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

Mengxiang Liu, Zhenyong Zhang, Pudong Ge, Ruilong Deng, *Senior Member, IEEE*, Mingyang Sun, *Senior Member, IEEE*, Peng Cheng, *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 summarized. A holistic 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**

ACRONYMS

AGC Automatic Generation Control.
AIC Availability, Integrity, Confidentiality.
AMI Advanced Metering Infrastructure.
ANN Artificial Neural Network.
AVC Automatic Voltage Control.

CNN Convolutional Neural Network.
CRE Cyber-resiliency Enhancement.
CVF Cooperative Vulnerability Factor.

DER Distributed Energy Resource.
DERMS DER Management System.
DMS Distribution Management System.
DMZ Demilitarized Zone.
DoS Denial-of-Service.

EIoT Energy Internet-of-Thing.
ESS Energy Storage System.
EV Electric Vehicle.

FDEMS Facilities DER Energy Management System.
FDI False Data Injection.

HIDS Host-based Intrusion Detection System.
HILP High Impact and Low Probability.
HOD High-order Differentiator.
HPC Hardware Performance Counter.
HSS Harmonic-State-Space.

ICS Industrial Control System.
ICT Information Communications Technology.
IDS Intrusion Detection System.
IED Intelligent Electronic Device.
IMS Intrusion Mitigation System.
ISO Independent System Operator.
IT Information Technology.

LDAP Lightweight Directory Access Protocol.
LFC Load Frequency Control.
LSTM Long Short-Term Memory.

ML Machine Learning.
MTD Moving Target Defense.

NDN Named Data Networking.
NIDS Network-based Intrusion Detection System.

OT Operation Technology.

P2P Peer-to-Peer.
PIDS Physics-based Intrusion Detection System.
PKI Public Key Infrastructure.
PLL Phase Lock Loop.
PV Photovalitic.

RBAC Role-based Access Control.
REP Retail Energy Provider.
RTO Regional Transmission Organization.

SCADA Supervisory Control and Data Acquisition.
SCED Security-Constrained Economic Dispatch.
SCOPF Security-Constrained Optimal Power Flow.
SDN Software-defined network.
SMO Sliding Mode Observe.
STL Signal Temporal Logic.
SVR Support Vector Regression.

TLS Transport Layer Security.

UBB Uniformly Ultimately Bounded.
UIO Unknown Input Observer.

VLAN Virtual Local Area Network.
VPP Virtual Power Plant.

WMSR Weighted Mean Subsequence Reduced.
WT Wind Turbine.

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, P. Cheng, and J. Chen are with the College of Control Science and Engineering, Zhejiang University, Hangzhou, China.

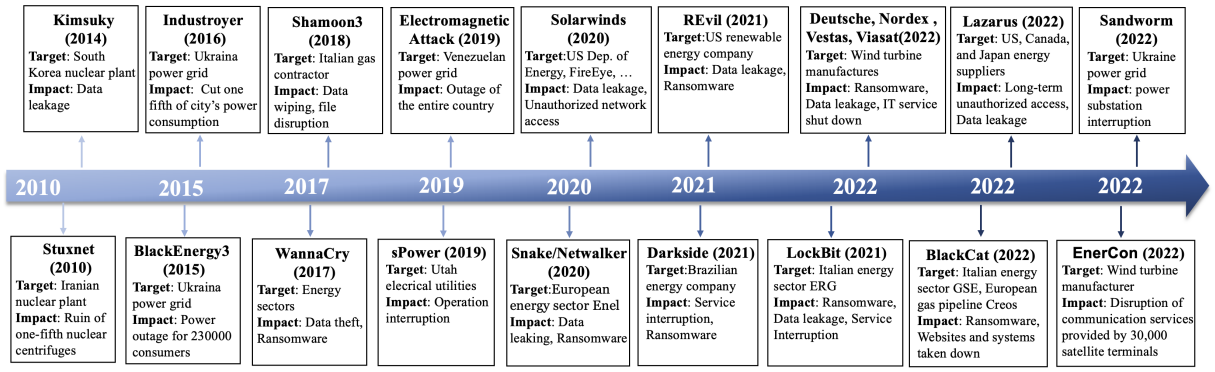


Fig. 1: Timeline of the cyberattacks targeting at power systems from 2010 to 2022 with an emphasis on the recent three years.

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. DERs including PVs, WTs, 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 Stdandard 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 ICT like 5G, EIoT, and SDN technologies. These technologies, together with smart inverter devices, offer numerous benefits for the transition. However, they also pose various cyber threats [5]–[7].

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 HILP cyberattack events [12]–[15]. Enhancing the cyber-resiliency is particularly crucial to pave the way towards the large-scale deployment of DERs.

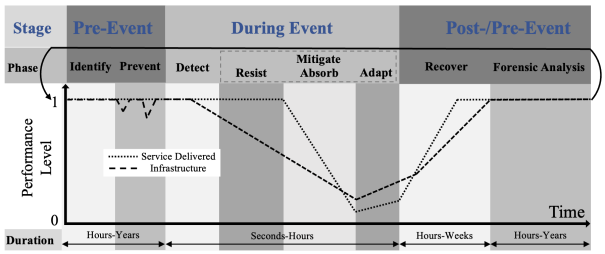
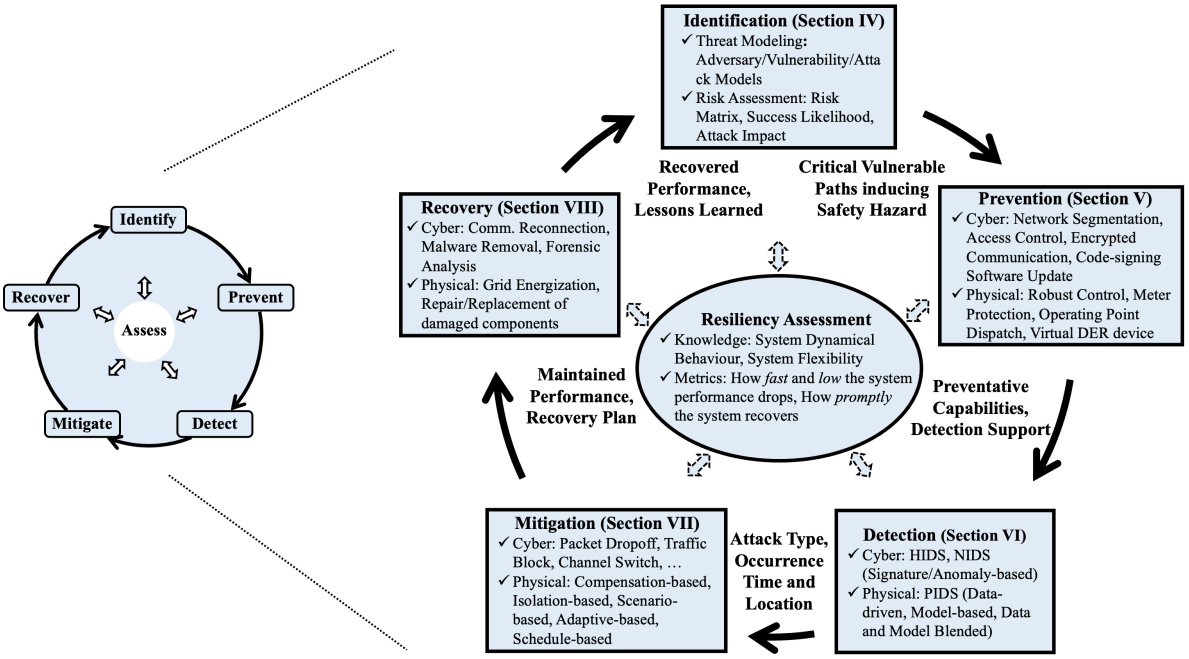


Fig. 2: Cyber-resiliency stages and phases.

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 AIC while also providing power generation, transmission, and distribution functionalities. In the pre-event stage (hours 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 AIC 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



(a) Conceptual demonstration (b) Detailed illustration

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

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 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 general risk assessment matrix is established to rank the attack scenarios' risk levels considering both their occurrence likelihoods and consequence severity.

3) The state-of-the-art developments of prevention, detection, and mitigation technologies are comprehensively reviewed, systematically classified according to their work principles, and rigorously summarized to highlight their implementation guidelines and respective cons and pros. Besides, the necessity and focus of the cyber-recovery under HILP cyberattack events are clarified for the first time.

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 Surveys

There exist several surveys regarding the cybersecurity of DER-based smart grid [10], [17], [20], [40]–[42]. Zografopou-

TABLE I: Comparison between this survey and existing ones

Resilience Enhancement Phases		[40]	[20]	[17]	[10]	[41]	[42]	[43]	This Survey
Threat Identification	Adversary Model	F	N	N	N	N	N	N	F
	Vulnerability Coverage	M	P	P	M	M	M	F	F
	Risk Assessment	P	F	P	F	F	P	P	F
Defense-in-Depth Strategies	Prevention	M	N	M	N	M	P	N	F
	Detection	P	N	N	M	M	M	M	F
	Mitigation	P	P	P	P	P	M	P	F
	Recovery	N	N	N	N	N	N	N	F

F: Fully Covered, M: Mostly Covered, P: Partially Covered, N: Not Covered

los *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 both in the grid-connected and standalone modes. Vosughi *et al.* [17] discussed 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. Nguyen *et al.* [43] presented a comprehensive review of the system structure and vulnerabilities of typical inverter-based power system with DER integration, nature of several types of cyberattacks, state-of-the-art defense strategies including detection and mitigation techniques.

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, [10], [20], [43] did not discuss prevention technologies, and [20] and [17] did not consider IDSs. All literature includes IMSs but only [42] briefly classified and summarized them. Moreover, recovery scheduling is not covered in any of the literature. To fill these gaps as indicated by TABLE I, 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.

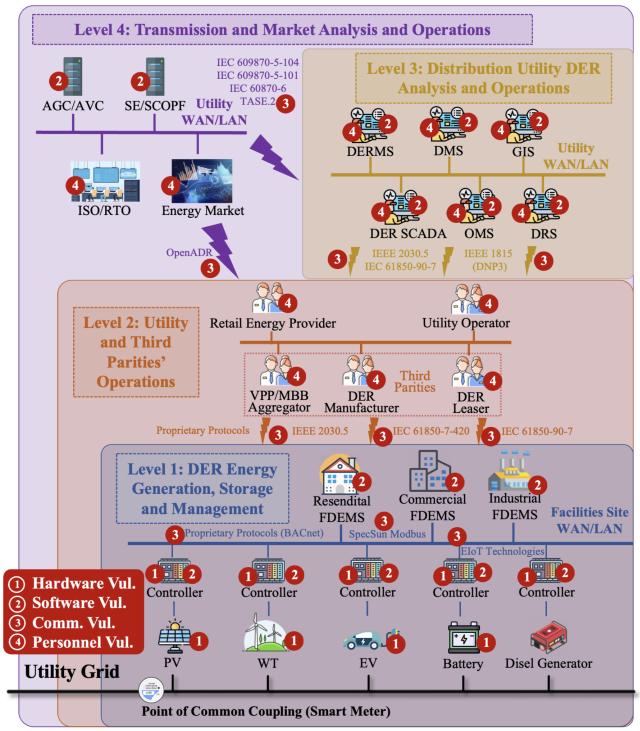


Fig. 4: Hierarchical framework of DER-based smart grid and and the associated vulnerabilities.

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: 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 [44]), proprietary protocols (BACnet [45]), and emerging IoT technologies (ZigBee, WiFi, and 5G) are widely adopted to enable the real-time interaction among DER units and FDEMSs, and thus provide DER's autonomous response capabilities

and ancillary services [17]. Level 2 includes the actors beyond local sites like utility operators, REPs, as well as third parities like VPPs [46], microgrids [3], DER manufacturers, and DER leasers. Communication standards including IEEE 2030.5 ((Smart Energy Profile 2.0)) [47], IEC 61850-90-7 and IEC 61850-7-420 [48], 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 [49].

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, DERMS, and DMS. 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, IEC 61850-90-7, IEEE 1815 (DNP3) [50], 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 AGC, AVC, SCED, SCOPF, and ISO and RTO balancing authorities should be reconsidered given the uncertainty, variability, and market participation of geographically dispersed DER units. The AMI plays a fundamental role for two-way data exchange between remote DER units and the transmission control center [5], [51], [52].

Compared with the existing DER System architectures [16], [41], the uniqueness of the proposed hierarchical framework is reflected through the following aspects: i) The four-level framework comprising the DER device, DER aggregator, distribution utility, and transmission operation is proposed for the first time. ii) Actors, functionalities, and communication protocols in each layer are specified to clarify potential vulnerabilities and possible consequences; iii) Newly emerging DER-related entities like VPP and MBB aggregators and the P2P energy trading mode are incorporated.

