1-1-2021

CPS Attacks Mitigation Approaches on Power Electronic Systems with Security Challenges for Smart Grid Applications: A Review

Mahmoud Amin
Manhattan College

Fayez F.M. El-Sousy
Prince Sattam Bin Abdulaziz University

Ghada A.Abdel Aziz
Department of Power electronics

Khaled Gaber
Faculty of Engineering

Osama A. Mohammed
Florida International University

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 10, 2021, accepted February 26, 2021, date of publication March 2, 2021, date of current version March 15, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3063229

CPS Attacks Mitigation Approaches on Power Electronic Systems With Security Challenges for Smart Grid Applications: A Review

MAHMOUD AMIN[1,3], (Senior Member, IEEE), FAYEZ F. M. EL-SOUSY[2], (Member, IEEE), GHADA A. ABDEL AZIZ[3], (Member, IEEE), KHALED GABER[4], AND OSAMA A. MOHAMMED[5], (Life Fellow, IEEE)

[1]Electrical and Computer Engineering Department, Manhattan College, Riverdale, NY 10471, USA
[2]Department of Electrical Engineering, College of Engineering, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[3]Power Electronics and Energy Conversion Department, Electronics Research Institute, Cairo 12611, Egypt
[4]Department of Electrical Engineering, Faculty of Engineering, Al-Azhar University, Cairo 11771, Egypt
[5]Electrical and Computer Engineering Department, Florida International University, Miami, FL 33174, USA

Corresponding author: Mahmoud Amin (mahmoud.amin@manhattan.edu)

This work was supported by the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia, under Project 1289.

ABSTRACT This paper presents an inclusive review of the cyber-physical (CP) attacks, vulnerabilities, mitigation approaches on the power electronics and the security challenges for the smart grid applications. With the rapid evolution of the physical systems in the power electronics applications for interfacing renewable energy sources that incorporate with cyber frameworks, the cyber threats have a critical impact on the smart grid performance. Due to the existence of electronic devices in the smart grid applications, which are interconnected through communication networks, these networks may be subjected to severe cyber-attacks by hackers. If this occurs, the digital controllers can be physically isolated from the control loop. Therefore, the cyber-physical systems (CPSs) in the power electronic systems employed in the smart grid need special treatment and security. In this paper, an overview of the power electronics systems security on the networked smart grid from the CP perception, as well as then emphases on prominent CP attack patterns with substantial influence on the power electronics components operation along with analogous defense solutions. Furthermore, appraisal of the CPS threats attacks mitigation approaches, and encounters along the smart grid applications are discussed. Finally, the paper concludes with upcoming trends and challenges in CP security in the smart grid applications.

INDEX TERMS Cyber-security, cyber-attacks, cyber-physical system, voltage source converter, smart grid, security attacks mitigation.

I. INTRODUCTION

Cyber-physical system (CPS) is considered a significant type of digital technology in power systems, medical, industrial control, communication, energy system, transportation, as well as precarious infrastructures. The CPSs employ physical as well as computational components to validate a process in the real-time world [1]. The CPS has three main categories: cyber, physical, along with cyber-physical (CP) elements. The cyber parts of the software components do not have a direct link with the real world. These elements comprise computing, control, and communication to accomplish the system's robustness, stability, reliability, and efficiency in the physical systems applications. Meanwhile, the physical refers to the physical elements or the hardware components, which do not have a direct link with the cyber elements. These hardware components comprise transmission lines, generator stations, along load models. The CP refers to the equipment that has direct contact with both the physical and the cyber world. For the industrial control system, the actuator, the programmable logic controller, along with the sensor, are entirely CP aspects because of their direct connections with the physical world. The actuator and the sensor wireless aptitudes are also considered CP. Meanwhile, for the smart grid, the control center has a CP aspect when disconnect/connect commands are sent via the advanced metering infrastructure headend

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

to the smart meters. Furthermore, the CP aspect can appear in the smart meter itself because of its aptitude to carryout cyber operations, e.g. sending measurements to the grid, and physical operations, e.g. disconnecting/connecting electricity services. Supplementary field instruments in the generation, transmission automation, along with distribution plants have a high existence of the CP aspect because of their direct connections with physical aspects of smart grids. The exponential growth in smart sensors, networking, data acquisition, management framework, embedded controllers, and instrumentations empowered us to improve new applications and systems that change our life [2]. The CPS brought innovation to many industrial applications due to its prospect of integrating technologies from different sectors, transforming conventional developments in numerous application areas, and permitting new processes. These applications areas include smart grids, industrial control systems, medical instruments, and miscellaneous applications. CPS security and the security of software and hardware systems employed in databases; are critical and challenging because of their model [3]. As the computation system needs to be incorporated into a sensitive environment, challenges increase because of the computations required for real-time implementation.

The CPS has computational abilities that can sense the embedded data from the framework and convert it into beneficial information [4]. Indeed, the cyber system attained the data from the physical system via sensors' usage and fed back the control signal to the physical system. This useful data may be speed/current/voltage measurements, energy consumption, or medical condition. Based on this data, special action can be performed on the system, such as control action or protection procedure against system malfunction or fault condition. In the CPS, there is a real-time reaction for each cyber action. These actions greatly influence the safety of the physical environment and increase CPS reliability [5]. Moreover, some CPS systems require employing warning threat techniques in real-time applications.

The CPSs greatly influence the smart grids, the transportation systems, and the digitally-controlled power electronic systems. However, both cyber and physical instabilities may have a negative impact on the smart grid's performance. Moreover, employing solid-state devices, e.g., diodes, thyristors, bipolar junction transistors (BJTs), silicon controlled rectifiers (SCRs), insulated-gate bipolar transistors (IGBTs), and triode for alternating currents (TRIACs) in the conversion of electric power and control is called power electronics. Because of the digital features, the power converters have inherited networking aptitudes. The networked power converters can be employed in renewable energy generation systems, smart grid [6], telecommunication, smart home [7], machine drives, battery management systems [8], etc. Fig. 1 depicts the power converters with various control hierarchies. The 3-tier is the widely employed hierarchy, which comprises the regulatory controller at the 1st tier followed by subsystem controllers and slave controllers.

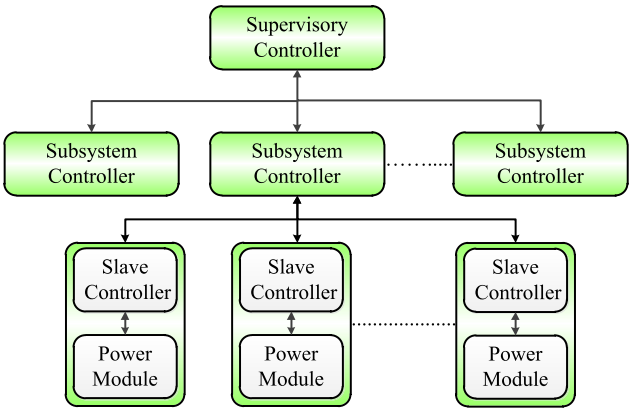

FIGURE 1. The control hierarchies for the power converters.

The supervisory controller may be a Programmable Logic Controller (PLC) or other controllers able to monitor the subsystem level controllers and hand over the user's dynamic commands, e.g., speed/torque commands along with emergency commands, i.e., shutdown [9].

The supervisory level communication is not destined via firm timing requisites. The subsystems comprise the transformer, the drive system, power converter module, etc. For the converter module level, the information exchange can be correlated to the power electronic building block modules, which comprise the voltage and current measurements, error flags along with pulse width modulation (PWM) references. At this level, the communication should be isochronous for the fixed packet size at a fixed rate [10]. The power converter components can be subjected to numerous serious threats, attacks, faults, false data injection attacks, unpredicted failures, and cyber-physical switching attacks [11]. As an example of the power electronics applications, the machine drives typically comprise speed or torque reference feedback signals for the process optimization. Moreover, the reliability along with security is the most critical conditions in the power converters [12]. The system reliability can be assured if correct fault detection and tolerance are employed and accurate encoding signaling of faults. Thus, a hardware-based interference-detection and attack blocking solution well-matched with the equipment's time constants may be favored at the component level [13]. Moreover, the complexity of the physical and cyber components in the digitally controlled power electronics applications can make the system unsecured against threats and constraints. These threats include the interruptions and malfunction of the physical infrastructures and the communication abilities of the CPSs. Therefore, digitally-controlled power electronics systems must be reliable and secured from serious attacks and threats.

The CPS attack mitigation must be performed via a defense-in-depth pattern using detection and reaction methodologies to protect and employ them at different levels. The defenses against the CPS severe attacks can be categorized into prevention, detection, and response [14].

The prevention of denotes security techniques that prevent attacks by providing verification, security policies, and network segmentation in the CPS. Meanwhile, the attack detection techniques are designed to identify the strange/irregular behaviors and attacks in the CPS system. As most of the CPSs are real-time constraints, a security technique may need to operate automatically to mitigate the attack quickly.

In the digitally-controlled power electronics systems, smart devices are responsible for carrying the power flow and transmitting the data for monitoring and control applications [15]. The intricacy of the digitally-controlled power electronic system has emphasized the future challenges to its security and resilience. Moreover, cyber integration needs considerable investments in CPS security designs and promotions to contradict cyberspace's unexpected patterns and attacks [16]. Thus, the CPS must be designed and practically implemented to be straightforwardly extendable and accessible. Indeed, the CPS security solution will include both the hardware and the software-based solutions with various defense layers against the cyber-attacks.

The CPS's significant focus in the digitally-controlled power electronics applications is the investigation of composite attack patterns. The attackers can comprehend trickery patterns by exploiting both zero-day and known vulnerabilities in the power electronic system. Also, the threats of the attack can cause power supply failures, cascaded failures in the system. It can also damage consumer instruments and threaten the human safety. Thus, the evaluations of vulnerabilities and flexibility alongside the CPS attacks will provide the bases for inclusive protective strategies as well as emergency responses for the serious electrical power structure [17]. Investigating the CPS attacks threats in power electronics systems and the security approaches' improvements are non-stop research areas.

The cyber as well as the physical security assessments are necessary for securing the digitally-controlled power electronics systems. Still, neither direction alone can afford comprehensive identifications and solutions despite integrating the other. Though various discovered attack threats in the CP systems are supplemented with detection, protection, or attacks mitigation approaches, some of the unknown threats still endure for being addressed. Moreover, employing the CPS in the digitally-controlled power electronics systems can be subjected to various vulnerabilities as well as approaches; the famous threats can provide fast reappraisal according to the new developments [18].

The conventional cyber analysis may not work for the digitally-controlled power electronics applications due to the interruption into cyber-asset. This action needs reconsideration of the customarily used security approaches to indicate the physical and cyber systems' interconnection. A composite CP analysis of the power electronic system and the related cyber design requires establishing criteria for evaluating the CPS vulnerabilities [19].

This paper presents a comprehensive survey as mapped in Fig. 2 of the digitally-controlled power electronic system

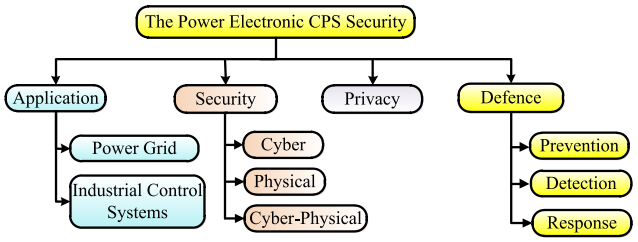

FIGURE 2. Security taxonomy for power electronic CPS.

CPS focusing on the security, threats, vulnerabilities, attacks mitigation approaches.

We believe that the CPS research topic is valuable to provide an intensive overview of the previous surveys to present the CPS research trends and its challenges systematically.

As depicted in Fig. 2, the power electronics system CPS focuses on the CPS security systems of the power electronics in the networked smart grid and the industrial control system. Indeed, the users' privacy for innovative technologies in the smart grid and the industrial control system must be secured; as various sensors can be employed, which can be subjected to sensitive information leakage. Furthermore, the data collection from CPS operation over long time intervals can reveal behavioral patterns of users that allow their characterization along with identification beyond the scope of applications, violating privacy rights. Moreover, after recognizing the CPS vulnerabilities, it is necessary to employ defense techniques for preventing the CPS attacks.

Various survey papers have been conducted on the CPS security of the smart grid as illustrated in Table 1. However, the main scopes of this paper are: presenting a comprehensive background on the CPS security in the power electronic systems applications, potential threat sources and their motivations are extensively surveyed, existing vulnerabilities in the networked smart grid are presented with highlighting the main reasons with real examples, introducing the impact along with vulnerability analysis of the control, communication as well as physical layer employed for handling the voltage source converters, existing control mechanisms for the networked smart grid are summarized by identifying the unsolved issues, introducing research trends and challenges in securing the CPS in the networked smart grid, according to this review, further research problems are addressed and their early solutions as future directions.

This paper is organized as follows; Section II presents the architecture of digitally-controlled power electronic CPSs. Scenarios of cyber-attacks on the networked smart grid are addressed in Section III. Section IV introduces the CP viewpoint of networked smart grid security. Section V presents the power electronics CPS security threats. Section VI offers the power electronics applications CPS security vulnerabilities. Section VII presents the CP vulnerabilities in the smart grid. Section VIII introduces the analysis and impact of cyber-attacks vulnerability on controlling the voltage source converters. The CPS attack mitigation techniques are

TABLE 1. List of CPS surveys on the smart grid.

Survey Content	Survey Area	Year of Publication	Reference
Survey on protection methods for large renewable integration in smart grids, wireless charging in EVs, power technologies for CPS reliability, transactive smart railway grid, along with real-time simulation of shipboard power systems.	Power electronics, smart grids, IoT, technological innovation, voltage control, market research, renewable energy sources	2021	[15]
Survey on the different types of cyber-attack detection and mitigation control approaches for the power system	Cyber-physical power system, CPPS modeling, CPPS simulation, cyber-physical social system (CPSS), cyber-attack, cyber security, and smart grid.	2020	[18]
Survey on the model-based and the data-driven algorithms for detecting the FDI attack according to the pros and cons of each algorithm.	Cyber-physical attacks, smart grid, data-driven detection algorithms, machine learning, false data injection, model-based detection algorithms, state estimation, and stealth attacks.	2020	[40]
Survey on cyber-physical smart grid testbeds for providing a taxonomy along with insightful guidelines for the development and identifying the significant features and design decisions while emerging future smart grid testbeds.	CPS, testbed, and smart grid	2017	[80]
Survey on industrial CPS monitoring and control based on data-driven realization.	CPS, system monitoring, data-driven, fault diagnosis, plug-and-play control, and smart grid,	2018	[92]
Survey on different prospects, merits, approaches, and technical challenges of employing the blockchain technology in the smart grid.	Smart grids, blockchain, consensus algorithm, industries, renewable energy sources	2019	[123]
A survey on the implementation of differential privacy in the healthcare and medical systems, the energy systems, transportation systems, and industrial IoT.	Differential privacy, CPSs, smart grid, health care systems, industrial IoT, and privacy preservation.	2020	[135]

addressed in Section IX. Section X presents the CPS security challenges in the networked smart grids. Finally, Section XI concludes the paper.

II. ARCHITECTURE OF DIGITALLY-CONTROLLED POWER ELECTRONIC CPSs

Fig. 3 illustrates the structural design of AC smart grid-tied voltage-source-converter system. As depicted, the entire power conversion chain has six stages: the input stage, the grid-connected voltage source converter stage, the input-side power converter stage, DC voltage stage, the cyber stage, along the AC grid stage.

This structural design is the most generally employed for interfacing renewable energy sources such as the PV, wind, energy storage systems [20], and the electric vehicle charging arrangement with the networked smart grid [21].

For enhancing the networked smart grid's robustness along with resiliency, the voltage source converter systems are expected to be connected via communication links into a particular comprehensive CP networked smart grid.

The detailed control stages can be discussed as follows:

A. THE PHYSICAL STAGE

On the left side of Fig. 3, the standard input power sources/sinks are placed. In the input stage, some units, e.g., energy storage system, the grid can absorb or inject the power.

The power exchanged between the input-side along with the intermediate DC stage, can be regulated via input-side converters. These converters are employed for exchanging the energy between the input-stage along with the DC voltage stage. Indeed, the DC stage is used as a power buffer between the input as well as the AC stage for operating autonomously from the AC stage as in the DC microgrid [22].

To integrate the source from the input stage into the grid, a grid-connected voltage source converter operates as an interface between the DC-link stage and the AC grid. As illustrated in Fig. 3, their output is connected through the interface filter to an AC microgrid, standalone AC loads, or an AC grid.

Based on the interconnection between diverse AC stages, numerous standards are appropriate. In the networked smart grid, the main concern lies with the grid current regulation with high power qualitative signatures at the transient's occurrence (voltage swells, voltage sags, as well as unbalances) [23]. Lately, an increasing number of grid-supplementary services correlated to grid voltage and frequency support are likewise mandatory [24]. Moreover, their performance in the less inertia autonomous system (i.e., microgrids) can be basically controlled by sharing aptitudes for reactive as good harmonics throughout the transients, steady-state, and the active power.

B. THE CYBER STAGE

The networked smart grid contains various voltage source converters. Together with traditional synchronous generators, they conjointly control the grid as well as all of these units is considered an agent for a standard part of a smart grid with interconnected voltage source converters.

The communication topology can be distinct as the physical layout of the network nodes along with the connecting cables. The most widely employed communication topologies are star, bus, ring, dual ring, tree, mesh, daisy chain, and hybrid as depicted in Fig. 4 [132], [138], [162], [209]. This figure shows the graphic depiction of both the cyber structures, as the dotted lines refer to the information flow. In general, for the power converters, the most employed control topologies are star, bus, ring, along with daisy chain.

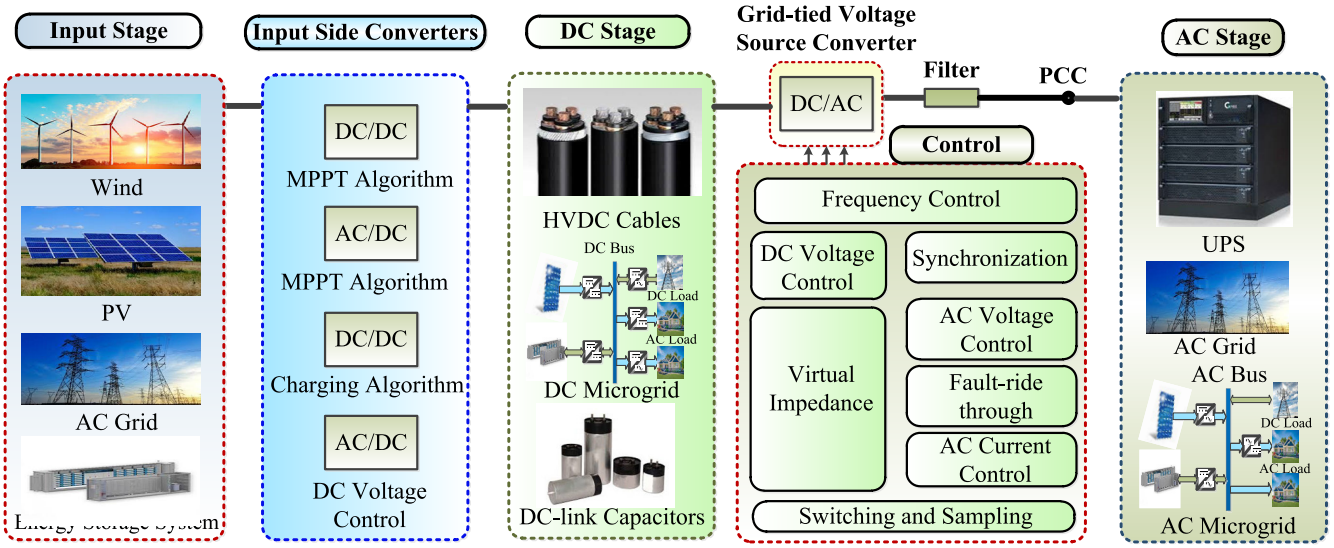

FIGURE 3. The structure of the AC smart grid-tied voltage-source-converter system.

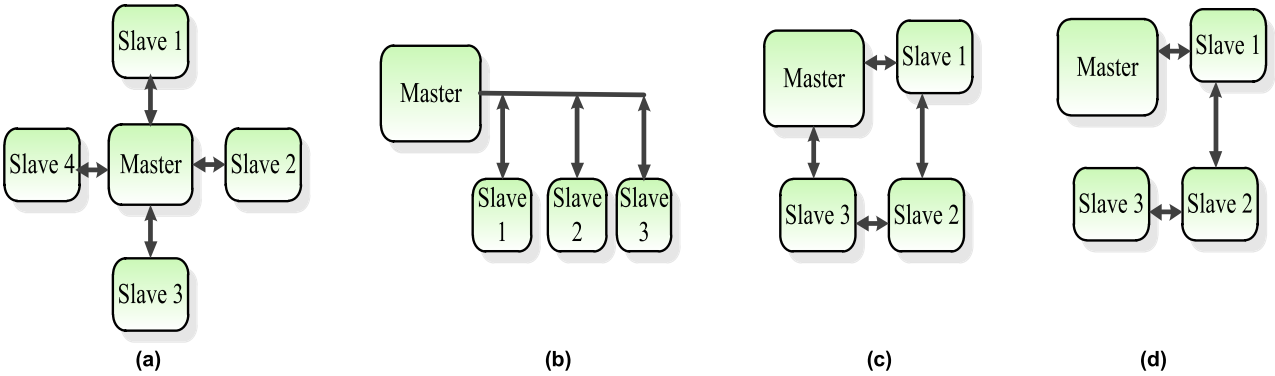

FIGURE 4. The communication topologies for the cyber structures: (a) Star topology (b) Bus topology (c) Ring topology (d) Daisy chain topology.

