Enhancing Cyber-Resiliency of DER-based Smart Grid: A Survey

Mengxiang Liu, Zhenyong Zhang, *Member, IEEE*, Pudong Ge, *Student Member, IEEE*, Ruilong Deng, *Senior Member, IEEE*, Mingyang Sun, *Senior Member, IEEE*, Jiming Chen, *Fellow, IEEE*, and Fei Teng, *Senior Member, IEEE*

***Abstract*—The rapid development of information and communications technology has enabled the use of digital-controlled and software-driven distributed energy resources (DERs) to improve the flexibility and efficiency of power supply, and support grid operations. However, this evolution also exposes geographically-dispersed DERs to cyber threats, including hardware and software vulnerabilities, communication issues, and personnel errors, etc. Therefore, enhancing the cyber-resiliency of DER-based smart grid - the ability to survive successful cyber intrusions - is becoming increasingly vital and has garnered significant attention from both industry and academia. In this survey, we aim to provide a systematical and comprehensive review regarding the cyber-resiliency enhancement (CRE) of DER-based smart grid. Firstly, an integrated threat modeling method is tailored for the hierarchical DER-based smart grid with special emphasise on vulnerability identification and impact analysis. Then, the defense-in-depth strategies encompassing prevention, detection, mitigation, and recovery are comprehensively surveyed, systematically classified, and rigorously compared. A CRE framework is subsequently proposed to incorporate the five key resiliency enablers. Finally, challenges and future directions are discussed in details. The overall aim of this survey is to demonstrate the development trend of CRE methods and motivate further efforts to improve the cyber-resiliency of DER-based smart grid.**

***Index Terms*—Cyber-resiliency enhancement, DER-based smart grid, threat identification, defense-in-depth strategies**

I. Introduction

The power system is rapidly transitioning to address the ever-increasing power demand, energy crisis, and critical climate challenges. This transition involves the decentralization of generation and digitization of customer services. Distributed energy resources (DERs), such as photovoltaic (PV) panels, wind turbines (WTs), electric vehicles (EVs), batteries, and diesel generators, are driving this transition from the traditional large spinning generation to the sustainable and decarbonized DER-dominated generation [1]–[3]. The utilization of digital-controlled and software-driven DERs can greatly enhance the flexibility and efficiency of power supply to customers. Moreover, IEEE Std. 1547-2018 has been put on the table to formalize the interconnection and interoperability of DERs with associated power system interfaces, such as frequency disturbance ride-through capability, to support grid operations [4]. Along with the transition towards the low-carbon future, there is an increasing demand for advanced information and communications technology (ICT) like 5G, Industrial Internet of Things (IIoT) technologies, and software-defined networks (SDN), etc. These technologies, together with smart inverter devices, offer numerous benefits for the transition. However, they also pose various cyber threats [5]–[7].

M. Liu, P. Ge, and F. Teng are with the Department of Electrical and Electronic Engineering, Imperial College London, London, UK.

Z. Zhang, R. Deng, M. Sun, and J. Chen are with the College of Control Science and Engineering, Zhejiang University, Hangzhou, China.

A timeline documenting the major cyberattacks against power grid between 2010 and 2022 with a focus on the last three years is shown in Fig. 1. The power grid, being a critical infrastructure of a country, has been a prime target for state-sponsored or profit-driven attackers. Recent cyberattacks, such as REvil [8] and EnerCon [9], indicate that renewable energy resources are frequently targeted by adversaries seeking to extort ransom or disrupt communication links. Furthermore, as DERs are physically connected to the power grid and extensively involved in grid operations, attackers can maliciously control their behaviors to cause system-wide impact, such as frequency/voltage instability, line failure, and power outages. [10]. Given the unique characteristics of DER-based smart grid, several exclusive cybersecurity challenges are summarized: i) Utility operators do not have complete access to DERs installed and maintained by individuals and third parties; ii) Geographically dispersed DER systems lack security mechanisms to prevent physical intrusion; and iii) Numerous private and public network access points do not have sufficient security measures in place.

To address these challenges, cyber-resiliency - the ability to survive successful cyber intrusions - must be integrated into the planning, control, and management processes of DER hardware, software, and communication networks. This integration will ensure continuous electricity flow to meet the critical load of customers, even during cyberattacks. Resiliency, which was first defined by Holling in 1973 as a system's ability to maintain its functionality and behavior after a disturbance [11], was initially proposed to address natural disasters. However, given the increasing threat of cyberattacks, cyber-resiliency has recently been defined as a system's ability to limit the impact, duration, and extent of degradation caused by high impact and low probability (HILP) cyberattack events [12]–[15]. Enhancing the cyber-resiliency is particularly crucial to pave the way towards large-scale deployment of DERs.

The cyber-resiliency oriented system can be classified into three stages and five phases based on the occurrence time of HILP cyberattack events as shown in Fig. 2. The three stages are pre-event, during event, and post-event, while the five phases are identification, prevention, detection, mitigation, and recovery. Two distinctive perspectives on the smart grid performance level are relevant: 1) The extent and quality of power supply services to customers; 2) The infrastructure's ability to maintain data confidentiality, integrity, and availability (CIA) while also providing power generation, transmission, and distribution functionalities. In the pre-event stage (hours

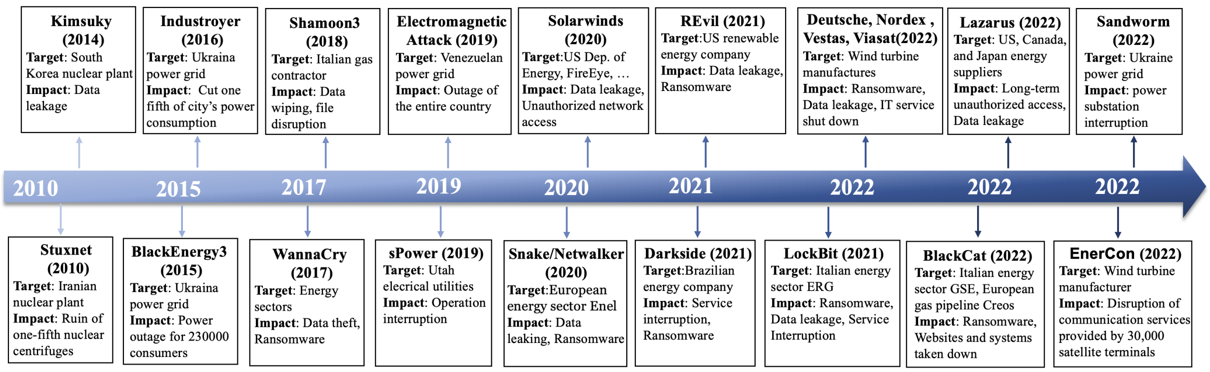


Fig. 1: Timeline of the cyberattacks targeting at power systems from 2010 to 2022 with an emphasis on the recent three years.

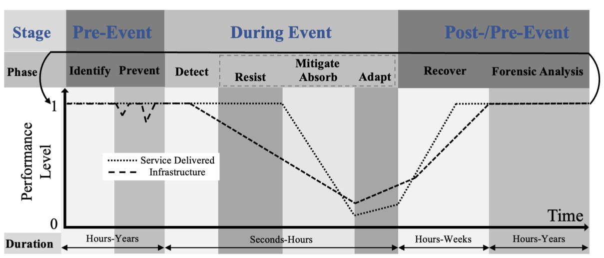


Fig. 2: Cyber-resiliency stages and phases.

to years), threat identification [16]–[23] as well as prevention technologies [24]–[27] are needed to identify possible vulnerabilities and provide preventative capabilities against common and naive cyberattacks, under which the data CIA might be compromised but will recover soon. Given undisclosed zero-day vulnerabilities and inappropriate configuration or management of prevention technologies, they may be bypassed and invalidated by powerful and persistent adversaries. During a successful cyber intrusion event, a basic need is to detect anomaly [28]–[30] and mitigate attack impacts [31]–[33] in a timely manner (seconds to hours), where the mitigation phase can be further divided into resistance, absorption, and adaption [12]. In the post-event stage, when the system under attacks is maintained stable, recovery actions should be activated to thoroughly remove the malware from the system, reconstruct the communication network, and repair the power line outage to restore the normal operations [34]–[36], after which forensic analysis will be conducted for further guideline development [37]. This stage can take hours to weeks/years§, where the power supply is first recovered, after which the power and cyber infrastructure will be restored sequentially.

Drawing inspiration from the NIST cybersecurity improvement framework [38], which provides a high-level and strategic view of the lifecycle of an organization's management of cybersecurity risk, we propose a holistic cyber-resiliency enhancement (CRE) framework tailored for the DER-based smart grid, as shown in Fig. 3. In addition to the risk-based approaches to managing cybersecurity, the CRE framework specifies the detection, mitigation, and recover capabilities by utilizing the characteristics, controllability, and flexibility of field physical devices. Furthermore, short- and long-term resiliency assessment are included to measure how quickly and to what extent system performance drops, as well as how promptly the system recovers, based on knowledge of system dynamics and flexibility [13], [39]. To improve the system's resiliency, all five phases should be considered in a holistic approach, as the resiliency level is determined by the phase with the worst performance, akin to the "Buckets effect". Specifically, actions designed within each phase must consider their interactions with other phases, including how information from the preceding phase can be used and how it can serve the next phase. This requires a global understanding of the CRE process. In this context, we aim to provide a systematic and comprehensive survey of recent CRE developments and future directions for DER-based smart grid. The detailed contributions of this survey are listed as follows:

1) The hierarchical architecture of DER-based smart grid is demonstrated to illustrate the participating actors and the corresponding functionalities.

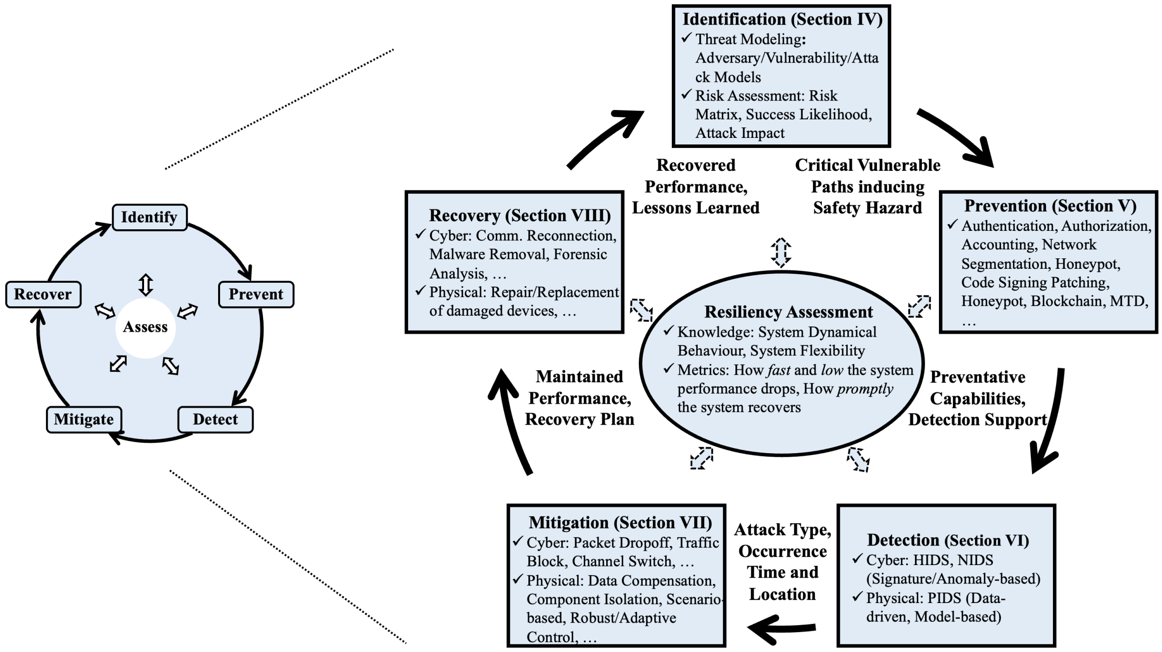
2) An integrated threat modeling method is tailored for the hierarchical DER-based smart grid to clarify the adversary model, asset/vulnerability model and attack model, after which a risk matrix is developed to assess the risk of threats considering both their success likelihood and associated impacts.