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 [53], NIST electric utility guidelines [54], and European Union Agency for Cybersecurity threat landscape [55], 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 [56], and can be classified as 1) White-box with *full* knowledge; 2) Gray-box with *partial* knowledge; 3) Black-box with *zero* knowledge [57]. The adversary access includes physical access through serial/USB/Ethernet interfaces [58], remote access through phishing emails [59], and close proximity access through wireless compromise [60]. 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 [61]–[64]. 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 DERs makes it particularly impressionable to this kind of vulnerability and should be paid enough attention. According to the development trend of DER-based smart grid, the typical software vulnerabilities are summarized as 1) Insufficient test and validation on firmware and user code [65], 2) Insecure supply chain [66], [67], and 3) Zero-day vulnerabilities [68].

The communication vulnerability is the most well-known type and can come from communication protocols, network component/participator, network services, etc. According to the literature and technical reports, the communication protocol related vulnerabilities include 1) Insufficient security mechanisms in SunSpec Modbus [44], [69], 2) Scalability gaps of IEEE 2030.5's security features [69], 3) Security flaws of IEC 62351 [70], [71], 4) Inadequate security consideration in DNP3-SA and DNP3Sec [72], [73], and 5) Security flaws of transmission communication protocols [72]. 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 segmentation between DER systems [7], 2) Unknown trust level among multiple stakeholders [74], 3) Multiple access points from external networks [75], [76], and 4) Indirect and delayed feedback from third parties. Based on the communication infrastructure, numerous network 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 [77], 2) Security challenges of P2P energy trading [78]–[80], and 3) Vulnerable ML based applications [81], [82]. 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 the involved number is large. According to Fig. 4, the hardware vulnerability is mainly from DERs and field controllers, and the personnel vulnerability is among the operation and management staff in upper levels.

TABLE II: Attack Techniques Summary and Classification

Types	Attack Techniques	Description and Direct Impacts
Initial access acquisition	Network service exploitation	Use directory traversal, cross-site scripting, SQL injection to illegally access DER network [83].
	Wireless compromise	Exploit wireless protocol vulnerability to obtain illegal remote access to DER network [84].
	Supply-chain compromise	Gain control systems' access by manipulation of products before receipt by end consumers [67].
	Zero-day attack	Exploit zero-day vulnerability to get illegal access to the DER system [85].
	Social engineering attack	Use personal information or subterfuge to learn a legal user's password [86].
Information discovery	Insider attack	Employ persons within the organization that have access to critical information [87].
	Side-channel attack	Analyze time/power/electromagnetic information to infer critical information [88].
	Eavesdropping attack	Take screenshot of HMI and workstation or listen to communicated confidential [89].
Execution and Implication	Malicious firmware installation	Install malicious firmware into inverter/converter to execute illegal actions [90].
	Trojan attack	A malware disguising itself as legitimate code or software and gain legitimate users' privileges [91].
	Hall spoofing attack	Mislead hall sensor's measurement by placing a camouflaged attack tool near the inverter [64].
	PLL attack	Inject false pulse voltage signal to mislead PLL reading to DER controller [92].
	Control logic modification	Modify control logic of DER controller to manipulate outputs or trigger overflow bug [93].
	Brute force attack	Repetitively change I/O point values to impact the process function associated with that point [94].
	DoS attack	Deliberately overload a DER stakeholder and prevent it from performing normal functions [95].
	Adversary-in-the-middle/FDI attack	Modify and inject data streams exchanged in the DER network [76]
	Replay attack	Replace current transmission data with previously recorded data in the DER network [96]
	EIoT Botnet attack	Manipulate a large volume of high-watt IoT loads to induce frequency instability [97].
	P2P energy market attack	Submission of fake contract, modification of transaction, etc. to gain illegal profits [78]–[80].
	ML adversarial attack	Create adversarial examples with imperceptible perturbation to mislead ML outputs [81].

Moreover, software and communication vulnerabilities spread throughout all the levels.

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. Inspired by the MITRE ATT&CK Matrix for ICSs, the attack techniques are divided into initial access acquisition, information discovery, and execution and implication according to the adversary's intrusion and execution phases [98]. As shown in TABLE II, specific description and impacts of attack techniques are provided. According to the statistical data published on HACKMAGEDDON[1], the top attack techniques adopted by the cyber attack events against ICSs during 2022 are depicted in Fig. 5 to provide a high-level understanding of different attack techniques' risks and occurrence. In particular, the malware from supply-chain compromise, malicious firmware installation, and Trojan attacks is the most common adopted attack technique, followed by known/zero-day vulnerabilities, targeted attacks, and account takeover attacks. One take home message from these attack statistics is that the observed cyber-attack events are becoming more and more mature, implying the adversary's increasing intelligence. Moreover, the human-involved threats like insiders and social engineering attacks are gaining increasing attentions. Note that TABLE II merely lists the attack techniques against smart grid, and it does not include all attack techniques highlighted in Fig. 5.

Following the perspective of AIC, the potential attack impacts on the DER-based smart grid are divided into security- and privacy-related. 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 [99], [100], 3) Poor power quality [4], [101], 4) Intentional islanding failure [4], 5) Increased power loss [4],

[1]https://www.hackmageddon.com/

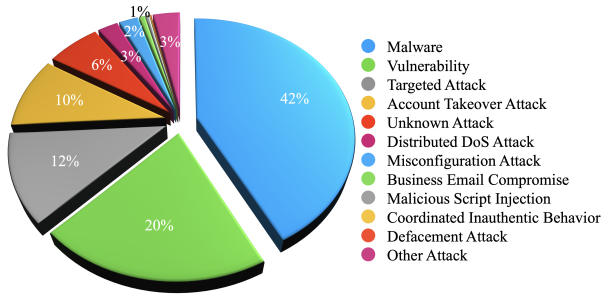


Fig. 5: Statistics of attack techniques adopted by the cyberattack events against ICSs during 2022.

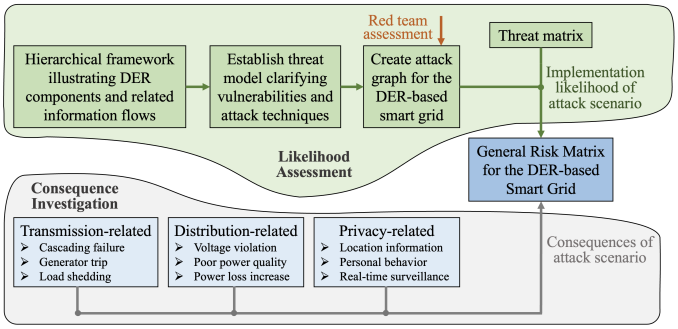


Fig. 6: Generation scheme of the risk matrix for the DER-based smart grid.

6) Aggravated equipment wear, and 7) Voltage violation [21], [22]. In the transmission level, the security-related impact consists 1) Energy price/load manipulation [102], 2) Generator trip and load shedding [21], and 3) Cascading failure and large-scale blackout [97]. 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]. 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].

C. Risk Assessment Matrix

After identifying the potential vulnerabilities and associated attack techniques in the DER-based smart grid, it would be helpful to assess the risk of each attack scenario using these adversarial resources. A general risk matrix is proposed to accomplish this objective, which basically takes the inputs of attack implementation likelihoods and attack consequences as illustrated in Fig. 6.

In the likelihood assessment phase, based on the previously established threat model, the red team will first conduct multiple assessment activities comprising visits to manufacturing facilities, development and testing labs, and assessments of fielded DER systems. The team mainly assesses the cybersecurity posture of state-of-the-art DER equipment using authorized, adversary-based assessment techniques, often in close collaboration with the vendors. Then, attack graphs will be created to show the steps an adversary must take to move from a system/network access point to a consequence or objective. A demonstrative example that illustrates the deployment of malicious firmware against EVs [21] is shown in Fig. 7. The first step in this attack graph is to craft the payload that will be delivered to the deployed EV supply equipment. Afterwards, the adversary will gain access to the business network using either a malicious insider or using remote attack techniques, followed by pivoting through the business network until getting access to the firmware repository. Different methods will be chosen to insert malicious firmware depending on if the update requires code signing. Finally, by triggering shutdown signals following specific strategics, expected consequences can be induced.

The attack graphs will then be utilized to estimate the skill and time it would take adversaries to execute different attack scenarios. Combined with the general threat matrix, which enables government entities and intelligence organizations to categorize threat into a common vocabulary [103], the attack implementation likelihoods are qualitatively classified as Almost Certain, Likely, Possible, Unlikely, and Rare according to the adversary's knowledge, funding, and time. Note that other threat attributes like intents and targets and more granular classification levels can be incorporated into the risk matrix, and here the simplified version is shown only for demonstrative purpose.

In the consequence investigation phase, the consequences of attack scenarios on smart grid are observed from the experimental results obtained using high-fidelity smart grid simulator like OPAL-RT and Typhoon HIL [104] and privacy inference simulation results [105]. According to the impact scale and severity on smart grid, the attack consequences are qualitatively classified as Severe, Major, Moderate, Minor, and Insignificant. For example, the privacy leak normally not affects the power system operation and thus is deemed as insignificant, while the large-scale transmission level cascading failure and blackout will severely affect the power supply and hence is assumed as severe. Finally, the generated risk matrix is presented in Fig. 8 with the columns being the consequence levels and rows being the likelihood levels. As indicated by the colors of entries, the qualitatively classified risk levels include

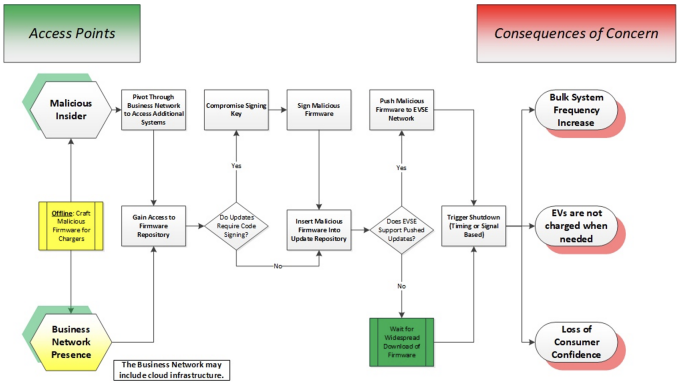


Fig. 7: Attack graph illustrating the malicious firmware deployment against EVs [21].

Extreme, High, Medium, and Low, and play a vital role in determining what kinds of defense technologies and methods should be adopted. A thorough risk assessment process against EV supply equipment has been conducted coordinately by multiple National Laboratories of United State of America and is detailed in [21]. Some insights can be synthesised from this practice as follows.

- The attack with almost certain probability cannot currently be achieved as no public scripts and tools that can indeed impact the power system exist.
- The skilled actor/team or nation state can cause insignificant and minor impact on the 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 [99], [100].
- 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], [106]. 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 [107].

Attack Implementation Likelihoods	Attack Consequences					
	Insignificant No Observable Impact like Privacy Leak	**Minor** Small Distribution Impact like Poor Power Quality	**Moderate** Large Distribution Impact like Feeder Voltage Voliation	**Major** Small Transmission Impact like Energy Price Manipulation	**Severe** Large Transmission Impact like Cascading Failure and Blackout
Almost Certain Attacker: Script Kiddie Funding: No Time: Days	**Medium**	**High**	**High**	**Extreme**	**Extreme**
Likely Attacker: Skilled Actor Funding: Little Time: Weeks	**Medium**	**Medium**	**High**	**Extreme**	**Extreme**
Possible Attacker: Moderately-Skilled Team Funding: Some Time: Months	**Low**	**Medium**	**Medium**	**High**	**Extreme**
Unlikely Attacker: Skilled Team Funding: Substantial Time: Years	**Low**	**Low**	**Medium**	**High**	**High**
Rare Attacker: Nation State Funding: Substantial Time: Years	**Low**	**Low**	**Low**	**Medium**	**High**

Fig. 8: Risk matrix reference for the DER-based smart grid.

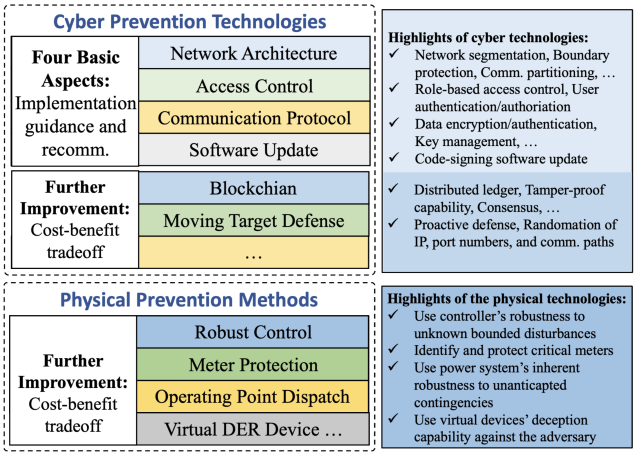


Fig. 9: Summary of Prevention Technologies and Methods

IV. Defense-in-Depth Strategies: Prevention

Preventive technologies are divided into cyber- and physics-based according to their application scenarios. Cyber-based technologies are collected from the IT domain like encryption and authentication, and they can be deployed at host, protocol, system, and network levels to *prevent the adversary from intruding into the system network*. Physics-based methods aim to exploit the robustness of control and operation algorithms or deploy extra protection and virtualized devices in the OT environment to *prevent the attack from inducing hazardous consequences on the system operation*. For example, by modeling the attack as an unknown and bounded disturbance, the famous robust control tool can be adopted to ensure the proper functionality of the controller [108].

