Physical	Attack target	Defense strategy
Man-in-the-Middle	✓		Confidentiality	Subset meters protection [115]
Denial of Service (DoS)	✓	✓	Availability	Detection [121], encryption & authentication [147]
False Data Injection (FDI)	✓		Integrity	Anamolies detection [148], [149]
Session Hijacking	✓		Integrity, Confidentiality	Network defence in depth strategies [117]
Address Resolution Protocol (ARP) spoofing	✓		Integrity, Confidentiality	Security patches and intrusion detection [117]
MAC Flooding	✓		Integrity, Availability	Distributed resilient control methods [150], [151]

of meter data and control commands is largely limited to revenue loss. However, the integrity of the software is crucial since compromised software or malware can control a set of devices and components in the power system [69].

Table 2 classifies the different attack models that threaten distribution networks [67], [102], security requirements targets, and defense mechanisms against these attacks.

C. COMMUNICATION NETWORK SECURITY REQUIREMENTS

The first line of defence for power grids is compliance with security standards and regulations. Several regulations and protocols requirements are being issued by Institute of Electrical and Electronics Engineers (IEEE), National Renewable Energy Laboratory (NREL), North American Electric Reliability Corporation (NERC), International Electrotechnical Commission (IEC) (e.g. IEC 62351 and IEC 62443 standard series) and the National Institute of Standards and Technology (NIST) to meet the security requirements of Smart Grids. Smart grid communication protocols, standards and requirements are surveyed recently in [152] and [153]. With a focus on cybersecurity issues, Leszczyna reviewed them in [154]. A few papers also focused on the distribution networks from the communication point of view [66], [67], [102], [120]. In this section, we highlight the latest requirements, standards and protocols concerning communication in ADNs to be used for a secure network.

Different categories of standards have been developed to tackle different aspects regarding the security of ADNs. The IEC 62351 standards have been developed by Working Group 15 (WG15) of IEC's Technical Committee (TC) 57 and consider various aspects of cybersecurity for the communication protocols developed by this committee. As such, the recommendations of these standards tackle several elements in the converged IT and OT power grid environment [155], [156], [157], [158], [159], [160], [161], [162], [163], [164]. Another relevant family of standards for the cybersecurity of Industrial Automation and Control Systems (IACS) is the IEC 62443 standard series which relies essentially on the fundamental concepts included in the ANSI/ISA-62443 (formerly ISA-99) reports, created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) [165], [166], [167], [168], [169]. Some IEEE standards drafted by the Power and Energy Society of the IEEE also address smart grid cybersecurity such as [170] and [171]. The NISTIR 7628 [104] is addressed to utilities, equipment manufacturers, system operators, regulators, researchers and network specialists, providing guidelines that incorporate the perspectives of the information technology industry, the telecommunications sector and the electric power industry. In this report, smart grid vulnerabilities have been defined in four categories including 1) people, policy and procedure (this is where training and operator awareness get into the picture), 2) platform software/firmware vulnerabilities, 3) Platform vulnerabilities, and 4) network vulnerabilities. The vulnerability classification therein, including communication network and protocol vulnerabilities, can be used by utility operators to conduct advanced risk assessment studies that would be necessary for security professionals to design more resilient ADN.

IV. CYBER-PHYSICAL SECURITY OF DEVICES AND SENSORS IN ADNs

The advancement in measuring devices and smart sensors has played a major role in accelerating the ADNs development, from both the utility side and customer side. In this section, we review the latest trends, security capabilities, and applications of devices needed for control, monitoring, and protection such as PMUs, AMI, and protection relays. We specifically focus on their CPS applications.

A. PHASOR MEASUREMENT UNITS (PMUs)

Despite the PMUs' enhanced capabilities in monitoring power systems states, they remain vulnerable to a number of cyber-physical attacks [25], [111]. A variety of cyber-attacks can be launched against PMUs including packet injection (FDI), time synchronization attacks (TSAs), and DoS attacks [147]. Authors in [111] prove that undetectable time synchronization attacks (TSAs) can be launched against PMUs by satisfying the constraints imposed by the PMU clock servo. In addition, it is shown that the attacks bypass robust DSSE as well. In [25], authors investigate resilient three-phase DSSE approaches against TSAs in unbalanced distribution networks. In addition, although time-stamped measurements are one of the most important functionalities that PMUs provide, the feasibility of time synchronization and spoofing attacks on the GPS receiver clock of PMUs have been demonstrated in [111], [172], and [112]. An overview of cyber-security threats against PMUs and the impacts of FDI attacks are presented in [147].

In order to maintain network observability, Mousavian et al. adopted a probabilistic approach to limit the spread of a cyber-attack from compromised PMUs [173]. The approach is based on calculating the threat level of cyber-attack propagation to intact PMUs and developing an optimal response model for the operator to minimize the threat level and thus reduce the attack severity. The authors assume that after detecting that a subset of PMUs are compromised, there is a probability that the attack has spread to other PMUs given by

$$\Pr(A_j(\Delta t) = 1) = 1 - \prod_{i \in \Gamma} (1 - \alpha_{ij}) \quad \forall j \notin \Gamma \tag{1}$$

where $A_j(t)$ is a random variable set to 1 if PMU$_j$ is attacked and 0 otherwise, (Δt) is time passed after initial detection of an attack, α_{ij} is the probability that the attack propagates from compromised PMU$_i$ to uncompromised PMU$_j$ during time Δt, and Γ is the set of PMUs detected as compromised. The response model is obtained by minimizing the maximum threat of all devices within the network at time $(m+2)\Delta t$:

$$Z = \min_{\mathbf{x}} \max_{j} (\theta_j)((m+2)\Delta t \times x_j) \quad \forall j \notin \Gamma \tag{2}$$

where Z is the objective function of the response model, x_j is the binary decision variable which equals 1 if PMU$_j$ is connected and 0 otherwise, and $m\Delta t$ is assumed the time required by the operator to conclude a false alarm. Experimental results on the 6-bus and 24-bus systems reveal that the response model successfully limits the propagation of cyber-attacks [173]. An assumption is made that cyber-attacks are single occurrences and not compounded, due to the exceeding high complexity of analyzing multiple successive attacks.

B. SMART METERS AND ADVANCED METERING INFRASTRUCTURE (AMI)

The AMI presents numerous benefits to several smart grid applications, as presented in Section II-C. These benefits include the improvement of power quality, asset management, online meter reading and control, and customer satisfaction [12], [174]. However, these benefits are countered by increasing CPS issues in the distribution system [175], [176], [177], [178]. AMIs require a communication infrastructure to provide interconnectivity. Hence, the vulnerabilities that expose other inter-networking systems will lead to security threats to AMI systems with high probability [12]. For instance, in the case of AMI deployment for demand side management, demand side management introduces a cyber-physical interconnection between the smart meters (cyber layer) and power provided to consumers [179]. A meter data management system (MDMS) lies under utility control to control the meter's configuration, connects to an AMI device which forwards commands, and aggregates data collected from the meters throughout the infrastructure [13].

Energy theft is one of the serious concerns related to the non-technical losses (NTL) in distribution systems which account for 10%-40% of energy distribution. According to to [180], NTL changes slightly based on the topology of the secondary electricity distribution system. The authors of [181] proposed a methodology to estimate the losses due to thefts and frauds in distribution systems. Overall, the financial loss of utility companies due to energy theft around the world is estimated to be more than $25 billion every year [182]. In the USA, the amount of stolen electricity accounts up to over 1 TWh, which causes 0.5%-3.5% loss in the annual gross revenues of utility companies, e.g., as high as $1.6 billion [183], [184], [185], [186].

The power usage at each endpoint of the distribution network is recorded and sent to the remote utility by smart meters which are equipped at each of these points. Due to some technical vulnerabilities, these smart meters can be attacked by malicious users who attempt to cut their electricity bills in an illegal way. To overcome this problem, feeder remote terminal units (FRTUs) have been applied in distribution automation. It is not only been used for fault detection, prediction, isolation, and service restoration but it is also being used to detect energy theft by narrowing the search zone for an attacked smart meter. FRTUs monitor the downstream electricity and send the readings to the control center over wireless communication. The central billing center compares the reading of the FRTU with the summation of the readings of the smart meters in the downstream network of that FRTU. If the smart meters are not sending out the actual energy usage readings, the comparison will show a significant discrepancy. This means that the smart meters downstream of the FRTU are attacked. Hence, only the smart meters downstream of the FRTU need to be checked instead of all smart meters in the distribution network. However, due to the high cost of FRTUs, utility companies can only afford to insert the minimum possible number of them. This creates challenges to deploy the minimum number of FRTUs while each smart meter is still effectively monitored [184], [187].

Energy theft detection schemes have been categorized into two main categories in [188] including classification-based and state-based. The authors in [182] added a third category i.e., game theory-based detection schemes. However, the first two types of schemes are the most commonly used. Classification-based schemes use the average electricity consumption of a customer to detect abnormal energy usage patterns. State estimation-based schemes utilize the fact that wireless sensor networks are cheap and not complicated in the implementation, and use these advantages to construct a monitoring stat to improve the detection rate of energy theft. Game theory-based schemes provide a new perspective to detect energy theft. Table 3 classifies the schemes mentioned in the literature according to the aforementioned criteria. Selected schemes are highlighted in the following few paragraphs.

The authors of [187] proposed a technique based on historical data to detect the anomaly in the load profile of the consumers of the user level or the secondary distribution system. The proposed technique used a limited number of

TABLE 3. **Classification of energy theft detection.**

Detection approach	References
Classification based	[182], [189]–[195]
State based	[183], [186], [196]–[199]
Game theory based	[200], [201]

FRTUs to match a specific low budget. Since this algorithm is based on historical data, it has the disadvantages of being inherent heuristic and non-deterministic in nature which does not guarantee the quality of the solution. In addition, it may fail with large distribution networks due to the scalability issue. Therefore, the authors of [184] proposed an improved version of the algorithm that enabled them to get a better performance with an 18.8% reduction in the number of FRTUs compared to the original. The latter work used the minimum possible number of the FRTUs, and distributed them in the distribution network based on the attack probability of each smart meter in the distribution network i.e., more FRTUs in the areas where the smart meters are frequently attacked. Then, the algorithm evaluates every candidate solution in a bottom-up fashion using a pruning technique.

Different approaches that use consumption patterns were proposed. An online approach that identifies malicious consumers and their locations based on the consumption pattern is proposed in [185]. Recently, another approach is proposed in [194] to compare the total amount of usage reported by the smart meters with the total consumption of each neighbourhood which is measured by transformer meters. If at this level NTL is detected, the area with abnormal patterns will be selected as a suspicious area. For each customer in the suspicious area, a multi-class support vector machine (SVM) is trained using the historic data of the user as well as a synthetic attack dataset. A classifier is then used to decide whether a new sample is normal or malicious. A basic scanning method, called the Brute-Force strategy, is used in [186] to inspect malicious meters. Due to the limitations of this method when the malicious meter ratio is low, the authors combined it with a proposed adaptive-tree-based inspection approach, which performs better than scanning in this situation. Finally, based on the results, the authors recommended the adaptive tree approach as a decent choice in general circumstances. Leite *et al.* proposed a cost-effective approach to detect non-technical losses by comparing data from the grid domain and the customer domain [202]. The methodology is based on the statistical selection of reliable measurements from field devices and PMUs to look for any mismatch. With some assumptions made about the reliability of the real-time state estimation, results proved the efficiency in attacks-detection.

C. PROTECTION RELAYS AND RECLOSERS

The dominance of ADNs requires a flexible protection system that includes devices capable of adapting their settings following any changes in the system. Communication technologies play a crucial role in this system where these protection devices need to be coordinated. Authors in [203] and [204] have recently reviewed the state-of-the-art on adaptive protection techniques that are based on communications in distribution systems and microgrids. The issues concerning the security of protective relays in distribution substations and communication paths between different locations are also covered in the report [205] published by The IEEE PES Power System Relaying Committee Working Group C1. The following is a summary of the issues/ recommendations:

- The protection engineer is the only person who has the right to access relay settings and documentation. A second secure level is reserved for relay engineers and test technicians to change settings. Testing contractors may use temporary passwords to do specific changes and settings. Others can be allowed to have view-only users' passwords.
- A relay re-commissioning after any settings change must include a careful review of the impact on all devices due to the change of communication and security settings.
- The communication media (routes) which are used to access a device in a substation include 1) typical point-to-point communication (plain old telephone lines, leased line for SCADA systems, wireless via mobile and 900 MHz radio waves), 2) Microwave and 3) T1, SONET and Ethernet.
- Directional comparison is the most widely used pilot scheme because of its low channel requirements. Another popular pilot scheme is the current differential system which compares the magnitude and/or phase of the current from all terminals. This later type has higher channel requirements. Attacks which can be done to pilot relaying are DoS and MitM.
- Examples of the possible physical threats are mentioned as well as examples of possible threats to inadvertent compromise of an IED or automation system. Some of the threats may be caused by inadvertent actions by authorized employees or malicious actions of both authorized and unauthorized people. Examples of threat sources are mentioned.
- Vulnerabilities are categorized into groups i.e., software security, network security, system administration, personnel-related, and miscellaneous and unusual vulnerabilities. Examples of each category were included.
- Market and complexity of operations of power systems are two forces that give high importance to the security of communication protocols.
- An intrusion detection system (IDS) must look at both internal and external intrusions as studies show that up to 70% of attacks are internally initiated. The IDS may shut down the communication link or send any alarm referring to a potential attack to the responsible personnel for intrusion detection, and not to SCADA operators.

The issue of cybersecurity of protection schemes can be viewed as a significant drawback in most adaptive protection proposals. Addressing this concern, Habib et al. [19] conducted a study on the ramifications of communication failures on adaptive microgrid (MG) protection schemes. The study highlighted, for instance, that in the event of communication failure, relay settings remain unchanged, leading to the ineffective implementation of any adaptive protection scheme. The authors also illustrated various types of cyberattacks that could impact adaptive protection schemes. For instance, an attacker might inject malicious code into an IED and inject oversized data to induce a buffer overflow. In another scenario, the attacker could intercept and retain Generic Object-Oriented Substation Events (GOOSE) messages, subsequently triggering a message to trip a circuit breaker during normal operation, resulting in an undesirable outcome.