3) The progresses made in prevention, detection, and mitigation technologies are comprehensively reviewed, systematically classified according to work principles (cyber/physical, signature-/anomaly-based, self-/detection-triggered, etc.), and rigorously compared based on detection/mitigation performance. Besides, the necessity and aim of recovery scheduling are highlighted under HILP cyberattack events.

4) A holistic CRE framework that incorporates the five key enablers of resiliency is proposed, with their challenges and future directions being discussed in details.

II. Related Works

There exist several surveys regarding the cybersecurity of DER-based smart grid [10], [17], [20], [40]–[42]. Zografopoulos *et al.* [40] provided a DER cybersecurity outlook covering the device- and communication-levels vulnerabilities, attacks, impacts, and mitigation schemes. Sahoo *et al.* [20] presented a brief review of the vulnerabilities in the control and cyber layer of the voltage source converters (VSCs) both in the grid-connected and standalone modes. Vosughi *et al.* [17] discussed



(a) Conceptual demonstration

(b) Detailed illustration

Fig. 3: The cyber-resiliency enhancement framework for DER-based smart grid.

the latest trends in the DER control schemes along with the cyber-physical vulnerabilities, standard communication protocols, and key security mechanisms. Ye *et al.* [10] discussed the challenges and future visions of the cyber-physical security of PV systems from firmware, network, PV converter control, and grid security perspectives. Qi *et al.* [41] proposed a holistic attack-resilient framework compromising threat modeling and defensive actions (attack prevention, detection, and response) to help ensure the secure integration of DER without harming the grid reliability and stability. Li *et al.* [42] presented a comprehensive review of critical attacks and defense strategies for smart inverters and inverter-based systems like microgrids. Nevertheless, the existing literature either lacks systematical threat modeling, risk assessment methods or neglects a comprehensive review of existing defense-in-depth strategies. For threat modeling and assessment, only [40] detailed the adversary model, while [20] and [17] lack comprehensive vulnerability investigation. For defense-in-depth strategies, [20] and [10] did not discuss prevention technologies, and [20] and [17] did not consider intrusion detection systems (IDSs). All literature includes impact mitigation systems (IMSs) but only [42] classified and summarized them. Moreover, recovery scheduling is not covered in any of the literature. To fill these gaps, this paper aims to provide a high-level threat modeling framework, specific risk assessment method, and systematical review of state-of-the-art defense-in-depth strategies.

III. Identification: Threat Modeling and Risk Assessment

In this paper, we adopt the bottom-up principle to identify potential threats arouse from hardware, software, communication, and personnel, and then assess their risk considering the success probability and consequence severity. Before introducing the technical parts, a refined description of the hierarchical framework of DER-based smart grid will be first presented.

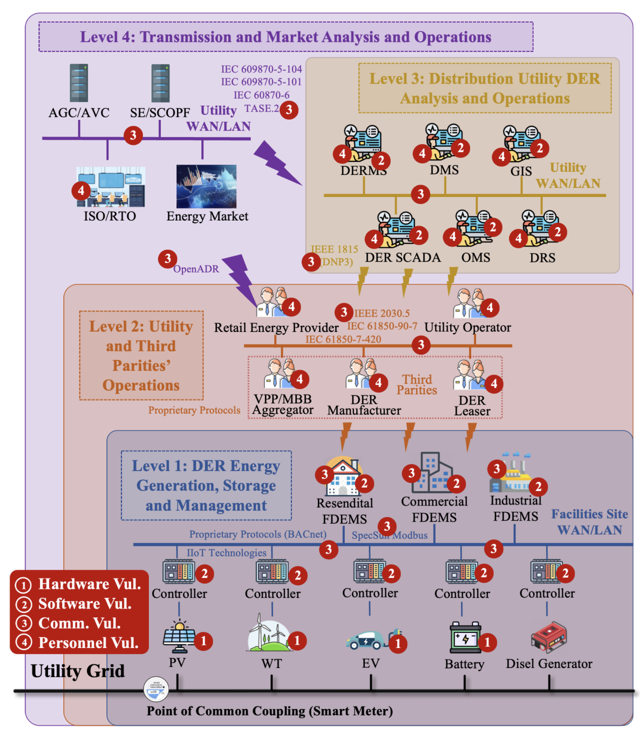


Fig. 4: Hierarchical framework of DER-based smart grid and vulnerabilities.

A. Hierarchical Framework of DER-based Smart Grid

Given the large and increasing amount of geographically dispersed DER systems, it is difficult for utility operators and stakeholders to directly control and manage their operations, and a generic hierarchical architecture is in need to interact with them. According to the functionalities and corresponding properties of actors involved in the DER-based smart grid, they are divided into four levels [16]: 1) Level 1 - DER energy generation, storage, and management; 2) Level 2 - Utility and third parities' operations; 3) Level 3 - Distribution utility DER analysis and operations; and 4) Level 4 - Transmission and market analysis and operations.

Level 1 collects the basic DER units compromising renewable energy source (PV, WT, EV), non-renewable energy source (disel generator), and storage systems (battery). Open standard communication protocols (SunSpec Modbus [43]), proprietary protocols (BACnet [44]), and emerging IoT technologies (ZigBee, WiFi, and 5G) are widely adopted to enable the real-time interaction among DER units and facilities DER energy management systems (FDEMSs), and thus provide DER's autonomous response capabilities and ancillary services [17]. Level 2 includes the actors beyond local sites like utility operators, retail energy providers (REPs), as well as third parities including virtual power plants (VPPs) [45], microgrids [3], DER manufacturers, DER leasers, etc. Communication standards including IEEE 2030.5 (SEP 2.0) [46], IEC 61850-90-7 and IEC 61850-7-420 [47], as well as the proprietary protocols of third parties and utilities are used to achieve the interaction among DER units, utilities, and third parties, enabling regular maintenance and energy market services [48].

Level 3 is responsible for the state analysis and operation determination of DER units in the region of the distribution power system. Many utility actors including DER SCADA, DER management system (DERMS), distribution management system (DMS), etc. are employed to ensure the safe, efficient, and reliable operation and scheduling of wide-area dispersed DER units. The involved communication protocols include IEEE 2030.5 (Smart Energy Profile 2.0, SEP 2.0), IEC 61850-90-7, IEEE 1815 (DNP3) [49], and proprietary protocols of utilities. Level 4 is responsible for the analysis and operation of wide-area dispersed transmission system and related energy trading market. Applications including automatic generation/voltage control (AGC/AVC), security-constrained economic dispatch /security-constrained optimal power flow (SED/SCOPF), and independent system operator/regional transmission organization (ISO/RTO) balancing authority should be reconsidered given the uncertainty, variability, and market participation of geographically dispersed DER units. The advanced metering infrastructure (AMI) plays a fundamental role for two-way data exchange between remote DER units and the transmission control center [5], [50], [51].

B. Threat Modeling

Threat modeling aims to identify, classify and describe threats to highlight a campaign of attacks or attackers. Based on the innovative threat modeling of smart grid [6], MITRE ATT&CK knowledge base [52], NIST electric utility guidelines [53], and European Union Agency for Cybersecurity threat landscape [54], a holistic threat modeling framework that integrates both IT and OT perspectives are tailored for the DER-based smart grid, comprising the adversary model, key vulnerability and attack model.

1) Adversary Model: The adversary model details the identity, motivation, knowledge, access, and resource of a threat, based on which the defender is able to evaluate the capabilities, intentions, and objectives of the attacker. The threat actors include state-sponsored actors, terrorists, cybercriminals, hacktivists, cyber fighters, and disgruntled employees, among which the state-sponsored actor is most terrifying as they have top-notch fund support. The adversary motivation include ransomware, competitor discrediting, cyberwarfare, economic gain, and terrorism/political. The adversary knowledge includes both the cyber-domain operational information [55], and can be classified as 1) White-box with *full* knowledge; 2) Gray-box with *partial* knowledge; 3) Black-box with *zero* knowledge [56]. The adversary access includes physical access through serial/USB/Ethernet interfaces [57], remote access through phishing emails [58], and close proximity access through wireless compromise [59]. The adversary resource consists of substantial and limited privileges. The state-sponsored actor has substantial privileges for unlimited resources while the hacktivist only has limited privileges.

2) Key Vulnerability: DER-based smart grid is a typical human-in-the-loop cyber-physical system, where the cyber vulnerabilities may come from hardware, software, communication, and personnel and exist in every layer. The typical hardware vulnerability is the weak physical access control to DER assets, which directly exposes various communication interfaces to the adversary. More recently, the hall sensor widely adopted in inverters has been proved to be vulnerable to the external magnetic field excited by the adversary [60]–[63]. The software vulnerabilities can exist in the firmware, user code, management software, etc, and allow the adversary to access the system illegally, steal sensitive data, and disrupt system services. The software-driven principle of DER makes it particularly impressionable to this kind of vulnerability and should be paid enough attention. Summarizing the current development trend of DER-based smart grid, the typical software vulnerabilities include 1) Insufficient test and validation on firmware and user code [64], 2) Insecure supply chain [65], [66], and 3) Zero-day vulnerabilities [67].

The communication vulnerability is the most well-known type and come from communication protocols, network component/participator, and communication services. According to the literature and technical reports, the communication protocol related vulnerabilities include 1) Insufficient security mechanisms in SunSpec Modbus [43], [68], 2) Scalability gaps of IEEE 2030.5's security features [68], 3) Security flaws of IEC 62351 [69], [70], 4) Inadequate security consideration in DNP3-SA and DNP3Sec [71], [72], 5) Security flaws of transmission communication protocols [71]. As the integration of third parties into the system operation, management, and maintenance, some network component/participator related vulnerabilities are also induced: 1) Insufficient network seg-

TABLE I: Attack Techniques Summary and Classification

Attack Techniques		Description
Hardware-targeted	Hall spoofing attack	Mislead hall sensor's measurement by placing a camouflaged attack tool near the inverter [63]
	Phase-locked loop (PLL) attack	Inject false pulse voltage signal to mislead PLL reading to DER controller [82]
	Side-channel attack	Analyze time/power/electromagnetic information to infer critical information [83]
Software-targeted	Control logic modification	Modify control logic of DER controller to manipulate outputs or trigger overflow bug [84]
	Malicious firmware installation	Install malicious firmware into inverter/converter to leave backdoor for remote access [85]
	Trojan attack	Inject Trojan malware into control code, firmware, or software to damage file and leak data [86]
	Zero-day attack	Exploit zero-day vulnerability to get illegal access to the DER system
	Supply-chain attack	Install rootkit or hardware-based eavesdropping program to compromise delivered products [66]
Communication-targeted	Wireless compromision	Exploit wireless protocol vulnerability to obtain illegal remote access to DER network [87]
	Online service exploitation	Use directory traversal, cross-site scripting, SQL injection to illegally access DER network [88]
	Brute force attack	Repetitively change I/O point values to impact the process function associated with that point [89]
	Denial-of-service attack	Deliberately overload a DER stakeholder and prevent it from performing normal functions [90]
	Man-in-the-middle attack	Modify and inject data streams exchanged in the DER network [75]
	Eavesdropping attack	Take screenshot of HMI and workstation or listen to communicated confidential [91]
	IoT Botnet attack	Manipulate a large volume of high-watt IoT loads and control their on/off simultaneously [92]
	P2P energy market attack	Submission of fake contract, double spending of energy/money, modification of transaction [77]–[79]
	Evasion and backdoor attack	Create adversarial example with imperceptible perturbation to mislead AI/ML output [80]
Personnel-targeted	Social engineering	Use personal information or subterfuge to learn a legal user's password [93]
	Insider	Person within the organization leak cyber-physical domain critical information [94]

mentation between DER systems [7], 2) Unknown trust level among multiple stakeholders [73], 3) Multiple access points from external networks [74], [75], 4) Indirect and delayed feedback from third parties. Based on the communication infrastructure, numerous services can be provided to enable convenient device management and cost-efficient operation. These services also expose service oriented vulnerabilities, including 1) Insecure remote management services on DER systems [76], 2) Security challenges of P2P energy trading [77]–[79], 3) Vulnerable artifical intelligence and machine learning (AI/ML) based applications [80], [81]. The personnel vulnerability appears as a critical concern as the wide integration of human-involved control and management into the DER-based smart grid. However, it is hard to guarantee the security qualification of the staff of all stakeholders especially when involving a large number of stakeholders.