A. Cyber Prevention Technologies

Various cyber preventative technologies can be found from the IT domain, and here we mainly summarize the results of the SunSpec/Sandia DER Cybersecurity Workgroup [109], whose primary objective is to advance cybersecurity in the DER community by creating consensus around DER cybersecurity standards, guidelines, and best practice documents. As shown in Fig. 9, the subsequent parts will be expanded following the four basic aspects including network architectures guidelines, access control requirements, communication requirements, and patching requirements as well as two further improving technologies comprising blockchain and MTD.

Network Architecture Guidelines: A practical set of cybersecurity requirements pertaining to the network components supporting DER communications has been provided to minimize the likelihood, duration, or impact of a successful cyberattack [110]. This set of requirements does not make any assumption to the communication protocols, particular functional standards, or certain ownership/business models in terms of their effectiveness in cybersecurity. Rather, it aims to provide a holistic view of the interconnected DER-based smart grid, and it suggests how they can be protected from cyberattacks. Four aspects of requirements and their implementation guidelines are detailed.

- (*Resource Criticality Level*) Each DER or supporting system participating in DER communications must be categorized into one of three distinct criticality levels—high impact, medium impact, or low impact as shown in Fig. 10. The resource's criticality level is determined by the impact of any misuse of that resource to grid reliability, public safety, finances, and privacy. Different headends are allocated to different critical groups to accomplish separate control paths.
- (*Network Segmentation*) Resources with different criticality levels must be located in different security zones. As shown in Fig. 10, the central management systems will typically consist of multiple zones containing headends of various criticality levels and a zone containing the core managing system, which will have the highest criticality of all the zones. Moreover, communications between two different security zones must be routed through the security gateways with access controls like a firewall. In particular, communications between a system/resource in the high-impact zone and a system/resources in the low-impact zone must be routed through a DMZ[2] like the managing system in Fig. 10 communicating with low-impact residential DERs).
- (*Boundary Protection*) Access controls in security gateways should be configured to deny a connection request from a lower-security zone to a higher security zone by default. In Fig. 10, traffic should be blocked from the Internet to the DMZs and from the DMZs to the managing system, and should only be allowed in the opposite direction. Security gateways at the boundary of high-impact zones and interfacing with external networks must be monitored on a 24/7 basis to detect security events negatively impacting the operation of systems or resources in the security zone.
- (*Communications Partitioning*) DER communications to/from must be physically or logically partitioned from other types of communication. In Fig. 10, a shared switch uses VLANs to segregate the corporate VLAN from the DB VLAN. Communications required for the administration of network infrastructure must be physically or logically partitioned from other types of communication. The reference architecture in Fig. 10 shows a management VLAN for several switches and firewalls.

It is noted that the network security architecture addresses only a portion of the cybersecurity risks associated with DER integration. To protect DER and the connected grid adequately, a more comprehensive cybersecurity standard including communication security, access control, patch management, etc, as introduced in the following subsections must be developed and implemented.

Role-based Access Control: With multiple entities needing differing levels of access to DER data and control modes, there is a need to establish robust access control security policies and technologies. Access control restricts access to resource func-

[2]The DMZ is a separate network zone where traffic entering and exiting the DMZ is controlled by the relevant security gateways, but an additional level of control/ traffic filtering is exerted by the devices inside the DMZ.

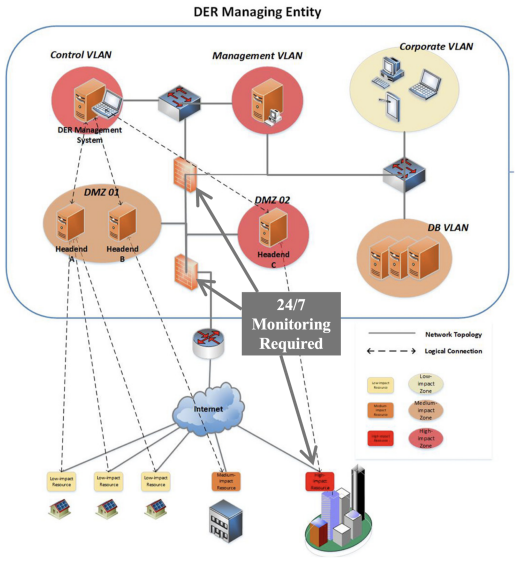


Fig. 10: Reference network segmentation for DER-based smart grid [110].

tionality unless the user is authorized, preventing unauthorized users from changing power system control settings. RBAC is a natural choice for DER communication environments because there are clear roles for subjects based their company of employment, job position, and responsibilities [25]. Establishing an RBAC mechanism for the DER-based smart grid requires detailed information on the hardware and software. Based on the IEC 62351-8 RBAC implementation, these requirements are covered below.

- (*User Authentication*) Users must provide one or more proofs of identity to ensure they are who they claim to be. Some options for user authentication includes Challenge-Response, Kerberos [111], and Digital Signatures.
- (*User Authorization*) Users are permitted to access data, services, resources, or objects granted by the security policy. Two types of authorization mechanisms are structured query language [112] and LDAP [113].

When selecting these mechanisms for the DER access control implementation, the administrative overhead and ease of implementing administration delegation are important. For instance, it is common to use Kerberos for authentication and LDAP for authorization. The implementation of RBAC can be achieved through push and pull models. The push model requires the subject to fetch the token from the identity provider before sending it to the object. Whereas the pull model requires the object to fetch the token from the identity provider. Depending on the type of operational environment and object, the use of either the push or pull models may be appropriate. Access tokens are used to transport roles, whose distribution is provided by an LDAP-enabled repository/server/device. When communicating with the repository, LDAP v3 with TLS should be used with unique user identifier, authentication information, and access token entries.

It would be absolutely preferred to establish protocol-agnostic access control requirements. However, due to the unique characteristics of each of the IEEE 1547-2018 protocols, there are specific considerations needed when building an access control system for each of these protocols. This is primarily because IEEE 2030.5 client/server implementations naturally make the IEEE 2030.5 server the access control object; while DNP3 and Modbus implementations work best with the DER acting as the object. Interested readers can refer to [25] to see potential DER RBAC implementation cases for IEEE 2030.5, IEEE 1815, and SunSpec Modbus.

Communication Requirements: In IEEE 1547-2018 interconnection and interoperability standard [4], standardized information exchange interfaces between associated DER entities like IEEE 2030.5, IEEE 1815, SunSpec Modbus, and IEC 61850-7-420 have been identified to improve the interoperability. To ensure the security of information that flows over public or private networks, DER communications and their corresponding security measures must be standardized, to prevent malicious control or misuse of DERs. For instance, some protocols lack authentication and authorization, allowing unauthorized control of DER equipment by individuals with network access and knowledge of the DER's address. Moreover, implementing cryptographic methods in protocols lacking inherent security features may require a bump-in-the-wire approach, which does not provide application layer security and can introduce latency. Therefore, to ensure the security of data-in-transit for DER equipment, it is crucial to address the security requirements to: i) assure the data authenticity flowing over the network, 2) verify the device identity, 3) confirm that encryption keys are securely managed, and 4) provide access control.

Based on a thorough analysis of the security strengths and weakness of communication technologies, a unified set of security recommendations for DER application protocols has been proposed [24]:

- (*Data Encryption and Data Authentication for Bulk Traffic*) Adopt TLS v1.3 with authenticated encryption using additional data such as Advanced Encryption Standard Galois Counter Mode [114].
- (*Device Authentication*) Use X.509v3 digital certificates with mutual client/server authentication [115].
- (*Key Management*) Align with TLS v1.3, adopt Elliptic Curve for ephemeral symmetric key exchange and Rivest–Shamir–Adlema generated node authentication signatures [116].

Conflicts still exist between these security requirements and the processing limitations of DER equipment. For example, DER equipment without cryptographic hardware relies heavily on standard software libraries to support encryption, authentication, and hashing operations executed on the CPU, which may induce unacceptable latency for communication-based control of devices supplying grid-support functions. Nevertheless, some preliminary case studies indicate that the proper implementation of these security features will not impact DER-based grid control systems (well below the IEEE 1547-2018 limits for DER latency) but improved the security posture of the devices and networked system [117]. The change in roundtrip time due to addition of encryption is on the order of *milliseconds*. In order to meet the stringent latency

and messaging throughput requirements while retaining the benefits of public key cryptography, less-online/more-offline signatures model was proposed to allow the verification to be divided into online/offline phases such that online verification does not perform any expensive operations [118]. It is promising to further alleviate the computation burden when integrated with the rapidly developing quantum computation technologies.

Code-Signing Software Patching: Since the DER equipment is expected to operate in the field for 25 or more years, there will undoubtedly be newly discovered vulnerabilities in software packages or custom code that is running on the equipment during this period. In those situations, it is necessary to improve the security level of software supply chain using code signing or equivalent mechanisms, which identify the source of the patch and confirm the integrity of the data. Based on many standards and guides for patch management in the literature and an active community researching solutions for ICSs [119] and EIoT device's firmware updates, the application of these requirements and recommendations within DER environments has been fully investigated. The primary technology used for secure patching in the DER environment is the code-signing scheme [26], which uses 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. Basically, three main actors are included in the code-signing scheme:

- The *developer* of the code or data who submits the code to the signer.
- The *signer* entity that is responsible for managing the signing keys. The signer securely generates the private/public key pair and then provides the public key to a certification authority through a certificate signing request to tie their identity to the public key.
- The *verifier* that is responsible for validating the signed code signature.

In particular, PKI code-signing with digital signatures is recommended in that it has better security features in terms of integrity, authentication, and non-repudiation compared to other cryptographic primitives like hashes, message authentication code, and hash-based message authentication code. A reference implementation of the PKI-based coding signing for the DER environments is provided in [26]. Nevertheless, there are still multiple threats to the code-signed firmware. For example, it is possible that software developed by an organization has malicious firmware embedded in the signed version. This could be perpetrated by an *insider* or through compromise of the firmware development environment, as was the case in the well-known SolarWinds attack. Awareness of this type of risk and application of appropriate mitigation methods are critical for all DER vendors. A list of suggested firmware update requirements for DER equipment, product suppliers, integrators, aggregators, and owners is also provided to adress this issue [26].

Blockchain: Blockchain is a digital data structure comprised of a shared, decentralised, and distributed database or ledger with a continuous log of chronological transactions. Each block contains transaction data, a timestamp, and a hash point which is linked to the previous block. The hash values are crucial to its tamper-proof capability as the compromise of the block content requires to alter all subsequent blocks, which is practically impossible [120]. Additionally, blockchain provides a consensus mechanism to prevent one node from continuously adding blocks, making it more difficult to alter blocks with a sufficient rapid rate. The blockchain technology can be introduced to establish a trustworthy network for multiple stakeholders comprising DER owners, DER aggregators, and utility operator without requiring a trusted third party. 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 [121], smart contract [122], energy management [123], competitive pricing [124], and secure control [125]–[127] using blockchain has been widely investigated. Currently, the investment costs and technological infrastructure are the greatest obstacles in integrating the blockchain into the DER-based smart grid.

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 [117]. The goals of MTD include [128]: i) Increase uncertainty and complexity for any adversary of the system, ii) Decrease the opportunities for the attacker to identify vulnerable system components, and iii) Introduce higher cost in launching attacks or scans. The MTD technologies can be thought of as additional layers of defense to help protect a system from an adversary attempting to gain an understanding of a system in the early stages of an attack. The application of a MTD tool that leverages the SDN to randomize application port numbers, IP addresses, and communication paths in a ICS communication network was verified in [129].

B. Physical Prevention Methods

This subsection shows three representative physical preventative methods comprising robust control, meter protection and operating point dispatch, and virtual DER devices, that have been widely discussed in the literature.

Robust Control: The robust control based preventive method treats injected bounded biases as unknown uncertainties and the robust controller is designed to ensure that the tracking error under attacks could be bounded, which typically requires no other investments besides inducing some extra computation burdens. 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 [130]. Once several key resiliency-related indices are designed to be large enough, the system states can converge to expect values with arbitrary small errors.