Hansen et al. [206] documented a real cyberattack case in 2015 when a Russian hacker group targeted the Ukrainian power grid. The hackers installed malicious malware in the computers of 3 distribution companies. This malware allowed them to remotely manipulate substation breakers, leading to a blackout that impacted over 225,000 customers. Regrettably, such attacks are feasible due to vulnerabilities in IEDs and communication networks. A CIGRE publication [207] underscores that IEDs, particularly those based on IEC 61850, face similar threats as other industrial distributed control systems using TCP/IP/Ethernet protocols. Various suggestions to mitigate these issues are presented in references [19] and [208].

Several research works have been recently proposed to study and address these different security issues in the protection schemes/devices of ADNs [77]. Liu et. al. in [209] studied the risk associated with malicious attacks on the settings and parameters of the bus and transmission line protection systems located in a substation. Cyber-physical attacks targeting communication-assisted protection schemes are studied in [210]. The authors showed that cyber attackers can jeopardize transient angle stability by targeting such protection schemes. To overcome this problem, [210] considered the redundancy in communication channels and used more advanced protection schemes that take into consideration the loss of communication channels. Machine learning techniques are also used in [211] and [212] to detect cyber-attacks against the differential relays in power substations. Despite the efforts of these researchers, the challenges mentioned persist in implementing a dependable adaptive protection scheme and should be the focus of future studies.

To conclude this section, it can be seen that the advancements in sensor technologies make it easier to monitor the ADNs and accordingly issue protection and control orders. It also facilitates a large variety of applications in the ADNs. However, it increased the vulnerabilities of the ADNs to different kinds of cyberattacks. Given these vulnerabilities, the following sections shed light on the cybersecurity aspects of the critical operations in the ADNs as well as the most immerging application drivers and enablers in modern ADNs including MGs, EVs and IoT-based smart homes. The efforts that have been made to address the CPS of these applications are also reviewed.

V. CYBER-PHYSICAL SECURITY OF CRITICAL OPERATIONS IN ADNs

In this section, we formulate cyber-attacks against these integral operations and discuss state-of-the-art techniques and approaches to identify threats, detect attacks and mitigate the possible effects of these attacks. The flow of this section is based on the classification of the main operations in ADNs identified in Section II, e.g. VVC, DSSE and DSOPF.

A. VOLT-VAR CONTROL (VVC)

Isozaki et al. [213] investigated the impact of cyber-attacks on voltage regulation in distribution systems, in the presence of Photovoltaic (PV) systems and the usage of communication-based sensors. The authors demonstrate that voltage regulations can occur if measurements are subject to FDI attacks, and a detection algorithm is presented to limit the damage of attacks, especially in the case of the limited number of attacked sensors. The attacker falsifies measurement data to cause irregular tap changes in the load ratio control transformers (LRTs), thus causing voltage violations at feeder nodes. Two possible attack scenarios are considered: Suppressing tap changes at the LRT or Inducing tap changes at the LRT. Both scenarios may lead to under-voltage/over-voltage at some nodes, based on the load profile at each node. In order to achieve the most efficient attack, the attacker's aim is to maximize the voltage variation, constrained by lower and upper limits of voltage values. The proposed algorithm is composed of four steps [213]:

1) Checking whether a measurement value V_i falls within the admissible range of upper and lower limit values for voltage at node i.
2) Checking of nodes voltage order. In the case of no power injections through PVs, then node voltage values are smaller than those upstream. This step is ignored in the presence of operating PVs.
3) Checking voltage Variation rate. If a tap change did not occur in the previous time step $(k-1)$, then the difference, at node i, between $V_i(k)$ and $V_i(k-1)$ is lower than a time-varying upper bound.
4) Checking lower bound on voltage differences, which is achieved by checking that the difference between the maximum and minimum voltage values at a given node is bigger than a time-varying lower bound.

The results show that falsification of measurements can be detected in the case of a limited number of attacked nodes, while voltage violation can result due to a larger number of attacks. Also, attacks that target PV output power have been investigated. Teixeira et al. [106] addressed stealthy attacks that target integrated VVC measurements. Considering $\mathbb{C}_{\mathbb{F}}$, a subset of capacitor bank configuration $\mathbb{C}$ that satisfy all operational constraints in system state $\mathbf{x}$, the optimal configuration for cost minimization is found as:

$$C(\mathbf{x}) = \underset{C \in \mathbb{C}_{\mathbb{F}}(\mathbf{x})}{\arg\min} \; V(\mathbf{x}, C) \tag{3}$$

The attacker's objective is to maximize adverse impact without being detected. Therefore, under the assumption of access only to voltage measurements, a $\mathbb{C}_k$ stealth attacks can be defined as [106]: an attack vector $\mathbf{a}$ is a $\mathbb{C}_k$ stealthy attack *iff* there exists $\Delta\mathbf{y} \in \mathbb{C}^n$ such that

$$\begin{cases} \mathbf{a} = H_v(C_k)\Delta\mathbf{y} \\ 0 = H_S(C_k)\Delta\mathbf{y}. \end{cases} \tag{4}$$

where H_v and H_S are matrices derived from system topology. Moreover, the authors present a game-theoretic framework to limit the adversary action space. The operator strategically bases countermeasures to detect and mitigate possible action strategies adopted by the adversary. Results reveal damages that occur from data manipulation while the operator continues to apply normal system configuration. The VVC was evaluated on the IEEE-13 node feeder, using the GridLab-D [214] software. For a stealthy attack of adding and subtracting 50 volts at two distinct nodes, respectively, the VVC was able to bring the voltages from 2450 volts to 2350 volts, although the actual desired level is 2300 volts.

B. DISTRIBUTION SYSTEM STATE ESTIMATION (DSSE)

Majumdar et al. investigated malicious attacks that target the DSSE and affect the operation of VVC optimization, and they presented two approaches to mitigate the attack effects [215]. The first solution depends on the local controller set-point, where it proposes the usage of DERs power generation instead of attacked measurements. The second solution is to use the historical data to build a density function of the attacked state. Deng et al. incorporated FDI in DSSE [24]. Although multiple FDI attacks schemes have been proposed and analyzed on several occasions [126], [216], [217], the FDI was based on an attack model that assumes a strong condition of having access to the states in the system. This strong condition may be valid and practical on the transmission level, however, it is not the case on the distribution level due to differences in topologies and properties of the two systems. Nodal voltage phasor values, used as system states, cannot be easily obtained in the distribution systems due to the limiting availability of PMUs. To tackle this challenge, authors in [24] proposed the construction of local FDI attacks, based on approximate states obtained from local measurements. Using the voltage and phase angles as system states, approximation of voltage magnitude and phase angle at node j, V_j and θ_j are given by [24]:

$$\begin{cases} V_j \approx V_i - (P_{ij}r_{ij} + Q_{ij}x_{ij}) & \forall j \in \mathbb{N} \\ \theta_j \approx P_{ij}x_{ij} - Q_{ij}r_{ij} & \forall \{i, j\} \in \mathbb{L} \end{cases} \tag{5}$$

where P_{ij}, Q_{ij} and r_{ij}, x_{ij} are the active and reactive power flow, line resistance and reactance between nodes i and j, respectively, while $\mathbb{N}, \mathbb{L}$ are the set of nodes and set of lines respectively. Accordingly, approximations of nodal voltages and phase angles are obtained from local meter measurements. The information is used to launch a local FDI attack. It is worth mentioning that the authors did not consider VVC in their model. Also, the strong condition stated by the authors is valid for using nodal voltage-based state estimation. Alternative techniques such as the Branch Current State Estimation (BCSE) [218] may represent a more suitable approach for the DSSE. This technique fits the nature of distribution systems and thus achieves more accurate estimation. Accordingly, it may have stronger capabilities in detecting potential threats.

C. DISTRIBUTION SYSTEM OPTIMAL POWER FLOW (DSOPF)

The growing number of DERs in radial topologies renders the DSOPF a challenging task in ADN operation, and simultaneously increases its vulnerability. Information leakage in radial systems has been investigated and proven to be a serious concern [219]. Without proper precautions, private information such as local energy consumption, local power generation, and local cost function parameters are exposed in traditional DSOPF approaches. The authors proposed a privacy countermeasure by injecting stochastic noise into signals communicated between neighbouring buses. The effects of FDI attacks on DSOPF have been studied in [26]. Stealthy FDI attack vectors are injected into the power flow measurements as follows:

$$z = h(x) + e \tag{6}$$

where x is the system states vector, $h(x)$ is the nonlinear function that maps the states to the measurements vector z, and e is the measurement error vector. The attacker injects the attack vectors a which deviate the DSOPF from its optimality point and increase system losses, formulated as

$$a = h(\hat{x} + c) - h(\hat{x}) \tag{7}$$

where c is the added values to the perceived states. The attacker synthesizes these attack vectors based on an optimization formulation:

$$\begin{aligned} &\text{maximize} && f(x) && \text{(8a)} \\ &\text{subject to} && g(x) = 0 && \text{(8b)} \\ &&& h(x) \geq 0 && \text{(8c)} \\ &&& \|diag(z_a - h(\hat{x}_{bad}))\| \leq \tau && \text{(8d)} \end{aligned}$$

where (8a), (8b), (8c) constituent the objective function and constraints of the system operator, and 8d is the added attack constraint. The attacker formulation allows an opponent to inject FDI attacks that bypass the DSSE security measures and increases the DSOPF cost. As the attack model does not violate physical laws or system constraints, the system operator is not able to detect such stealthy attacks.

It can be observed from the previous discussion that cyber-attacks have a large impact on the critical operation of the ADNs and consequently on the system operation reliability. Measurement devices and sensors are therefore lucrative targets that an attacker can exploit to gain system access to disrupt operations. In the next section, the vulnerabilities of measurement devices and sensors are discussed in detail.

VI. MICROGRIDS AND DISTRIBUTED ENERGY RESOURCES

MG operations can be severely impeded by well-known cyber-physical attacks such as FDI and DoS. For instance, it has been shown that through FDI, an adversary is capable of driving MGs to instability. While Nejabatkhah et al. [78] has recently surveyed work in the area of MG CPS, in this section, we review the most recent efforts.

A. IMPACT OF CYBER-PHYSICAL ATTACKS

One key operational aspect of the MGs is that they have the capability of working as interconnected hubs of energy or operating in isolated mode, and switching between the two modes, thus, increasing the reliability of the overall power grid [75]. Cyber-physical adversaries can tamper however with the process of partitioning the MG networks. The authors in [220] investigated the effects of FDI attacks on dynamic MG partitioning process into energy nodes. By intelligently varying the supply and demand power measurements of each partition, the attacker can create i) a deficiency in energy supply by a given node, ii) an increase in energy demand, or iii) a combination of i) and ii). This attack outcome is a total increase of energy loss, resulting from the mismatch between calculated energy supply (demand) and actual energy supply (demand) for energy supply (demand) nodes.

Cyber-attacks on the dynamic performance of the islanded MG frequency control are studied in [221], [222], and [223]. The impact of FDI and DoS attacks is investigated using a Canadian urban benchmark distribution system and the authors showed that the dynamic performance of the secondary frequency control system in an islanded MG could be significantly affected by DoS and FDI attacks. Chlela et al. in [224] studied the effect of FDI attacks on the operation of an MG centralized Energy Management System (EMS). They manipulated the active power dispatch points to affect the frequency stability and the operation of under-frequency load shedding. A combined droop and virtual inertial control strategy is proposed to mitigate the effect of such attacks.

Zhang et al. present a theoretical analysis of FDI effects on load sharing of MGs that have DGs and local loads [225]. Equipped with full system knowledge, an attacker targets the load-sharing control and drives the MG out of the stability region. Teixeira et al. [226] studied the impact of cyber-attacks against the voltage control schemes in interconnected MGs. Two attack scenarios were studied including the manipulation of measurement data reference signals received by voltage droop controllers in order to manipulate the voltage control decisions.

B. DEFENSE, PROTECTION AND MITIGATION STRATEGIES

A framework to detect FDI attacks on DC MGs is presented in [227]. Their attack detection strategy depended on identifying changes in sets of interred candidate MG properties that do not change over time. Koynev et al. [228] proposed a communication architecture that aimed at securing the communication of MGs control and operation processes. They proposed a new security protocol that was based on network, data and attack models. The proposed protocol has the advantages of data confidentiality and authentication while meeting the real-time communication needs of the MG. However, due to the need to transmit point-to-point authentication tags in multi-cast communications, there is a communication overhead. In [229], Rana et al. proposed a recursive systematic convolutional (RSC) code and a Kalman filter-based method to increase the redundancy of the MG states. They also proposed a semidefinite programming-based optimal feedback controller to tune system states after being estimated by the Kalman filter so that the power system can use it to mitigate cyber-attacks.

Jin et al. [230] proposed a Software-Defined Network (SDN) communication layer to be added to the MG architecture, in order to be resilient to cyber-attacks. Through an open platform and high-level Application Programming Interfaces (APIs), the SDN manages, controls and communicates with the network devices. As the first line of defence, the authors devise a mitigation plan to stop disruptions cascading. The proposed scheme is based on 1) isolation of the compromised devices, 2) cutting traffic of surrounding attack sources, and 3) re-connection of sensors to the communication layer to ensure the continuation of network observability. Secondly, for the self-healing process, the communication network permits a quick reset and switches reconfiguration to isolate compromised devices (such as PMUs) and establishes new communication routes to prevent the cascading of attack effects. Additionally, in order to significantly minimize the attacker operation window, on-demand control paths are to be enabled. The SDN introduces great flexibility in the resiliency strategy of MGs. However special efforts are to be deployed in order to seamlessly integrate the additional layer with the existing power grid and to limit the vulnerabilities introduced by the software implementations and any unexpected failures of the SDN.

C. DERS AND SMART INVERTERS

A main factor in the strength and resiliency of ADNs is the decentralization and diversification of their components. For power generation, there is an array of DERs, each of which has its own characteristics and power profile. They include photovoltaic (PV) panels, wind generators, Diesel generators and Distributed Generators (DGs) in general. However,

TABLE 4. Common communication protocols for smart inverters [232].

Protocol/Feature	SunSpec Modbus	IEEE 1815	IEEE 2030.5	IEC 61850
Information Model	SunSpec	DNP3 Application Note	CSIP	IEC 61850-90-7
Security Requirements	None	IEEE 1815	IEEE 2030.5 + CSIP	IEC 62351 Series
Authentication Support	Non-native	Optional	Yes	Non-native
Encryption Capability	Bump-in-the-wire	Bump-in-the-wire	Yes	Non-native

this multitude of equipment creates potential risks to be compromised or hacked to launch a cyber-physical attack.