Fig. 4(a) depicts the star topology, which is the simplest topology as each power electronic building block is connected to the subsystem master controller through a single full duplex connection. A very simple communication protocol is adequate. Though, this topology restricts the maximum number of power electronic building blocks connected to the master controller; it is less resilience and hard to scale up. Indeed, it requires complex wiring, circuit along with dense computational load executed upon the master making it a vulnerable single point of failure.

Fig. 4(b) depicts the bus topology, which has a common trunk shared via all the power electronic building blocks connected to the master. It is quite easier to add a new power electronic building block making it flexible. Instead, it needs a complex communication protocol with extra features.

Fig. 4(c) depicts the ring topology [25]. In this topology, the power electronic building blocks are connected one after another, therefore, it needs only one pair of transmitter along with receiver making it scalable, though a complex communication protocol is needed for supporting the synchronization.

Fig. 4(d) depicts the daisy chain, which is a sub form of the ring topology without the loop back to master. This topology is a scalable one but is vulnerable to single point of failure.

Each agent has a distributed controller that can process the data from local and neighboring agents and from other remote locations. These data can be acquired via employing phasor measurement units (PMUs) that include the dynamic voltage phasors. The communication between the local controllers and the PMUs can be accomplished in a centralized manner, as the measurements from entire agents are centrally gathered for processing and decision making. Supervisory control and data acquisition (SCADA) system is considered the most effective technique of coordination between agents as in [26] for easing the monitoring in the smart grid networks. For higher numbers of agents, this technique not only needs substantial communication resources, but it is also susceptible to probable cyber-attacks.

The decentralized control denotes a scheme as only local measurements are employed. Meanwhile, the distributed control paradigm is flexible as the computational resources are consistently allocated to attain coordination. Therefore, low

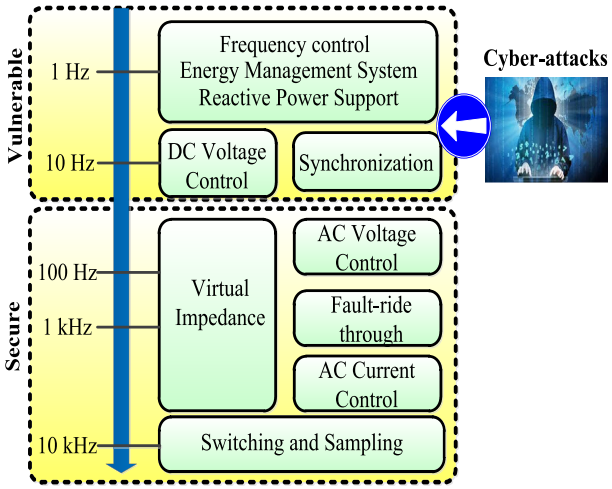

FIGURE 5. Traditional control structure for 2-level voltage source converter – Secure as well as vulnerable control layers alongside cyber-attacks.

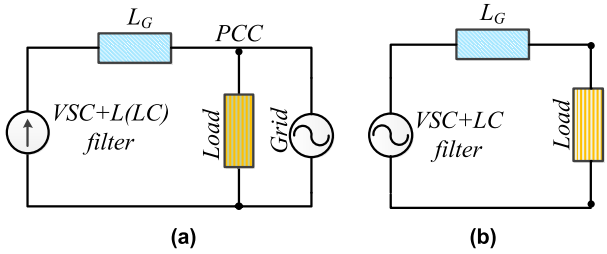

FIGURE 6. Voltage source converter representation with basic types: (a) Grid-feeding and (b) Grid-forming voltage source converter.

bandwidth communication channels are used for accomplishing the same function. Nevertheless, it provides noticeable criteria of valuation of interruption attempts, vulnerability to cyber-attacks cannot be essentially assured for coordinated attacks [27], [28]. This can be clarified because inadequate information exists in every node, which does not function as sufficient inclusive information for cyber-attack detection.

Fig. 5 depicts an outline of the control functions of AC-grid-connected voltage source converters according to their timescales. As depicted, the control loops are illustrated next to each other for operating simultaneously (i.e., DC-link voltage control along with synchronization [29], fault-ride through (FRT) along with AC current control [30], or active damping as well as virtual impedance/admittance control [31]).

C. THE ROLE OF VOLTAGE SOURCE CONVERTERS

In the microgrids, along with the renewable-based power systems, the voltage source converters' main role is categorized as the grid-feeding, grid-supporting, and grid-forming units [32]. These roles can be addressed as follows:

1) Grid-feeding voltage source converter unit: This unit's main function is injecting a definite current into the grid. Thus, they are signified as current sources, as depicted in Fig. 6(a). For real-time implementation, they contain a dedicated synchronization unit, an outer DC voltage control loop, as well as an inner current control loop with embedded passive or active damping [33]. In order to generate the current command, outer power controllers are employed for supplementing the DC voltage controller.

2) Grid-forming voltage source converter unit: This unit is employed for regulating the local voltage. Thus, it is signified as an ideal voltage source, as depicted in Fig. 6(b). Because of its rigid voltage regulation, this unit is deliberated as the system's master, which outlines the local AC grid. Consequently, this unit does not require to have any dedicated synchronization along with power-sharing aptitudes. For the real-time implementation, this unit can be realized through an inner current loop along with an outer voltage loop [34]. This functionality is utilized as an elementary philosophy in standalone applications as the microgrid [35].

According to the paralleled voltage source converters in the standalone microgrid, the principal control law can be employed for both reactive along with active power to align the frequency ω^* along with the voltage reference V* respectively for synchronization as illustrated in (1), (2):

$$V^* = V_{ref} - N_Q \left(Q - Q^*\right) \tag{1}$$

$$\omega^* = \omega_{ref} - M_P \left(P - P^*\right) \tag{2}$$

where V_{ref}, ω_{ref}, Q^*, P^* denote the global voltage, frequency, reactive and active power references, respectively. Meanwhile, N_Q, M_P, Q along with P represent the reactive power droop, active power droop, measured reactive as well as active power, respectively.

3) Grid-supporting voltage source converter unit: this unit comprises of wider spectrum of control functionalities, from grid frequency/voltage support, reactive/active power sharing to impedance/admittance emulation along with virtual inertia [36].

III. SCENARIOS OF CYBER-ATTACKS

This section addresses the main causes and the cyber-attacks scenarios on the networked smart grid. Furthermore, it discusses the cyber-attacks impacts on the networked smart grid by considering the technical failures and triggering events' resultant effects.

A. CAUSES OF CYBER-ATTACKS

The networked smart grid in its structure comprises communication systems along with hybrid of power, which renders vulnerabilities that can be compromised during the cyber-attack. These vulnerabilities include confidentiality, integrity along with availability, or the CIA abbreviation [37].

The networked smart grid is characterized as a CPS as depicted in Fig. 7, which comprises sensor/actuator, physical, network, information, and control layers. Each layer's operation is conceivable but does not certainly mean an interruption detection component or system prerequisites to be applied in the whole layer. Information can flow between entire layers as they maneuver merely in a cycle [38].

Cyber-attacks can appear in numerous forms. Its main definition is human-made manipulation of the smart grid

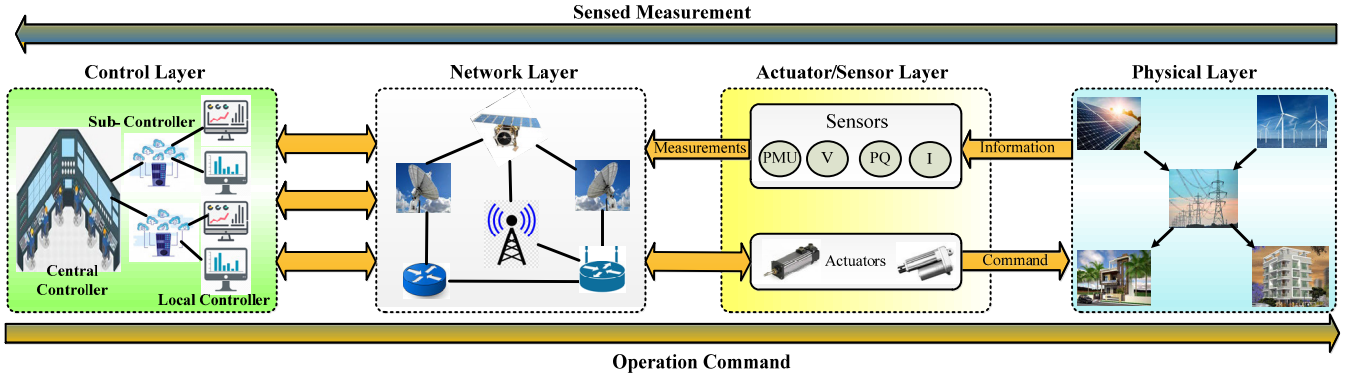

FIGURE 7. The CPS architecture with multiple layers.

TABLE 2. Cyber-attacks in the smart grids.

	Transmission System	Distribution System	Instrument	System	Type of Attack
State Estimator	√			√	DoS/FDI
SCADA	√	√		√	DoS/FDI
Data Concentrator	√	√		√	Delay/FDI/Jamming
Power Market	√			√	DoS/FDI/Delay
Communication Channel	√	√		√	Delay/Jamming/DoS
Phasor Measurement Unit	√	√	√		Delay/Jamming/DoS
Remote Terminal Unit	√	√	√		Delay/Jamming/DoS/FDI
Intelligent Electronic Device		√	√		Jamming/FDI
Advanced Meter Infrastructure		√	√		Jamming/FDI
Programmable Logic Controller	√	√	√		Jamming/Delay/FDI
Control System	√		√	√	DoS/FDI

and conveying the power flow to where it is unassigned via the network operator, as illustrated in Table 2. Different interoperability layers in the networked smart grid comprise function, physical, and business layers.

These layers are interrelated via a communication layer for information exchange attack surfaces that are broader than those illustrated in Table 2. Though, in this table, the most common surfaces that can be attacked in present modern power systems are reviewed as a basis for identifying the common attacks domain as well as type.

These attacks include denial of service (DoS), false data injection (FDI), insertion of worms or malware, energy theft [39], as well as physical damage of the smart grid, e.g., causing apparatus to self-damage [40]–[42].

- The DoS attacks can be recognized via jamming the communication channels by the attacker. These attacks aim at the electronic maneuvers and attack the routing protocols for cramming the communication channels and causing delays. Indeed, the DoS attack can restrict the legitimate user's access to the services along with resources via overflowing the communication network with excessive traffic [43].
- FDI attack scenarios are recognized when the attacker injects false data on the control center's communication line and the field sensors. Thus, the attacker can disturb the state estimation processes and betray the network operator [44]. The FDI attack can result in various outcomes relying on the intention of the intruder, which comprises error in the locational marginal prices (LMP) for illegal market profits, energy theft, along with physical destruction through the network. FDI attacks can affect the LMP by confusing the state estimation, which then unsympathetically involves the contingency analysis processes [45].
- Insertion of worms or malware can range from malicious software that operates in backgrounds to decelerate the smart grid computers' operations via employing Trojan software for stealing the certificates of practical security [46].

To detect cyber-attacks on the Internet-of-Things (IoT) applications, the sensors available in the system is utilized along with monitoring the physical system possible models. Cyber-attack does not nearly have to arise in the power system itself. It can initiate from different systems that frequently interrelate with the grid, e.g., electric vehicle (EV) supply equipment [47]. In [48], the malware attack model has been designed to attack the infrastructure of the EV, along with its communication systems when EVs are charging. In some cases, attacks can be undetectable, e.g., malicious data injection attacks that can change the measurements values without being identified; thus, serious consequences can occur.

Based on the engineering perception, the smart grids can be subjected to cyber-attacks owing to the widespread and dependence on intelligent electronic devices (IEDs) [49]–[52], distributed advanced metering infrastructure (AMI) [53], as well as wireless and off-the-shelf

communications components along with systems through the power network. The cyber infrastructure can increase autonomous decision-making and the system's connectivity via regular information protocols that frequently have visibly documented vulnerabilities. The energy industry privatization and market deregulation have increased the competition between energy suppliers to improve consumer-centricity. Moreover, threats can occur in the form of disappointed utility insiders, electricity customers, as well as cyber-attacks.

B. CYBER-ATTACKS IMPACTS ON SMART GRID

In the networked smart grid, control systems are further vulnerable due to their coupling with new communication as well as information technologies along with the CPS physical controllers [54]. The distribution management system (DMS) in distribution networks along with the energy management systems (EMSs) in the transmission networks are critical equipment systems that are significantly influenced or abused throughout the attack. These platforms are used for collecting the data from distributed or remote meters along with sensors through the network. Via injecting false meter data as a cyber-attack, the DMS or EMS functions at the control center will be deceived through the state estimators that can make power dispatch, inaccurate decisions on contingency analysis, and even billing transactions [55], [56].

Smart grid has synchrophasor-based cyber-security that can provide real-time data to the EMS for controlling and monitoring the physical network [57], [58]. Modern synchrophasor instruments, e.g., digital fault record (DFR), PMU, along with protecting relays with PMU functionality, are vulnerable to various errors [59], [60]. These comprise cyber-attacks, which is considered a challenging issue as the equipment is intertwined with numerous legacy instruments with protection/no protection alongside cyber-attacks [61].

In [62], CPS security has been analyzed where a trickery attack has targeted the actuators, sensors, and actuators and sensors. The FDI attack probability relies on two possibilities: (i) the hacker can control the sensor nodes as well as (ii) the hacker knows the system perfectly or its precise topology at entirely instants throughout the attack [63]. Commonly, the most significant influence of an attack can be recognized when the attacker has access to the SCADA systems and performs control actions [64]. The attackers can settle raw data measurements that result in unobserved errors to factor into estimates of state variables e.g., bus voltage magnitudes and angles. This can arise when the attacker takes the merits of small errors tolerated through state estimate approaches. Eventually, this numerously threatens the security of the power system [65]. The state estimation disturbances can increase the state estimates mean square errors and fluctuations in the electricity market's simultaneous prices. The impact of invalid state estimates for mean square errors can make the network operators make incorrect decisions, and alterations in the real-time prices of the electricity market can profit only the attacker [66].

Through the FDI attacks, the smart grid can undergo load redistribution attacks, economic attacks, or misleading energy attacks. The economic attack is a sort of FDI attack that can affect the deregulated electricity market operations, which includes two markets: the real-time market and the day-ahead market. In this case, the attacker can handle the market prices of the power along with acquiring financial gains.

For the load redistribution attack, the smart grid operation can be effected via hacking on the security-constrained economic dispatch (SCED) [67]. The main purpose of the SCED is to reduce the cost of the whole system operation; though, in case the raw measurements are handled via the attacker, the SCED will cause an overload of the lines. The latter may not be detected by the system operator and originates significant physical damages to the smart grid.

The deceptive energy attack can affect the distributed energy routing process; basically, this is a scheme for identifying the optimal energy routes for a generation or load demand. In case the measured data is corrupted, inaccurate energy demand or supply messages can be recruited [68]. Generally, cyber-attacks can impact four foremost aspects of the huge power systems: energy market, state estimation, voltage control, and automatic generation control. FDI attacks can deceive the system operators by believing that the operating conditions' status is safe both economically and physically when they are not [69].

Moreover, the FDI attacks can affect the system's security stability. For detecting the FDI attack, spatiotemporal cyber-state correlations can be employed.

Via monitoring the progressive consistencies of the spatial correlations between state estimations, potential anomalies can be detected [70].

The attacker can affect the communication network via attempting to connect and dial-up to intelligent electronic devices or a remote terminal unit (RTU). This can permit them to spy on telecommunications, perform a wide-area network (WAN) transmission or a local-area network (LAN) as depicted in Fig. 8. The attackers can similarly attack the corporate information technology (IT) systems and gain entrance access to the connected SCADA or EMS systems; internet service providers (ISP) and telecommunications can also be attacked. The smart grid suppliers are dependent on corporate IT systems as well as their connected SCADA systems can increase the electric smart grid vulnerability significantly [71].

Cyber-attacks, along with disturbances, can arise numerous times from a single origin as well as extend to diverse areas. In the electric vehicle charge stations, the consumer can charge its EV at numerous stations; thus, the malware can spread due to the communications between electric vehicle charge stations and vehicle-to-infrastructure. The EV attack can apply to the electric vehicle charge station's smart grid infrastructure to the utility systems [72]. The power systems and transportation integration can leave numerous open doors for the attackers. Particularly in the connected environment,

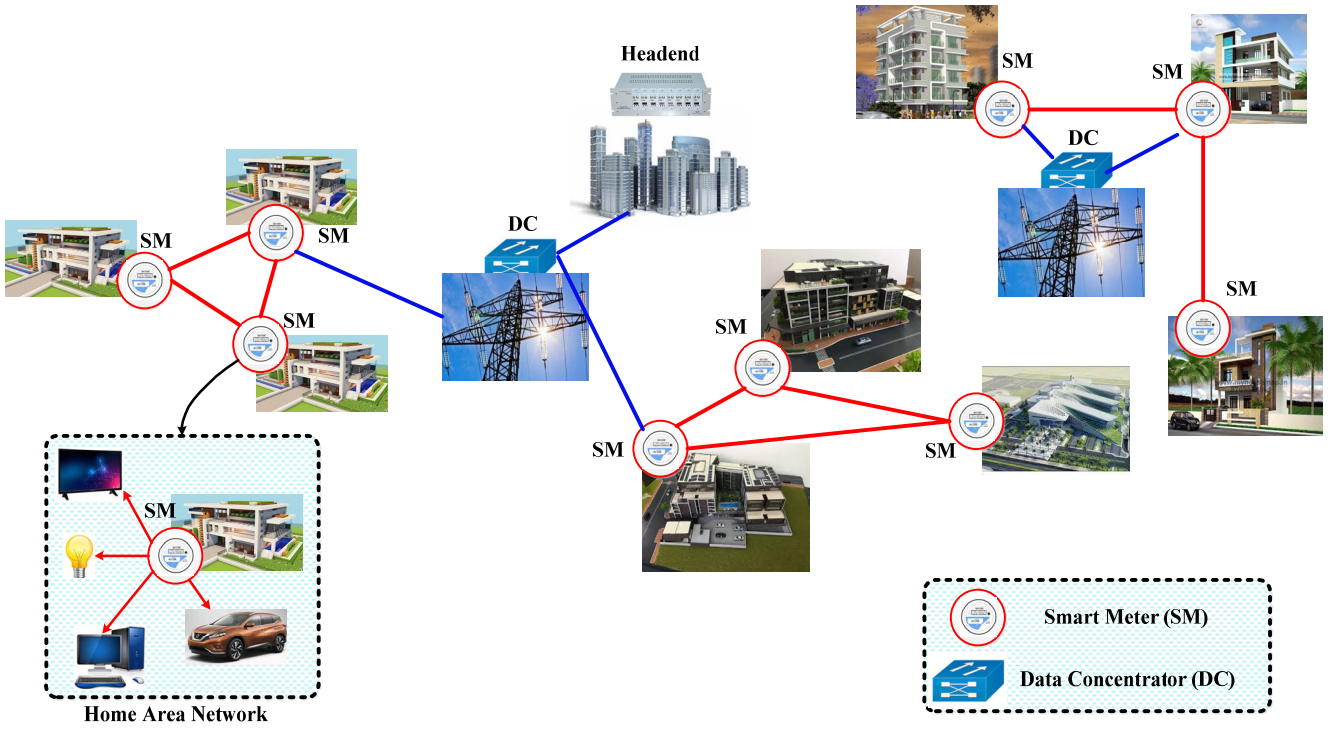

FIGURE 8. The infrastructures of the advanced metering.

e.g., the infrastructure of the EV, comprising electric vehicle charge stations, EVs, meters along with other roadside infrastructures as well as when intensely integrated with severe infrastructure systems [73]–[75].

IV. CP VIEWPOINT OF NETWORKED SMART GRID SECURITY

A. SMART GRID AS A CP SYSTEM

The smart grid is built on a vast physical infrastructure of electrical power systems that can be categorized into generation, transmission, and distribution systems [24]. In the conventional power system operations paradigm, the electricity is generated in power plants and delivered along with the transmission systems to the customers in the distribution systems. The EMSs placed in control canters can monitor as well as control this unidirectional process via employing SCADA systems [76]. These SCADA systems are typically hosted on dedicated communication infrastructures, including the local area networks, wide-area networks (WANs), and field area networks. The networked sensors' main function is to collect measurements, such as currents as well as voltage, then transmit the data to the control system via employing remote terminal units (RTUs) in the SCADA system. These RTUs are liable for the actuators' operation for adjusting topology and the dynamic system parameters [77].

The physical systems of generation, transmission, and distribution are interconnected via transmission lines and substations positioned in the field.

On top of these infrastructures, regional transmission organizations, along with independent system operators, coordinate the system's operations among service providers and consumers in the electricity market. Fig. 9 depicts the infrastructure of the entire networked smart grid, identified by the National Institute of Standards and Technologies (NIST), which comprises 7-domains of generation, transmission, distribution, electricity markets, operation, service providers, along with customers [78], [79].

In the networked smart grid, innovative technologies have transformed the conventional power systems in various areas [80]–[82]. The upward integration of renewable energy systems enhances the economics along with the sustainability of generation systems. The distributed energy resources (DERs) permit customer-side power generation as well as management with more reliability and flexibility, converting the existing patterns of power flows from unidirectional into bidirectional. In the transmission systems, the phasor measurement unit (PMU) employs a global positioning system (GPS) for providing more precise, frequent, and reliable synchronized measurements, enabling the wide-area monitoring, protection, and control (WAMPAC) implementation over high-speed communication networks [83]. The AMI systems with numerous smart meters in the distribution systems provide new 2-way, real-time communications in the smart grid, which endorse various profits from energy management, demand response, along with consumer engagement. Moreover, the increasing existence of energy storage, electric vehicles, and other emerging approaches are consistently introducing innovative changes to electricity generation, transmission, as well as distribution.