Meter Protection and Operating Point Dispatch: By strategically protecting a set of meters like smart meters from being compromised by the adversary, the attack-induced impact region can be bounded. From this perspective, Deng *et al.* focused on designing the least-budget defense strategy to protect

power systems against FDI attacks, which was then extended to investigate choosing which meters to be protected and determining how much defense budget to be deployed on each of these meters [131]. By exploiting power system's inherent N-k robustness against unanticipated contingencies, the system operating point can be simultaneously dispatched to tolerate certain attacks. A cybersecure corrective dispatch scheme was proposed in [132] to secure the flow levels, i.e., prevent the physical overloads, against certain data attacks. Normally, the meter protection is scheduled in the system planning stage, based on which the operating point is dispatched accordingly to attain the optimal cost-efficiency.

Virtualized DER Devices: As one of the typical deception technologies, the virtualized DER device can offer multiple cybersecurity defense functionalities to capture adversary tactics and techniques to expand our understanding of the threat landscape and DER vulnerabilities. In particular, the virtualized DER device will be configured to provide protection by directing adversary's focus away from critical assets and detection by sending alerts when the adversary interacts with the artificial equipment. Virtual DER devices are usually deployed in the forms of i) Honeypots–internet-connected applicants to capture adversary actions, and ii) Canaries–virtualized device alongside real DER units. A Laboratory Directed Research and Development project was conducted to design high-fidelity DER honeypot/canary prototypes [27], providing informative references for further development. Besides virtual DER devices, the methodology of creating virtual IEDs named as DecIED that imitates the device characteristics and communication models of IEC 61850-compliant IEDs was proposed, which can realize k-anonymous smokescreen by virtually showing $k-1$ indistinguishable decoy devices [133].

Due to the space limitation, we merely list several representative prevention technologies, while not covering all potential prevention technologies such as quantum communication [134].

Lessons Learned: As indicated by Fig. 9, the cyber prevention technologies play a leading role in the prevention phase, and basic implementation guidance and recommendations have been detailed to pave the way towards a resilient DER-based smart gird. The further prevention improvement resulted from MTD and physical prevention methods is usually not mandatory and depends on the vulnerability level and security demand of the specific scenario. For example, in the SCADA centre, the advanced MTD technology is recommended to ensure its functionality under extreme cyberattack events [135]. In general, the cost-benefit tradeoff of adopting these advanced technologies and methods should be clearly analyzed to guarantee the cost-efficiency.

Moreover, one critical perception is that there is no combination of cyber and physical prevention technologies/methods that can ensure 100% security, i.e., all potential adversaries are prevented. Intuitive explanations to this kind of dilemma include zero-day vulnerabilities and insiders. Besides, the prevention capability improvement of physical methods can induce unacceptable control and performance degradation. It is not recommended to reach an extreme high security level while not considering the security budget or seriously degrading the system performance. Instead, the integration of a timely and effective monitoring and response framework has received much recognition recently and is much more recommended, which will be covered in the following sections.

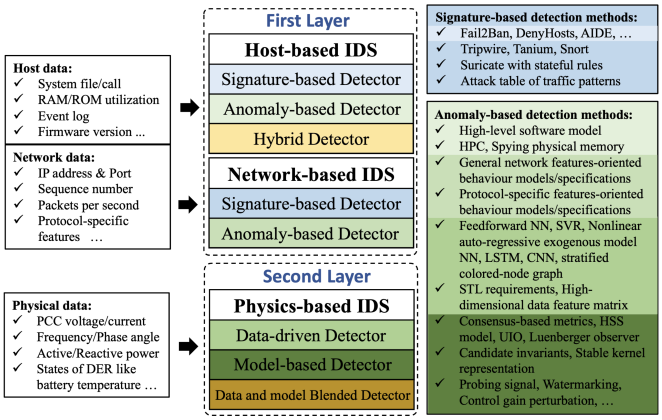


Fig. 11: Summary and classification of IDSs.

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. 11, IDSs can be classified into three classes according to the origination of data: i) The 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, and firmware version. ii) The NIDS aims to monitor and analyze network related attributes such as IP addresses, service ports, traffic volumes, and protocol attributes. iii) The PIDS is to detect the anomaly of physical measurements like PCC voltages/currents, frequency, and active/reactive power. Depending on the type of analysis carried out, each IDS can be further classified as signature-based or anomaly-based [136]. 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, 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, PIDSs are further classified as data-driven, model-based, or data-model blended. The data-driven PIDS captures data-oriented characteristics of normal behaviours like ML models, while the model-based PIDS extract model-oriented properties of normal operations such as observers. The data-model blended PIDS uses both data and model knowledge to feature the normal behaviours.

A. Host-based IDS

The HIDS is usually deployed at critical and vulnerable hosts like servers and workstations and IED 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 AMI used in modern power systems, the security of smart meter has attracted great attention. Tabrizi *et al.* [137] 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 [138]. To identify malicious instructions and counterfeit firmware within the inverter controller, Zografopoulos *et al.* [139], [140] developed an anomaly-based HIDS utilizing custom-built HPCs and time series classifiers.

B. Network-based IDS

The NIDS is usually deployed at strategic points in the 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], [141], [142]. The collaboration among multiple NIDSs placed at field device and control center levels are investigated in [143], 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 [144]. 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 [145].

The anomaly-based NIDSs are further classified into three 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 netural network algorithm with online update capability [29], [146]. A distributed NIDS framework is developed for AMI, where intelligent modules are deployed at three layers to perceive malicious network traffic collaboratively [147]. 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 [148]. *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 [149]. A finite state machine model for network communication was defined to detect the GOOSE-based poisoning attacks [150]. 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 [151]. For ZigBee-based HAN, a normal behaviour model is established according to SEP 2.0 and IEEE 802.15.4 standards [152]. The third group concerns both general network and protocol-specific features. Using both statistical analysis of traditional network features and specification-based metrics of GOOSE and MMS, Kwon *et al.* proposed a novel behavior-based NIDS [153]. By monitoring the traffic data characteristics of transport, operation, and content levels in SCADA network, Ren *et al.* developed a edge-based multi-level anomaly detection framework [154].

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 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 SVR model is adopted to predict the system margin of the time of interest [155]. By employing the Isolation Forest algorithm, which is trained on features determined from local current measurements, Saber *et al.* proposed an anomaly-based scheme for detecting false-tripping attacks against line current differential relays, in the form of relay attacks, replay attacks, general false-data-injection attacks, and time-synchronization attacks [156]. 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 neural network for the real-time estimation of voltages and currents in DC microgrids [157]. 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 LSTM and CNN classifiers are able to distinguish between normal conditions, component failures, and FDI attacks in EVs and PV farms [158], [159]. Besides attack detection and identification, the raw waveform data can also be used in the location of attack sources [160], [161]. To reduce the amount of required training data, transfer learning was incorporated into the cyberattack detection framework [162]. The specifications and data features

extracted from physical data are also used to construct PIDSs, which is training-free compared with the ML methods. STL requirements, which are formalisms to monitor the output voltages and currents of DC microgrids against predefined specifications, were employed for anomaly detection [163].

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. Based on on-the-fly power system dynamics simulation results, command authentication schemes were proposed to evaluate the legitimacy and validity of remote control commands near the edge of smart grid infrastructure (e.g., in substations), which can enhance the attack detection capability compared to the traditional schemes solely using steady-state information [164], [165]. Due to the widespread adoption of consensus based secondary control in microgrids, various consensus-oriented detection metrics such as CVF [166] 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 [167]. To further improve the detection accuracy, the physical dynamics obtained from Kirchhoff circuit laws were incorporated into the design of attack detectors. The HSS model was developed to predict current measurements of PV farms, which were then used for integrity verification [99]. By synthesising a Luenberger observer and a bank of UIOs, a distributed monitoring scheme was established for each DER unit to verify the integrity of neighbors' data [168]. Considering the robustness against unknown disturbances and parameter variations, a multi-objective optimization problem was formulated to design the generation scheme of detection residuals [169]. 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 [170]. 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 [171].

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 [172]. Further, by adding watermarks to communicated data between DERs, the replay attack could be detected by testing the existence of statistical properties of watermarks [173], [174]. 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 [175].

The data and model blended PIDS has also attracted increasing attention recently due to its benefits in performance enhancement and data requirement reduction. By incorporating physical dynamics into the data recovery algorithm, Xu *et al.* proposed a blending data-driven and physics-based approach to improve the detection accuracy while reduce the operational cost resulted from MTD [176]. Based on the combination of prior knowledge of physics and system metrics, a physics-informed context-based anomaly detection method was proposed to counter the stealthy attacks against AGC [177]. To alleviate the data reliance on system topology and line parameters, a physically-inspired data-driven model was proposed for electricity theft detection with merely smart meter data comprising power consumption and voltage magnitudes [178]. Given that cyberattacks can be strategically counterfeited to replicate grid faults, a physics-informed spline learning approach-based anomaly diagnosis mechanism was designed in [179], which not only provides compelling accuracy with limited data, but also reduces the training and computational resources significantly. To achieve timely and accurate attack localization and also output explainable detection results, Peng *et al.* incorporated the nodal admittance matrix and physical property of power grid into the graph convolutional network [180].

The reviewed literature is summarized in TABLEs III and IV with particular attentions on applied scenarios, adopted tools/methods, and evaluation metrics. The cons and pros of each type of IDS as well as research trends and gaps are highlighted in learned lessons. Moreover, from a high-level perspective, a set of evaluation metrics regarding the IDS is refined from the summary: 1) Performance-related metrics: detected attack types, detection accuracy, and detection latency; 2) Cost-related metrics: memory and computation overhead, hardware investment, and control and operation performance sacrifice. The design of IDS should at least consider one type of performance- and cost-related metrics and address the tradeoff issue between them. However, it is indeed difficult to give a comparative study regarding all detection and mitgation methods in the literature due to the lack of a set of benchmark testbeds or datasets. On one hand, it is unrealistic to establish a high-fidelity smart grid testbed without considering space and budget limitation. On the other hand, the sensitivity information contained in the real-world power system data hinders its disclosure for research purpose. Many efforts are still required from academic and industry as well as governments to address this critical issue and pave the way towards the cyber-resilient smart grid under highly penetrated DERs.

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

TABLE III: Summary of IDSs

Type	Lit.	Scenario	Tools/Methods	Evaluation Metrics	Lessons Learned
Host-based IDSs					
Signature-	[28]	Upper hosts	Tripwire, Tanium, OSSEC, etc.	Attack: Known attacks; Detection latency: Timely	1) Current research status regarding HIDSs mainly focuses on the upper hosts and smart meters. 2) As the most basic components that interfaces renewable sources with power grid, the energy conversion devices like converters have not obtained enough attention. 3) It is challenging to attain comparable performance using strictly limited resources on these conversion devices.
Anomaly-	[137]	Smart meter	Abstract model based verification of core system calls	Attack: Known and unknown; Coverage: 100% known and 69.9% unknown; Latency: 10s; Memory overhead: 4.15%	
	[139], [140]	Inverter controller	Custom-built HPCs and time series analysis	Attack: Firmware modification; Accuracy: 97.22%	
Hybrid	[138]	Smart meter	Collaborative signature and anomaly combined detection	Attack: Known and unknown; Accuracy: >80%; Memory overhead: 0.8%	
Network-based IDSs					
Signature-	[29]	DER comm. network	Snort with default rules	Attack: 5 scenarios; Detection coverage: 60%; Memory overhead: 31.25%	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 planning 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 NIDS's detection performance 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.
	[143]	DER comm. network	Cross-level Snort-based detection with tailored rules	Attack: DoS attack; Accuracy: 100%; Latency: ≤500ms	
	[144]	DER comm. network	Suricate with stateful rules	Attack: FDI attack; Accuracy: 100%; Latency: N.A.	
	[145]	DER comm. network	Attack table, Temporal failure propagation graph	Attack: DoS and FDI attacks; Accuracy: 100%; Latency: N.A.	
Anomaly-	[29], [146]	DER comm. network	Adaptive resonance theory artificial neural network	Attack: 5 scenarios; Detection coverage: 80%; Memory overhead: 45%; Train/test latency: 33ms/14ms	
	[147], [148]	AMI	Support vector machine, Artificial immune systems, State machines	Attack: FDI, DoS, and eavesdropping attacks; Accuracy: 99.33%; Latency: N.A.	
	[149]	GOOSE and SV network	Collaborative and distributed intrusion detection with normal behaviour model	Attack: FDI attack; Accuracy: N.A.; Latency: 2ms; Memory overhead: 2%	
	[150]	GOOSE network	A finite state machine model	Attack: FDI attack; Accuracy: 95%; Latency: 0.06ms;	
	[151]	IEC 61850 network	Access control, Protocol whitelisting, Multiparameter-based detection	Attack: DoS and FDI attacks; Accuracy: 100%; Latency: <0.3ms	
	[152]	ZigBee network	Normal behaviour model established referring to SEP 2.0 and IEEE 802.15.4 standards	Attack: FDI, replay, and DoS attacks; Accuracy: ≥92.5%; Latency: N.A.	
	[153]	GOOSE and MMS network	Statistical traffic features and specification-based metrics	Attack: 27 scenarios; Accuracy: 98.89%; Latency: N.A.	
	[154]	SCADA network	Traffic data characteristics of transport, operation, and content levels	Attack: 12 scenarios; Accuracy: 100%; Latency: 423ms	
Physics-based IDSs					
Data-	[155]	EMS	Kernel SVR	Attack: FDI attack; Accuracy: 100%; Latency: 2 hours	1) 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. But the PIDS works as the last detection layer by observing the induced physical impacts when the HIDS and PIDS are both invalidated. 2) The data-driven and model-based PIDSs have their own cons and pros. 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 widespread application. 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.
	[157]	Microgrid	Auto-regressive exogenous model neural network	Attack: FDI attack; Accuracy: 100%; Latency: N.A.	
	[158], [159]	EV and PV farm	LSTM and CNN classifiers, Physics-guided features	Attack: Replay and FDI attacks; Accuracy: ≥98.44%; Latency: N.A.	
	[160]–[162]	PV farm	LSTM and CNN classifiers, Transfer learning	Attack: FDI attack; Accuracy: ≥95.23%; Latency: N.A.	
	[163]	Microgrid	STL requirements based specifications	Attack: DoS and FDI attacks; Accuracy: 100%; Latency: <1s	
Model-	[164], [165]	Substation	On-the-fly power system dynamics simulation	Attack: FDI attack; Accuracy: 83%; Latency: 859ms	
	[166]	Microgrid	Consensus-oriented metric CVF	Attack: FDI attack; Accuracy: 100%; Latency: <1s	
	[167]	Microgrid	Dual variable-related detection metrics	Attack: FDI attack; Accuracy: 100%; Latency: <1s	
	[168], [169]	Microgrid	Luenberger observer, UIO	Attack: FDI attack; Accuracy: 100%; Latency: <1s	
	[170]	Microgrid	Candidate invariant	Attack: FDI attack; Accuracy: 100%; Latency: <1s	
	[171]	Microgrid	Stable kernel representation	Attack: FDI attack; Accuracy: 100%; Latency: <1s	
	[173]–[175]	Microgrid	Watermarking, Primary control gain perturbation	Attack: FDI and replay attacks; Accuracy: 100%; Latency: <1s; Proactive cost: Neglectable	