3) Attack Model: The attack model specifies the attack techniques by exploiting those vulnerabilities and potential attack impacts in the context of DER-based smart grid. Similar as the vulnerabilities, the attack techniques are classified as hardware-, software-, communication-, and personnel-targeted as shown in TABLE I. The attack impact is divided into privacy-related and security-related. From the perspective of CIA, the privacy-related impact concerns the customer information leak caused by data confidentiality violation, including location information, personal behavior patterns and activities inside home, and real-time surveillance information [19].

The security-related impact focuses on how can the cyber-physical attacks impact/disrupt the data availability and integrity, and thus affecting the device-level functionalities and grid-level process and operation. In the distribution level, the security-related impact includes 1) Consumer expense increase in residential units [20], 2) Frequency/voltage deviation and power sharing failure in microgrids [95], [96], 3) Poor power quality [4], 4) Intentional islanding failure [4], 5) Increased power loss [4], 6) Aggravated equipment wear, and 7) Voltage violation [21], [22]. In the transmission level, the security-related impact consists 1) Energy price/load manipulation [97], 2) Generator trip and load shedding [21], and 3) Load-generation imbalance [92]. It is intuitive that the impact scale is up to the scale of DER systems (Residential, Commercial, or Utility) that is compromised by the adversary [10].

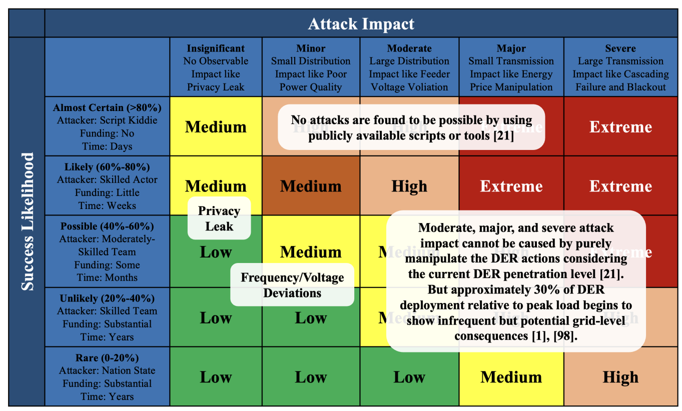


Fig. 5: Threat and risk matrix for DER-based smart grid.

C. Risk Assessment

Based on the threat modeling, we propose the threat risk matrix for DER-based smart grid in Fig. 5 that incorporates both characteristics from IT and OT domains. For each threat scenario, the success likelihood of attacks and attack impact are used to evaluate the risk level. The success likelihood is related to the attack actors, funding level, and time used to prepare for the attack, and the exact likelihood is estimated from the red team assessments and attack graphs [21]. The attack with almost certain probability cannot currently be achieved as no public scripts and tools that can indeed impact the power system exist [21]. Since the DER penetration is not high, moderate, major, and severe attack impact cannot be caused by purely manipulate the DER actions. It has been pointed out that approximately 30% of DER deployment relative to peak load begins to show infrequent but potential grid-level consequences [1], [98]. Hence, attention should be paid this threat that is currently impossible, but is likely to be possible under the global trend towards the low-carbon power system [99]. The skilled actor/team or nation state can cause insignificant and minor impact on DER-based smart grid. For example, the personal behavior pattern may be inferred after eavesdropping the energy usage and DER generation data from smart meters/PMUs and data servers [19], and frequency/voltage deviations can appear in islanded microgrids when multiple primary/secondary controllers are compromised by a skilled team [95], [96].

IV. Defense-in-Depth Strategies: Prevention

Prevention technologies deploying at host and network levels aim to prevent the adversaries from intruding into the DER network. This section summarizes the development status and trend of protection technologies in the DER-based smart grid from the literature and reports, including encryption and authentication, role-based access control, network segmentation and boundary protection, virtualized DER equipment, blockchain, as well as moving target defense (MTD).

Encryption and Authentication: The basic method to protect the security of data-in-transit is to integrate encryption and authentication attributes into the DER communication protocols like IEEE 2030.5, IEEE 1815, SunSpec Modbus, and IEC 61850. From the aspects of data encryption, device authentication, and key management, the SunSpec/Sandia DER Cybersecurity Workgroup summarized three requirements for DER communities to implement data transmission [24]: 1) The authenticated encryption with associated data allows a recipient to check the integrity of both the encrypted and unencrypted information in a message [100]. 2) The X.509 digital certificates help devices establish a secure connection in a public key infrastructure by formally binding cryptographic keys to a device's identity using a digital signature [101]. 3) The elliptic curve cryptography public key cryptography based on elliptic curves over finite fields can provide the same cryptographic strength with significantly smaller keys than those of RSA [102].

Role-based Access Control: Access control restricts access to resource functionality unless the user is authorized. Since multiple users with varying roles and responsibilities need differing levels of access to DER data and/or DER control modes, a set of role-based access control (RAC) security policies and technologies was established to minimize the risk of unauthorized electronic access to DER systems [25]. The RAC system aims to define a strict control environment where users are authorized to access DER monitoring and control features through three steps: 1) User is identified using a proof-of-identity, 2) User is authenticated by a managed database, and 3) User is authorized for a specific level of access.

Network Segmentation and Boundary Protection: The DER resources with the same criticality level, which is determined based on the impact of any misuse of the resource to grid reliability, public safety, finances, and privacy, are usually grouped [103]. Network segmentation and boundary protection technologies are needed to block the propagation of attack impacts from groups with lower criticality levels to those with higher criticality levels.

Code-Signing Software Patching: Since DER equipment is expected to operate in the field for 25 or more years, during this period, there will undoubtedly be newly discovered vulnerabilities in software packages or custom code that is running on the equipment. In those situations, it may be necessary to secure the software supply chain using code signing or equivalent mechanisms, which identify the source of the patch and confirm the integrity of the data. The primary technology underpinning good patching practices is code signing, using a digital signature mechanism to verify the identity of the data source and a checksum/hash to verify the data has not been altered in transit [26].

Virtualized DER Equipment: Virtualized OT equipment can provide practitioners with situation awareness and better understanding of adversary tactics, techniques, and procedures. In practices, the virtualized DER equipment can be configured to provide protection by directing adversary focus away from critical assets and detection by sending alerts when the adversary interacts with the artificial equipment [27]. Virtual DER units can be deployed in i) Honeypots–internet-connected applicants to capture adversary actions; ii) Canaries–virtualized device deployed alongside real DER units.

Blockchain: Blockchain is a digital data structure comprised of a shared, decentralised, and distributed database or ledger with a continuous log of chronological transactions [104]. The blockchain technology can be introduced to establish a trust relationship between any two stakeholders (including DER owners, DER aggregators, utility operator, and third parties) who do not trust each other. Due to the decentralised data sharing/management scheme and transparent and immutable transaction for security, the potential of implementing DER-involved applications such as P2P energy trading [105], smart contract [106], energy management [107], competitive pricing [108], etc. using blockchain has been widely investigated.

Moving Target Defense: Moving target defense (MTD) is a proactive defense mechanism aiming to enhance security by dynamically modifying the controlling the attack surface through system configuration manipulation, rather than eliminating all vulnerabilities of system components [109]. The goals of MTD include [110]: 1) Increase uncertainty and complexity for any adversary of the system, 2) Decrease the opportunities for the attacker to identify vulnerable system components, and 3) Introduce higher cost in launching attacks or scans. The MTD tool that leverages the software define network can be leveraged to randomize network parameters and communication paths in a DER network [111].

Lessons Learned: Although many advanced prevention technologies are available from IT domain, nontrivial adjustments are still needed before they can be applied to DER-based smart grid. However, the adoption of IT security technologies should consider the balance among three key properties i.e., system performance, security requirement, and security budget. It is not recommended to reach an extreme high security level while degrading the system performance a lot or exceeding the budget. In summary, it is impossible to design a 100% secure system as all systems have some visible and invisible vulnerabilities and can be subjected to various forms of cyberattacks.

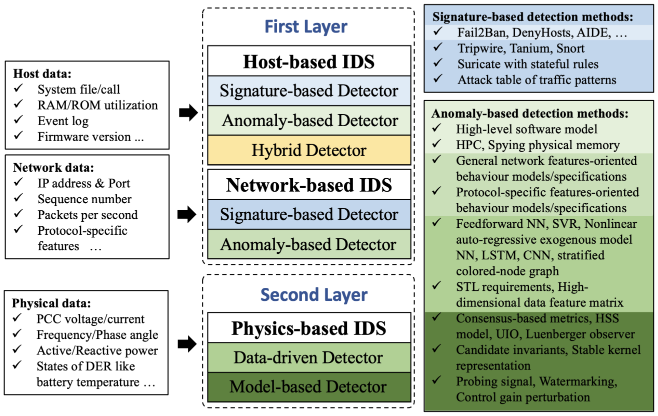


Fig. 6: Summary and classification of IDSs.

V. Defense-in-Depth Strategies: Intrusion Detection System

The IDS is responsible for detecting malicious activities by monitoring and analyzing the behaviour features originated from hosts, network devices, or physical-side sensors. According to Fig. 6, the IDSs can be classified into three classes according to the origination of data: i) The Host-based IDS (HIDS) is to inspect the integrity of the host itself by examining the host-based features such as system files, system calls, processes, RAM/ROM utilization, firmware version, etc.; ii) The Network-based IDS (NIDS) aims to monitor and analyze network related attributes such as IP addresses, service ports, traffic volumes, protocol attributes, etc.; iii) The Physics-based IDS (PIDS) is to detect the anomaly of physical measurements like PCC voltages/currents, frequency, active/reactive power, etc. Depending on the type of analysis carried out, each IDS can be further classified as signature-based and anomaly-based [112]. The signature-based IDS aims to seek predefined *patterns/signatures* of cyberattacks within the analyzed data. The anomaly-based IDS attempts to estimate the *normal* behaviour of the system to be monitored using metrics, specifications, rules, observers, AI/ML training models, etc., and generates an anomaly whenever the deviation between the actual system and the *normal* system exceeds a predefined threshold. Different from HIDSs and NIDSs, the cyberattack signatures/patterns cannot be easily extracted from physical states, and thereby majority of PIDSs are anomaly-based. According to the type of knowledge used to describe normal behaviours, the PIDS is further classified as data-driven and model-based. The data-driven PIDS captures data-oriented characteristics of normal behaviours like AI/ML models, while the model-based PIDS extract model-oriented properties of normal operations such as observers.

A. Host-based IDS

The HIDS is usually deployed at critical and vulnerable hosts like servers and workstations and intelligent electronic devices (IEDs) to detect cyber intrusion. There are many signature-based HIDS software available that can be directly installed into the upper hosts. Lai *et al.* [28] comprehensively reviewed these HIDSs including Fail2Ban, DenyHosts, AIDE, Tripwire, OSSEC, Samhain, etc., analyzed their application scenarios, and highlight their features. As an integral component of advanced AMI used in modern power systems, the security of smart meter has attracted great attention. Tabrizi *et al.* [113] proposed an anomaly-based HIDS based on the high-level model of the smart meter software, imposing little performance overhead, even under severe memory constraints, and effectively detecting both known and unknown attacks. To further improve the detection performance, Liu *et al.* designed a hybrid and collaborative HIDS for smart meters by setting spying domain randomly in physical memory in combination with using secret information and event log, under which illegal reading and writing is identified once the spying domain is modified [114]. To identify malicious instructions and counterfeit firmware within the inverter controller, Zografopoulos *et al.* [115], [116] developed an anomaly-based HIDS utilizing custom-built Hardware Performance Counters (HPCs) and time series classifiers (TSCs).

Lessons Learned: Current research status regarding HIDSs mainly focuses on the upper hosts and smart meters. However, as the most basic components that integrate physical DER equipment with cyber-side control and management, the converters and inverters have not obtained enough attention. Compared with the HIDSs for smart meters, the biggest challenge for inverters and converters lies in that their computation and memory resources are strictly restricted.

B. Network-based IDS

The NIDS is usually deployed at strategic points in a DER communication network, and careful considerations of the hardware and network components are needed to ensure effective security monitoring. The NIDS using Snort equipped with default rules has been verified to be effective in detecting malevolent traffic in-between an aggregator and a single PV inverter induced by naive cyberattacks [29], [117], [118]. The collaboration among multiple NIDSs placed at field device and control center levels are investigated in [119], where field device NIDSs monitor Modbus-related traffic and control center NIDSs monitor DNP3- and IEEE 2030.5-related traffic. To incorporate the physical characteristics into the design of NIDS, Kang *et al.* proposed a novel framework allowing stateful analysis methods to define its stateful rules that can be run on Suricata [120]. To relief the reliance on IDS software, Sun *et al.* developed a signature-based NIDS by establishing an attack table compromising the information of attack patterns in terms of attack types and time sequence of anomaly events based on the temporal failure propagation graph technique [121].