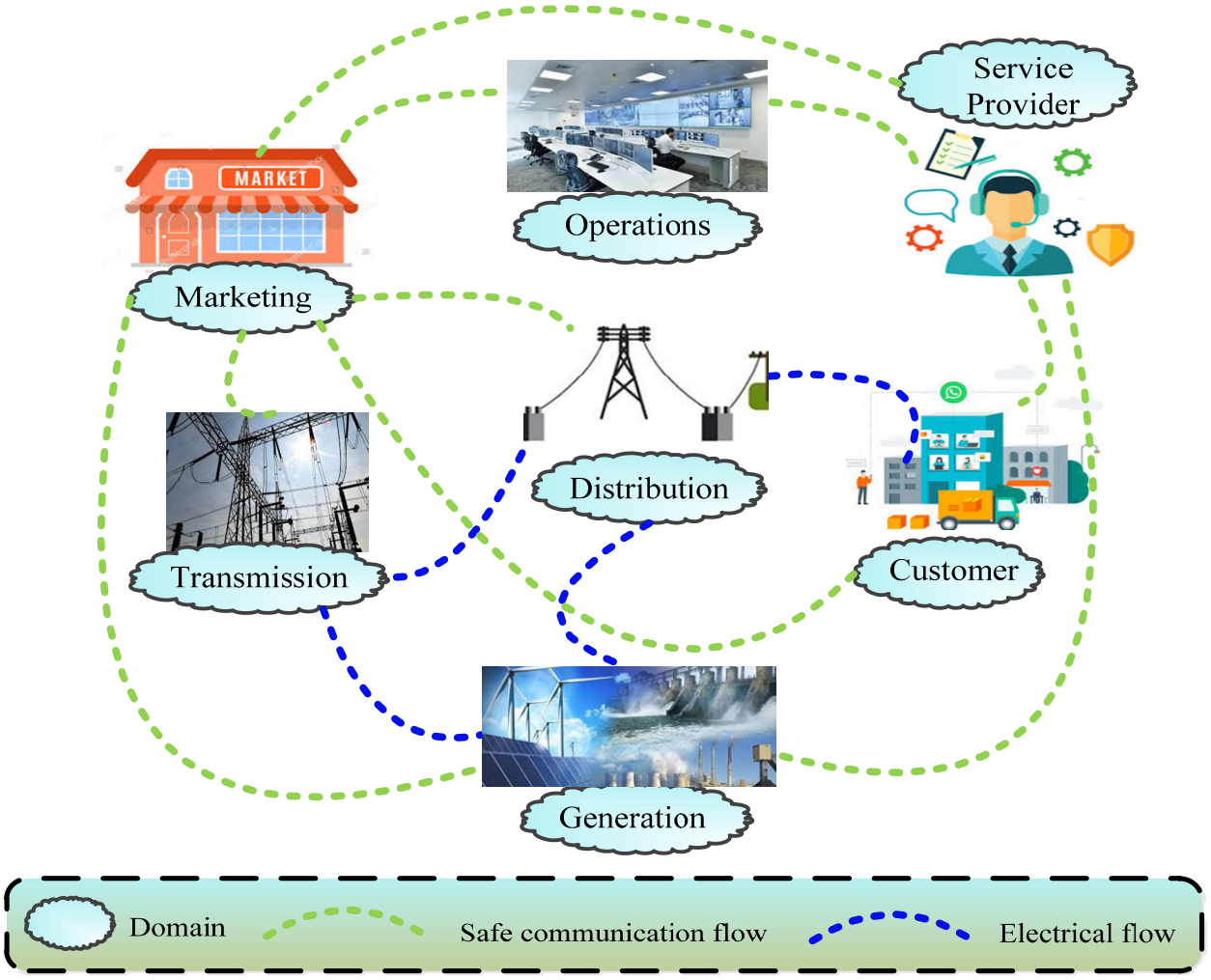

FIGURE 9. The networked smart grid conceptual model via NIST.

The communication systems, information, as well as computations in the smart grid have instituted a global cyber infrastructure interlinked with the physical systems. The commands as well as measurements are regularly generated and transmitted between cyber and physical systems. The physical systems measurements mainly consist of analog data and status data: the status data comprises the smart grid components; the analog data represent the system dynamics measurements. Basically, in the measurements, operators determine the optimum control strategies as well as produce the control commands for coordinating the actuators in the physical systems [84].

During the fault or disturbance occurrence, diagnostic logs are recorded via employing add-on recording instruments to support the location, assessment, mitigation, as well as repairs at the emergencies.

The sensor measurements can be processed via employing distributed along with centralized computation instruments positioned at different places in the smart grid. In the conventional centralized operations, critical calculations in the EMS, comprising optimal power flow (OPF), the state estimation (SE), automatic generation control (AGC), along with economic dispatch (ED) are hosted in the control centers. For better efficiency, resiliency, and flexibility, the latest advances in intelligent electronic devices along with programmable logic circuits have increased the employment of localized as well as distributed computations in the smart grid [85].

In the smart grid, communications have been mainly hosted on registered networks as well as SCADA systems. Industrial protocols, e.g., DNP3 as well as International Electrotechnical Commission (IEC 61850) have been established for communications between and within substations along with control centers [86].

New communication standards are being performed in the smart grid to accommodate the integration of energy storage, renewable energies, and PMUs. Furthermore, due to the increasing efficiency requests and cost pressures, the smart grid also increasingly depends on public communication infrastructures.

Via employing the ICT interfaces, the industrial control systems can access the internet. Two-way communications

between customers as well as service providers are also widely established via the AMI system, permitting flexible demand response for economic profits along with reliability.

B. CP SECURITY OF THE SMART GRID

In the smart grid, the security challenges have been widely increased in both cyber along physical spaces [87]. The power systems have intrinsic physical vulnerabilities, which can cause massive blackouts from incidents. The renewable energy sources integration can suffer from non-linearity, uncertainty, time-variance to existing power systems, and the new patterns from DER are inducing substantial influences on the stability [88].

The cyber-integration has vital security challenges, as great threats arise from the attacker's aptitude to launch remote, trickery, simultaneous, as well-coordinated attacks from the cyberspace. The scheme of informed attack can cause serious damages along with disruptions such as power blackouts, service interruptions, economic losses, to life-threatening threats, where societal, personal, as well as national securities may entirely be influenced [89].

The research on the security of the smart grid CP advances on a frontier of CPS, determined at the physical security intersection of energy and power systems and the cyber-security of communication, information, and computation systems [90]. The strengths incorporation of cyber and physical security is a significant requisite for the resilience and security of this critical infrastructure.

1) CYBER-SECURITY

Cyber-security is considered a significant component in smart grid development [91]. The principles of integrity, confidentiality, as well as availability have been established for the system's information security.

The firewalls, along with intrusion detection systems (IDSs) have been employed to protect field devices as well as control centers against exterior intrusions. Indeed, secure protocols have been established for protecting the SCADA communications within and between control centers, actuators, along with substations. Secure wireless or wired networks have also provided reliable communications for the emerging AMI and PMU systems.

Meanwhile, the smart grid's cyber-security also prerequisites further accommodate physical properties, dependencies, and power systems requirements. For instance, denying the access to an account after several unsuccessful log-in attempts; is regularly undesirable in the power system control. Attackers may employ a mechanism to lock operators out of the system, causing ruinous consequences [93] .

Furthermore, in the smart grid, signature-based IDSs and anomaly also requisite the adaptation of diversifying and emerging patterns for identifying the malicious attempts effectively. Indeed, the real-time data streams also have big data challenges to the analysis of the cyber-security in the smart grid. Moreover, there is a crucial requisite for incorporating the physical aspects into the smart grid's cyber-security [93].

2) PHYSICAL SECURITY

The power system's physical security can be protected via the evaluation along with the screening of the contingencies. The contingency analysis (CA) assesses the security of the power system after trustworthy inadvertent contingencies on the selection of operating points [94]. Usually, the CA can cover disturbances, faults, as well as planned outages, among others.

The constraints of contingency-related security are subsequently established via the CA for guaranteeing the power systems' survivability with marginal interruptions to the electricity delivery. For the smart grid, the analysis of both steady-state, as well as transient security power systems serves as the foundation of CP security. Nevertheless, the emerging CPS as well as the interconnected power systems, have challenges to the analysis of physical security.

The CA complication and cost is increasing dramatically when the system scales, interpretation it challenging to implement $N - k$ security or conduct multi-CA in bulk power systems [95]. The complexity and heterogeneity of software, operations, and hardware in power systems also limit the precise and timely evaluation of remotely located incidents whose influence could propagate over a long distance at the speed of electromagnetic waveform. Without adequate wide-area coordination, various local remedial actions may compete, rather than collaborate, with each other, causing deteriorate influences, i.e., blackouts or cascading failures [96]. Furthermore, cyber-integration can introduce emerging challenges. Most systems as well as field devices are not designed with adequate security features alongside malicious events, especially from cyberspace.

As the cyber-integration can expose the system to access resources as well as points in cyberspace, researchers have been revealing vulnerabilities, both indefinite and zero-day, in the evolving smart grid. The shortage of adequate protection alongside coordinated cyber-attacks could be disastrous, as demonstrated in the cyber-attack on a Ukraine regional grid [98]. They were automated along with intelligent systems, which have been designed to improve the reliability as well as the security of the system, maybe turned as weapons alongside the smart grid itself. With all these developing threats, the conventional power system security advantages an in-depth overhaul in the era of the smart grid.

3) CP SECURITY

A secure smart grid depends on the integrative security that combines the strength in both cyber-security and physical analyses against malignant and accidental events. The smart grid operators should be conscious of the measurement risks and commands corrupted via attackers internally and externally. Restoration efforts and mitigation need to be guided with sufficient security consciousness for evading secondary recompenses in the post-attack systems [98].

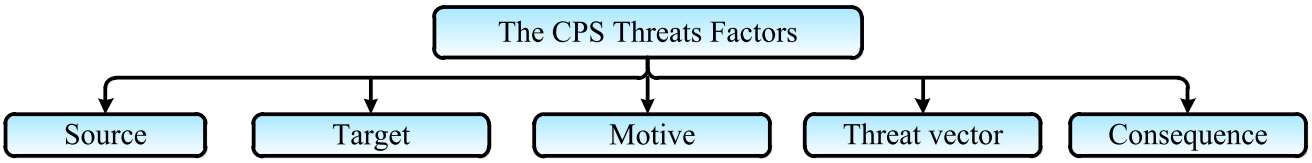

FIGURE 10. The CPS threats factors.

In the security analysis, serious vulnerabilities are often discovered by scenarios where attackers are characterized by feasible objectives, resources, as well as knowledge. The investigation of the attack schemes frequently serves as the 1st step for establishing security in the vulnerable system. Though it is unfeasible to exhaust entire potential attack schemes, the worst-case analysis is of concrete meaning to realize the feasibility along with the possible attack threat impact [99].

The smart grid security investigations have revealed various attack schemes that exploit critical vulnerabilities with various damages and disruptions. The sympathetic of these schemes is acute for improving the CP security of the technologies in the smart grid. Moreover, it will also help the researchers realize new vulnerabilities and solutions for the emerging CPS in this critical infrastructure [100].

4) CP RELIABILITY AND RESILIENCY OF POWER SYSTEM

The system's security should be robust adequate to avoid the cyber-attacks as well as provide advanced controls for system reliability along with stability. Reliability of the system comprised of adequacy along with security, which includes availability. The availability means that the data can be delivered securely and is available in a timely manner. Consequently, NIST has developed the standards for the communications network to integrate smart grid security [51].

Reliable information storage along with secure transportation are crucial for smart grid, billing functions, and grid control [43]. Resilience alongside faults and attacks must be addressed via a defense-in-depth paradigm whereby detection, prevention, along with reaction techniques for protection are used at numerous levels. Effective security mechanisms along with standardization efforts for the smart grid protection should be conducted for preventing the cyber-attacks. The most serious demand for smart grid is to guarantee process reliability. Instead, higher energy usages, older power infrastructure, along with higher demand are vital reasons to raise smart grid reliability issues. Therefore, the employment of modern communication protocols, quicker and robust control devices, communication & IT technologies, along with embedded smart devices can enhance the system's robustness and reliability [100]. The smart grid deployments in large scale can present brilliant options for wireless technologies, e.g. security, limited bandwidth, along with minimized installation costs. Though, wired technology is luxurious [5], [42]. Thus, a hybrid communication method integrated with wired along with wireless technologies is used for guaranteeing the robustness, reliability, along with availability.

V. THE POWER ELECTRONICS CPS SECURITY THREATS

Identifying the potential and serious threats that can attack the power electronic system is a severe issue and holds various challenges [101]. Our target is to discuss the various CPS security threats in general and then on two power electronics applications, e.g., smart grid and industrial control systems.

A. GENERAL CPS THREATS FACTORS

In the CPS system, the security solution may respond in an inverse manner when it is attacked. The security attacks can be defined as the actions that may cause loss or damage in the CPS system [102]. The damage refers to harming people, systems, and the environment, whereas the loss can be in the availability of the resources, safety measures, integrity, and sustainability. Some of these attacks may be harmful as they can overthrow the CPS's IT system by holding up the communication and the activity of the system entirely or injecting harmful information that may damage the security policies [103].

The CPS threats have five significant factors: sources, target, motive, threat vector, and the consequences of the threat, as illustrated in Fig. 10. These factors are discussed as follows:

The 1st CPS threat factors are the threat sources that are the threats' imitators and may affect CPS security. The threat sources comprise the physical, cyber, along with CP threats as depicted in Fig. 11.

The cyber threat sources include passive as well as active threats, as depicted in Fig. 11. The passive threats contain information harvesting and tracking. Meanwhile, the active threats include the denial of service and impersonation. Both the active and passive threats invade CPS integrity, availability, confidentiality, and authentication [104].

The physical threat sources include environmental, accidental, and adversarial threats. The environmental threats encompass natural disasters e.g., floods, and earthquakes, indeed the man-caused disasters e.g., fires and explosions [105]. The accidental threats are the threats that occur accidentally or via the authentic CPS components [106]. Meanwhile, malicious threats pose malicious purposes from states or individuals, groups' organizations [107].

The CP threat source is a mix of cyber and physical sources. As the protocols can lack encryption, thus, the data can be susceptible to eavesdropping along with severe attacks or false data can be injected due to the lack of authentication.

The 2nd CPS threat factors threat the target: the CPS applications and their users or components [108]. The 3rd factor

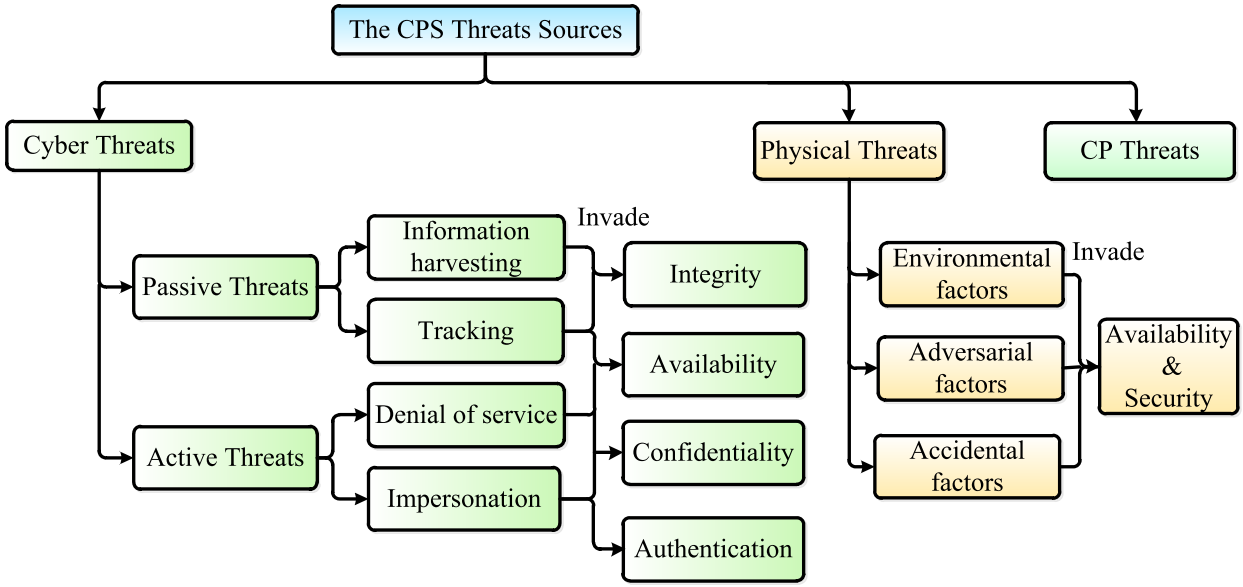

FIGURE 11. The sources of the threats in the CPS and the properties they invade.

TABLE 3. The CPS security threats In the smart grid and industrial control system.

Application		Attack Target	Attack Scenarios
Smart Grid	Generation threats	Wide control area [83], [104], [136], [193]	Bad command generation of automatic generation control and manipulate sampling data
	Transmission threats	SCADA [26], [76], [77]	Triggering false alarms and injecting false data, and changing the switch states
	Distribution threats	Distributed power supply and meter infrastructure [28], [55], [57], [96]	Modifying the instrument's readings, disturbing the management of the distribution, and reducing the credibility of the power generation.
	Physical threats	Damaging or vandalize components of smart grids [7], [40], [81], [93], [120], [141], [147]	Causing service disturbance and potentially blackouts
	Political threats	Initiating a cyberwar from a national power system against another country's national power system [17], [18], [19], [38], [57], [69]	Large scale blackouts, turbulences, or financial losses
	Financial threats	Tricking a utility company's billing system [40], [56], [61], [62], [87], [95], [120]	Tampering the smart meters to reduce the electricity bill
Industrial Control Systems	Intelligence agencies threats	Performing investigation operations targeting a nation's CI [54], [134]	Secrecy violations of critical data
	Criminal threats	Exploiting the wireless capabilities to control the industrial control system application remotely [5], [154], [162], [208]	Disturbing the industrial control system operation
	Physical threats	Spoofing a temperature sensor in a specific environment [53], [39], [45], [63], [161]	Sending deceptive, false measurements to the control center
	Political threats	Initiating a cyberwar from a nation against another nation [54], [134]	System's shutdown, damage in components, or environmental pollution
	Financial threats	Reducing the utility bill to deceive the utility [40], [56], [61], [95], [120]	Losing the financial

of the CPS threats is the motive of the danger in which the CPS assailants have reason to make an attack, e.g., spying, cyberwar, or criminal [109]. The 4th factor of the CPS threats is the threat vector, which can do one of four mechanisms for a successful attack, e.g., alteration, disruption, fabrication, and interception. The 5th factor of the CPS threats is the threat's potential consequences, which comprise the CPS integrity, confidentiality, availability, privacy, as well as safety [110].

B. THE CPS SECURITY THREATS IN THE SMART GRID AND INDUSTRIAL CONTROL SYSTEMS

This section gives potential CPS security threats in both the smart grid and industrial control systems as shown in Table 3. The smart grid comprises the generation, transmission, and distribution systems. Accordingly, the threats include generation, transmission, distribution, physical, political, and financial sections. Meanwhile, the industrial control

system refers to technologies that can monitor and control electrical, industrial, and manufacturing processes [111]. As a result, the threats comprise intelligence agencies, criminal, physical, political, and financial sections.

For successful operation of the smart grid, three significant connotations must be satisfied, e.g., communication flexibility, the resilience of the control system, and the smart of the distribution. Nevertheless, it is hard to fulfill such goals, particularly in insecure environments.

The smart grid can be subjected to malicious threats in the physical along with cyber components [112].

The physical threats aim at the power system components, e.g., transmission lines, generators, and transformers, that can change the power system's topology or trigger cascading failures [113]–[115]. As the transmission lines can spread over a large area, it is easy to be attacked than the substations. These threats can be easily detected using protection devices that indicate the failure or the operation of the physical components. Additionally, the cyber threats aim at the SCADA system that deceives the power system operation. This can cause high economic losses and is difficult to be detected if the threat vector is well-structured [17], [116], [117].

The assessment of the CPS security system performance and its threats in the smart grid and the industrial control system can be executed via the continuous monitoring of the data in the CPS system by assessing the efficiency and the state of the infrastructure. For the power electronics components used in the power distribution in the smart grid and the industrial control system, a detailed analysis of the power consumed between the industrial and residential areas is performed [118].

For securing the CPS, it must satisfy three significant security requirements: availability, safety, along with the integrity, as illustrated in Fig. 12.

The 1st requisite in the CPS security is the availability that comprises the reliability, resiliency, and restoration in which the CPSs can provide critical functions; therefore, it must operate without any interruptions. Thus, the cyber and the physical components implementation must be synchronized for ensuring continuous-time operation. In addition, in case an attack is occurred in the system, thus, the system must have sufficient resiliency and restoration for maintaining the operational status of the system, possibly at a degraded level of stability or security. Also, a balance between the energy/power is essential for the computation process and the energy/power consumed by the resource impressed for the actuation of the system. Moreover, for highly critical systems, patching processes are evaded as the patching needs to restart the system. These patches may trigger other procedures that may interfere with the system's operation. Since these systems' availability can compensate for the high risks of the vulnerabilities, they endure unpatched [119].