TABLE IV: Summary of IDSs (Continue of TABLE III)

Physics-based IDSs					
#	**Lit.**	**Scenarios**	**Tools/Methods**	**Evaluation Metrics**	**Lessons Learned**
Data and model blended	[176]	State estimation	LSTM, Event-triggered MTD	Attack: FDI attack; Accuracy: 98.16%; Operation cost: 0.5%	3) The data and physics blended PIDS has became a prevailing topics as it is particularly suitable for the DER-based smart grid with massive measurement data and well-known physical dynamics. 4) The proactive detection strategy by perturbing system parameters can enhance the detection capability against powerful adversaries with acceptable sacrifice on either control or operation performance.
	[177]	AGC	CNN, LSTM, knowledge of physics	Attack: FDI atatck; Accuracy: 93.2%; Latency: N.A.	
	[178]	Energy theft	Linear regression, Power flow dynamics	Attack: FDI attack; Accuracy: 94%; Latency: N.A.	
	[179]	Grid-tied converter	Spline learning, Power electronics dynamics	Attack: FDI attack; Accuracy: 98.23%; Latency: 25ms	
	[180]	State estimation	Graph convolutional network	Attack: FDI attack; Accuracy: 99.25%; Latency: N.A.	

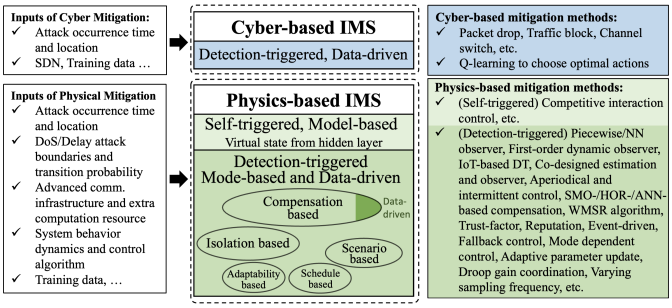


Fig. 12: Summary and classification of IMSs.

drop to exclude the malicious components from the remaining network; The physics-based IMS adopts local control capability 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 in the absence of inputs from IDS. As shown in Fig. 12, 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. In parallel with the detection- and self-triggered classification metrics, IMSs can be also classified as data-driven and model-based. All cyber-based IMSs are data-driven, and most physics-based IMSs are model-based with only a small portion of detection-triggered IMSs being data-driven as illustrated by Fig. 12.

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. When a DER unit is found subject to DoS attacks, it will enter the protective mode where only outgoing network traffic is permitted [31], [149]. In the worst case, if anomaly is detected twice while the compromised unit cannot be located, then all DER units will enter protective mode to gain time for the control center to attend to the aroused security issues. For the microgrid enabled by 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 [181]. To achieve the cost-benefit tradeoff, Jokar *et al.* presented a Q-learning based intrusion prevention system for the ZigBee-based home area network to automatically adjust the mitigation strategies facing a wide varieties of cyberattacks [152].

The cyber-side mitigation strategies are suitable for the pure IT system where the data availability is not the primary concern. However, when involving the closed-loop control functionalities that require real-time interaction with the physical plant, these cyber-side strategies can be too aggressive as the 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 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 [182]. To guarantee the tracking performance of variable-speed WTs when the rotor velocity measurement is unavailable under DoS attacks, Zhao *et al.* proposed a dual-triggered adaptive control strategy [183]. 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 [184]. Similar to the idea of hidden network layer, Saad *et al.* established a IoT-based DT by emulating the dynamics of cyber-physical networked

microgrids to help estimate the unavailable data induced by DoS attacks [185].

In terms of FDI attacks, the same idea also works by estimating/observing injected biases and healthy states. The estimation/observer can be accomplished using the corrupted signal together with some extra securely communicated data. Jiang *et al.* designed distributed SMO and HOD based resilient secondary controllers for DC microgrids to compensate for the adverse impact of bounded FDI attacks [186]. 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 [187]. To guarantee the UBB voltage regulation and proportional load sharing under *unbounded* FDI attacks, an adaptive observer is employed to estimate the aggregated term induced by attacks on the secondary control input [188]. In addition, an ANN based decentralized cyberattack mitigation framework was proposed to relief the reliance on model accuracy [189]. The incorporation of physical circuit dynamics can benefit 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 [190]. Based on the information (voltage varying slope) observed from attack impacts, a distributed estimator was designed as per explicit impact analysis results to obtain the injected bias [191]. To guarantee the tracking performance of variable-speed WTs 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 [192].

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 [193]. For the consensus-based economic dispatch and secondary frequency/voltage regulation in microgrids, Zhang and Yassaie *et al.* employed the *WMSR* algorithm to discard the the extreme values among the data received from neighbors [194], [195]. 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 [196]–[198]. 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 [199], [200]. 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 [201], [202]. 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 ESS and energy management system 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 [203]. To handle the excessive latency and damaged cyber connectivity under DoS attacks in islanded microgrids, an event-triggered network reconfiguration scheme was proposed [204]. 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 [205]. 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 [206]. 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 [207]. Moreover, the sampling scheme with time-varying frequency was proposed to restore the communication as soon as the DoS attack terminates [208], [209].

C. 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. The type of IMS relies on the construction of a compensation term,

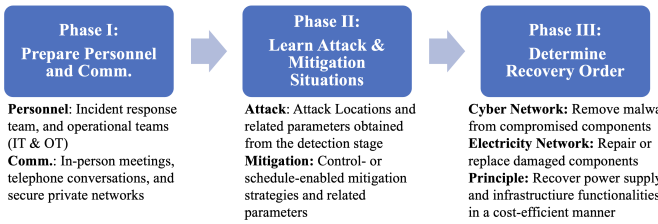


Fig. 13: Phases included in the general recovery plan under cyberattacks.

which can be just a variable with no physical meaning 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], [210]. 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 [211].

The reviewed literature is summarized in TABLE V with particular attentions on applied scenarios, adopted tools/methods, and evaluation metrics. The cons and pros of each type of IMS as well as research trends and gaps are highlighted in learned lessons. Moreover, from a high-level perspective, a set of evaluation metrics regarding the IMS is refined from the summary: 1) Performance-related metrics: mitigated attack types and mitigation effect; 2) Cost-related metrics: computation and communication overhead and hardware investment. It is recommended to appropriately balance the tradeoff between these metrics when designing IMSs. Due to the lack of benchmark testbeds, it is also difficult to comparatively study the performance of these IMSs.

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. To the best of the authors' knowledge, the recovery schedule problem under HILP cyberattack accidents has rarely been discussed in the literature.

According to NIST's guide for cybersecurity event recovery [212], the recovery schedule comprises Phase I: Prepare personnel and communication, Phase II: Learn attack and mitigation situations, and Phase III: Determine recovery the order as shown in Fig. 13. Phases I and II are more like preparation steps based on the information from the previous detection and mitigation steps, and Phase III is the core part that determines the recovery order of blackout areas, compromised cyber components, and damaged physical equipment to achieve the restoration of power supply and infrastructure functionalities. In particular, the power supply restoration is given the first priority and should be completed timely (hours) [12], where both cyber and physical recovery actions will be involved. 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 power supply, 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. Compared to the power supply restoration, the full restoration of infrastructure functionalities requires a much longer period (days/weeks). 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. The key challenge here is to schedule the recovery actions in multiple time scales to achieve power supply and infrastructure restoration in a cost-efficient manner considering resource constraints and performance requirements. 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.

In summary, TABLE VI is given to clarify the differences between the focused cyber-recovery and conventional black-start and physical-recovery. In particular, the black-start service aims to energize power grid without requiring external power supplies in the event of partial or total shutdown, and the generator providing this service is called as black-start capable generator like diesel generators. The feasibility of using DERs to provide a "bottom-up" black start approach has been investigated [213], which has potential advantages of reduced restoration time and more flexible recovery procedure compared with the conventional large thermal plants. These black-start capable DER units can also provide ancillary services like reactive power support to assist the voltage control during synchronization and grid reconnection [214].

The black-start capable units are adopted in both the physical- and cyber-recovery processes to restore the power supply service in the physical side. Besides that, the reestablish of communication network is also involved when the extreme event damages/compromises cyber components and induces network disconnection. The difference between physical- and cyber-recovery processes in restoring the power supply service lies in their focuses. The physical-recovery *mainly* focuses on the power grid energization in the *physical* side since natural disasters usually first damage physical power lines and