With a focus on PV and wind DERs, the authors in [231] presented a comprehensive review of the key vulnerabilities in communication protocols used by the DERs to better understand the DER security challenges. DER communication systems are composed of 4 layers; 1) the physical layer that includes fundamental devices and channels employed for connectivity, 2) the data link layer, which includes different protocols such as Ethernet, Frame relay and Asynchronous Transfer Mode, 3) the network layer that defines the data packet paths within the communication network, and 4) the transport layer where Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) connections are made. These layers are prone to different physical and cybersecurity issues. For example, the physical layer is vulnerable to data and/or hardware theft, unauthorized changes to the functional environment and undetectable data interception. The data link and network layers are prone to unauthorized access and network expansion. Last but not least, the attackers can access the network and/or the transport layers if they predict the TCP sequence numbers.

The cybersecurity of smart inverters in smart grids has been recently discussed in [232], and the vulnerabilities associated with their communication protocols, including IEEE 1815 (DNP3), SunSpec Modbus, IEC 61850 and IEEE 2030.5, are discussed in detail in [233], [234], and [235]. It is a requirement by IEEE 1547.2018 that DER devices must support at least one of these communication protocols. A brief comparison between the features of these protocols is provided in Table 4 in terms of the information model and cybersecurity capabilities.

In order to assess the vulnerability of DERs, Shelar and Amin considered a three stages defender-attacker-defender (DAD) game [236]. The game assumes that the operator has an initial plan of securing a subset of the DERs, then the adversary is able to compromise a set of DERs, and finally, the operator responds by controlling non-compromised DERs and loads. Faced with the nonlinear power flow and mixed integers, rendering the optimization problem non-convex, the authors choose to relax the problem by implementing a traceable ϵ-linear power flow. The DAD game results in an optimal attack strategy aimed to create voltage violations at the compromised nodes. In addition, the physical impact of cyber-attacks against a real PV system is investigated by Kang et al. in [237] using a test-bed environment that includes a PV system and communication devices and is based on IEC 61850. The malicious attacks aimed at manipulating the power limits, hence changing the physical operation of the PV inverter devices or changing their status while blinding the system operator. Liu et al. studied the impact of cyber-attacks on MGs when the control parameters of the solar PV and ESS control systems are intentionally modified [109].

In [238] and [239], the authors studied the effect of cyber-attacks on distributed economic dispatch between DGs and proposed a strategy that isolates the misbehaving DGs under attack. A holistic attack-resilient framework that aimed at protecting the integrated DER and the critical power grid infrastructure from malicious cyber-attacks was proposed in [240]. Using a Hardware-in-the-Loop testing platform, Chlela et al. in [241] proposed a rule-based fallback control strategy to enhance the resiliency of the MG to DoS cyber-attacks by managing the ESS state of charge in a decentralized manner.

VII. ELECTRIC VEHICLES

Integrating EVs into ADNs provides enhanced opportunities for energy storage while changing load patterns and introducing new communications/control to enable EV charging. As discussed in this section, such integration can also increase the risk of cyber-attack vulnerabilities. EV charging is enabled by Electric Vehicle Supply Equipment (EVSE), which employs a protocol to decide on the charging/discharging rate, and then begins the charging or discharging process of the vehicle. In most cases, the EV charging process interacts with the user agent, EVSE, distribution system, and payment method to control energy flow and billing. Such interactions may invoke security breaches within the associated ADNs making the charging process a target of multiple attacks [96], [242], [243], [244].

Moreover, the EV charging ecosystem employs a variety of standards and proprietary protocols to manage EV charging and billing actions. While these protocols make it possible for ADNs to meet the increasing energy demands of a growing population of EVs [79], [245], [246], they, too, have the effect of increasing the cyberattack surface.

A. EV COMMUNICATION AND SIGNALLING

The ISO/IEC 15118-1/2/3 and IEC 61850 protocols specify the communication and signaling between an EV and EVSE for smart charging [247], [248]. The EVCC (Electric Vehicle Communication Controller) is a key component of the EV that exchanges information with the SECC (Supply Equipment Communication Controller) within the external charger to regulate current flow during charging. The EVCC and SECC use ISO/IEC 15118 V2G messages to address charging actions, including session initiation, entrance into a charging loop, and termination of the charging session [247], [249].

The IEC 61850 protocol stack of the intelligent grid involves object-oriented modeling using the TCP/IP protocol suite to establish role-based access control [250], [251]. European EV stakeholders developed the OCPP (Open Charge Point Protocol) in 2009; OCPP is an open-source communication standard employed by EV charging stations and network software companies or CPO (Charge Point Operator; a company that manages a family of charging points) such that an EV charging station that is OCPP-compliant can be configured to run OCPP-compliant software. This reduces overall integration and investment costs [247]; however, the protocol is yet to be standardized.

The Clearinghouse (CH) utilizes the OCHP (Open Clearing House Protocol) for exchanging information for billing and eMIP (eMobility Inter-Operation Protocol) to enable roaming with eMSP (E-Mobility Service Provider). Once the EV selects a CPO, the CPO uses OCPI to communicate with eMSP for smart charging and billing. The OpenADR (Open Automated Demand Response) protocol, developed by the US Department of Energy, enables the communication between the EVSE and DSO (Distribution System Operator) to balance demand to sustainable supply either by tariffs, incentives, or emergency signals [247], [252], [253].

The extra power needed during EV charging at peak hours may overload an ADN. Consequently, attacks on charging protocols or infrastructure can potentially create more significant threats that can cause power delivery disruption, power quality degradation, system stability, and monetary losses [254], [255], [256]. Moreover, in some cases, OEM uses I2C, SPI, CAN bus, USART to exchange V2G messages between EV and EVSE. Encryption and authentication deployment in the higher layer ISO/IEC 15118 V2G messages potentially eliminate the vulnerabilities in these physical layer protocols. However, wiretapping, physical access and plain text messaging between the charging system and EV may exploit them; thus increasing attack space in ADN [257].

B. IMPACT OF EV ATTACKS ON THE ADNs

ADNS must address security, capacity, and energy management to facilitate large-scale EV integration. Since EV charging infrastructure is tightly coupled electrically (physical) and in terms of information flow (cyber), an attack on a charging system could severely impact both ADN electrical stability and information security [254], [258], [259], [260], [261], [262]. Table 3 summarizes ways in which EV integration in ADNs, impacts CPS and the following refers to references in the table.

Pirouzi et al. [264] showed that compromised EV infrastructure and ADNs might increase the penetration rate of EVs, causing voltage instability, increased operational cost, and lower ADN security. To minimize the operational cost and maximize the voltage security margin of distribution, [264] proposed an optimization model and implemented it on the 33-bus test system for active and reactive power management. Further, Research on ADN security demonstrated that spoofing attacks targeting EV and EVSE can lead to voltage and frequency instability [243], [244], [272], [278]. To address this, Park et al. devised a key management protocol to mitigate spoofing attacks on EVSE within ADNs [272].

Numerous studies considered tampering attacks (see Table 5) on EV and ADNs that impact fair electricity pricing, voltage security, V2G energy trading, and ADN data confidentiality [243], [263], [264], [266], [268], [272], [276], [277]. D. Niyato et al. introduced the novel concept of a cyber-insurance policy for the V2G system for fair pricing of EV charging [263]. In contrast, [264] presented a mathematical optimization model to minimize the operational cost due to tampering with the power flow parameters of the distribution system. However, [266] offered secure V2G energy trading by leveraging blockchain technology, contact theory, and edge computing.

MitM attacks targetting EV, EVSE, and CS (Central Server) of CPO have been addressed by several research groups [243], [244], [265], [266], [267], [268], [272], [278]. The ISO/IEC 15118-1/2/3 and OCPP recommend using the TLS protocol for smart charging; however, most OEMs (Original Equipment Manufacturers) do not implement vulnerable locally verified certificates to reduce the charging software product costs. To reduce the risk of MitM attack, [265] proposed to split meter values and send them separately by interleaving data of different transactions to the EVSE. Authors in [267] proposed message sequence, frequency, subscription period, and power measurement validation to mitigate MitM, DoS, and inaccurate power use reporting. Moreover, [268] proposed a Physical Unclonable Function (PUF)-based secure user key exchange authentication (SUKA) protocol involving two steps of mutual authentication between the EV and ADN to mitigate MitM, impersonation, replay, and tampering attacks.

Customized attacks presented in [245], [264], [270], [271], [273], [274], [275], [278], and [276] aim to maximize attack damage to ADNs via an optimization process, then devise a solution to mitigate the attacks. As such, the attack model is represented by a combination of actions compromising confidentiality, integrity, and availability. For example, [270] adopted a spatial-temporal forecast model based on analysis of three types of EVs to maximize attack benefits.

Although the articles above (summarized in Table 5) discuss various attack detection and mitigation techniques on EV charging to minimize the impact on ADN, the charging system allows attackers to design new vulnerabilities to destabilize the ADN cyber-physical space. Several lower-level protocols, including CAN bus, SPI, and I2C, do not have any scope to add extra information for authentication,

TABLE 5. EV integration: impacts on ADNs security.

Study		Threat		Attack Class							
Attack	*Defence*	*EVs*	*EVSE& DS*	*Spoofing*	*Tampering*	*MitM*	*Repudiation*	*DoS*	*Privacy Breach*	*Customizing Attack*	*Impact on ADNs*
✓	✓	✓			✓				✓		Fair Transaction [263]
✓	✓		✓		✓				✓	✓	Voltage Security [264]
✓	✓		✓			✓					Confidentiality [265]
	✓		✓							✓	Communication Security [245]
	✓	✓	✓		✓	✓		✓	✓		V2G Energy Trading Security [266]
✓			✓	✓		✓		✓			Compromised EVSE-Power Grid network [244]
	✓	✓	✓			✓		✓			EV & DS Sensor [267]
	✓	✓	✓		✓	✓					Authentication Keys [268]
✓			✓					✓			EVSE & Power grid DDoS attack [269]
✓			✓							✓	Voltage Deviation, instability [270]
	✓	✓	✓							✓	Hardening Security [271]
✓	✓	✓	✓	✓	✓	✓	✓		✓		Dynamic V2G Key Management [272]
	✓	✓	✓					✓		✓	Availability [273]
✓	✓	✓	✓							✓	Risk Assessment [274]
✓			✓							✓	DS security risk [275]
✓		✓	✓		✓					✓	Confidentiality, Availability, Integrity [276]
✓		✓	✓					✓			Line congestion & voltage limit violation [258]
✓	✓	✓	✓		✓		✓	✓			compromise wireless network [277]
✓			✓	✓		✓				✓	Integrity & stability [278]
✓	✓	✓	✓						✓		malfunction or damage [279]
✓		✓	✓	✓	✓	✓			✓		data driven voltage and frequency stability [243]

certification, and encrypted communications; such an addition may make the protocol incompatible to use. In deploying charging systems, OEMs widely use these protocols for EV charging. However, in these cases, attackers need physical access to the charging network using the ODB II interface or charging station cable tapping. Attackers may inject false messages, play the DoS, replay attacks, and temper lower-level protocol messages, severely impacting ADN power stability, availability, battery damage, and electricity theft. Although, the attacks are only successful when the upper layer message or payload is in plain text. In encrypted payload cases, the message's tempering in I2C, SPI, or CAN bus attack may not be plausible [257], [280]. Including the lower-level protocol, the ADN network is vulnerable to invisible stealthy attacks, requiring extra effort for attack detection, prevention, and mitigation.

VIII. IoT CYBER-PHYSICAL SECURITY AND SMART HOME LOADS ATTACKS

As a salient aspect of ADNs, an increase in the prevalence of smart homes is being evidenced due to advancements in IoT technology. IoT has significant merits over traditional ADNs and smart home communication technologies including real-time monitoring, situational awareness and intelligence, control and CPS [99]. These advantages, however, come at the cost of vulnerabilities that IoT technology brings to the ADNs through, for example, data transmission mechanisms [100], [101]. In 2014, Komninos et al. and Bekara et al. surveyed the challenges and countermeasures of smart grids including IoT-based smart homes in [142] and [101]. The authors of [142] classified the potential impact of cyber-attacks on smart homes into three categories: low, moderate and high according to the degree of adverse effects of the attack on the target system(s). Hossain et al. [281] conducted a comprehensive review on the application of Big Data and Machine Learning in IoT-integrated smart grids. In this section, we also aim to cover the most recent contributions to this topic.

Heartfield et al. proposed an intrusion detection system called MAGPIE [282]. MAGPIE autonomously adjusts the decision function of its anomaly detection models based on the changing condition of the smart home. In addition to utilizing the cyber layer data, it employs physical sources of data i.e., human presence to utilize models that exhibit the highest accuracy. In [283] Davis et al. compared the security postures between different vendors through misuse and abuse case analyses. They advised having a stronger focus on the lesser-known vendors' security posture due to their lack of regulation. Speech recognition became one of the most popular methods to control voice controllable systems. In [284], Mao et al. studied the effect of ultrasonic-based inaudible voice attacks against smart home devices e.g. mobile phones. They proposed a two-step detection algorithm to identify the attacked voice signal. Utilizing the high integrity and confidentiality of the blockchain, Lin et al. proposed a blockchain-based secure mutual authentication System for smart homes called "HomeChain" [285]. HomeChain integrated blockchain, group signature and message authentication code to anonymously authenticate group members and efficiently authenticate the home gateway. This showed robustness against different types of attacks. However, one of the drawbacks of this system is the high communication and computation costs especially when a higher security level is needed. Liu et al. [286] studied the coordinated pricing cyber-attacks and energy theft in smart homes. They studied the impact of such attacks under different attacking scenarios and showed that these attacks can reduce the electricity bills of the attacker by 32.65%. They also utilized a partially observable Markov decision process (POMDP) to develop a detection framework that could effectively mitigate the impacts of coordinated cyber-attacks. Majumder et al. [287] proposed a cyber-physical system to Detect IoT security threats of a smart home heterogeneous wireless sensor node using a Raspberry Pi and a smartphone. They employed the behavioural power profiling of the sensor devices and used different general multivariate logistic regression models and statistical classification techniques to detect abnormal behaviours and notify the admin. One of the limitations of this proposed system is that it focused on specific devices and does not cover all smart home devices.