The 2nd requirement in CPS security is safety: for any CPS system, the safety of each component is a vital part. The CPS has smart context-aware system that takes decisions to stimulus the state's nearby physical and all its elements. The CPS should consider all the operating scenarios and count for all possible yield decisions. For the power electronics in the smart grid applications, mechanisms must be employed to guarantee that the power will not interrupt and no over-voltage delivery can occur [120].

The 3rd requirement in CPS security is integrity: the integrity of price information is considered a serious issue. For example, the hacker's negative prices can originate from an electricity employment spike as several devices would concurrently turn on to benefit the low bill. Though the integrity of commands and meter data is vital, their effect is commonly restricted to revenue loss. Instead, software integrity is serious since malware or compromised software can control any grid component along with the device [121].

Both cyber and physical securities should be secured. Indeed, they must be protected against environmental conditions and illegal interfering. For the power electronics in the smart grid applications, all the outdoors equipment should be placed in a weatherproof housing. Moreover, protocols and policies must be performed such that both information and the operational amenities of the CPS system are only accessed with tolerable authorization. Similarly, the confidentiality of the sensitive information of the CPS physical components must also be protected. The significant feature in the security of the CPS system is that cyber threats have a physical influence. Therefore, software security solutions that launch CPS threats are not enough. Hence, an inclusive methodology that considers both the cyber and the critical physical procedures of the CPS system [122]. There are two significant factors in designing the critical attack system: the attacker cost and the defender cost. The attacker cost comprises the knowledge and the resources mandatory for mitigating the attack. Meanwhile, the defender costs include power outages, equipment damages, and economic losses [123].

VI. THE POWER ELECTRONICS APPLICATIONS CPS SECURITY VULNERABILITIES

This section provides the main reasons for the vulnerabilities of the CPS security in the applications, which include the power electronics, e.g., smart grid and the industrial control systems. Then, we present the cyber CP, along with physical vulnerabilities in the power electronic systems existing in networked smart grid and industrial control systems applications. The CPS security vulnerabilities in the power electronics applications can be categorized into three types according to the CPS security aspect: the vulnerabilities in the cyber, vulnerabilities in the CP, and the vulnerabilities in the physical [124]. The main reasons and vulnerabilities of power electronics in the smart grid and the industrial control systems are summarized in Table 4. These vulnerabilities causes are discussed in detail as follows:

A. THE VULNERABILITIES REASONS IN THE POWER ELECTRONICS APPLICATIONS

1) ISOLATION ASSUMPTION

The main concern in designing the power electronic system is to be reliable, secure, and operate in a safe mode as the

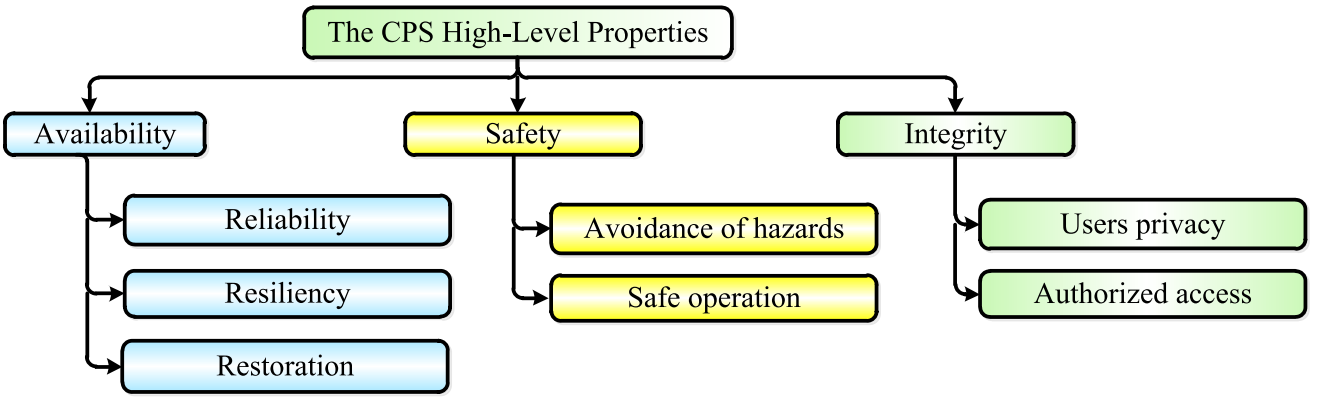

FIGURE 12. The CPS high-level properties.

TABLE 4. Summary of CP vulnerabilities types and reasons in smart grid and industrial control systems.

Application	Vulnerabilities	Type	The Main Cause
Smart Grid	Communication protocols	Cyber	Connectivity or isolation assumption
	Customers' privacy attack	Cyber	Connectivity, isolation assumption, or heterogeneity
	Insecure protocols	CP	Connectivity or isolation assumption
	Equipment physical stoppage	Physical	Isolation assumption
	Software	Cyber	Connectivity, isolation assumption, or heterogeneity
	Insecure smart meters	CP	Connectivity, isolation assumption, or heterogeneity
	Interconnected field instruments	CP	Connectivity, isolation assumption, or heterogeneity
Industrial Control Systems	Wired communications	Cyber	Isolation assumption or heterogeneity,
	Web-based attacks	Cyber	Connectivity or heterogeneity
	Software	CP	Connectivity or heterogeneity
	Equipment physical stoppage	Physical	Isolation assumption
	Open communication protocols	Cyber	Isolation assumption or openness
	Insecure secondary access points	CP	Connectivity or isolation assumption
	Insecure protocols	CP	Connectivity or isolation assumption

system design is supposed to be isolated from the outside world as well as, thus secure. The security was not important in the power electronic system, as the systems were thought to be outside isolated from the world, and consequently, considered secure. For instance, in the smart grid and the industrial control system, security depends on the supposition that systems are outside isolated from the world, as well as the control and monitoring operations are accomplished locally. Moreover, the implantable medical instruments were initially designed to be isolated from other external interactions as well as networks. Indeed, this isolation supposition also exists in the smart cars as the electronic control units' intercommunications security depends on their isolation from adversaries. Recent improvements in the CPS applications do not follow this isolation supposition, but somewhat more connectivity has been introduced. As more connectivity increases the number of access points to cars, therefore, more attack surfaces arise [125].

2) HETEROGENEITY

The CPS system comprises various components, and each section in this system has its own security problem. For instance, the component can be manufactured, implemented, or specified via various entities, as well as finally integrated via the system deployers. Therefore, the CPS building components are more incorporated rather than designed. This incorporation invites the intrinsic vulnerabilities of each product. Moreover, the inside details of incorporated heterogeneous components are unidentified, and consequently, they may cause unanticipated behavior when they are organized. This integration can invite the inherent vulnerabilities of every product. For instance, one step of the Stuxnet attack was to abuse the default password in Siemens programmable logic controller to access a computer operating a Windows OS. Most recent, the heterogenous components internal details are unidentified, as well as accordingly, unexpected behavior can be produced when they are deployed. Actually, most of the bugs that led to efficacious attacks in smart cars, for instance, were found at the boundaries of interconnected components fabricated via various vendors, where the improper suppositions interact [126].

3) COMPLEX CONNECTIVITY

The CPS system has many connections in which the manufacturers add various services that rely on wireless technologies and open networks. Both the smart grids and the industrial control systems are connected to the internet via control centers or business associated networks. These connections are complex and can make the system expose to serious attacks. Actually, most industrial control system attacks have been

internal till 2001; after that the furthermost of the attacks initiate from Internet-based sources. This is obviously, because of the increased connectivity used in the industrial control system. Furthermore, for rapid incident response along with more ease, some instruments are connected directly to the Internet. The medical instruments can have wireless abilities for easing the monitoring along with the reconfiguration. Smart cars can have more connectivity, thus, they are denoted as ''connected cars.'' This connectedness depends on wireless communications for example cellular, Bluetooth, satellite radio communications, along with RFID [127].

B. THE CP VULNERABILITIES IN THE POWER ELECTRONICS APPLICATIONS

The power electronic system CP security depends on protocols, e.g., Modbus, DNP3, and IEC 61850. Moreover, these protocols' deficiencies can affect the power of electronic system performance and the framework [50]. The protocols that lack encryption can make the data susceptible to eavesdropping and severe attacks or injecting false data due to the lack of authentication.

Other vulnerabilities in the power electrons applications are the usage of the smart meters, which have two-way communications that donate to various security concerns about the attacker's capabilities to avail the interaction. As the smart meter has a backdoor, it can make the attacker abuse to have full control over the device [128].

C. THE CYBER VULNERABILITIES IN THE INDUSTRIAL CONTROL SYSTEM

1) INDUSTRIAL CONTROL SYSTEMS COMMUNICATION VULNERABILITIES

The industrial control system depends on standard protocols like the TCP/IP and ICCP, which makes the industrial control system insecure due to insecure protocols. The TCP/IP's vulnerabilities have been inspected in [129], [130], but this protocol still has security concerns as it is not anticipated to be secure via the design. Indeed, the remote procedure call (RPC) protocol has security vulnerabilities, although it contributed to the renowned Stuxnet attack [131]. Moreover, the ICCP protocol, which interrelates control centers, deficiencies significant security measures like authentication and encryption [132].

The wired communications comprise the fiber-optic along with the Ethernet. The Ethernet can be employed in the substations in local area networks. The Ethernet can be exposed to interception and man-in-the-middle (MITM) attacks as the communication with the Ethernet uses the same medium.

The attacker can cause the MITM attack by interrupting the communication packet and altering its contents or forcing a sensor node to transmit incorrect data [133].

2) INDUSTRIAL CONTROL SYSTEMS SOFTWARE VULNERABILITIES

The most prevalent web-related vulnerabilities in the industrial control system software is SQL injection, in which the attackers can attack the databases' records without any authorization [54]. These databases are linked directly or indirectly to the industrial control system and comprising secret data, e.g., user's information or historical data. Moreover, electronic mails can denote malware dispersal to the network.

Furthermore, the deceivers can attack the network via the industrial control system connected to computers. Consequently, both the industrial control system and the network as a whole can be at risk. Indeed, the vulnerabilities can also include the connected devices to the internet such as the laptops of the employees' and smartphones, which can be exposed to do malicious activities, which affect the desired control devices operations [134].

D. THE CYBER VULNERABILITIES IN THE SMART GRID

1) SMART GRID COMMUNICATION VULNERABILITIES

The smart grid infrastructure information relies on internet protocols with familiar vulnerabilities that are used in launching the attacks on the grid. The TCP/IP is employed for the general-purpose connection to the internet and is not utilized for connecting to the control centers. The internet-faced networks directly or indirectly connected to the smart grid because of the network misconfiguration [135]. Moreover, the ICCP protocol for data exchange between control centers has serious buffer overflow vulnerabilities [136].

2) SMART GRID SOFTWARE VULNERABILITIES

In the networked smart grid, the smart meters can be easily attacked as it is remotely upgraded. The attacker can make a blackout via controlling the meters, either from the meters individually, or the control center. These vulnerabilities can be exploited via a software bug. The grid constituents can be accessible and provide a potential access point for pernicious hackers [137].

3) SMART GRID PRIVACY VULNERABILITIES

This vulnerability has emerged as a consequence of the 2-way communications between smart meters placed at the customers' houses along with the utility companies. Hackers can intercept the enormous amount of traffic produced from smart meters as well as infer secretive information about the customers [138]. The type of information hackers can be interested in, e.g., regular habits as well as residences' absence/ presence.

E. SMART GRID PHYSICAL VULNERABILITIES

The smart grids' field instruments are placed in insecure environments. Thus, numerous physical components can be highly exposed without physical security, and therefore, vulnerable to direct physical damage. For instance, the power lines can be susceptible to accidental, malicious, and natural attacks. Moreover, smart meters attached to houses, buildings, and remote areas, make them an easy goal to numerous physical attacks. It is even infeasible to attain sufficient physical protection of real assets in smart grids. Thus, it is

necessary to develop detection along with inhibition solutions [139].

VII. CP VULNERABILITIES IN SMART GRID

A. THE VULNERABILITIES IN SMART GRID COMMUNICATION

The infrastructure of the power system in the smart grids depends on these protocols, e.g., Modbus as well as DNP3. Moreover, IEC 61 850 has also been introduced lately as an enhancement of these protocols in the substations' communications. The shortage of security features in these protocols has a different influence on the smart grids' situation. For instance, protocols without encryption can make the data in transit vulnerable to eavesdropping, which results in various attacks, e.g., injection of false data because of the lack of authentication [140] or the implication of customers' usage patterns [141]. Indeed, it is also conceivable to inject false data, resulting in decisions based on false information [142], or inject the network with false packets that target to flood it, resulting in a DoS attack.

The smart grids comprise of heterogeneous components run through diverse entities. For instance, a generation plant of a grid correlates with a transmission plant, where the transmission plant can interact with the distribution plant. Finally, the distribution conveys electricity to customers. Each kind of interface is regularly administered as well as run via various companies, which introduce vulnerabilities in communication and collaboration [143], [144].

B. SMART GRID VULNERABILITIES WITH SMART METERS

Smart meters depend on two communication methods, which donate to several new security prospects about an attacker's aptitudes to abuse such interaction [145]. For instance, the smart meter can have a backdoor as the attacker may exploit to have full control of the device. Aside from the customers' accounts with restricted aptitudes employed for elementary configurations, this login account can give full control to the manipulator over the smart meter. Furthermore, the communication can be transmitted via telnet which is recognized for major security weaknesses, such as sending data in clear text lacking encryption.

In case complete control on the smart meter occurs, three possible attacks may arise:

1) Power disturbance via malicious connections with supplementary devices for altering their desired power consumption, or indirectly, via injecting false information as the control center can receive false data and make incorrect decisions.

2) Employing the meter as a ''bot'' for launching attacks alongside other smart meters or systems in the smart grid network.

3) The meter's collected data can be interfered with so that the bill reveals false data for minimizing the bill to the consumer [146].

VIII. ANALYSIS AND IMPACT OF CYBER-ATTACKS VULNERABILITY ON CONTROLLING THE VOLTAGE SOURCE CONVERTERS

A. CYBER-SECURITY

As communication technologies are fast spreading, the disturbances on the cyber components are becoming a reality. These disturbances can considerably affect the performance of the smart grid. Indeed, due to the increased penetration of voltage source converters in the smart grids, their serious effect on the system as it can be easily attacked cannot be ignored. This makes researchers concentrate on designing safe control approaches besides conventional encryption-based methods. In general, spoofing attacks can be caused by communication links along with sensors, where the signals are either quantized, interrupted, or intimidated. The spoofing attacks types include caller ID spoofing, website spoofing, email spoofing, IP spoofing, GPS spoofing, and text message spoofing. These spoofing attacks occur when the attacker or the malicious program effectively acts on another person's (or program's) behalf via mimicking the data. Moreover, the attacker can pretend to be someone else or another computer, device, etc. For the IP address spoofing attack, the attacker can send the IP packets from a spoofed source address for disguising itself. The DoS attacks often employ the IP spoofing to overload networks along with devices with packets, which seem to be from legitimate source IP addresses. The FDI attacks are caused by injecting auxiliary signals or altering the measurement content conveyed via the sensors [147]. Meanwhile, the MITM attack occurs in the communication links [148]. In the case of signal jamming, which may lead to an interruption in transmitting the signals, this attack is known as DoS attack [149].

The cyber-attacks can be performed on load aggregators, smart meters, as well as sensors in an active distribution network for degrading the power flow management, voltage stability, frequency regulation based ancillary services, etc. In addition, any argumentative outbreak into the cyber channels via numerous methods, e.g., changing the measurements communication, jamming the information flow, and disabling cyber links can introduce system shutdown. The guarded nature of these attacks relies on several factors, e.g., the attacker's ability to pierce into the system particulars and the degree of system information developed via the hacker.

The control layers can be implemented in real-time processors. The intrusion into the control layer only permits access to the commanded set-points (frequency, DC-link voltage) throughout the run-time rather than the inner control layers [150].

The inner loops can be compiled into the processor's read-only memory; thus, the sensor values disturbance cannot mislead the system operation. The system dynamics can fluctuate when the references are altered to activate the protection layer or trigger instability. This can be described mathematically employing the state-space representation of i^{th} voltage

source converter for:

$$\begin{cases} \frac{dX_i}{dt} = AX_i(t) + BU_i(t) \\ Y_i(t) = CX_i(t) + DU_i(t) \end{cases} \quad (3)$$

$\forall i \in n$, where $X_i = [V_G, I_G, P, Q, V_{DC}]^T$, meanwhile, $U = [\omega^*, V_{DC}^*, P^*, Q^*, E^*]^T$ with the state parameters represented through the grid voltage, grid current, active power, reactive power, DC-link voltage, respectively; and the input comprising of the frequency command, DC-link voltage command, active power command, reactive power command along with inverter voltage command for i^{th} voltage source converter, respectively. Indeed, $X \in \Re^n, Y \in \Re^S, U \in \Re^m, A \in \Re^{n\times n}, B \in \Re^{n\times m}, C \in \Re^{p\times n}, D \in \Re^{p\times m}$.

For simplification, the output variable as well as each state can be individually compromised via the deceiver. The attack signal $\xi_i(t) \in \Re^{p+n}$ relies definitely on the strategy of the attack. In case $\Sigma = \{\xi_1 + \xi_2, \ldots \xi_{n+p}\}$ represents a null vector. Thus, the response of the system is unbiased. For detecting the existence of the cyber-attack element, a residual signal $R : \Re \geq 0 \rightarrow \Re^p$ test can be followed. It does not consider a design parameter, as it relies on the attacker's intent [151].

Remark 1: The attack signal's nature and magnitude can be unbounded/bounded and entirely reliant on the attacker's intention. Though the corrective control measures design to guarantee a resilient system is always performed, the nature of the attack remains.

The attacks can be detected by employing a centralized attack detection filter using a modified Luenberger observer. Thus, the estimated dynamics of i^{th} voltage source converter with identified initial states *X(0)* are defined by (4):

$$\begin{cases} \frac{d\hat{X}_i}{dt} = (A + GC)\hat{X}_i(t) - GY_i(t) \\ R_i(t) = C\hat{X}_i(t) - Y_i(t) \end{cases} \quad (4)$$

where $\hat{X}_i(t)$ represents the estimated state. Indeed, $\hat{X}_i(0) = X_i(0)$ as well as the injection matrix output $G \in \Re^{n\times p}$ is such that $(A + GC)$ is Hurwitz.

Remark 2: $R_i(t) \leq \bar{R}$ if and only if $\xi_i(t) = 0$ for $t \in \Re \geq 0$ where $\bar{R}$ is an inconsiderable value.

The physical disorders, e.g., faults, load change, line outage, will always follow Remark 2 as the model dynamics will always be unchanged via employing the unbiased measurements throughout these disorders. Instead, the inner control loops are robust against the cyber-attacks as it works with a tracking objective for each state. The inner control loop is full against cyber-attacks only when the outer control loop is unattacked [152].

The artificial dynamics produced by the attack element is nullified in (3), if (5) is fulfilled:

$$\sum_{i=1}^{n} \xi_i = 0 \quad (5)$$

Indeed, the attacks in the attack set $\sum$ can be classified as unidentified from the monitors, if and only if $X \in \Re^n$ when $\|sI - A\| o + \|CX\| o = \phi$, where $|\Sigma| = \phi$. These attacks are generally designated as coordinated attacks, as they are efficiently bypassing the attack filters illustrated in (4).

Via employing (5), the control inputs can either be manipulated in the communication links or the controller through an external entity. Due to the strict couple between the cyber and control layers, the exposure to cyber-attacks intensifies for an interconnected system of voltage source converters. Due to the increase in attack-vulnerable points, the ancillary sustenance provided by the connected voltage source converters can be simply misled, causing system collapse. These outcomes ultimately cause techno-economic disasters by defaming the electric network with the FDI attack vectors into the CP layer [153].