The anomaly-based NIDSs are further classified into two groups according to the feature types adopted to develop normal behaviour models. *The first NIDS group* uses general network features regardless of the protocol types. Based on the length and number of packets, the inverter behaviour model is learned using the adaptive resonance theory artificial NN algorithm with online update capability [29], [122]. A distributed NIDS framework is developed for AMI, where intelligent modules are deployed at three layers to perceive malicious network traffic collaboratively [123]. To effectively trade false positives for a high detection probability, lightweight specification-based behavior rules are defined for critical devices of a modern electrical grid [124]. *The second NIDS group* adopts protocol-specific features. Based on the semantics of GOOSE and SV messages, the specifications that define the normal behaviours of IEDs are developed and embedded in the built-in NIDS inside IEDs to detect the GOOSE and SV related intrusions [125]. Through incorporating substation configuration description language and normal IEC 61850 traffic contents, the normal and correct behaviour models using in-depth protocol analysis are defined [126]. Using both statistical analysis of traditional network features and specification-based metrics, Kwon *et al.* proposed a novel behavior-based NIDS [127]. For ZigBee-based home area networks, a normal behaviour model is established according to SEP 2.0 and IEEE 802.15.4 standards [128].

Lessons Learned: 1) Extra communication components like switches and network taps are usually required to ensure that NIDSs can access required network traffic for monitoring, and thus achieve expected detection performance. Therefore, the deployment cost of NIDSs has to be concerned in the design phase with numerous geographically dispersed terminal devices in the DER-based smart grid. 2) The signature-based NIDS can generate a highly reliable result regarding known attacks, but is not capable of addressing unknown attacks even if they are very similar to known attacks. On the contrary, the anomaly-based NIDS can handle unknown attacks such as zero-day attacks, while its rate of false positive alarms is higher than that of the signature-based NIDS. The combination of the basic principles of signature- and anomaly-based methods to enhance detection perfromance is still not clear. 3) The NIDS based on general network features can be easily applied to various scenarios regardless of the communication protocol and communication architecture, while the NIDS using specific protocol-specific features can lead to better detection performance in terms of accuracy and response time. To meet the increasing applicability and performance requirements, more efforts should be devoted to the design of NIDSs incorporating both general network and protocol-specific features.

C. Physics-based IDS

The PIDS is usually deployed near the field devices, regarded as the last detection line, to directly interact with sensors or controllers for the sake of real-time measurement acquisition. The principal part of data-driven NIDS is to train a AI/ML model using normal physical data, formulate specifications, or extract data features from normal physical data such that data-oriented characteristics of normal behaviours can be captured. After taking inputs of monitored data comprising of multi-interval DER dispatch signals and corresponding network status including nodal voltage magnitudes and phase angles, a kernel support vector regression (SVR) model is adopted to predict the system margin of the time of interest [129]. When it involves complex and fast-varying control dynamics, the prediction of system states would be even more challenging. Habibi *et al.* tried to address this issue by adopting a nonlinear auto-regressive exogenous model NN for the real-time estimation of voltages and currents in DC microgrids [130]. The usage of electrical waveform data has been verified to be powerful in the root cause diagnosis of anomalous events. Based on time-domain mean current vector-based features originated from raw waveform data, the long short-term memory (LSTM) and convolutional NN (CNN) classifiers are able to distinguish between normal conditions, component failures, and false data injection (FDI) attacks in EVs and PV farms [131], [132]. Besides attack detection and identification, the raw waveform data can also be used in the location of attack sources [133], [134]. To reduce the amount of required training data, transfer learning was incorporated into the cyberattack detection framework [135]. The specifications and data features extracted from physical data are also used to construct PIDSs, which is training-free compared with the AI/ML methods. Signal temporal logic (STL) requirements, which are formalisms to monitor the output voltages and currents of DC microgrids against predefined specifications, were employed for anomaly detection [136].

The key part of model-based PIDSs is to develop consensus-based metrics, establish predictors/observers, or identify invariants based on the underlying model dynamics derived from physical structures and control algorithms such that the model-oriented properties of normal operations can be extracted. Due to the widespread adoption of consensus based secondary control in microgrids, various consensus-oriented detection metrics such as cooperative vulnerability factor (CVF) [137] were derived to detect anomalous sensor measurements and communicated data in DC microgrids. When utilizing the primal-dual algorithm to solve the consensus optimization problem in isolated microgrids, dual variable-related detection metrics could be designed to detect FDI attacks [138]. To further improve the detection accuracy, the physical dynamics obtained from Kirchhoff circuit laws were incorporated into the design of attack detectors. The Harmonic-State-Space (HSS) model was developed to predict current measurements of PV farms, which were then used for integrity verification [95]. By synthesising a Luenberger observer and a bank of unknown input observers (UIOs), a distributed monitoring scheme was established for each DER unit to verify the integrity of neighbors' data [139]. Considering the robustness against unknown disturbances and parameter variations, a multi-objective optimization problem was formulated to design the generation scheme of detection residuals [140]. The system properties that do not vary over time under normal operations are also adopted as indicators for the anomaly induced by cyberattacks. By identifying the variation of inferred candidate invariants that are extracted from both physical plant and controller software, Beg *et al.* proposed a FDI attack detection scheme for DC microgrids [141]. With the small-signal model of islanded microgrids, Zografopoulos *et al.* adopted the subspace method to identify its stable kernel representation in the attack-free situation such that any violation could be perceived [142].

Besides the passive anomaly perception principle, the proactive incentive-based detection scheme has also attracted great attention, which proactively adds secret perturbations to system dynamics or signals, for stealthy FDI attack detection. After generating specified small probing signals and then injecting them into controllers, the output signals are compared with pre-determined values to locate infracted controller components in microgrids [143]. Further, by adding watermarks to communicated data between DERs, the replay attack could be detected by testing the existence of statistical properties of watermarks [144]. Considering the system dynamics involved in DC microgrids, the primary control gain was perturbed in a specific manner to uncover the inconsistency between original data and injected one [145].

Lessons Learned: 1) The data-driven and model-based PIDSs have their respective advantages and disadvantages. The data-driven PIDS can achieve satisfactory detection performance against a wide varieties of cyberattacks without requiring any model knowledge. But it relies heavily on the diversity of training data and requires powerful computation resource, and the inexplicable detection results also limits its application to national critical infrastructure. The model-based PIDS is capable to detect known types of cyberattacks in a timely and reliable manner with explainable detection results and acceptable computation burden. However, the detection performance can degrade significantly when the system parameters vary and it only works under limited types of cyberattacks. The joint design of data- and model-based detection principles still requires further efforts. 2) Generally speaking, the HIDS and NIDS can perceive the anomalous traces on host and network related features resulted from malicious intruders, with a quicker rate, than the PIDS as the adversary will not disrupt the physical functionalities immediately after intruding the DER communication network. The cross-layer coordination of PIDS and HIDS/NIDS may significantly increase the detection accuracy and reduce detection latency.

VI. Defense-in-Depth Strategies: Impact Mitigation

The IMS aims to restrict the impacts caused by cyberattacks and tries to restore the system performance. According to the basic knowledge domain of adopted mitigation actions, IMSs are classified as cyber-based and physics-based: The cyber-based IMS uses intuitive cyber-side actions like packet drop to exclude the malicious components from the remaining network; The physics-based IMS adopts local control or global resource schedule flexibility to compensate for the data integrity/availability loss (FDI/DoS). Furthermore, based on the activation scheme of the mitigation action, IMSs are divided into self-triggered and detection-triggered. The detection-triggered IMS can be only activated when the IDS alarms while the self-triggered IMS can work autonomously regardless of the IDS. As shown in Fig. 7, the cyber-based IMSs are all detection-triggered as the cyber-involved mitigation actions can only work after taking inputs of attack occurrence time and location. The physics-based IMSs consist of both self-triggered and detection-triggered, and some concepts like compensation, robustness, adaptability are further utilized to distinguish the specific methods applied in IMSs.

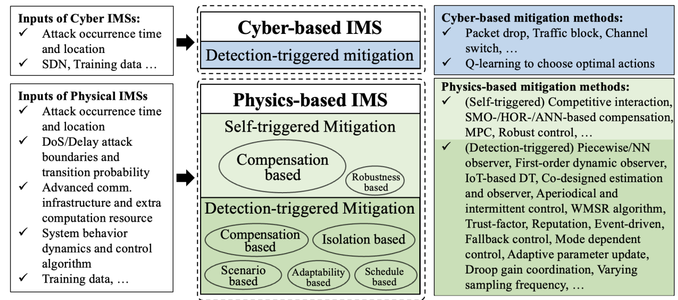


Fig. 7: Summary and classification of IMSs.

A. Cyber-based Detection-triggered IMS

This type of IMS adopts the most intuitive cyber-side mitigation actions encompassing packet drop, traffic block, channel switch to thwart the cyber-side propagation of attack impacts. The simplest mitigation decision is to block the associated malicious network traffic regardless of the anomaly type. Appiah *et al.* designed several mitigation actions against DoS attacks in a DER penetrated distribution automation system [31]. For the microgrid enabled by software define network (SDN) technologies, the SDN controller is designed to block the network traffic from/to the malicious DER unit to guarantee the normal operation of the remaining units when anomaly is perceived [146]. To achieve the cost-benefit tradeoff, Jokar *et al.* presented a Q-learning based intrusion prevention system for the ZigBee-based HAN to automatically adjust the mitigation strategies facing a wide varieties of cyberattacks [128].

Lessons Learned: The cyber-side mitigation strategies are suitable for the IT domain where the data availability is not the primary need. However, when involving the closed-loop control functionalities that require real-time interaction with the physical plant, any data availability loss may induce severe stability issues. Moreover, it is not enough to thwart the propagation of attack impacts by merely excluding the cyber-side malicious sources as the physical couplings could also be exploited for impact propagation. Hence, the cyber-side actions are usually not regarded as the primary choice for impact mitigation in the DER-based smart grid.

B. Physics-based Self-triggered IMS

Since the DoS attack can be easily detected and the subsequent mitigation actions will be activated accordingly, the self-triggered IMS mainly focuses on the FDI attack. According to the adopted methods, the self-triggered IMSs are further classified as compensation-based and robustness-based according to the adopted methods. The compensation-based IMS relies on the construction of a compensation term, which can be just a variable with no physical meaning or the estimation of injected biases or healthy states, such that the attack impact can be mitigated to a certain extent after incorporating the compensation term into the controller. With the assistance of a *hidden and secure* network layer enabled by advanced SDN technologies, a series of virtual states are established to interact with the original control layer such that the anomalous activities could be corrected in an autonomous manner. Liu and Chen *et al.* designed resilient secondary controllers for micorgrids such that the frequency synchronization and active power sharing can be regulated to an arbitrarily small region around the expected point under bounded FDI attacks [32], [147]. To handle *unbounded* FDI attacks, Zuo *et al.* proposed a novel attack-resilient control framework to assure the uniformly ultimately bounded (UUB) voltage containment and frequency regulation [148].

Compared with using virtual states to correct the deviations induced by FDI attacks, an alternative idea is to estimate/observe injected biases or healthy states. The estimation/observer can be accomplished using the corrupted signal together with some extra securely communicated data. Jiang *et al.* designed distributed sliding mode observer (SMO) and high-order differentiator (HOR) based resilient secondary controllers for DC microgrids to compensate for the adverse impact of bounded FDI attacks [149]. Taking inputs of legitimate voltage and frequency information, a distributed observer was established to observe the healthy reactive and active power measurements, respectively, guaranteeing L_2-gain performance under FDI attacks [150]. To guarantee the UBB voltage regulation and proportional load sharing under *unbounded* FDI attacks, an adaptive observer (AO) is employed to estimate the aggregated term induced by attacks on the secondary control input and achieve UBB stability [151]. In addition, an artificial NN (ANN) based decentralized cyberattack mitigation framework was proposed to relief the reliance on model accuracy [152]. Considering the *unbounded* FDI attacks in the *centralized* load frequency control (LFC) of islanded AC microgrids, Hu *et al.* designed a piecewise observer to provide real-time estimates of unknown FDI attack vectors [153]. The incorporation of physical circuit dynamics can be also helpful for the estimation of injected biases or healthy states. Based on the nonlinear DER *circuit dynamics* along with constant power loads, distributed nonlinear adaptive observer and high-order SMOs were established to jointly track the current variation, which may be corrupted by cyberattacks [154], [155].