IX. CYBER-PHYSICAL SECURITY SOLUTIONS FROM MANUFACTURERS

Manufacturers are critical in contending with the adaptation of ADNs to provide state-of-the-art solutions to both utilities and consumers. As such, manufacturers are at the front line for enabling and impacting the grid's cybersecurity posture by prioritizing and integrating security-aware solutions [288]. Moreover, regulatory bodies incentivize both manufacturers and utilities to integrate security-strategic approaches given the gravity of enabling a safe and secure power distribution system. This section surveys the latest products/solutions by well-known manufacturers that incorporate CPS requirements for ADNs including accounting for how new communication features and their impact on enabling system vulnerabilities.

In [289], Sukumara et al. from ABB surveyed some of the practices and methods to achieve the security of substations and distribution automation systems. These practices include 1) physical protection, 2) the principle of "least privileges" that provides the right person right privileges to operate/work on substation operation and control, 3) the use of an audit trail to review security-critical events, discover attempts of cyber-attacks, track users' access and perform analysis, 4) network separation into security zones, 5) removing and deactivating all unused processes, communication ports and services, 6) use of secured applications and 7) securing sensitive data and operational information.

Siemens also supported the OT Role-Based Access Control (OT-RBAC) infrastructure to cover protection relay IEDs, RTUs, controllers, gateways, power quality devices, and service PCs in substations and other power systems [290]. In addition, Siemens has recently taken into consideration the MITRE ATT&CK that targets ICS and added mitigation features into their recent products such as SIPROTEC 5 protection relays and SICAM A8000 RTUs.

In order to protect smart meters at ADNs, Schweitzer Engineering Laboratories (SEL) developed Padlock and Watchdog in collaborative projects with the U.S. Department of Energy (DOE). Padlock is a digital security entryway that distinguishes physical and computerized changes, while Watchdog is a managed switch that performs deep packet inspection using a white list configuration approach to establish a set of known, allowed communications. Another collaborative project between SEL and DOE is the Alliance project which aimed at developing a proximity card reader and controller that monitors both cyber and physical security access [291].

One salient characteristic of many manufacturers is their commitment to providing lifecycle services and support for the devices and equipment they develop and help deploy. While this provides advantages in some contexts, natural questions arise that we discuss in the next section.

X. ENERGY SECURITY

The previous section highlighted the influence that manufacturers have on the cyber posture of ADNs. While it is imperative that products account for the needs of an evolving ADN, questions arise related to the risks associated with the participation of a growingly diverse set of stakeholders. Further, the increased collaboration amongst citizen-owned devices and international original equipment manufacturers (OEMs) brings forth concerns about the dependence of cybersecurity on a variety of stakeholders with varying security postures and competing agendas. This affects energy infrastructure in general making it a priority for national regulators and operators. As such, we conclude this survey with a brief discussion of energy security as it motivates the cybersecurity of ADNs and critical infrastructure protection overall.

Energy security is the foundation upon which a society can thrive, which links the goals of national security (as it relates to the affordable availability and access of energy) to a country's natural resources. The definition of energy security is increasingly being related to the security of its associated infrastructure [292]. Moreover, advances in information and communications technologies have been empirically related to affecting energy security [293] in both positive and negative ways. Traditional system weaknesses stemming from the lack of physical protection around energy equipment and limited resilience to natural disasters have "modernized" to shortcomings of cyberinfrastructure that allow remote attackers to assault energy infrastructure from across the globe. Supply chain attacks, as discussed in Section III-A, exploit a growing cyber attack surface from the participation of a variety of distributed entities in the design, production and deployment of critical ADN equipment. Furthermore, a growing number of cyberattacks are being influenced by geopolitical conflicts [294], [295].

TABLE 6. **Cyber-physical attacks on ADNs.**

Ref	Category	Area	Limitations
[106], [213]–[215], [296]	Critical Operations	VVC	• No consideration of BDD in DSSE
[24], [26], [106], [126], [215]–[218]	Critical Operations	DSSE	• Assumption of system topology knowledge • Assumption of having access to system states • No consideration of VVC devices
[26], [219]	Critical Operations	DSOPF	• Consideration of DC DSOPF model
[25], [111], [112], [147], [172], [173]	Devices & Sensors	PMUs	• Assumption that cyber-attacks are single occurrences and not compounded • Dependency on communication protocols that are vulnerable against cyber-attacks.
[12], [13], [174]–[182], [182]–[184], [184]–[188], [194], [202]	Devices & Sensors	SMs & AMIs	• Using historical data for cyber-attack detection which is inherent heuristic and non-deterministic in nature, and does not guarantee the quality of the solution. • Approaches may fail with large distribution networks due to the scalability issue.
[77], [205], [209]–[212]	Devices & Sensors	Protection Relays	• Assumption of communication redundancy • lack of literature in the area of cyber-security of distribution systems protection
[75], [78], [109], [220], [222]–[241]	Applications & Enablers	Microgrids	• Detection is based on MG properties that do not change over time • Communication overhead due to the need to transmit point-to-point authentication tags in multi-cast communications • Using communication technologies such as SDNs introduces new vulnerabilities due to the software implementations and any unexpected failures of the SDN
[243], [244], [254]–[256], [258]–[264], [266], [268], [272], [276]–[278]	Applications & Enablers	Electric Vehicles	• Charging system allows attackers to design new vulnerabilities to destabilize the ADN cyber-physical space • Several lower-level protocols, including CAN bus, SPI, and I2C, do not have any scope to add extra information for authentication, certification, and encrypted communications
[101], [142], [281]–[287]	Applications & Enablers	IoT & Smart Homes	• Dependency on human presence to utilize models that exhibit the highest accuracy • High communication and computation costs especially when a higher security level is needed • Some approaches focus on specific devices and do not cover all smart home devices

Sovereign capability is becoming an essential goal for safety and survivability, especially in a sophisticated geopolitical climate. By its very nature, the power grid is a highly physically connected system, often spanning across national boundaries. Coupled with the expanding cyber connectivity, especially at the distribution level, opportunities exist for international and inter-continental energy impacts. As such, CPS challenges are of paramount and growing interest at a broader scale. In this way, we believe that a discussion of CPS, as provided through this survey, is of utmost importance from both technical and non-technical perspectives. Ultimately, it is our hope that increased opportunities for multidisciplinary discourse across technical, regulatory, economic and political sectors are possible.

XI. CONCLUDING REMARKS AND FUTURE RESEARCH

While existing literature has focused on CPS aspects of smart grids at the bulk transmission level, as shown in this survey, dangerous cyber-attacks can be initiated from within the distribution grid. As such, this paper reviews the progress and recent advancements in ADNs from CPS perspectives; a variety of critical operations and components, including VVC, DSSE, and DSOPF, were reviewed. Given the distinct nature of these critical operations, the application of each and their associated cyber threats must, in part, be separately addressed in further detail as future research. There is, however, a definite need for stakeholders to come up with an ADN reference framework (or set of architectures given the diversity of ADNs) for CPS studies that accounts for modern changes in the threat landscape. We consider this an important step for future work.

In addition, CPS aspects of MGs, IoT-based smart homes and EVs were reviewed with the most recent works being presented. Moreover, the cyber-attack problems related to smart meters and sensors as well as energy theft have been thoroughly surveyed. Future work should focus on in-depth studies of monitoring, control and protection of MGs, EVs and AMIs with CPS aspects being accounted for in the future design of these schemes and systems.

In fact, given the variety of stakeholders (utilities, consumers, manufacturers, aggregators and other third parties) involved in the subsystems that compromise EV, AMI and DER infrastructures, additional research gaps must be addressed related to robust monitoring and intrusion detection. For instance, the implementation of reliable and synchronized mechanisms for data collection from distributed IT, OT and other sources and the development of efficient methods for the correlation and the real-time analysis of the converged data pose significant challenges. Future cybersecurity solutions for these infrastructures and other ADN applications can leverage their distributed nature to enable collaborative approaches for threat mitigation and incident response for overall system resilience. Further, such distributed and collaborative cybersecurity enhancement solutions should consider key business requirements and consumer privacy and government regulations.

This paper reviewed several different manufacturer solutions for CPS of ADNs. Despite such vendor activity, much needs to be done to ensure compliance with the increasing number of emerging CPS standards. Manufacturer solutions have focused more on access management and have also focused on the protection and mitigation processes at the device level.

Improving the security best practices is of significant importance for industrial systems security and includes the implementation of measures such as 1) identification of the systems that must be protected, 2) logical separation of the systems into functional groups to reduce the surface of attack by tightly locking down and controlling specific services that are arranged in functional groups, 3) implementation of a defence-in-depth strategy around each system or group of systems, 4) control of the access into and between each group, 5) monitoring within and between groups, 6) limitation of the actions that can be executed within and between groups. Finally, future research directions related to system and network visibility along with detection and monitoring principles that account for adversary behaviours are of utmost importance and should focus on ADNs environments. Aligned with this last recommendation, we emphasize the necessity to design and implement monitoring solutions that provide efficient and timely intrusion detection without compromising operational continuity while balancing the need for security professionals to effectively manage information in an, often overwhelming, big data high-speed smart grid ecosystem.

CLASSIFICATION TABLE

A summary of the literature reviewed on cyber-physical attacks against ADNs is provided in Table 6. The references are classified based on the area that they cover. In addition, the last column of the table mentions the limitations found in these references. It is worth noting that not all references have all limitations. However, all limitations are included to serve as potential future work directions.

REFERENCES

[1] P. Ge, B. Chen, and F. Teng, "Cyber-resilient self-triggered distributed control of networked microgrids against multi-layer DoS attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 4, pp. 3114–3124, Jul. 2023.

[2] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2886–2927, 3rd Quart., 2019.

[3] J. M. Morales, S. Pineda, and Y. Dvorkin, "Learning the price response of active distribution networks for TSO-DSO coordination," *IEEE Trans. Power Syst.*, vol. 37, no. 4, pp. 2858–2868, Jul. 2022.

[4] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Trans. Syst. Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1554–1569, Aug. 2019.

[5] *Cybersecurity and A. C. D. A. Infrastructure Security Agency. Cyber-Attack Against Ukrainian Critical Infrastructure*. Accessed: Feb. 2, 2024. [Online]. Available: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

[6] H. Goyel and K. S. Swarup, "Data integrity attack detection using ensemble-based learning for cyber–physical power systems," *IEEE Trans. Smart Grid*, vol. 14, no. 2, pp. 1198–1209, Mar. 2023.

[7] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Elect. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018.

[8] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[9] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 397–422, 1st Quart., 2017.

[10] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 13–27, Dec. 2016.

[11] R. Mahmud, R. Vallakati, A. Mukherjee, P. Ranganathan, and A. Nejadpak, "A survey on smart grid metering infrastructures: Threats and solutions," in *Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT)*, May 2015, pp. 386–391.

[12] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 5–20, 1st Quart., 2013.

[13] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[14] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[15] G. N. Ericsson, "Cyber security and power system communication—Essential parts of a smart grid infrastructure," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1501–1507, Jul. 2010.

[16] P. Lau, L. Wang, Z. Liu, W. Wei, and C.-W. Ten, "A coalitional cyber-insurance design considering power system reliability and cyber vulnerability," *IEEE Trans. Power Syst.*, vol. 36, no. 6, pp. 5512–5524, Nov. 2021.

[17] M. Khalaf, "Cyber-physical security of wide-area frequency-based applications in power systems," Ph.D. thesis, Univ. Waterloo, Waterloo, ON, Canada, Oct. 2020.

[18] Z. Zhang, R. Deng, Y. Tian, P. Cheng, and J. Ma, "SPMA: Stealthy physics-manipulated attack and countermeasures in cyber-physical smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 581–596, 2023.

[19] H. F. Habib, C. R. Lashway, and O. A. Mohammed, "A review of communication failure impacts on adaptive microgrid protection schemes and the use of energy storage as a contingency," *IEEE Trans. Ind. Appl.*, vol. 54, no. 2, pp. 1194–1207, Mar. 2018.

[20] B. Mcmillin and T. Roth, "Cyber-physical security and privacy in the electric smart grid," *Synth. Lectures Inf. Secur., Privacy, Trust*, vol. 9, no. 2, pp. 1–64, Aug. 2017.

[21] T. M. Blasi, C. C. C. B. de Aquino, R. S. Pinto, M. O. de Lara Filho, T. S. P. Fernandes, C. U. Vila, A. R. Aoki, R. B. dos Santos, and F. H. Tabarro, "Active distribution networks with microgrid and distributed energy resources optimization using hierarchical model," *Energies*, vol. 15, no. 11, p. 3992, May 2022.

[22] H. Gao, X. Lyu, S. He, L. Wang, C. Wang, and J. Liu, "Integrated planning of cyber-physical active distribution system considering multidimensional uncertainties," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 3145–3159, Jul. 2022.

[23] W. Liu, Y. Chen, L. Wang, N. Liu, H. Xu, and Z. Liu, "An integrated planning approach for distributed generation interconnection in cyber physical active distribution systems," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 541–554, Jan. 2020.

[24] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2871–2881, May 2019.

[25] M. Delcourt, E. Shereen, G. Dän, J.-Y. Le Boudec, and M. Paolone, "Time-synchronization attack detection in unbalanced three-phase systems," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4460–4470, Sep. 2021.

[26] A. Ayad, H. Farag, A. Youssef, and E. El-Saadany, "Cyber–physical attacks on power distribution systems," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 5, no. 2, pp. 218–225, Jun. 2020.

[27] D. Ranamuka, K. M. Muttaqi, and D. Sutanto, "Flexible AC power flow control in distribution systems by coordinated control of distributed solar-PV and battery energy storage units," *IEEE Trans. Sustain. Energy*, vol. 11, no. 4, pp. 2054–2062, Oct. 2020.

[28] R. Mohammadi, H. R. Mashhadi, and M. Shahidehpour, "Market-based customer reliability provision in distribution systems based on game theory: A bi-level optimization approach," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3840–3848, Jul. 2019.

[29] Z. S. Hosseini, M. Mahoor, and A. Khodaei, "AMI-enabled distribution network line outage identification via multi-label SVM," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 5470–5472, Sep. 2018.

[30] R. A. Walling, R. Saint, R. C. Dugan, J. Burke, and L. A. Kojovic, "Summary of distributed resources impact on power delivery systems," *IEEE Trans. Power Del.*, vol. 23, no. 3, pp. 1636–1644, Jul. 2008.