B. VULNERABILITY ANALYSIS OF CYBER-ATTACKS ON THE CONTROL OF VOLTAGE SOURCE CONVERTERS

1) Grid-forming control for voltage source converters: Fig. 13 depicts the traditional control structure for the grid-forming voltage source converters. The black and blue lines in Fig. 13 signify the communication layer along with attack elements injected into communication link/sensors, respectively. The grid-forming voltage source converters can regulate the frequency as well as the voltage locally. For the synchronization with other AC sources, a primary droop control needs to be aligned locally via employing the available measurements. This structure is significantly safe from the cyber-space aspect as the attackers cannot access the physical layer. Furthermore, beamforming is widely employed as suitable physical layer security [154]. Though, the decentralized control strategies undergo an operational perspective in matching the commercial, regulatory standards [155]. This disadvantage has been solved via employing a secondary controller using the information from other voltage source converters. The centralized or distributed secondary control strategies can be imposed on the primary control law for offsets compensation. Though, this creates a large vulnerable space for the hackers to find the attacked data either into the controller, the communication link, or the sensors. The common intrusion techniques for manipulating each component are discussed below:

- Sensors: The sensors' data can be used via the adversary penetration in the control platform. This penetration is simply accomplished via Trojan Horse [156] in which the remote systems are employed as hosts. From the acquisition panel, the sensor output is usually within 15 V. For calibrating it alongside the real measurement, acquisition gains using a linear plotting system is utilized. The attacker usually tries to alter the acquisition gains to create a bias in the reported measurements.
- Communication Links: Communicated data is handled either inside the communication stage comprising

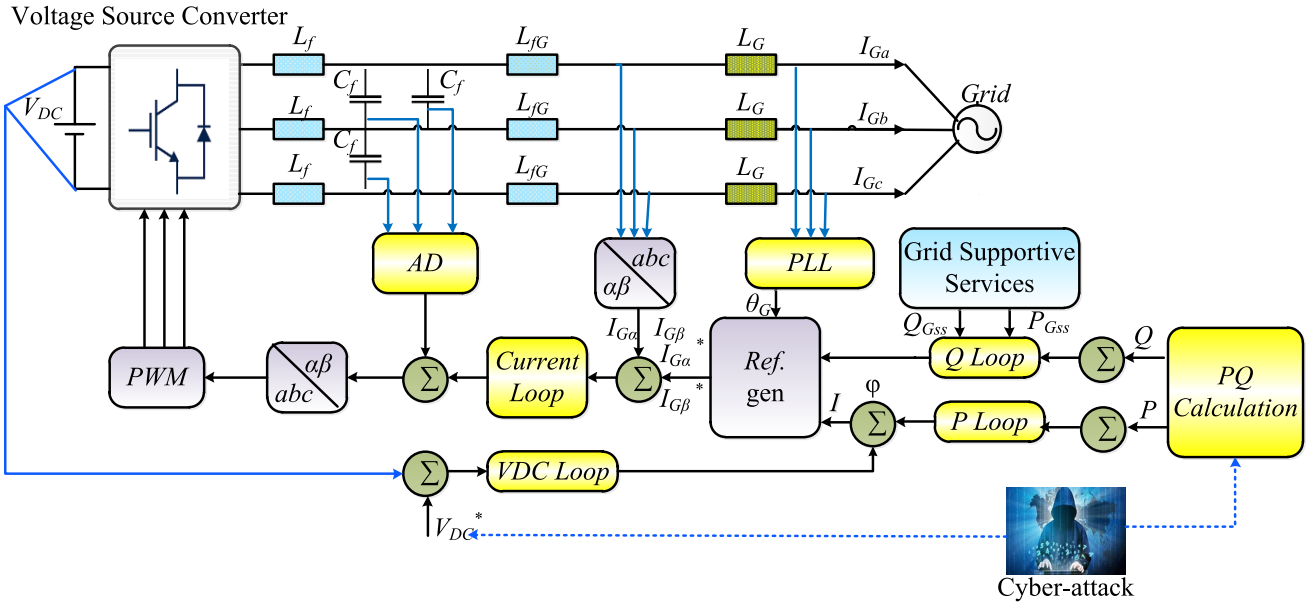

FIGURE 13. The *P-Q* control of grid-supportive voltage source converter: The black and blue lines signify the communication layer as well as attack elements injected into communication link/sensors, respectively.

a decoder/router/encoder or the controller. There are numerous ways in which the transmitted data can be managed, e.g., rerunning the transmitted information from the past, disruption of the transmission of signals, authorization violation, illegal opening of information logs, etc.

- Controller: The controller can be illegally accessed via employing Trojan Horse for altering the reference inputs used in the secondary controller for controlling the voltage source converters or the outer control loop.

2) Grid-feeding and supporting control for voltage source converters: For the voltage source converters, the grid feeding control is used for injecting reactive/active power in the grid-forming units. This strategy is widely employed in grid-connected applications to integrate renewable energy sources [157]. Via adding the desired control inputs to the overlaying grid-forming controller, the supportive grid services can be enhanced, as depicted in Fig. 13.

The commanded DC-link voltage V_{DC}^* or the measured DC-link voltage via the sensor V_{DC} are generally vulnerable to cyber-attacks, as the attacker can either increase or limit the flow of the power from the voltage source converters, thus making a coordination/stability problem in the network. Furthermore, the output of the grid-supportive service Q_{Gss} as well as P_{Gss} can also be multifaceted with false data for misleading the controlled units.

Table 5 summarizes the vulnerable points of the attack in the grid-feeding as well as grid-forming voltage source converters control. It is clear that the references or the measurement signals, signified as X_j, can be transmitted by supplementary units to the upper-level control, whichever for secondary control objectives or for grid-supportive services [158].

IX. THE CPS ATTACKS MITIGATION

In case the signs of the attack have been endorsed, thus, mitigation efforts will be performed via the system operator for reducing the damages along with potential disruptions. When the attack is cleared from the system, prevailing restoration as well as mitigation mechanisms can successfully continue the safe along with consistent power system operations. Though, if the attacking threat is not detected, thus, the operator needs to consider persisting malicious endeavors in the system. In these interactive scenarios, mitigation approaches are generally modeled as well as solved via bi-level optimization or game-theoretic approaches [159]. The detailed common CPS controls, smart grid cyber controls, smart grid CP controls, along with the defense mechanisms are discussed below.

A. COMMON CPS CONTROLS

Via addressing the causes of the vulnerability, the proper solution can be employed for mitigating the severe attacks as discussed below:

1) Controls alongside extra connectivity: Innovative security concerns must be considered for safeguarding the access point from illegal access. Moreover, the communication protocols employed for recognizing such connectivity are either copyrighted protocols, e.g., DNP3 and Modbus in deployed the smart grids, or open protocols, e.g., IP/TCP. The copyrighted protocols are burdened with various vulnerabilities as a result of the isolation supposition when designing the protocols [160].

2) Communication Controls: The security solutions at the communication level in the smart grid should consider the differences with conventional IT solutions. For instance, an intrusion detection system (IDS) should be time-critical as long delays are excruciating [161].

TABLE 5. The vulnerable points in the control stages of different voltage source converters types.

	Current Control	Outer Control	Secondary Controller	Grid-supportive Services
Grid-forming	x	Q^*, P^*	MITM attack on V_j, ω_j (j: represents the communicated measurements), DoS/ FDI on (V_i, ω_i, P_{sec}, Q_{sec}) (sec: denotes the secondary controller)	x
Grid-feeding	x	V_{DC}^*, V_{DC}	x	x
Grid-supporting	x	x	x	P_{Gss}, ω^*, Q_{Gss}, E^*

3) Device Verification: CPS components with running software requisite to authenticate the software's authenticity.

This authentication can minimize malware effectively. For instance, hardware-based solutions, e.g., trusted platform module (TPM), afford code attestation.

Though, TPM is supposed to be physically secure, which is unpractical to assure in the smart grid CPS applications.

Moreover, the TPM is the computational overhead on the restricted resource CPS applications. Hence, the TPMs emerging generation, which takes into account the restricted CPS resources, is required [162].

B. SMART GRID CYBER CONTROLS

a) DoS controls: The attacks on the communication components should be prohibited and easily detected. The DoS attack prevention is generally accomplished by reconfiguration of network architecture, rate-limiting, along filtering malicious packets. The DoS and communication components attacks can occur in smart grids, while the DoS attack is difficult because of its comparatively static nature. Moreover, the physical layer techniques are employed to prevent the attacks of the nature of wireless jamming. Instead, DoS detection methods can be classified into four types:

1) Hybrid detection; 2) Proactive detection; 3) Packet-based detection; along with 4) Signal-based detection techniques [163].

b) Privacy-protective controls: The shortage of confidentiality in data aggregation protocols (DAPs) can result in a privacy attack on consumers' information. For example, the energy use patterns and billing information [164], while the shortage of integrity disturbance in the consumption reports along with state estimation [165]. Consequently, various privacy-preserving methods have emerged to provide aggregated data with integrity and confidentiality when in transit between control centers and smart meters [166]. Another privacy that can affect safety or finance is the aptitude to identify the (in) occupancy to break in. Chen *et al.* in [167] have introduced combined privacy as well as heat mechanism for making the poser convention data always seems like the house is occupied and, thus, tricks occupancy detection methods.

c) FDI controls: Yang *et al.* in [168] introduced a polynomial-based compromise-resilient en-route filtering approach. This approach has been designed to prevent the FDI attacks by filtering the false data successfully and accomplishing a high resilience to the number of compromised nodes without depending on node localization and static routes.

d) Standardization: Several bodies, e.g., the National Institute of Standards and Technology (NIST) and IEC, have established a set of standards for safeguarding smart grids' communications. For instance, IEC's have established standards 61850 and TC57 [169]. Meanwhile, NIST has established recommendations for smart grids in report 7628 [170].

C. SMART GRID CP CONTROLS

a) IDS: The IDS for smart grids is considered an enduring problem, which is not developed yet. The IDS design for smart grids is a complicated assignment because of the vast size of the grids as well as the heterogeneity of their components [171]. Furthermore, IDS employed for conventional IT systems will not essentially work for the smart grids. They are precisely designed for smart grids to minimize the probability of false detection rates. G. Pu *et al.* in [172] introduced an anomaly-based IDS, which can detect malicious actions by employing artificial ants with a Bayesian reasoning approach. Moreover, H. Hindy *et al.* in [173] have introduced behavior-rule-based IDS for attack detection on CP devices in the smart grids, e.g., subscriber energy meters, headends, as well as DAPs [174]. Y. Peng *et al.* in [175] have presented an IDS for bad data injection attacks detection aiming the smart grids. Their technique depends on combining detecting methods from the conventional IDS along with physical models. M. Eskandari *et al.* in [176] have introduced another IDS based on two detection methods: 1) watermarking and 2) anomaly detection methods.

b) Low-level authentication and authorization: The common obstacle in the smart grids is users' authorization and authentication for accessing low-level layers, e.g., field devices. Generally, entire field devices can share the same password that employees know. This results in the unfeasibility of the nonrepudiation security requisite. The malicious employee can gain access to the field device and perform unwanted alterations to the system, and who did it is traced. Thus, T. Dimitriou *et al.* in [177] have introduced an authorization and authentication mechanism, which can provide legitimate employees the aptitude for accessing the field devices in smart grids' substation automation systems. This technique depends on elliptic curve cryptography because of its low computation and key size desires compared with former public key methods.

c) Emerging designs: emerging, innovative security issues need numerous aspects of smart grids to be

approached differently. The CP system's nature needs to be taken into consideration. P. S. P. Pessim *et al.* in [178] have presented CP security, an innovative technique that combines cyber-security controls and systems-theoretic. They introduced two examples, which showed the applicability of their approach on two attacks on the smart grids: 1) stealthy deception as well as 2) replay attack. They endorsed the requisite for taking into account those two types of components, physical- and cyber-components, for the smart grids.

d) Security extensions: Adding-on security trends to prevailing components of the smart grids has been emerging. Protocols such as IEC 61850, DNP3, and IEC 62351 are extended to capture the security properties. For instance, a secure DNP3 protocol is an extended DNP3, which has elementary confidentiality, integrity, and authentication services. The security geographies are added via interleaving a security layer in these protocols' communication stacks [179].

e) Smart meters' deactivating inhibition: For avoiding remote attackers who can exploit the deactivating inhibition in the smart meters, A. S. Sani *et al.* in [180] have proposed that smart meters can be programmed for notifying customers in enough time beforehand before the command takes outcome as well as deactivates meters. This measure can indicate the early detection of DoS attempts before occurrence.

D. DEFENSE MECHANISMS

Attacks have been investigated in numerous applications that are intensively reliant on distribution systems with solar farms [181] and power electronics converters. It also contains smart grid components with voltage support devices [182]. Power electronics have driven HVAC (heating, ventilation, as well as air conditioning) systems [183], along with microgrids [184], [185]. They generally concentrate on either detecting or analyzing cyber-attacks influencing grid functionality, stability, and operating costs. Quick detection, as well as identifying the cyber-attacks, is crucial for a reliable along with the safe operation of the smart grid. The attacks can be avoided via a defense-in-depth pattern that can detect, prevent, and safeguard the system against these attacks.

The defense techniques use mechanisms that barricade the attack's accomplishment to limit its influence on the power electronic systems. These defense techniques embrace the encryption and secure communication protocols, which are the 1st seed in the defense against cyber-attacks; the circuit breakers along with relays are considered defense devices that can prevent severe faults [186].

The defense alongside the CP attacks in the power electronic system can be categorized into three groups:

Detection: the detection techniques are used when defense methods are failing in thwarting the disturbance; these methods employ models of the anomalous behavior in addition to the system measurements to recognize the abnormalities. The detection methods can also be performed via utilizing sensors to identify the attacks faster or by adding extra layers of security to the elements exposed to attacks. Moreover, the detection techniques can detect the undesirable system state's incident, actual cyber-attack, or both of them. Additionally, reaction techniques can be employed to recover the system from the disturbance and control the power electronics system operation effectively [187].

Prevention: the prevention refers to the security approaches that avert the attacks by employing authentication, security policies, access controls, and network segmentation. Since the attack is intelligent and can respond to the prevention action, the incorporation between the defender and the attacker is modeled via game theory.

Response: as the power electronic system CPS has real-time restraints, the security approach needs to act automatically without human intrusion for rapid attack mitigation. Actions executed after a detected attack are reactive responses that aim to restore the power electronic system and mitigate the attack influence. After detecting an attack, a mechanism is updated and modified automatically to counteract the attack [122].

Comprehensive researches have been conducted for fulfilling the smart grid security via detecting as well as identifying the cyber threats and protecting the smart grid from the attackers as illustrated in Table 6 with detailed discussion below:

In [188], the distributed multi-agent approach has been developed for identifying as well as detecting the cyber threats on smart grids protection systems. The agent-based intrusion detection system employed the relay status logs, synchrophasor data, as well as network event monitor logs for identifying the events precisely. Moreover, the designed agent-based approach successfully discriminated the attack from the fault as well as the agents' employed accessible information for preceding their operation in case the communication disappointment. In addition, the results provided a platform for implementing the proposed approach on the infrastructure of the relay, which is an effective tool for detecting along with counter measuring probable cyber threats.

In [189], a rapid decentralized technique for detecting the cyber-attack via employing the maximum likelihood (ML) estimation which can exploit the near chordal sparsity of smart grid for establishing an effective framework to elucidate the associated ML estimation problem via applying the Kron reduction of the Markov graph of phase angles. This detection technique is afterward decomposed to numerous local ML estimation problems for guaranteeing privacy as well as reducing the underlying problem complexity. The simulation results validated the efficacy of the proposed technique in detecting real complex stealthy FDI attacks.

In [190], an online attack/anomaly detection problem has been formulated as a partially observable Markov decision process (POMDP) problem, as well as a universal, robust online detection algorithm has been proposed via employing the framework of model-free reinforcement learning (RL) for POMDPs. The numerical results endorsed the proposed

TABLE 6. The CPS defense mechanisms in the smart grid.

Technique	For Detecting	Reference
The distributed multi-agent approach	Cyber threats	[188]
Maximum likelihood (ML) estimation approach	Cyber-attack, FDI attacks	[189]
Model-free reinforcement learning for POMDPs	Cyber-attacks	[190]
Unsupervised anomaly detection technique according to the statistical correlation between measurements	Distinguishing the real fault from the disturbance	[191], [192]
Supervised machine learning along with a model-based logic	Evaluating the type of activity e.g. normal, perturbation, attack and perturbation-and-attack.	[193]
The interval state estimation-based defense	Sparse cyber-attacks	[194]
Wavelet singular values as input index of deep learning approach	FDI attack detection	[195]
Unsupervised machine learning-based approach	CDIA in the communications networks	[196]
An enhanced online RL approach entitled nearest sequence memory Q-learning approach	FDI attacks	[197]
The deep reinforcement learning	Cyber-attacks	[198]
Cognitive dynamic system	FDI attacks	[200], [201]

RL-based technique's effectiveness in timely along with precise cyber-attacks detection aiming the smart grid.

In [191], an unsupervised anomaly detection technique according to the statistical correlation between measurements has been introduced. Via this technique, a scalable anomaly detection engine has been designed for large-scale smart grids, which can distinguish the real fault from the disturbance as well as a smart cyber-attack. In this technique, a symbolic dynamic filtering (SDF) has been employed for reducing the calculation burden while realizing causal exchanges between the subsystems. According to the free energy as the anomaly index, learning algorithms based on the Boltzmann machine and dynamic Bayesian network perception have been employed to detect the unnoticeable attacks. This technique has been assessed on various IEEE test systems under different operating conditions for numerous measures (false positive rate, true positive rate, and accuracy) values. The outcomes revealed that the system had fulfilled a precision of 99%, a true positive rate of 98%, and a false-positive rate of less than 2%.

Moreover, due to the wide developments in the IoT along with the artificial intelligence technologies, various research interests are pointed towards employing the data science as well as the big principles to secure systems from adversarial attacks. The usage of the machine learning and artificial intelligence for cyber-security initiated with its implementation in IDS. The research in this area comprised anomaly along with malware detection in communication and information systems. The machine learning has been employed to attain cyber-security in IoT and smart grid systems [191], [192].

Great efforts have been performed to address the IoT networks issues of the security and privacy via conventional cryptographic techniques. Nevertheless, the distinctive characteristics of IoT nodes render the current solutions inadequate to cover the entire security spectrum of the IoT networks. Machine learning along with deep learning approaches, which are capable of providing embedded intelligence in the IoT networks and devices, can be leveraged to deal with different security problems.

In [193], an anomaly detection (AD) approach employing supervised machine learning along with a model-based logic for mitigation has been proposed. This approach considered the input of the wide-area damping control measurement signals and the output of wide-area damping control signals as input for evaluating the type of activity e.g. normal, perturbation, attack and perturbation-and-attack. For the anomaly detection, the mitigation module tuned the wide-area damping control signal and made the control status mode as either local mode or wide-area mode.

In [194], an interval state estimation-based defense approach has been introduced innovatively for detecting the sparse cyber-attacks in the smart grid. In this approach, the upper as well as lower bounds of each state variable are modeled as a dual optimization problem for maximizing the variation intervals of the system variable. A typical deep learning, i.e., stacked auto-encoder, has been designed for properly extracting the nonlinear characteristics in electric load data. These characteristics are then applied for enhancing the precision for electric load forecasting, causing a more narrow width of state variables.

In [195], a novel approach of FDI attack detection has been proposed based on wavelet singular values as input index of deep learning approach. Via this approach, a switching surface based on sliding mode control (SMC) breaks down has been employed for adjusting precise factors of wavelet transform. Afterwards, features of wavelet coefficients have been extracted via singular value decomposition. Indexes have been determined based on the wavelet singular values in switching surface of current along with voltage which states the input indexes of deep learning as well as detecting the FDI attack.

In [196], an unsupervised machine learning-based approach for detecting the covert data integrity assault (CDIA) in the smart grid communications networks employing non-labeled data has been introduced. This approach employed a state-of-the-art technique, entitled isolation forest, as well as detected the CDIA according to the hypothesis that the assault possesses the shortest mean path length in a constructed random forest. For tackling the

dimensionality issue from the growth in power systems, the authors employed a principal component analysis-based characteristic extraction approach.

In [197], an enhanced online RL approach entitled nearest sequence memory Q-learning has been adopted for making the attack more effective. In this approach, an inherent property of viruses has been described employing a propagation-evolution model, which served as the exploration mechanism for the FDI attack. In addition, for validating this approach, co-simulations of daily operations of the IEEE 39-bus system have been performed in which both the automatic voltage control system and the proposed FDI attack have been modeled.

For recovering from a cyber-attack, it is recommended to reclose the transmission lines when the attack is detected. Nevertheless, this can cause various influences on the power system, e.g. power swing along with current inrush. Thus, it is serious to accurately select the reclosing time for mitigating these influences. In [198], a recovery approach for reclosing the tripped transmission lines at the optimal reclosing time has been proposed. Particularly, the deep reinforcement learning approach can be adopted for endowing the strategy with the aptitude of real-time decision-making as well as the compliance of uncertain cyber-attack scenarios. In this context, the environment has been established for simulating the dynamics of the power system at the attack-recovery procedure as well as generating the training data. Via these data, the deep reinforcement learning based approach can be trained for determining the optimal reclosing time.

The investigation of the coordinated topology attacks in smart grid, which employs a cyber-topology attack along with a physical topology attack has been introduced in [199]. The physical attack first trips the transmission line (TL). For deceiving the control center, the hacker can mask the tripped line outage signal in the cyber layer and afterwards can create a fake outage signal for another TL. The main target of the coordinated topology attacks is to overload a critical line, which differs from the physical tripped line as well as the fake outage line via confusing the control center into making incorrect dispatch. Thus, for determining the attack strategy, a deep-reinforcement-learning-based approach has been proposed for identifying the physical tripped line along with the fake outage line and determining the minimal attack resources.

As the FDI attacks have been considered to be the most dangerous cyber-attack in the smart grid, as it can lead to cascaded bad decision making throughout, a new approach of thinking that can characterize itself via uniting two entities, a cognitive dynamic system (CDS) has been introduced in [200]. This approach can provide an indication of the smart grid's health on a cycle-to-cycle basis as well as it can be employed for detecting the FDI attacks. Accordingly, enhancing the entropic state is the target of the supervisor.

The CDS has a structured research tool along with physical model inspired via certain characteristics of the brain. The cognitive risk control is considered an improved characteristic of the CDS, which can embody the predictive adaptation concept permitting it to bring risk under control in situations containing unpredicted or irregular uncertainty as the cyber-attack [201].

X. THE CPS SECURITY CHALLENGES

Though challenges, threats, and vulnerabilities terminology are sometimes employed interchangeably, each terminology is used to shed light on a diverse perspective of the CPS security.

Challenges are open problems which are still mysterious as well as research struggles are performed for solving these problems.

Meanwhile, the vulnerabilities denote the system's internal security weaknesses, which can be exploited via the attackers, whereas threats are external situations, which are possibly destructive. In this section, CPS challenges are addressed based on the observations from the literature survey as well as categorize into common along with application-specific challenges [202].

A. COMMON CPS SECURIT CHALLENGES

1) CP Security: Both the cyber and physical aspects in the smart grid applications should be secured by the designers. Thus, cyber-attacks with physical significance will be better predicted as well as accordingly mitigated [203]. S. Rafi in [204] proposed that in case the basic differences between physical and cyber aspects are not taken into account, CP solutions are commonly disregarded, and the emphasis becomes cyber-only solutions. This urges the requisite for taking into account both physical- along with cyber-aspects.