The robustness-based IMS treats injected bounded FDI attacks as unknown uncertainties and the robust controller is designed to ensure that the tracking error under attacks could be bounded, which requires no extra resource except some extra computation burden but the mitigation performance is not that prefect. Sadbadai *et al.* designed a series of distributed cyber-resilient controllers for (parallel) DC and AC micorgrids (focusing on frequency regulation and active power sharing) to mitigate the adverse impact resulted from the bounded FDI attacks against secondary communication links and actuator signals [156]. Once several key resiliency-related indices are designed to be large enough, the system states can converge to expect values with arbitrary small errors.

Lessons Learned: The biggest advantage of the self-triggered mitigation actions is that they can work without requiring any outputs from IDSs, and thus the adverse impact of false positive alarms could be avoided. However, several requirements also come along with this characteristic: 1) A hidden secure network layer that is independent from the original control layer is needed to run virtual states; 2) In addition to original corrupted data, some extra securely transmitted data is needed to guarantee the estimation/observer accuracy of the injected biases/healthy states; 3) The mitigation scheme needs to be run all the time regardless of the occurrence of cyberattacks, which might induce heavy computation burden especially in the distributed scenario. In summary, the operation of self-triggered IMSs requires extensive supports ranging from communication infrastructure to computation capability, and the associated security cost should be reconsidered when defending against HILP cyberattack events.

C. Physics-based Detection-triggered IMS

According to the adopted mitigation methods, the detection-triggered IMSs are further classified as compensation-based, isolation-based, scenario-based, adaptability-based, and schedule-based. The compensation-based methods involved in this type of IMS are to estimate/observe the unavailable data (DoS attack) or injected bias (FDI attack) after the IDS perceives anomaly. The mitigation strategies against DoS attacks are mainly detection-triggered. Given the duration-restricted DoS attacks in the *centralized* LFC of islanded AC microgrids, a piecewise observer was established to provide real-time estimates of unavailable system states [153]. To guarantee the tracking performance of variable-speed wind turbines (VSWTs) when the rotor velocity measurement is unavailable under DoS attacks, Zhao *et al.* proposed a dual-triggered adaptive control strategy [157]. In addition, considering the *distributed* secondary control in multi-bus DC microgrids subject to DoS attacks, a first-order dynamic observer is adopted to estimate the unavailable load information [158]. Similar to the idea of hidden network layer, Saad *et al.* established a IoT-based digital twin (DT) by emulating the dynamics of cyber-physical networked microgrids to help estimate the unavailable data induced by DoS attacks [159]. In terms of FDI attacks, some detection-triggered compensation methods have also been proposed. To guarantee the tracking performance of VSWTs in the presence of the FDI attacks tampering with velocity measurements, Zhao *et al.* co-designed the estimator and observer to estimate the impact induced by cyberattacks and observe the injected biases simultaneously [160]. After knowing that the data transmitted from neighbors is corrupted by FDI attacks in DC microgrids, Jin *et al.* tried to estimate the injected bias based on the extracted state slopes [161].

The isolation-based IMSs aim to isolate the malicious components from the remaining parts to restrict the attack impact with acceptable performance degradation. Different from directly blocking network traffic in the cyber-based IMS, the isolation-based strategy will not only involve the cyber-side traffic block but also incorporate the knowledge of system dynamics and control algorithms to further enhance the mitigation performance. By switching the data exchange mode among DERs and master controllers in an aperiodical and intermittent manner, FDI attacks resulting in unexpected data transmission modes can be easily detected and *both the communication links and associated DERs* will be isolated [162]. For the consensus-based economic dispatch (ED) and secondary frequency/voltage regulation in microgrids, Zhang and Yassaie *et al.* employed the *weighted mean subsequence reduced (WMSR) algorithm* to discard the the extreme values among the data received from neighbors [163], [164]. Moreover, based on the consensus objectives from either deterministic or statistical perspectives, the *trust-factors* implying the trust level of its own observation and the data received from neighbors are incorporated into the secondary control to eliminate the adverse impact and isolate suspected malicious components [165]–[167]. Besides simply discarding the corrupted data, some further actions can be adopted to mitigate the impact of data loss like replacing the transmitted anomalous data with a local calculated safe but not accurate one. The idea of *reputation* was integrated into the consensus-based ED in microgrids to thwart non-colluding and colluding FDI attacks [168], [169]. If the reputations of half of its neighbors are lower than a predefined threshold, the malicious information will be replaced with locally calculated one. In addition, Sahoo *et al.* proposed a event-driven impact mitigation scheme against the FDI attacks in islanded DC/AC microgrids [170], [171]. The event, defined as the attack detection, will trigger the mitigation strategy to replace the compromised data with the one received from trustworthy neighbors.

The scenario-based IMS will adjust the control algorithm to adapt to different attack scenarios (the number and location of malicious components), which can largely reduce the performance degradation induced by control conservativeness but only work under a number-limited attack scenarios. Considering the DoS attack targeting at the communication link connecting the energy storage system (ESS) and energy management system (EMS) in microgrids, Chlela *et al.* designed a rule-based fallback control strategy to mitigate its impact. When the ESS cannot receive dispatch signals from the EMS, it will enter the decentralized control mode and manage the state of charge in a standalone manner [172]. To handle the excessive latency and damaged cyber connectivity under DoS attacks in islanded microgrids, an event-triggered network reconfiguration scheme was proposed [173]. By modeling random DoS attacks as markovian jumps, Liu *et al.* proposed a mode-dependent resilient controller to restore the control performance of centralized islanded microgrids [174]. The chosen of control parameters under different DoS attacks scenarios (namely different modes) is explicitly investigated to guarantee the stochastic stability of microgrids.

The adaptability-based IMS is to adjust the control algorithm in an adaptive manner without knowing the specific attack scenarios. Obviously, this type of mitigation strategy may be subject to the problem of excessive performance degradation when a over-conservative control parameters are chosen. A self-adaptive resilient control algorithm was proposed to preserve secondary consensus in hierarchical networked microgrids under multi-layer DoS attacks [33]. For the centralized event-triggered control framework of DC microgrids subject to DoS attacks, Hu *et al.* developed an adaptive parameter update scheme to mitigate the attack impact [175]. The schedule-based IMS tries to schedule flexible resources like DERs and sampling frequency to mitigate the impacts of cyberattacks. By adjusting the droop gains of DERs, the destabilizing effect of load alteration attacks (a type of FDI attack) could be effectively mitigated [176]. Moreover, the sampling scheme with time-varying frequency was proposed to restore the communication as soon as the DoS attack terminates [177], [178].

Lessons Learned: 1) Compared with the self-triggered IMS, much more types of detection-triggered mitigation methods are available due to the incorporation of IDS outputs. Moreover, since the detection-triggered mitigation action will be only activated when the anomaly is in presence as a emergency response, its security cost is not as high as that of the self-triggered mitigation action, which is expected to run even in the normal operations. Therefore, standing on the perspective of cost-benefit balance, it is better to use detection-triggered mitigation methods to defend against HILP cyberattack events. 2) In a broad sense, the compensation-/isolation-/scenario-/adaptability-based mitigation methods try to enhance the tolerance of control algorithms against cyberattacks and need to work immediately once perceiving anomaly. While the schedule-based ones aim to employ available flexible resource to resist against cyberattacks and will be only activated when the severity of cyberattacks exceeds the tolerable level of control algorithms. Although numerous research efforts have been devoted to designing either resilient control algorithms or resilient schedule schemes, the holistic integration of the two mitigation strategies is still unclear.

VII. Defense-in-Depth Strategies: Recovery

The recovery scheduling is to recover the degraded system states after mitigation to the normal states. It is vital as after the response of IMSs the blackout/isolated areas cannot be reconnected, the malicious payloads inserted by adversaries still exist, and the damaged electrical devices need repair/replacement. However, to the best of our knowledge, there exists no literature investigating the recovery schedule problem in the presence of HILP cyberattack accidents.

The recovery scheduling can be classified into two phases comprising 1) service restoration and 2) infrastructure recovery according to different time scales [12], where both cyber and physical recovery actions will be involved. In the service restoration phase, the cyber-related restoration actions aim to reconnect the communication network using flexible emergency communication vehicles. The physics-related restoration actions try to restore the electricity supply to the blackout area in transmission and isolated areas in distribution via emergency generators like mobile power supply vehicles or other black-start-capable local generators. After the restoration of customer services, the infrastructure recovery will be activated to repair/replace the compromised/damaged software and hardware facilities to enable properties of $N-1$ security and loss-efficiency, as well as economical dispatch. The cyber-related recovery actions include the removal of virus, malware, and other malicious payloads from the computation and communication environment, generally completed through software reinstall and antivirus tools. The physics-related recovery actions aim to repair the damaged power lines and transformers, synchronize the grid islands to return to interconnected operation, and replace backup and emergency systems with components used in normal operation. As such, the recovery of system states can be finally formulated as a resource allocation problem considering resource constraints, performance requirements from multiple time scales, and cyber-physical interactions. Forensic analysis should be conducted to summarize and learn lessons from the pre-, during, and post-event phases, providing guidelines for better prevention, detection, and mitigation capabilities.

VIII. Challenges and Future Directions

In this section, challenges and future directions are discussed from the five phases including identification, prevention, detection, mitigation, and recovery.

A. Threat Identification

In terms of threat identification, the potential vulnerabilities and corresponding attack impact have been extensively investigated. Standing on the perspective of attacker, a successful attack event requires to exploit multiple vulnerabilities and coordinate them appropriately to induce targeted and precise consequences. There still lack **high-integrated and automatic tools** to identify vulnerability exploitation paths that can cause critical hazards given specific system configurations. This research direction is vital as its outputs can guide the design of defense strategies, but meanwhile is difficult as both the expert knowledge of IT and OT domains are required in the top-bottom design process. Moreover, the automation of the identification tool is a key challenge as the power system modeling involving various cyber and physical components, complex couplings among them, and strict functionality requirements usually needs substantial manual interventions [179].

B. Prevention Technology

Prevention technologies with high security levels have been standardized for the interaction between DERs and power systems. Nevertheless, the MTD, virtualized DER equipment, blockchain technology, and internet architecture can be enhanced to enable further security improvement:

1) **MTD**: The triggering scheme, cost, and performance of MTD can be systematically optimized. More adaptive MTD triggering schemes need to be developed, which requires the advanced detection or learning capabilities of the defender [110]. The key challenge is how to infer an adversary's action or learn system security condition to guide MTD deployment.

2) **Virtualized DER equipment**: To make the emulated virtualized DERs indistinguishable from DER devices, the physical/plant dynamics should be deeply integrated to mimic the behaviours of DER devices instead of simply displaying the historically recorded inputs and outputs. The key challenge is how to emulate complex physical/plant dynamics using resource constrained computation and storage capabilities.

3) **Blockchain**: To enable the implementation of blockchain in the DER-based smart grid, the future efforts should focus on the optimisation of computation complexity, data handling, and number of transactions in blockchain to reduce its energy consumption and provide timely response while guaranteeing required security levels.

4) **Network architecture**: Inspired by a growing awareness of unsolved problems in contemporary internet architectures like IP, the named data networking (NDN) appears to be promising solution to support cybersecure multi-party communications and control using any communication link [180]. It might be of great interest to apply NDN to the DER smart grid to address the multi-party secure communication issue.

C. Intrusion Detection System

Existing IDSs can perceive anomalous activities with satisfactory performance using single-domain features (host, network, or physical) but require add-on detection hardware. The next step needs to integrate IDSs into embedded hardware like inverters, where the computation and memory resource is highly restricted, and investigate the possibility of improving the detection performance by fusing multi-domain features and coordinating multi-layer resources.

1) **Light-weight HIDS for grid edge devices**: Tailoring HIDSs for inverters can greatly help counter against the threats arouse from Trojan, firmware manipulation, supply-chain, etc. The primary challenging is that the HIDS's detection overhead on computation and memory cannot significantly decrease/affect the original control performance of inverters.

2) **Deep integration of cross-domain features**: Both host and network features can shorten the detection latency for perceiving anomalous activities, and physical features can reduce the false alarms flagged by host/network features. The deep integration of cross-domain features can improve the detection performance, but the investigation of an appropriate fusion scheme of multiple domain data is particularly challenging.