[31] R. Céspedes and J. F. Reyes, "Smart grid voltage control for electrical power distribution system operation optimization," in *Proc. IEEE ANDESCON*, Oct. 2016, pp. 1–4.

[32] H. E. Z. Farag and E. F. El-Saadany, "A novel cooperative protocol for distributed voltage control in active distribution systems," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1645–1656, May 2013.

[33] K. E. Antoniadou-Plytaria, I. N. Kouveliotis-Lysikatos, P. S. Georgilakis, and N. D. Hatziargyriou, "Distributed and decentralized voltage control of smart distribution networks: Models, methods, and future research," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2999–3008, Nov. 2017.

[34] H. J. Liu, W. Shi, and H. Zhu, "Distributed voltage control in distribution networks: Online and robust implementations," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6106–6117, Nov. 2018.

[35] M. Ali, R. J. Millar, and M. Lehtonen, "A framework to split the benefits of DR between wind integration and network management," *IEEE Trans. Power Syst.*, vol. 33, no. 2, pp. 1443–1450, Mar. 2018.

[36] A. Kulmala, S. Repo, and P. Järventausta, "Coordinated voltage control in distribution networks including several distributed energy resources," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 2010–2020, Jul. 2014.

[37] Y.-J. Kim, S.-J. Ahn, P.-I. Hwang, G.-C. Pyo, and S.-I. Moon, "Coordinated control of a DG and voltage control devices using a dynamic programming algorithm," *IEEE Trans. Power Syst.*, vol. 28, no. 1, pp. 42–51, Feb. 2013.

[38] B. Zhang, A. Y. S. Lam, A. D. Domínguez-García, and D. Tse, "An optimal and distributed method for voltage regulation in power distribution systems," *IEEE Trans. Power Syst.*, vol. 30, no. 4, pp. 1714–1726, Jul. 2015.

[39] J. Barr and R. Majumder, "Integration of distributed generation in the Volt/VAR management system for active distribution networks," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 576–586, Mar. 2015.

[40] H. Zhu and H. J. Liu, "Fast local voltage control under limited reactive power: Optimality and stability analysis," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3794–3803, Sep. 2016.

[41] S. Ghosh, S. Rahman, and M. Pipattanasomporn, "Distribution voltage regulation through active power curtailment with PV inverters and solar generation forecasts," *IEEE Trans. Sustain. Energy*, vol. 8, no. 1, pp. 13–22, Jan. 2017.

[42] C. Ahn and H. Peng, "Decentralized voltage control to minimize distribution power loss of microgrids," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1297–1304, Sep. 2013.

[43] N. Yorino, Y. Zoka, M. Watanabe, and T. Kurushima, "An optimal autonomous decentralized control method for voltage control devices by using a multi-agent system," *IEEE Trans. Power Syst.*, vol. 30, no. 5, pp. 2225–2233, Sep. 2015.

[44] L. Yu, D. Czarkowski, and F. de Leon, "Optimal distributed voltage regulation for secondary networks with DGs," *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 959–967, Jun. 2012.

[45] C. N. Lu, J. H. Teng, and W.-H. E. Liu, "Distribution system state estimation," *IEEE Trans. Power Syst.*, vol. 10, no. 1, pp. 229–240, Feb. 1995.

[46] Ayad, Abdelrahman. (2019). *Cyber-physical Security of Power Distribution Systems*. [Online]. Available: http://hdl.handle.net/10012/14459

[47] K. Li, "State estimation for power distribution system and measurement impacts," *IEEE Trans. Power Syst.*, vol. 11, no. 2, pp. 911–916, May 1996.

[48] M. E. Baran and A. W. Kelley, "State estimation for real-time monitoring of distribution systems," *IEEE Trans. Power Syst.*, vol. 9, no. 3, pp. 1601–1609, Aug. 1994.

[49] J.-H. Teng, "Using voltage measurements to improve the results of branch-current-based state estimators for distribution systems," *IEE Proc. Gener., Transmiss. Distrib.*, vol. 149, no. 6, p. 667, 2002.

[50] M. E. Baran, J. Jung, and T. E. McDermott, "Including voltage measurements in branch current state estimation for distribution systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2009, pp. 1–5.

[51] A. K. Ghosh, D. L. Lubkeman, M. J. Downey, and R. H. Jones, "Distribution circuit state estimation using a probabilistic approach," *IEEE Trans. Power Syst.*, vol. 12, no. 1, pp. 45–51, Feb. 1997.

[52] Z. J. Simendic, V. C. Strezoski, and G. S. Svenda, "In-field verification of the real-time distribution state estimation," in *Proc. 18th Int. Conf. Exhib. Electr. Distrib. (CIRED)*, Jun. 2005, pp. 1–4.

[53] N. Katic, L. Fei, G. Svenda, and Z. Yongji, "Field testing of distribution state estimator," in *Proc. 22nd Int. Conf. Exhib. Electr. Distrib. (CIRED)*, Jun. 2013, pp. 1–4.

[54] J. Wu, Y. He, and N. Jenkins, "A robust state estimator for medium voltage distribution networks," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1008–1016, May 2013.

[55] H. Li, "An improved state estimator in distribution systems," in *Proc. IEEE Int. Conf. Comput. Sci. Autom. Eng.*, vol. 3, Jun. 2011, pp. 30–34.

[56] C. Muscas, M. Pau, P. A. Pegoraro, S. Sulis, F. Ponci, and A. Monti, "Multiarea distribution system state estimation," *IEEE Trans. Instrum. Meas.*, vol. 64, no. 5, pp. 1140–1148, May 2015.

[57] L. D. A. Garcia and S. Grenard, "Scalable distribution state estimation approach for distribution management systems," in *Proc. 2nd IEEE PES Int. Conf. Exhib. Innov. Smart Grid Technol.*, Dec. 2011, pp. 1–6.

[58] S. Sarri, M. Paolone, R. Cherkaoui, A. Borghetti, F. Napolitano, and C. A. Nucci, "State estimation of active distribution networks: Comparison between WLS and iterated Kalman-filter algorithm integrating PMUs," in *Proc. 3rd IEEE PES Innov. Smart Grid Technol. Eur. (ISGT Eur.)*, Berlin, Germany, Oct. 2012, pp. 1–8.

[59] M. Brown Do Coutto Filho and J. C. S. de Souza, "Forecasting-aided state estimation—Part I: Panorama," *IEEE Trans. Power Syst.*, vol. 24, no. 4, pp. 1667–1677, Nov. 2009.

[60] J. Carpentier, "Contribution a l'etude du dispatching economique," *Bull. de la Societé Francaise des Electriciens*, vol. 3, no. 1, pp. 431–447, 1962.

[61] E. Dall'Anese, H. Zhu, and G. B. Giannakis, "Distributed optimal power flow for smart microgrids," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1464–1475, Sep. 2013.

[62] L. Gan, N. Li, U. Topcu, and S. H. Low, "Exact convex relaxation of optimal power flow in tree networks," 2012, *arXiv:1208.4076*.

[63] L. Gan and S. H. Low, "Convex relaxations and linear approximation for optimal power flow in multiphase radial networks," in *Proc. Power Syst. Comput. Conf.*, Aug. 2014, pp. 1–9.

[64] S. K. Sen, *Fieldbus and Networking in Process Automation*. Boca Raton, FL, USA: CRC Press, 2014.

[65] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. H. Chin, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 21–38, 1st Quart., 2013.

[66] Q. Yang, J. A. Barria, and T. C. Green, "Communication infrastructures for distributed control of power distribution networks," *IEEE Trans. Ind. Informat.*, vol. 7, no. 2, pp. 316–327, May 2011.

[67] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 42–49, Jan. 2013.

[68] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[69] Y. Mo, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[70] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.

[71] W. Luan, D. Sharp, and S. Lancashire, "Smart grid communication network capacity planning for power utilities," in *Proc. IEEE PES T&D*, Apr. 2010, pp. 1–4.

[72] H. Lin, Y. Deng, S. Shukla, J. Thorp, and L. Mili, "Cyber security impacts on all-PMU state estimator—A case study on co-simulation platform GECO," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2012, pp. 587–592.

[73] A. Hooshyar and R. Iravani, "Microgrid protection," *Proc. IEEE*, vol. 105, no. 7, pp. 1332–1353, Jul. 2017.

[74] C. Abbey, D. Cornforth, N. Hatziargyriou, K. Hirose, A. Kwasinski, E. Kyriakides, G. Platt, L. Reyes, and S. Suryanarayanan, "Powering through the storm: Microgrids operation for more efficient disaster recovery," *IEEE Power Energy Mag.*, vol. 12, no. 3, pp. 67–76, May 2014.

[75] A. Gholami, F. Aminifar, and M. Shahidehpour, "Front lines against the darkness: Enhancing the resilience of the electricity grid through microgrid facilities," *IEEE Electrific. Mag.*, vol. 4, no. 1, pp. 18–24, Mar. 2016.

[76] J. A. P. Lopes, N. Hatziargyriou, J. Mutale, P. Djapic, and N. Jenkins, "Integrating distributed generation into electric power systems: A review of drivers, challenges and opportunities," *Electr. Power Syst. Res.*, vol. 77, no. 9, pp. 1189–1203, Jul. 2007.

[77] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.

[78] F. Nejabatkhah, Y. W. Li, H. Liang, and R. R. Ahrabi, "Cyber-security of smart microgrids: A survey," *Energies*, vol. 14, no. 1, p. 27, Dec. 2020.

[79] J. Antoun, M. E. Kabir, B. Moussa, R. Atallah, and C. Assi, "A detailed security assessment of the EV charging ecosystem," *IEEE Netw.*, vol. 34, no. 3, pp. 200–207, May 2020.

[80] B. Yagcitekin, M. Uzunoglu, B. Ocal, E. Turan, and A. Tunc, "Development of smart charging strategies for electric vehicles in a campus area," in *Proc. Eur. Model. Symp.*, Nov. 2013, pp. 432–436.

[81] M. Bilal and M. Rizwan, "Electric vehicles in a smart grid: A comprehensive survey on optimal location of charging station," *IET Smart Grid*, vol. 3, no. 3, pp. 267–279, Jun. 2020.

[82] Q. Wang, X. Liu, J. Du, and F. Kong, "Smart charging for electric vehicles: A survey from the algorithmic perspective," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1500–1517, 2nd Quart., 2016.

[83] S. Mehar, S. Zeadally, G. Rémy, and S. M. Senouci, "Sustainable transportation management system for a fleet of electric vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 3, pp. 1401–1414, Jun. 2015.

[84] M. Ahmadi, N. Mithulananthan, and R. Sharma, "A review on topologies for fast charging stations for electric vehicles," in *Proc. IEEE Int. Conf. Power Syst. Technol. (POWERCON)*, Wollongong, NSW, Australia, Sep. 2016, pp. 1–6.

[85] Y. Cao, O. Kaiwartya, Y. Zhuang, N. Ahmad, Y. Sun, and J. Lloret, "A decentralized deadline-driven electric vehicle charging recommendation," *IEEE Syst. J.*, vol. 13, no. 3, pp. 3410–3421, Sep. 2019.

[86] A. Pan, T. Zhao, H. Yu, and Y. Zhang, "Deploying public charging stations for electric taxis: A charging demand simulation embedded approach," *IEEE Access*, vol. 7, pp. 17412–17424, 2019.

[87] E.-F. Ibrahim, K. Driss, and A. Rachid, "Framework for optimizing the charging time of electric vehicles in public supply station deployed in smart cities," in *Proc. IEEE 5th Int. Congr. Inf. Sci. Technol. (CiSt)*, Oct. 2018, pp. 537–541.

[88] Z. Bendiabdellah, S. M. Senouci, and M. Feham, "A hybrid algorithm for planning public charging stations," in *Proc. Global Inf. Infrastruct. Netw. Symp. (GIIS)*. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers, Sep. 2014, pp. 1–3.

[89] V. Bobanac, H. Pandzic, and T. Capuder, "Survey on electric vehicles and battery swapping stations: Expectations of existing and future EV owners," in *Proc. IEEE Int. Energy Conf. (ENERGYCON)*, Jun. 2018, pp. 1–6.

[90] G. Yatnalkar and H. Narman, "Survey on wireless charging and placement of stations for electric vehicles," in *Proc. IEEE Int. Symp. Signal Process. Inf. Technol. (ISSPIT)*, Dec. 2018, pp. 526–531.

[91] Y. J. Jang, "Survey of the operation and system study on wireless charging electric vehicle systems," *Transp. Res. C, Emerg. Technol.*, vol. 95, pp. 844–866, Oct. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0968090X18304649

[92] K. Clement-Nyns, E. Haesen, and J. Driesen, "The impact of charging plug-in hybrid electric vehicles on a residential distribution grid," *IEEE Trans. Power Syst.*, vol. 25, no. 1, pp. 371–380, Feb. 2010.

[93] O. Yarkoni. *The Hidden Cyber Risks of Electric Vehicles*. Accessed: Feb. 2, 2024. [Online]. Available: https://upstream.auto/blog/the-hidden-cyber-risks-of-electric-vehicles/

[94] G. A. Putrus, P. Suwanapingkarl, D. Johnston, E. C. Bentley, and M. Narayana, "Impact of electric vehicles on power distribution networks," in *Proc. IEEE Vehicle Power Propuls. Conf.*, Sep. 2009, pp. 827–831.

[95] C. Hodge, K. Hauck, S. Gupta, and J. Bennett, "Vehicle cybersecurity threats and mitigation approaches," Nat. Renew. Energy Lab., U.S. Dept. Energy, Tech. Rep. NREL/TP-5400-74247, Aug. 2019.

[96] A. C.-F. Chan and J. Zhou, "A secure, intelligent electric vehicle ecosystem for safe integration with the smart grid," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 3367–3376, Dec. 2015.

[97] D. Schuler, G. Gabba, L. Kung, and V. Peter, "How a city prepares to e-mobility in terms of public charging infrastructure case study—The city of Zurich," in *Proc. World Electr. Vehicle Symp. Exhib. (EVS27)*, Nov. 2013, pp. 1–7.

[98] Equiterre. (2020). *The Running Electric 2020 Brochure Choose a Vehicle That Meets Your Needs*. [Online]. Available: https://vehiculeselectriques.gouv.qc.ca/assets/pdf/english/Brochure-running-electric-EN-2020.pdf

[99] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, "Review of Internet of Things (IoT) in electric power and energy systems," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 847–870, Apr. 2018.