2) Security through Design: Security is not considered in the CPS design as a consequence of their isolation in physically protected environments without any connection to further networks, for example, the Internet. Therefore, physical security has been practically the only security measure [205].

3) Real-Timeliness Nature: Real-time requisite is significantly needed as its absence can affect the security posture [206]. During the attack, real-time decisions in CPS are vital for the survivability of the systems. Thus, taking into account the interactions between cyber and physical-features in the design of the CPS security can give the system a complete picture, which helps in designing superior attack-detection, risk-assessment, and attack-resilient solutions [207]. Moreover, cryptographic mechanisms can cause various delays, which can affect the real-time deadlines. Thus, lightweight along with hardware-based mechanisms should be taken into consideration.

4) Uncoordinated Change: The CPS stakeholders' number is somewhat large. This comprises operators, implementers, consumers, administrators, as well as manufacturers. Their privileges along with activities vary, and therefore must be managed accurately [208]. The enormous numbers of heterogeneous CPS components along with stakeholders need management change. This is considered another challenge which is somewhat disregarded. When a cluster of CPS components

has changed, careful coordination is requisite at a certain level through the stakeholders. These alterations may include hardware changing, software changing, or updating, as well as improving new aptitudes [209]. The uncoordinated alteration can change the preliminary assumptions concerning CPS security; thus, numerous vulnerabilities can be introduced.

B. SMART GRID CHALLENGES

1) 2-Way Communication: This communication is considered one of the distinctive geographies of the smart grids because of employing the AMI. The smart meters are employed in the AMI on the consumers' houses, which can be effortlessly reachable via the physical attackers for communicating with utility companies. This increases a new challenge for protecting the instruments [210].

2) Access Control Approaches: Because of the large number of stakeholders and the vast geographical coverage of smart grids, proper access control approaches are required [211]. Each probable access to the smart grids' network, data, or instruments must be controlled as well as managed. Furthermore, throughout the emergency, access control approaches requisite to having adequate flexibility for giving proper treats for the correct sections.

3) Privacy Prospects: Due to the significance of consumers' data in the smart grids' traffic; thus, privacy regards became a big challenge. The consumers' data must be encrypted, and anonymization approaches are correspondingly requisite for preventing the inference and further attacks from inferring patterns by the encrypted data for disclosing secretive information [212]. Various cryptographic-based solutions have been introduced. W. Gao *et al.* in [213] introduced a homomorphic encryption mechanism for safeguarding the privacy of the consumers while keeping low overhead on smart grids' traffic. Though, this technique does not inhibit the deceiver from contributing in the data aggregation as the smart meter via mimicking a legitimate smart meter or injecting false data. Thus, designing mechanisms, which can aggregate and encrypt data securely, is a challenging issue.

4) Inclusive Security: Security tools and measures virtually present at higher levels in smart grids as well as their efficacy reduce to lower levels. The security measures complexity reduces in low levels because of the inadequate aptitudes in low-level instruments. Thus, security is needed to be included in each part of the smart grids, initiating from the lowest levels such as field devices and their protocols to high levels, such as the control centers. Via implementing the security at lower levels; thus, the performance costs will be increased. Hence, the solutions for lightweight are preferred. Encryption is essential for providing integrity and confidentiality at entire smart grids levels. Deploying the encryption is not a challenge, but the real challenge is in achieving it cost-effectually in the components of low level [214].

5) Obvious Trust: Sent commands and sensed data should not be obviously trusted. Instead, innovative mechanisms are required for detecting unauthorized commands as well as false data. Due to the large size of smart grids, the FDI attacks can be detected easily depending on techniques, which have been designed for detecting and identifying faults only.

6) Alteration Management: Smart grids are undoubtedly more different as well as have numerous stakeholders than ICS applications, along with their alteration management aptitudes are restricted. This alters the management in the protected smart grids.

XI. CONCLUSION WITH CHALLENGES

In this paper, a comprehensive survey on the CPS security on the digitally-controlled power electronics for the networked smart grid application has been presented. The potential threat sources, along with their motivations, have been extensively surveyed. This paper also discussed the existing vulnerabilities in the networked smart grid by highlighting the main reasons with real examples and the mitigation approaches for the CP attacks. Indeed, the impact and vulnerability analysis of the control, communication, and physical layer employed for handling the voltage source converters have been presented.

Furthermore, the existing control mechanisms for the networked smart grid have been summarized with identifying the unsolved issues. The research trends and challenges in securing the CPS in the networked smart grid have been introduced.

As a result of the complicity, variability, as well as smartness of network attacks, the prevailing security solutions cannot be attained via one definite solution. Based on the control-theoretic-approaches, the side of the attack always attempts their effort to exploit their damages on the control performance, whereas the defense side will spare no struggle to reduce the effects of the analogous attacks. Consequently, the networked smart grid CP security should be taken into account from both physical-security along cyber-security.

The subsequent issues should be addressed for safeguarding the networked smart grids.

1) Security detection associated with modern approaches: Enormous amount of data generated via the power distribution devices, AMIs, and other smart instruments enact lots of problems on security analysis and detection in the smart grids. Thus, it is very significant to improve some emerging new transmission systems to enhance communication efficiency; indeed, the big data and clouding computing technique can provide a new chance for anomaly detection, electric load anticipating, and demand-side management approaches. Hence, security detection associated with modern analysis approaches is a motivating issue in the future.

2) Distributed detection as well as estimation of attacks: The smart grid's complexity as well as spatial distributions, which are integrated with CP-control, increases the estimation dramatically along with detection difficulties, particularly in the distributed environment. Furthermore, multiple attacks can occur at the same time for such a large scale of networked smart grids. Accordingly, how to estimate as well as locate diverse attacks in a distributed way is of vital significance.

3) Modeling the attacks via employing experimental conditions: There are some particular assumptions, e.g., probability and periodic distributions that are often presented in various smart grids' researches. Nevertheless, these assumptions violate the point of view that the attacks are usually stealthy as well as arbitrary. For instance, the packet dropouts issued from the DoS attacks may not follow Bernoulli distribution in the smart grids. Particular prevailing results based on the unfeasible assumptions are away from real applications. Thus, modeling these attacks in a different realistic manner needs to be studied more.

4) Resilient control approaches: As a counterpart of IT safeguard technique, security control approaches' design plays a vital role in preserving the smart grids. When conventional IT safeguards are worthless, the control implementations will lead to a noteworthy enhancement in assuring the performance of the smart grid. In addition, the control design should fulfill general requisites when no attacks are existing. Instead, it is still valid for malicious attacks rather than changing or redesigning the controller. Consequently, how to design a security controller in a resilient manner is an encouraging issue in the future.

There will be different approaches for detection, mitigation, along protection alongside cyber-attacks than those addressed in this review. Well, innovative approaches and measures will definitely be developed in the future for safeguarding the smart grid components from malicious attacks. This survey collected the state-of-the-art implemented previously otherwise explored solutions for providing an origin for upcoming developments and research. Implementing these numerous approaches on actual environments or testbeds will lastly permit the developments in protection, resilience, monitoring, as well as mitigation of the smart grids alongside the future serious cyber-attacks threats.

REFERENCES

[1] H. Parastvand, O. Bass, M. A. S. Masoum, A. Chapman, and S. Lachowicz, "Cyber-security constrained placement of FACTS devices in power networks from a novel topological perspective," *IEEE Access*, vol. 8, pp. 108201–108215, 2020, doi: 10.1109/ACCESS.2020.3001308.

[2] J. Tavcar and I. Horvath, "A review of the principles of designing smart cyber-physical systems for run-time adaptation: Learned lessons and open issues," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 1, pp. 145–158, Jan. 2019.

[3] K.-K.-R. Choo, M. M. Kermani, R. Azarderakhsh, and M. Govindarasu, "Emerging embedded and cyber physical system security challenges and innovations," *IEEE Trans. Depend. Sec. Comput.*, vol. 14, no. 3, pp. 235–236, May 2017.

[4] R. Altawy and A. M. Youssef, "Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices," *IEEE Access*, vol. 4, pp. 959–979, 2016.

[5] A. Burg, A. Chattopadhyay, and K.-Y. Lam, "Wireless communication and security issues for cyber–physical systems and the Internet-of-Things," *Proc. IEEE*, vol. 106, no. 1, pp. 38–60, Jan. 2018.

[6] B. Wang, P. Dehghanian, and D. Zhao, "Chance-constrained energy management system for power grids with high proliferation of renewables and electric vehicles," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2324–2336, May 2020.

[7] P. Jokar, *Model-Based Intrusion Detection for Home Area Networks in Smart Grids*. Bristol, U.K.: Univ. Bristol, 2012, pp. 1–19.

[8] B. Zhang, P. Dehghanian, and M. Kezunovic, "Optimal allocation of PV generation and battery storage for enhanced resilience," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 535–545, Jan. 2019.

[9] M. Milton, C. D. L. O, H. L. Ginn, and A. Benigni, "Controller-embeddable probabilistic real-time digital twins for power electronic converter diagnostics," *IEEE Trans. Power Electron.*, vol. 35, no. 9, pp. 9850–9864, Sep. 2020, doi: 10.1109/TPEL.2020.2971775.

[10] S. Y. Kim, S. G. Song, and S. J. Park, "Minimum loss discontinuous pulse-width modulation per phase method for three-phase four-leg inverter," *IEEE Access*, vol. 8, pp. 122923–122936, 2020, doi: 10.1109/ACCESS.2020.3006245.

[11] S. Gu, X. Du, Y. Shi, P. Sun, and H.-M. Tai, "Power control for grid-connected converter to comply with safety operation limits during grid faults," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 8, no. 1, pp. 866–876, Mar. 2020, doi: 10.1109/JESTPE.2018.2888552.

[12] W.-H. Yang, S.-W. Chiu, C.-C. Kuo, Y.-T. Lin, Y.-J. Lai, H.-W. Chen, Y.-S. Ma, K.-H. Chen, Y.-H. Lin, S.-R. Lin, and T.-Y. Tsai, "A true-random-number-based pseudohysteresis controller for buck DC–DC converter in high-security Internet-of-everything devices," *IEEE Trans. Power Electron.*, vol. 35, no. 3, pp. 2969–2978, Mar. 2020, doi: 10.1109/TPEL.2019.2928420.

[13] S. Soltan, M. Yannakakis, and G. Zussman, "Power grid state estimation following a joint cyber and physical attack," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 499–512, Mar. 2018, doi: 10.1109/TCNS.2016.2620807.

[14] X. Feng and Q. Sun, "Stochastic games for power grid coordinated defence against coordinated attacks," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 5, no. 3, pp. 292–300, Sep. 2020, doi: 10.1049/iet-cps.2020.0002.

[15] M. Kouki, B. Marinescu, and F. Xavier, "Exhaustive modal analysis of large-scale interconnected power systems with high power electronics penetration," *IEEE Trans. Power Syst.*, vol. 35, no. 4, pp. 2759–2768, Jul. 2020, doi: 10.1109/TPWRS.2020.2969641.

[16] X. Hong, G. Zhang, and D. Lu, "Control strategies for crowd emotional contagion coupling the virtual and physical cyberspace in emergencies," *IEEE Access*, vol. 8, pp. 37712–37726, 2020, doi: 10.1109/ACCESS.2020.2975808.

[17] Z. Zhang, S. Huang, F. Liu, and S. Mei, "Pattern analysis of topological attacks in cyber-physical power systems considering cascading outages," *IEEE Access*, vol. 8, pp. 134257–134267, 2020, doi: 10.1109/ACCESS.2020.3006555.

[18] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020, doi: 10.1109/ACCESS.2020.3016826.

[19] O. Hariri, M. M. Esfahani, and O. Mohammed, "Collective distribution of mobile loads for optimal and secure operation of power systems," in *Proc. IEEE Ind. Appl. Soc. Annu. Meeting*, Baltimore, MD, USA, Oct. 2019, pp. 1–8, doi: 10.1109/IAS.2019.8912331.

[20] D. Perez-Estevez, J. Doval-Gandoy, and J. M. Guerrero, "AC-voltage harmonic control for stand-alone and Weak-Grid-Tied converter," *IEEE Trans. Ind. Appl.*, vol. 56, no. 1, pp. 403–421, Jan. 2020, doi: 10.1109/TIA.2019.2942265.

[21] S. Chen, Q. Jiang, Y. He, R. Huang, J. Li, C. Li, and J. Liao, "A BP neural network-based hierarchical investment risk evaluation method considering the uncertainty and coupling for the power grid," *IEEE Access*, vol. 8, pp. 110279–110289, 2020, doi: 10.1109/ACCESS.2020.3002381.

[22] P. Prabhakaran and V. Agarwal, "Novel boost-SEPIC type interleaved DC–DC converter for mitigation of voltage imbalance in a low-voltage bipolar DC microgrid," *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 6494–6504, Aug. 2020, doi: 10.1109/TIE.2019.2939991.

[23] Z. Lin, X. Ruan, L. Wu, H. Zhang, and W. Li, "Multi resonant component-based Grid-Voltage-Weighted feedforward scheme for grid-connected inverter to suppress the injected grid current harmonics under weak grid," *IEEE Trans. Power Electron.*, vol. 35, no. 9, pp. 9784–9793, Sep. 2020, doi: 10.1109/TPEL.2020.2970514.

[24] M. Wen, Y. Li, X. Xie, Y. Cao, Y. Wu, W. Wang, L. He, Y. Cao, B. Xu, and L. Huang, "Key factors for efficient consumption of renewable energy in a provincial power grid in Southern China," *CSEE J. Power Energy Syst.*, vol. 6, no. 3, pp. 554–562, Sep. 2020, doi: 10.17775/CSEE-JPES.2019.01970.

[25] N. M. Dehkordi and S. Z. Moussavi, "Distributed resilient adaptive control of islanded microgrids under sensor/actuator faults," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2699–2708, May 2020, doi: 10.1109/TSG.2019.2960205.

[26] S. Selvarajan, M. Shaik, S. Ameerjohn, and S. Kannan, "Mining of intrusion attack in SCADA network using clustering and genetically seeded flora-based optimal classification algorithm," *IET Inf. Secur.*, vol. 14, no. 1, pp. 1–11, Jan. 2020, doi: 10.1049/iet-ifs.2019.0011.

[27] S. D. Roy and S. Debbarma, "Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2023–2031, Jun. 2020, doi: 10.1109/JSYST.2019.2943921.

[28] H. Long, Z. Wu, C. Fang, W. Gu, X. Wei, and H. Zhan, "Cyber-attack detection strategy based on distribution system state estimation," *J. Mod. Power Syst. Clean Energy*, vol. 8, no. 4, pp. 669–678, 2020, doi: 10.35833/MPCE.2019.000216.

[29] A. Rodriguez-Cabero, J. Roldan-Perez, M. Prodanovic, J. A. Suul, and S. D'Arco, "Coupling of AC grids via VSC-HVDC interconnections for oscillation damping based on differential and common power control," *IEEE Trans. Power Electron.*, vol. 35, no. 6, pp. 6548–6558, Jun. 2020, doi: 10.1109/TPEL.2019.2952656.

[30] K. Ma, J. Wang, X. Cai, and F. Blaabjerg, "AC grid emulations for advanced testing of grid-connected converters—An overview," *IEEE Trans. Power Electron.*, vol. 36, no. 2, pp. 1626–1645, Feb. 2021, doi: 10.1109/TPEL.2020.3011176.

[31] M. Graungaard Taul, X. Wang, P. Davari, and F. Blaabjerg, "Robust fault ride through of converter-based generation during severe faults with phase jumps," *IEEE Trans. Ind. Appl.*, vol. 56, no. 1, pp. 570–583, Feb. 2020, doi: 10.1109/TIA.2019.2944175.

[32] M. A. Awal, H. Yu, I. Husain, W. Yu, and S. M. Lukic, "Selective harmonic current rejection for virtual oscillator controlled grid-forming voltage source converters," *IEEE Trans. Power Electron.*, vol. 35, no. 8, pp. 8805–8818, Aug. 2020, doi: 10.1109/TPEL.2020.2965880.

[33] J. Chen, F. Milano, and T. O'Donnell, "Assessment of grid-feeding converter voltage stability," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 3980–3982, Sep. 2019, doi: 10.1109/TPWRS.2019.2920516.

[34] J. Fang, H. Deng, and S. M. Goetz, "Grid impedance estimation through grid-forming power converters," *IEEE Trans. Power Electron.*, vol. 36, no. 2, pp. 2094–2104, Feb. 2021, doi: 10.1109/TPEL.2020.3010874.

[35] M. Ahmed, L. Meegahapola, A. Vahidnia, and M. Datta, "Stability and control aspects of microgrid Architectures–A comprehensive review," *IEEE Access*, vol. 8, pp. 144730–144766, 2020, doi: 10.1109/ACCESS.2020.3014977.

[36] J. Johnson, R. Ablinger, R. Bruendlinger, B. Fox, and J. Flicker, "Interconnection standard grid-support function evaluations using an automated hardware-in-the-loop testbed," *IEEE J. Photovolt.*, vol. 8, no. 2, pp. 565–571, Mar. 2018, doi: 10.1109/JPHOTOV.2018.2794884.

[37] K. Ding, Y. Qian, Y. Wang, P. Hu, and B. Wang, "A data-driven vulnerability evaluation method in grid edge based on random matrix theory indicators," *IEEE Access*, vol. 8, pp. 26495–26504, 2020, doi: 10.1109/ACCESS.2020.2971030.

[38] H. Pan, H. Lian, C. Na, and X. Li, "Modeling and vulnerability analysis of cyber-physical power systems based on community theory," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3938–3948, Sep. 2020, doi: 10.1109/JSYST.2020.2969023.

[39] L. Che, X. Liu, Z. Shuai, Z. Li, and Y. Wen, "Cyber cascades screening considering the impacts of false data injection attacks," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6545–6556, Nov. 2018, doi: 10.1109/TPWRS.2018.2827060.

[40] 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, doi: 10.1109/TSG.2019.2949998.

[41] K. Huang, L.-X. Yang, X. Yang, Y. Xiang, and Y. Y. Tang, "A low-cost distributed Denial-of-Service attack architecture," *IEEE Access*, vol. 8, pp. 42111–42119, 2020, doi: 10.1109/ACCESS.2020.2977112.

[42] H. Boche, R. F. Schaefer, and H. V. Poor, "Denial-of-service attacks on communication systems: Detectability and jammer knowledge," *IEEE Trans. Signal Process.*, vol. 68, pp. 3754–3768, 2020, doi: 10.1109/TSP.2020.2993165.

[43] X.-M. Zhang, Q.-L. Han, X. Ge, and L. Ding, "Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3616–3626, Aug. 2020, doi: 10.1109/TCYB.2019.2956137.

[44] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 854–864, Feb. 2020, doi: 10.1109/TII.2019.2922215.

[45] M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine-learning-based technique for false data injection attacks detection in industrial IoT," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8462–8471, Sep. 2020, doi: 10.1109/JIOT.2020.2991693.

[46] S. M. P. Dinakarrao, X. Guo, H. Sayadi, C. Nowzari, A. Sasan, S. Rafatirad, L. Zhao, and H. Homayoun, "Cognitive and scalable technique for securing IoT networks against malware epidemics," *IEEE Access*, vol. 8, pp. 138508–138528, 2020, doi: 10.1109/ACCESS.2020.3011919.

[47] M. M. Rana, "IoT-based electric vehicle state estimation and control algorithms under cyber attacks," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 874–881, Feb. 2020, doi: 10.1109/JIOT.2019.2946093.

[48] R. M. Pratt and T. E. Carroll, "Vehicle charging infrastructure security," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, Jan. 2019, pp. 1–5, doi: 10.1109/ICCE.2019.8662043.

[49] J. Wang and D. Shi, "Cyber-attacks related to intelligent electronic devices and their countermeasures: A review," in *Proc. 53rd Int. Universities Power Eng. Conf. (UPEC)*, Glasgow, U.K., Sep. 2018, pp. 1–6, doi: 10.1109/UPEC.2018.8542059.

[50] J. Hong and C.-C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 271–281, Jan. 2019, doi: 10.1109/TSG.2017.2737826.

[51] M. Bahrami, M. Fotuhi-Firuzabad, and H. Farzin, "Reliability evaluation of power grids considering integrity attacks against substation protective IEDs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1035–1044, Feb. 2020, doi: 10.1109/TII.2019.2926557.

[52] T. S. Ustun, S. M. Farooq, and S. M. S. Hussain, "A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard," *IEEE Access*, vol. 7, pp. 156044–156053, 2019, doi: 10.1109/ACCESS.2019.2948117.

[53] Q. Bin, C. Ziwen, X. Yong, H. Liang, and S. Sheng, "GPS spoofing-based time synchronisation attack in advanced metering infrastructure and its protection," *J. Eng.*, vol. 2020, no. 9, pp. 809–815, Sep. 2020, doi: 10.1049/joe.2020.0022.

[54] H. Pearce, S. Pinisetty, P. S. Roop, M. M. Y. Kuo, and A. Ukil, "Smart I/O modules for mitigating cyber-physical attacks on industrial control systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4659–4669, Jul. 2020, doi: 10.1109/TII.2019.2945520.

[55] M. S. Hossan and B. Chowdhury, "Integrated CVR and demand response framework for advanced distribution management systems," *IEEE Trans. Sustain. Energy*, vol. 11, no. 1, pp. 534–544, Jan. 2020, doi: 10.1109/TSTE.2019.2897333.

[56] A. Imran, G. Hafeez, I. Khan, M. Usman, Z. Shafiq, A. B. Qazi, A. Khalid, and K.-D. Thoben, "Heuristic-based programable controller for efficient energy management under renewable energy sources and energy storage system in smart grid," *IEEE Access*, vol. 8, pp. 139587–139608, 2020, doi: 10.1109/ACCESS.2020.3012735.