3) **Local-centralized coordination of data-driven and model-based PIDSs**: Co-designing model-based and data-driven PIDSs in a local-centralized collaboration manner can help incorporate their respective advantages. Specifically, the data-driven PIDS is employed in the control centre to perceive the existence of anomaly, while the model-based PIDS is adopted in each distributed entity to reveal the malicious component location.

D. Impact Mitigation System

Although numerous IMSs have been proposed to quickly respond to cyberattacks, the design phases ignored the cost-efficiency, cross-level coordination, and adaptability of IMSs, leading to possible future directions:

1) **Cost-efficient data reconstruction method**: Fusing data characteristics of multiple domains can help improve the data reconstruction performance while reducing the cost of extra hardware. The statistical and spatio-temporal correlation properties can be employed to predict the *data interval* of the next time slot, while the semantic information can be used to construct estimators to quickly and accurately find the value within the interval.

2) **Coordination of device- and system-level mitigation methods**: The coordination of device- and system-level mitigation methods can respond to cyberattacks with varying

severity. Device-level mitigation methods will be first adopted to enhance the tolerance of control algorithms against cyberattacks. When the attack severity exceeds the tolerance of control algorithms, the system-level mitigation method will be activated to dispatch flexible resources like DERs to further enhance the attack tolerance.

3) **Autonomous adjustment of mitigation actions**: In practice, the vulnerable components could be subject to both FDI and DoS attacks, and thereby the IMS is expected to be able to autonomously decide the optimal mitigation action based on actual situations. The optimal mitigation action could be affected by multiple factors like the type, duration, and severity of cyberattacks, and an intelligent decision algorithm/module is needed to take all of these factors into account.

4) **MTD-oriented mitigation method**: MTD-oriented IMSs are designed to improve the containment capability against powerful adversary by adding uncertainties to the mitigation actions in a periodical or triggered manner. The key challenge is to design appropriate perturbation schemes to balance the tradeoff between the containment and mitigation performance.

E. Recovery Scheduling

Although many efforts have been devoted to designing recovery schemes under natural disasters like extreme weathers [34], the **recovery scheduling problem under HILP cyberattacks** has not been extensively investigated yet. The cyberattack aims to affect physical functionalities by compromising cyber-side components like firmware and ICT components, while the disaster directly destroys cyber and physical infrastructure. The key difference between cyberattacks and disasters is that the cyberattack consists of a series of intentional actions launched by the adversary, who can interacts with the environment and respond to changes. More specifically, when implementing the cyber recovery scheduling, it is likely for the adversary to perceive corresponding variations and thus recognize the adoption of recovery actions. Then the adversary may adjust the original attack strategy against the recognized actions. Hence, the disaster recovery frameworks are not suitable for the cyberattack events, and substantial efforts are still required to design appropriate cyber recovery frameworks in the DER-based smart grid. **The adversary's response capability to the environment** should be modelled into the cyber recovery scheduling problem, which can complicate the scheduling problem and thereby make it challenging to solve the problem in a timely manner. Besides, as the autonomous intelligence of DERs is being increasingly improved, how to model and solve the cyber recovery scheduling problem in a distributed manner would be another challenge.

IX. Conclusion

In this paper, we provided a comprehensive survey regarding the CRE process in the DER-based smart grid, where threat modeling and risk assessment as well as defense-in-depth strategies are involved. First, a hierarchical architecture of the cyber-physical DER-based smart grid was presented to illustrate the actors and their functionalities. A integrated threat modeling method was tailored for the hierarchical DER-based smart grid with special emphasises on vulnerability identification and impact analysis, after which a risk matrix was established to assess the risk (severity) of threats considering both their success likelihood and associated impacts. Then, the progresses made in prevention, detection, mitigation, and recovery technologies were comprehensively reviewed, systematically classified, and carefully compared. It is observed that current CRE-related literature mainly focuses on the improvement of security-oriented performance and utilization of local and single-domain resources while rarely considers the restriction of security cost and coordination of multi-layer and cross-domain resources. Based on this, challenges and future directions were finally pointed out and discussed in details.

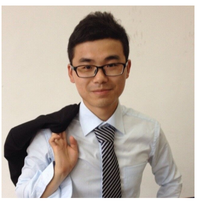
References

[1] U.S. Department of Energy, "Cybersecurity considerations for distributed energy resources on the u.s. electric grid," Tech. Rep., 2022.
[2] North American Electric Reliability Coration, "2020 long-term reliability assessment," Tech. Rep., 2020.
[3] U.S. Department of Energy, "Doe oe 2021 strategy white papers on microgrids: Program vision, objectives, and r&d targets in 5 and 10 years," Tech. Rep., 2021.
[4] "Ieee standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," *IEEE Std 1547-2018*, pp. 1–138, 2018.
[5] M. Emmanuel *et al.*, "Communication technologies for smart grid applications: A survey," *Journal of Network and Computer Applications*, vol. 74, pp. 133–148, 2016.
[6] M. Nafees *et al.*, "Smart grid cyber-physical situational awareness of complex operational technology attacks: A review," *CSUR*, 2022.
[7] Z. Cheng *et al.*, "To centralize or to distribute: That is the question: A comparison of advanced microgrid management systems," *IEEE Industrial Electronics Magazine*, vol. 12, no. 1, pp. 6–24, 2018.
[8] K. M. Brian Eckhouse, "Clean-energy giant invenergy suffers hack claimed by revil," Accessed: 2023, [Online].
[9] A. Durakovic, "Vestas indicates cyber security incident was ransomware attack," Accessed: 2023, [Online].
[10] J. Ye *et al.*, "A review of cyber–physical security for photovoltaic systems," *IEEE JESTPE*, vol. 10, no. 4, pp. 4879–4901, 2022.
[11] C. S. Holling, "Resilience and stability of ecological systems," *Annual review of ecology and systematics*, vol. 4, no. 1, pp. 1–23, 1973.
[12] IEEE PES Task Force, "Methods for analysis and quantification of power system resilience," *IEEE TPS*, pp. 1–14, 2022.
[13] R. Arghandeh *et al.*, "On the definition of cyber-physical resilience in power systems," *RSER*, vol. 58, pp. 1060–1069, 2016.
[14] L. Xu *et al.*, "On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective," *RSER*, vol. 152, p. 111642, 2021.
[15] S. Paul *et al.*, "On vulnerability and resilience of cyber-physical power systems: A review," *IEEE Systems Journal*, vol. 16, no. 2, pp. 2367–2378, 2021.
[16] C. Frances *et al.*, "Cyber security for der systems," Electric Power Research Institute, Tech. Rep., 2013.
[17] A. Vosughi *et al.*, "Cyber–physical vulnerability and resiliency analysis for der integration: A review, challenges and research needs," *RSER*, vol. 168, p. 112794, 2022.
[18] J. Johnson *et al.*, "Distributed energy resource cybersecurity standards development - final project report." 2022.
[19] V. Y. Pillitteri *et al.*, "Guidelines for smart grid cybersecurity," 2014.
[20] S. Sahoo *et al.*, "Cyber security in control of grid-tied power electronic converters—challenges and vulnerabilities," *JESTPE*, vol. 9, no. 5, pp. 5326–5340, 2019.
[21] J. Johnson *et al.*, "Cybersecurity for electric vehicle charging infrastructure." Sandia National Lab, Tech. Rep., 2022.
[22] D. M. Shilay *et al.*, "Catching anomalous distributed photovoltaics: An edge-based multi-modal anomaly detection," *arXiv preprint arXiv:1709.08830*, 2017.
[23] T. S. Ustun, "Cybersecurity vulnerabilities of smart inverters and their impacts on power system operation," in *ICPECA*. IEEE, pp. 1–4.
[24] I. Onunkwo, "Recommendations for data-in-transit requirements for securing der communications." Sandia National Lab, Tech. Rep., 2020.
[25] J. Johnson, "Recommendations for distributed energy resource access control," Sandia National Lab, Tech. Rep., 2021.
[26] J. Johnson *et al.*, "Recommendations for distributed energy resource patching," Sandia National Lab, Tech. Rep., 2021.
[27] ——, "Design considerations for distributed energy resource honeypots and canaries," Sandia National Lab, Tech. Rep., 2021.
[28] C. Lai *et al.*, "Review of intrusion detection methods and tools for distributed energy resources." Sandia National Lab, Tech. Rep., 2021.
[29] C. B. Jones *et al.*, "Implementation of intrusion detection methods for distributed photovoltaic inverters at the grid-edge," in *ISGT*. IEEE, 2020, pp. 1–5.
[30] A. Kavousi-Fard *et al.*, "A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids," *IEEE TII*, vol. 17, no. 1, pp. 650–658, 2020.
[31] J. Appiah-Kubi *et al.*, "Decentralized intrusion prevention (dip) against co-ordinated cyberattacks on distribution automation systems," *IEEE OAJPE*, vol. 7, pp. 389–402, 2020.