[100] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *J. Cleaner Prod.*, vol. 140, pp. 1454–1464, Jan. 2017.

[101] C. Bekara, "Security issues and challenges for the IoT-based smart grid," *Proc. Comput. Sci.*, vol. 34, pp. 532–537, Jan. 2014.

[102] T. T. Tesfay, "Cybersecurity solutions for active power distribution networks," M.S. thesis, EPFL, Lausanne, Switzerland, 2017.

[103] O. Alexander, M. Belisle, and J. Steele, "Mitre ATT&CK for industrial control systems: Design and philosophy," MITRE Corp., McLean, VA, USA, Tech. Rep. MP01055863, 2020.

[104] *7628 Revision 1-Guidelines for Smart Grid Cyber Security*, Smart Grid Testing P.-S. Grid and Certification Committee NISTIR, Gaithersburg, MD, USA, 2014, vol. 1–3.

[105] R. R. Nejad and W. Sun, "Distributed load restoration in unbalanced active distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5759–5769, Sep. 2019.

[106] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R. B. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated volt/VAR control and countermeasures," in *Proc. Amer. Control Conf.*, Jun. 2014, pp. 4372–4378.

[107] R. Fu, X. Huang, Y. Xue, Y. Wu, Y. Tang, and D. Yue, "Security assessment for cyber physical distribution power system under intrusion attacks," *IEEE Access*, vol. 7, pp. 75615–75628, 2019.

[108] M. Bai, W. Sheng, Y. Liang, K. Liu, X. Ye, T. Kang, Y. Wang, and Y. Zhao, "Research on distribution network fault simulation based on cyber physics system," in *Proc. IEEE 3rd Int. Electr. Energy Conf. (CIEEC)*, Sep. 2019, pp. 1112–1116.

[109] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, "Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1330–1339, May 2017.

[110] G. Cao, "Operational Risk Evaluation of Active Distribution Networks Considering Cyber Contingencies," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 3849–3861, Jun. 2020.

[111] E. Shereen, M. Delcourt, S. Barreto, G. Dán, J. Le Boudec, and M. Paolone, "Feasibility of time-synchronization attacks against PMU-based state estimation," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 6, pp. 3412–3427, Jun. 2020.

[112] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Domı'nguez-Garcı'a, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3253–3262, Aug. 2013.

[113] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," *SANS Inst. InfoSec Reading Room*, vol. 1, p. 24, Oct. 2015.

[114] E. M. Hutchins, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues Inf. Warfare Secur. Res.*, vol. 1, no. 1, p. 80, 2011.

[115] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, Jul. 2013.

[116] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state estimation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1460–1470, Jul. 2014.

[117] F. Skopik and P. D. Smith, *Smart Grid Security: Innovative Solutions for a Modernized Grid*. Rockland, MA, USA: Syngress, 2015.

[118] S. Ntalampiras, "Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling," *IEEE Trans. Ind. Informat.*, vol. 11, no. 1, pp. 104–111, Feb. 2015.

[119] A. Kemmeugne, M. Khalaf, M. Au, and D. Kundur, "Mitigation of denial of service and time delay attacks on the automatic generation control of power systems," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, Sep. 2023, pp. 410–415.

[120] T. T. Tesfay, J.-P. Hubaux, J.-Y. Le Boudec, and P. Oechslin, "Cyber-secure communication architecture for active power distribution networks," in *Proc. 29th Annu. ACM Symp. Appl. Comput.*, Mar. 2014, pp. 545–552.

[121] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1871–1879.

[122] D. Jin, D. M. Nicol, and G. Yan, "An event buffer flooding attack in DNP3 controlled SCADA systems," in *Proc. Winter Simul. Conf. (WSC)*, Dec. 2011, pp. 2614–2626.

[123] A. Huseinovic, S. Mrdovic, K. Bicakci, and S. Uludag, "A survey of denial-of-service attacks and solutions in the smart grid," *IEEE Access*, vol. 8, pp. 177447–177470, 2020.

[124] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods," *IEEE Access*, vol. 7, pp. 51691–51713, 2019.

[125] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, p. 13, Jun. 2011.

[126] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[127] M. Khalaf, A. Ayad, M. M. A. Salama, D. Kundur, and E. F. El-Saadany, "Mitigation of cyber-attacks on wide-area under-frequency load-shedding schemes," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2377–2389, May 2023.

[128] M. Khalaf, A. Ayad, and D. Kundur, "Protection of power system state estimation against false data injection attacks," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, Sep. 2023, pp. 387–392.

[129] Y. Li and Y. Wang, "False data injection attacks with incomplete network topology information in smart grid," *IEEE Access*, vol. 7, pp. 3656–3664, 2019.

[130] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

[131] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[132] S. Bi and Y. J. Zhang, "Using covert topological information for defense against malicious attacks on DC state estimation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1471–1485, Jul. 2014.

[133] A. Tarali and A. Abur, "Bad data detection in two-stage state estimation using phasor measurements," in *Proc. 3rd IEEE PES Innov. Smart Grid Technol. Eur. (ISGT Eur.)*, Oct. 2012, pp. 1–8.

[134] J. Huddleston, P. Ji, S. Bhunia, and J. Cogan, "How VMware exploits contributed to SolarWinds supply-chain attack," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2021, pp. 760–765.

[135] J. Martínez and J. M. Durán, "Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study," *Int. J. Safety Security Eng.*, vol. 11, no. 5, pp. 537–545, 2021.

[136] R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, "Solar winds hack: In-depth analysis and countermeasures," in *Proc. 12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2021, pp. 1–7.

[137] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Secur. Privacy*, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.

[138] V. Delgado-Gomes, J. F. Martins, C. Lima, and P. N. Borza, "Smart grid security issues," in *Proc. 9th Int. Conf. Compat. Power Electron. (CPE)*, Jun. 2015, pp. 534–538.

[139] I. H. Lim, S. Hong, M. S. Choi, S. J. Lee, T. W. Kim, S. W. Lee, and B. N. Ha, "Security protocols against cyber attacks in the distribution automation system," *IEEE Trans. Power Del.*, vol. 25, no. 1, pp. 448–455, Jan. 2010.

[140] T. Mander, L. Wang, R. Cheung, and F. Nabhani, "Adapting the pretty good privacy security style to power system distributed network protocol," in *Proc. Large Eng. Syst. Conf. Power Eng.*, Jul. 2006, pp. 79–83.

[141] T. Mander, F. Nabhani, L. Wang, and R. Cheung, "Integrated network security protocol layer for open-access power distribution systems," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jun. 2007, pp. 1–8.

[142] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.

[143] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in *Proc. SoutheastCon*, Apr. 2015, pp. 1–6.

[144] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. F. Wang, "Impact of cyber-security issues on smart grid," in *Proc. 2nd IEEE PES Int. Conf. Exhib. Innov. Smart Grid Technol.*, Dec. 2011, pp. 1–7.

[145] K. Bhat, V. Sundarraj, S. Sinha, and A. Kaul, "Smart grid research: Cyber security—IEEE cyber security for the smart grid," *IEEE Cyber Secur. Smart Grid*, pp. 1–122, Sep. 2013, doi: 10.1109/IEEESTD.2013.6613505.

[146] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. R. Al Ali, "Smart grid cyber security: Challenges and solutions," in *Proc. Int. Conf. Smart Grid Clean Energy Technol. (ICSGCE)*, Oct. 2015, pp. 170–175.

[147] S. Basumallik, S. Eftekharnejad, N. Davis, N. Nuthalapati, and B. K. Johnson, "Cyber security considerations on PMU-based state estimation," in *Proc. 5th Cybersecurity Symp.*, Apr. 2018, p. 14.

[148] A. Ayad, H. E. Z. Farag, A. Youssef, and E. F. El-Saadany, "Detection of false data injection attacks in smart grids using recurrent neural networks," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Jun. 2018, pp. 1–5.

[149] S. Soltan, M. Yannakakis, and G. Zussman, "Joint cyber and physical attacks on power grids: Graph theoretical approaches for information recovery," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 43, no. 1, pp. 361–374, Jun. 2015.

[150] Z. Lian, F. Guo, C. Wen, C. Deng, and P. Lin, "Distributed resilient optimal current sharing control for an Islanded DC Microgrid under DoS attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4494–4505, Sep. 2021.

[151] S. Weng, D. Yue, J. Chen, X. Xie, and C. Dou, "Distributed resilient self-triggered cooperative control for multiple photovoltaic generators under denial-of-service attack," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 53, no. 1, pp. 226–237, Jan. 2023.

[152] L. Tightiz and H. Yang, "A comprehensive review on IoT Protocols' features in smart grid communication," *Energies*, vol. 13, no. 11, p. 2762, Jun. 2020.

[153] E. Kabalci and Y. Kabalci, *Smart Grids and Their Communication Systems*. Cham, Switzerland: Springer, 2019.

[154] R. Leszczyna, "A review of standards with cybersecurity requirements for smart grid," *Comput. Security*, vol. 77, pp. 262–276, Aug. 2018.

[155] *Power Systems Management and Associated Information Exchange Data and Communications Security—Part 3: Communication Network and System Security—Profiles Including TCP/IP*, International Electrotechnical Commission (IEC), London, U.K., 2014.

[156] *Power Systems Management and Associated Information Exchange Data and Communications Security—Part 4: Profiles Including Mms and Derivatives*, International Electrotechnical Commission (IEC), London, U.K., 2018.

[157] *Power Systems Management and Associated Information Exchange Data and Communications Security—Part 5: Security for IEC 60870-5 and Derivatives*, International Electrotechnical Commission (IEC), London, U.K., 2013.

[158] *Power Systems Management and Associated Information Exchange Data and Communications Security—Part 6: Security for IEC 61850*, International Electrotechnical Commission (IEC), London, U.K., 2007.

[159] *Power Systems Management And Associated Information Exchange-Data and Communications Security—Part 7: Network and System Management (NSM) Data Object Model*, International Electrotechnical Commission (IEC), London, U.K., 2017.

[160] *Power Systems Management and Associated Information Exchange Data and Communications Security—Part 8: Role-Based Access Control*, International Electrotechnical Commission (IEC), London, U.K., 2011.

[161] *Power Systems Management and Associated Information Exchange Data and Communications Security—Part 9: Cyber Security Key Management for Power System Equipment*, International Electrotechnical Commission (IEC), London, U.K., 2017.

[162] *Power Systems Management and Associated Information Exchange Data and Communications Security—Part 11: Security for XML Documents*, International Electrotechnical Commission (IEC), London, U.K., 2016.

[163] *Power Systems Management And Associated Information Exchange Data and Communications Security—Part 12: Resilience and Security Recommendations for Power Systems With Distributed Energy Resources (DER) Cyber-Physical Systems*, International Electrotechnical Commission (IEC), London, U.K., 2016.

[164] *Power Systems Management and Associated Information Exchange Data and Communications Security—Part 90-2: Deep Packet Inspection of Encrypted Communications*, International Electrotechnical Commission (IEC), London, U.K., 2018.

[165] E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls Into the Modern Power Infrastructure*. San Francisco, CA, USA: Newnes, 2013.

[166] *Security for Industrial Automation and Control Systems—Part 2–3: Patch Management in the IACS Environment*, International Electrotechnical Commission (IEC), London, U.K., 2015.

[167] *Industrial Communication Networks Network and System Security—Part 3-1: Security Technologies for Industrial Automation and Control Systems*, International Electrotechnical Commission (IEC), London, U.K., 2009.

[168] *Industrial Communication Networks Network and System Security—Part 3-3: System Security Requirements and Security Levels*, International Electrotechnical Commission (IEC), London, U.K., 2013.

[169] *Security for Industrial Automation and control Systems—Part 4–1: Secure Product Development Lifecyle Requirements*, International Electrotechnical Commission (IEC), London, U.K., 2018.

[170] *IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities*, Standard IEEE Std 1686-2013 (Revision IEEE Std 1686-2007), 2014, pp. 1–29.

[171] *IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems*, Standard IEEE C37.240-2014, 2015, pp. 1–38.

[172] E. Shereen and G. Dán, "Model-based and data-driven detectors for time synchronization attacks against PMUs," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 1, pp. 169–179, Jan. 2020.

[173] S. Mousavian, J. Valenzuela, and J. Wang, "A probabilistic risk mitigation model for cyber-attacks to PMU networks," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 156–165, Jan. 2015.

[174] D. Backer, "Power quality and asset management the other 'two-thirds' of AMI value," in *Proc. IEEE Rural Electr. Power Conf.*, May 2007, p. C6.

[175] F. M. Cleveland, "Cyber security issues for advanced metering infrasttructure (AMI)," in *Proc. IEEE Power Energy Soc. Gen. Meeting Convers. Del. Electr. Energy 21st Century*, Jul. 2008, pp. 1–5.

[176] S. Wang, D. Liang, L. Ge, and X. Wang, "Analytical FRTU deployment approach for reliability improvement of integrated cyber-physical distribution systems," *IET Gener., Transmiss. Distrib.*, vol. 10, no. 11, pp. 2631–2639, Aug. 2016.

[177] V. V. G. Krishnan, S. Gopal, Z. Nie, and A. Srivastava, "Cyber-power testbed for distributed monitoring and control," in *Proc. Workshop Modeling Simulation Cyber-Phys. Energy Syst. (MSCPES)*, Apr. 2018, pp. 1–6.

[178] Y. H. Chang, P. Jirutitijaroen, and C.-W. Ten, "A simulation model of cyber threats for energy metering devices in a secondary distribution network," in *Proc. 5th Int. Conf. Crit. Infrastruct. (CRIS)*, Sep. 2010, pp. 1–7.

[179] D. S. Callaway and I. A. Hiskens, "Achieving controllability of electric loads," *Proc. IEEE*, vol. 99, no. 1, pp. 184–199, Jan. 2011.

[180] S. Yorukoglu, F. Nasibov, M. Mungan, and M. Bagriyanik, "The effect of the types of network topologies on nontechnical losses in secondary electricity distribution systems," *IEEE Trans. Ind. Appl.*, vol. 52, no. 5, pp. 3631–3643, Sep. 2016.

[181] M. Madrigal, J. J. Rico, and L. Uzcategui, "Estimation of non-technical energy losses in electrical distribution systems," *IEEE Latin Amer. Trans.*, vol. 15, no. 8, pp. 1447–1452, May 2017.