[57] A. R. Sayed, C. Wang, J. Zhao, and T. Bi, "Distribution-level robust energy management of power systems considering bidirectional interactions with gas systems," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2092–2105, May 2020, doi: 10.1109/TSG.2019.2947219.

[58] A. Sangswang and M. Konghirun, "Optimal strategies in home energy management system integrating solar power, energy storage, and vehicle-to-grid for grid support and energy efficiency," *IEEE Trans. Ind. Appl.*, vol. 56, no. 5, pp. 5716–5728, Sep. 2020, doi: 10.1109/TIA.2020.2991652.

[59] N. M. Manousakis and G. N. Korres, "Optimal allocation of phasor measurement units considering various contingencies and measurement redundancy," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 6, pp. 3403–3411, Jun. 2020, doi: 10.1109/TIM.2019.2932208.

[60] M. Jamei, R. Ramakrishna, T. Tesfay, R. Gentz, C. Roberts, A. Scaglione, and S. Peisert, "Phasor measurement units optimal placement and performance limits for fault localization," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 1, pp. 180–192, Jan. 2020, doi: 10.1109/JSAC.2019.2951971.

[61] A. Mohammadi and K. N. Plataniotis, "Noncircular attacks on phasor measurement units for state estimation in smart grid," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 4, pp. 777–789, Aug. 2018, doi: 10.1109/JSTSP.2018.2840517.

[62] R. Pal and V. Prasanna, "The STREAM mechanism for CPS security the case of the smart grid," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 36, no. 4, pp. 537–550, Apr. 2017, doi: 10.1109/TCAD.2016.2565201.

[63] A. Chattopadhyay and U. Mitra, "Security against false data-injection attack in cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 2, pp. 1015–1027, Jun. 2020, doi: 10.1109/TCNS.2019.2927594.

[64] S. Liu, Y. Liu, S. Li, and B. Xu, "H_∞ control for time-varying cyber-physical system under randomly occurring hybrid attacks: The output feedback case," *IEEE Access*, vol. 8, pp. 60780–60789, 2020, doi: 10.1109/ACCESS.2020.2980978.

[65] J. Wurm, Y. Jin, Y. Liu, S. Hu, K. Heffner, F. Rahman, and M. Tehranipoor, "Introduction to cyber-physical system security: A cross-layer perspective," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 3, no. 3, pp. 215–227, Jul. 2017.

[66] J. C. Balda, A. Mantooth, R. Blum, and P. Tenti, "Cybersecurity and power electronics: Addressing the security vulnerabilities of the Internet of Things," *IEEE Power Electron. Mag.*, vol. 4, no. 4, pp. 37–43, Dec. 2017.

[67] X. Zhu, Z. Yu, and X. Liu, "Security constrained unit commitment with extreme wind scenarios," *J. Modern Power Syst. Clean Energy*, vol. 8, no. 3, pp. 464–472, 2020, doi: 10.35833/MPCE.2018.000797.

[68] W. Mesbah, "Securing smart electricity meters against customer attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 101–110, Jan. 2018, doi: 10.1109/TSG.2016.2545524.

[69] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying FDI attacks in power system state estimation," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 4, pp. 763–776, Aug. 2018, doi: 10.1109/JSTSP.2018.2846542.

[70] C. Liu, H. Liang, T. Chen, J. Wu, and C. Long, "Joint admittance perturbation and meter protection for mitigating stealthy FDI attacks against power system state estimation," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1468–1478, Mar. 2020, doi: 10.1109/TPWRS.2019.2938223.

[71] P. Key and R. Steinberg, "Pricing, competition and content for Internet service providers," *IEEE/ACM Trans. Netw.*, vol. 28, no. 5, pp. 2285–2298, Oct. 2020, doi: 10.1109/TNET.2020.3010550.

[72] 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.)*, Milan, Italy, Jun. 2017, pp. 1–6, doi: 10.1109/EEEIC.2017.7977729.

[73] M. El Hariri, E. Harmon, H. F. Habib, T. Youssef, and O. A. Mohammed, "A targeted attack for enhancing resiliency of intelligent intrusion detection modules in energy cyber physical systems," in *Proc. 19th Int. Conf. Intell. Syst. Appl. Power Syst. (ISAP)*, San Antonio, TX, USA, Sep. 2017, pp. 1–6, doi: 10.1109/ISAP.2017.8071363.

[74] A. O. Hariri, M. El Hariri, T. Youssef, and O. A. Mohammed, "A bilateral decision support platform for public charging of connected electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 129–140, Jan. 2019, doi: 10.1109/TVT.2018.2879927.

[75] S. Faddel, A. T. Elsayed, and O. A. Mohammed, "Bilayer multi-objective optimal allocation and sizing of electric vehicle parking garage," *IEEE Trans. Ind. Appl.*, vol. 54, no. 3, pp. 1992–2001, May 2018, doi: 10.1109/TIA.2018.2803151.

[76] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: Secure protocols, incidents, threats and tactics," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1942–1976, 3rd Quart., 2020, doi: 10.1109/COMST.2020.2987688.

[77] S. Ghosh and S. Sampalli, "A survey of security in SCADA networks: Current issues and future challenges," *IEEE Access*, vol. 7, pp. 135812–135831, 2019, doi: 10.1109/ACCESS.2019.2926441.

[78] C. Ruben, S. Dhulipala, K. Nagaraj, S. Zou, A. Starke, A. Bretas, A. Zare, and J. McNair, "Hybrid data-driven physics model-based framework for enhanced cyber-physical smart grid security," *IET Smart Grid*, vol. 3, no. 4, pp. 445–453, Aug. 2020, doi: 10.1049/iet-stg.2019.0272.

[79] A. Sundararajan, A. S. Hernandez, and A. I. Sarwat, "Adapting big data standards, maturity models to smart grid distributed generation: Critical review," *IET Smart Grid*, vol. 3, no. 4, pp. 508–519, Aug. 2020, doi: 10.1049/iet-stg.2019.0298.

[80] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 446–464, 1st Quart., 2017.

[81] J. Khazaei, "Stealthy cyberattacks on loads and distributed generation aimed at multi-transmission line congestions in smart grids," *IEEE Trans. Smart Grid*, early access, Nov. 16, 2020, doi: 10.1109/TSG.2020.3038045.

[82] A. J. Wilson, D. R. Reising, R. W. Hay, R. C. Johnson, A. A. Karrar, and T. D. Loveless, "Automated identification of electrical disturbance waveforms within an operational smart power grid," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4380–4389, Sep. 2020, doi: 10.1109/TSG.2020.2990079.

[83] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389–1407, Jul. 2017, doi: 10.1109/JPROC.2017.2686394.

[84] V. Venkataramanan, A. Hahn, and A. Srivastava, "CP-SAM: Cyber-physical security assessment metric for monitoring microgrid resiliency," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1055–1065, Mar. 2020, doi: 10.1109/TSG.2019.2930241.

[85] M. H. Variani and K. Tomsovic, "Distributed automatic generation control using flatness-based approach for high penetration of wind generation," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3002–3009, Aug. 2013, doi: 10.1109/TPWRS.2013.2257882.

[86] S. M. S. Hussain, M. A. Aftab, F. Nadeem, I. Ali, and T. S. Ustun, "Optimal energy routing in microgrids with IEC 61850 based energy routers," *IEEE Trans. Ind. Electron.*, vol. 67, no. 6, pp. 5161–5169, Jun. 2020, doi: 10.1109/TIE.2019.2927154.

[87] M. D. Smith and M. E. Paté-Cornell, "Cyber risk analysis for a smart grid: How smart is smart enough? A multiarmed bandit approach to cyber security investment," *IEEE Trans. Eng. Manage.*, vol. 65, no. 3, pp. 434–447, Aug. 2018.

[88] 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.

[89] X. Lyu, Y. Ding, and S.-H. Yang, "Bayesian network based C2P risk assessment for cyber-physical systems," *IEEE Access*, vol. 8, pp. 88506–88517, 2020, doi: 10.1109/ACCESS.2020.2993614.

[90] Y. Zhang, V. V. G. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn, and S. Suresh, "Cyber physical security analytics for transactive energy systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 931–941, Mar. 2020, doi: 10.1109/TSG.2019.2928168.

[91] K. Huang, C. Zhou, Y. Qin, and W. Tu, "A game-theoretic approach to cross-layer security decision-making in industrial cyber-physical systems," *IEEE Trans. Ind. Electron.*, vol. 67, no. 3, pp. 2371–2379, Mar. 2020, doi: 10.1109/TIE.2019.2907451.

[92] Y. Jiang, S. Yin, and O. Kaynak, "Data-driven monitoring and safety control of industrial cyber-physical systems: Basics and beyond," *IEEE Access*, vol. 6, pp. 47374–47384, 2018.

[93] A. Farraj, E. Hammad, and D. Kundur, "A cyber-physical control framework for transient stability in smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1205–1215, Mar. 2018.

[94] T. A. Simões, C. L. Borges, and J. Mitra, "Use of performance indices for contingency screening for rapid assessment of dynamic security region," *IET Gener., Transmiss. Distrib.*, vol. 14, no. 18, pp. 3896–3904, Sep. 2020, doi: 10.1049/iet-gtd.2020.0223.

[95] P. Akaber, B. Moussa, M. Ghafouri, R. Atallah, B. L. Agba, C. Assi, and M. Debbabi, "CASeS: Concurrent contingency analysis-based security metric deployment for the smart grid," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2676–2687, May 2020, doi: 10.1109/TSG.2019.2959937.

[96] G. Cao, W. Gu, P. Li, W. Sheng, K. Liu, L. Sun, Z. Cao, and J. Pan, "Operational risk evaluation of active distribution networks considering cyber contingencies," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 3849–3861, Jun. 2020, doi: 10.1109/TII.2019.2939346.

[97] M. Li, Y. Xue, M. Ni, and X. Li, "Modeling and hybrid calculation architecture for cyber physical power systems," *IEEE Access*, vol. 8, pp. 138251–138263, 2020, doi: 10.1109/ACCESS.2020.3011213.

[98] H. Tu, Y. Xia, C. K. Tse, and X. Chen, "A hybrid cyber attack model for cyber-physical power systems," *IEEE Access*, vol. 8, pp. 114876–114883, 2020, doi: 10.1109/ACCESS.2020.3003323.

[99] F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab, "Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2716–2725, Apr. 2020, doi: 10.1109/TII.2019.2956474.

[100] Y. Zhang and O. Yagan, "Robustness of interdependent cyber-physical systems against cascading failures," *IEEE Trans. Autom. Control*, vol. 65, no. 2, pp. 711–726, Feb. 2020, doi: 10.1109/TAC.2019.2918120.

[101] C. Roberts, A. Scaglione, M. Jamei, R. Gentz, S. Peisert, E. M. Stewart, C. McParland, A. McEachern, and D. Arnold, "Learning behavior of distribution system discrete control devices for cyber-physical security," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 749–761, Jan. 2020, doi: 10.1109/TSG.2019.2936016.

[102] J. Feng, L. T. Yang, R. Zhang, S. Zhang, G. Dai, and W. Qiang, "A tensor-based optimization model for secure sustainable cyber-physical-social big data computations," *IEEE Trans. Sustain. Comput.*, vol. 5, no. 2, pp. 223–234, Apr. 2020, doi: 10.1109/TSUSC.2018.2881466.

[103] J. Li, Y. Liu, T. Chen, Z. Xiao, Z. Li, and J. Wang, "Adversarial attacks and defenses on Cyber–Physical systems: A survey," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5103–5115, Jun. 2020, doi: 10.1109/JIOT.2020.2975654.

[104] T. Becejac, C. Eppinger, A. Ashok, U. Agrawal, and J. O'Brien, "PRIME: A real-time cyber-physical systems testbed: From wide-area monitoring, protection, and control prototyping to operator training and beyond," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 5, no. 2, pp. 186–195, Jun. 2020, doi: 10.1049/iet-cps.2019.0049.

[105] C. Yang, Z. Shi, H. Zhang, J. Wu, and X. Shi, "Multiple attacks detection in cyber-physical systems using random finite set theory," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 4066–4075, Sep. 2020, doi: 10.1109/TCYB.2019.2912939.

[106] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Vulnerability assessments of electric drive systems due to sensor data integrity attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3301–3310, May 2020, doi: 10.1109/TII.2019.2948056.

[107] C. Bakker, A. Bhattacharya, S. Chatterjee, and D. L. Vrabie, "Learning and information manipulation: Repeated hypergames for cyber-physical security," *IEEE Control Syst. Lett.*, vol. 4, no. 2, pp. 295–300, Apr. 2020, doi: 10.1109/LCSYS.2019.2925681.

[108] S. Kwon, H. Yoo, and T. Shon, "IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system," *IEEE Access*, vol. 8, pp. 77572–77586, 2020, doi: 10.1109/ACCESS.2020.2989770.

[109] L. Cao, X. Jiang, Y. Zhao, S. Wang, D. You, and X. Xu, "A survey of network attacks on cyber-physical systems," *IEEE Access*, vol. 8, pp. 44219–44227, 2020, doi: 10.1109/ACCESS.2020.2977423.

[110] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong, "A survey on decentralized consensus mechanisms for cyber physical systems," *IEEE Access*, vol. 8, pp. 54371–54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

[111] 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, doi: 10.1049/iet-cps.2019.0032.

[112] M. V. Chester and B. R. Allenby, "Perspective: The cyber frontier and infrastructure," *IEEE Access*, vol. 8, pp. 28301–28310, 2020, doi: 10.1109/ACCESS.2020.2971960.

[113] D. Lin, Q. Liu, Z. Li, G. Zeng, Z. Wang, T. Yu, and J. Zhang, "Elaborate reliability evaluation of cyber physical distribution systems considering fault location, isolation and supply restoration process," *IEEE Access*, vol. 8, pp. 128574–128590, 2020, doi: 10.1109/ACCESS.2020.3007477.

[114] Y. Qin, T. Xie, C. Xu, A. Astorga, and J. Lu, "CoMID: Context-based multiinvariant detection for monitoring cyber-physical software," *IEEE Trans. Rel.*, vol. 69, no. 1, pp. 106–123, Mar. 2020, doi: 10.1109/TR.2019.2933324.

[115] H. Li, J. Peng, J. He, Z. Huang, J. Wang, L. He, and J. Pan, "Pinning-based switching control of cyber-physical supercapacitor energy storage systems," *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 4, pp. 1520–1533, Jul. 2020, doi: 10.1109/TCST.2019.2916039.

[116] Y. Pang, H. Xia, and M. J. Grimble, "Resilient nonlinear control for attacked cyber-physical systems," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 6, pp. 2129–2138, Jun. 2020, doi: 10.1109/TSMC.2018.2801868.

[117] Y. Ni, Z. Guo, Y. Mo, and L. Shi, "On the performance analysis of reset attack in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 65, no. 1, pp. 419–425, Jan. 2020, doi: 10.1109/TAC.2019.2914655.

[118] A. Munir and F. Koushanfar, "Design and analysis of secure and dependable automotive CPS: A Steer-by-Wire case study," *IEEE Trans. Depend. Sec. Comput.*, vol. 17, no. 4, pp. 813–827, Jul. 2020, doi: 10.1109/TDSC.2018.2846741.

[119] L. Chen, D. Yue, C. Dou, J. Chen, and Z. Cheng, "Study on attack paths of cyber attack in cyber-physical power systems," *IET Gener., Transmiss. Distrib.*, vol. 14, no. 12, pp. 2352–2360, Jun. 2020, doi: 10.1049/iet-gtd.2019.1330.

[120] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access*, vol. 5, pp. 26022–26033, 2017, doi: 10.1109/ACCESS.2017.2769099.

[121] P. A. Oyewole and D. Jayaweera, "Power system security with cyber-physical power system operation," *IEEE Access*, vol. 8, pp. 179970–179982, 2020, doi: 10.1109/ACCESS.2020.3028222.

[122] A. Kanellopoulos and K. G. Vamvoudakis, "A moving target defense control framework for cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 65, no. 3, pp. 1029–1043, Mar. 2020, doi: 10.1109/TAC.2019.2915746.

[123] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K.-K.-R. Choo, "A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5110–5118, Aug. 2020, doi: 10.1109/TII.2019.2957140.

[124] Z. Cao, Y. Niu, and J. Song, "Finite-time sliding-mode control of Markovian jump cyber-physical systems against randomly occurring injection attacks," *IEEE Trans. Autom. Control*, vol. 65, no. 3, pp. 1264–1271, Mar. 2020, doi: 10.1109/TAC.2019.2926156.

[125] T.-Y. Zhang and D. Ye, "Distributed secure control against denial-of-service attacks in cyber-physical systems based on K-connected communication topology," *IEEE Trans. Cybern.*, vol. 50, no. 7, pp. 3094–3103, Jul. 2020, doi: 10.1109/TCYB.2020.2973303.

[126] X. Fu, G. Chen, and D. Yang, "Local false data injection attack theory considering isolation physical-protection in power systems," *IEEE Access*, vol. 8, pp. 103285–103290, 2020, doi: 10.1109/ACCESS.2020.2999585.

[127] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei, "Survey on unmanned aerial vehicle networks: A cyber physical system perspective," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1027–1070, 2nd Quart., 2020, doi: 10.1109/COMST.2019.2962207.

[128] Z. Ghaffar, S. Ahmed, K. Mahmood, S. H. Islam, M. M. Hassan, and G. Fortino, "An improved authentication scheme for remote data access and sharing over cloud storage in cyber-physical-social-systems," *IEEE Access*, vol. 8, pp. 47144–47160, 2020, doi: 10.1109/ACCESS.2020.2977264.

[129] F. Shang, B. Wang, T. Li, J. Tian, and K. Cao, "CPFuzz: Combining fuzzing and falsification of cyber-physical systems," *IEEE Access*, vol. 8, pp. 166951–166962, 2020, doi: 10.1109/ACCESS.2020.3023250.

[130] H. Karimipour and H. Leung, "Relaxation-based anomaly detection in cyber-physical systems using ensemble Kalman filter," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 5, no. 1, pp. 49–58, Mar. 2020, doi: 10.1049/iet-cps.2019.0031.

[131] J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, "Moving target defense approach to detecting stuxnet-like attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 291–300, Jan. 2020, doi: 10.1109/TSG.2019.2921245.

[132] 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, doi: 10.1109/TPWRS.2019.2924441.

[133] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "MARINE: Man-in-the-middle attack resistant trust model in connected vehicles," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3310–3322, Apr. 2020, doi: 10.1109/JIOT.2020.2967568.

[134] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An ensemble deep learning-based cyber-attack detection in industrial control system," *IEEE Access*, vol. 8, pp. 83965–83973, 2020, doi: 10.1109/ACCESS.2020.2992249.

[135] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 746–789, 1st Quart., 2020, doi: 10.1109/COMST.2019.2944748.

[136] H. Cui, F. Li, and K. Tomsovic, "Cyber-physical system testbed for power system monitoring and wide-area control verification," *IET Energy Syst. Integr.*, vol. 2, no. 1, pp. 32–39, Mar. 2020, doi: 10.1049/iet-esi.2019.0084.

[137] Y. Zhu and W. X. Zheng, "Observer-based control for cyber-physical systems with periodic DoS attacks via a cyclic switching strategy," *IEEE Trans. Autom. Control*, vol. 65, no. 8, pp. 3714–3721, Aug. 2020, doi: 10.1109/TAC.2019.2953210.

[138] Y. Wu, H. Xu, and M. Ni, "Defensive resource allocation method for improving survivability of communication and information system in CPPS against cyber-attacks," *J. Mod. Power Syst. Clean Energy*, vol. 8, no. 4, pp. 750–759, 2020, doi: 10.35833/MPCE.2019.000148.

[139] Q. Zhang, K. Liu, Y. Xia, and A. Ma, "Optimal stealthy deception attack against cyber-physical systems," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 3963–3972, Sep. 2020, doi: 10.1109/TCYB.2019.2912622.

[140] S. Zhao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Secure beamforming for full-duplex MIMO two-way untrusted relay systems," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3775–3790, 2020, doi: 10.1109/TIFS.2020.3001733.

[141] X. Luo, Y. Li, X. Wang, and X. Guan, "Interval observer-based detection and localization against false data injection attack in smart grids," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 657–671, Jan. 2021, doi: 10.1109/JIOT.2020.3005926.

[142] L. Zhao, M. Ni, H. Tong, and Y. Li, "Design and application of distributed co-simulation platform for cyber physical power system based on the concepts of software bus and middleware," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 5, no. 1, pp. 71–79, Mar. 2020, doi: 10.1049/iet-cps.2018.5084.

[143] A. K. Sikder, H. Aksu, and A. S. Uluagac, "A context-aware framework for detecting sensor-based threats on smart devices," *IEEE Trans. Mobile Comput.*, vol. 19, no. 2, pp. 245–261, Feb. 2020, doi: 10.1109/TMC.2019.2893253.

[144] Z. Zhao, Y. Li, Y. Yang, L. Li, Y. Xu, and J. Zhou, "Sparse undetectable sensor attacks against cyber-physical systems: A subspace approach," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 11, pp. 2517–2521, Nov. 2020, doi: 10.1109/TCSII.2019.2953238.

[145] Y. Wu, B. Chen, J. Weng, Z. Wei, X. Li, B. Qiu, and N. Liu, "False load attack to smart meters by synchronously switching power circuits," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2641–2649, May 2019, doi: 10.1109/TSG.2018.2806896.