TABLE V: Summary of IMSs

Types	Lit.	Scenarios	Methods/Ideas	Evaluation Metrics	Lessons Learned
Cyber-based IMSs					
Detection-triggered, Data-driven	[31], [149]	DER comm.	Block network traffic	Attack: DoS and FDI attacks; Effect: Isolation; Extra cost: No	1) Cyber-side aggressive actions may affect physical functionalities. 2) Knowledge from the physical side can be integrated to improve the performance.
	[181]	Microgrid comm.	SDN enabled traffic block	Attack: FDI and replay attacks; Effect: Isolation; Extra cost: SDN	
	[152]	ZigBee HAN	Q-learning	Attack: FDI and replay attacks; Accuracy: 93.46%; Latency: Neglectable	
Physics-based IMSs					
Detection-triggered, Compensation-based	[182]	LFC	Piecewise observer based robust control	Attack: Resources constrained FDI and DoS attacks; Effect: H_∞ performance guarantee; Extra cost: No	**Comparisons between Detection- and Self-triggered IMSs:** 1) Majority of physics-based IMSs are detection-triggered, and only a small portion are self-triggered. 2) Although the self-triggered does not require the inputs from IDSs, which can avoid potential false positive alarms, two limitations also come along with this cons: i) A hidden secure network layer independent from the original control layer should run all the time, inducing extra computation and communication overheads; ii) The introduction of hidden layer can expose larger attack surfaces if not equipped with appropriate security strategies. The two limitations hinder the further investigation of self-triggered IMSs. **Comparisons of different Detection-triggered IMSs:** 3) After incorporating the inputs of IDSs, much more mitigation strategies like isolation- and scenario-base for the detection-triggered IMSs. The most common compensation-based strategy can work for both FDI and DoS attacks, and usually needs to integrate robust control, adaptive control, and NN methods to estimate the injected bias/healthy data. The isolation-based IMS can be regarded as the simplest strategy, but it only works under FDI attacks and is subject to the number of attacks. The scenario- and adaptability-based IMSs are usually used to counter DoS attacks, where the former is customized for attack scenarios (less conservativeness, limited attack scenarios) and the latter adapts automatically without requiring specific attack information (more conservativeness, unlimited attack scenarios). The schedule-based IMS can mitigate both FDI and DoS attacks by utilizing extra flexible resources. 4) It is not hard to observe that the performance of each IMS can be guaranteed only when the adversary's capability is restricted like bounded FDI attacks. In particular, the compensation-/isolation-/scenario-/adaptability-based IMSs try to enhance the tolerance of control algorithms against cyberattacks and can work immediately once perceiving anomaly. When the adversary's capability exceeds control algorithms' tolerance, the schedule-based IMS is expected to alleviate the severe consequence by adopting available flexible resources. Hence, the cooperative design of control-enabled and schedule-driven mitigation strategies can defend against a wider range of attacks. 5) The investigation of data-driven physics-based IMSs is rare, and most of them are model-based. This phenomenon is caused by the inherent difficulty of recovering control-acceptable healthy data from compromised data using purely data-driven methods, since it is difficult to train the model covering all attack forms.
	[183]	Variable-speed WT	NN observer, Dual-triggered control	Attack: Resources constrained DoS attack; Effect: Exponential convergence guarantee; Extra cost: No	
	[184]	Microgrid control	First-order dynamic observer	Attack: Resource constrained DoS attack; Effect: Exponential convergence; Extra cost: No	
	[185]	Microgrid control	IoT-based DT, Luenberger observer	Attack: DoS and FDI attacks; Latency: Timely; Extra cost: DT, Cloud service	
	[186]	Microgrid control	SMO and HOD	Attack: Bounded FDI attack; Effect: Lyapunov stable; Extra cost: No	
	[187]	Microgrid control	Robust output feedback control	Attack: Bounded FDI attacks; Effect: L_2-gain boundedness; Extra cost: No	
	[188]	Microgrid control	Adaptive observer	Attack: Bounded (unbounded) FDI attacks; Effect: UUB (Asymptotic) stability; Extra cost: No	
	[189]	Microgrid control	ANN, PI-based controller	Attack: FDI attack; Effect: Compensation error $\leq 0.02\%$; Latency: <0.15s; Extra cost: No	
	[190]	Microgrid control	Nonlinear adaptive observer	Attack: FDI attack; Effect: Input-to-state stability; Extra cost: No	
	[191]	Microgrid control	Impact-oriented compensation	Attack: Constant FDI attack; Latency: 2s; Extra cost: No	
	[192]	Variable-speed WT	Adaptive resilient control	Attack: Bounded FDI attack; Effect: UUB stability; Extra cost: No	
Detection-triggered, Isolation-based	[193]	Microgrid control	Aperiodically intermittent control	Attack: Quantitatively limited FDI attack; Effect: Asymptotically stability; Extra cost: No	
	[194], [195]	ED and Microgrid	WMSR algorithm	Attack: Quantitatively limited FDI attack; Effect: Optimal dispatch, Asymptotically stability; Extra cost: No	
	[196]–[198]	Microgrid control	Trust-factor based control	Attack: Quantitatively limited FDI attack; Effect: Asymptotically stability; Extra cost: No	
	[199], [200]	ED	Reputation-driven bad data replacement	Attack: Quantitatively limited FDI attack; Effect: Optimal dispatch; Extra cost: Multiple-hop communications	
	[201], [202]	Microgrid control	Event-driven bad data replacement	Attack: Quantitatively limited FDI attack; Effect: Successful mitigation: Extra cost: No	
Detection-triggered, Scenario-based	[203]	ESS management	Rule-based fallback control	Attack: DoS attack; Effect: Maintain ESSs' SOC within allowable limits; Extra cost: No	
	[204]	Microgrid control	Adaptive control, network reconfiguration	Attack: Resource constrained DoS attack; Effect: Stochastic stability; Extra cost: network configuration	
	[205]	Microgrid control	Mode dependent control	Attack: Resource constrained Markovian DoS attack; Effect: Stochastic stability; Extra cost: No	
Detection-triggered, Adaptability-based	[33]	Microgrid control	Adaptive control	Attack: Resource constrained DoS attack; Effect: Secure consensus; Extra cost: No	
	[206]	Microgrid control	Adaptive event-triggered control	Attack: Resource constrained DoS attack; Effect: Global asymptotically stability; Extra cost: No	
Detection-triggered, Schedule-based	[207]	LFC	DER droop schedule	Attack: IoT Botnet attack; Effect: Exponentially stability; Extra cost: Operational cost	
	[208], [209]	Microgrid control	Sampling frequency adjustment	Attack: Resource constrained DoS attack; Effect: Asymptotically stability; Extra cost: More communication overhead	
Self-triggered, Compensation-based	[32], [210], [211]	Microgrid control	Competitive interaction control	Attack: Bouded and unbounded FDI attacks; Effect: Input-to-state and UUB stability; Extra cost: SDN based secure hidden communication layer	

TABLE VI: Comparsions between black-start, physical-recovery, and cyber-recovery.

Tasks	Black-Start	Phyical-Recovery under Natural Disasters	Cyber-Recovery under Attacks
Power Supply Service	*Physical*: Energize power grid without requiring external power supplies in the event of partial or total shutdown	*Cyber*: Reestablish comm. network utilizing mobile comm. vehicles or other resources (*Occasional*) *Physical*: Energize power grid utilizing mobile generation vehicles and black-start generators (*Main*)	*Cyber*: Reestablish comm. network utilizing mobile comm. vehicles or other resources (*Main*) *Physical*: Energize power grid utilizing mobile generation vehicles or black-start generators (*Main*)
Infrastructure Function	N.A.	*Cyber and Physical*: Repair or replace damaged components	*Cyber*: Remove cyber malware *Physical*: Repair or replace damaged components

TABLE VII: Pairwise Comparisons of the Capability between Defense-in-Depth Strategies

Defense-in-Depth Strategies		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Prevention	Network Segmentation (1)		N	N	N	N	N	N	N	N	N
	Access Control (2)	D		N	N	N	N	N	N	N	N
	Secure Comm. Protocol (3)	D	D		N	N	C	C	C	C	C
	Software Upd. Verification (4)	D	D	D		N	N	N	N	N	N
Detection	Host-based IDS (5)	N	N	N	N		N	N	N	N	N
	Network-based IDS (6)	N	N	C	N	N		N	N	N	N
	Physics-based IDS (7)	N	N	C	N	N	N		N	N	N
Mitigation	Detection-triggered IMS (8)	N	N	C	N	D	D	D		N	N
	Self-triggered IMS (9)	N	N	C	N	N	N	N	N		N
Cyber-physical Interdependent Recovery (10)		N	N	C	N	D	D	D	D	D	

D : Dependency, N : Neural, C : Conflict

generators [34]. While the cyber-recovery needs to concern both the physical side's grid energization and cyber side's communication network reestablishment as cyberattacks will first invalidate cyber components and then affect the power supply service. In restoring the infrastructure functionality, the cyber-recovery needs to additionally schedule recovery crews to remove the cyber malware compared with the physical-recovery. Two key challenges of cyber-recovery are thereby identified: i) Particular attention should be paid to the cyber-side modeling and the resultant strong cyber-physical coupling may complicate the recovery schedule problem; ii) Additional attack movements may occur when the adversary perceives the recovery actions. The incorporation of this kind of attack movement usually requires to solve multiple-level optimization problems, posing nontrivial challenges for the solving process.

Pairwise comparisons of the capability between defense-in-depth strategies are summarized in TABLE VII, i.e., how much each defense mechanism supports one another to achieve defense-in-depth protection [215]. In particular, the network segmentation is the most basic cyber prevention technology, and it does not requires dependencies from other technologies. Based on a well-segmented network architecture, an appropriate access control mechanism is developed to grant participators' accesses to resources with different criticality. Then, secure communication protocols are designed to allow entities to transmit information in a secure manner. On top of these three prevention technologies, the code-signing software update scheme is established to guarantee the integrity of installed software. The conflict mainly comes from the computation burden resulted from encryption-enabled secure communication protocols, which may degrade the subsequent detection, mitigation, and recovery performance and even invalidate these functionalities. Moreover, the dependency relation also exists between IDSs and detection-triggered IMSs as well as recovery and IDSs/IMSs.

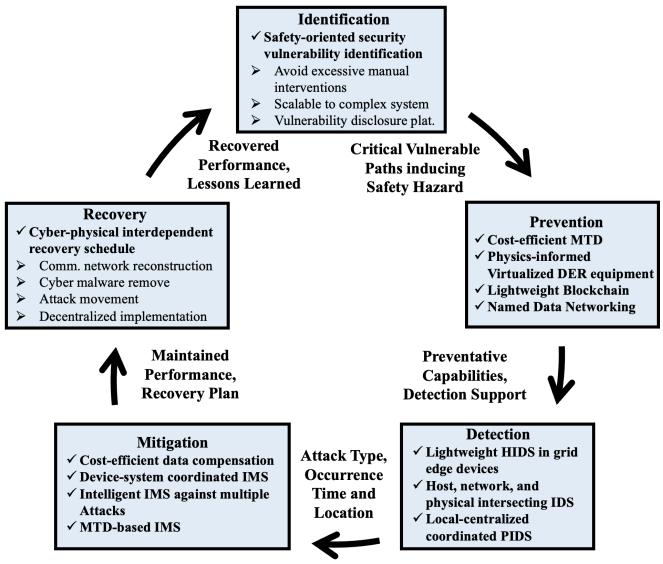


Fig. 14: ComparsionsFuture directions that can further enhance grid resilience.

VIII. Challenges and Future Directions

In this section, challenges and future directions are discussed from six 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 a **high-integrated and automatic** framework to identify vulnerability exploitation paths that can cause critical hazards given specific system

configurations. This research direction is vital as its outputs can identify the most critical parts needed to be protected, 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 challenging as the power system modeling involving various cyber and physical components, complex couplings among them, and strict functionality requirements usually needs substantial manual interventions [216]. Besides, it is of great importance to establish a sharing platform of security issues and cyber vulnerabilities where the participators' privacy will not be leaked by the disclosure of these critical information.

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) **Cost-efficient 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 [128]. The key challenge is how to infer an adversary's action or learn system security condition to guide MTD deployment.

2) **Physics-informed 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) **Lightweight 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) **Named Data Networking**: Inspired by a growing awareness of unsolved problems in contemporary internet architectures like IP, the NDN appears to be promising solution to support cybersecure multi-party communications and control using any communication link [217]. 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) **Lightweight HIDS in 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) **Host, Network, and Physical Intersecting IDS**: 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. Pan *et al.* has made their attempts towards this direction and successfully applied a data mining technique called common path mining to automatically and accurately learn patterns for scenarios, which are used to identify attacks from normal control operations and external disturbances, from a fusion of synchrophasor measurement data, and information from relay, network security logs, and EMS logs [218], [219]. Nevertheless, much more research efforts are needed to address the issues of limited amount of available data, real-time decision-making requirement, and increasingly complicated system dynamics with the penetration of DERs.

3) **Local-centralized coordinated PIDS**: 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**: 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) **Device-system Coordinated IMS**: 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) **Intelligent IMS against Multiple Attacks**: 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. This challenging task may be accomplished by incorporating the advantages of both data-driven and model-based methods.

4) **MTD-based IMS**: MTD-based 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 **cyber-physical interdependent recovery schedule 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, risk assessment, and defense-in-depth strategies encompass the key enablers. First, a hierarchical architecture of the cyber-physical DER-based smart grid was presented to illustrate the actors and their functionalities. An integrated threat modeling methodology was tailored for the hierarchical DER-based smart grid with special emphasises on vulnerability identification and consequence investigation, based on which a general risk assessment matrix can be established to inform the system operator about attack scenarios' severity. Then, the state-of-the-art progresses made in prevention, detection, mitigation, and recovery technologies were comprehensively reviewed, systematically classified, and extensively summarized. It is observed that current CRE-related researches mainly focus on the improvement of security-oriented performance and utilization of local and single-domain resources while rarely consider the restriction of security cost and coordination of multi-layer and cross-domain resources. Based on this, challenges and future directions were highlighted 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," *ACM Computing Surveys*, 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 Journal of Emerging and Selected Topics in Power Electronics*, 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 Transactions on Power Systems*, pp. 1–14, 2022.

[13] R. Arghandeh *et al.*, "On the definition of cyber-physical resilience in power systems," *Renewable & Sustainable Energy Reviews*, 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," *Renewable & Sustainable Energy Reviews*, 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," *Renewable & Sustainable Energy Reviews*, 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," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 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 *2019 International Conference on Power Electronics, Control and Automation (ICPECA)*. IEEE, 2019, 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 *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (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 Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 650–658, 2020.

[31] Appiah-Kubi *et al.*, "Decentralized intrusion prevention (dip) against co-ordinated cyberattacks on distribution automation systems," *IEEE Open Access Journal of Power and Energy*, vol. 7, pp. 389–402, 2020.