[182] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Sci. Technol.*, vol. 19, no. 2, pp. 105–120, Apr. 2014.

[183] C.-H. Lo and N. Ansari, "CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 1, pp. 33–44, Jun. 2013.

[184] Y. Zhou, X. Chen, A. Y. Zomaya, L. Wang, and S. Hu, "A dynamic programming algorithm for leveraging probabilistic detection of energy theft in smart home," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 4, pp. 502–513, Dec. 2015.

[185] Y. Guo, C.-W. Ten, and P. Jirutitijaroen, "Online data validation for distribution operations against cybertampering," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 550–560, Mar. 2014.

[186] Z. Xiao, Y. Xiao, and D. H. C. Du, "Exploring malicious meter inspection in neighborhood area smart grids," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 214–226, Mar. 2013.

[187] C. Liao, C.-W. Ten, and S. Hu, "Strategic FRTU deployment considering cybersecurity in secondary distribution network," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1264–1274, Sep. 2013.

[188] S.-C. Yip, K. Wong, W.-P. Hew, M.-T. Gan, R. C.-W. Phan, and S.-W. Tan, ''Detection of energy theft and defective smart meters in smart grids using linear regression,'' *Int. J. Electr. Power Energy Syst.*, vol. 91, pp. 230–240, Oct. 2017.

[189] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and F. Nagi, ''Improving SVM-based nontechnical loss detection in power utility using the fuzzy inference system,'' *IEEE Trans. Power Del.*, vol. 26, no. 2, pp. 1284–1285, Apr. 2011.

[190] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and M. Mohamad, ''Nontechnical loss detection for metered customers in power utility using support vector machines,'' *IEEE Trans. Power Del.*, vol. 25, no. 2, pp. 1162–1171, Apr. 2010.

[191] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and R. C. Green, ''High performance computing for detection of electricity theft,'' *Int. J. Electr. Power Energy Syst.*, vol. 47, pp. 21–30, May 2013.

[192] E. W. S. Angelos, O. R. Saavedra, O. A. C. Cortés, and A. N. de Souza, ''Detection and identification of abnormalities in customer consumptions in power distribution systems,'' *IEEE Trans. Power Del.*, vol. 26, no. 4, pp. 2436–2442, Oct. 2011.

[193] W. Han and Y. Xiao, ''NFD: A practical scheme to detect non-technical loss fraud in smart grid,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 605–609.

[194] P. Jokar, N. Arianpoo, and V. C. M. Leung, ''Electricity theft detection in AMI using customers' consumption patterns,'' *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016.

[195] S. Salinas, M. Li, and P. Li, ''Privacy-preserving energy theft detection in smart grids: A P2P computing approach,'' *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 257–267, Sep. 2013.

[196] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, ''A multi-sensor energy theft detection framework for advanced metering infrastructures,'' *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1319–1330, Jul. 2013.

[197] Z. Xiao, Y. Xiao, and D. H. C. Du, ''Non-repudiation in neighborhood area networks for smart grid,'' *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 18–26, Jan. 2013.

[198] S.-C. Huang, Y.-L. Lo, and C.-N. Lu, ''Non-technical loss detection using state estimation and analysis of variance,'' *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2959–2966, Aug. 2013.

[199] B. Khoo and Y. Cheng, ''Using RFID for anti-theft in a Chinese electrical supply company: A cost-benefit analysis,'' in *Proc. Wireless Telecommun. Symp. (WTS)*, Apr. 2011, pp. 1–6.

[200] S. Amin, G. A. Schwartz, and H. Tembine, ''Incentives and security in electricity distribution networks,'' in *Proc. Int. Conf. Decis. Game Theory Secur.* Cham, Switzerland: Springer, 2012, pp. 264–280.

[201] A. A. Cárdenas, S. Amin, G. Schwartz, R. Dong, and S. Sastry, ''A game theory model for electricity theft detection and privacy-aware control in AMI systems,'' in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1830–1837.

[202] J. B. Leite and J. R. S. Mantovani, ''Detecting and locating non-technical losses in modern distribution networks,'' *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1023–1032, Mar. 2018.

[203] D. Gutierrez-Rojas, P. H. J. Nardelli, G. Mendes, and P. Popovski, ''Review of the state of the art on adaptive protection for microgrids based on communications,'' *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 1539–1552, Mar. 2021.

[204] P. H. A. Barra, D. V. Coury, and R. A. S. Fernandes, ''A survey on adaptive protection of microgrids and distribution systems with distributed generators,'' *Renew. Sustain. Energy Rev.*, vol. 118, Feb. 2020, Art. no. 109524.

[205] S. Ward, ''Cyber security issues for protective relays; c1 working group members of power system relaying committee,'' in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jun. 2007, pp. 1–8.

[206] A. Hansen, J. Staggs, and S. Shenoi, ''Security analysis of an advanced metering infrastructure,'' *Int. J. Crit. Infrastruct. Protection*, vol. 18, pp. 3–19, Sep. 2017.

[207] D. Holstein, T. Cease, H. L. Li, and A. Meneses, ''The impact of implementing cyber security requirements using IEC 61850,'' Electra, CIGRE Work. Group B5.38, pp. 1–83, 2010.

[208] H. F. Habib, A. O. Hariri, A. ElSayed, and O. A. Mohammed, ''Deployment of electric vehicles in an adaptive protection technique for riding through cyber attack threats in microgrids,'' in *Proc. IEEE Int. Conf. Environ. Electr. Eng. IEEE Ind. Commercial Power Syst. Eur. (EEEIC/I&CPS Eur.)*, Jun. 2017, pp. 1–6.

[209] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, ''Power system risk assessment in cyber attacks considering the role of protection systems,'' *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 572–580, Mar. 2017.

[210] A. A. Jahromi, A. Kemmeugne, D. Kundur, and A. Haddadi, ''Cyber-physical attacks targeting communication-assisted protection schemes,'' *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 440–450, Jan. 2020.

[211] M. Z. Jahromi, A. A. Jahromi, S. Sanner, D. Kundur, and M. Kassouf, ''Cybersecurity enhancement of transformer differential protection using machine learning,'' in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2020, pp. 1–5.

[212] Y. M. Khaw, A. Abiri Jahromi, M. F. M. Arani, S. Sanner, D. Kundur, and M. Kassouf, ''A deep learning-based cyberattack detection system for transmission protective relays,'' *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2554–2565, May 2021.

[213] Y. Isozaki, ''Detection of cyber attacks against voltage control in distribution power grids with PVs,'' *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1824–1835, Jul. 2016.

[214] D. P. Chassin, K. Schneider, and C. Gerkensmeyer, ''GridLAB-D: An open-source power systems modeling and simulation environment,'' in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo.*, Apr. 2008, pp. 1–5.

[215] A. Majumdar, Y. P. Agalgaonkar, B. C. Pal, and R. Gottschalg, ''Centralized Volt–Var optimization strategy considering malicious attack on distributed energy resources control,'' *IEEE Trans. Sustain. Energy*, vol. 9, no. 1, pp. 148–156, Jan. 2018.

[216] J. Wang, L. C. K. Hui, S. M. Yiu, E. K. Wang, and J. Fang, ''A survey on cyber attacks against nonlinear state estimation in power systems of ubiquitous cities,'' *Pervas. Mobile Comput.*, vol. 39, pp. 52–64, Aug. 2017.

[217] J. Liang, O. Kosut, and L. Sankar, ''Cyber attacks on AC state estimation: Unobservability and physical consequences,'' in *Proc. IEEE PES Gen. Meeting | Conf. Expo.*, Jul. 2014, pp. 1–5.

[218] M. E. Baran and A. W. Kelley, ''A branch-current-based state estimation method for distribution systems,'' *IEEE Trans. Power Syst.*, vol. 10, no. 1, pp. 483–491, Feb. 1995.

[219] E. Liu and P. Cheng, ''Mitigating cyber privacy leakage for distributed DC optimal power flow in smart grid with radial topology,'' *IEEE Access*, vol. 6, pp. 7911–7920, 2018.

[220] X. Zhang, X. Yang, J. Lin, and W. Yu, ''On false data injection attacks against the dynamic microgrid partition in the smart grid,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7222–7227.

[221] A. Mohamed, M. Khalaf, and D. Kundur, ''On the use of safety critical control for cyber-physical security in the smart grid,'' in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2023, pp. 1–5.

[222] S. Liu, P. X. Liu, and X. Wang, ''Effects of cyber attacks on islanded microgrid frequency control,'' in *Proc. IEEE 20th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2016, pp. 461–464.

[223] K. Shi, X. Cai, K. She, S. Zhong, Y. Soh, and O. Kwon, ''Quantized memory proportional–integral control of active power sharing and frequency regulation in island microgrid under abnormal cyber attacks,'' *Appl. Energy*, vol. 322, Sep. 2022, Art. no. 119540.

[224] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, ''Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks,'' in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.

[225] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, ''Distributed load sharing under false data injection attack in an inverter-based microgrid,'' *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1543–1551, Feb. 2019.

[226] A. Teixeira, K. Paridari, H. Sandberg, and K. H. Johansson, ''Voltage control for interconnected microgrids under adversarial actions,'' in *Proc. IEEE 20th Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2015, pp. 1–8.

[227] O. A. Beg, T. T. Johnson, and A. Davoudi, ''Detection of false-data injection attacks in cyber-physical DC microgrids,'' *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.

[228] V. Kounev, D. Tipper, A. A. Yavuz, B. M. Grainger, and G. F. Reed, ''A secure communication architecture for distributed microgrid control,'' *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2484–2492, Sep. 2015.

[229] M. M. Rana, L. Li, and S. W. Su, ''Cyber attack protection and control of microgrids,'' *IEEE/CAA J. Autom. Sinica*, vol. 5, no. 2, pp. 602–609, Mar. 2018.

[230] D. Jin, Z. Li, C. Hannon, C. Chen, J. Wang, M. Shahidehpour, and C. W. Lee, "Toward a cyber resilient and secure microgrid using software-defined networking," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2494–2504, Sep. 2017.

[231] A. Sundararajan, A. Chavan, D. Saleem, and A. Sarwat, "A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security," *Energies*, vol. 11, no. 9, p. 2360, Sep. 2018.

[232] L. Yuanliang and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Trans. Power Electron.*, vol. 38, no. 2, pp. 2364–2383, Feb. 2023.

[233] J. Johnson, B. Fox, K. Kaur, and J. Anandan, "Evaluation of interoperable distributed energy resources to IEEE 1547.1 using SunSpec modbus, IEEE 1815, and IEEE 2030.5," *IEEE Access*, vol. 9, pp. 142129–142146, 2021.

[234] J. Obert, P. Cordeiro, J. T. Johnson, G. Lum, T. Tansy, N. Pala, and R. Ih, "Recommendations for trust and encryption in der interoperability standards," Kitu Syst., Sandia National Lab. (SNL-NM), Albuquerque, NM, USA, Tech. Rep. SAND2019-1490, 2019.

[235] C. Carter, C. Lai, N. Jacobs, S. Hossain-McKenzie, P. Cordeiro, I. Onunkwo, and J. T. Johnson, "Cyber security primer for der vendors aggregators and grid operators," Sandia Nat. Lab. (SNL-NM), Albuquerque, NM, USA, Tech. Rep. SAND2017-13113, 2017.

[236] D. Shelar and S. Amin, "Security assessment of electricity distribution networks under DER node compromises," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 23–36, Mar. 2017.

[237] B. Kang, "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," in *Proc. IEEE 20th Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2015, pp. 1–8.

[238] Y. Liu, H. Xin, Z. Qu, and D. Gan, "An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2923–2932, Nov. 2016.

[239] P. Li, Y. Liu, H. Xin, and X. Jiang, "A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4343–4352, Oct. 2018.

[240] J. Qi, A. Hahn, X. Lu, J. Wang, and C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 28–39, Dec. 2016.

[241] M. Chlela, D. Mascarella, G. Joós, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702–4711, Sep. 2018.

[242] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Smart electric vehicle charging: Security analysis," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2013, pp. 1–6.

[243] S. Acharya, Y. Dvorkin, H. Pandžic, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214434–214453, 2020.

[244] R. Gottumukkala, R. Merchant, A. Tauzin, K. Leon, A. Roche, and P. Darby, "Cyber-physical system security of vehicle charging stations," in *Proc. IEEE Green Technol. Conf. (GreenTech)*, Apr. 2019, pp. 1–5.

[245] B. Vaidya and H. T. Mouftah, "Deployment of secure EV charging system using open charge point protocol," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 922–927.

[246] D. Reeh, F. Cruz Tapia, Y.-W. Chung, B. Khaki, C. Chu, and R. Gadh, "Vulnerability analysis and risk assessment of EV charging system under cyber-physical threats," in *Proc. IEEE Transp. Electrific. Conf. Expo. (ITEC)*, Jun. 2019, pp. 1–6.

[247] J. Schmutzler, C. A. Andersen, and C. Wietfeld, "Evaluation of OCPP and IEC 61850 for smart charging electric vehicles," in *Proc. World Electr. Vehicle Symp. Exhib. (EVS27)*, Nov. 2013, pp. 1–12.

[248] B. Vaidya and H. T. Mouftah, "Multimodal and multi-pass authentication mechanisms for electric vehicle charging networks," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 371–376.

[249] K. Hänsch, A. Pelzer, P. Komarnicki, S. Gröning, J. Schmutzler, C. Wietfeld, J. Heuer, and R. Müller, "An ISO/IEC 15118 conformance testing system architecture," in *Proc. IEEE PES Gen. Meeting | Conf. Expo.*, Jul. 2014, pp. 1–5.

[250] P. Nsonga, S. M. S. Hussain, I. Ali, and T. S. Ustun, "Using IEC 61850 and IEEE WAVE standards in ad-hoc networks for electric vehicle charging management," in *Proc. IEEE Online Conf. Green Commun. (OnlineGreenComm)*, Nov. 2016, pp. 39–44.

[251] Y. Xiong, B. Wang, Z. Cao, C.-c. Chu, H. Pota, and R. Gadh, "Extension of IEC61850 with smart EV charging," in *Proc. IEEE Innov. Smart Grid Technol. Asia (ISGT-Asia)*, Nov. 2016, pp. 294–299.