[146] X. Xia, Y. Xiao, and W. Liang, "ABSI: An adaptive binary splitting algorithm for malicious meter inspection in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 445–458, Feb. 2019, doi: 10.1109/TIFS.2018.2854703.

[147] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in smart grids based on graph signal processing," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1886–1896, Jun. 2020, doi: 10.1109/JSYST.2019.2927469.

[148] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing SDN infrastructure of IoT–fog networks from MitM attacks," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1156–1164, Oct. 2017, doi: 10.1109/JIOT.2017.2685596.

[149] S. Ohira, A. K. Desta, I. Arai, H. Inoue, and K. Fujikawa, "Normal and malicious sliding windows similarity analysis method for fast and accurate IDS against DoS attacks on in-vehicle networks," *IEEE Access*, vol. 8, pp. 42422–42435, 2020, doi: 10.1109/ACCESS.2020.2975893.

[150] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, "Electric power grid resilience to cyber adversaries: State of the art," *IEEE Access*, vol. 8, pp. 87592–87608, 2020, doi: 10.1109/ACCESS.2020.2993233.

[151] L. An and G. Yang, "Opacity enforcement for confidential robust control in linear cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 65, no. 3, pp. 1234–1241, Mar. 2020, doi: 10.1109/TAC.2019.2925498.

[152] A. Sturaro, S. Silvestri, M. Conti, and S. K. Das, "A realistic model for failure propagation in interdependent cyber-physical systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 2, pp. 817–831, Apr. 2020, doi: 10.1109/TNSE.2018.2872034.

[153] M. R. Camana Acosta, S. Ahmed, C. E. Garcia, and I. Koo, "Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks," *IEEE Access*, vol. 8, pp. 19921–19933, 2020, doi: 10.1109/ACCESS.2020.2968934.

[154] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138406–138446, 2020, doi: 10.1109/ACCESS.2020.3012006.

[155] A. J. M. Milne, A. Beckmann, and P. Kumar, "Cyber-physical trust systems driven by blockchain," *IEEE Access*, vol. 8, pp. 66423–66437, 2020, doi: 10.1109/ACCESS.2020.2984675.

[156] R. Lu, H. Shen, Z. Feng, H. Li, W. Zhao, and X. Li, "HTDet: A clustering method using information entropy for hardware trojan detection," *Tsinghua Sci. Technol.*, vol. 26, no. 1, pp. 48–61, Feb. 2021, doi: 10.26599/TST.2019.9010047.

[157] J. Chen, M. Liu, T. O'Donnell, and F. Milano, "Impact of current transients on the synchronization stability assessment of grid-feeding converters," *IEEE Trans. Power Syst.*, vol. 35, no. 5, pp. 4131–4134, Sep. 2020, doi: 10.1109/TPWRS.2020.3009858.

[158] J. Fang, J. Yu, Y. Zhang, and S. M. Goetz, "An estimation-based solution to weak-grid-induced small-signal stability problems of power converters," *IEEE J. Emerg. Sel. Topics Power Electron.*, early access, Oct. 13, 2020, doi: 10.1109/JESTPE.2020.3030720.

[159] J. Milosevic, H. Sandberg, and K. H. Johansson, "Estimating the impact of cyber-attack strategies for stochastic networked control systems," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 2, pp. 747–757, Jun. 2020, doi: 10.1109/TCNS.2019.2940253.

[160] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5643–5654, Sep. 2020, doi: 10.1109/TII.2019.2956734.

[161] D. Ye and T.-Y. Zhang, "Summation detector for false data-injection attack in cyber-physical systems," *IEEE Trans. Cybern.*, vol. 50, no. 6, pp. 2338–2345, Jun. 2020, doi: 10.1109/TCYB.2019.2915124.

[162] D. Sun, Q. Zhang, D. Wei, and M. Zhang, "A secure constellation design for polarized modulation in wireless communications," *IEEE Access*, vol. 8, pp. 130588–130597, 2020, doi: 10.1109/ACCESS.2020.3006833.

[163] S. Gao, Z. Peng, B. Xiao, A. Hu, Y. Song, and K. Ren, "Detection and mitigation of DoS attacks in software defined networks," *IEEE/ACM Trans. Netw.*, vol. 28, no. 3, pp. 1419–1433, Jun. 2020, doi: 10.1109/TNET.2020.2983976.

[164] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges," *IEEE Access*, vol. 8, pp. 24746–24772, 2020, doi: 10.1109/ACCESS.2020.2970576.

[165] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and privacy in smart farming: Challenges and opportunities," *IEEE Access*, vol. 8, pp. 34564–34584, 2020, doi: 10.1109/ACCESS.2020.2975142.

[166] H. W. Lim, G. S. Poh, J. Xu, and V. Chittawar, "PrivateLink: Privacy-preserving integration and sharing of datasets," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 564–577, 2020, doi: 10.1109/TIFS.2019.2924201.

[167] S. Wang, H. Wang, J. Li, H. Wang, J. Chaudhry, M. Alazab, and H. Song, "A fast CP-ABE system for cyber-physical security and privacy in mobile healthcare network," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4467–4477, Aug. 2020, doi: 10.1109/TIA.2020.2969868.

[168] X. Yang, J. Lin, W. Yu, P.-M. Moulema, X. Fu, and W. Zhao, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 4–18, Jan. 2015.

[169] F. Andren, R. Brundlinger, and T. Strasser, "IEC 61850/61499 control of distributed energy resources: Concept, guidelines, and implementation," *IEEE Trans. Energy Convers.*, vol. 29, no. 4, pp. 1008–1017, Dec. 2014, doi: 10.1109/TEC.2014.2352338.

[170] M. Weiss, Y.-S. Li-Baboud, D. Anand, P. Boynton, K. G. Brady, and M. Burns, "A calibration of timing accuracy in NIST cyber-physical systems testbed," in *Proc. IEEE Int. Symp. Precis. Clock Synchronization Meas., Control, Commun. (ISPCS)*, Geneva, Switzerland, Sep. 2018, pp. 1–6, doi: 10.1109/ISPCS.2018.8543081.

[171] I. Dutt, S. Borah, and I. K. Maitra, "Immune system based intrusion detection system (IS-IDS): A proposed model," *IEEE Access*, vol. 8, pp. 34929–34941, 2020, doi: 10.1109/ACCESS.2020.2973608.

[172] G. Pu, L. Wang, J. Shen, and F. Dong, "A hybrid unsupervised clustering-based anomaly detection method," *Tsinghua Sci. Technol.*, vol. 26, no. 2, pp. 146–153, Apr. 2021, doi: 10.26599/TST.2019.9010051.

[173] H. Hindy, D. Brosset, E. Bayne, A. K. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," *IEEE Access*, vol. 8, pp. 104650–104675, 2020, doi: 10.1109/ACCESS.2020.3000179.

[174] 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*, Pittsburgh, PA, USA, 2008, pp. 1–5, doi: 10.1109/PES.2008.4596535.

[175] Y. Peng, Y. Song, W. Huang, H. Deng, Y. Wang, Q. Chen, M. Liao, and J. Hua, "Self-layer and cross-layer bilinear aggregation for fine-grained recognition in cyber-physical-social systems," *IEEE Access*, vol. 8, pp. 55826–55833, 2020, doi: 10.1109/ACCESS.2020.2981950.

[176] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6882–6897, Aug. 2020, doi: 10.1109/JIOT.2020.2970501.

[177] T. Dimitriou and G. O. Karame, "Enabling anonymous authorization and rewarding in the smart grid," *IEEE Trans. Depend. Sec. Comput.*, vol. 14, no. 5, pp. 565–572, Sep. 2017, doi: 10.1109/TDSC.2015.2496211.

[178] P. S. P. Pessim and M. J. Lacerda, "State-feedback control for cyber-physical LPV systems under DoS attacks," *IEEE Control Syst. Lett.*, vol. 5, no. 3, pp. 1043–1048, Jul. 2021, doi: 10.1109/LCSYS.2020.3009176.

[179] B. Moussa, M. Kassouf, R. Hadjidj, M. Debbabi, and C. Assi, "An extension to the precision time protocol (PTP) to enable the detection of cyber attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 18–27, Jan. 2020, doi: 10.1109/TII.2019.2943913.

[180] A. S. Sani, D. Yuan, W. Bao, and Z. Y. Dong, "A universally composable key exchange protocol for advanced metering infrastructure in the energy Internet," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 534–546, Jan. 2021, doi: 10.1109/TII.2020.2971707.

[181] K. G. Lore, D. M. Shila, and L. Ren, "Detecting data integrity attacks on correlated solar farms using multi-layer data driven algorithm," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Beijing, China, May 2018, pp. 1–9, doi: 10.1109/CNS.2018.8433159.

[182] M. N. I. Sarkar, L. G. Meegahapola, and M. Datta, "Reactive power management in renewable rich power grids: A review of grid-codes, renewable generators, support devices, control strategies and optimization algorithms," *IEEE Access*, vol. 6, pp. 41458–41489, 2018, doi: 10.1109/ACCESS.2018.2838563.

[183] M. Aibin, "The weather impact on heating and air conditioning with smart thermostats," *Can. J. Electr. Comput. Eng.*, vol. 43, no. 3, pp. 190–194, 2020, doi: 10.1109/CJECE.2020.2978459.

[184] A. Rasool, X. Yan, U. Rasool, F. Abbas, M. Numan, H. Rasool, and M. Jamil, "Enhanced control strategies of VSG for EV charging station under a low inertia microgrid," *IET Power Electron.*, vol. 13, no. 13, pp. 2895–2904, Oct. 2020, doi: 10.1049/iet-pel.2019.1592.

[185] X. Wu, Y. Xu, J. He, X. Wang, J. C. Vasquez, and J. M. Guerrero, "Pinning-based hierarchical and distributed cooperative control for AC microgrid clusters," *IEEE Trans. Power Electron.*, vol. 35, no. 9, pp. 9865–9885, Sep. 2020, doi: 10.1109/TPEL.2020.2972321.

[186] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A survey of moving target defenses for network security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1909–1941, 3rd Quart., 2020, doi: 10.1109/COMST.2020.2982955.

[187] H. Hu, Y. Liu, C. Chen, H. Zhang, and Y. Liu, "Optimal decision making approach for cyber security defense using evolutionary game," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 3, pp. 1683–1700, Sep. 2020, doi: 10.1109/TNSM.2020.2995713.

[188] M. S. Rahman, M. A. Mahmud, A. M. T. Oo, and H. R. Pota, "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 436–447, Apr. 2017, doi: 10.1109/TII.2016.2612645.

[189] R. Moslemi, A. Mesbahi, and J. M. Velni, "A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4930–4941, Sep. 2018, doi: 10.1109/TSG.2017.2675960.

[190] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2019, doi: 10.1109/TSG.2018.2878570.

[191] H. Karimipour, A. Dehghantanha, R. M. Parizi, K.-K.-R. Choo, and H. Leung, "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids," *IEEE Access*, vol. 7, pp. 80778–80788, 2019, doi: 10.1109/ACCESS.2019.2920326.

[192] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1686–1721, 3rd Quart., 2020, doi: 10.1109/COMST.2020.2986444.

[193] G. Ravikumar and M. Govindarasu, "Anomaly detection and mitigation for wide-area damping control using machine learning," *IEEE Trans. Smart Grid*, early access, May 18, 2020, doi: 10.1109/TSG.2020.2995313.

[194] H. Wang, J. Ruan, G. Wang, B. Zhou, Y. Liu, X. Fu, and J. Peng, "Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4766–4778, Nov. 2018, doi: 10.1109/TII.2018.2804669.

[195] M. Dehghani, A. Kavousi-Fard, M. Dabbaghjamanesh, and O. Avatefipour, "Deep learning based method for false data injection attack detection in AC smart islands," *IET Gener., Transmiss. Distrib.*, vol. 14, no. 24, pp. 5756–5765, Dec. 2020, doi: 10.1049/iet-gtd.2020.0391.

[196] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2765–2777, Oct. 2019, doi: 10.1109/TIFS.2019.2902822.

[197] Z. Wang, Y. Chen, F. Liu, Y. Xia, and X. Zhang, "Power system security under false data injection attacks with exploitation and exploration based on reinforcement learning," *IEEE Access*, vol. 6, pp. 48785–48796, 2018, doi: 10.1109/ACCESS.2018.2856520.

[198] F. Wei, Z. Wan, and H. He, "Cyber-attack recovery strategy for smart grid based on deep reinforcement learning," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2476–2486, May 2020, doi: 10.1109/TSG.2019.2956161.

[199] Z. Wang, H. He, Z. Wan, and Y. Sun, "Coordinated topology attacks in smart grid using deep reinforcement learning," *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 1407–1415, Feb. 2021, doi: 10.1109/TII.2020.2994977.

[200] M. I. Oozeer and S. Haykin, "Cognitive dynamic system for control and cyber-attack detection in smart grid," *IEEE Access*, vol. 7, pp. 78320–78335, 2019, doi: 10.1109/ACCESS.2019.2922410.

[201] M. I. Oozeer and S. Haykin, "Cognitive risk control for mitigating cyber-attack in smart grid," *IEEE Access*, vol. 7, pp. 125806–125826, 2019, doi: 10.1109/ACCESS.2019.2939089.

[202] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10250–10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.

[203] B. Jiang, J. Yang, G. Ding, and H. Wang, "Cyber-physical security design in multimedia data cache resource allocation for industrial networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6472–6480, Dec. 2019, doi: 10.1109/TII.2019.2917693.

[204] S. Rafi, W. Yu, M. A. Akbar, A. Alsanad, and A. Gumaei, "Prioritization based taxonomy of DevOps security challenges using PROMETHEE," *IEEE Access*, vol. 8, pp. 105426–105446, 2020, doi: 10.1109/ACCESS.2020.2998819.

[205] J. Hamilton, "Cyber security: Advice from the front line," *ITNOW*, vol. 62, no. 1, pp. 38–39, Mar. 2020, doi: 10.1093/itnow/bwaa017.

[206] S. Y. Enoch, Z. Huang, C. Y. Moon, D. Lee, M. K. Ahn, and D. S. Kim, "HARMer: Cyber-attacks automation and evaluation," *IEEE Access*, vol. 8, pp. 129397–129414, 2020, doi: 10.1109/ACCESS.2020.3009748.

[207] H. Chen, Q. Han, S. Jajodia, R. Lindelauf, V. S. Subrahmanian, and Y. Xiong, "Disclose or exploit? A game-theoretic approach to strategic decision making in cyber-warfare," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3779–3790, Sep. 2020, doi: 10.1109/JSYST.2020.2964985.

[208] C. Miranda, G. Kaddoum, E. Bou-Harb, S. Garg, and K. Kaur, "A collaborative security framework for software-defined wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2602–2615, 2020, doi: 10.1109/TIFS.2020.2973875.

[209] M. M. Rana and R. Bo, "IoT-based cyber-physical communication architecture: Challenges and research directions," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 5, no. 1, pp. 25–30, Mar. 2020, doi: 10.1049/iet-cps.2019.0028.

[210] M. I. Ali, S. Kaur, A. Khamparia, D. Gupta, S. Kumar, A. Khanna, and F. Al-Turjman, "Security challenges and cyber forensic ecosystem in IoT driven BYOD environment," *IEEE Access*, vol. 8, pp. 172770–172782, 2020, doi: 10.1109/ACCESS.2020.3024784.

[211] M. Zhan, J. Wu, H. Wen, and P. Zhang, "A novel error correction mechanism for energy-efficient cyber-physical systems in smart building," *IEEE Access*, vol. 6, pp. 39037–39045, 2018, doi: 10.1109/ACCESS.2018.2854794.

[212] D. Ye, T. Zhu, S. Shen, and W. Zhou, "A differentially private game theoretic approach for deceiving cyber adversaries," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 569–584, 2021, doi: 10.1109/TIFS.2020.3016842.

[213] W. Gao, W. Yu, F. Liang, W. G. Hatcher, and C. Lu, "Privacy-preserving auction for big data trading using homomorphic encryption," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 2, pp. 776–791, Apr. 2020, doi: 10.1109/TNSE.2018.2846736.

[214] L. Chen, D. Yue, C. Dou, J. Chen, and Z. Cheng, "Evaluation of cyber-physical power systems in cascading failure: Node vulnerability and systems connectivity," *IET Gener., Transmiss. Distrib.*, vol. 14, no. 7, pp. 1197–1206, Apr. 2020, doi: 10.1049/iet-gtd.2019.1286.

MAHMOUD AMIN (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Florida International University, Miami, FL, USA, in 2012. He is currently an Associate Professor with the ECE Department, Manhattan College, Riverdale, NY, USA, a Courtesy Research Associate Professor with Florida International University, and a Researcher with the Electronic Research Institute. He is the Director of the Sustainable Energy Systems Laboratory, Manhattan College. He has one edited book, one book chapter, and over 60 papers in professional journals and refereed international conference proceedings. His research interests include applications of power electronics in renewable energy systems, microgrids, adjustable speed drives, and smart grid. He was a recipient of the IEEE PES GM 2010 Paper Contest Award, the main award in Typhoon HIL's 10 for 10 Program, the 7 × 24 University Challenge Award, the Intel FPGA University Program Grant Award, and the Grand Challenge $2M Grant. He is an Editor of the *Machines* (MDPI) and a Guest Editor of IEEE TRANSACTIONS ON ENERGY CONVERSION and IEEE TRANSACTIONS ON MAGNETICS.

FAYEZ F. M. EL-SOUSY (Member, IEEE) received the B.Sc. degree in electrical engineering from Menoufia University, Al Minufya, Egypt, in 1988, and the M.Sc. and Ph.D. degrees in electrical engineering from Cairo University, Giza, Egypt, in 1994 and 2000, respectively.

Since 1990, he has been with the Department of Power Electronics and Energy Conversion, Electronics Research Institute, Giza, where he is currently a Full Professor. From August 1995 to June 2003, he was with the Department of Electrical Engineering, October Six University, Giza. From April 2004 to February 2007, he was a Postdoctoral Visiting Researcher with the Graduate School of Information Science and Electrical Engineering, Kyushu University, Fukuoka, Japan. From 2007 to 2010, he was with the Department of Electrical Engineering, College of Engineering, King Saud University, Riyadh, Saudi Arabia. From 2010 to 2014, he was with the Department of Electrical Engineering, College of Engineering, Salman bin Abdulaziz University, Al-Kharj, Saudi Arabia. Since 2014, he has been with the Department of Electrical Engineering, College of Engineering, Prince Sattam Bin Abdulaziz University, Saudi Arabia. His research interests include modeling and control of motor drives, motion-control systems, wind energy systems, digital signal processing-based computer control systems, computational intelligent of power electronics and electric drives, intelligent control theories including fuzzy logic, neural networks, and wavelets, nonlinear control and optimal control, robust control, and intelligent control of Maglev vehicle transportation systems.

GHADA A. ABDEL AZIZ (Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from Minofiya University, Egypt, in 2006 and 2009, respectively, and the Ph.D. degree in electrical engineering from Cairo University, Egypt, in 2015. From 2006 to 2008, she was TA with several academic institutions in Egypt. Since 2009, she has been a Research Assistant with the Electronics Research Institute, Egypt. Since 2015, she has been a Researcher with the Electronics Research Institute. She has over 35 published papers in professional journals and refereed international conference proceedings. Her current research interests include control of electrical machines, electrical machines drives, fault tolerant control, fault tolerant design of electric machine, power electronics in renewable energy systems, and smart grid security. She was awarded as the Best Researcher at the Electronics Research Institute due to her published articles at IEEE, in 2018 and 2019. She is an Associate Editor of the *Journal of Electrical Systems and Information Technology*.

KHALED GABER received the B.Sc. and M.Sc. degrees in electronics and communications engineering from the Arab Academy for Science, Technology and Maritime Transport (AASTMT), Egypt, in 2005 and 2011, respectively, and the Ph.D. degree in electronics and communications engineering from Al-Azhar University, Cairo, Egypt, in 2020. He is participating in several academic research activities at the National Research Center (NRC) and the Electronics Research Institute (ERI), Cairo. Since 2005, he started his career in different sectors of telecom industries. He is holding many certificates in project and program management, including PRINCE2 Agile®Foundation & Practitioner, Synergy®V.6 Foundation & Practitioner, ITIL V4®, and Certified Scrum Master®. He is a Project Director and International B2GaaS Program Manager in one of the leading multinational telecom firms. His current research interests include MEMS sensors, attitude determination in small satellites, cyber security, and control of electronic and communication systems.

OSAMA A. MOHAMMED (Life Fellow, IEEE) is currently a Distinguished Professor of electrical engineering and the Associate Dean of Research with the College of Engineering and Computing, Florida International University, Miami, FL, USA. He is also the Director of the Energy Systems Research Laboratory, FIU. He has more than 16 patents awarded or filed and has published more than 800 papers in refereed journals and other IEEE refereed international conference records. His research interests include computational electromagnetics, design optimization of EM devices, physics-based modeling in electric drives, and power electronic systems. His research also involves diagnostics through EM signatures, EMI, energy cyber-physical systems, and smart grid communications. He is recently involved in utilizing wideband gap devices and packaging designs for improved power densities and thermal management for transportation electrification and renewable energy and storage applications. He is an elected fellow of the Applied Computational Electromagnetic Society. He received the IEEE PES Cyril Veinott Electromechanical Energy Conversion Award, the 2012 Outstanding Research Award from Florida International University, and the 2017 Outstanding Doctoral Mentor. He was named as a Distinguished Professor at FIU, in 2018. He has served or currently serving as the International Steering Committee Chair for the IEEE IEMDC, the IEEE CEFC, ACES, and COMPUMAG. He also served as a General Chair for more than ten major international conferences. He was the President of the Applied Computational Electromagnetic Society (ACES).