[32] Y. Liu *et al.*, "Robust and resilient distributed optimal frequency control for microgrids against cyber attacks," *IEEE Transactions on Industrial Informatics*, 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 Transactions on Smart Grid*, 2022.

[34] C. Wang *et al.*, "Cyber-physical interdependent restoration scheduling for active distribution network via ad hoc wireless communication," *IEEE Transactions on Smart Grid*, 2023.

[35] X. Liu *et al.*, "Towards optimal and executable distribution grid restoration planning with a fine-grained power-communication interdependency model," *IEEE Transactions on Smart Grid*, 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 Transactions on Smart Grid*, 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 Transactions on Power Systems*, 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 Transactions on Power Electronics*, 2022.

[43] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy," *IEEE Access*, vol. 10, pp. 35 846–35 875, 2022.

[44] S. Alliance, "Sunspec der information model specification," *SunSpec Alliance: San Jose, CA, USA*, 2021.

[45] S. T. Bushby *et al.*, "Bacnet today," *ASHRAE journal*, vol. 10, pp. 10–18, 2002.

[46] 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.

[47] "Ieee standard for smart energy profile application protocol," *IEEE Std 2030.5-2018*, pp. 1–361, 2018.

[48] "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.

[49] 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.

[50] "Ieee standard for electric power systems communications-distributed network protocol (dnp3)," *IEEE Std 1815-2012*, pp. 1–821, 2012.

[51] C. Bennett and D. Highfill, "Networking ami smart meters," in *2008 IEEE Energy 2030 Conference*. IEEE, 2008, pp. 1–8.

[52] International Electronic Technical Commission, "Systems interface between customer energy management system and the power management system," 2013.

[53] MITRE ATT&CK, "Ics techniques," (Accessed: 2023).

[54] J. McCarthy *et al.*, "Situational awareness for electric utilities," National Institute of Standards and Technology, Tech. Rep., 2019.

[55] A. Sfakianakis *et al.*, "Enisa threat landscape report 2018: 15 top cyberthreats and trends," vol. 10, p. 622757, 2019.

[56] J.-S. Brouillon *et al.*, "Bayesian error-in-variables models for the identification of distribution grids," *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1289–1299, 2023.

[57] 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.

[58] J. Staggs *et al.*, "Wind farm security: attack surface, targets, scenarios and mitigation," *International Journal of Critical Infrastructure Protection*, vol. 17, pp. 3–14, 2017.

[59] H. Holm *et al.*, "Cyber security for a smart grid-what about phishing?" in *IEEE PES ISGT Europe*. IEEE, 2013, pp. 1–5.

[60] J. Staggs, "Adventures in attacking wind farm control networks," (Accessed: 2023).

[61] S. Taranovich, "Teardown: The power inverter from sunlight to power grid," (Accessed: 2023).

[62] "An1444: Grid-connected solar microinverter reference design," 2023.

[63] 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.

[64] A. Barua *et al.*, "Hall spoofing: A non-invasive dos attack on grid-tied solar inverter," in *USENIX Security*, 2020, pp. 1273–1290.

[65] U. Bayer *et al.*, "Dynamic analysis of malicious code," *Journal in Computer Virology*, vol. 2, no. 1, pp. 67–77, 2006.

[66] National Cyber Security Centre, "Supply chain security guidance," (Accessed: 2023).

[67] S. Oladimeji *et al.*, "Solarwinds hack explained: Everything you need to know," (Accessed: 2023).

[68] L. Bilge and T. Dumitraş, "Before we knew it: an empirical study of zero-day attacks in the real world," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 833–844.

[69] J. Obert *et al.*, "Recommendations for trust and encryption in der interoperability standards," 2019.

[70] S. S. Hussain *et al.*, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5643–5654, 2019.

[71] R. Schlegel *et al.*, "A security evaluation of IEC 62351," *Journal of Information Security and Applications*, vol. 34, pp. 197–204, 2017.

[72] A. Volkova *et al.*, "Security challenges in control network protocols: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 619–639, 2018.

[73] N. Rodofile *et al.*, "Real-time and interactive attacks on dnp3 critical infrastructure using scapy," in *Proceedings of the 13th Australasian Information Security Conference (AISC 2015)*. Australian Computer Society, 2015, pp. 67–70.

[74] N. Jefferies *et al.*, "A proposed architecture for trusted third party services," in *Cryptography: Policy and Algorithms: International Conference Brisbane, Queensland, Australia, July 3–5, 1995 Proceedings*. Springer, 1996, pp. 98–104.

[75] A. A. Almutairi *et al.*, "Web security: Emerging threats and defense." *Comput. Syst. Sci. Eng.*, vol. 40, no. 3, pp. 1233–1248, 2022.

[76] J. Johnson, "A pathway to DER cybersecurity," in *International Conference on the Integration of Renewable & Distributed Energy Resources*, pp. 1–26, 2022.

[77] F. Bret-Mounet, "All your solar panels are belong to me," *DEF CON*, vol. 24, pp. 4–7, 2016.

[78] 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.

[79] 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.

[80] K. Shuaib *et al.*, "Cognitive radio for smart grid with security considerations," *Computers*, vol. 5, no. 2, p. 7, 2016.

[81] X. Yuan *et al.*, "Adversarial examples: Attacks and defenses for deep learning," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 9, pp. 2805–2824, 2019.

[82] M. Jagielski *et al.*, "Manipulating machine learning: Poisoning attacks and countermeasures for regression learning," in *2018 IEEE symposium on security and privacy (S&P)*. IEEE, 2018, pp. 19–35.

[83] ICS-CERT, "Ics alert (ics-alert-14-281-01e), ongoing sophisticated malware campaign compromising ics," 2016.

[84] C. Carter *et al.*, "Cyber security primer for der vendors aggregators and grid operators," 11 2017.

[85] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[86] Cedric Carter, and others, "Cyber security primer for der vendors, aggregators, and grid operators," Sandia National Laboratories, Tech. Rep., 2017.

[87] 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.

[88] F.-X. Standaert, "Introduction to side-channel attacks," in *Secure integrated circuits and systems*. Springer, 2010, pp. 27–42.

[89] L. Jacqueline, "Apt33 targets aerospace and energy sectors and has ties to destructive malware," 2017.

[90] L. Garcia *et al.*, "Hey, my malware knows physics! attacking plcs with physical model aware rootkit." in *NDSS*, 2017, pp. 1–15.

[91] C. Konstantinou *et al.*, "Taxonomy of firmware trojans in smart grid devices," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 2016, pp. 1–5.

[92] H. M. Albunashee *et al.*, "A test bed for detecting false data injection attacks in systems with distributed energy resources," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 1, pp. 1303–1315, 2022.

[93] 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.

[94] A. Cherepanov, "Win32/industroyer: A new threat for industrial control systems," *White paper, ESET (June 2017)*, 2017.

[95] S. Lyngaas, "Utah renewables company was hit by rare cyberattack in march," (Accessed: 2023).

[96] A. J. Gallo *et al.*, "Distributed cyber-attack detection in the secondary control of dc microgrids," in *IEEE European Control Conference (ECC)*, pp. 344–349, 2018.

[97] S. Soltan *et al.*, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," in *USENIX Security*, 2018, pp. 15–32.

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

[99] J. Zhang, L. Guo, and J. Ye, "Cyber-attack detection for photovoltaic farms based on power-electronics-enabled harmonic state space modeling," *IEEE Transactions on Smart Grid*, pp. 1–1, 2021.

[100] M. Liu *et al.*, "False data injection attacks and the distributed countermeasure in dc microgrids," *IEEE TCNS*, vol. 9, no. 4, pp. 1962–1974.

[101] S. Peng *et al.*, "Stealthy data integrity attacks against grid-tied photovoltaic systems," in *2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS)*. IEEE, 2023, pp. 1–7.

[102] Y. Liu *et al.*, "Real-time pricing response attack in smart grid," *IET Generation, Transmission & Distribution*, 2022.

[103] M. Mateski, C. M. Trevino, C. K. Veitch, J. Michalski, J. M. Harris, S. Maruoka, and J. Frye, "Cyber threat metrics," *Sandia National Laboratories*, vol. 30, 2012.

[104] M. Liu *et al.*, "Demo abstract: A hil emulator-based cyber security testbed for dc microgrids," in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2021, pp. 1–2.

[105] C. Cuijpers and B.-J. Koops, "Smart metering and privacy in europe: Lessons from the dutch case," *European data protection: Coming of age*, pp. 269–293, 2013.

[106] R. McAllister *et al.*, "New approaches to distributed pv interconnection: Implementation considerations for addressing emerging issues," 2019.

[107] T. J. Foxon *et al.*, "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.

[108] K. Zhou *et al.*, *Essentials of robust control*. Prentice hall Upper Saddle River, NJ, 1998, vol. 104.

[109] J. Johnson *et al.*, "Distributed energy resource cybersecurity standards development-final project report." Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2022.

[110] EPRI, "Epri security architecture for the distributed energy resources integration network," Accessed: 2023, [Online].

[111] B. C. Neuman *et al.*, "Kerberos: An authentication service for computer networks," *IEEE Communications magazine*, vol. 32, no. 9, pp. 33–38, 1994.

[112] H.-P. Halvorsen, *Structured query language*. University College of Southeast Norway, 2016.

[113] W. Yeong *et al.*, "Lightweight directory access protocol," Tech. Rep., 1995.

[114] P. Rogaway, "Authenticated-encryption with associated-data," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 98–107.

[115] I. T. U. (ITU), "X.509 : Information technology," Accessed: 2023, [Online]. Available: https://www.itu.int/rec/T-REC-X.509.

[116] D. Hankerson *et al.*, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[117] I. Onunkwo, B. J. Wright, P. G. Cordeiro, N. Jacobs, C. F. Lai, J. T. Johnson, T. Hutchins, W. M. Stout, A. D. Chavez, B. T. Richardson *et al.*, "Cybersecurity assessments on emulated der communication networks," Sandia National Lab, Tech. Rep., 2019.

[118] E. Esiner *et al.*, "Lomos: Less-online/more-offline signatures for extremely time-critical systems," *IEEE Transactions on Smart Grid*, vol. 13, no. 4, pp. 3214–3226, 2022.

[119] "Ieee recommended practice for microprocessor-based protection equipment firmware control," *IEEE Std C37.231-2006*, pp. 1–25, 2007.

[120] K. Y. Yap *et al.*, "Blockchain technology for distributed generation: A review of current development, challenges and future prospect," *Renewable & Sustainable Energy Reviews*, vol. 175, p. 113170, 2023.

[121] A. Yildizbasi, "Blockchain and renewable energy: Integration challenges in circular economy era," *Renewable Energy*, vol. 176, pp. 183–197, 2021.

[122] 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.

[123] X. Luo, K. Xue, J. Xu, Q. Sun, and Y. Zhang, "Blockchain based secure data aggregation and distributed power dispatching for microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5268–5279, 2021.

[124] 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.

[125] J. Yang *et al.*, "A proof-of-authority blockchain-based distributed control system for islanded microgrids," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 8287–8297, 2022.

[126] Y. Yu *et al.*, "Blockchain protocol-based predictive secure control for networked systems," *IEEE Transactions on Industrial Electronics*, vol. 70, no. 1, pp. 783–792, 2023.

[127] ——, "Blockchain protocol-based secondary predictive secure control for voltage restoration and current sharing of dc microgrids," *IEEE Transactions on Smart Grid*, vol. 14, no. 3, pp. 1763–1776, 2023.

[128] J.-H. Cho *et al.*, "Toward proactive, adaptive defense: A survey on moving target defense," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 709–745.

[129] R. E. Cox *et al.*, "Artificial diversity and defense security (addsec)," 5.

[130] M. S. Sadabadi *et al.*, "Distributed control of parallel dc–dc converters under fdi attacks on actuators," *IEEE Transactions on Industrial Electronics*, vol. 69, no. 10, pp. 10 478–10 488, 2021.

[131] R. Deng *et al.*, "Defending against false data injection attacks on power system state estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, 2015.

[132] L. Che *et al.*, "Mitigating false data attacks induced overloads using a corrective dispatch scheme," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3081–3091, 2018.

[133] D. Yang *et al.*, "Decied: Scalable k-anonymous deception for iec61850-compliant smart grid systems," in *Proceedings of the 6th ACM on Cyber-Physical System Security Workshop*, 2020, pp. 54–65.

[134] Z. Tang, P. Zhang, and W. O. Krawec, "A quantum leap in microgrids security: The prospects of quantum-secure microgrids," *IEEE Electrification Magazine*, vol. 9, no. 1, pp. 66–73, 2021.

[135] Z. Zhang, R. Deng, D. K. Yau, P. Cheng, and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2320–2335, 2019.

[136] 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.