[32] Y. Liu *et al.*, "Robust and resilient distributed optimal frequency control for microgrids against cyber attacks," *IEEE TII*, vol. 18, no. 1, pp. 375–386, 2021.
[33] P. Ge *et al.*, "Cyber-resilient self-triggered distributed control of networked microgrids against multi-layer dos attacks," *IEEE TSG*, 2022.
[34] C. Wang *et al.*, "Cyber-physical interdependent restoration scheduling for active distribution network via ad hoc wireless communication," *IEEE TSG*, 2023.
[35] X. Liu *et al.*, "Towards optimal and executable distribution grid restoration planning with a fine-grained power-communication interdependency model," *IEEE TSG*, vol. 13, no. 3, pp. 1911–1922, 2022.
[36] Z. Ye *et al.*, "Boost distribution system restoration with emergency communication vehicles considering cyber-physical interdependence," *IEEE TSG*, vol. 14, no. 2, pp. 1262–1275, 2023.
[37] M. Erol-Kantarci *et al.*, "Smart grid forensic science: applications, challenges, and open issues," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 68–74, 2013.
[38] "Framework for improving critical infrastructure cybersecurity," National Institute of Standards and Technology, Tech. Rep., 2018.
[39] M. Panteli *et al.*, "Metrics and quantification of operational and infrastructure resilience in power systems," *IEEE TPS*, vol. 32, no. 6, pp. 4732–4742, 2017.
[40] I. Zografopoulos *et al.*, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *arXiv preprint arXiv:2205.11171*, 2022.
[41] J. Qi *et al.*, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 28–39, 2016.
[42] Y. Li *et al.*, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE TPE*, 2022.
[43] S. Alliance, "Sunspec der information model specification," *SunSpec Alliance: San Jose, CA, USA*, 2021.
[44] S. T. Bushby *et al.*, "Bacnet today," *ASHRAE journal*, vol. 10, pp. 10–18, 2002.
[45] D. Pudjianto *et al.*, "Virtual power plant and system integration of distributed energy resources," *IET Renewable power generation*, vol. 1, no. 1, pp. 10–16, 2007.
[46] "Ieee standard for smart energy profile application protocol," *IEEE Std 2030.5-2018*, pp. 1–361, 2018.
[47] "Ieee recommended practice for implementing an iec 61850-based substation communications, protection, monitoring, and control system," *IEEE Std 2030.100-2017*, pp. 1–67, 2017.
[48] W. Su *et al.*, "A game theoretic framework for a next-generation retail electricity market with high penetration of distributed residential electricity suppliers," *Applied Energy*, vol. 119, pp. 341–350, 2014.
[49] "Ieee standard for electric power systems communications-distributed network protocol (dnp3)," *IEEE Std 1815-2012*, pp. 1–821, 2012.
[50] C. Bennett *et al.*, "Networking ami smart meters," in *Energy 2030 Conference*. IEEE, 2008, pp. 1–8.
[51] International Electronic Technical Commission, "Systems interface between customer energy management system and the power management system," 2013.
[52] MITRE ATT&CK, "Ics techniques," (Accessed: 2023).
[53] J. McCarthy *et al.*, "Situational awareness for electric utilities," National Institute of Standards and Technology, Tech. Rep., 2019.
[54] A. Sfakianakis *et al.*, "Enisa threat landscape report 2018: 15 top cyberthreats and trends," vol. 10, p. 622757, 2019.
[55] J.-S. Brouillon *et al.*, "Bayesian error-in-variables models for the identification of distribution grids," *IEEE TSG*, vol. 14, no. 2, pp. 1289–1299, 2023.
[56] I. Zografopoulos *et al.*, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29 775–29 818, 2021.
[57] J. Staggs *et al.*, "Wind farm security: attack surface, targets, scenarios and mitigation," *IJCIP*, vol. 17, pp. 3–14, 2017.
[58] H. Holm *et al.*, "Cyber security for a smart grid-what about phishing?" in *IEEE PES ISGT Europe*. IEEE, 2013, pp. 1–5.
[59] J. Staggs, "Adventures in attacking wind farm control networks," (Accessed: 2023).
[60] S. Taranovich, "Teardown: The power inverter from sunlight to power grid," (Accessed: 2023).
[61] "An1444: Grid-connected solar microinverter reference design," 2023.
[62] J. Hu *et al.*, "An improved pmsm rotor position sensor based on linear hall sensors," *IEEE Transactions on Magnetics*, vol. 48, no. 11, pp. 3591–3594, 2012.
[63] A. Barua *et al.*, "Hall spoofing: A non-invasive dos attack on grid-tied solar inverter," in *USENIX Security*, 2020, pp. 1273–1290.
[64] U. Bayer *et al.*, "Dynamic analysis of malicious code," *Journal in Computer Virology*, vol. 2, no. 1, pp. 67–77, 2006.
[65] National Cyber Security Centre, "Supply chain security guidance," (Accessed: 2023).
[66] S. Oladimeji *et al.*, "Solarwinds hack explained: Everything you need to know," (Accessed: 2023).
[67] L. Bilge *et al.*, "Before we knew it: an empirical study of zero-day attacks in the real world," in *CCS*, 2012, pp. 833–844.
[68] J. Obert *et al.*, "Recommendations for trust and encryption in der interoperability standards," 2019.
[69] S. S. Hussain *et al.*, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE TII*, vol. 16, no. 9, pp. 5643–5654, 2019.
[70] R. Schlegel *et al.*, "A security evaluation of IEC 62351," *Journal of Information Security and Applications*, vol. 34, pp. 197–204, 2017.
[71] A. Volkova *et al.*, "Security challenges in control network protocols: A survey," *IEEE COMST*, vol. 21, no. 1, pp. 619–639, 2018.
[72] N. Rodofile *et al.*, "Real-time and interactive attacks on dnp3 critical infrastructure using scapy," in *AISC*. Australian Computer Society, 2015, pp. 67–70.
[73] N. Jefferies *et al.*, "A proposed architecture for trusted third party services," in *CPA*. Springer, 1995, pp. 98–104.
[74] A. A. Almutairi *et al.*, "Web security: Emerging threats and defense." *Comput. Syst. Sci. Eng.*, vol. 40, no. 3, pp. 1233–1248, 2022.
[75] J. Johnson, "A pathway to DER cybersecurity," in *International Conference on the Integration of Renewable & Distributed Energy Resources*, pp. 1–26, 2022.
[76] F. Bret-Mounet, "All your solar panels are belong to me," *DEF CON*, vol. 24, pp. 4–7, 2016.
[77] F. Aloul *et al.*, "Smart grid security: Threats, vulnerabilities and solutions," *International Journal of Smart Grid and Clean Energy*, vol. 1, no. 1, pp. 1–6, 2012.
[78] N. Z. Aitzhan *et al.*, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2016.
[79] K. Shuaib *et al.*, "Cognitive radio for smart grid with security considerations," *Computers*, vol. 5, no. 2, p. 7, 2016.
[80] X. Yuan *et al.*, "Adversarial examples: Attacks and defenses for deep learning," *IEEE TNNLS*, vol. 30, no. 9, pp. 2805–2824, 2019.
[81] M. Jagielski *et al.*, "Manipulating machine learning: Poisoning attacks and countermeasures for regression learning," in *S&P*. IEEE, 2018, pp. 19–35.
[82] H. M. Albunashee *et al.*, "A test bed for detecting false data injection attacks in systems with distributed energy resources," *IEEE JESTPE*, vol. 10, no. 1, pp. 1303–1315, 2022.
[83] F.-X. Standaert, "Introduction to side-channel attacks," in *Secure integrated circuits and systems*. Springer, 2010, pp. 27–42.
[84] D. Tychalas *et al.*, "Icsfuzz: Manipulating i/os and repurposing binary code to enable instrumented fuzzing in ics control applications," in *USENIX Security*, 2021, pp. 2847–2862.
[85] L. Garcia *et al.*, "Hey, my malware knows physics! attacking PLCs with physical model aware rootkit." in *NDSS*, 2017.
[86] C. Konstantinou *et al.*, "Taxonomy of firmware trojans in smart grid devices," in *PESGM*. IEEE, 2016, pp. 1–5.
[87] C. Carter *et al.*, "Cyber security primer for der vendors aggregators and grid operators," 11 2017.
[88] ICS-CERT, "Ics alert (ics-alert-14-281-01e), ongoing sophisticated malware campaign compromising ics," 2016.
[89] A. Cherepanov, "Win32/industroyer: A new threat for industrial control systems," *White paper, ESET (June 2017)*, 2017.
[90] S. Lyngaas, "Utah renewables company was hit by rare cyberattack in march," (Accessed: 2023).
[91] L. Jacqueline, "Apt33 targets aerospace and energy sectors and has ties to destructive malware," 2017.
[92] S. Soltan *et al.*, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," in *USENIX Security*, 2018, pp. 15–32.
[93] Cedric Carter, and others, "Cyber security primer for der vendors, aggregators, and grid operators," Sandia National Laboratories, Tech. Rep., 2017.
[94] J. Hunker and C. Probst, "Insiders and insider threats - an overview of definitions and mitigation techniques," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 2, pp. 4–27, 2011.
[95] J. Zhang, L. Guo, and J. Ye, "Cyber-attack detection for photovoltaic farms based on power-electronics-enabled harmonic state space modeling," *IEEE TSG*, pp. 1–1, 2021.
[96] M. Liu *et al.*, "False data injection attacks and the distributed countermeasure in dc microgrids," *IEEE TCNS*, vol. 9, no. 4, pp. 1962–1974.
[97] Y. Liu *et al.*, "Real-time pricing response attack in smart grid," *IET Generation, Transmission & Distribution*, 2022.
[98] R. McAllister *et al.*, "New approaches to distributed pv interconnection: Implementation considerations for addressing emerging issues," 2019.
[99] T. J. Foxon, G. P. Hammond, and P. J. Pearson, "Developing transition pathways for a low carbon electricity system in the uk," *Technological Forecasting and Social Change*, vol. 77, no. 8, pp. 1203–1213, 2010.
[100] P. Rogaway, "Authenticated-encryption with associated-data," in *CCS*, 2002, pp. 98–107.
[101] I. T. U. (ITU), "X.509 : Information technology," Accessed: 2023, [Online]. Available: https://www.itu.int/rec/T-REC-X.509.
[102] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.
[103] EPRI, "Epri security architecture for the distributed energy resources integration network," Accessed: 2023, [Online].
[104] K. Y. Yap *et al.*, "Blockchain technology for distributed generation: A review of current development, challenges and future prospect," *RSER*, vol. 175, p. 113170, 2023.
[105] A. Yildizbasi, "Blockchain and renewable energy: Integration challenges in circular economy era," *Renewable Energy*, vol. 176, pp. 183–197, 2021.
[106] S.-V. Oprea *et al.*, "Two novel blockchain-based market settlement mechanisms embedded into smart contracts for securely trading renewable energy," *IEEE Access*, vol. 8, pp. 212 548–212 556, 2020.
[107] X. Luo, K. Xue, J. Xu, Q. Sun, and Y. Zhang, "Blockchain based secure data aggregation and distributed power dispatching for microgrids," *IEEE TSG*, vol. 12, no. 6, pp. 5268–5279, 2021.
[108] L. Wang *et al.*, "Two-way dynamic pricing mechanism of hydrogen filling stations in electric-hydrogen coupling system enhanced by blockchain," *Energy*, vol. 239, p. 122194, 2022.
[109] I. Onunkwo *et al.*, "Cybersecurity assessments on emulated der communication networks," 2019.
[110] J.-H. Cho *et al.*, "Toward proactive, adaptive defense: A survey on moving target defense," *IEEE COMST*, vol. 22, no. 1, pp. 709–745.
[111] R. E. Cox *et al.*, "Artificial diversity and defense security (addsec)," 5.