[252] ElaadNL. *EV Related Protocol Study*. Accessed: Mar. 2, 2023. [Online]. Available: https://www.elaad.nl/uploads/downloads/downloads_download/EV_related_protocol_study_v1.1.pdf

[253] D. Kettles. *Electric Vehicle Charging Technology Analysis and Standards*. Accessed: Mar. 2, 2023. [Online]. Available: http://enerjiye.com/en/wp-content/uploads/2018/12/FSEC-CR-1996-15.pdf

[254] J. C. Gómez and M. M. Morcos, "Impact of EV battery chargers on the power quality of distribution systems," *IEEE Trans. Power Del.*, vol. 18, no. 3, pp. 975–981, Jul. 2003.

[255] S. Rahman, I. A. Khan, and M. H. Amini, "A review on impact analysis of electric vehicle charging on power distribution systems," in *Proc. 2nd Int. Conf. Smart Power Internet Energy Syst. (SPIES)*, Sep. 2020, pp. 420–425.

[256] Y.-J. Liu, T.-P. Chang, H.-W. Chen, T.-K. Chang, and P.-H. Lan, "Power quality measurements of low-voltage distribution system with smart electric vehicle charging infrastructures," in *Proc. 16th Int. Conf. Harmon. Quality Power (ICHQP)*, May 2014, pp. 631–635.

[257] H. Zhang, Y. Pan, Z. Lu, J. Wang, and Z. Liu, "A cyber security evaluation framework for in-vehicle electrical control units," *IEEE Access*, vol. 9, pp. 149690–149706, 2021.

[258] O. G. M. Khan, E. El-Saadany, A. Youssef, and M. Shaaban, "Impact of electric vehicles botnets on the power grid," in *Proc. IEEE Electr. Power Energy Conf. (EPEC)*, Oct. 2019, pp. 1–5.

[259] Y. Zheng, Z. Y. Dong, Y. Xu, K. Meng, J. H. Zhao, and J. Qiu, "Electric vehicle battery charging/swap stations in distribution systems: Comparison study and optimal planning," *IEEE Trans. Power Syst.*, vol. 29, no. 1, pp. 221–229, Jan. 2014.

[260] L. P. Fernandez, T. G. S. Roman, R. Cossent, C. M. Domingo, and P. Frias, "Assessment of the impact of plug-in electric vehicles on distribution networks," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 206–213, Feb. 2011.

[261] S. Shafiee, M. Fotuhi-Firuzabad, and M. Rastegar, "Investigating the impacts of plug-in hybrid electric vehicles on power distribution systems," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1351–1360, Sep. 2013.

[262] M. Yilmaz and P. T. Krein, "Review of the impact of vehicle-to-grid technologies on distribution systems and utility interfaces," *IEEE Trans. Power Electron.*, vol. 28, no. 12, pp. 5673–5689, Dec. 2013.

[263] D. Niyato, D. T. Hoang, P. Wang, and Z. Han, "Cyber insurance for plug-in electric vehicle charging in Vehicle-to-Grid systems," *IEEE Netw.*, vol. 31, no. 2, pp. 38–46, Mar. 2017.

[264] S. Pirouzi, J. Aghaei, M. Shafie-khah, G. J. Osório, and J. P. S. Catalão, "Evaluating the security of electrical energy distribution networks in the presence of electric vehicles," in *Proc. IEEE Manchester PowerTech*, Jun. 2017, pp. 1–6.

[265] J. E. Rubio, C. Alcaraz, and J. Lopez, "Addressing security in OCPP: Protection against man-in-the-middle attacks," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Feb. 2018, pp. 1–5.

[266] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Trans. Syst. Man, Cybern., Syst.*, vol. 50, no. 1, pp. 43–57, Jan. 2020.

[267] C. Niddodi, S. Lin, S. Mohan, and H. Zhu, "Secure integration of electric vehicles with the power grid," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2019, pp. 1–7.

[268] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for V2G using physical unclonable function," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7234–7246, Jul. 2020.

[269] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable?" *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5099–5113, Nov. 2020.

[270] Y. Zhang, Y. Jiang, A. Xu, C. Hong, and J. Chen, "Method to evaluate the impact of cyberattacks against charging piles on distribution network," in *Proc. 12th IEEE PES Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Sep. 2020, pp. 1–5.

[271] S. Bogosyan and M. Gokasan, "Novel strategies for security-hardened BMS for extremely fast charging of BEVs," in *Proc. IEEE 23rd Int. Conf. Intell. Transp. Syst. (ITSC)*, Sep. 2020, pp. 1–7.

[272] K. Park, Y. Park, A. K. Das, S. Yu, J. Lee, and Y. Park, "A dynamic privacy-preserving key management protocol for V2G in social Internet of Things," *IEEE Access*, vol. 7, pp. 76812–76832, 2019.

[273] S. Mousavian, M. Erol-Kantarci, L. Wu, and T. Ortmeyer, "A risk-based optimization model for electric vehicle infrastructure response to cyber attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6160–6169, Nov. 2018.

[274] J. Yang, W. Hao, L. Chen, J. Chen, J. Jin, and F. Wang, "Risk assessment of distribution networks considering the charging-discharging behaviors of electric vehicles," *Energies*, vol. 9, no. 7, p. 560, Jul. 2016. [Online]. Available: https://www.mdpi.com/1996-1073/9/7/560

[275] H. Nafisi, H. A. Abyaneh, and M. Abedi, "Network security perspectives of plug-in hybrid electric vehicles," *Arabian J. Sci. Eng.*, vol. 39, no. 8, pp. 6197–6205, Aug. 2014, doi: 10.1007/s13369-014-1204-6.

[276] S. Abedi, A. Arvani, and R. Jamalzadeh, "Cyber security of plug-in electric vehicles in smart grids: Application of intrusion detection methods," in *Plug in Electric Vehicles in Smart Grids*. Springer, 2015.

[277] H. Su, M. Qiu, and H. Wang, "Secure wireless communication system for smart grid with rechargeable electric vehicles," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 62–68, Aug. 2012.

[278] C. Alcaraz, J. Lopez, and S. Wolthusen, "OCPP protocol: Security threats and challenges," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2452–2459, Sep. 2017.

[279] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 88–98, Aug. 2017.

[280] M. A. Khelif, J. Lorandel, and O. Romain, "Non-invasive I2C hardware trojan attack vector," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT)*, Oct. 2021, pp. 1–6.

[281] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, "Application of big data and machine learning in smart grid, and associated security concerns: A review," *IEEE Access*, vol. 7, pp. 13960–13988, 2019.

[282] R. Heartfield, G. Loukas, A. Bezemskij, and E. Panaousis, "Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1720–1735, 2020.

[283] B. D. Davis, J. C. Mason, and M. Anwar, "Vulnerability studies and security postures of IoT devices: A smart home case study," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10102–10110, Oct. 2020.

[284] J. Mao, S. Zhu, X. Dai, Q. Lin, and J. Liu, "Watchdog: Detecting ultrasonic-based inaudible voice attacks to smart home systems," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8025–8035, Sep. 2020.

[285] C. Lin, D. He, N. Kumar, X. Huang, P. Vijaykumar, and K.-K. R. Choo, "HomeChain: A blockchain-based secure mutual authentication system for smart homes," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 818–829, Feb. 2020.

[286] Y. Liu, Y. Zhou, and S. Hu, "Combating coordinated pricing cyberattack and energy theft in smart home cyber-physical systems," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 3, pp. 573–586, Mar. 2018.

[287] A. J. Alam Majumder, C. B. Veilleux, and J. D. Miller, "A cyber-physical system to detect IoT security threats of a smart home heterogeneous wireless sensor node," *IEEE Access*, vol. 8, pp. 205989–206002, 2020.

[288] J. Chevrette, F. Ellermeier, and J. Janchar, "2018 Strategic directions: Smart cities & utilities report," Black Veatch's, 2018.

[289] T. Sukumara, S. Sudarsan, J. Starck, and T. R. Vittor, "Cyber security–security strategy for distribution management system and security architecture considerations," *CIRED-Open Access Proc. J.*, vol. 2017, no. 1, pp. 2653–2656, 2017.

[290] C. Bisale, R. Falk, S. Fries, and A. Guettinger, "Supporting role-based access control in the digital grid," in *Proc. Int. ETG Congr.*, Nov. 2017, pp. 1–6.

[291] S. E. Laboratories. *Partners and Projects: Focused Research and Development, With Practical Commercial Application*. Accessed: Feb. 2, 2024. [Online]. Available: https://selinc.com/solutions/sfci/partners-and-projects/

[292] B. W. Ang, W. L. Choong, and T. S. Ng, "Energy security: Definitions, dimensions and indexes," *Renew. Sustain. Energy Rev.*, vol. 42, pp. 1077–1093, Feb. 2015.

[293] C.-C. Lee, Z. Yuan, and Q. Wang, "How does information and communication technology affect energy security? International evidence," *Energy Econ.*, vol. 109, May 2022, Art. no. 105969.

[294] F. Teichmann, S. R. Boticiu, and B. S. Sergi, "The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate?" *Int. Cybersecurity Law Rev.*, vol. 4, no. 3, pp. 259–280, Sep. 2023.

[295] L. Gjesvik and K. Szulecki, "Interpreting cyber-energy-security events: Experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout," *Eur. Secur.*, vol. 32, no. 1, pp. 104–124, Jan. 2023.

[296] A. Majumdar and B. C. Pal, "Bad data detection in the context of leverage point attacks in modern power networks," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 2042–2054, May 2018.

MOHSEN KHALAF (Senior Member, IEEE) was born in Asyut, Egypt, in 1990. He received the B.Sc. and M.Sc. degrees in electrical engineering from Assiut University, Asyut, in 2012 and 2015, respectively, and the Ph.D. degree in electrical engineering from the University of Waterloo, Waterloo, ON, Canada, in 2020. He is currently a Postdoctoral Fellow with the University of Toronto, Toronto, ON, Canada, working in collaboration with Hydro Quebec, Montreal, QC, Canada, to identify power systems vulnerabilities against cyber attackers. He is also an Assistant Professor with Assiut University. His research interests include smart grid monitoring, protection and control, distributed generation, and cyber-physical security of power systems. He is also a Registered Professional Engineer with Professional Engineers Ontario, Canada, and the Egyptian Syndicate of Engineering in Egypt.

ABDELRAHMAN AYAD (Graduate Student Member, IEEE) received the B.Sc. degree in electrical power engineering from Alexandria University, Alexandria, Egypt, in 2016, and the M.A.Sc. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2019. He is currently pursuing the Ph.D. degree in electrical engineering with McGill University, Montreal, QC, Canada. He is also a Research Assistant with the Renewable Energy Integration Group, CanmetEnergy, Natural Resources Canada, Varennes, QC, Canada. In 2021, he was a recipient of the Natural Sciences and Engineering Research Council (NSERC) Alexander Graham Bell Canada Graduate Scholarship-Doctoral (CGS-D) and Fonds de Recherche du Québec—Nature et Technologies (FRQNT) Doctoral Scholarship. His main research interests include low-carbon energy systems long-term planning, large-scale renewable energy resources integration, and the applications of machine learning in modern energy systems.

MOSADDEK HOSSAIN KAMAL TUSHAR (Member, IEEE) received the B.Sc. degree in applied physics and electronics and the M.Sc. degree in computer science from Dhaka University, Dhaka, Bangladesh, in 1993 and 1995, respectively, the master's degree in information technology from The University of New South Wales, Sydney, NSW, Australia, in 2006, and the Ph.D. degree in electrical and computer engineering from Concordia University, Montreal, QC, Canada, in May 2017. He was a Postdoctoral Fellow with CIISE, Concordia University, from May 2017 to January 2018, and an NSERC Postdoctoral Fellow with ECE, University of Toronto, Canada, from January 2020 to June 2022. He is currently a Faculty Member of the Department of Computer Science and Engineering, University of Dhaka, Dhaka, Bangladesh. His current research interests include the IoT, embedded systems, smart grid cybersecurity, energy management, network design, game theory, and optimization.

MARTHE KASSOUF received the B.Sc. degree in computer engineering from École Supérieure des Ingénieurs de Beyrouth, Lebanon, in 1997, the M.Sc. degree in computer engineering from École Polytechnique de Montréal, Canada, in 1999, and the Ph.D. degree in electrical engineering from McGill University, Canada, in 2008. Since 2008, she has been a Researcher with the Hydro Quebec Research Institute (IREQ), where she has been contributing to the implementation of different projects aiming at the enhancement of the information and telecommunications infrastructure supporting the power grid, mainly in the areas of wireless communication systems, time synchronization, and cybersecurity. She has been the Project Manager of the Cybersecurity Research Project at IREQ, since 2018. She is also an Adjunct Professor with the Department of Electrical and Computer Engineering, McGill University. She was a member in the Working Group 15 (WG15) of the International Electrotechnical Commission (IEC) Technical Committee (TC) 57. Since 2015, she has been contributing to the development of IEC 62351 standards for the cybersecurity of power system information infrastructure. Her research interests include telecommunication networks, time synchronization systems, power grid automation, and cybersecurity for smart grids.

DEEPA KUNDUR (Fellow, IEEE) received the B.A.Sc., M.A.Sc., and Ph.D. degrees in electrical and computer engineering from the University of Toronto, in 1993, 1995, and 1999, respectively.

She is currently a Professor and the Chair of The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto. She is the author of over 200 journals and conference papers and is a recognized authority on cybersecurity issues. Her research interests include the interface of cybersecurity, signal processing, and complex dynamical networks.

Prof. Kundur's is a fellow of the Canadian Academy of Engineering and a Senior Fellow of Massey College. Her research has received best paper recognitions at numerous venues, including the 2015 IEEE Smart Grid Communications Conference, the 2015 IEEE Electrical Power and Energy Conference, the 2012 IEEE Canadian Conference on Electrical & Computer Engineering, the 2011 Cyber Security and Information Intelligence Research Workshop, and the 2008 IEEE INFOCOM Workshop on Mission Critical Networks. She has also been a recipient of teaching awards from the University of Toronto and Texas A&M University. She has served as the Honorary Chair for the 2021 IEEE Electric Power and Energy Conference and as the General Chair for 2021 International Conference on Smart Grids for Smart Cities. She has served in numerous conference executive organization roles, including as the Publicity Chair for ICASSP 2021, the Track Chair for the 2020 IEEE International Conference on Autonomous Systems, the General Chair of the 2018 GlobalSIP Symposium on Information Processing, Learning and Optimization for Smart Energy Infrastructures, and the TPC Co-Chair for IEEE SmartGridComm 2018.