[137] F. M. Tabrizi *et al.*, "A model-based intrusion detection system for smart meters," in *2014 IEEE 15th International Symposium on High-Assurance Systems Engineering*. IEEE, 2014, pp. 17–24.

[138] X. Liu *et al.*, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2435–2443, 2015.

[139] 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.

[140] 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.

[141] H. Li *et al.*, "Designing snort rules to detect abnormal dnp3 network data," in *2015 International Conference on Control, Automation and Information Sciences (ICCAIS)*. IEEE, 2015, pp. 343–348.

[142] T. H. Morris *et al.*, "Deterministic intrusion detection rules for modbus protocols," in *2013 46th Hawaii International Conference on System Sciences*. IEEE, 2013, pp. 1773–1781.

[143] A. Singh, "Distributed intrusion detection system for modbus protocol," 2020.

[144] B. Kang *et al.*, "Towards a stateful analysis framework for smart grid network intrusion detection," in *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4*, 2016, pp. 124–131.

[145] C. Sun *et al.*, "Cyber attack and defense for smart inverters in a distribution system," in *CIGRE Study Committee D2 Colloquium*, 2019.

[146] C. B. Jones *et al.*, "Unsupervised online anomaly detection to identify cyber-attacks on internet connected photovoltaic system inverters," in *2021 IEEE Power and Energy Conference at Illinois (PECI)*. IEEE, 2021, pp. 1–7.

[147] Y. Zhang *et al.*, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 796–808, 2011.

[148] R. Mitchell *et al.*, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1254–1263, 2013.

[149] J. Hong *et al.*, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 271–281.

[150] A. Bohara *et al.*, "Ed4gap: Efficient detection for goose-based poisoning attacks on iec 61850 substations," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2020, pp. 1–7.

[151] Y. Yang *et al.*, "Multidimensional intrusion detection system for iec 61850-based scada networks," *IEEE Transactions on Power Delivery*, vol. 32, no. 2, pp. 1068–1078, 2016.

[152] P. Jokar and V. C. Leung, "Intrusion detection and prevention for zigbee-based home area networks in smart grids," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1800–1811, 2016.

[153] Y. Kwon *et al.*, "A behavior-based intrusion detection technique for smart grid infrastructure," in *PowerTech*. IEEE, 2015, pp. 1–6.

[154] W. Ren *et al.*, "Edmand: Edge-based multi-level anomaly detection for scada networks," in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2018, pp. 1–7.

[155] J. Kim *et al.*, "Identification of intraday false data injection attack on der dispatch signals," in *SmartGridComm*. IEEE, 2022, pp. 40–46.

[156] A. Mohammad Saber *et al.*, "Anomaly-based detection of cyberattacks on line current differential relays," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4787–4800, 2022.

[157] M. R. Habibi *et al.*, "Detection of false data injection cyber-attacks in dc microgrids based on recurrent neural networks," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5294–5310, 2020.

[158] L. Guo *et al.*, "Cyberattack detection for electric vehicles using physics-guided machine learning," *IEEE TTE*, vol. 7, no. 3, pp. 2010–2022, 2020.

[159] ——, "Data-driven cyber-attack detection for pv farms via time-frequency domain features," *IEEE Transactions on Smart Grid*, vol. 13, no. 2, pp. 1582–1597, 2021.

[160] Q. Li *et al.*, "Adaptive hierarchical cyber attack detection and localization in active distribution systems," *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2369–2380, 2022.

[161] F. Li *et al.*, "Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network," *IEEE Transactions on Power Electronics*, vol. 36, no. 3, pp. 2495–2498, 2020.

[162] Q. Li *et al.*, "Data-driven cyber-attack detection for photovoltaic systems: A transfer learning approach," in *APEC*. IEEE, 2022, pp. 1926–1930.

[163] O. A. Beg *et al.*, "Signal temporal logic-based attack detection in dc microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3585–3595, 2018.

[164] D. Mashima *et al.*, "Securing substations through command authentication using on-the-fly simulation of power system dynamics," in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2018, pp. 1–7.

[165] S. Meliopoulos *et al.*, "Command authentication via faster than real time simulation," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 2016, pp. 1–5.

[166] S. Sahoo *et al.*, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.

[167] L.-Y. Lu *et al.*, "Intrusion detection in distributed frequency control of isolated microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6502–6515, 2019.

[168] 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.

[169] S. Tan *et al.*, "False data injection cyber-attacks detection for multiple dc microgrid clusters," *Applied Energy*, vol. 310, p. 118425, 2022.

[170] O. A. Beg *et al.*, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2693–2703, 2017.

[171] I. Zografopoulos *et al.*, "Detection of malicious attacks in autonomous cyber-physical inverter-based microgrids," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 5815–5826, 2022.

[172] Y. Li *et al.*, "Active synchronous detection of deception attacks in microgrid control systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 1, pp. 373–375, 2017.

[173] T. Huang *et al.*, "Detection of cyber attacks in renewable-rich microgrids using dynamic watermarking," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2020, pp. 1–5.

[174] H. Zhu *et al.*, "Detection-performance tradeoff for watermarking in industrial control systems," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2780–2793, 2023.

[175] M. Liu *et al.*, "Converter-based moving target defense against deception attacks in dc microgrids," *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 3984–3996.

[176] W. Xu *et al.*, "Blending data and physics against false data injection attack: An event-triggered moving target defence approach," *IEEE Transactions on Smart Grid*, vol. 14, no. 4, pp. 3176–3188, 2023.

[177] M. N. Nafees *et al.*, "On the efficacy of physics-informed context-based anomaly detection for power systems," in *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2022, pp. 374–379.

[178] Y. Gao *et al.*, "A physically inspired data-driven model for electricity theft detection with smart meter data," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 5076–5088, 2019.

[179] V. S. B. Kurukuru *et al.*, "Cybersecurity in power electronics using minimal data – a physics-informed spline learning approach," *IEEE Transactions on Power Electronics*, vol. 37, no. 11, pp. 12 938–12 943, 2022.

[180] S. Peng *et al.*, "Localizing false data injection attacks in smart grid: A spectrum-based neural network approach," *IEEE Transactions on Smart Grid*, pp. 1–1, 2023.

[181] Y. Li *et al.*, "Sdn-enabled cyber-physical security in networked microgrids," *IEEE Transactions on Software Engineering*, vol. 10, no. 3, pp. 1613–1622, 2018.

[182] S. Hu *et al.*, "Resilient load frequency control of islanded ac microgrids under concurrent false data injection and denial-of-service attacks," *IEEE Transactions on Smart Grid*, vol. 14, no. 1, pp. 690–700, 2022.

[183] S. Zhao *et al.*, "Dual-triggered adaptive torque control strategy for variable-speed wind turbine against denial-of-service attacks," *IEEE Transactions on Smart Grid*, 2022.

[184] Y. Li *et al.*, "Distributed aperiodic control of multibus dc microgrids with dos-attack resilience," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4815–4827.

[185] A. Saad *et al.*, "On the implementation of iot-based digital twin for networked microgrids resiliency against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5138–5150, 2020.

[186] Y. Jiang *et al.*, "A high-order differentiator based distributed secondary control for dc microgrids against false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 4035–4045, 2021.

[187] M. Shi *et al.*, "Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded ac microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1953–1963, 2021.

[188] S. Zuo *et al.*, "Distributed resilient secondary control of dc microgrids against unbounded attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3850–3859, 2020.

[189] M. R. Habibi *et al.*, "Decentralized coordinated cyberattack detection and mitigation strategy in dc microgrids based on artificial neural networks," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4629–4638, 2021.

[190] 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 Transactions on Power Electronics*, vol. 37, no. 3, pp. 2801–2814, 2021.

[191] J. Zexuan *et al.*, "Distributed data recovery against false data injection attacks in dc microgrids," in *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2022, pp. 265–270.

[192] S. Zhao *et al.*, "Adaptive resilient control for variable-speed wind turbines against false data injection attacks," *IEEE Transactions on Software Engineering*, vol. 13, no. 2, pp. 971–985, 2022.

[193] Q. Zhou *et al.*, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3690–3701, 2020.

[194] W. Zhang *et al.*, "Resilient economic control for distributed microgrids under false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4435–4446, 2021.

[195] N. Yassaie *et al.*, "Resilient control of multi-microgrids against false data injection attack," *ISA transactions*, vol. 110, pp. 238–246, 2021.

[196] S. Abhinav *et al.*, "Synchrony in networked microgrids under attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6731–6741, 2017.

[197] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, "Detection and mitigation of data manipulation attacks in ac microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2588–2603, 2019.

[198] R. Lu *et al.*, "Distributed observer-based finite-time control of ac microgrid under attack," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 157–168, 2020.

[199] B. Huang *et al.*, "A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 2, pp. 880–890, 2021.

[200] Z. Cheng *et al.*, "Resilient collaborative distributed energy management system framework for cyber-physical dc microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 4637–4649, 2020.

[201] J. Zhang *et al.*, "Mitigating concurrent false data injection attacks in cooperative dc microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 8, pp. 9637–9647.

[202] S. Sahoo *et al.*, "Resilient operation of heterogeneous sources in cooperative dc microgrids," *IEEE Transactions on Power Electronics*, vol. 35, no. 12, pp. 12 601–12 605, 2020.

[203] M. Chlela *et al.*, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4702–4711, 2017.

[204] W. Yao, Y. Wang, Y. Xu, and C. Deng, "Cyber-resilient control of an islanded microgrid under latency attacks and random dos attacks," *IEEE Transactions on Industrial Informatics*, 2022.

[205] S. Liu *et al.*, "Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4066–4075, 2018.

[206] S. Hu *et al.*, "Attack-resilient event-triggered controller design of dc microgrids under dos attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 67, no. 2, pp. 699–710, 2019.

[207] Z. Chu *et al.*, "Mitigating load-altering attacks against power grids using cyber-resilient economic dispatch," *IEEE Transactions on Smart Grid*, 2022.

[208] Z. Lian *et al.*, "Distributed resilient optimal current sharing control for an islanded dc microgrid under dos attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4494–4505, 2021.

[209] C. Deng *et al.*, "Distributed resilient secondary control for dc microgrids against heterogeneous communication delays and dos attacks," *IEEE Transactions on Industrial Electronics*, vol. 69, no. 11, pp. 11 560–11 568, 2021.

[210] Y. Chen *et al.*, "A fdi attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1929–1938, 2020.

[211] S. Zuo *et al.*, "Resilient networked ac microgrids under unbounded cyber attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3785–3794, 2020.

[212] M. Bartock *et al.*, "Guide for cybersecurity event recovery," 2016.

[213] W. Yan *et al.*, "Feasibility studies on black start capability of distributed energy resources," 2021.

[214] K. B. Ganesh *et al.*, "Ancillary services from ders for transmission and distribution system operators," in *2022 22nd National Power Systems Conference (NPSC)*. IEEE, 2022, pp. 482–487.

[215] H. C. Tan *et al.*, "Tabulating cybersecurity solutions for substations: Towards pragmatic design and planning," in *2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia)*. IEEE, 2019, pp. 1018–1023.

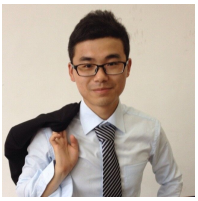
[216] L. M. Castiglione *et al.*, "Ha-grid: Security aware hazard analysis for smart grids," in *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2022, pp. 446–452.

[217] L. Zhang *et al.*, "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[218] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3104–3113, 2015.

[219] U. Adhikari *et al.*, "A cyber-physical power system test bed for intrusion detection systems," in *2014 IEEE PES General Meeting — Conference & Exposition*, 2014, pp. 1–5.

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 Assistant 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.



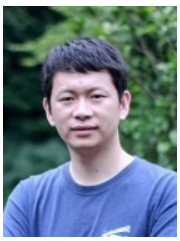
Zhenyong Zhang (Member, IEEE) received his Ph.D. degree from Zhejiang University, Hangzhou, China, in 2020, and bachelor degree from Central South University, Changsha, China, in 2015. He was a visiting scholar in Singapore University of Technology and Design, Singapore, from 2018 to 2019. Currently, 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.

Peng Cheng (M'10) received the B.Sc. and Ph.D. degrees in control science and engineering from Zhejiang University, Hang Zhou, China, in 2004 and 2009, respectively. He is currently a Professor and an Associate Dean of the College of Control Science and Engineering, Zhejiang University. He has been awarded the 2020 Changjiang Scholars Chair Professor. He serves as Associate Editors for the IEEE Transactions on Control of Network Systems. He also serves/served as Guest Editors for IEEE Transactions on Automatic Control and IEEE Transactions on Signal and Information Processing over Networks. His research interests include networked sensing and control, cyber-physical systems, and control system security.



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 on the editorial boards of multiple IEEE TRANSACTIONS.

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.