[112] P. Garcia-Teodoro *et al.*, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *computers & security*, vol. 28, no. 1-2, pp. 18–28, 2009.
[113] F. M. Tabrizi and K. Pattabiraman, "A model-based intrusion detection system for smart meters," in *HASE*. IEEE, 2014, pp. 17–24.
[114] X. Liu *et al.*, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE TSG*, vol. 6, no. 5, pp. 2435–2443, 2015.
[115] A. P. Kuruvila *et al.*, "Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids," *International Journal of Electrical Power & Energy Systems*, vol. 132, p. 107150, 2021.
[116] I. Zografopoulos *et al.*, "Time series-based detection and impact analysis of firmware attacks in microgrids," *Energy Reports*, vol. 8, pp. 11 221–11 234, 2022.
[117] H. Li *et al.*, "Designing snort rules to detect abnormal dnp3 network data," in *ICCAIS*. IEEE, 2015, pp. 343–348.
[118] T. H. Morris *et al.*, "Deterministic intrusion detection rules for modbus protocols," in *HICSS*. IEEE, 2013, pp. 1773–1781.
[119] A. Singh, "Distributed intrusion detection system for modbus protocol," 2020.
[120] B. Kang *et al.*, "Towards a stateful analysis framework for smart grid network intrusion detection," in *ICS-CSR*, 2016, pp. 124–131.
[121] C. Sun *et al.*, "Cyber attack and defense for smart inverters in a distribution system," in *CIGRE Study Committee D2 Colloquium*, 2019.
[122] C. B. Jones *et al.*, "Unsupervised online anomaly detection to identify cyber-attacks on internet connected photovoltaic system inverters," in *PECI*. IEEE, 2021, pp. 1–7.
[123] Y. Zhang *et al.*, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE TSG*, vol. 2, no. 4, pp. 796–808, 2011.
[124] R. Mitchell and R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE TSG*, vol. 4, no. 3, pp. 1254–1263, 2013.
[125] J. Hong and C.-C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE TSG*, vol. 10, no. 1, pp. 271–281.
[126] Y. Yang *et al.*, "Multidimensional intrusion detection system for iec 61850-based scada networks," *IEEE TPD*, vol. 32, no. 2, pp. 1068–1078, 2016.
[127] Y. Kwon *et al.*, "A behavior-based intrusion detection technique for smart grid infrastructure," in *PowerTech*. IEEE, 2015, pp. 1–6.
[128] P. Jokar and V. C. Leung, "Intrusion detection and prevention for zigbee-based home area networks in smart grids," *IEEE TSG*, vol. 9, no. 3, pp. 1800–1811, 2016.
[129] J. Kim *et al.*, "Identification of intraday false data injection attack on der dispatch signals," in *SmartGridComm*. IEEE, 2022, pp. 40–46.
[130] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "Detection of false data injection cyber-attacks in dc microgrids based on recurrent neural networks," *IEEE JESTPE*, vol. 9, no. 5, pp. 5294–5310, 2020.
[131] L. Guo, J. Ye, and B. Yang, "Cyberattack detection for electric vehicles using physics-guided machine learning," *IEEE TTE*, vol. 7, no. 3, pp. 2010–2022, 2020.
[132] L. Guo, J. Zhang, J. Ye, S. J. Coshatt, and W. Song, "Data-driven cyber-attack detection for pv farms via time-frequency domain features," *IEEE TSG*, vol. 13, no. 2, pp. 1582–1597, 2021.
[133] Q. Li *et al.*, "Adaptive hierarchical cyber attack detection and localization in active distribution systems," *IEEE TSG*, vol. 13, no. 3, pp. 2369–2380, 2022.
[134] F. Li *et al.*, "Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network," *IEEE TPE*, vol. 36, no. 3, pp. 2495–2498, 2020.
[135] Q. Li *et al.*, "Data-driven cyber-attack detection for photovoltaic systems: A transfer learning approach," in *APEC*. IEEE, 2022, pp. 1926–1930.
[136] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in dc microgrids," *IEEE TSG*, vol. 10, no. 4, pp. 3585–3595, 2018.
[137] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE TPE*, vol. 34, no. 8, pp. 8162–8174, 2018.
[138] L.-Y. Lu, H. J. Liu, H. Zhu, and C.-C. Chu, "Intrusion detection in distributed frequency control of isolated microgrids," *IEEE TSG*, vol. 10, no. 6, pp. 6502–6515, 2019.
[139] A. J. Gallo *et al.*, "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3800–3815, 2020.
[140] S. Tan, P. Xie, J. M. Guerrero, and J. C. Vasquez, "False data injection cyber-attacks detection for multiple dc microgrid clusters," *Applied Energy*, vol. 310, p. 118425, 2022.
[141] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE TII*, vol. 13, no. 5, pp. 2693–2703, 2017.
[142] I. Zografopoulos *et al.*, "Detection of malicious attacks in autonomous cyber-physical inverter-based microgrids," *IEEE TII*, vol. 18, no. 9, pp. 5815–5826, 2022.
[143] Y. Li, P. Zhang, L. Zhang, and B. Wang, "Active synchronous detection of deception attacks in microgrid control systems," *IEEE TSG*, vol. 8, no. 1, pp. 373–375, 2017.
[144] T. Huang *et al.*, "Detection of cyber attacks in renewable-rich microgrids using dynamic watermarking," in *PESGM*. IEEE, pp. 1–5.
[145] M. Liu *et al.*, "Converter-based moving target defense against deception attacks in dc microgrids," *IEEE TSG*, vol. 13, no. 5, pp. 3984–3996.
[146] Y. Li *et al.*, "Sdn-enabled cyber-physical security in networked microgrids," *IEEE TSE*, vol. 10, no. 3, pp. 1613–1622, 2018.
[147] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, "A fdi attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE TSG*, vol. 12, no. 3, pp. 1929–1938, 2020.
[148] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient networked ac microgrids under unbounded cyber attacks," *IEEE TSG*, vol. 11, no. 5, pp. 3785–3794, 2020.
[149] Y. Jiang *et al.*, "A high-order differentiator based distributed secondary control for dc microgrids against false data injection attacks," *IEEE TSG*, vol. 13, no. 5, pp. 4035–4045, 2021.
[150] M. Shi *et al.*, "Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded ac microgrids," *IEEE TSG*, vol. 12, no. 3, pp. 1953–1963, 2021.
[151] S. Zuo, T. Altun, F. L. Lewis, and A. Davoudi, "Distributed resilient secondary control of dc microgrids against unbounded attacks," *IEEE TSG*, vol. 11, no. 5, pp. 3850–3859, 2020.
[152] M. R. Habibi *et al.*, "Decentralized coordinated cyberattack detection and mitigation strategy in dc microgrids based on artificial neural networks," *IEEE JESTPE*, vol. 9, no. 4, pp. 4629–4638, 2021.
[153] S. Hu *et al.*, "Resilient load frequency control of islanded ac microgrids under concurrent false data injection and denial-of-service attacks," *IEEE TSG*, vol. 14, no. 1, pp. 690–700, 2022.
[154] A. Cecilia *et al.*, "On addressing the security and stability issues due to false data injection attacks in dc microgrids—an adaptive observer approach," *IEEE TPE*, vol. 37, no. 3, pp. 2801–2814, 2021.
[155] ——, "Detection and mitigation of false data in cooperative dc microgrids with unknown constant power loads," *IEEE TPE*, vol. 36, no. 8, pp. 9565–9577, 2021.
[156] M. S. Sadabadi *et al.*, "Distributed control of parallel dc–dc converters under fdi attacks on actuators," *IEEE TIE*, vol. 69, no. 10, pp. 10 478–10 488, 2021.
[157] S. Zhao *et al.*, "Dual-triggered adaptive torque control strategy for variable-speed wind turbine against denial-of-service attacks," *IEEE TSG*, 2022.
[158] Y. Li *et al.*, "Distributed aperiodic control of multibus dc microgrids with dos-attack resilience," *IEEE TSG*, vol. 13, no. 6, pp. 4815–4827.
[159] A. Saad *et al.*, "On the implementation of iot-based digital twin for networked microgrids resiliency against cyber attacks," *IEEE TSG*, vol. 11, no. 6, pp. 5138–5150, 2020.
[160] S. Zhao *et al.*, "Adaptive resilient control for variable-speed wind turbines against false data injection attacks," *IEEE TSE*, vol. 13, no. 2, pp. 971–985, 2022.
[161] Z. Jin *et al.*, "Distributed data recovery against false data injection attacks in dc microgrids," in *SmartGridComm*. IEEE, pp. 265–270.
[162] Q. Zhou *et al.*, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE TSG*, vol. 11, no. 5, pp. 3690–3701, 2020.
[163] W. Zhang *et al.*, "Resilient economic control for distributed microgrids under false data injection attacks," *IEEE TSG*, vol. 12, no. 5, pp. 4435–4446, 2021.
[164] N. Yassaie, M. Hallajiyan, I. Sharifi, and H. Talebi, "Resilient control of multi-microgrids against false data injection attack," *ISA transactions*, vol. 110, pp. 238–246, 2021.
[165] S. Abhinav *et al.*, "Synchrony in networked microgrids under attacks," *IEEE TSG*, vol. 9, no. 6, pp. 6731–6741, 2017.
[166] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, "Detection and mitigation of data manipulation attacks in ac microgrids," *IEEE TSG*, vol. 11, no. 3, pp. 2588–2603, 2019.
[167] R. Lu, J. Wang, and Z. Wang, "Distributed observer-based finite-time control of ac microgrid under attack," *IEEE TSG*, vol. 12, no. 1, pp. 157–168, 2020.
[168] B. Huang *et al.*, "A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks," *IEEE TII*, vol. 18, no. 2, pp. 880–890, 2021.
[169] Z. Cheng and M.-Y. Chow, "Resilient collaborative distributed energy management system framework for cyber-physical dc microgrids," *IEEE TSG*, vol. 11, no. 6, pp. 4637–4649, 2020.
[170] J. Zhang *et al.*, "Mitigating concurrent false data injection attacks in cooperative dc microgrids," *IEEE TPE*, vol. 36, no. 8, pp. 9637–9647.
[171] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Resilient operation of heterogeneous sources in cooperative dc microgrids," *IEEE TPE*, vol. 35, no. 12, pp. 12 601–12 605, 2020.
[172] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE TSG*, vol. 9, no. 5, pp. 4702–4711, 2017.
[173] W. Yao, Y. Wang, Y. Xu, and C. Deng, "Cyber-resilient control of an islanded microgrid under latency attacks and random dos attacks," *IEEE TII*, 2022.
[174] S. Liu, Z. Hu, X. Wang, and L. Wu, "Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks," *IEEE TII*, vol. 15, no. 7, pp. 4066–4075, 2018.
[175] S. Hu, P. Yuan, D. Yue, C. Dou, Z. Cheng, and Y. Zhang, "Attack-resilient event-triggered controller design of dc microgrids under dos attacks," *IEEE TCAS-I*, vol. 67, no. 2, pp. 699–710, 2019.
[176] Z. Chu, S. Lakshminarayana, B. Chaudhuri, and F. Teng, "Mitigating load-altering attacks against power grids using cyber-resilient economic dispatch," *IEEE TSG*, 2022.
[177] Z. Lian *et al.*, "Distributed resilient optimal current sharing control for an islanded dc microgrid under dos attacks," *IEEE TSG*, vol. 12, no. 5, pp. 4494–4505, 2021.
[178] C. Deng *et al.*, "Distributed resilient secondary control for dc microgrids against heterogeneous communication delays and dos attacks," *IEEE TIE*, vol. 69, no. 11, pp. 11 560–11 568, 2021.
[179] L. M. Castiglione *et al.*, "Ha-grid: Security aware hazard analysis for smart grids," in *SmartGridComm*, 2022, pp. 446–452.
[180] L. Zhang *et al.*, "Named data networking," *ACM SIGCOMM CCR*, vol. 44, no. 3, pp. 66–73, 2014.

Mengxiang Liu received the B.Sc. degree in Automation from Tongji University, Shanghai, in 2017 and the Ph.D. degree in Cyberspace Security from Zhejiang University, Hangzhou, in 2022. He is currently a Research Associate with the Department of Electrical and Electronic Engineering, Imperial College London, London, UK. His research interests include cyber resiliency, DER-based smart grid, active defense.



Zhenyong Zhang (Member, IEEE) received his Ph.D. degree from Zhejiang University, Hangzhou, China, in 2020, and bachelor degree from Central South University, Changsha, China, in 2015. He was a visiting scholar in Singapore University of Technology and Design, Singapore, from 2018 to 2019. Currently, he is a professor in the college of Computer Science and Technology, Guizhou University, Guiyang, China. His research interests include cyber-physical system security, applied cryptography and machine learning security.

Pudong Ge (Student Member, IEEE) received the M.Sc degree in electrical engineering from Southeast University, Nanjing, China, in 2019, and he is currently a Ph.D Student at the Department of Electrical and Electronic Engineering, Imperial College London. His current research focuses on the distributed control of cyber-physical coupling microgrids, and cyber-resilient energy system operation and control.

Ruilong Deng (Senior Member, IEEE) received the B.Sc. and Ph.D. degrees both in Control Science and Engineering from Zhejiang University, Hangzhou, Zhejiang, China, in 2009 and 2014, respectively. He was a Research Fellow with Nanyang Technological University, Singapore, from 2014 to 2015; an AITF Postdoctoral Fellow with the University of Alberta, Edmonton, AB, Canada, from 2015 to 2018; and an Assistant Professor with Nanyang Technological University, from 2018 to 2019. Currently, he is a Professor with the College of Control Science and Engineering, Zhejiang University, where he is also affiliated with the School of Cyber Science and Technology. His research interests include cyber security, smart grid, and communication networks. Dr. Deng serves/served as an Associate Editor for IEEE Transactions on Smart Grid, IEEE Power Engineering Letters, IEEE/CAA Journal of Automatica Sinica, and IEEE/KICS Journal of Communications and Networks, and a Guest Editor for IEEE Transactions on Emerging Topics in Computing, IEEE Transactions on Cloud Computing, and IET Cyber-Physical Systems: Theory & Applications. He also serves/served as a Symposium Chair for IEEE SmartGridComm'19 and IEEE GLOBECOM'21.

Mingyang Sun (Senior Member, IEEE) received the Ph.D. degree from the Department of Electrical and Electronic Engineering, Imperial College London, London, U.K., in 2017. From 2017 to 2019, he was a Research Associate and a DSI Affiliate Fellow with Imperial College London. He is currently a Professor of Control Science and Engineering under the Hundred Talents Program at Zhejiang University, Hangzhou, China. Also, he is an Honorary Lecturer at Imperial College London. His research interests include AI in energy systems and cyber-physical energy system security and control.

Jiming Chen (Fellow, IEEE) received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2005. He is currently a Professor with the Department of Control Science and Engineering, Zhejiang University, where he is also the Vice Dean of the Faculty of Information Technology. His research interests include network optimization and control, cyber security, and internet of things (IoT) and big data for industry. He was a recipient of the 7th IEEE ComSoc Asia/Pacific Outstanding Paper Award, the JSPS Invitation Fellowship, and the IEEE ComSoc AP Outstanding Young Researcher Award. He serves as the general Co-Chairs for the IEEE RTCSA'19, the IEEE Datacom'19, and the IEEE PST'20. He is an IEEE VTS Distinguished Lecturer. He serves/served as an Associate Editor for IEEE Transactions on Industrial Informatics, IEEE Transactions on Network Science and Engineering, IEEE Transactions on Control of Network Systems, and IEEE Transactions on Industrial Electronics.

Fei Teng (Senior Member, IEEE) received the B.Eng. degree in electrical engineering from Beihang University, China, in 2009, and the M.Sc. and Ph.D. degrees in electrical engineering from Imperial College London, U.K., in 2010 and 2015, respectively, where he is currently a Senior Lecturer with the Department of Electrical and Electronic Engineering. His research focuses on the power system operation with high penetration of inverterbased resources (IBRs) and the cyber-resilient and privacy-preserving cyber-physical power grid. He serves/served as an Associate Editor for IEEE Transactions on Power System, Control Engineering Practice, IEEE Open Access Journal of Power and Energy, and IEEE Power Engineering Letters and a Guest Editor for IEEE Transactions on Cloud Computing, IEEE Transactions on Industry Applications, Applied Energy, and IET Renewable Power Generation.